УДК 343.2/.7
ББК 67.408

DOI 10.22394/1682-2358-2022-2-17-23

G.V. Vershitskaya, *Candidate of Sciences (Law), Docent of the Administrative and Criminal Law Department, Povolzhsky Institute of Management named after P.A. Stolypin, Branch of the Russian Presidential Academy of National Economy and Public Administration*

POSSIBILITIES OF USING VIRTUAL TRACES IN CYBERCRIME INVESTIGATIONS

The legal and forensic aspects of virtual traces collection and use during cybercrime investigations are considered. Modern practice of investigating and solving cybercrime is analyzed. The problems arising in the course of cybercrime investigation are studied.

Key words and word-combinations: cybercrime, virtual traces, digital evidence.

Г.В. Вершицкая, *кандидат юридических наук, доцент кафедры административного и уголовного права Поволжского института управления имени П.А. Столыпина — филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (email: vershickaya@yandex.ru)*

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНЫХ СЛЕДОВ В ХОДЕ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. Рассматриваются правовые и криминалистические аспекты сбора и использования виртуальных следов в ходе расследования преступлений, совершенных с применением информационных технологий. Анализируется современная следственная практика по раскрытию и расследованию киберпреступлений. Изучаются проблемы, возникающие в ходе расследования киберпреступлений.

Ключевые слова и словосочетания: киберпреступления, виртуальные следы, цифровые доказательства.

В последнее время цифровые технологии стали неотъемлемой частью многих жизненных сфер общества. Мир разделился на две части: реальный мир с материальными объектами и виртуальную реальность. Люди, сами того не замечая, погрузились в «дополнительную» действительность всевозможными средствами.

Развитие информационных технологий привело к появлению новых видов преступлений в виртуальной сфере, в специальной литературе получивших название киберпреступлений. С.И. Буз определяет киберпреступление как «любое преступление, совершенное с помощью информационных технологий либо в информационном пространстве» [1].

Действующий УК РФ в главе 28 закрепляет следующие объекты уголовно-правового регулирования, связанные с «киберпространством»: неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1) [2].

Поскольку любое преступление влечет за собой ряд изменений в окружающей обстановке его совершения, называемых в криминалистике следами, то для раскрытия и расследования киберпреступлений возникла необходимость использования виртуальных (или цифровых) следов. В связи с этим в криминалистике образовалось и развивается новое направление исследования преступлений, которые совершаются с применением высоких информационных технологий.

Известно, что следы как источник криминалистически значимой информации подразделяются по виду их носителя на материальные и идеальные. Материальные следы возникают при контактном взаимодействии субъекта или объекта с элементами вещной обстановки окружающей среды (следы рук и обуви, биологические следы, пули и гильзы и др.). Идеальные следы отражают объективную реальность, связанную с событием преступления, в сознании человека и хранятся в его памяти в виде образов, сформированных при восприятии произошедшего события. Место виртуальных следов в общепринятой криминалистической классификации окончательно не определено. В специальной литературе высказываются различные точки зрения по поводу места и роли данных следов в криминалистическом следоведении.

Прежде всего носителями цифровой информации являются материальные объекты с определенными физическими характеристиками (например, жесткие диски, флеш-карты и др.). С другой стороны, цифровая информация — результат мыслительной деятельности конкретного человека, которая может быть обнаружена только с использованием специальных технических устройств и для исследования которой требуются особые знания. В связи с этим можно утверждать, что виртуальные следы с криминалистической точки зрения имеют двойственную природу и могут быть выделены в отдельную категорию, используемую при раскрытии и расследовании киберпреступлений.

По мнению В.Б. Вехова, форма существования виртуальных следов вполне объективна, но опосредована через материальный носитель [3, с. 156].

Виртуальные следы как источники информации о преступлениях, совершенных в виртуальном пространстве, можно классифицировать по различным основаниям. По форме их носителя они могут быть обнаружены на оптических дисках (CD, DVD и пр.), флеш-картах и жестких дисках.

По форме возникновения виртуальные следы можно подразделить на непосредственные (электронные документы, записи в социальных сетях и т.п.) и опосредованные (данные телеметрии).

Виртуальные следы как источник информации о киберпреступлении могут быть обнаружены на устройствах преступника (например, вредоносная программа или шаблоны для поддельных документов), на компьютере потерпевшего (например, функционирующая вредоносная программа), компьютерах других лиц (например, электронная почта организации или учреждения).

Н.А. Зигура дифференцирует цифровую информацию по связи с событием преступления (является ли она средством совершения преступления, объектом преступного посягательства, носителем следов преступления или иной информацией, относящейся к расследуемому уголовному делу) [4, с. 20]. Безусловно, эта классификация имеет важное методическое значение для расследования преступлений, совершаемых в виртуальном пространстве, и именно на ее основе должна разрабатываться частная методика расследования указанных преступлений.

Поскольку киберпреступления — относительно новый вид преступлений, при совершении которых образуется специфическая категория следов в виртуальном пространстве, то к их раскрытию и расследованию требуется особый подход. Установление фактических обстоятельств события преступления и изобличение виновных лиц в соответствии со ст. 73 УПК РФ [5] традиционными криминалистическими приемами, методами и средствами в данном случае малоэффективно. Используемая в настоящее время методика расследования также не обеспечивает высокий процент раскрываемости.

В связи с этим в ходе расследования киберпреступлений правоохранительные органы сталкиваются с рядом проблем, которые обусловлены криминалистическими особенностями данных деликтов. Прежде всего это проблема достоверности информации, содержащейся в виртуальных следах. Киберпреступления совершаются в среде, где существуют различные механизмы анонимности (пароли, шифровки и т.д.), без непосредственного физического контакта преступника с жертвой. Подтвердить правдивость обнаруженной цифровой информации и относимость ее к конкретному преступлению практически не представляется возможным. Для

решения этой проблемы можно воспользоваться международным опытом. Например, регистрация в социальных сетях Китая проводится только с подтверждением личности регистрируемого лица другим пользователем. В случае удаления страницы администрация сети всегда может связаться с человеком, который подтвердил регистрацию, и через него установить личность преступника. Регистрацию в соцсети можно подтверждать также фотографией, которая будет доступна только администрации сайта. В случае необходимости личность интересующего правоохранительные органы субъекта может быть установлена с использованием искусственного интеллекта, например компьютерной системой распознавания лиц [6].

Вторая проблема связана с высокой латентностью киберпреступлений и недолговечностью виртуальных следов. Для этого вида деликтов характерна динамичность способов и возможность совершения одновременно из нескольких мест, с помощью нескольких устройств. Потерпевшие не всегда своевременно обращаются в правоохранительные органы с заявлением о преступлении, что приводит к утрате актуальной цифровой информации, поскольку преступники могут уничтожить виртуальные следы: удалить аккаунт, использованный для совершения преступления, поменять IP-адрес устройства, отключить либо утилизировать устройство, обналичить либо удалить из сети похищенные деньги и т.п. Кроме того, получение криминалистически значимой информации затрудняется из-за того, что сроки ее хранения в сети устанавливаются по усмотрению провайдера и не регламентируются нормативно, как в некоторых зарубежных странах. К тому же обнаруженная цифровая информация может быть изъята только копированием, что не обеспечивает ее сохранности в первоначальном виде и приводит к утрате фактической даты и времени создания. Отсутствие соответствующих правовых норм в действующем уголовно-процессуальном законодательстве может привести к признанию скопированной информации недостоверным доказательством по делу, поскольку такое доказательство было получено не процессуальными средствами и не из процессуальных источников.

Анонимность Интернета порождает также проблему, затрудняющую процесс расследования киберпреступлений, связана она с недостаточностью виртуальных следов для получения информации о личности преступника. Киберпреступник, как правило, находится на большом расстоянии от жертвы, часто на территории другого государства. Какие же следы оставляет он в виртуальном пространстве? По мнению Н.Д. Аскольской, информация о деятельности человека в Интернете содержится в log-файлах, по которым можно определить IP-адрес компьютера преступника, дату создания файла, время его изменения, время последней работы с ним и многое другое [7]. Но log-файлы не содержат информации о местополо-

жении преступника и его личностных особенностях. С определенной долей вероятности можно лишь предположить, что киберпреступник имеет высокий образовательный и интеллектуальный уровень, обладает специальными знаниями в области информационных технологий, навыками психологического манипулирования потенциальной жертвой и умением грамотно уничтожать следы. В большинстве случаев это молодые люди в возрасте 18—30 лет.

Киберпреступления являются новым, малоизученным видом преступлений, совершаемых с использованием информационных технологий. В настоящее время в России деятельность в легальном интернет-пространстве практически не регулируется на законодательном уровне. При этом, кроме общедоступной части Всемирной сети, существует еще так называемый «глубокий Интернет», являющийся платформой для совершения множества различных преступлений — от продажи наркотиков до распространения детской порнографии.

В связи с этим возникает еще одна проблема: противодействие киберпреступности осложняется недостатком практического опыта субъектов криминалистической деятельности по раскрытию и расследованию данной категории преступлений, а также отсутствием специальных знаний в области информационных технологий. Для решения задач расследования правоохранительные органы довольно часто используют помощь специалистов компаний по предотвращению и расследованию киберпреступлений. Например, специалисты российской компании Group-IB привлекаются к участию в проведении процессуальных действий и оперативно-розыскных мероприятий для собирания виртуальных следов и получения доказательств, участвуют в судебных разбирательствах.

Тем не менее, несмотря на перечисленные проблемы, электронная информация активно используется в практике уголовного судопроизводства в качестве доказательств. Следует отметить, что в соответствии с действующим уголовно-процессуальным законодательством доказательства, полученные таким образом, считаются вещественным доказательством либо иными документами. Более того, содержание понятия «цифровое доказательство» не закреплено ни в одном нормативном правовом акте.

На основании положений ст. 84 УПК РФ документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ [5]. Документы, обладающие признаками, указанными в части первой ст. 81 УПК РФ, признаются вещественными доказательствами согласно части четвертой ст. 84 УПК РФ [5].

Однако в контексте виртуальных следов содержание понятий «документ вещественное доказательство» и «иной документ» могут иметь двоякое толкование и даже заменять друг друга. В традиционном понимании документ как вещественное доказательство представляет собой материальный объект, содержащий следы криминального воздействия на его содержание. Иной документ должен содержать информацию о юридически значимых фактах в сущностном содержании на каком-то материальном носителе. В криминалистическом смысле цифровая информация — это зафиксированные компьютерной системой на цифровом материальном носителе данные о совершении каких-либо действий в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей, то есть любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации.

В свою очередь, термин «цифровое доказательство» — это, как представляется, документ в форме, пригодной для восприятия с использованием электронных технологий, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Цифровые доказательства, как и другие его виды, получают в ходе проведения процессуальных действий (например, обыск, выемка, следственный осмотр, судебная экспертиза) и оперативно-розыскных мероприятий. Но информация, полученная оперативным путем, может приобрести статус доказательства только при условии ее оформления с соблюдением требований уголовно-процессуального законодательства [8].

По нашему мнению, с целью повышения эффективности использования виртуальных следов для целей розыска и доказывания по уголовным делам необходимо на законодательном уровне установить правила их собирания, исследования и оценки. Данное требование обусловлено тем, что в силу специфических особенностей виртуальные следы неосязаемы, поэтому для их обнаружения требуются специальные знания в области информационных технологий. Кроме того, виртуальные следы, в отличие от традиционных следов, гораздо легче изменяются и уничтожаются, поэтому своевременность их обнаружения и оперативность исследования с использованием специальных знаний в области информационных технологий и технико-криминалистических средств имеют большое значение для раскрытия и расследования киберпреступлений. Простое копирование обнаруженной цифровой информации на соответствующие носители может существенно повлиять на установление истинных обстоятельств уголовного дела.

Использование виртуальных следов в качестве источников цифровых доказательств в ходе расследования является одним из перспективных

направлений, а разработка криминалистической методики расследования киберпреступлений позволит успешно решать перечисленные проблемы.

Для повышения эффективности противодействия киберпреступности целесообразно активно развивать форензику как одну из отраслей криминалистической техники. Основное внимание следует уделять разработке приемов, методов и средств собирания и исследования виртуальных следов для получения цифровых доказательств в ходе расследования и судебного разбирательства по уголовным делам, связанным с компьютерной информацией. Грамотный подход к проведению следственных действий и оперативно-розыскных мероприятий с целью получения цифровых доказательств позволит не только устанавливать фактические обстоятельства события киберпреступления и изобличать виновные лица, но и выявлять причины киберпреступности. Немаловажное значение при этом приобретает целенаправленная подготовка специалистов в области противодействия киберпреступности для правоохранительных органов.

Библиографический список

1. *Буз С.И.* Киберпреступления: понятие, сущность и общая характеристика. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika/viewer.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 1 июля 2021 г., с изм. и доп., вступившими в силу с 1 дек. 2021 г. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

3. *Вехов В.Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сборник науч.-практ. трудов. М., 2016. № 1.

4. *Зигура Н.А.* Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск, 2010.

5. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ (в ред. от 1 июля 2021 г., с изм. от 23 сент. 2021 г.) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

6. *Вершицкая Г.В., Зябина А.С., Кудашева К.А.* Технология биометрической идентификации: система распознавания лиц // Цифровое будущее: нам жить!: сборник научных трудов. Саратов, 2021. С. 185–191.

7. *Аскольская Н.Д.* Виртуальные следы как элемент криминалистической характеристики компьютерных преступлений. URL: https://cyberleninka.ru/article/n/virtualnye-sledy-kak-element-kriminalisticheskoy-harakteristiki-kompyuternyh-prestupleniy/viewer.

8. *Вершицкая Г.В., Овсянников В.А.* Использование результатов оперативно-розыскной деятельности для раскрытия и расследования мошенничества // Борьба с правонарушениями в сфере экономики: правовые, процессуальные и криминалистические аспекты: сборник материалов международной научно-практической конференции в рамках международного юридического форума «Право и экономика: национальный опыт и стратегии развития». Новосибирск, 2020. С. 18–22.