К ВОПРОСУ О ПОИСКЕ, ОБНАРУЖЕНИИ И ОСМОТРЕ ВИРТУАЛЬНЫХ СЛЕДОВ

Дедковский А. А.
Республика Беларусь, г. Минск
Международный университет «МИТСО»,
заведующий кафедрой уголовно-правовых дисциплин,
кандидат юридических наук, доцент

Осмотр предметов (документов) и его результативность в последнее время играют весомую роль в организации и тактике предварительного расследования в современных технических условиях, собирании доказательств материального и виртуального характера.

Анализ криминалистической и уголовно-процессуальной литературы свидетельствует об отсутствии научных исследований вопросов организации и тактики осмотра электронно-цифровой информации и устройств ее хранения при расследовании общеуголовных преступлений. Как правило, такие исследования и рекомендации учеными и правоприменителями излагаются лишь в контексте расследования киберпреступлений [1–4], по которым и умысел преступников, и следовая картина существенно отличаются от традиционных для нашего общества преступлений.

Не затрагивая вопросов исследования природы и технических аспектов формирования виртуальных следов, отметим уникальность их местонахождения с точки зрения материалистической диалектики – на цифровых носителях информации и способа передачи информации – в виде электромагнитных сигналов по проводным или беспроводным каналам связи. Ошибочное представление некоторых ученых относительно сути виртуальных следов приводит к дискуссии о предмете осмотра их материального носителя как самостоятельного следственного действия. С точки зрения правоприменительной практики для следствия не менее важным является материальное выражение оболочки носителя электронно-цифровой информации. Более того, рассматривая осмотр предмета через призму классической теории криминалистики, которая в первую очередь соотносит это следственное действие с описанием традиционных материальных характеристик (геометрическая форма, цвет, масса, запах, наличие повреждений, индивидуальных

особенностей и т. д.), следы преступления, запечатленные в виде электронно-цифровой информации (видео-, фото- или текстовых файлов) и сохраненные в виртуальном (невозможном к обозрению в физическом смысле) хранилище электронно-цифрового носителя, останутся не обнаруженными и не осмотренными. Поэтому, на наш взгляд, в ходе проведения рассматриваемого следственного действия следует вести речь об осмотре не самого материального носителя, например, смартфона, планшета или flash-накопителя, а электронно-цифровой информации, представленной в виде различного рода файлов, аккумулирующихся в этих носителях. При этом сам носитель выступает лишь в роли средства для ее визуализации.

Наличие правового пробела в части отсутствия следственного действия, позволяющего подвергать осмотру саму электронно-цифровую информацию, а не ее носителя, послужило основанием для нормотворческой инициативы со стороны Следственного комитета Республики Беларусь в 2019 году по дополнению Уголовно-процессуального кодекса Республики Беларусь (далее – УПК) процессуальным действием «осмотр электронной информации» (ч. 2 ст. 173, ст. 203) и установлению регламента по копированию электронной информации в ходе производства осмотра, выемки или обыска (ст. 204, 210).

В зависимости от целей и способов возникновения виртуальных следов к наиболее типичным следует отнести как программное обеспечение, поврежденные файловые данные систем ПК, следы создания, пересылки и запуска вредоносного программного обеспечения, их дистрибутивы, вирусы, так и программные, текстовые и графические файлы, файлы поддержки, мультимедиа (аудио-, видео-), регистрации (log-файлы), хранения сообщений электронной почты и другие файловые данные.

В контексте расследования общеуголовных преступлений наиболее типичными являются такие виртуальные следы, как видео-, аудиофайлы, текстовые файлы (электронная переписка в интернет-мессенджерах, страничка в социальных сетях или посты на выложенную в общий или приватный доступ видеозапись хулиганства), log-файлы, свидетельствующие о создании, передаче видеофайла, наличии на девайсе ПО видеостримингового сервиса и т. д. Специфика их поиска и осмотра во многом связана со способами использования преступниками виртуального

пространства и местом хранения электронно-цифровой информации о событии преступления.

Запечатленное при помощи смартфона или планшета событие, содержащее признаки преступления, может оставаться как в модуле памяти (оперативном запоминающем устройстве – ОЗУ) самого электронного устройства, так и в используемом вместе с ним гаджете, например дополнительной карте памяти (miniSD, microSD, SD – до 4 Гб, SDHC – до 32 Гб, SDXC – до 2 Тб), переносном носителе электронно-цифровой информации (оптическом диске (CD/DVD/Blue-Ray), карте flash-памяти, портативном внешнем жестком диске (HDD) и прочих электронных запоминающих устройствах). В случае использования видеорегистратора, в котором ОЗУ, как правило, отсутствует, электронно-цифровая информация сохраняется на встраиваемую карту памяти (например, miniSD). В целях передачи (распространения) электронно-цифровой информации в виде видеофайлов преступниками в основном используются интернет-мессенджеры, т. е. компьютерные программы, мобильные приложения или web-сервисы, предназначенные для мгновенного обмена сообщениями. Наиболее популярными в настоящее время являются Viber и WhatsApp. В таких случаях в задачи следователя входит не только обнаружение в ОЗУ девайса преступника самого видеофайла с событиями преступления, но и изучение log-файлов, системных файлов постоянного запоминающего устройства (ПЗУ) девайса и содержимого аккаунта интернет-мессенджера, софт которого установлен в электронном устройстве. Их исследование позволит следственным путем установить не только адресатов и точное время отправки видеофайла, но и информацию о потенциальных соучастниках преступления или свидетелях.

В описанных случаях изучению девайсов и гаджетов, как правило, предшествует их изъятие в ходе личного досмотра подозреваемых при задержании в порядке ст. 108 УПК или обыска (выемки), о чем составляется протокол с описанием их названия, цвета и по возможности IMEI.

По целевому предназначению такие электронно-цифровые устройства можно подразделить на две основные группы: девайсы (от англ. device – техническое устройство) и устройства хранения электронно-цифровой информации. Девайсы – это сложные законченные технические самостоятельные устройства, которым для работы нужна лишь энергия в виде аккумулятора или

подключения к сети. Они представляют криминалистический интерес при расследовании преступлений, так как являются средствами преобразования информации о событии преступления в электронно-цифровую форму, хранения и передачи в виртуальное пространство, а также просмотра и визуализации в удобном для восприятия виде. Вторая группа предметов представляет собой технические устройства, предназначенные лишь для хранения и обработки электронно-цифровой информации. Наиболее встречаемыми в следственной практике являются flash-накопители, карты памяти девайса, HDD.

Рассматривая электронно-цифровую информацию как доказательство, следует отметить, что ее допустимость и достоверность могут быть поставлены под сомнение, так как она относится к категории последующих, опосредованных. Соответственно, возможно искажение содержащихся в нем фактов или событий, равно как и при оценке таких идеальных следов преступления, как показаний участников уголовного процесса [5]. В этой связи к специфическим особенностям осмотра электронно-цифровой информации следует отнести целесообразность использования следователями программно-аппаратных комплексов, позволяющих создать побитовую копию электронно-цифровой информации, находящейся как в ОЗУ, так и в ПЗУ девайса.

Таким образом, процесс собирания доказательств в современных высокотехнологичных условиях требует от следователя владения не только навыками частной криминалистической методики расследования преступления, но и минимальными научно-практическими знаниями по применению девайсов (в частности, смартфонов), современных интернет-сервисов по передаче информации в виртуальном пространстве, специализированного оборудования и программного обеспечения, необходимого для поиска следов в виртуальном пространстве, их фиксации и обеспечения сохранности в неизменном виде.

Специфика поиска, обнаружения и осмотра виртуальных следов, равно как и их оценка на предмет достаточности, достоверности и допустимости, заключается в:

особенностях материальной оболочки самого носителя информации;

необходимости создания копии электронно-цифровой информации для ее сохранения в искомом виде и исследования;

месте их нахождения (например, памяти девайса, гаджете, винчестере ноутбука или ПК, резервной копии девайса, ЦОД или дата-центре);

возможности физического изъятия носителя электронно-цифровой информации;

возможности его исследования без подключения к компьютеру или использования специальных программно-аппаратных комплексов;

получении доступа к изучению его виртуального содержимого файловой системы;

необходимости использования технических и программных средств поиска и копирования электронно-цифровой информации;

необходимости использования программного обеспечения, позволяющего сохранить обнаруженные виртуальные следы в неизменном виде.

Список цитированных источников

1. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. – Воронеж : Изд-во Воронеж. гос. ун-та, 2002. – С. 94–119.

2. Краснова, Л. Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09 / Л. Б. Краснова. – Воронеж, 2005. – 24 с.

3. Поляков, В. В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : автореф. дис. ... канд. юрид. наук : 12.00.09 / В. В. Поляков. – Мин-во внутр. дел Рос. Федерации, Ом. акад. – Омск, 2008. – 22 с.

4. Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // Законность. – 2012. – № 8. – С. 43–45.

5. Бикмиев, Р. Г. Собирание электронных доказательств в уголовном судопроизводстве [Электронный ресурс] / Р. Г. Бикмиев, Р. С. Бурганов // Информ. право. – 2015. – № 3. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2020.