"Российский следователь", 2020, N 4

ЦИФРОВАЯ КРИМИНАЛИСТИКА: ОБЪЕКТ И НАПРАВЛЕНИЯ РАЗВИТИЯ

С.Ю. СКОБЕЛИН

Скобелин Сергей Юрьевич, заведующий кафедрой криминалистики Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент.

В статье раскрывается понятие цифровых следов. Рассматриваются основные направления цифровой криминалистики и цифровые следы, используемые в следственной практике.

Ключевые слова: цифровые преступления, расследование, цифровая криминалистика, цифровые следы.

Digital Criminalistics: The Object and Development Areas

S.Yu. Skobelin

Skobelin Sergey Yu., Head of the Department of Criminalistics of the Moscow Academy of the Investigative Committee of the Russian Federation, PhD (Law), Associate Professor.

The article reveals the concept of digital traces. The main areas of digital forensics and digital traces used in investigative practice are considered.

Key words: digital crime, Investigation, digital forensics, digital footprints.

Цифровизация жизнедеятельности человека не могла не отразиться на таком негативном социальном явлении, как преступность, а следовательно, и на способах противодействия этому явлению. Развитие компьютерных технологий, мобильной связи, сети Интернет по всему миру привело к тому, что современный человек уже не мыслит себя без использования электронных технических средств и тех возможностей, которые они дают <1>.

<1> Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. N 3. С. 27.

Ноутбук, планшет, цифровой браслет (часы), электронная книжка, смартфон или простой сотовый телефон имеются практически у каждого взрослого человека и даже ребенка. Все эти электронные устройства напрямую связаны сетью "Интернет", часто синхронизированы. Одним из основных способов передачи информации и общения между людьми (текстовые сообщения, звуковые сигналы, изображения, видео) стали программы мгновенного обмена сообщениями - мессенджеры (WhatsApp, Viber, Telegram, Skype, Facebook, Line, WeChat и др.), социальные сети ("ВКонтакте", Instagram, "Одноклассники", Facebook, Twitter), электронная почта и др.

Многофункциональность и постоянное совершенствование цифровых устройств (гаджетов) только расширяют пользовательские и, соответственно, криминалистические возможности.

В этой связи в криминалистической теории наблюдается тенденция изучения так называемых цифровых (электронных, виртуальных, компьютерных) следов преступной деятельности.

Определены основные направления цифровой криминалистики.

В узком направлении - это предупреждение, раскрытие и расследование собственно преступлений в сфере компьютерной информации (глава 28 УК РФ). Данные преступления (неправомерный доступ к

компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и др.) чаще являются предикатными для совершения (или сокрытия) других преступлений: хищений, распространения экстремистских материалов, фальсификации итогов голосования и др.

В широком направлении - противодействие киберпреступности (в сфере информационных технологий), т.е. не только преступлений, указанных выше, но и совершенных с использованием компьютерных и телекоммуникационных технологий (чаще сети Интернет).

Речь идет о доведении с использованием сети Интернет до самоубийства или склонении к самоубийству; дистанционных хищениях в финансово-банковской сфере; призывах к осуществлению террористической, экстремистской деятельности, массовым беспорядкам; сбыте наркотических средств, оружия; обороте порнографических материалов или предметов, организации азартных игр, преступлениях против половой неприкосновенности несовершеннолетних и др.

При этом темпы роста таких преступлений колоссальны. Согласно данным ФКУ "Главный информационно-аналитический центр МВД России" в 2018 г. <2> количество подобных преступлений составило 132 733 (7% от всех зарегистрированных преступлений), это более чем в два раза (112,7%) превысило аналогичный показатель за 2017 г. Только за 10 месяцев 2019 г. таких преступлений было зарегистрировано 240 200 (14% в общем числе выявленных преступлений), а это на 70% превышает аналогичный период 2018 г. <3>. Представляется, что тенденция увеличения преступлений, совершенных таким способом, будет продолжаться.

<2> URL: https://xn--b1aew.xn--p1ai/reports/item/16053092/.

<3> URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/. Отметим, что в 2019 г. в статистических данных МВД отдельно выделен раздел, посвященный сведениям о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, что еще раз подтверждает актуальность рассмотрения данной темы.

Половина таких преступлений - это тяжкие и особо тяжкие преступления (48,7%), совершенные с использованием сети Интернет (126,3 тыс., или 52,6%), а более трети (38,5%) - с помощью средств мобильной связи (92,4 тыс.).

Относительно видов преступной деятельности в основном (79,0%) это кражи или мошенничества (189,8 тыс.), а также преступления, связанные с незаконным оборотом (производство, сбыт, пересылка) наркотических средств (8,6%).

Актуальность раскрытия и расследования преступлений, где в качестве средств и способов совершения используются информационно-телекоммуникационных технологии, привела к созданию в правоохранительных органах специализированных подразделений: технико-криминалистическое управление, а также специализированные компьютерно-технические и инженерно-технические экспертные подразделения в Главном управлении криминалистики (Криминалистическом центре) Следственного комитета Российской Федерации, управление "К" в МВД России и др.

Анализ следственной практики свидетельствует о том, что цифровые следы в криминалистике следует рассматривать значительно шире. Они актуальны при проведении процессуальных проверок и расследовании любых преступлений независимо от объекта и способа посягательства, категории или формы вины, осведомленности или неосведомленности лица об их оставлении, а также принадлежности тому или иному участнику уголовного процесса (подозреваемому, потерпевшему или свидетелю).

Такие следы понимаются и классифицируются учеными по различным критериям (объекту следоносителя, механизму образования, месту нахождения и др.). Важно, что цифровой след помогает раскрыть преступление, объективно расследовать его. Поэтому практическое значение имеет деление полученной цифровой информации на ориентирующую - помогающую следователю верно выстроить ход расследования, наметить правильные версии, следственные действия, назначить необходимые

экспертизы, и идентифицирующую - имеющую непосредственно доказательственное значение, изобличающее виновных.

В практическом аспекте на сегодняшний день внимание уделяется следующим цифровым следам, наиболее часто используемым в следственной практике при доказывании виновности (невиновности) подозреваемых:

- сведения с камер видеозаписи (съемка с звуковым сопровождением либо без такового может производиться как самими преступниками, так и помимо их воли) подготовки, совершения, сокрытия преступлений;

- биллинговая информация о соединениях между абонентами (абонентскими устройствами);

- информация, содержащаяся в памяти смартфона, телефона участника уголовного судопроизводства <4>;

- криминалистически значимая информация, находящаяся в памяти домашнего (рабочего) компьютера (ноутбука, планшета, моноблока) участника;

- метаданные и иная цифровая информация различных устройств, позволяющая определить местонахождение гаджета и его владельца в интересующее следствие время;

- социальные сети как источник криминалистически значимой информации;

- сведения об истории журналов браузеров пользователя (программ просмотра содержимого сайтов);

- данные дистанционного зондирования поверхности Земли;

- цифровые данные компьютерных систем авто-, мототранспорта в раскрытии и расследовании преступлений (датчики EDR и IV).

<4> Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. N 2. С. 23.

Безусловно, отдельным направлением цифровой криминалистики стали цифровые устройства и программы обнаружения, фиксации, изъятия и исследования следов (не обязательно цифровых), орудий и иных объектов преступной деятельности (цифровые фото-, видеокамеры, микроскопы, эндоскопы, приборы нелинейной и металлолокации, датчики радиоэлектронной обстановки, программы "Конструктор места происшествия" и др.).

Также к группе цифрового обеспечения качественного расследования преступлений относятся современные особенности использования высокотехнологичной техники <5>, специальных программ для работы с цифровыми следами, тактические особенности получения и последующего использования цифровой информации при доказывании виновности (невиновности) лица в совершении преступления.

<5> Шеметов А.К. О понятии виртуальных следов в криминалистике // Российский следователь. 2014. N 20. С. 52.

Грамотные и правильно процессуально оформленные обнаружение, фиксация, изъятие и сохранение цифровой информации в значительной мере способствуют оперативному изобличению всех участников преступного события, розыску и задержанию последних, поиску скрытых трупов, похищенного и в целом обеспечению надежной доказательственной базы для органов следствия.

Литература

1. Багмет А.М. Извлечение данных из электронных устройств как самостоятельное следственное действие / А.М. Багмет, С.Ю. Скобелин // Право и кибербезопасность. 2013. N 2. С. 22 - 27.

2. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности / С.Ю. Скобелин // Российский следователь. 2019. N 3. С. 26 - 28.

3. Шеметов А.К. О понятии виртуальных следов в криминалистике / А.К. Шеметов // Российский следователь. 2014. N 20. С. 52 - 54.

Подписано в печать

01.04.2020