УДК 343.985.3

ЭЛЕКТРОННО-ЦИФРОВЫЕ СЛЕДЫ: КРИМИНАЛИСТИЧЕСКОЕ ПОНЯТИЕ И РОЛЬ В РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫМ СПОСОБОМ

Н. И. Старостенко
Краснодарский университет МВД России,
адъюнкт кафедры криминалистики
e-mail: nstarostenko1996@mail.ru

Аннотация. *В статье рассматриваются аспекты современных проблем понятия и значения электронно-цифровых следов, необходимых для эффективного расследования мошенничеств, совершенных в информационно-телекоммуникационной среде. Целью исследования явился анализ научных взглядов на обозначенную проблематику, а также обоснование своей точки зрения по рассматриваемому вопросу. Установлено криминалистическое понятие электронно-цифровых следов.*

Ключевые слова: *криминалистика, мошенничество, следы, информационно-телекоммуникационная среда, виртуальные среды, электронно-цифровые следы.*

Annotation. *The article examines aspects of modern problems of the concept and meaning of electronic digital traces necessary for the effective investigation of frauds committed in the information and telecommunications environment. The aim of the study was to analyze scientific views on the designated problems, as well as to substantiate their point of view on the issue under consideration. The forensic concept of electronic digital traces has been established.*

Keywords: *Forensic science, fraud, traces, information and telecommunication environment, virtual environments, electronic digital traces.*

В наши дни стремительное развитие вычислительной и телекоммуникационной техники, ежедневно прогрессирующий рост количества пользователей IT-технологий, а также увеличение инновационных возможностей в предоставлении услуг вполне обоснованно привело к тому, что противоправные явления интегрировали в сегмент информационно-телекоммуникационной среды. Глобальная информатизация общества создала благоприятные предпосылки для возникновения новых видов преступлений, а также способов их совершения.

В опубликованных статистических данных МВД России обращается внимание на прогрессирующий рост количества мошенничеств, совершенных с применением IT-технологий. В отчетном периоде (с января 2020 по сентябрь 2020 года) их совершено на 77 % больше, чем год назад, в том числе с использованием сети Интернет — на 93,2 %, при помощи средств мобильной связи — на 97,7 % [1].

Основными источниками криминалистически значимой информации по таким преступлениям являются следы. Благодаря такой информации правоохранительные органы получают данные о событии преступления, позволяющие установить и изобличить преступника. Вот почему изучение механизма образования следов преступления и работа следователя (суда), связанная с их обнаружением и анализом, составляют основу криминалистики. В настоящее время в криминалистической науке, безусловно, стойко утвердилось понятие следа. При этом в широком смысле под следом понимают любые изменения окружающей обстановки, причинно связанные с расследуемым преступлением, а в зависимости от формы отражения их делят на идеальные и материальные [2, с. 49].

Вместе с тем результаты изучения криминалистической литературы свидетельствуют о том, что в настоящее время существует ряд неразрешенных проблем теоретического и практического характера, связанных с определением понятия, места, а также значения электронно-цифровых следов, используемых для эффективного расследования мошенничеств, совершенных в сфере информационно-телекоммуникационных технологий.

Способы совершения деяний рассматриваемого вида предопределяют специфику механизма следообразования и свидетельствуют о дистанционном характере преступлений, что обуславливает необходимость изучения и выявления закономерностей механизма следообразования не только материальных и идеальных следов, но и электронно-цифровых. Так, собранные в процессе предварительного расследования электронно-цифровые доказательства можно использовать для привлечения нарушителей закона к уголовной ответственности. К тому же электронно-цифровые доказательства могут раскрыть механизм совершения преступления, выявить последовательность его совершения, предоставить следствию информацию о случившемся, опровергнуть или подтвердить показания свидетелей и идентифицировать вероятных подозреваемых.

В процессе проведения исследования следов, образованных в информационном пространстве, на практике возникают разного рода проблемные вопросы, вызванные следующими обстоятельствами. Мошенники, стараются приложить максимальные усилия для удаления доказательств их преступных действий из памяти средств сотовой связи, персонального компьютера, а также памяти интернет-браузера, хранящего истории посещения сайтов, ссылки на фишинговые страницы и так далее. А. Л. Осипенко указывает на особую сложность обнаружения электронно-цифровых следов, обуславливая это тем, что данные следы рассматриваются по множеству объектов, таких как компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы [3, с. 187].

Анализируя обозначенные обстоятельства, мы пришли к выводу о том, что формирование и широкое распространение информационных технологий, а также их использование в криминальной деятельности стали основаниями для выделения электронно-цифровых следов в самостоятельную группу следов, принимающих участие в воссоздании картины механизма следообразования рассматриваемых преступлений.

В подтверждение названной позиции об электронно-цифровых следах необходимо учесть мнение П. В. Мочагина, который предлагает к двум традиционным формам следообразования добавить третью, выраженную в закреплении следов в виртуально-информационной и технико-компьютерной сфере [4, с. 89]. С мнением П. В. Мочагина трудно не согласиться, так как развитие информационных технологий вызывает потребность не только в совершенствовании тактики расследования новых преступлений, но и в обновлении современных представлений о механизме следообразования и классификации следов преступной деятельности.

Вместе с тем согласно позиции, высказанной В. А. Мещеряковым, под «виртуальными следами понимаются любые изменения состояния автоматизированной информационной системы (образованного ею кибернетического пространства), связанные с событием преступления и зафиксированные в виде компьютерной информации (т. е. информации в виде, пригодном для машинной обработки). По мнению автора, «виртуальные следы» занимают промежуточное положение между идеальными и материальными следами. В обоснование необходимости выделения следов такого рода В. А. Мещеряков указывает на то, что «виртуальные следы» приближены к материальным следам, так как существуют реально на материальном носителе, их обнаружение и изъятие возможно только с применением программно-технических средств, потому что непосредственно они восприниматься не могут. В то же время включить их в состав материальных следов нельзя, в них существует доля субъективной природы, т. к. зависят они от способа их считывания, не имеют жесткой связи с устройством, осуществившим запись информации, являются весьма неустойчивыми, что приближает их к идеальным следам. Идеальными виртуальные следы также не являются, т. к. хранятся не в памяти человека, а в памяти технического устройства [5, с. 104].

Кроме того, рассматривая сущность таких следов, оставляемых мошенниками в информационно-телекоммуникационной среде при совершении противоправных деяний, можно выделить некоторые их особенности:

1. Электронно-цифровые следы могут быть изменены или уничтожены злоумышленниками, не оставляя при этом никаких явных признаков искажения.

2. Электронно-цифровые следы можно восстановить, их копию исследовать так, как если бы это был оригинал. Зачастую успешной практикой при работе с рассматриваемыми следами считается изучение их копий. Это позволяет избежать риска изменения или повреждения оригинального источника доказательства.

3. При исследовании электронно-цифровых следов можно определить была ли информация подделана или изменена.

4. Электронно-цифровые следы практически невозможно уничтожить. В случае удаления какого-либо файла, его можно восстановить, используя при этом специальные инструменты.

Таким образом, в результате исследования было установлено криминалистическое понятие электронно-цифровых следов, под которыми предложено понимать изменение состояния автоматизированной системы, а также информации, которая содержится в памяти электронно-вычислительных средств (приборов), непосредственно связанных с преступной деятельностью злоумышленника. Отметим, что, в свою очередь, электронно-цифровые следы занимают пограничное положение между идеальными и материальными следами.

Необходимо подчеркнуть, что сотрудники правоохранительных органов часто встречаются с процедурными проблемами, такими как несвоевременное получение доступа к данным на зашифрованных устройствах или в облаке. К тому же необходимо неизменно устанавливать связи между виртуальными и физическими носителями информационных следов и оценивать вероятность получения доказательств по одной теории в сравнении с альтернативными [6, с. 146–151].

Анализ особенностей электронно-цифровых следов ставит перед необходимостью выразить мнение о том, что быстрое развитие технологий и компьютерной преступности вызвало значительный спрос на людей, которые могут собирать, анализировать и интерпретировать рассматриваемые следы более эффективно.

Учитывая данный факт, необходимо привлечение специально подготовленных и обученных лиц в области цифровых расследований, которые могут использовать электронно-цифровые данные для анализа материальных следов предметов, изучение которых позволит извлекать электронно-цифровые следы, хранящие информацию о мотивах, целях преступной деятельности мошенника. Такой специалист, анализируя полученные данные, может получить максимально полную информацию о жертве, мошеннике, а также взаимосвязи мошенника и его персонального компьютера или сотового телефона.

В связи с этим мы пришли к выводу о том, что, несмотря на распространенность электронно-цифровых следов, в нашей стране мало специалистов, ко-

торые на должном уровне обладают специальными знаниями и разбираются в доказательственных и технических вопросах, связанных с рассматриваемыми следами. В результате электронно-цифровые следы часто становятся упущенными из виду следователем либо остаются собранными с различными нарушениями обращения с такими следами и анализируются правоохранителями неверно. Именно поэтому, по нашему мнению, так необходимо развитие цифровой криминалистики, в частности вопросов, касающихся следственных аспектов обработки электронно-цифровых следов.

Обобщая сказанное, требуется сказать о важности и криминалистической значимости постоянного обновления учебных программ в высших учебных заведениях, принимая во внимание тот факт, что повсеместное распространение информационных технологий требует, чтобы каждый сотрудник правоохранительных органов имел более глубокие знания об электронно-цифровых следах. В частности, растет потребность в квалифицированных специалистах, обладающих навыками сохранения цифровых следов, извлечения из них полезной информации и интерпретации этих следов для понимания ключевых аспектов информационно-телекоммуникационного мошенничества. Даже когда сбор, анализ и трактовку цифровых следов выполняет один человек, целесообразно рассматривать эти задачи отдельно, так как каждая область специализации требует различных навыков и процедур, и рассмотрение их по отдельности упрощает определение обучения и стандартов в каждой области. Невозможно переоценить важность общепринятых стандартов практики и обучения в области цифровой криминалистики, поскольку они снижают риск неправильного обращения с доказательствами и ошибок при их анализе и интерпретации. А недостатки, возникающие в процессе обнаружения, исследования, а также сбора электронно-цифровых следов, представляют угрозу для эффективного расследования, предотвращения преступлений в сфере информационных технологий, задержания или преследования правонарушителей.

---

1. Краткая характеристика состояния преступности в Российской Федерации за январь – сентябрь 2020 года [Электронный ресурс] // Официальный сайт МВД. URL: https://мвд.рф/reports/item/21551069/ (дата обращения 12.11.2020). Перейти к источнику Вернуться к статье

2. Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. М. 2001. С. 49. Вернуться к статье

3. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск : Омская академия МВД России, 2009. 480 с. Вернуться к статье

4. Мочагин П. В. Новые формы следообразований в криминалистике и судебной экспертизе // Судебная экспертиза в парадигме российской науки: материалы 54-х криминалистических чтений. М. : Академия управления МВД России. 2013. С. 98. Вернуться к статье

5. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. С. 104. Вернуться к статье

6. Островский О. А. Аспекты современных проблем расследования преступлений, связанных с изъятием цифровых следов и предоставлением соответствующих доказательств // Вестн. Алтайск. акад. экономики и права. № 3. 2019. С. 146–151. Вернуться к статье