УДК 343.98
DOI 10.36511/2078-5356-2021-1-167-172

Старцева Екатерина Александровна
Ekaterina A. Startseva

кандидат юридических наук, доцент кафедры криминалистики
Нижегородская академия МВД России (603950, Нижний Новгород, Анкудиновское шоссе, 3)

candidate of sciences (law), associate professor of the department of criminalistics
Nizhny Novgorod academy of the Ministry of internal affairs of Russia (3 Ankudinovskoye shosse, Nizhny Novgorod, Russian Federation, 603950)

E-mail: Starceva-EA@yandex.ru

Тактические особенности производства следственного осмотра при расследовании мошенничества в сфере компьютерной информации

Tactical features of the production of an investigative examination in the investigation of fraud in the field of computer information

В статье рассматриваются тактические особенности проведения различных видов осмотров в ходе расследования мошенничества в сфере компьютерной информации. Проанализированы проблемные вопросы проведения следственных осмотров. Делаются выводы о необходимости привлечения к проведению рассматриваемых следственных действий соответствующих специалистов.

Ключевые слова: криминалистическая тактика, следственный осмотр, мошенничества в сфере компьютерной информации.

The article discusses the tactical features of various types of inspections during the investigation of fraud in the field of computer information. The problematic issues of conducting investigative examinations are analyzed. Conclusions are made about the need to involve relevant specialists in the investigative actions under consideration.

Keywords: forensic tactics, investigative examination, fraud in the field of computer information.

Когда началось использование первых гаджетов и цифровых сетей, очень мало усилий затрачивалось на то, чтобы защитить их от вторжения. Вскоре стало очевидным, что методология цифровой безопасности абсолютно необходима. Тогда же стало понятно, что системы защиты и контроля информации физических и юридических лиц не исключают на 100% рисков несанкционированного воздействия злоумышленников на информационные активы. Однако цифровая безопасность заключается в добавлении в цифровую сеть (компьютерную сферу) дополнительных слоев, которые предотвращают несанкционированный доступ, а также могут обнаружить и сохранить довольно длинную историю всех доступов и определенных точек входа. Тем более выяснилось, что при проведении сетевого криминалистического анализа (исследования, экспертизы) часто приходится работать *with live systems* — в системе, которую нельзя выключать (маршрутизаторы, переключатели и другие виды сетевых устройств, в том числе и критические серверы).

Тяжело признать, но стало совершенно ясно: только «цифровые следователи» и специалисты в «компьютерной криминалистике» тактически грамотно могут расследовать «цифровые» преступления. Для выполнения подобных задач необходимы отдельные человеческие ресурсы и их 100-процентное вовлечение в процесс расследования. При этом необходима высокая квалификация специалистов — владение методиками и процедурами сбора и представления доказательств, их подачи в компетентные инстанции, знание законодательных нормативов и тонкостей для формирования понятного состава обвинения (в условиях работы со случаями нарушения законодательства в узкоспециали-

зированной сфере, которая обычно недостаточно понятна представителям судебно-административной системы).

Участившиеся случаи мошеннических действий посредством вмешательства в нормальную работу компьютерных сетей и модифицирования компьютерной информации послужили поводом для законодателя России ввести в Уголовный Кодекс Российской Федерации статью 159[6] — мошенничество в сфере компьютерной информации. И не случайно, что при расследовании этих преступлений к числу неотложных и первоначальных следственных действий относятся проведение следственных осмотров: осмотр места происшествия, осмотр компьютерного оборудования и персональных компьютеров, осмотр сервера компьютерной сети и компьютерного хранилища информационных данных, осмотр документарных источников криминалистически значимой информации, хранимых в персональных компьютерах и пр. [1, с. 50]

На сегодняшний день, на наш взгляд, самыми распространенными способами мошенничества в сфере компьютерной информации преступления являются:

1) мошенническое использование регистрационных данных различных учетных записей (app store, google market и т. п.) с последующей их реализацией в криминальных схемах;

2) использование различных интернет-ресурсов (как в российском сегменте сети «Интернет», так и за его пределами) при осуществлении необходимых платежных операций с последующим обналичиванием денежных средств, либо с покупкой товаров, располагая для совершения транзакции необходимыми данными банковской карты жертвы;

3) размещение информации о возможности быстрого получения сверхкрупных прибылей от краткосрочных инвестиций с последующим заключением виртуальных сделок и переводом денежных средств на счет в банке за границей;

4) рассылка вредоносного программного обеспечения либо ссылок на него с последующим хищением денежных средств (их обналичиванием), переводом на другие счета, оплата услуг либо товаров через электронные платежные системы (*Yandex Money, Webmoney, PayPal, Qiwi* и др.);

5) рассылка писем-«спамов» с предложениями с предложениями разного характера — о приобретении медикаментов; надомной работе при условии приобретения жертвой оборудования, комплектующих и прочих принадлежностей (эксперты в области IT-технологий полагают, что ежегодно направляется до 25—30 млн таких писем);

6) создание сайтов-двойников известных интернет-магазинов, проведение электронных торгов (с несуществующими лотами) или «интернет-аукционов» (с целью завышения цены аукционного товара продавцы-мошенники делают на него ставки);

7) проведение благотворительных акций через Интернет с использованием сайтов-двойников реальных благотворительных организаций или счетов конкретных лиц (инвалидов, тяжело больных, нуждающихся в срочных операциях и т. п.).

Дать исчерпывающий перечень способов совершения компьютерных мошенничеств вряд ли возможно. Однако возможно представить эти способы в качестве версий и вывести вероятные следствия в виде следов, которые возможно обнаружить в ходе осмотров мест происшествий.

К следам по делам о мошенничестве в сфере компьютерной информации, по нашему мнению, можно отнести:

— следы человека в местах нахождения конкретного лица в момент совершения преступления (следы пальцев рук на клавиатуре и других компьютерно-технических средствах, следы обуви, слюны, запаховые следы, следы, содержащие ДНК;

— компьютерные следы, которые при любых действиях с компьютерными или иными программируемыми устройствами (мобильными телефонами, смартфонами, планшетами и т. д.) получают свое отображение в электронной памяти.

Логичное положение: осмотр места происшествия является средством проверки версий как о способах мошенничества, так и о субъектах, их совершивших.

Учитывая специфику способов и следов компьютерного мошенничества, нельзя не согласиться с мнением Е.Р. Россинской и А.И. Усова, утверждающих то, что при проведении следственных действий в ходе расследования компьютерных преступлений привлечение специалистов в соответствующей сфере специальных знаний является обязательным. Напрашивается аналогия с частью 1 статьи 178 УПК РФ, в которой регламентируется обязательное участие специалиста в области медицины при осмотре трупа или его эксгумации. Причина понятна — некорректные и непрофессиональные манипуляции с трупом, а равно — с компьютерным оборудованием, компьютерными и информа-

ционно-телекоммуникационными сетями могут повлечь безвозвратную утрату информационных данных, имеющих доказательственную значимость, а кроме того, и прямой ущерб владельцам такой информации [2, с. 93]. Но — и это главное — без специалистов-компьютерщиков на месте осмотра практически невозможно проверить имеющиеся версии или построить новые. Вызов специалиста и порядок его участия в осмотре места происшествия определяются статьей 168 и статьей 270 УПК РФ.

Специалист — довольно активный участник осмотра места происшествия. Он может (с разрешения дознавателя или следователя) задавать вопросы участникам следственного действия, знакомиться с протоколом осмотра, в котором он участвовал, делать заявления и замечания, которые подлежат занесению в протокол; приносить жалобы на действия (бездействие) и решения дознавателя, начальника подразделения дознания, начальника органа дознания, органа дознания, следователя, ограничивающие его права. Специалист не вправе уклоняться от участия в осмотре места происшествия, а также разглашать данные предварительного расследования, ставшие ему известными в связи с участием в производстве по уголовному делу в качестве специалиста, если он был об этом заранее предупрежден в порядке, установленном статьей 161 УПК РФ. За разглашение данных предварительного расследования специалист несет ответственность в соответствии со статьей 310 УК РФ.

Тактически важное обстоятельство: специалист, который участвует в осмотре, возможно, станет экспертом по расследуемому событию преступления. А это значит, что он «как бы для себя» выявляет следы, причинно связанные с преступлением, вполне бережно относится к их сохранности при хранении и транспортировке. Наконец, «как бы сам для себя» определяет предмет экспертизы — вопросы, подлежащие разрешению в ходе экспертного исследования.

Существенное значение имеют данные о месте возможного обнаружения следов рассматриваемого деяния. Учитывая высокую мобильность криминальных элементов и, как следствие этого, мобильность средств компьютерной техники, используемых при совершении данного вида преступлений, стационарность нахождения компьютера — характеристика неустойчивая. Рассматривая характерные особенности функционирования компьютерной сети, следует учитывать, что, с одной стороны, местом совершения мошенничества в сфере компьютерной информации является сама информационно-телекоммуникационная сеть, в которой происходит ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, а с другой стороны, местом совершения мошенничества в сфере компьютерной информации является местонахождение конкретного компьютера, с которого осуществляется неправомерный доступ, именно в этом месте находится основной объем информации, характеризующий процесс совершение преступления (способ, орудия и средства, место, время, обстановка), следовая информация.

Большинство компьютерных мошенничеств совершается на удаленном доступе по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение. Приходится констатировать, что такое положение негативно сказывается на процессе выявления, раскрытия и расследования мошенничества, особенно в тех случаях, когда неправомерный доступ к информации осуществляется из-за рубежа. Кроме телекоммуникационной сети, реального места нахождения компьютера (дополнительных устройств), местом совершения мошенничества является и место «обналичивания» денежных средств, полученных путем обмана (процесс легализации материальных ценностей значительно влияет на характер следообразования).

Технико-криминалистическое обеспечение специалиста, прежде всего — это компьютерное устройство чаще всего представлено в виде переносного персонального компьютера — ноутбука, оборудованного набором специальных компьютерных программ, позволяющих не только выявлять следы преступного вмешательства в компьютерное оборудование, несанкционированного вмешательства в информационные данные, но и при необходимости восстанавливать удаленные или поврежденные электронные ресурсы. Одним из основных требований к специальной компьютерной технике — наличие устойчивой возможности ускоренного копирования информационных данных и их экспресс-анализа на месте проведения осмотра [3, с. 126].

Кроме специального переносного компьютерного устройства, при проведении осмотра места происшествия в процессе расследования мошенничества в сфере компьютерной инфор-

мации в распоряжении следователя должен находиться обязательный набор специального компьютерного оборудования и комплектующих: различные компьютерные шины, шнуры, разнообразные средства накопления больших объемов компьютерной информации — выносные жесткие диски, флэш-накопители информационных данных и пр. Исходя из имеющейся предварительной информации о характере компьютерного мошенничества, механизма его осуществления, типе компьютерного оборудования и персональных компьютеров, используемых как потерпевшими, так и мошенниками, следователь осуществляет подбор накопителей информации для выявления, копирования и последующего хранения на них информационных данных, экспресс-диагностики компьютерного оборудования и сетей.

Реалии нашей жизни дают основания признать частично устаревшим мнение А.В. Касаткина, который в своем диссертационном исследовании в числе проблемных вопросов тактики проведения осмотра места происшествия компьютерного преступления называл недостаточное доверие отдельных сотрудников органа дознания данным, получаемым в ходе экспресс-анализа следов вмешательства в компьютерную информацию и ординарную работу компьютерных сетей. По мнению данного исследователя, тактические промахи при проведении «осмотровых» следственных действий возникают из консерватизма и неприятия новых технологий субъектами деятельности по выявлению и расследованию преступлений [4]. Полагаем, что на сегодняшний день бурное совершенствование компьютерных технологий, проблема недоверия к специальной компьютерной технике себя изжила.

Использование при проведении осмотра места происшествия при расследовании мошенничеств в сфере компьютерной информации видеофиксации дает следователю и суду возможность гораздо более подробно и детально зафиксировать как общую картину места, так его отдельные, содержащие следовую информацию, детали места происшествия. Тактически оправданно фиксировать и участников осмотра (не только специалистов, но и понятых). Одновременно на видео фиксируется весь процесс проведения следственного действия, а также его результаты, выявленные, зафиксированные и подлежащие изъятию материальные следы мошенничества в сфере компьютерной информации.

Информационные данные, имеющие доказательственное значение по уголовному делу о компьютерном мошенничестве, могут находиться не только на жестком диске персонального компьютера. Местом их хранения могут быть оптические компактные диски (CD, CD-R, DVD и пр.), съемные жесткие диски, флэш-накопители, компьютерные планшеты и смартфоны, а также иные технически сложные устройства, имеющие «электронную память» [5, с. 212]. В случае возникновения необходимости изъятия в ходе проведения следственного действия указанных предметов следователь из тактических соображений консультируется со специалистом на предмет визуального обнаружения устройств, включение которых одновременно с компьютерными устройствами или запуском компьютерной сети может инициировать сильное электромагнитное излучение и повреждение (уничтожение) компьютерной информации. При обнаружении такового, следователь обращает на него внимание понятых, узнает у специалиста о возможности устранения данной угрозы и при наличии к тому возможности отключает такое вредоносное устройство, о чем в протоколе делается соответствующая запись.

Иное компьютерное оборудование, не содержащее в своей структуре устройств хранения информации, изъятию не подлежит ввиду нецелесообразности.

Достаточно часто в ходе проведения осмотра места происшествия при расследовании мошенничества в сфере компьютерной информации следователем принимается решение о необходимости изъятия принтера, на котором распечатывались документы, имеющие криминалистическое и доказательственное значение для расследования. С тактической точки зрения изъятие печатающего устройства для последующего направления его на судебную экспертизу на предмет идентификации места изготовления подложных документов имеет смысл и криминалистическую значимость лишь в тех случаях, когда принтер (плоттер) относится к категории матричных или игольчатых. Изъятие струйных и лазерных принтеров с точки зрения криминалистической тактики, и судебной экспертизы зачастую безрезультатны. При наличии в осматриваемом помещении печатающих устройств именно таких типов изъятию подвергаются лишь распечатанные электронные документы из памяти компьютерного хранилища электронных документов, а также распечатки, находящиеся в готовом виде на принтере и непосредственной близости от него, как содержание криминалистически значимую компьютерную информацию [1, с. 83].

Достаточно своеобразной особенностью тактики проведения осмотра места происшествия, в ходе которого изымается компьютерная техника, выступает их упаковка и транспортировка к месту исследования и временного хранения. Жесткие компьютерные диски (винчестеры) не переносят удары и какие-либо внешние механические повреждения. Их перевозка в кузове или багажнике служебного автомобиля может привести либо к утрате компьютерной информации, либо к чрезвычайному усложнению исследовательского процесса [6, с. 959].

Учитывая тактические особенности расследования анализируемых преступлений по результатам проведенного смотра компьютерной техники, в распоряжении следователя должны находиться следующие фотоснимки:

— общий панорамно-ориентирующий снимок персонального компьютера с соответствующими окружающими его периферийными устройствами в обстановке места происшествия;

— более детальный снимок персонального компьютера и его периферии с фиксацией принципа и схемы организации связи между компьютерными устройствами;

— максимального разрешения фотоснимки изображения экрана компьютерного устройства на момент начала осмотрового следственного действия, всех выявленных источников и носителей следовой информации, последнего (перед началом осмотра) распечатанного документа, иных доказательств вещественного характера, выявленных следователем и сотрудниками органа дознания. Для детальной фиксации криминалистически важных и значимых для предстоящего расследования элементов предметов материального мира и носителей следовой информации специалист-криминалист, осуществляющий фотофиксацию процесса и результатов осмотра компьютерной техники, должен использовать тактику выравнивающего освещения. Оно достигается задействованием экранов и отражателей, используемых в профессиональной фотосъемке. В рамках данной методики удается достигнуть выделения и соответствующего затемнения значимых для расследования фрагментов предмета, а тем самым большей контрастности фотоснимка [7, с. 183].

Необходимо учитывать и неукоснительно соблюдать ряд ограничений при проведении осмотра компьютерной техники и элементов компьютерных сетей. В частности, запрещается использование источников сильного электромагнитного излучения, излучателей ультрафиолетового и инфракрасного спектров, специальных материалов, имеющих кислотную или активно щелочную среду [1, с. 62].

Вполне актуально мнение Н.Н. Федорова, полагавшего, что, имея качественную и новую специальную компьютерную технику, криминалист может обойтись лишь этим устройством ввиду его универсального характера [5, с. 28]. В тех случаях когда в процессе проведения осмотра получить доступ к информационным данным, находящимся в памяти осматриваемого персонального компьютера, на выносном жестком диске и прочем, не представляется возможным ввиду установленных электронных средств защиты информации, тактика осмотра требует принятия следователем решения об изъятии персонального компьютера, устройства хранения информации и т. п. Современная специальная компьютерная техника позволяет следователю осуществить не только ускоренное копирование информационных данных и воспроизведение данных с выносного жесткого диска, но и восстановление удаленных данных, поиск сокрытых данных и пр.

Помимо компьютерно-электронной составляющей процесса осмотра персонального компьютера и компьютерного оборудования в ходе проведения соответствующего следственного действия, следователь, руководящий осмотром, не должен оставлять без внимания такие «традиционные» тактические составляющие осмотра, как выявление возможных следов рук, как на клавиатуре компьютера, так и на устройствах выключения компьютерного оборудования, тыльных и боковых сторонах компьютерного оборудования. Криминалистический интерес должны вызывать все рукописные документы и их фрагменты, обнаруженные в ходе осмотра. В полной мере должна быть использована зарекомендовавшая себя криминалистическая методика выявления и фиксации маловидимых следов [8, с. 73].

Особого внимания заслуживает осмотр электронного документа на персональном компьютере. Скриншот монитора компьютера возможен, как и возможна его последующая распечатка на принтере, а также электронное копирование документа на съемный носитель информации. Результаты листинга приобщаются к соответствующему протоколу осмотра [5, с. 17]. В то же время тактически и технически рискованно использовать вещественное доказательство как инструмент для манипулирования в целях фиксации компьютерной информации.

Интернет и компьютерные сети уже давно достигли того уровня, когда мы не можем в полной

мере проанализировать и осмыслить их функционирование. Мы можем понять лишь некоторые фрагменты этой системы, сделать широкие обобщения; но дело в том, что мы, люди, уже создали монстра слишком мощного и сложного, чем можем в полной мере его понять. Учитывая формат публикации, вряд ли возможно указать все имеющиеся тактические особенности при проведении следственных осмотров при расследовании компьютерных мошенничеств, но попытались указать наиболее важные из них.

Примечания

1. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практическое пособие. Изд. 2-е, доп. и испр. М.: ЛексЭст, 2004.

2. Российская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М., 2001.

3. Преступления в сфере компьютерной информации: квалификация и доказывание: учебное пособие / под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2003.

4. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. … канд. юрид. наук. М., 1997.

5. Федотов Н.Н. Форензика — компьютерная криминалистика. М.: Юридический мир, 2007.

6. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Российская Е.Р. Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М.: Норма, 2001.

7. Душенин С.В., Егоров А.Г., Зайцев В.В., Хрусталев В.Н. Судебная фотография / под. ред. А.Г. Егорова. СПб.: Питер, 2005.

8. Криминалистика: учебник / под. ред. А.Г. Филиппова. М.: Высшее образование, 2007.

References

1. Vekhov V.B., Popova V.V., Ilyushin D.A. Tactical features of investigating crimes in the field of computer information: scientific-practical. allowance. Ed. 2nd, add. and rev. Moscow: LexEst Publ., 2004. (In Russ.)

2. Rossiyskaya E.R., Usov A.I. Forensic computer-technical expertise. Moscow, 2001. (In Russ.)

3. Crimes in the field of computer information: qualification and proof: textbook. manual / ed. Yu.V. Gavrilin. Moscow: YI MVD RF Publ., 2003. (In Russ.)

4. Kasatkin A.V. Tactics of collecting and using computer information in the investigation of crimes. Dissertation... candidate of legal sciences. Moscow, 1997. (In Russ.)

5. Fedotov N.N. Forensics — computer forensics. Moscow: Legal world Publ., 2007. (In Russ.)

6. Averyanova T.V., Belkin R.S., Korukhov Yu.G., Rossiyskaya E.R. Forensic science: textbook for universities / ed. R.S. Belkin. Moscow: Norma Publ., 2001. (In Russ.)

7. Dushenin S.V., Egorov A.G., Zaitsev V.V., Khrustalev V.N. Sudebnaya fotografiya / ed. by A.G. Yegorov. St. Petersburg: Piter Publ., 2005. (In Russ.)

8. Forensic science: textbook / under. ed. A.G. Filippov. Moscow: Higher education Publ., 2007. (In Russ.)