Рекомендуемое количество образцов для проведения идентификационной экспертизы – 10–15 распечатанных листов формата А4.

Качество предоставленных образцов зависит от того, насколько полно и объективно они передают признаки лазерного принтера. Обязательным условием в данном случае является наличие образцов, относящихся к тому же временному периоду, что и исследуемый документ, учитывая интенсивность использования лазерного принтера. Определяющим критерием в данном случае выступает частота заправки картриджа, а также факт ремонта или замены частей и механизмов лазерного принтера.

Бумага с образцами и бумага исследуемого документа должны иметь максимально возможное сходство по плотности, цвету, проклейке, характеру поверхности, а также в случае наличия – по рисунку, структуре и цвету защитной сетки и иных элементов защиты или элементов художественного оформления документа.

В процессе предварительного осмотра представленных объектов важным моментом является оценка их состояния, обусловленного соблюдением правил упаковки, хранения и обращения с вещественными доказательствами.

В ходе раздельного исследования необходимо установить факт изготовления исследуемых документов и образцов для сравнительного исследования на лазерном принтере. В изображениях будут наблюдаться следующие признаки: наличие по краям штрихов выступов и точек, наличие сплавленных частиц порошка в штрихах, блеск штрихов при косопадающем освещении, бугристая поверхность в наиболее темных участках штрихов, неравномерная окраска штрихов, наличие мелких точек на пробельных участках, ореол частиц красящего вещества вокруг основных штрихов, осыпание красящего вещества в местах перегиба документа.

К общим признакам лазерных принтеров можно отнести дефекты, вызванные износом комплектующих деталей и механизмов, которые будут наблюдаться в распечатанном документе: полоса хаотично разбросанных вдоль листа точек, серая полоса с нечеткими краями вдоль листа, увеличение насыщенности изображения по краям или в центре листа, тонкая белая полоса с четкими границами вдоль листа, посторонний фон, повторяющийся с одинаковым интервалом либо расположенный на всем листе, белая полоса (чаще по центру листа) с нечеткими границами, ширина которой увеличивается от копии к копии, и т. д.

Ряд дефектов качества печатного текста имеют обыкновение повторяться: на распечатанном листе через определенные периоды повторяются черные полосы, пятна, пробелы и другие дефекты. Данные повторяющиеся дефекты могут являться индивидуализирующими признаками лазерного принтера. При описании данных признаков следует указывать расстояние между группами признаков и направление повторения, расстояние от левого и верхнего краев листа до основного (наиболее заметного) признака, форму основного признака (описывается геометрическая форма, размеры, наличие выступающих элементов и их направление). При описании последующих (менее характерных) признаков их привязывают к основному признаку (расстояние, угол направления относительно вертикали или горизонтали).

При проведении идентификационной экспертизы необходимо учитывать, что на документах, изготовленных при помощи цветных лазерных принтеров, имеются скрытые метки размером около 0,1 мм, окрашенные в желтый цвет и невидимые невооруженным глазом, которые располагаются по всей поверхности документа, в том числе на незапечатанных участках. Данные метки сохраняются даже после замены любых узлов устройства.

Сравнительное исследование в процессе проведения экспертизы осуществляется методами сопоставления и наложения. Недостатком таких методов является низкая точность анализа искажений печати и невозможность получения количественных данных об искажениях печати и достоверной идентификации принтеров.

На наш взгляд, наиболее подходящим для решения данных задач является устройство анализа искажений печати, содержащее последовательно соединенные цифровой сканер, контроллер, блок сдвига цифрового изображения по горизонтали и вертикали, процессор, блок анализа растяжения и сжатия печати и блок идентификации печати. Недостатком этого устройства является невозможность построения карты сдвигов корреляции и, следовательно, невысокая точность идентификации печати принтеров.

Данный недостаток устраняется введением в устройство идентификации печати принтеров блока анализа сдвигов исследуемого изображения, вход которого соединен с контроллером, а выход – с процессором, и блока построения карты сдвигов корреляции, вход которого соединен с процессором. Этим обеспечивается возможность построения карты сдвигов корреляции и повышение точности идентификации печати принтеров. Карта сдвигов корреляции позволяет получить количественные данные об искажениях печати исследуемого документа относительно образцов для сравнительного исследования и, следовательно, сделать вывод от том, изготовлены ли два документа на одном и том же лазерном принтере либо на разных.

Таким образом, для более достоверного и эффективного процесса идентификации лазерных принтеров по печатным текстам наряду с традиционными методами сравнительного исследования необходимо применять автоматизированные устройства и программные комплексы, обеспечивающие получение количественных данных искажений печати.

УДК 343.985

Н.Н. Беломытцев

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПРИ ПОСТУПЛЕНИИ ЗАЯВЛЕНИЙ И СООБЩЕНИЙ О ХИЩЕНИИ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В последние пять лет отмечается значительный рост хищений, совершенных с использованием компьютерной техники: если в 2016 г. было зарегистрировано 1 844 таких преступления, то в 2020 г. – 23 574. В 2019 г. из всего массива уголовных дел, возбужденных по различным частям ст. 212 УК Республики Беларусь, только 15,7 % уголовных дел переданы прокурору

для направления в суд. Сложившаяся ситуация обусловлена рядом объективных и субъективных факторов, к числу которых следует отнести ошибки, допускаемые сотрудниками органов уголовного преследования в ходе проведения осмотра места происшествия при производстве по материалам и уголовным делам, возбужденным по ст. 212 УК Республики Беларусь.

Анализ судебной и следственной практики показал, что по изученным уголовным делам о хищениях имущества путем модификации компьютерной информации осмотр места происшествия проводился по 56 из 231 изученного уголовного дела. При этом 43,9 % опрошенных нами следователей (всего опрошено 176 сотрудников) считают, что осмотр места происшествия имеет наибольшее доказательственное значение при расследовании рассматриваемых хищений.

На наш взгляд, эффективность рассматриваемого следственного действия определяется четкой организацией деятельности сотрудников различных правоохранительных структур, входящих в состав следственно-оперативной группы, соблюдением норм уголовно-процессуального закона, требований криминалистического характера.

На основе анализа судебно-следственной практики полагаем возможным предложить следующий алгоритм действий следователя (лица, производящего дознание) при поступлении заявления, сообщения о хищении имущества путем модификации компьютерной информации.

1. Сообщить оперативному дежурному органа внутренних дел перечень специалистов, которых нужно привлечь к участию в осмотре места происшествия, в том числе ГКСЭ Республики Беларусь, в случае необходимости – работников иных органов и организаций.

В 60,7 % изученных нами уголовных дел при проведении осмотра места происшествия отсутствовали соответствующие специалисты. Данный факт явился одной из причин некачественного и неполного производства следственного действия, что повлекло за собой неустановление всех обстоятельств преступления. Как правило, в качестве специалистов выступают сотрудники подразделений главного управления по противодействию киберпреступности МВД Республики Беларусь.

Согласно ст. 62 УПК Республики Беларусь специалистом является не заинтересованное в исходе уголовного дела лицо, обладающее специальными знаниями в науке, технике, искусстве, ремесле и иных сферах деятельности, вызванное органом, ведущим уголовный процесс, для участия и оказания содействия в производстве следственных и других процессуальных действий. В связи с чем следователю (лицу, производящему дознание) необходимо убедиться в специальной квалификации и профессиональном опыте лица, привлекаемого в качестве специалиста для участия в осмотре места происшествия, а также в его незаинтересованности в исходе уголовного дела.

Сбор соответствующих специалистов должен происходить незамедлительно. Мы разделяем мнение российских исследователей М.В. Старичкова и А.А. Шаевича, что в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации могут входить следователь, желательно специализирующийся на расследовании уголовных дел рассматриваемой категории или смежных составов (как правило, по преступлениям в сфере расследования преступлений против информационной безопасности); специалист-криминалист, знающий особенности работы со следами преступлений данной категории; специалисты по средствам компьютерной техники, информационно-телекоммуникационному оборудованию и сетевым технологиям, системам связи и др.; оперативные сотрудники (подразделений по противодействию киберпреступности, по борьбе с экономическими преступлениями и др.); участковый инспектор милиции, обслуживающий данную территорию; кинолог со служебно-розыскной собакой (если имели место физические манипуляции, например с банкоматом); инспектор по делам несовершеннолетних (если есть основания предполагать, что преступление совершено несовершеннолетним); другие незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта.

2. Четко определить цели и задачи предстоящего осмотра, в том числе для получения новых и проверки имеющихся доказательств; осуществить построение криминалистических версий; определить программно-технические и технико-криминалистические средства для обнаружения, фиксации и изъятия следов преступления, в частности электронно-цифровых. Согласовать их использование с привлекаемым к участию в следственном действии специалистом.

3. По прибытии на место происшествия обеспечить организационную и согласованную деятельность всех членов следственно-оперативной группы, направленную на обнаружение, фиксацию, изъятие и обеспечение сохранности следов (в том числе электронно-цифровых), предметов (программно-технических средств), документов и иных объектов, которые могут быть признаны вещественными доказательствами.

При необходимости поручить сотрудникам органов внутренних дел привлечь к участию в осмотре понятых, иных участников, а также удалить с места происшествия посторонних лиц, если это не было сделано ранее. В зависимости от складывающейся на месте происшествия ситуации в некоторых случаях нужно ограничить доступ персонала, работающего в месте осмотра, ко всем осматриваемым устройствам и элементам электронно-цифровой сети. Целесообразно провести подбор и инструктаж понятых, обладающих необходимыми знаниями в области информационных технологий, а также следует разъяснить их права и обязанности.

Нужно исключить включение-выключение осматриваемых устройств или разрыв соединения между ними, они должны оставаться в неизменном состоянии до окончания осмотра специалистом. Кроме того, специалист должен оказывать помощь следователю (лицу, производящему дознание) в определении границ осмотра места происшествия, предлагать виды, формы и методы применения специальных знаний, технико-криминалистические средства и использовать их с разрешения следователя (лица, производящего дознание).

Осуществить сбор дополнительной исходной информации о системах организации процесса функционирования программно-технических устройств, а также установить те из них, которые могли быть использованы для совершения преступления. Выяснить сведения об изменениях, внесенных в обстановку места происшествия, категории обрабатываемой компьютерной информации (вид и степень ограниченности доступа), а также о действиях потерпевшего, иных лиц до прибытия следственно-оперативной группы. Необходимо также установить факт наличия и применения на месте осмотра (объекте

осмотра) организационных методов защиты информации (порядок осуществления пропускного режима в осматриваемом месте, типичные места хранения электронных носителей информации, возможность проникновения посторонних лиц к осматриваемому месту и др.); технических методов защиты информации (фильтры, экраны на аппаратуру, ключ для блокировки клавиатуры, устройства аутентификации, электронные ключи на микросхемах и др.); программных методов защиты информации (блокировка экрана и клавиатуры, использование средств парольной защиты BIOS и др.).

В случае наличия сведений о лице, предположительно совершившем преступление, нужно сконцентрировать внимание на программно-технических устройствах и предметах, в ходе предварительного осмотра которых можно выявить следы преступной деятельности установленных лиц. В случае отсутствия сведений о лице, совершившем преступление, принять меры по его установлению и розыску с учетом выявленных сведений на месте происшествия.

Таким образом, рассмотренный алгоритм действий в ходе осмотра места происшествия по уголовным делам о хищениях имущества путем модификации компьютерной информации позволяет повысить результативность следственного действия, избежать утери доказательственной информации, с помощью которой возможно установление различных обстоятельств совершенного преступления.

УДК 343.8

П.Л. Боровик

СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ, СОПРЯЖЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Разнообразие современных способов мошенничества с использованием средств электронных платежей диктует необходимость их комплексного изучения с целью выработки научно обоснованных рекомендаций по противодействию им. В контексте растущей общественной опасности данных уголовно наказуемых деяний особую важность приобретает необходимость научного осмысления типичных способов их совершения. Полагаем, что знание таких способов позволит практическому сотруднику более качественно оценить информацию об обстоятельствах уголовно наказуемого деяния в конкретной следственной ситуации и принять верное тактическое и уголовно-процессуальное решение в условиях недостаточной информационной определенности.

Одним из наиболее распространенных способов совершения преступлений указанного вида является фишинг (англ. phishing, от password fishing – выуживание паролей). В классической интерпретации термин означает введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной интернет-системы, предполагающей идентификацию пользователя. Главная задача мошенника – завлечь пользователя на этот сайт и убедить его сообщить идентификационные данные. Для этого злоумышленники используют следующие приемы и методы:

рассылка спама (недобросовестная реклама товаров, которые можно приобрести в интернет-магазине, причем в рекламе обязательно приводится ссылка на сайт магазина-однодневки либо поддельный сайт, визуально неотличимый от настоящего) – осуществляется с помощью СМС-сообщений, электронной почты, рекламных баннеров на веб-сайтах, новостных лент, популярных интернет-мессенджеров (WhatsApp, Viber, Telegram, Facebook), коммуникативно-развлекательных мобильных приложений (Snapchat, TikTok) и социальных сетей (Instagram, «ВКонтакте», Twitter, Tinder и др.);

использование вредоносных программ класса «Троян» (например, Trojan.Win32.DNSChanger), проникающих в компьютер пользователя под видом легитимного программного обеспечения (в данную категорию обычно входят программы, выполняющие различные неподтвержденные пользователем действия – сбор информации о банковских платежных карточках и передача этой информации злоумышленнику, использование ресурсов компьютера в целях майнинга, нелегальной торговли и др.).

Разновидностью фишинга является преднамеренное введение пользователя в заблуждение посредством использования программного обеспечения класса Hoax (англ. – обман) с целью получения финансовой выгоды. Такие программы обычно выдают на экран информацию о несуществующих ошибках в работе компьютера, вынуждая пользователя заплатить деньги, чтобы избавить компьютер от якобы обнаруженных ими угроз. При этом подобные программы чаще всего именно вынуждают, а не предлагают себя приобрести, объявляя пользователю, что иным способом проблему не решить.

Следующим не менее актуальным способом совершения преступления, сопряженного с использованием средств электронных платежей, является фарминг (англ. pharming – скрытное перенаправление на ложный IP-адрес). При его реализации происходит подмена оригинального сетевого ресурса на мошеннический и скрытое перенаправление пользователя на поддельный сайт с целью завладения личными данными пользователя. Посредством использования вредоносных программ класса XSS (англ. Cross-Site Scripting – межсайтовый скриптинг) осуществляется внедрение в выдаваемую веб-системой страницу вредоносного кода либо подмена кэша DNS на конечном устройстве пользователя или на сетевом оборудовании провайдера услуг связи. Возможна также модификация системных настроек (например, перенастройка браузера на работу через троянский прокси-сервер или подмена DNS-сервера провайдера в настройках TCP/IP на троянский DNS-сервер).

Еще одним современным видом мошенничества, направленного на несанкционированное получение доступа к средствам электронных платежей, является взлом сети, составляющей интернет вещей пользователя. Используя специальное программное обеспечение (например, поисковые системы Shodan и Censys), злоумышленники осуществляют поиск незащищенных роутеров, IP-камер, элементов системы «умный дом», носимых смарт-гаджетов и других устройств, использующих установленные по умолчанию логины и пароли либо имеющих иные уязвимости. После чего, подключаясь к этим устройствам, правонарушители получают доступ к персональной информации владельца (сведения об аккаунте, цифровом окруже-