Григорович В. Л., Ходасевич А. В.

ПРОВЕДЕНИЕ ОСМОТРА И ОБЫСКА ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, *lawcrim@bsu.by*

Проведен анализ порядка подготовки и проведения осмотра и обыска при расследовании хищений имущества путем модификации компьютерной информации. Рассмотрены процессуальные основания проведения указанных следственных действий. Предлагаются рекомендации для повышения эффективности результатов проведения осмотра и обыска и меры по обеспечению сохранности полученных данных.

Ключевые слова: компьютерная информация; модификация компьютерной информации; проведение обыска; проведение осмотра; хищение имущества путем модификации компьютерной информации; следственное действие, следы преступления.

Осмотр и обыск при расследовании хищений имущества путем модификации компьютерной информации являются важнейшими следственными действиями, которые проводятся на первоначальном этапе расследования хищения имущества путем модификации компьютерной информации. Информация, полученная в ходе осмотра и обыска, может содержать сведения о следах, позволяющих установить механизм совершения преступления. Поэтому качественное проведение осмотра и обыска при расследовании хищений имущества путем модификации компьютерной информации будет способствовать получению важной криминалистически значимой информации о преступлении.

Отметим, что исследования, посвященные порядку проведения осмотра и обыска по делам о хищениях имущества путем модификации компьютерной информации, представлены в трудах Григоровича В. Л. и Ходасевич А. В. [1], Маркаряна Э. С. [2], Мельника Л. Л. [3–5], Шнейдеровой Д. И. [6, 7] и др.

Осмотр компьютерной информации при расследовании хищений имущества путем модификации компьютерной информации является одним из основных следственных действий, направленных на обнаружение, фиксацию и изъятие цифровых следов.

Суть осмотра заключается в непосредственном исследовании следователем, лицом, производящим дознание, а также другими участниками следственного действия обстановки места происшествия; выявлении, изучении, фиксации и изъятии в установленном законом

порядке материальных объектов и следов на них с целью получения сведений и доказательств, имеющих значение для раскрытия и расследования преступлений, а также событий, содержащих признаки преступления [2, с. 146].

Объекты, подлежащие осмотру компьютерной информации при расследовании хищений имущества путем модификации компьютерной информации, можно разделить на следующие группы:

1. Технические устройства, в памяти которых сохранились электронно-цифровые следы преступления (мобильный телефон или иное компьютерное устройство потерпевшего, подозреваемого (обвиняемого), устройства, в памяти которых сохранились программы для доступа к интернет-банкингу потерпевшего; устройства с приложениями социальных сетей, удаленного доступа, мессенджерами, иными программами, которые использовались при совершении преступления; электронная почта; истории браузеров; флеш-карты; жесткие диски; диски).

2. Ресурсы сети Интернет, доступ к которым осуществляется удаленно (тематические форумы, социальные сети, торговые площадки).

В случае осмотра технического устройства, в памяти которого сохранились цифровые следы, основным исследуемым объектом является компьютерная информация, однако компьютерная информация в данном случае неотделима от технического устройства, соответственно необходимо прибегнуть к осмотру предметов и компьютерной информации.

При осмотре ресурсов в сети Интернет, доступ к которым осуществляется удаленно, вид осмотра будет определяться исходя из того, с какого устройства осуществляется осмотр. Если осмотр осуществляется со стационарного компьютера сотрудника правоохранительного органа, тогда следует прибегнуть к осмотру компьютерной информации, так как стационарный компьютер сотрудника правоохранительного органа не имеет отношение к материалам проверки либо уголовного дела. В случае, если осмотр производится с технического устройства, использующегося при совершении преступления, следует прибегнуть к осмотру предметов и компьютерной информации.

В соответствии с ч. 2 ст. 204-1 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК), осмотр компьютерной информации, доступ к которой осуществляется посредством аутентификации пользователя либо которая содержит информацию о частной жизни лица, сведения, составляющие охраняемую законом тайну, или иную информацию, распространение и (или) предоставление которой ограничено, проводится только с согласия обладателя информации и в его присутствии или по постановлению следователя, органа дознания с санкции прокурора или его заместителя. В случаях, не терпящих отлагательства, осмотр компьютерной информации может быть проведен по постановлению

следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном осмотре.

Анализ положений ч. 2 ст. 204-1 УПК позволяет утверждать, что одним из оснований проведения осмотра компьютерной информации является согласие обладателя информации на проведение осмотра одновременно с его присутствием. Обратим внимание, что на практике обладатели информации в большинстве случаев не возражают против проведения осмотра, самостоятельно предоставляют логины, пароли от устройств, приложений, аккаунтов, однако высказывают мысль о нежелании личного присутствия при проведении следственного действия (невозможность прибытия, потеря личного времени). В связи с этим предлагаем внести соответствующие изменения в ст. 204-1 УПК, указывающие на возможность вынесения постановления о проведении осмотра компьютерной информации в отсутствие обладателя информации при наличии письменного согласия последнего.

Кроме того, считаем необходимым рассмотреть ситуацию, когда технические устройства, в памяти которых сохранились электронно-цифровые следы преступления, изымаются при проведении несанкционированных выемки, обыска, осмотра места происшествия. При осмотре таких устройств сотрудник правоохранительного органа заранее не может знать о том, содержит ли накопитель информацию, распространение и (или) предоставление которой ограничено. Следовательно, во избежание признания полученного доказательства недопустимым, сотрудник правоохранительного органа вынужден получить согласие и привлечь к осмотру обладателя информации или вынести постановление и провести осмотр с санкции прокурора.

По нашему мнению, осмотр компьютерной информации должен быть проведен в соответствии с ч. 2 ст. 204-1 УПК в отношении: личных и служебных технических устройств, а также устройств, которые требуют аутентификации пользователя. Осмотр общедоступной компьютерной информации, а именно: компьютерных устройств, носителей информации, нереализованных торговыми сетями; видеозаписей с камер видеонаблюдения, установленных в местах общего доступа, а также содержащихся в республиканской системе мониторинга общественной безопасности; общедоступных интернет-ресурсов – новостных, развлекательных, личных страниц пользователей в социальных сетях, которые доступны для обозрения другим лицам, должен быть проведен без вынесения постановления о проведении осмотра компьютерной информации, санкции прокурора, а также согласия и присутствия обладателя информации [8].

Актуальным остается вопрос исследования и последующего осмотра информации, полученной в ходе проведения компьютерно-технической

экспертизы и экспертизы радиоэлектронных устройств. В рамках проведения исследования эксперт получает доступ, знакомится и копирует, в том числе, информацию о частной жизни лица, сведения, составляющие охраняемую законом тайну, или иную информацию, распространение и (или) предоставление которой ограничено. При этом согласие и присутствие обладателя информации, получение санкции прокурора на проведение экспертизы не требуется. В связи с этим предлагаем внести соответствующие изменения в ст. 204-1 УПК, указывающие на необходимость получения предварительного согласия обладателя информации на проведение экспертизы либо, в случае несогласия последнего, – получение санкции прокурора на проведение экспертизы.

Обыск по делам о хищениях имущества путем модификации компьютерной информации – неотложное следственное действие, проводимое, как правило, на первоначальном этапе расследования и направленное на поиск и изъятие объектов и цифровых следов, имеющих доказательственное значение для расследуемого уголовного дела, в рамках обследования помещений, иных мест [6].

Основной задачей проведения обыска по делам о хищениях имущества путем модификации компьютерной информации является отыскание технических устройств, которые сохранили цифровые следы преступления.

Субъектный состав участников обыска белорусским уголовно-процессуальным законодательством конкретно не определен, позволяя следователю, лицу, производящему дознание, установить его самостоятельно.

В соответствии с ч. 4 ст. 210 УПК, в необходимых случаях при обыске участвует специалист.

В случае, если техническое устройство выключено, следователю, лицу, производящему дознание, не вызовет трудностей изъять данное устройство и в последующем произвести его осмотр. При изъятии включенного устройства с доступом к сети Интернет ситуация иная.

Так, например, в производстве Фрунзенского (г. Минска) районного отдела Следственного комитета Республики Беларусь находилось уголовное дело №22121081265, возбужденное по ч. 1 ст. 212 УК Республики Беларусь. В рамках возбужденного уголовного дела в ходе проведения обыска сотрудником органа внутренних дел изъят планшет подозреваемого И. с активным сеансом интернет-соединения, а затем передан следователю. При этом, как впоследствии выяснилось, на планшете представляла интерес информация, содержащаяся в аккаунте И. в мессенджере «Телеграм». К осмотру планшета следователь преступил через некоторое время и при проведении следственного действия обнаружил, что аккаунт удален, то есть информация, имеющая значение для расследования уголовного дела, утрачена. В ходе допроса подозреваемый И. сообщил, что

в настройках его аккаунта мессенджера «Телеграм» он установил автоматическое удаление аккаунта при его неиспользовании на протяжении определенного времени [9].

Считаем, что не только в рассматриваемой ситуации, но и в каждом случае при проведении обыска по делам о хищениях имущества путем модификации компьютерной информации необходимо привлекать специалиста.

Данная необходимость выявлена следующими причинами: во-первых, перед началом следственного действия следователь, лицо, производящее дознание, не могут обладать информацией о состоянии технических устройств, подлежащих изъятию и имеющих значение для расследования уголовного дела; во-вторых, у специалиста имеются необходимые принадлежности – наборы отверток, нужные упаковочные материалы, устройства для предотвращения внесения непреднамеренных изменений на жесткий диск; в-третьих, если в ходе обыска возникнет ситуация, при которой следователь, лицо, производящее дознание, выяснят, что не могут самостоятельно изъять либо копировать необходимую информацию, обыск придется окончить, так как приостановление обыска уголовно-процессуальным законодательством не предусмотрено.

Кроме того, при проведении обыска может возникнуть ситуация, при которой подлежащие изъятию технические устройства находятся во включенном состоянии с активным сеансом интернет-соединения, а на мониторе устройств отображается информация (например, переписка в мессенджерах с пособником, потерпевшим; открыты аккаунты подозреваемого в социальных сетях, мессенджерах, доступ к которым в последующем может быть не получен в связи с отказом подозреваемого предоставить логин и пароль), требующая незамедлительного осмотра из-за угрозы ее удаленного уничтожения, видоизменения.

Ч. 13-1 ст. 210 УПК устанавливает, что, при невозможности или нецелесообразности изъятия объекта, содержащего компьютерную информацию, при проведении обыска или выемки может осуществляться ее копирование (фиксация) в отображаемой форме, в том числе создание образа носителя компьютерной информации [8]. Данная норма предоставляет возможность копирования уже отобразившейся информации (например, открытой во вкладке браузера страницы с перепиской) либо копирование путем присоединения своего устройства и создание образа системы, жесткого диска только в случае невозможности или нецелесообразности изъятия объекта.

Таким образом, при возникшей необходимости проведения осмотра устройства, обнаруженного в ходе обыска, согласно действующему уголовно-процессуальному законодательству, следователю, лицу, производящему дознание, необходимо соблюдать следующий порядок:

прекратить проведение обыска и приступить к осмотру компьютерной информации. Если предполагаемая информация связана с частной жизнью лица и подпадает под действие ч. 2 ст. 204-1 УПК, то на проведения такого осмотра необходимо согласие обладателя информации (в случае проведения обыска без санкции прокурора). Такое согласие подозреваемый может не дать, для последующего изъятия осмотренного устройства вновь потребуется вынесение постановление о проведении обыска.

Такой процессуальный порядок значительно затягивает время проведения следственных действий, в связи с чем, по нашему мнению, для обеспечения процессуальной возможности проведения осмотра компьютерной информации при проведении обыска в случаях, не терпящих отлагательств, предлагаем внести соответствующие изменения в ст. 210 УПК.

Обратим внимание, что на практике также возникают ситуации, когда в ходе обыска при изъятии технических устройств зарядные устройства к ним не изымаются. В случае, если изъятое техническое устройство новой марки и (или) модели, зарядное устройство к нему у следователя, эксперта может отсутствовать. В связи с этим вместо осмотра необходимо прибегать к проведению компьютерно-технической экспертизы, что существенно затягивает срок получения необходимой информации.

В ходе проведения обыска по делам о хищениях имущества путем модификации компьютерной информации важно обращать внимание не только на технические устройства. Важно установить наличие: документов (блокнотов, записей и т.д.), которые могут содержать в себе информацию о логинах, паролях, реквизитах банковских платежных карт; бумажных криптокошельков; банковских платежных карт. Указанные объекты также будут способствовать получению важной для расследования дела информации, в том числе позволяющей получить доступ к техническим устройствам.

На основании изложенного отметим, что, осмотр и обыск являются важнейшими инструментами установления обстоятельств расследуемого события и главными процессуальными способами изъятия вещественных доказательств по делам о хищениях имущества путем модификации компьютерной информации [2, с. 146].

Таким образом, можно отметить, что, в связи с тем, что компьютерная информация содержит информацию о частной жизни лица, сведения, составляющие охраняемую законом тайну, или иную информацию, распространение и (или) предоставление которой ограничено, а также в связи с тем, что доступ к компьютерной информации осуществляется посредством аутентификации пользователя, законодатель выделил ее осмотр в самостоятельное следственное действие и установил порядок его проведения. При этом специфика такого следственного действия не была

учтена в полном объеме. С целью устранения возникающих противоречий предлагаем:

1. В случае наличия письменного согласия обладателя информации на проведение осмотра компьютерной информации проводить осмотр такой информации в отсутствие последнего с вынесением при этом постановления о проведении осмотра компьютерной информации в отсутствие обладателя информации.

2. При направлении технического устройства, в памяти которого сохранились электронно-цифровые следы преступления, для проведения компьютерно-технической экспертизы и экспертизы радиоэлектронных устройств, получать предварительное согласие обладателя информации на проведение экспертизы либо, в случае несогласия последнего, – получать санкцию прокурора на проведение экспертного исследования.

Кроме того, по нашему мнению, при проведении обыска по делам о хищениях имущества путем модификации компьютерной информации во всех случаях необходимо привлекать специалиста. Это позволит надлежащим образом изъять обнаруженные технические устройства, а также не утратить информацию, имеющую значение для расследования уголовного дела.

С целью обеспечения процессуальной возможности проведения осмотра компьютерной информации при проведении обыска в исключительных случаях, не терпящих отлагательств, предлагаем внести соответствующие изменения в ст. 210 УПК.

Библиографический список

1. Григорович, В. Л. Проведение обыска при расследовании хищений имущества путем модификации компьютерной информации [Электронный ресурс] / В. Л. Григорович, А. В. Ходасевич // Борьба с преступностью: теория и практика: тезисы докладов XII Международной научно-практической конференции (Могилев, 19 апреля 2024 года) / МВД Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь»; редкол.: А.В. Лубенков (отв. ред.) [и др.]. – Могилев: Могилев. институт МВД, 2024. – С. 194–197.

2. Маркарян, Э. С. Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют / Э. С. Маркарян // Актуальные проблемы российского права, 2018. – № 6 (91). – С. 146–152.

3. Мельник, Л. Л. Осмотр компьютерных систем / Л. Л. Мельник // Проблемы укрепления законности и правопорядка: наука, практика, тенденции, 2020. – № 13. – С. 280–287.

4. Мельник, Л. Л. О некоторых аспектах рабочего этапа обыска при расследовании преступлений, совершенных с использованием токенов и электронных денег / Л. Л. Мельник // Вестник Академии МВД Республики Беларусь, 2022. – С. 147–152.

5. Мельник, Л. Л. Особенности проведения обыска при расследовании преступлений против информационной безопасности [Электронный ресурс] / Л. Л. Мельник // Правовая культура в современном обществе: сборник научных статей / МВД Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь»; редкол.: И. А. Демидова (отв. ред.) [и др.]. – Могилев: Могилев. институт МВД, 2020 – Режим доступа: https://elib.institutemvd.by/bitstream/MVD_NAM/4551/1/melnik.pdf. – Дата доступа: 14.09.2024.

6. Шнейдерова, Д. И. Обыск по уголовным делам о хищениях в сфере оборота криптовалют: тактические и процессуальные проблемы [Электронный ресурс] / Д. И. Шнейдерова // Актуальные проблемы уголовного процесса и криминалистики: сб. науч. ст. / Могилев. ин-т МВД; редкол.: Ю. П. Шкаплеров (председ.) [и др.]. – Могилев, 2023.

7. Шнейдерова, Д. И. Особенности тактики проведения осмотра по делам о хищениях в сфере оборота криптовалют: подготовительный этап [Электронный ресурс] / Д. И. Шнейдерова // Проблемы выявления и раскрытия мошенничеств, совершаемых в сети Интернет: материалы междунар. науч.-практ. конф., Алматы, 14 октября 2022 г. / ООНИиРИР Алматинской академии МВД Республики Казахстан; редкол. А. М. Сайтбеков (гл. ред.) [и др.]. – Алматы, 2022. – С. 107–111.

8. Пянтковский, Г. Р. Уголовно-процессуальный порядок получения доступа к компьютерной информации [Электронный ресурс] / Г. Р. Пянтковский, П. В. Седых // Вестн. Могилев. ин-т М-ва внутр. дел Респ. Беларусь, 2021. – № 2 (4). Режим доступа: https://elib.institutemvd.by/jspui/bitstream/MVD_NAM/5961/1/pjantkovskij.pdf. – Дата доступа: 12.09.2024.

9. Архив Фрунзенского (г.Минска) районного отдела Следственного комитета Республики Беларусь за 2022 г. – Уголовное дело № 22121081265.