

УДК 343.98

В. Л. Григорович

*доцент кафедры криминалистики юридического факультета
Белорусского государственного университета,
кандидат юридических наук, доцент*

А. В. Ходасевич

*аспирант юридического факультета
Белорусского государственного университета*

ПРОВЕДЕНИЕ ОБЫСКА ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

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, что позволяет следователю, лицу, производящему дознание, установить его самостоятельно.

В соответствии с ч. 4 ст. 210 Уголовно-процессуального кодекса (далее — УПК) Республики Беларусь, в необходимых случаях при обыске участвует специалист [1].

В случае если техническое устройство выключено, следователю, лицу, производящему дознание, не составит 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, возбужденное по ч. 1 ст. 212 Уголовного кодекса Республики Беларусь [2]. В рамках возбужденного уголовного дела в ходе проведения обыска сотрудником органа внутренних дел был 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 приступил 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.

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 обусловлена 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.

Часть 13¹ 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. Данная норма предоставляет возможность копирования уже отобразившейся информации (например, открытой во вкладке браузера страницы с перепиской) либо копирования путем присоединения своего устройства и создания образа системы, жесткого диска только в случае невозможности или нецелесообразности изъятия объекта [1].

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:

1. Прекратить проведение обыска и приступить к осмотру компьютерной информации. Если предполагаемая информация связана с частной жизнью лица и осмотр компьютерной информации подпадает под действие ч. 2 ст. 204¹ УПК, то на проведение такого осмотра необходимо согласие обладателя информации (в случае проведения обыска без санкции прокурора). Такое согласие подозреваемый может не дать.

2. Для последующего изъятия осмотренного устройства вновь потребуются вынесение постановления о проведении обыска [1].

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, 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. Кроме того, 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.

Список основных источников

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 17.07.2023 г. Доступ из информ.-поисковой системы «ЭТАЛОН». [Вернуться к статье](#)

2. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 09.03.2023 г. Доступ из информ.-поисковой системы «ЭТАЛОН». [Вернуться к статье](#)