УДК 343.9.01

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОБЫСКА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л. Л. Мельник
следователь по особо важным делам,
главное следственное управление
Следственного комитета Республики Беларусь
e-mail: l_melnik@sk.gov.by

Аннотация. *В статье на основе анализа практического опыта следователей центрального аппарата Следственного комитета Республики Беларусь определены особенности тактики проведения обыска при расследовании преступлений против информационной безопасности, способствующие ее совершенствованию.*
Ключевые слова: *компьютерная техника, тактика проведения обыска, электронные следы, носители электронной информации, доказательство.*

Annotation. *Based on the analysis of the practical experience of investigators of the Investigative Committee of the Republic of Belarus, the author identifies the features of the search tactics during the investigation of thecrimes against information security that contribute to its improvement.*
Keywords: *computer equipment, search tactics, electronic tracks, electronic information carriers, evidence.*

Состояние криминогенной обстановки по направлению деятельности подразделений МВД Республики Беларусь в сфере высоких технологий за 2019 г., в сравнении с предыдущими периодами, указывает о значительном увеличении (в 2,2 раза; с 4 741 до 10 539) количества зарегистрированных киберпреступлений [1]. Значительный рост данных преступлений требует повышения качества расследования, одной из мер которого является совершенствование тактики производства обыска по вышеуказанным уголовным делам.

Главной особенностью проведения обыска по таким уголовным деламявляются объекты, подлежащие изъятию, которые имеют «цифровое» происхождение и в дальнейшем при наличии оснований могут являться «электронными» доказательствами.

Перед проведением обыска на его подготовительном этапе лицо, которое его будет осуществлять, с целью получения и сохранности «электронных» доказательств обязано провести ряд действий и мероприятий, направленных на получение необходимого материального обеспечения, на предварительное изучение личности лица, у которого будет производиться обыск, а также на изучение обстановки места его проведения, в том числе:

- обеспечить наличие необходимого оборудования (отвертки, антистатические пузырчатые обертки, иные упаковочные материалы (следует избегать пенопласта, так как он вызывает статическое электричество), служебные съемные жесткие диски, устройства для предотвращения внесения непреднамеренных изменений на жесткий диск (для целей работы с данными на месте обыска), фото- и видеокамеры для съемки места обыска и изображений на экране устройств), перчаток;

– планировать количество сотрудников, участвующих в обыске, позволяющее выполнить задачу по сохранности изымаемой техники, контроля окружающей обстановки, для пресечения попытки сокрытия лица, у которого производится обыск;

– изучить нахождение компьютерной техники по месту предполагаемого проведения обыска, на которой, по мнению следствия, могут иметься «электронные» доказательства. Данный аспект является важным при проведении обысков в момент пользования преступником компьютерной техники, в том числе при доступе в сеть Интернет, так как задержка с обеспечением сохранности данной техники и сведений на ней в момент начала проведения обыска может повлечь уничтожение доказательств.

Далее лицу, проводящему обыск, на поисковом этапе его проведения, необходимо:

– запретить доступ к компьютерной технике, а также к ее источникам питания лицам, по месту нахождения которых проводится обыск;

– использовать защитные перчатки, чтобы избежать уничтожения следов человека, а также обеспечить успешный сбор следов, пригодных для идентификации личности по следам рук и ДНК, в случае если это будет вызвано необходимостью по уголовному делу;

– используя эффект неожиданности, выяснить у лиц, находящихся по месту производства обыска, реквизиты доступа к мобильным телефонам, компьютерной технике, которая находится в месте его проведения, наличие зашифрованной информации на данной технике, пароли доступа к указанной информации;

– проверить рабочее состояние компьютерной техники (к указанной категории в данном случае относятся стационарные ПЭВМ и ноутбуки). Если компьютерная техника выключена, ее включать не надо, так как ее запуск приведет к изменению данных на ней и может уничтожить доказательства. В случае, если компьютерная техника выключена, необходимо извлечь из неекабель питания, при этом не следует его извлекать первоначально из розетки и подготовить таким образом ее к изъятию. Что касается действий следователя при обнаружении ноутбука, то необходимо достать из него батарею. В некоторых устрой-

ствах есть дополнительные батареи, которые находятся в многофункциональном отсеке на месте оптического дисковода, их также следует извлекать. Операционные системы Windows Server, Unix, Linux, macOS, по возможности необходимо выключить с помощью специальной команды shutdown;

– в случае если компьютерная техника работает, проверить ее подключение к сети Интернет. Далее необходимо зафиксировать посредством фотовидеосъемки снимок экрана монитора, в том числе работающие программы. Затем действия лица, производящего обыск, зависят от следственной ситуации, которая сложилась к данному моменту.

При первой следственной ситуации, когда подозреваемый выражает согласие на сотрудничество со следствием и своими действиями подтверждает это, а также имеются основания полагать, что «электронные» доказательства на компьютерной технике будут в сохранности и не будет запрета на доступ к ним, с компьютерной техникой следует произвести те же действия, как и в случае если бы она была выключена.

Вторая следственная ситуация возникает, когда у лица, которое проводит обыск, появляются основания предполагать, что «электронные» доказательства на обнаруженной компьютерной технике могут быть уничтожены, или оно больше не получит доступ к ним при их дальнейшем осмотре после изъятия. Данные основания возникают в следующих случаях: 1) лицо, у которого производится обыск, категорически отрицает ранее достоверно установленные факты своей преступной деятельности или пользования компьютерной техникой, обнаруженной по месту проведения обыска; 2) у лица, производящего обыск, имеются основания полагать об утаивании лицом, у которого производится обыск, какой-либо информации по делу; 3) имеются сведения об иных соучастниках или осведомленных лицах, которые могут удаленно уничтожить «электронные» доказательства на обнаруженной компьютерной технике или в сети Интернет; 4) в ходе визуального осмотра монитора компьютера установлено, что его операционная система, возможно, зашифрована специальными компьютерными программами (Veracrypt, Truecrypt или иными), а пароль доступа к ней не обнаружен. При наличии вышеуказанных оснований следует предпринять действия по сохранению доказательств, находящихся на компьютерной технике. С этой целью посредством специального оборудования — аппаратного или программного блокираторов (например, торговой марки Tableau), которое позволяет не вносить каких-либо изменений на исследуемый носитель информации, осуществить присоединение к данной компьютерной технике служебного носителя электронной информации без каких-либо сторонних записей на нем, после чего осуществить копирование на него информации в объемах, необходимых для сохранения всех возможных «электронных» доказательств по уго-

ловному делу. После окончания копирования в протоколе обыска необходимо указать объем скопированной информациии, ее контрольную сумму. Затем компьютерная техника может быть выключена вышеуказанным способом. Служебный носитель информации с записанными на него сведениями описывается в протоколе обыска и подлежит изъятию.

Частным случаем второй следственной ситуации является использование в преступной деятельности удаленных интернет-ресурсов и учетных записей на них, информация на которых может быть уничтожена или доступ к ней может быть заблокирован без оперативного ее сохранения. Примером этой ситуации может служить обнаруженная на компьютерной технике переписка в интернет-мессенджере Telegram, в связи с чем необходимо вышеуказанным способом осуществить выгрузку данных сведений на служебный носитель информации.

При обнаружении и изъятии RAID-систем (представляют собой аппаратные решения для хранения данных: выделенное аппаратное оборудование для хранения данных с двумя или более дисками (HDD, SSD, SSHD), обычно конфигурируемые в матрице RAID) лицу, производящему обыск на поисковом этапе, следует:

– осуществить поиск кабелей сети передачи данных и кабелей питания, в том числе в других помещениях обыскиваемых помещений или в подозрительных зонах. Как правило, этот тип решений для хранения данных чаще всего используется в центрах обработки данных, однако из-за упрощенного подключения его также можно найти в частных помещениях, в изолированных областях (чердаки, подвалы, поддельные стены и т. д.), требующие только кабель питания и, возможно, также кабель для передачи данных для подключения к сети (если оборудование не обеспечивает беспроводную связь);

– изъять запоминающие устройства вместе с аппаратным устройством, в котором они установлены.

При обнаружении и изъятии мобильных устройств (мобильные телефоны, планшеты) лицу, производящему обыск, следует:

–если устройство мобильной связи выключено, не включать его. Проверить наличие SIM-карты и указать в протоколе ее серийный номер. Аналогичны действия к картам памяти (miniSD, microSD), а также номерам IMEI.

– если устройство мобильной связи включено, следует переключить его в режим «полета», чтобы минимизировать непреднамеренное изменение записей в его памяти, а также избежать удаленной блокировки и удаления информации, содержащейся на нем.

Важным в ходе обыска является определение и иных, на первый взгляд, не представляющих значение объектов — носителей «электронных» доказательств. Определить данные объекты можно как физические устройства, со-

держащие встроенную электронику, которая подключает это устройство удаленно или через сеть к локальной сети, сети Интернет или обоим (Интернет вещей). Примерами данных объектов являются: аппаратура «умный дом», промышленные роботы, системы сигнализации, датчики / системы управления движением. Большинство таких устройств предоставляют, по крайней мере, информацию о том, когда они использовались. В некоторых случаях данные сведения помогут понять образ действий, их последовательность, иногда (не) проверять алиби лиц.

При обнаружении и изъятии объектов, относящихся к Интернету вещей, лицу, производящему обыск, необходимо осуществить следующие действия:

– ввиду того, что некоторые устройства создают свои собственные незащищенные точки доступа Wi-Fi или пытаются подключиться через Bluetooth, следует, чтобы все лица, участвующие при проведении обыска, отключили функции Wi-Fi и Bluetooth на своих собственных мобильных устройствах. В противном случае их устройства могут подключаться к незащищенным сетям и изменять данные (например, создавать новые записи журнала, перезаписывать старые записи журнала устройств) или даже инициировать действия;

– если это возможно, проанализировать информацию о данных устройствах во время их работы, поскольку большинство таких устройств теряют часть своих данных при выключении.

Как показывает практика, кроме источников «электронных» доказательств, поиск иных предметов и документов может предоставить следствию данные для последующего анализа устройств — источников «электронных» доказательств. Это могут быть «неэлектронные», но связанные с ними доказательства, такие как: пароли и другие заметки, отображенные на бумажных носителях информации, руководства по использованию аппаратного и программного обеспечения, бумажные кошельки для криптовалют, банковские платежные карточки. В совокупности указанные объекты способствуют установлению новых обстоятельств, в том числе предоставляют доступ к «электронным» доказательствам.

На заключительном этапе обыска следует уделить особое внимание упаковке изымаемых предметов. Ввиду их хрупкости вышеуказанные носители «электронных» доказательств следует упаковывать в картонные коробки или бумажные пакеты, а не в пластиковые материалы, и отдельно от других доказательств.

Таким образом, использование вышеуказанных тактических мер следователями и сотрудниками органа дознания при проведении обыска у лиц, совершивших преступления против информационной безопасности, будет способствовать получению доказательств по уголовному делу, которые в своей сово-

купности будут являться основанием для привлечения к установленной законом ответственности виновных лиц и тем самым способствовать в борьбе с указанными преступлениями.

1. Статистика УРПСВТ [Электронный ресурс]. URL: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt (дата обращения: 28.02.2020). Вернуться к статье