УДК 34.343

Кирилл Владимирович ПРЯНИК
Санкт-Петербургский государственный университет
79217479359@yandex.ru

ПРОЦЕССУАЛЬНО-КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ РАБОТЫ СЛЕДОВАТЕЛЯ С НОСИТЕЛЯМИ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

PROCEDURAL AND FORENSIC ASPECTS OF AN INVESTIGATOR'S WORK WHILE EXAMINING ELECTRONIC STORAGE DEVICES

В статье рассматриваются проблемы законодательной регламентации и практической реализации изъятия и исследования информации, содержащейся в памяти электронных устройств, в целях получения доказательств при расследовании преступлений.

The article considers the issues of legislative regulation and practical implementation of seizing and examining information from electronic storage devices for the purpose of obtaining evidence in criminal investigations.

Ключевые слова: *информация, электронное устройство, следственные действия, изъятие, осмотр.*

Keywords: *information, electronic device, investigative activities, seizure, examination.*

На сегодняшний день электронная аппаратура (мобильные телефоны, смартфоны, компьютеры, портативные устройства GPS или ГЛОНАСС, цифровые фотоаппараты и видеокамеры, видеорегистраторы, платежные терминалы и пр.) все чаще используется при подготовке, совершении и сокрытии преступлений, а также может являться средством совершения преступления. Информация о событиях преступного деяния порой фиксируется на цифровые устройства без направленности на это воли субъектов преступлений. Следовательно, особую актуальность получил вопрос, связанный с обнаружением, фиксацией, изъятием и исследованием электронных следов, полученных из памяти электронных устройств, содержащих какую-либо информацию о преступлении.

Представляется, что существуют определенные проблемы, связанные с самим изъятием таких следов, а именно регламентацией процедуры такого изъятия и легализацией результатов изъятия в качестве доказательств по уголовному делу, а также с нарушением прав человека на частную жизнь.

Первая – проблема регламентации процедуры изъятия электронного устройства и изъятия информации из его памяти. Электронные носители информации могут признаваться вещественными доказательствами по уголовному делу (п. 4 ч. 2 ст. 74 УПК РФ), следовательно, могут быть изъяты в ходе следственных действий. В соответствии с положениями ч. 9.1 ст. 182 и ч. 3 ст.183 УПК РФ при производстве выемки или обыска для осуществления изъятия

электронного носителя информации обязательно участие специалиста. Отметим, что обязательность участия специалиста установлена законодателем в силу того, что необходимо соблюсти технически верный способ изъятия таких объектов, поскольку не каждый следователь обладает специальными знаниями для работы с электронно-вычислительной техникой. В рамках данной проблемы нам представляется необходимым расширить перечень таких следственных действий, при которых возможно изъятие электронного носителя информации, т.к. по своей сущности изъятие носителя в ходе осуществления обыска ничем не отличается от изъятия носителя, например, в ходе осмотра места происшествия.

Кроме того, УПК РФ содержит требование об обязательном участии специалиста в таких случаях, однако не содержит какой-либо регламентации участия такого специалиста. С учетом того, что получение доказательств является строго формальной процедурой, такая регламентация является необходимой. Она возможна путем издания соответствующих нормативно-правовых актов, регулирующих деятельность специалиста в данной сфере. При формулировании конкретного алгоритма действий специалиста необходимо учитывать, что участие специалиста обусловлено необходимостью препятствования осуществлению сокрытия информации, содержащейся на различных устройствах, удалению такой информации, а также привнесению внешней информации в память устройств. Соответственно, необходима разработка последовательности действий, которая технически исключала бы возможность осуществления таких действий.

Возникает также вопрос о том, какие устройства можно отнести к категории электронных носителей информации. В соответствии с положениями подп. 3.1.9 ГОСТа 2.051-2013 под электронным носителем понимается "материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники" [1]. Использование данной формулировки в контексте рассматриваемых норм уголовно-процессуального законодательства позволяет относить к электронным носителям информации неограниченный перечень устройств, что на практике приводит к значительным затруднениям организационного характера. Из-за того что к этой категории можно отнести любое электронное запоминающее устройство, участие специалиста получается необходимо, например, при изъятии компакт-диска или USB-флэш-накопителя, хотя в большинстве случаев тактическая необходимость в этом отсутствует, к тому же это идет вразрез с принципом процессуальной экономии.

Следует отметить, что в пояснительной записке к Федеральному закону от 28 июля 2012 г. № 143-ФЗ определен перечень электронных носителей информации, при изъятии которых необходимо участие специалиста: компьютерные блоки, серверы, ноутбуки, карты памяти. Но не ясно, почему в данном перечне нет смартфонов, которые, по сути, являются полноценными компьютерами, но в небольшом форм-факторе. Следовательно, этот момент требует доработки законодателем, необходимо указать, при изъятии каких конкретно носителей информации требуется участие специалиста, причем речь идет не о составлении перечня предметов, а о создании четких категорий. В противном случае перечень будет подвергаться постоянному изменению в связи с техническим прогрессом и появлением новых устройств, а это нецелесообразно.

Представляется, что получение информации из электронного устройства должно производиться в два этапа. [3, с. 252]

Первый этап – изъятие электронного носителя информации в ходе осуществления соответствующего следственного действия. Порядок осуществления такого изъятия в ходе обыска и выемки прямо закреплен соответствующими положениями УПК РФ и, как представляется, не должен отличаться и в случае изъятия носителя в ходе осуществления иных следственных действий. Так, электронные устройства упаковываются, опечатываются и удостове-

ряются подписями следователя, специалиста и понятых в целях обеспечения сохранности как самого устройства, так и информации, содержащейся в его памяти.

Возникает вопрос: всегда ли есть возможность изъятия устройства при осуществлении соответствующего следственного действия? Представляется, что в данном случае необходимо руководствоваться общими положениями ст. 177, 182 УПК РФ, указывающими на то, что предмет должен иметь отношение к уголовному делу, другими словами, следователь должен при осуществлении такого изъятия обладать достаточными данными, позволяющими сделать вывод о том, что предмет (или информация, в нем содержащаяся) имеет отношение к соответствующему уголовному делу.

Второй этап – извлечение и исследование информации, содержащейся в памяти изъятого электронного устройства, – непосредственно связан с проблемой легализации полученной информации в качестве доказательства по уголовному делу.

Возникает вопрос: в ходе какого следственного действия возможно осуществление такого извлечения и исследования информации. Самый распространенный способ в практической деятельности – осуществление следователем с участием специалиста осмотра предмета (в данном случае электронного устройства), в ходе которого осуществляется извлечение информации и результаты которого оформляются протоколом осмотра предмета. В таком протоколе описываются все действия следователя, а также вся обнаруженная при помощи специальных средств информация.

В настоящее время универсальным устройством извлечения информации является мобильно-криминалистический комплекс UFED израильской компании Cellebrite, позволяющий извлекать, декодировать и анализировать данные с мобильных устройств, а также создавать соответствующие отчеты на необходимом качественном уровне. UFED поддерживает большинство мобильных устройств, оснащенных такими операционными системами, как iOS, Android, Symbian, Widows. А также, что немаловажно, является портативным устройством. Однако данный мобильно-криминалистический комплекс – разработка не российского производителя, а ее приобретение доступно любым гражданским лицам. Следовательно, видится целесообразным проводить разработки российских мобильно-криминалистических комплексов с целью снижения рисков, связанных со шпионажем, а также рисков того, что злоумышленники смогут создать схемы защиты своих собственных данных в связи с открытой продажей UFED.

Процессуальной основной использования таких специальных средств, в частности системы UFED, принято считать положения ч. 6 ст. 164 УПК РФ, которые устанавливают, что при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. То есть такие специальные средства имеют процессуальный статус технического средства обнаружения, фиксации и изъятия следов преступления в ходе осуществления следственного действия. Такой подход представляется небесспорным, исходя из самого содержания такого следственного действия, как осмотр предмета. Осмотр предмета – это следственное действие, направленное на собирание информации путем внешнего осмотра предмета и отражения его результата в протоколе осмотра, а не изъятие информации с помощью специальных средств. Таким образом, электронное устройство может быть предметом осмотра только в случае, если с его помощью было совершено преступление, оно являлось орудием совершения преступления или предметом хищения. Исходя из этого необходимо сначала извлечь информацию из памяти электронного устройства, а затем ее осматривать при помощи такого следственного действия, как осмотр предмета, с оформлением соответствующего протокола. Также следует отметить, что не все суды знакомы с мобильно-криминалистическими комплексами, в частности UFED, принципами его работы, при этом

практика его применения только формируется. Представляется целесообразным внести соответствующие изменения в УПК РФ, выделив изъятие информации из памяти электронного устройства в отдельное следственное действие. [2, с. 22-23]

Еще один вариант процессуального оформления изъятия информации – это извлечение информации из памяти электронного устройства посредством проведения компьютерно-технической экспертизы. В таком случае перед экспертом ставятся вопросы о наличии в устройстве каких-либо файлов (сообщений, фотографий, видеозаписей и др.), эксперт извлекает соответствующую информацию и отображает ее в своем заключении. Данный способ также представляется весьма спорным, поскольку перед экспертом ставятся вопросы о наличии соответствующих фактов, и, соответственно, в своем заключении эксперт должен дать ответ именно на вопрос о наличии или отсутствии соответствующих файлов, но никак не об их содержании.

При осуществлении изъятия информации возможна ситуация изъятия не только информации, связанной с совершенным преступлением, но и информации о частной жизни владельца электронного устройства, не связанной с преступлением. Например, из смартфона извлекаются фотографии, не имеющие отношения к расследованию уголовного дела. Возникает проблема: соответствует ли такая ситуация положениям ст. 23 Конституции РФ, гарантирующей право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Нам представляется, что в таком случае сам факт изъятия электронного устройства и извлечение из его памяти информации не будет являться нарушением права на частную жизнь, поскольку для целей расследования будет использоваться только информация, связанная с совершенным преступлением, распространение же иной информации осуществлено не будет. К такому выводу приходит и судебная практика (например, апелляционное постановление Приморского краевого суда № 22-5674/15 22К-5674/2015 от 24 сентября 2015 г. URL: sudact.ru). Исходя из этого необходимо отметить, что следователю при наличии на то возможности, необходимо дать специалисту конкретные указание на то, какая информация должна быть получена (например, указать на конкретную дату, время и др.), с целью максимально уменьшить возможность изъятия информации, не связанной с уголовным делом.

Самым распространенным для изъятия электронным устройством является смартфон, память которого содержит информацию о телефонных соединениях, сообщениях, видео-, фото -, аудиозаписях и др. При этом возникает вопрос о необходимости получения судебного решения для осуществления изъятия устройства и получения информации из его памяти. Так, в соответствии с ч. 2 ст.23 Конституции РФ ограничение права на тайну переписки и телефонных переговоров возможно только на основании судебного решения. В продолжение этих положений в ст. 29 УПК РФ установлено, что для получения информации о соединениях между абонентами и для изъятия корреспонденции из организаций связи необходимо решение суда. С одной стороны, положения Конституции РФ прямо устанавливают запрет на получение информации о переписке без судебного решения, с другой – в соответствии с положениями УПК РФ судебного решения требует выемка корреспонденции только из учреждений связи. Думается, в данном случае положения УПК РФ не соответствуют смыслу той гарантии прав, которую предоставляют положения Конституции РФ, поскольку содержание корреспонденции никак не меняется в зависимости от того, в какой форме она существует – бумажной или электронной и где находится – в учреждении связи или в смартфоне. Поэтому можно сделать вывод о том, что если целью изъятия информации с электронного устройства является получение информации о соединениях или о переписке, то для такого изъятия необходимо решение суда.

Таким образом, изъятие информации из памяти электронных устройств является необходимым инструментом расследования уголовных дел. Однако действующее законодательство не содержит достаточной регламентации осуществления соответствующих действий и нуждается в доработке с целью обеспечения баланса интересов государства и общества в раскрытии преступлений и права человека на охрану информации о его частной жизни.

Библиографический список

1. ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения : введен в действие приказом Росстандарта от 22.11.2013 № 1628-ст // СПС КонсультантПлюс.

2. Зуев, С.В. Электронное копирование информации – регламентация в УПК / С.В. Зуев // Законность. – 2013. – № 8.

3. Савицкая, И.Г.Участие специалиста в следственных действиях, связанных с изъятием электронных носителей информации / И.Г. Савицкая //Судебная власть и уголовный процесс. – 2016. – № 2.