О. С. Бутенко*

КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОСМОТРА МОБИЛЬНЫХ ТЕЛЕФОНОВ В РАМКАХ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ

Аннотация. *В статье анализируется такое следственное действие, как осмотр мобильных телефонов, которое весьма слабо освещено в научной литературе. Автор специально касается как криминалистического, так и процессуального аспекта следственного осмотра, поскольку регламентация требований к осмотру мобильных телефонов находится в стадии становления. Автором рассматриваются криминалистически значимые следы, которые могут быть обнаружены на мобильном телефоне, даются отдельные рекомендации по тактике проведения изъятия и осмотра мобильных устройств, рассматриваются общие требования и основания для проведения осмотра мобильных телефонов. Акцентируется внимание на том, что важной задачей, стоящей перед следователем на первоначальной стадии изъятия и осмотра мобильного устройства, является обеспечение полной сохранности криминалистически значимой информации в мобильном устройстве в неизменном виде. Далее автор анализирует современные программные и технические средства, применяемые в следственной практике для осмотра мобильных телефонов (программно-аппаратные комплексы UFED и XRY, иные программные и аппаратные методы, позволяющие изъять из мобильного телефона действующую и удаленную пользовательскую информацию). Кроме того, в статье рассматриваются и особенности иных методов получения информации из мобильных телефонов, таких как получение root-доступа к устройству, с точки зрения их криминалистического применения. Учитывая, что одной из нерешенных в настоящее время проблем является преодоление защиты на смартфонах iPhone (начиная с версии 4s), отдельно рассматривается разработанная в текущем году аппаратная система IP Box iPhone Password Unlock Tool, позволяющая подобрать пароль к смартфонам и планшетам компании Apple. Также рассматривается вопрос о правовом статусе информации, которая содержится в мобильном телефоне. Отдельно в статье рассматривается вопрос о необходимости получения судебного решения для проведения осмотра мобильных устройств, который в настоящее время является одним из самых дискуссионных в следственной практике по причине законодательного пробела в данной области. Отмечается, что необходимо регулярное обеспечение следователей актуальной криминалистической информацией и необходимыми для успешной работы практическими навыками, в том числе через систему дополнительного профессионального образования, осуществляемого Академией Следственного комитета Российской Федерации.*

© Бутенко О. С., 2016

* *Бутенко Олег Сергеевич*, кандидат юридических наук, доцент кафедры криминалистики первого факультета повышения квалификации (с дислокацией в г. Ростов-на-Дону) Института повышения квалификации Академии Следственного комитета Российской Федерации
butenko_os@mail.ru
344064, Россия, г. Ростов-на-Дону, ул. Волоколамская, д. 3в

Ключевые слова: *следственный осмотр, осмотр мобильных устройств, изъятие информации, восстановление информации, криминалистическая тактика осмотра, участие специалиста.*

DOI: 10.17803/1729-5920.2016.113.4.049-060

Технологии, построенные на использовании микроэлектроники, являющиеся технологиями пятого технологического уклада в экономике, нашли свое воплощение в миллиардах мобильных электронных устройств по всему миру. Сейчас трудно представить нашу жизнь без ежедневного их использования. Компьютеры, мобильные телефоны, навигаторы, телевизоры с возможностью выхода в Интернет и Skype становятся носителями огромного количества цифровой информации, и, следовательно, преступления, совершаемые с использованием этих устройств, оставляют в них электронные криминалистически значимые следы.

Мобильные телефоны и иные устройства используются при совершении преступлений в сфере экономики, компьютерной информации, телефонного мошенничества, при незаконном сбыте наркотических средств и т.д. При опросе следователей, проведенном Н. А. Архиповой, установлено, что 52 % следователей уделяют средствам мобильной связи особое внимание и принимают активные меры для получения информации, содержащейся в мобильных телефонах. Более 37 % следователей исследуют средства мобильной связи, если об этой возможности стало заранее известно в ходе расследования преступления, и только 7 % следователей не уделяют этому внимания и ранее не задумывались о возможностях хранения в средствах мобильной связи криминалистически значимой информации.

Н. А. Архипова также отмечает, что «практические работники нередко недооценивают технические возможности средств сотовой связи по хранению в них текстовой, звуковой информации, фото- и видеозаписей, сведений о входящих и исходящих телефонных номерах, содержание SMS-, EMS-, MMS-сообщений, что приводит к сужению доказательственной базы уголовного дела»[1].

Как отмечает Н. Н. Федоров, в случае, когда следы преступления отображаются в электронной форме, их обнаружение, изъятие и фиксация представляют достаточную сложность для большинства следственных работников.

Эксперты в области компьютерно-технической экспертизы (В. А. Егоров и О. Н. Ильиных) отмечают, что с мобильным устройством связаны следующие виды значимых для следствия следов:

— *следы на электронных носителях* — сведения о соединениях абонентов, о произведенных финансовых операциях, системе сотовой связи и т.д., хранящиеся у сотовых операторов либо на компьютерах, изъятых у подозреваемого (обвиняемого);
— *следы на мобильном устройстве* — абонентская книга телефона, сведения о соединениях абонентов сетей сотовой связи (журнал звонков, сообщения SMS, MMS), о произведенных финансовых операциях, системе сотовой связи, специальные программные средства для прошивки мобильных телефонов, SIM-карт, данные из прикладных приложений Viber, Skype, WhatsApp, Facebook, Vkontakte и др., которые могут содержать данные пользователей мобильных телефонов, IMEI-код, изменение последнего программными средствами, используемые телефонные номера, фотографии и видеозаписи, следы пальцев рук, микрочастиц;
— *следы на SIM-карте,* абонентская книга на 200 номеров, журнал звонков, сообщения SMS, данные о служебных сообщениях.

При осмотрах, обысках, выемках, сопряженных с изъятием как компьютерной техники, так и мобильных телефонов, зачастую возникает ряд общих проблем, связанных со спецификой изымаемых объектов.

Фактически оптимальный вариант изъятия мобильного телефона и носителей информации — это фиксация их и их конфигурации (в слу-

[1] *Архипова Н. А.* К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений : сб. мат-лов криминалист. чтений. Барнаул : Барнаульский юрид. институт МВД России. 2014. № 10. С. 16.

чае компьютерной техники) на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или в месте производства экспертиз с участием специалистов.

По прибытии на место осмотра или обыска следует принять меры к обеспечению сохранности информации на находящихся здесь компьютерах, мобильных телефонах и носителях информации. Для этого необходимо:

— не разрешать кому бы то ни было из лиц, присутствующих на месте происшествия или объекте обыска, прикасаться к работающим компьютерам, мобильным телефонам, носителям информации, включать и выключать их;
— самостоятельно не производить никаких манипуляций с компьютерной и сотовой техникой, если результат этих манипуляций заранее не известен;
— при наличии в помещении, где находятся средства компьютерной и сотовой техники, а также носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее их транспортировать в другое помещение.

Важной задачей, стоящей перед следователем, является обеспечение сохранения криминалистически значимой компьютерной информации в неизменном виде.

В криминалистической литературе продолжается дискуссия по поводу того, в каком состоянии должен изыматься мобильный телефон. Так, А. Н. Архипова в результате опроса сотрудников органов внутренних дел, проводивших изъятие мобильных телефонов в ходе проведения следственных действий (осмотра места происшествия, обыска, выемки), выявила, что опрошенные следователи изымали мобильные телефоны всегда в выключенном состоянии. В результате она рекомендует: если мобильный телефон включен, нужно произвести фотосъемку месторасположения мобильного телефона и его экрана, после чего телефон нужно корректно выключить. В протоколе следственного действия должны быть отражены: информация с экрана телефона, порядок выключения мобильного телефона, дата и время его отключения. Согласно автору данные действия обеспечат сохранность содержащейся в мобильном устройстве информации.

В свою очередь, Г. В. Семенов подчеркивает, что «при изъятии мобильного телефона не следует отключать его, т.к. при последующем включении могут потребоваться коды блокировки, необходимые для работы телефона и соответственно полноценного исследования его информационного содержимого»[2].

Как отмечает А. А. Шошин, следственный осмотр является одним из самых распространенных следственных действий. Суть осмотра заключается в том, что следователь сам непосредственно убеждается в наличии фактов, имеющих доказательственное значение. При этом могут применяться самые разные методы познания. «Осмотр — это не только наблюдение, но и производство различных измерений и вычислений, сравнение наблюдаемых объектов как между собой, так и с другими объектами и явлениями, экспериментирование с исследуемыми объектами и, наконец, описание и запечатление иными методами всего того, что обнаружено и выявлено следователем и другими участниками осмотра»[3].

Процессуальный порядок осмотра предусмотрен ст. 176—180 УПК РФ. В соответствии с положениями уголовно-процессуального закона следственный осмотр может проводиться в присутствии понятых. Следователь имеет право в необходимых случаях привлекать к участию в осмотре обвиняемого, подозреваемого, потерпевшего, свидетеля. Поскольку осмотр мобильных устройств отличается от иных видов осмотра тем, что компьютерная информация, содержащаяся в мобильном устройстве, зачастую не может восприниматься человеком непосредственно органами чувств, воспринимать (следовательно, и осмотреть в смысле УПК РФ) ее можно с помощью технических и программных средств.

Осмотр мобильных устройств, да и вообще любой компьютерной информации, это не столько осмотр как таковой, а скорее техническое исследование, требующее определенных знаний.

---

[2] *Семенов Г. В.* Расследование преступлений в сфере мобильных телекоммуникаций : автореф. дис. ... канд. юрид. наук. Воронеж, 2003. С. 17.

[3] *Шошин А. А.* Некоторые проблемы определения понятия «следственный осмотр» // Вестник Владимирского юридического института. 2011. № 4 (21). С. 175.

Н. Н. Федоров отмечает, что иногда в связи с технической сложностью осмотра мобильных устройств лучше в любом случае назначить судебную компьютерно-техническую экспертизу. В то же время проведение компьютерной экспертизы по каждому мобильному устройству зачастую невозможно, т.к. загруженность экспертов в регионах затягивает срок проведения экспертизы на четыре, а иногда даже на шесть месяцев. Поэтому законность и грамотность осмотра является необходимым элементом успешного окончания уголовного дела.

При производстве следственного осмотра следователь должен строго соблюдать требования законности, не допуская действий, унижающих достоинство или опасных для здоровья участников осмотра и тех лиц, интересы которых могут оказаться затронутыми производством осмотра. Если нужно, следователь может принять меры, предупреждающие разглашение результатов осмотра. Ход и результаты осмотра должны быть зафиксированы в установленном законом порядке.

При осмотре мобильных телефонов необходимо обеспечить выполнение следующих требований:

— своевременность;
— объективность;
— полнота;
— активность.

Осмотр мобильного телефона нужно проводить своевременно, сразу же, как только в этом возникает необходимость. Необоснованное промедление с осмотром может привести к неэффективности или невозможности следственного осмотра по причине того, что аккумулятор телефона разрядится либо информация будет специально уничтожена посредством удаленного доступа. Таким образом, выполнение требования своевременности следственного осмотра непосредственно влияет на результативность данного следственного действия и повышает вероятность получить доступ к максимально сохранной к моменту осмотра информации на мобильном устройстве.

Учитывая, что элементы субъективности могут иметь место при осмотре, как и в любой иной деятельности, выполняемой человеком, для проведения осмотра мобильного устройства важно выполнение требования объективности. Сутью данного требования является максимально точное запечатление и последовательная фиксация всего обнаруженного при проведении следственного осмотра мобильного устройства.

Требование объективности осмотра конкретизируется в нескольких аспектах.

Во-первых, внимательное исследование и четкая фиксация всего, что было обнаружено при проведении следственного осмотра, причем в том виде, в котором оно было в действительности.

Во-вторых, последовательное описание в протоколе осмотра всего, что было осмотрено, причем в той последовательности, в которой проводился осмотр.

В-третьих, беспристрастное исследование мобильного устройства, когда следователь проводит осмотр без предвзятости, предубеждения, не отдает предпочтения ни одной из проверяемых им гипотез и версий.

В-четвертых, беспристрастное ведéние протокола, отражающего результаты осмотра. В протоколе не должны присутствовать выводы, заключения и предположения следователя.

С требованием объективности тесно связано требование полноты следственного осмотра. Речь идет о выявлении, фиксации и об исследовании в ходе осмотра всех фактических данных, которые имеют доказательственное значение по делу. Границы исследования существенно расширяются благодаря квалифицированному применению современных научно-технических средств и программ при осмотре мобильного телефона, а также грамотному использованию приемов собирания и исследования доказательств.

Задача следователя — провести осмотр так, чтобы не упустить ни одного обстоятельства, имеющего значение для дела. Множество имеющихся у следователя версий помогают ему при осмотре определить, относятся ли к делу обнаруженные при осмотре данные. Все те, что, вероятно, относятся к делу, должны изыматься для последующего исследования и решения вопроса об их значимости для следствия. Здесь крайне важна профессиональная интуиция следователя, т.к. отношение к делу некоторых фактических данных, полученных в результате следственного осмотра, может выясниться лишь в результате сопоставления их с полученными доказательствами или даже в результате специального экспертного исследования. Таким образом, щепетильное выполнение требования полноты следственного осмотра обеспечивает возможность обнаружить максимальное количество необходимых сведений.

Требование активности данного следственного действия предполагает наличие у следо-

вателя активной профессиональной позиции, которая проявляется в том, что следователь проводит осмотр без дополнительных ходатайств заинтересованных лиц. Он принимает все возможные и необходимые меры для того, чтобы найти следы преступления, раскрыть его и обнаружить лицо, совершившее данное преступление. Реализация требования активности предполагает целеустремленность действий следователя, самостоятельное целеполагание и терпеливое следование целям, которых он рассчитывает достичь путем следственного осмотра.

Осмотр мобильных телефонов должен выполняться при соблюдении следующих условий:
— наличие понятых (не менее двух понятых, за исключением случаев, предусмотренных ч. 3 ст. 170 УПК РФ);
— привлечение к участию в осмотре эксперта, в случае невозможности его непосредственного участия предполагается последующее обращение к эксперту;
— осмотр не следует проводить в ночное время, за исключением случаев, не терпящих отлагательств.

Кроме того, при осмотре не допускается:
— применение принуждения (кроме случаев осмотра жилища, реализующегося в соответствии с ч. 5 ст. 165 УПК РФ или по решению суда);
— нарушения прав и законных интересов лиц, принимающих участие в осмотре, а также иных лиц, ограничение которых не предусмотрено уголовно-процессуальным законом;
— унижение чести и достоинства лиц, участвующих в производстве осмотра, а также угроза их жизни и здоровью;
— фиксация показаний потерпевшего, свидетелей и других принимающих участие в осмотре лиц.

Кроме того, О. А. Луценко выделяет ряд положений процессуального и тактического характера, которыми следует руководствоваться при проведении следственного осмотра:
— руководство осмотром должен осуществлять следователь, которому поручено расследование дела. Следователь является лицом, которое ответственно за результаты осмотра;
— использование научно-технических средств (UEFD, XRY, Oxygen Forensic и другие);
— обязательное присутствие понятых либо подробная фотофиксация хода следственного осмотра мобильного устройства;
— обеспечение всесторонности, активности и полноты следственного осмотра;
— правильное обращение с объектами при изъятии и фиксации.

Максимально полное выполнение этих требований позволит решить в полной мере задачи осмотра мобильных устройств:
— установить, носило ли происшедшее событие преступный характер;
— выяснить, при каких обстоятельствах оно происходило (время, место, способ, характер причиненного ущерба);
— выявить виновных лиц и мотивы их действий;
— получить данные о причинах преступления, которые способствовали его совершению.

При осмотре мобильных устройств должны соблюдаться следующие правила:
— объект до манипуляций с ним предварительно фотографируется, и в протоколе описывается его исходное состояние;
— если возникнет предположение о наличии на мобильном устройстве следов, которые не видны невооруженным глазом (отпечатки пальцев, следы биологического происхождения), необходимо применить специальные способы и средства их выявления;
— в случае если телефон заблокирован, желательно воспользоваться методами, которые не несут риска разрушения или повреждения информации, находящейся на мобильном устройстве. Например, если осматривается мобильный телефон под управлением операционной системы Android, часто возникает искушение получить максимально полный доступ к устройству, так называемый root-доступ, который позволит исследовать любой Android-телефон, вне зависимости от его конструктивных инженерных особенностей. Имея полный доступ к операционной системе Android, можно вносить изменения в файлы операционной системы, удалять стандартные программы операционной системы, запускать любые исполняемые файлы, предназначенные для Linux, создавать полную резервную копию установленной системы со всеми настройками и приложениями, используя дополнительные программы. Но возникает риск повреждения информации на мобильном телефоне, поскольку вносятся изменения в память устройства путем инсталляции специальной программы, открывающей root-доступ (Unlock Root, z4root, HTC Quick Root, Easy Rooting Toolkit, Gingerbreak,

SuperOneClick, Visionary, Unrevoked), а также происходит потеря заводской гарантии, что связано с возможным вредом операционной системе при неправильном или просто неосторожном обращении с повышенным уровнем доступа;

— информацию, которую невозможно скопировать на внешний носитель и проанализировать с помощью специализированного программного обеспечения, желательно зафиксировать любым иным образом (с помощью фото- или видеофиксации).

Участвующий в осмотре специалист должен оказать помощь следователю и в составлении протокола следственного осмотра, «обеспечивая правильность отражения в нем данных, характеризующих объекты осмотра, их взаимосвязь с другими следами и объектами»[4].

На завершающем этапе осмотра специалист должен оказать всю возможную помощь следователю в анализе результатов следственного действия; в выдвижении или корректировке следственных версий; «определении направлений и видов дальнейшего использования объектов осмотра, обнаруженных и изъятых следов и других вещественных доказательств»[5].

Специалист также может оказать помощь следователю в определении относимости, допустимости, достоверности, достаточности доказательств, полученных в ходе осмотра.

Как уже отмечалось выше, в ходе осмотра мобильных устройств крайне рекомендуется использование специализированного программного обеспечения и (или) программно-аппаратных комплексов. Таких комплексов в настоящее время существует два — это UFED (производства фирмы Cellebrite, Израиль) и XRY (производства компании Micro Systemation, Швеция).

В соответствии с приказом Председателя Следственного комитета РФ в 2012—2013 годах все следственные управления Следственного комитета РФ были обеспечены аппаратно-программными комплексами *UFED*. Исходя из спецификации данного оборудования, UFED представляет собой средство для проведения оперативного исследования мобильных устройств. Аппаратно-программный комплекс позволяет провести упрощенное и быстрое логическое извлечение информации из обширного ряда мобильных устройств: мобильных телефонов, смартфонов, планшетов, телефонов китайской сборки на базе микропроцессора, некоторых моделей GPS-приемников, симкарт мобильных устройств и карт памяти.

Используемый в следственных управлениях Следственного комитета РФ комплекс UFED Touch включает в себя:

— UFED Logical Analyzer — приложение для комплексного анализа и составления отчетов и логического извлечения данных;

— UFED Link Analyzer — приложение, которое определяет и визуализирует связи и коммуникационные методы между различными мобильными устройствами, основываясь на отчетах об извлечении данных;

— UFED Phone Detective — приложение для моментальной идентификации телефона.

UFED использует несколько механизмов анализа мобильных устройств, а именно:

1) извлечение данных на физическом уровне;
2) логическое извлечение;
3) извлечение файловой системы.

Извлечение данных на физическом уровне предполагает побитовое полное копирование содержания памяти мобильного устройства. Указанный метод извлечения данных позволяет извлечь не только неповрежденные данные, но и скрытые данные, а также те, которые были удалены.

Поддерживаемые типы данных, извлекаемые на физическом уровне, включают неповрежденные и удаленные пароли, установленные приложения, географические теги, информацию о местонахождении, файлы мультимедиа, такие как фото и видео пользователя.

Логическое извлечение предполагает извлечение данных при помощи операционной системы устройства. Это означает, что инструменты извлечения данных взаимодействуют с операционной системой устройства и запрашивают информацию из системы. Это позволяет получить большинство оперативных данных мобильного устройства.

Типы данных включают в себя пароли, списки звонков, журналы звонков, сохраненные на сим-карте, данные телефона (IMEI/ESN), записи телефонной книги, SMS, MMS, изображе-

[4] Следственный осмотр. Понятие, виды и доказательственное значение : учеб.-практ. пособие / отв. ред. О. А. Луценко. Элиста, 2007. С. 17.

[5] Следственный осмотр. С. 18.

ния, видео- и аудиофайлы и др. В большинстве случаев логическое извлечение невозможно для заблокированных устройств.

Извлечение файловой системы — это получение файлов, встроенных в память мобильного устройства. Извлечение файловой системы предоставляет доступ ко всем файлам, хранящимся в памяти мобильного устройства, в том числе изображениям, видео, системным файлам и журналам.

Исходя из практики применения программно-аппаратного комплекса UFED в отделах криминалистики следственных управлений Следственного комитета РФ, необходимо отметить высокую значимость данных, получаемых с помощью этого комплекса. Криминалистическое исследование мобильного телефона позволяет существенно сократить время, необходимое на осмотр каждого мобильного устройства, определить перечень объектов, которые необходимо направить на судебную компьютерную экспертизу, и получить данные, которые могут быть приобщены к материалам уголовного дела в качестве доказательств.

В то же время необходимо отметить обстоятельство, которое до сих пор препятствует более широкому распространению практики применения UFED в ходе расследования уголовных дел. Этим обстоятельством является трудозатратность проведения исследования с помощью UFED. Каждая модель мобильного устройства достаточно уникальна относительно возможности извлечения того или иного рода информации. Подчас требуется осуществить все указанные выше варианты извлечения информации для одного телефона. Поэтому исследование одного телефона может занимать от 2 до 5 часов. На наш взгляд, осмотр с помощью аппаратно-программного комплекса UFED сравним с проведением экспертизы того же устройства и по трудозатратам, и по требуемой квалификации сотрудника отдела криминалистики, который проводит данное исследование.

Второй упомянутый нами программно-аппаратный комплекс, *XRY*, появился на рынке раньше UFED, и на сегодня его активно используют в правоохранительной системе Великобритании и США.

Комплекс работает в трех режимах, сходных с режимами UFED:

— XRY Logical предназначен для быстрого извлечения активных данных из мобильного устройства путем логического взаимодействия программного обеспечения с операционной системой устройства. Эффективен в 80 % исследований. Обладает простым, интуитивно понятным и удобным интерфейсом;
— XRY Physical предназначен для физического извлечения (дампа) памяти мобильного устройства и ее последующего дешифрования. Обеспечивает глубокий анализ устройства с целью извлечения удаленных, защищенных или спрятанных данных;
— XRY Complete — полнофунциональное решение, объединяющее все инструменты и преимущества логического и физического извлечения данных. По информации производителя, программно-аппаратный комплекс предназначен для проведения защищенного извлечения цифровых данных из разнообразных мобильных устройств, таких как смартфоны, GPS-навигаторы, 3G-модемы, портативные аудиоплееры и планшетные компьютеры. Благодаря функции «Мастер одновременного извлечения» комплекс позволяет пользователю исследовать до трех мобильных устройств одновременно, что достаточно существенно экономит время и ресурсы.

Аналогично с комплексом UFED, в результате исследования телефонов создаются защищенные от несанкционированного доступа отчеты, которые можно вывести на печать или записать на компакт-диск. Функция экспорта XRY обеспечивает возможность создания отчетов в следующих форматах: html, xml, xlsx, xls, docx, doc и gpx.

В начале работы системы, после идентификации мобильного устройства, XRY подсказывает, какие данные можно извлечь из этой модели телефона, а какие нет.

После извлечения данных перед специалистом и следователем зачастую встает вопрос об анализе большого массива данных (особенно если речь идет о современных смартфонах), поэтому полезны инструменты приоритетной сортировки (Triage). Данная функция Списка особого контроля (Watch List Feature) помогает немедленно найти нужную следователю информацию для оперативного принятия решения.

Комплекс XRY позволяет извлекать данные из многочисленных программных приложений смартфонов. С его помощью можно извлечь данные вызовов IP-телефонии, картографическую информацию GPS и журналы средств оперативной пересылки сообщений.

Кроме того, в комплекс входят следующие модули:
— XACT — HEX — редактор для анализа физического дампа на низком уровне;
— ID SIM-Cloner — программный модуль для клонирования ID SIM-карт с целью обеспечения неизменности данных мобильного устройства.

XAMN — аналитический инструмент компании Micro Systemation, специально разработанный для визуализации извлеченных данных нескольких телефонов. XAMN позволяет пользователям визуализировать взаимосвязи, отображать на карте географические данные, а также просматривать хронологию событий одновременно для нескольких разных телефонов.

Для работы в сложных условиях Micro Systemation разработала специальный тип комплектов *XRY Field Edition* на основе защищенных ноутбуков Panasonic CF-19 и Algiz XRW.

Несмотря на универсальность указанных комплексов, ими не всегда можно воспользоваться. Сказывается дороговизна комплексов и, как следствие, небольшое их количество, высокая загруженность. Поэтому необходимо рассмотреть также иные программные средства и методы, которые могут быть использованы при осмотре мобильных устройств.

И. Ю. Михайлов приводит следующие методы изъятия информации из мобильного телефона:
1. Извлечение данных из микросхем памяти мобильного устройства методом Chip-off.
2. Извлечение данных из памяти мобильного устройства с использованием отладочного интерфейса JTAG.
3. Извлечение данных с помощью специализированных программ (например, Oxygen Forensic Suit).
4. Создание копии памяти мобильного устройства в ручном режиме.
5. Комбинированные методы.

В то же время, как отмечает указанный автор, нет единой программы, которая бы поддерживала извлечение данных из всех мобильных устройств, существующих в мире.

Необходимо также отметить, что есть и новые технологии, позволяющие обойти защиту мобильного телефона и, как следствие, провести осмотр с максимальной степенью эффективности. Так, обойти защиту iPhone (начиная с версии 4) исключительно программными методами практически невозможно без риска повреждения данных, но устройство IP Box iPhone Password Unlock Tool (Китай), которое появилось в открытой продаже во втором квартале 2015 года, позволяет подключиться в iPhone или iPad и методом брутфорса (перебора) подобрать запрашиваемый при загрузке операционной системы iOS пароль.

Необходимо отметить, что данный ключ безопасности, открывающий доступ к программной части смартфона, состоит из четырех цифр. Но в операционной системе iOS после 10 неправильно введенных паролей информация с устройства будет автоматически удалена. С помощью же IP Box процесс подбора пароля полностью автоматизируется и позволяет подобрать пароль к смартфону за несколько часов или дней без риска повреждения или уничтожения информации. Особенностью рассматриваемой системы, главный модуль которой подключается к мобильному устройству при помощи зарядного кабеля и напрямую к аккумуляторной батарее, является специальный датчик света. Последний крепится к дисплею и позволяет обойти систему защиты, реализованную в iOS. Примененное инженерное решение заключается в считывании текущего параметра яркости, которая в случае неверно введенного пароля остается прежней, а при вводе правильной комбинации — увеличивается. Соответственно, если яркость не изменилась, IP Box подает сигнал на блок питания смартфона или планшета, принудительно отправляя устройство в перезагрузку. При этом iOS не успевает регистрировать попытку ввести пароль, что делает данный способ защиты абсолютно бесполезным, а количество попыток — неограниченным.

Если представить, что на загрузку, ввод цифр затрачивается примерно 40 сек, то для подбора пароля из четырех цифр (всего 10 000 комбинаций) понадобится не более 112 часов. В заключение хочется отметить, что цена данного устройства не превышает 200 долл., поэтому оно является достаточно доступным для широкого применения.

Наиболее проблематичным и дискуссионным является вопрос о правовом статусе информации, которая содержится в сотовом телефоне. Наибольший интерес при этом вызывает вопрос о статусе сообщений электронной почты, SMS и MMS, мгновенных сообщениях Skype, Viber и WhatsApp, а также сообщениях, содержащихся в приложениях популярных социальных сетей — Vkontakte и др. Проблема кроется в том, что на уровне федерального за-

конодательства не закреплено даже понятие электронной почты, не говоря уже о данных переписки из приложений для мобильных устройств.

Так, статья 23 Конституции РФ предусматривает право граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Хотя в этой статье прямо не указано, что гражданин имеет право на тайну электронных сообщений, очевидно, что электронные сообщения подпадают под понятие «иные сообщения».

Электронные почтовые ящики могут быть созданы пользователями самостоятельно на собственных почтовых сервисах или на публичных почтовых сервисах. Собственные почтовые сервисы, как правило, предпочитают организации, они предоставляют к ним доступ сотрудникам. Для самостоятельного создания почтового сервиса необходимы специальные знания в области интернет-технологий и доменное имя. Электронные почтовые ящики, размещенные на публичных сервисах, крайне популярны. Их создание не требует специальных знаний, необходимо лишь заполнить простую форму на сайте публичного сервиса и получить электронный почтовый ящик в свое пользование.

Е. В. Митин предлагает считать электронный почтовый ящик, созданный пользователем на публичном почтовом сервисе, принадлежащим гражданину, если в регистрационных формах указаны реальные данные этого гражданина, в противном случае электронный почтовый ящик считается не принадлежащим гражданину.

На уровне высших судов также нет ясности по данному вопросу, поскольку в определениях Конституционного Суда РФ от 2 октября 2003 г. № 345-О и от 21 октября 2008 г. № 528-О к тайне связи относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи. В то же время в определении Верховного Суда РФ от 2 июня 2006 г. № 9-ДП06-10 говорится о том, что при выемке у операторов связи документов о входящих и исходящих сигналах соединений похищенного мобильного телефона тайна содержания переговоров сохраняется, поскольку целью выемки является только информация о входящих и исходящих звонках с похищенного телефона.

Один из исследователей в области компьютерно-технической экспертизы, А. Н. Яковлев, применительно к сообщениям электронной почты отмечает, что пока сообщение находится на компьютерном средстве пользователя, такие данные не являются тайной связи. Как только правообладатель коммуникационного сервиса «Мэйл.Ру», «Яндекс» или др. получает эти данные, пересылает оператору связи, данные являются электронными сообщениями или электронной почтой, охраняемой тайной связи. Будучи доставленными получателю, т.е. на компьютерное средство пользователя, они вновь становятся не охраняемыми законом данными, которые получил пользователь сети Интернет. Следовательно, как отмечает автор, возможно «получать информацию в порядке ст. 86 УПК РФ в ходе следственных действий... Решения суда при этом также не требуется»[6].

Данный подход, безусловно, имеет право на существование, но на практике зачастую следователям приходится обращаться с ходатайством в суд для проведения осмотра мобильного телефона. Нельзя сказать, что это повсеместная практика, но, безусловно, данный вопрос еще найдет разрешение в федеральном законодательстве Российской Федерации.

Таким образом, с появлением в 1990-х гг. в России средств мобильной связи и с их широким распространением следователи ежедневно сталкиваются с новыми высокотехнологичными криминалистическими объектами, особое место среди которых занимают мобильные телефоны. Глубокое понимание технических возможностей средств мобильной связи по хранению в них текстовой и звуковой информации, фото- и видеозаписей, содержания SMS- и MMS-сообщений, по анализу входящих и исходящих звонков как источника сведений о социальных связях субъекта и т.д. существенно расширяет доказательственную базу уголовного дела. В то же время, учитывая положительный опыт применения полиграфа в системе СК России (в отделах криминалистики следственных управлений выделяется отдельная ставка эксперта для работы с полиграфом),

[6] *Яковлев А. Н.* Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 46.

считаем необходимым применить аналогичный организационный подход и к применению UFED. Введение данного положения, во-первых, повысит эффективность применения UFED, во-вторых, сократит время на проведение судебных экспертиз и, в-третьих, позволит повысить эффективность работы отделов криминалистики за счет большей специализации его сотрудников.

Но и следователи не должны возлагать надежды исключительно на помощь специалистов и экспертов; необходимо помнить, что именно следователь является должностным лицом, ответственным за результаты осмотра, а без грамотного осмотра и поиска доказательств, в том числе в электронной форме, привлечение лица к уголовной ответственности зачастую становится проблематичным. Поэтому необходимо регулярное обеспечение следователей актуальной криминалистической информацией и необходимыми для успешной работы практическими навыками, в том числе через систему дополнительного профессионального образования, осуществляемого Академией Следственного комитета Российской Федерации.

БИБЛИОГРАФИЯ

1. *Алескеров В. И., Максименко И. А.* Особенности отдельных следственных действий при расследовании преступлений в сфере компьютерной информации // Вестник Всероссийского института повышения квалификации сотрудников МВД России. — 2010. — № 4 (16).
2. *Архипова Н. А.* К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений // Сборник материалов криминалистических чтений. — Барнаул, 2014. — № 10.
3. *Баженов С. В., Невский Е. П., Чердынцева И. А.* Получение информации о соединениях между абонентами и (или) абонентскими устройствами // Законодательство и практика. — 2011. — № 1.
4. *Варданян А. А., Цыкора А. А.* Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединениях между абонентами и (или) абонентскими устройствами // Известия Тульского государственного университета. Экономические и юридические науки. — 2013. — № 4—2.
5. *Варданян А. В., Никитина Е. В.* Расследование преступлений в сфере высоких технологий и компьютерной информации. — М., 2007.
6. *Гайдин А. И., Потанина И. В.* Особенности производства отдельных следственных действий при расследовании общеуголовного мошенничества с использованием средств сотовой связи // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : сборник материалов Всерос. науч.-практ. конференции. — Орел, 2015.
7. *Зигура Н. А.* Использование специальных знаний для обнаружения, изъятия, фиксации и закрепления энергозависимой компьютерной информации // Вестник ЮУрГУ. — Серия : Право. — 2007. — № 4.
8. *Кэрриэ Б.* Криминалистический анализ файловых систем. — М., 2007.
9. *Митин Е. В.* Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации // Теория и практика общественного развития. — 2012. — № 9.
10. *Морозова Е. В., Андроник Н. А.* Тактика контроля и записи переговоров: проблемы теории и практики // Вестник Уральского института экономики, управления и права. — Серия : Право. — 2013. — № 4 (25).
11. *Романенко М. А.* Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. — Серия : Право. — 2008. — № 1 (14).
12. *Романенко М. А.* Судебная дигитология — современный взгляд на содержание криминалистической техники // Вестник Омского университета. — Серия : Право. — 2007. — № 1 (10).
13. Следственный осмотр. Понятие, виды и доказательственное значение / отв. ред. О. А. Луценко. — Элиста, 2007.
14. *Старичков М. В.* Тактика осмотра и выемки носителей компьютерной информации // Вестник Восточно-Сибирского института Министерства внутренних дел России. — 2012. — № 2 (61).
15. *Стельмах В. Ю.* Технико-специальные следственные действия в российском уголовном процессе // Вестник Санкт-Петербургского университета МВД России. — 2015. — № 1 (65).
16. *Федоров Н. Н.* Форензика — компьютерная криминалистика : монография. — М., 2007.
17. *Федотова Н. В.* О предмете тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений // Бизнес в законе. — 2008. — № 2.

18. *Цыкора А. А.* Некоторые проблемы производства следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами» // Известия Тульского государственного университета. — Экономические и юридические науки. — 2013. — № 3—2.
19. *Шахматов А. В., Бажуков В. Б.* Оперативно-розыскное исследование электронных носителей информации при выявлении и раскрытии преступлений в кредитно-банковской сфере // Вестник Санкт-Петербургского университета МВД России. — 2014. — № 2 (62).
20. *Шейфер С. А.* Следственные действия. Основания, процессуальный порядок и доказательственное значение. — Самара, 2008.
21. *Шошин А. А.* Некоторые проблемы определения понятия «следственный осмотр» // Вестник Владимирского юридического института. — 2011. — № 4 (21).
22. *Яковлев А. Н.* Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. — 2014. — № 4.

Материал поступил в редакцию 27 августа 2015 г.

FORENSIC AND PROCEDURAL ASPECTS OF EXAMINING MOBILE PHONES DURING PRELIMINARY INVESTIGATION

BUTENKO Oleg Sergeevich — Ph.D. in Law, Associate Professor of the Department of Criminalistics of the First Faculty of Advanced Training (Rostov-on-Don) of the Academy of the Investigative Committee of the Russian Federation.
[butenko_os@mail.ru]
344064, Russia, Rostov-on-Don, ul. Volokalamskaya, 3B.

Review. *The article analyzes such an investigative act as examining mobile phones that is very poorly covered in scientific literature. To this end, the author deals with both forensic and procedural aspects of investigative examination as examination requirements are still being developed. The author considers forensically significant traces that can be detected in a mobile phone, provides guidelines concerning the tactics of the seizure and examination of mobile devices, addresses the general requirements and the reasons for inspecting mobile phones. The author draws attention to the fact that an important task the investigator needs to perform at the preliminary stage of seizing and examining a mobile device is to secure absolute safety of unchanged information significant for investigation in a mobile device. Then, the author analyses contemporary program and IT means applied in investigative practice to examine mobile phones (hardware and software UFED and XRY systems, other hardware and software techniques that enable investigators to remove existing and remote user information from a mobile phone). Moreover, the article considers another peculiarities of the methods of obtaining information from mobile phones such as root access to the device from the point of view of their investigative application. Given that one of the unsolved problems of practice is to overcome the iPhone protection system (4s and younger), the hardware ASIC theme IP Box iPhone Password Unlock Tool that has been developed this year and that allows to select the password to the smart phone and tablet of Apple is considered separately. The author also considers the legal status of the information contained in a mobile phone. Separately the article deals with the issue of necessity of obtaining the mobile phone examination order that still remains one of the disputable issues in the investigative practices due to the gap in legislation. It is noted that for successful operation investigators need to be regularly provided with relevant information and development of practical skills through the system of additional vocational training implemented by the Academy of the Investigative Committee of Russian Federation.*

Keywords: *investigative examination, examination of mobile devices, seizure of information, forensic tactics of examination, data recovery, forensic tactic of examination, expert's participation.*

BIBLIOGRAPHY

1. *Aleskerov, V. I., Maksimenko I. A.* Peculiarities of certain investigatory acts during investigation of crimes in the sphere of computer information // Bulletin of the All-Russian Institute of Advanced Training of the Officers of MIA of Russia. 2010. №4(16).
2. *Arkhipova, N. A.* The use of mobile communications capabilities in the detection and investigation of crimes // Collection of works of forensic readings. Barnaul Барнаул, 2014. № 10.

3. *Bazhenov, S. V., Nevsky, E. P., Cherdyntseva, I. A.* Getting information about connections between subscribers and (or) subscriber units // Legislation and Practice. 2011. № 1.
4. *Vardanyan, A. A., Tsykora , A. A.* The legal nature and tactical and forensic features of investigative acts associated with obtaining and analyzing information about telecommunication connections between subscribers and (or) subscriber units // Digest of the Tula State University. Economic and Legal Sciences. 2013. № 4-2.
5. *Vardanyan, A. V., Nikitina, E. V.* Investigation of crimes in the sphere of high technology and computer data. M., 2007.
6. *Gaydin, A. I., Potanin, I. V.* Peculiarities of certain investigative acts during the investigation of criminal fraud committed with the use of cellular communications // Proceedings of All-Russian scientific-practical conference "Criminal procedure and forensic problems of fight against crime." Orel, , 2015.
7. *Zigura, N. A.* The use of special knowledge for detection, removal, fixation and retention of volatile computer data // Vestnik of SUSU. "Pravo" Series. 2007. № 4.
8. *Kerrie, B.* Forensic analysis of file systems. M., 2007.
9. *Mitin, E. V.* The right to confidentiality of messages sent by e-mail: Implementation challenges // Theory and practice of social development. 2012. № 9.
10. *Morozova, E.V., Andronik, N.A.* Tactics of monitoring and recording negotiations: theory and practice problems // Bulletin of the Ural Institute of Economics, Management and Law. "Pravo" Series. 2013. №4(25).
11. *Romanenko, M. A.* Investigative examination in cases concerning criminal violation of copyright in software // Bulletin of Omsk University. "Pravo" Series. 2008. № 1 (14).
12. *Romanenko, M. A.* Forensic digitology - a modern view on the content of forensic equipment // Bulletin of Omsk University. "Pravo" Series. 2007. № 1 (10).
13. Investigative examination. The concept, types and evidentiary value / Ed. by Lutsenko, O.A. Elista, 2007.
14. *Starichkov, M. V.* The tactics of examination and seizure of computer data carriers // bulletin of The East-Siberian Institute of the Ministry of Internal Affairs of Russia. 2012. №2(61).
15. *Stelmakh, V. Y.* Technical and special investigative acts in the Russian criminal procedure // Bulletin of the St. Petersburg State University of the MIA of Russia. 2015. № 1(65).
16. *Fedorov, N. N.* Forensika - Computer Forensics: monograph. M., 2007.
17. *Fedotova, N. V.* On the subject of the privacy of correspondence, telephone conversations, postal, telegraph and other communications // Business in Law. 2008. № 2.
18. *Zykora, A.* Some problems of the investigative act of "obtaining information about the connections between subscribers and (or) subscriber units" // Digest of the Tula State University. Economic and Legal Sciences. 2013. № 3-2.
19. *Shakhmatov, A. V., Bazhukov, V.B.* Operative and investigative examination of electronic data carriers in identifying and detecting crimes in the banking system // Bulletin of the St. Petersburg University of MIA of Russia. 2014. № 2 (62).
20. *Shaifer, S.A.* Investigative acts. Grounds, procedural order and evidentiary value. Samara, 2008.
21. *Shoshin, A. A.* Some problems of defining the concept of "investigative examination" // Bulletin of the Vladimir Law Institute. 2011. № 4 (21).
22. *Yakovlev, N. A.* The legal status of digital information extracted from computer and mobile devices, "e-mail" // Bulletin of Voronezh Institute of Russian Ministry of Internal Affairs. 2014. № 4.