Министерство внутренних дел Российской Федерации

**Федеральное государственное казенное
образовательное учреждение высшего образования
«Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова»**

В.Н. Чаплыгина, В.Ф. Васюков, А.Н. Колычева

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВА

Практические рекомендации

**Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2019**

УДК 343.98
ББК 67.99(2)94
Ч-19

Рецензенты:
А.И. Гайдин, кандидат юридических наук, доцент
(Воронежский институт МВД России);
Л.Г. Делова
(СУ УМВД России по Орловской области)

Чаплыгина, В.Н.

Ч-19 **Тактические особенности использования компьютерной информации при расследовании мошенничества :** практические рекомендации / В.Н. Чаплыгина, В.Ф. Васюков, А.Н. Колычева. – Орел : Орловский юридический институт МВД России имени В.В. Лукьянова, 2019. – 77, [1] с. – 24 экз. – Текст : непосредственный.

В работе рассматривается криминалистическая характеристика мошенничеств, совершаемых с использованием компьютерной информации, а также тактика проведения отдельных следственных действий при расследовании преступлений указанной категории.

Практические рекомендации предназначены для сотрудников органов предварительного следствия, подразделений дознания, преподавателей, адъюнктов, курсантов и слушателей.

Издание представлено в авторской редакции.

УДК 343.98
ББК 67.99(2)94

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире высокие технологии занимают ведущее место и являются неотъемлемой частью практически всех сфер жизнедеятельности человека. Стремительными темпами происходит развитие компьютерных технологий и всесторонняя глобальная информатизация общества, которые влекут за собой, как положительные моменты, так и отрицательные, порождая ряд негативных последствий, одним из которых является криминализация сферы компьютерной информации и информационно-телекоммуникационных сетей связи. Внедрение все более совершенствованных информационных технологий в различные сферы деятельности человека, дает возможность злоумышленникам создавать новые виды преступных посягательств, которые зачастую непосильны в расследовании правоохранительных органов.

Технический прогресс, безусловно, является в большей степени позитивным явлением, улучшающим условия существования людей, делающим эту жизнь более комфортной. Однако, к нашему величайшему сожалению, технический прогресс имеет и обратную сторону, неся ряд негативных последствий. Одним из таких преступных деяний, потребовавших внесения изменений в действующее уголовное законодательство, стало мошенничество в сфере компьютерной информации. Случаи мошенничества, в основе которых лежит использование разнообразной экономически значимой компьютерной информации, в настоящее время получают все большее распространение. Многие пользователи компьютерной информации не уделяют должного внимания ее защите, тем самым облегчая действия мошенников.

На сегодняшний день мошенничество является самым противоречивым и противоправным деянием, так как совершение данного преступления связано с использованием обмана, манипулированием чужого доверия. Мошенничество в сфере компьютерной информации реализуется путем процедур ввода, видоизменения, стирания с жестких носителей или прекращения обращения к данным, имеющимся на компьютере. Данный вид мошенничества, на сегодняшний день является одним из распространенных, ни один гражданин не застрахован, не попасться на уловки злоумышленников, совершающих свои противоправные действия в сфере компьютерной информации.

В методических рекомендациях на основе проведенного исследования представлен юридический анализ сущности и понятия мошенничества в сфере компьютерной информации, произведена дифференциация со смежными составами хищений, совершаемых в сфере информационно-коммуникационных технологий; рассмотрены тактические положения организации и проведения отдельных следственных действий при расследовании мошенничества в сфере компьютерной информации, а также осо-

бенности оценки результатов, полученных в ходе данных следственных действий. Выявлены и исследованы проблемы, возникающие у следователей при квалификации указанной группы хищений, а также при взаимодействии с организациями и учреждениями, которые в установленном порядке хранят электронные сведения, имеющие значение для уголовного дела.

Актуальность подготовленной работы обусловлена увеличением числа преступлений в информационной сфере и выходом новых разъяснений Верховного суда Российской Федерации по поводу практики применения статьи о мошенничестве в сфере компьютерной информации.

Целью методических (практических) рекомендаций является рассмотрение мошенничества в сфере компьютерной информации в уголовно-процессуальном и криминалистическом аспектах, достижение которой возможно посредством междисциплинарного (системного) анализа основных проблем теории и практики с учетом положений постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Уголовная ответственность за мошенничество в сфере компьютерной информации установлена Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», которым уголовный закон был дополнен ст. 159.6 «Мошенничество в сфере компьютерной информации».

Родовым объектом мошенничества в сфере компьютерной информации являются экономические отношения – социальные взаимосвязи, складывающиеся в связи с производством, распределением, обменом и потреблением хозяйственных благ и ценностей. Одна из отличительных особенностей современной экономики – ее постиндустриальный характер, связанный с взрывообразным развитием электронно-информационных технологий. Новые виды экономических отношений начали зарождаться с появлением компьютерных устройств, систем и их сетей, которые дублируют предпринимательскую и иную экономическую деятельность, картотеки, архивы и т.д. Первостепенной чертой постиндустриализма является появление компьютерно-технологического производства. Оно основано на получении дохода и прибыли через использование соответствующих знаний, технологий, информации: интернет-аукционы, биржи, интернет-валюты, электронные платежные системы и пр.[1]

Видовым объектом мошенничества в сфере компьютерной информации следует считать отношения собственности. В уголовном праве России собственности присуще экономико-правовое (комплексное) понимание. В уголовно-правовом смысле указанной категорией охватываются:

а) собственнические отношения (общественные отношения, складывающиеся в связи с реализацией права владения, пользования и распоряжения имуществом, находящимся в частной, государственной, муниципальной и иной формы собственности граждан и юридических лиц, а также Российской Федерации, субъектов Российской Федерации, муниципальных образований);

б) другие вещные отношения (общественные отношения, складывающиеся в связи с реализацией таких вещных прав, как право хозяйственного ведения имуществом, право оперативного управления имуществом, сервитуты и др.);

в) обязательственные отношения (общественные отношения, складывающиеся в силу возникновения договорных и иных обязательств, когда

[1] Григорян Г.Р. Об объекте мошенничества в сфере компьютерной информации // Российская юстиция. 2018. № 5. С. 29–31.

одно лицо (должник) обязано совершить в пользу другого лица (кредитора) определенное действие, как то: передать имущество, выполнить работу, оказать услугу, внести вклад в совместную деятельность, уплатить деньги и т.п., либо воздержаться от определенного действия, а кредитор имеет право требовать от должника исполнения его обязанности); г) иные имущественные отношения[1].

Для мошенничества характерен видовой объект в виде, прежде всего, экономически совершенных форм собственности – акционерной, банковской, корпоративной. Основным непосредственным объектом мошенничества в сфере компьютерной информации являются конкретные имущественные отношения[2].

При этом согласно примечанию к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Отличительными чертами компьютерной информации являются: 1) неотделимость компьютерной информации от носителя; 2) виртуальность, которая означает, что только благодаря специальным устройствам, как обеспечивающим доступ к такой информации, так и позволяющим производить различные операции с такой информацией (копирование, изменение, распространение), она становится доступной для восприятия; 3) трансграничность, которая указывает на то, что компьютерная информация может без особых усилий перемещаться из одного устройства в другое и от одного пользователя к другому.

Под компьютерной информацией **как средством совершения преступления, предусмотренного ст. 159.6 УК РФ,** необходимо считать сведения, хранящиеся, обрабатываемые, принимаемые и передаваемые предназначенными для этих целей и снабженными соответствующим программным обеспечением техническими устройствами, функционирование которых основано на любых (различных) физических принципах действия[3].

Анализ конструкции ст. 159.6 УК РФ позволил выделить совершение рассматриваемых хищений на две группы технических средств, в работу которых происходит вмешательство:

1) средства хранения, обработки или передачи компьютерной информации;

2) информационно-телекоммуникационные средства.

Основываясь на положениях Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите

---

[1] Безверхов А.Г. О некоторых вопросах квалификации вымогательства // Уголовное право. 2016. № 2. С. 4–5.

[2] Григорян Г.Р. Об объекте мошенничества в сфере компьютерной информации // Российская юстиция. 2018. № 5. С. 29–31.

[3] Яни П.С. Специальные виды мошенничества // Законность. 2015. № 8. С. 35–40.

информации», который рассматривает **информационно-телекоммуникационную сеть** как *технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники*[1], представляется, что разница между средствами хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационными средствами заключается только в наличии технической возможности **передачи** информации по линиям связи. С учетом того, что подавляющее число средств хранения, обработки или передачи компьютерной информации в настоящее время имеет доступ к линиям связи, полагаем, что собственно средствами хранения, обработки или передачи компьютерной информации являются *карты памяти различных видов*[2] и *компьютеры, не подключенные к каким-либо линиям связи* (в том числе и к локальным сетям)[3].

Непосредственно действия по реализации преступного замысла производятся путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства.

Под **вводом** компьютерной информации следует понимать размещение сведений о средствах хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей для последующей обработки и (или) хранения данных сведений[4].

Удаление информации следует интерпретировать как действия, направленные на приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления.

При этом **блокирование** предусматривает осуществление системы действий фигуранта, направленные на изменение информации последствием которой является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме[5]. В свою очередь, блокирование информации, хотя ограничивает или закрывает доступ к компьютерному оборудованию и находящимся на нем ресурсам, не предполагает удаление компьютерной информации[6]. **Модификация** компьютерной информации

---

[1] Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1), ст. 3448.

[2] Степанов-Егиянц В.Г. Новая редакция статьи 274 Уголовного кодекса РФ: проблемы и пути решения // Мониторинг правоприменения. 2014. № 2. С. 18–23.

[3] Барчуков В.К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. 2016. № 5. С. 41–46.

[4] Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С. 27–28.

[5] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: утв. Генпрокуратурой России. Доступ из справ.-правовой системы «КонсультантПлюс».

[6] Барчуков В.К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. 2016. № 5. С. 41–46.

выражается во внесении изменений в компьютерную информацию (или ее параметры).

При этом в соответствии с п. 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» по смыслу ст. 159.6 УК РФ **вмешательством** в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается *целенаправленное* **воздействие** *программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.*

Особый интерес представляет позиция, указанная в рассматриваемом постановлении, которая указывает на необходимость **дополнительной квалификации** по ст. 272, 273 или 274.1 УК РФ в случае, если мошенничество в сфере компьютерной информации совершается *посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ.*

Таким образом, при реализации действий, направленных на хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей фигурант осуществляет доступ к компьютерной информации, которая не охраняется определенными нормативными режимами.

Так, например, М., работая в период с 5 октября 2016 года по 15 мая 2017 года в должности специалиста по сопровождению корпоративных клиентов Поволжского филиала – Саратовского регионального отделения ПАО «МегаФон», получив индивидуальный и конфиденциальный логин и пароль для работы в компьютерных программах, содержащих данные клиентов и персональные данные их лицевых счетов, находясь в офисе по адресу: г. Саратов, ул. Университетская, дом № 28, умышленно, из корыстных интересов, подключала к лицевому счёту номера, зарегистрированные на «...», с находящимися на нём денежными средствами, принадлежащими ПАО «МегаФон». Убедившись, что на указанном выше лицевом счете находятся денежные средства, в информационно-биллинговой системе изменила категорию клиента с «кредитный» на «предоплатный», статус клиента с «временно закрыт» на «действующий», класс клиента с «аннулированный» на «корпоративный».

Далее М. осуществила перевод денежных средств со счёта «...» на свой лицевой счёт, зарегистрированный на вымышленное имя и находящийся в пользовании М., похитив, тем самым, денежные средства в сумме 28 853 руб. 24 коп., и, получив реальную возможность ими распоряжаться.

Приговором Фрунзенского районного суда г. Саратова 19 июля 2018 года М. была признана виновной в совершении преступления, предусмотренного ч. 3 ст. 159.6 УК РФ, ей назначено наказание в виде лишения свободы сроком на 2 года (условным с испытательным сроком)[1].

Термин «охраняемая законом информация» имеет разные интерпретации в доктрине и правоприменительной практике. Зачастую под «охраняемой законом информацией» понимается информация, охрана которой прямо предусмотрена законом[2].

Данная позиция косвенно подтверждена в тексте Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3], в котором определены две основные категории информации. Первая категория — это общедоступная информация, к которой относятся общеизвестные сведения, а также иная информация, доступ к которой не ограничен (ст. 7 Федерального закона «Об информации, информационных технологиях и о защите информации» – далее Федерального закона об информации). Ко второй категории относится информация, доступ к которой ограничен законом (ст. 9 Федерального закона об информации). Как отмечают некоторые исследователи, «само существование такого разделения информации говорит об отсутствии уголовно-правовой защиты общедоступной информации от неправомерного доступа»[4]. Исходя из текста закона, по мнению сторонников такой интерпретации, общедоступная информация может использоваться любыми лицами без ограничений.

В ст. 9 Федерального закона об информации содержится прямое указание на то, что «ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства». Схожая позиция отражена в утвержденных Генеральной прокуратурой России методических рекомендациях, где под «охраняемой законом» понимается та информация, «для которой законом установлен специальный режим ее правовой защиты (например,

---

[1] Приговор Фрунзенского районного суда г. Саратова от 19 июля 2018 г. по делу № 1-66/2018.

[2] Дремлюга Р.И.Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 52–58.

[3] См.: Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: в ред. от 25 ноября 2017 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

государственная, служебная и коммерческая тайна, персональные данные и т.д.)»[1]. В данном методическом документе информация подразделена на ту, для которой явно установлен режим правовой защиты, и остальную, которая не является предметом преступления, предусмотренного ст. 272 УК РФ.

Подобную точку зрения можно встретить и в некоторых судебных решениях. *Так, в приговоре Верховного суда Чувашской Республики подчеркивается, что «компьютерная информация должна быть охраняема законом, то есть в отношении информации должен быть законом установлен специальный режим ее правовой защиты». Обвиняемому инкриминировали незаконную модификацию компьютерной информации на интернет-сайте образовательного учреждения, но так как сайт «является открытым и общедоступным, то информация на сайте является открытой и общедоступной» и не подлежит уголовно-правовой охране, по мнению суда. Согласно тексту данного приговора предметом преступления, предусмотренного ст. 272 УК РФ, является только компьютерная информация, охраняемая законом, поскольку «в отношении информации должен быть законом установлен специальный режим ее правовой защиты»*[2].

В правоприменительной практике существуют примеры, когда суд требовал от обвинения указать нормативные акты, закрепляющие охрану информации, к которой осуществлен неправомерный доступ. *Например, по инициативе суда уголовное дело возвращено прокурору «в связи с нарушением уголовно-процессуального закона, выразившемся в том, что ... в предъявленном обвинении по ч. 2 ст. 272 УК РФ отсутствует указание на положение закона или нормативно-правовой акт, в силу которого компьютерная информация, доступ к которой, по версии следствия, был осуществлен обвиняемым, является охраняемой законом информацией»*[3].

Позиция, когда к предмету преступления, предусмотренного ст. 272 УК РФ, относят только информацию, доступ к которой прямо ограничен законом, имеет очевидные преимущества: когда это явно определено в законе, на практике гораздо проще установить, является ли неправомерный доступ к определенному виду информации преступлением.

Чаще всего в законах, устанавливающих охраняемость того или иного вида информации, подробно регламентированы режим доступа к такой информации и порядок ознакомления других лиц в связи с тем, что такая информация является охраняемой по закону и т.д. Например, в ст. 5 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» перечислены сведения, которые не могут составлять коммерческую тайну, а ст. 10 и 11

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: утв. Генпрокуратурой России. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Апелляционный приговор Верховного суда Чувашской Республики от 3 июня 2015 г. по делу №22-1054/2015.

[3] Апелляционное постановление судебной коллегии по уголовным делам Верховного суда Республики Тыва от 26 октября 2017 г. по делу № 22-1534/2017.

определяют основные требования к организации доступа и мерам защиты коммерческой тайны[1].

В законе перечислены виды информации, которые не могут являться коммерческой тайной, но нет указания на то, что может относиться к такой информации. Статья 4 гласит: «Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона». То есть обладатель самостоятельно решает, какая информация является коммерческой тайной, и определяет режим доступа и круг лиц, имеющих к ней доступ.

Информация должна быть помечена грифом «коммерческая тайна» с указанием ее обладателя (ст. 10 Федерального закона «О коммерческой тайне»), чтобы считаться таковой. Отсутствие пометки означает, что режим коммерческой тайны не может считаться установленным[2]. Согласно Закону РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» информация, охраняемая законом, также должна помечаться соответствующим грифом, что является мерой по информированию о том, что доступ к данной информации ограничен. Право на отнесение информации к государственной тайне есть у органов государственной власти и должностных лиц Российской Федерации (ст. 3 Федерального закона «О государственной тайне»). Данный нормативный акт содержит перечень широких категорий информации, которая может быть отнесена к государственной тайне, но в каждом конкретном случае обладатель выбирает режим доступа к информации самостоятельно из трех предложенных («особой важности», «совершенно секретно» и «секретно»). Даже в случаях, когда компьютерная информация является охраняемой на основании прямого указания в законе, именно обладатель определяет ее режим. Более того, несмотря на указание в законе, в силу которого информация может рассматриваться как охраняемая, необходимо, чтобы обладатель указал ее в качестве таковой[3].

При этом лицо, совершающее мошенничество в сфере компьютерной информации в «чистом» виде не должен использовать заблаговременно созданные вредоносные компьютерные программы.

В целях определения момента окончания мошенничества в сфере компьютерной информации необходимо руководствоваться разъяснениями Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором зафиксировано, что мошенничество

---

[1] О коммерческой тайне [Электронный ресурс]: Федер. закон Рос. Федерации от 29 июля 2004 г. № 98-ФЗ: в ред. от 18 апреля 2018 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Постановление Суда по интеллектуальным правам от 5 мая 2014 г. № С01-331/2014 по делу № А40-41976/2013.

[3] Дремлюга Р.И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 52–58.

окончено с момента, когда имущество поступило в незаконное владение виновного или иных лиц, и у них появилась реальная возможность пользоваться или распоряжаться им по своему усмотрению[1]. В этом случае у лица, совершившего мошенничество в сфере компьютерной информации, появляется реальная возможность распоряжаться денежными средствами, поступившими на счет, по личному усмотрению, с момента их зачисления.

С **субъективной стороны** преступное деяние, предусмотренное ст. 159.6 УК РФ, характеризуется прямым умыслом, т.е. субъект понимает общественную опасность своих действий, ориентированных на хищение или приобретение права на чужую собственность, предвидит вероятность или неизбежность наступления отрицательных последствий и желает их наступления. Неотъемлемым признаком является корыстная цель – стремление лица получить материальную выгоду.

Субъект преступления – общий, физическое вменяемое лицо, достигшее возраста 16 лет.

В силу своих качеств, у информации отсутствует владелец, имеется только обладатель. Данный аспект нашел свое отображение в ряде законодательных актов информационной отрасли права. Используя термин информационного объекта, необходимо иметь в виду, что информация, обладая стоимостью, не считается имуществом. Следовательно, проблема о возможности рассмотрения информационной вещи как предмета мошенничества, на сегодняшний день не может решаться единым образом и поэтому требуется дальнейшая проработка данного вопроса.

Специфика состоит в том, что компьютерные средства не считаются следами преступления, потому как не обладают отличительными особенностями, однако при этом несут на себе следовую картину преступления. Это подтверждает изучение следственной практики, когда, к примеру, при производстве следственных действий из компьютерного устройства изымается лишь его «жесткий диск» – т.е. запоминающее устройство, предназначенное для хранения информации. Многие ученые полагают, что ключевой отличительной особенностью компьютерной техники является их способность сохранять информацию.

В соответствии с п. 19 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» **электронное средство платежа** – это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информаци-

[1] Иванченко Р. Б., Малышев А. Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России. 2014. № 1. С. 194–200.

онно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

В п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», предметом хищения и иного имущественного преступления признаются безналичные денежные средства, в том числе электронные денежные средства.

Следует особо подчеркнуть, что квалифицирующим составом мошенничества в сфере компьютерной информации является деяние, совершенное с банковского счета и (или) в отношении электронных денежных средств (п. «в» ч. 3 ст. 159.6 УК РФ).

При этом под **«электронными денежными средствами»** принято понимать денежные средства, которые предварительно предоставлены одним лицом другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. К электронным средствам платежа относятся: средства и (или) способы, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Положительным примером расследования преступлений о хищении в сфере компьютерной информации может служить уголовное дело № 678578 (Чувашская Республика), в ходе расследования которого установлено, что Гасанов Р.Р. и Колонщаков А.В. совместно с неустановленным пользователем сети Интернет под псевдонимом «Den Adel» («Robusto») путем подбора электронно-цифровой подписи и неправомерного доступа к аутентификационным данным агента, похитили денежные средства с расчетного счета ООО «СимМетрия» в платежной системе «КиберПлат» банка «Платина» на общую сумму более 3 млн рублей. Похищенные денежные средства перечислялись соучастниками на лицевые счета абонентских номеров оператора сотовой связи ОАО «ВымпелКом» и использовались ими по своему усмотрению. Уголовно дело направлено в суд Следственным департаментом МВД России. Действия Гасанова Р.Р. и Колонщакова А.В. квалифицированы по ч. 3 ст. 159.6 УК Российской Федерации. В суде состоялся обвинительный приговор, виновные получили наказание в виде лишения свободы сроком на 2 года условно.

Также, в г. Новосибирске окончено производством уголовное дело № 21139 по обвинению Миколенко Д.С. в совершении мошенничества в сфере компьютерной информации путем модификации данных по лицевым счетам умерших вкладчиков Сибирского банка ОАО «Сбербанк России», дальнейшего перевода денежных средств на подконтрольные ему счета, открытые в указанном банке, и хищения этих средств. Центральным районным судом г. Новосибирска Миколенко Д.С. признан виновным в совершении инкриминируемых ему преступлений, предусмотренных ч. 1 ст. 159.6, ч. 1 ст. 159.6, ч. 4 ст. 159.6, ч. 1 ст. 174.1 УК РФ и приговорен к 3 годам 2 месяцам лишения свободы.

Как уже нами упоминалось выше, мошенничество в сфере компьютерной информации криминализировано Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», вступившим в законную силу 29 ноября 2012 г. С момента появления данного состава в форме статьи 159.6 УК РФ у практиков и ученых возникают несколько дискуссионных вопросов о соотношении «компьютерного» мошенничества, «основного» мошенничества и кражи. Все это приводило к разночтениям закона в теории и на практике, не способствовало единообразию правоприменения и реализации принципа законности уголовного судопроизводства. При этом в связи с бурным развитием информационных технологий возросло число преступлений, совершаемых в информационной сфере, в том числе сети Интернет.

Диспозиция ст. 159 УК РФ определяет «мошенничество» как: хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверия.

Упоминая о мошенничестве в сфере компьютерной информации, следует подчеркнуть, что в ст. 159.6 УК РФ законодатель определил данный термин следующим образом: мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Так какое же из перечисленных нами видов мошенничества наносит наиболее значимые общественно-опасные последствия? Для ответа на данный вопрос, с точки зрения законодателя, необходимо обратиться к санкциям вышеуказанных статей уголовного закона. Говоря о «обычном мошенничестве», то в санкции ч. 1 ст. 159 УК РФ, то максимальное наказание по данной части составляет 2 года лишения свободы. В санкции ч. 1 ст. 159.6 УК РФ предельное наказание за совершенное преступление составляет арест лица до 4 месяцев. Из приведенных санкций за вышеуказанные преступления можно сделать вывод, что «мошенничество» предусматривает более суровое наказа-

ние, чем «компьютерное мошенничество». Позиция законодателя по данному вопросу полна критики и противоречий[1].

По небезапелляционному суждению, высказанному в литературе, законодатель не определил последствий совершения преступления в сфере компьютерной информации, ведь последствия наносят более существенных вред общественным отношениям, чем у «мошенничества» определенного в ст. 159 УК РФ.

Во-первых, это связано с получением полной персональной информации о человеке, которая впоследствии может быть неоднократно применена в корыстных целях. К такой информации можно отнести: сведения о банковских реквизитах, пароли от платежных карт, номер расчетного счета, номер мобильного телефона, сведения об электронном кошельке и т.д.[2]

Во-вторых, полученная информация может и не использоваться самостоятельно лицом, осужденным за данное преступление, но в дальнейшем такая информация может быть продана или передана другим лицам для совершения преступления.

В-третьих, похищенные данные в большинстве случаев попадает в открытые банки данных, пользователи которых с легкостью узнают персональную информацию о лице, в отношении которого было совершено мошенничество в сфере компьютерной информации[3].

В целях устранения возникающих на практике проблем правоприменения ст. 159.6 УК РФ Пленум Верховного Суда Российской Федерации 30 ноября 2017 г. впервые дал официальные разъяснения по вопросу квалификации мошенничества в сфере компьютерной информации в своем постановлении № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

В связи с изданием постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» и значительной долей преступлений, совершаемых в информационной сфере, множеством различных подходов к пониманию сущности мошенничества в сфере компьютерной информации является актуальным изучение соотношения мошенничества в сфере компьютерной информации с основным составом мошенничества и кражей.

Согласно положениям Пленума не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномо-

---

[1] Степанова К.В., Федоров А.С. О соотношении наказания за мошенничество и мошенничество в сфере компьютерной информации // Аллея науки. 2018. Т. 3. № 6 (22). С. 865–868.

[2] Русскевич Е.А. Мошенничество в сфере компьютерной информации (статья 159.6 УК РФ): неявные выгоды криминализации и очевидные проблемы применения // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 5 (55).

[3] Степанова К.В., Федоров А.С. Указ. соч. С. 865–868.

ченного работника кредитной организации. В этом случае содеянное следует квалифицировать как кражу.

В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража.

Такая позиция обусловлена тем, что в соответствии со ст. 128 ГК РФ, которая обозначает, что безналичные и электронные денежные средства относятся к имуществу, а не к праву на имущество, в связи с чем такие средства являются предметом хищения, а не мошенничества в форме приобретения права на имущество.

Согласно п. 20 постановления вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей должно признаваться любое целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, компьютеры, смартфоны, указанные сети, которое:

- нарушает установленный процесс обработки, хранения, передачи компьютерной информации;

- как следствие, позволяет «виновному или иному лицу» незаконно завладеть чужим имуществом или приобрести право на него.

Таким образом, с точки зрения Верховного Суда, вполне допустимой является ситуация, когда незаконное вмешательство осуществляется одним лицом, а хищение – другим. При отсутствии признаков незаконного вмешательства в работу серверов, компьютеров, самих информационно-телекоммуникационных сетей содеянное квалифицируется как кража, в том числе и в случаях, когда последствием такого хищения является изменение данных о состоянии банковского счета и (или) о движении денежных средств.

Важным для правоприменителя следует расценить указание на то, что, если хищение осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая Интернет, содеянное расценивается как «традиционное» мошенничество. Действительно, при создании поддельных сайтов, использовании электронной почты для «обманных» рассылок не происходит воздействия на функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Небезосновательно в литературе выражаются сомнения по указанию в постановлении на необходимость совокупной квалификации ст. 159.6 и ст. 272, 273 или 274.1 УК РФ. Дело в том, что неправомерный доступ к компьютерной информации, а также создание, использование и распространение вредоносных компьютерных программ, совершенные в целях хищения, т.е. сами по себе, уже являются тем или иным видом «вмешательства». Таким об-

разом, перечисленные действия являются неотъемлемой, имманентной составной частью объективной стороны «компьютерного» мошенничества в силу буквального понимания самой ст. 159.6 УК (в отличие, например, от использования поддельного официального документа, чужих личных либо иных официальных документов при совершении иных видов мошенничества), и квалификация по совокупности соответствующих преступлений нарушит запрет двойного вменения[1].

Общими чертами мошенничества в сфере компьютерной информации с основным составом мошенничества и кражей является объект посягательства – право собственности, что вытекает из структурного расположения таких статей в гл. 21 «Преступления против собственности».

Наиболее близким по содержанию мошенничеству в сфере компьютерной информации является кража. Сходство связано с тем, что преступление, предусмотренное ст. 159.6 УК РФ, согласно диспозиции статьи, является хищением, как и кража (ст. 158 УК РФ). Роднит два этих состава преступления и то, что они оба имеют своим последствием лишение кого-либо права собственности на конкретную вещь при отсутствии осведомленности в момент совершения преступного деяния об этом собственника вещи, то есть тайно и с корыстной целью. При этом существенное отличие состоит в том, что при краже преступник для завладения вещью оказывает на последнюю непосредственное физическое воздействие, что отсутствует при совершении мошенничества в сфере компьютерной информации, которое совершается исключительно путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[2].

Помимо этого в случае, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети, то такие действия в соответствии с п. 21 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» должны квалифицироваться как кража. Отличие между сравниваемым составами преступлениями состоит и в субъекте, которым в силу ст. 19, 20 УК РФ по ст. 158 УК РФ может быть физическое вменяемое лицо, достигшее возраста 14 лет, а по ст. 159.6 УК РФ – 16 лет.

---

[1] Кибальник А.Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда Рос. Федерации // Уголовное право. 2018. № 1. С. 61–67.

[2] Рогова Н.Н., Окишева Н.В. Соотношение мошенничества в сфере компьютерной информации с основным составом мошенничества и кражей // Общество. Наука. Инновации (НПК-2018): сборник статей XVIII Всероссийской научно-практической конференции. В 3 т. Вятский государственный университет, 2018. С. 710–717.

Как следует из содержания диспозиции и названия статьи 159.6 Уголовного кодекса Российской Федерации, преступление является разновидностью мошенничества наряду с составами преступлений, предусмотренных ст. 159.1–159.5 УК РФ.

Исходя из анализа диспозиции ст. 159 УК РФ, можно сделать вывод о том, что мошенничество это не что иное, как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Обман как способ осуществления мошенничества в сфере компьютерной информации в диспозиции ст. 159.6 УК РФ в отличие от ст. 159.1–159.5 УК РФ не предусмотрен. Данное обстоятельство подтверждается положением, изложенном в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 о том, что подобные преступления совершаются не путем обмана или злоупотребления доверием, то есть мошенничество в сфере компьютерной информации не является разновидностью мошенничества в классическом понимании данного понятия.

Помимо прочего, отличие от основного состава мошенничества согласно постановлению Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» выражается в том, что если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, то такое мошенничество следует квалифицировать по ст. 159 УК РФ, а не ст. 159.6 УК РФ.

Особого внимания заслуживают изменения, внесенные в п. 4 примечания к ст. 158 и примечание к ст. 159.1 УК РФ, в соответствие с которыми крупный и особо крупный размер хищения стал пониматься одинаково для кражи и основного состава мошенничества, а также преступлений, предусмотренных ст. 159.3 и 159.6 УК РФ. Установление Федеральным законом от 29 ноября 2012 г. № 207-ФЗ для преступлений, предусмотренных ст. 159.3 и ст. 159.6 УК РФ, более высоких по сравнению с кражей и основным составом мошенничества пороговых сумм для определения крупного и особо крупного размера подвергалось критике со стороны ученых и практиков[1].

Кроме того, с учетом того что предметом преступлений, предусмотренных ст. 159.3 и ст. 159.6 УК РФ, являлись безналичные и электронные денежные средства, которые к предмету кражи долгое время не относились, складывалась ситуация, когда аналогичные по сути хищения по-разному наказывались в зависимости от того, обратил виновный в свою пользу денежные средства потерпевшего в наличном или безналичном виде[2].

---

[1] Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4–9.

[2] Архипов А.В. Актуальные вопросы квалификации хищения безналичных денежных средств // Вестник Томского государственного университета. 2017. № 418. С. 195–198.

2. ТАКТИКА ПРОВЕДЕНИЯ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗВАНИЕМ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Тактика допроса. Подготовке к производству допроса в криминалистической литературе уделяется самое пристальное внимание, однако, по уголовным делам о мошенничествах, совершенных с использованием компьютерной информации она заключается в необходимости предварительной подготовки документов: выписки по транзакциям, совершаемых по банковским счетам, распечатки сведений о соединениях по абонентскому номеру, копии документации, подтверждающей осуществление хищения у потерпевшего.

Особенность проведения допроса при расследовании преступлений с использованием компьютерной информации выражается в отражении в протоколе *допроса потерпевшего* следующей информации: в какой кредитной организации, когда и какой именно счет открывался, условия пользования данным счетом; когда именно подключалась услуга дистанционного банковского обслуживания, разъяснялись ли сотрудниками банка условия пользования данной услугой; какой абонентский номер был прикреплен к дистанционному банковскому обслуживанию, как давно им пользовался потерпевший и когда перестал пользоваться, по какой причине.

Если абонентский номер зарегистрирован на другое лицо, необходимо допросить данное лицо, с указанием времени и причин передачи данного абонентского номера потерпевшему. Если допросить не представляется возможным, необходимо допросить иных лиц, которые могут подтвердить факт пользования потерпевшим данным абонентским номером); информировал ли банк о прекращении пользования абонентским номером, к которому привязана услуги дистанционного банковского обслуживания, если да, то когда и каким образом, если нет, то по какой причине; когда обнаружил пропажу денежных средств со счета, при каких обстоятельствах (к материалам уголовного дела приобщаются сведения, подтверждающие факт снятия денежных средств со счета); какие меры предпринял для установления причин списания денег со счета, а также предотвращения дальнейшего хищения денег; является ли причиненный в результате преступления ущерб значительным, если да, то к материалам дела приобщаются документы, подтверждающие данное обстоятельство (сведения о доходах потерпевшего и проживающих совместно с ним членов семьи, справка о составе семьи и т.д.)[1].

[1] Куприянов Е.И., Крашенинников С.В. Особенности производства отдельных следственных действий при расследовании преступлений, связанных с хищением денежных средств со счетов банковских карт посредством использования электронных платежных систем // Рос. следователь. 2018. № 6. С. 11–14.

Представляет особый интерес ситуация, получившая в настоящее время типичный характер, когда следователем предлагается потерпевшему в рамках проведения допроса, либо осмотра документа получить доступ к его личному абонентскому кабинету в целях получения детализации соединений за интересующий следствие период. Техническая особенность получения детализации счета из личного кабинета предполагает необходимость использования SIM-карты потерпевшим, которая была помещена в мобильное устройство в период, интересующий следствие. Только в этом случае имеется возможность получения доступа к личному кабинету. В связи с этим также возникает вопрос – возможно ли следователю получить информацию из личного кабинета абонента без его согласия? Представляется, что нет, так как технически автоматическая выборка соединений, производимая абонентом в сети Интернет, является разновидностью детализации входящих и исходящих соединений, которая в соответствии с позицией Конституционного Суда Российской Федерации, отраженной в определении от 2 октября 2003 г. № 345-О[1], охраняется тайной телефонных переговоров. Отличие такой детализации от представляемой оператором сотовой связи заключается лишь в том, что в ней не приводятся сведения об идентификационных номерах и адресах базовых станций, с помощью которых происходили соединения.

При допросе свидетелей непосредственно преступных действий следователю необходимо обратить внимание на два основных обстоятельства: на действия наблюдаемого лица по совершению преступления и на его приметы. Конкретизация этой части показаний позволит в будущем опровергнуть показания подозреваемого (обвиняемого), направленные на искажение своей роли в совершении мошенничества, а также сделает возможным проведение предъявления для опознания.

Учитывая отсутствие в настоящее время у подавляющего большинства следователей необходимых специальных знаний по делам рассматриваемой категории, при подготовке к допросу свидетелей им следует значительное внимание уделять изучению специальных вопросов, которые могут возникнуть в ходе его проведения. С этой целью перед началом допроса следователь должен: изучить специальную литературу; проконсультироваться с соответствующим специалистом; еще раз ознакомиться с результатами осмотра места происшествия, документов и иных предметов.

При определении круга участников допроса необходимо обратить внимание на то обстоятельство, что число лиц, которых возможно использовать в качестве свидетелей по таким уголовным делам, как правило, дос-

---

[1] Об отказе в принятии к рассмотрению запроса Советского районного суда г. Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи»: определение Конституционного Суда Рос. Федерации от 2 октября 2003 г. № 345-О // Вестник Конституционного Суда Рос. Федерации. 2004. № 1. С. 52.

таточно велико, поэтому при определении круга и очередности их допросов следует исходить из объема данных, которыми они могут располагать, и сложившейся на данный момент следственной ситуации.

Как показывает изучение следственной практики, допрос свидетелей происходит в условиях бесконфликтной ситуации. Однако это не означает, что достоверность показаний опрашиваемого будет при этом гарантирована. Анализ материалов уголовных дел показывает, что мошенничества совершаются в течение небольшого периода, в связи, с чем свидетелям в ходе допросов приходится вспоминать о прошедших событиях, поэтому важным в тактическом отношении является использование следователем различных способов активизации ассоциативных связей в памяти допрашиваемого. С той целью целесообразно первый допрос (если позволяет обстановка) провести уже на месте происшествия после его осмотра.

В зависимости от обстоятельств совершенного преступления, собранных доказательствах по делу, личности подозреваемого, последний может быть задержан в порядке ст. 91 УПК РФ, а за тем по решению суда в отношении последнего может быть применена мера пресечения в виде заключения под страду. В обязательном порядке в отношении подозреваемого необходимо избрать меру пресечения.

При допросе подозреваемого (обвиняемого) необходимо выяснять: обстоятельства, характеризующие его личность; где, когда отбывал наказание; от кого узнал о способе совершения мошенничества; почему решил совершать данный вид преступления; какие телефоны, телефонные номера, использовал при совершении мошенничества; на кого они были оформлены; как попали к нему; знали ли лица, на кого оформлены федеральные телефонные номера, для чего номера используются; на какие федеральные телефонные номера рассылал SMS-сообщения; их содержание, только ли он рассылал сообщения, если нет, то объяснял ли он участвующему цель их рассылки; где находился в момент разговоров с потерпевшими; что именно говорил потерпевшим для достижения своей цели; с использованием какой платежной системы и куда именно (на федеральные телефонные номера, пластиковую карту, счет платежной системы) перечислял денежные средства; порядок, способ, алгоритм перечисления денежных средств; кто, где, когда получал денежные средства, похищенные у потерпевших; в каких суммах; на что потрачены полученные путем мошенничества денежные средства; где в настоящее время находятся SIM-карты и мобильные телефоны, используемые при совершении мошенничества; признает ли вину в совершенном преступлении и т.д.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами по своей правовой сущности и направленности решает вопрос о получении новых доказательств путем ограничения конституционного права российских граждан на тайну телефонных переговоров. Подчеркнем, что речь идет о гражданах, которые в силу различ-

ных обстоятельств вовлечены в уголовное судопроизводство и имеют различный уголовно-процессуальный статус.

Задача следователя (дознавателя) состоит в том, чтобы установить данные, дающие основание полагать, что информация о входящих и исходящих сигналах соединения телефонных аппаратов используемых мошенниками может содержать сведения, имеющие значение для расследуемого преступления.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами следует проводить на первоначальном этапе расследования, так как полученные сведения могут указывать на лиц, с которыми общается субъект преступления, дату и продолжительность общения. По вескому замечанию Н.Г. Шурухнова, в последующем это позволит использовать полученную информацию в целях определения мест проведения обыска, выяснения истинных намерений подозреваемого, обвиняемого, установления его связей, покровителей, несущих по закону материальную ответственность за противоправные действия субъекта преступления, что позволит целенаправленно провести наложение ареста на имущество[1].

Производя оценку и анализ следственной ситуации, следователь (дознаватель) должен иметь в виду, что в одном и том же телефонном аппарате могут использоваться как одновременно, так и самостоятельно несколько SIM-карт, они могут меняться, переставляться в другие мобильные устройства, номерные значения нередко вводятся абонентами при пользовании ресурсами Интернета.

Обязательным требованием при расследовании любого преступления, стала идентификация абонентского устройства – определения его IMEI и (или) абонентского номера, а также определения местонахождения телефонного аппарата относительно базовой станции. Все это взаимосвязанные процессуальные действия и могут рассматриваться судами в рамках ст. 186.1 УПК РФ.

Принятие решения о производстве рассматриваемого следственного действия предполагает дополнительное изучение и анализ материалов дела, из которых усматривалась бы необходимость получения информации о соединениях между абонентами и (или) абонентскими устройствами[2]. Этому может предшествовать приобщение к уголовному делу материалов, свидетельствующих о том, что соединения, сопутствующие телефонному

---

[1] Шурухнов Н.Г., Жбанков В.А. Методика расследования преступлений, связанных с невозвращением из-за границы средств в иностранной валюте // Криминалистика: учебник / под ред. Засл. юриста Российской Федерации, д-ра юрид. наук, проф. В.А. Жбанкова. М., 2012. С. 357–374.

[2] Резцов А.В. Информация о соединениях между абонентами сотовой связи при установлении обстоятельств совершенного преступления // Законность. 2011. № 11. С. 19–21.

звонку интересующих следствие лиц, могут содержать информацию, представляющую интерес для расследования конкретного преступления. Интересующие следователя (дознавателя) данные могут содержаться в процессуальных документах, таких как протоколы допросов различных участников уголовного судопроизводства, справки органа дознания о проведении отдельных оперативно-розыскных мероприятий или оперативно-розыскного сопровождения расследуемого преступления[1].

Рассматриваемое следственное действие возможно провести при наличии достаточных оснований полагать, что информация имеет значение для расследования преступления. Это означает, что требуется совокупность сведений, позволяющих выдвинуть обоснованное предположение, что данные о соединениях между абонентами и (или) абонентскими устройствами будут иметь значение для расследования.

Так, благодаря исследованию детализации телефонных переговоров по резонансному уголовному делу, возбужденному в отношении членов организованной преступной группы, деятельностью которой руководила Цапок Н.А., следователем было доказано, что разговоры, которые вели между собой указанные лица, подтверждают причастность подсудимых к совершению преступления в составе организованной группы. Цапок Н.А. в период нахождения за границей РФ звонила по абонентскому номеру оператора сотовой связи Израиля около 30 раз. То есть, руководство ОПГ осуществлялось из Израиля (куда она выезжала) посредством использования сотовой связи. Соответственно, у суда не возникло сомнений в том, что количество звонков, произведенных в короткий промежуток времени, свидетельствовало о том, что Цапок Н.А. получала отчеты о состоянии дел, давала указания о деталях действий для достижения результата[2].

В рассматриваемом контексте следует поддержать высказанные мнения ученых о том, что фактические основания проведения рассматриваемого уголовно-процессуального средства как минимум должны свидетельствовать о том, что:

1) проведение следственного действия, предусмотренного ст. 186.1 способствует формированию системы сведений, имеющих значение для расследования преступления;

2) в материалах уголовного дела имеются данные, указывающие на необходимость ограничения соответствующих конституционных прав человека и гражданина в интересах расследования преступления.

Довольно часто следователи (дознаватели) получают у операторов сотовой связи в порядке ч. 4 ст. 21 УПК РФ, работающих в данном регионе, сведения о том, пользуется ли их услугами связи интересующее след-

---

[1] Шагара Г.В. Конституционное право граждан на тайну телефонных переговоров и его ограничение уголовно-процессуальными средствами: дис. ... канд. юрид. наук / Моск. гуманит. ун-т. М., 2014. 188 с.

[2] Приговор по делу 1-116/2011, Кущёвский районный суд Краснодарского края, 2011 г.

ствие лицо. Такой механизм используется в целях установления факта, располагает ли данный оператор сотовой связи информацией о соединениях определенных абонентов и (или) абонентских устройств. Положительная информация позволяет получить сведения о персональных (паспортных) данных зарегистрированного в сети абонента, а также в случае, если известны только такие данные, следователь может получить информацию об абонентском номере, номере SIM-карты, которыми пользовался устанавливаемое лицо.

Между тем, до конца неразрешенным остается и вопрос о возможности получения информации о неустановленном круге абонентов, которые находились в определенном месте и в определенный промежуток времени. Как показало изучение судебной практики, в этом случае судом неоднозначно применяются нормы ст. 186.1 УПК РФ.

Так, по уголовному делу дознаватель обратился в суд с ходатайством, согласованным с первым заместителем прокурора г. Москвы, о разрешении получения у оператора сотовой связи информации о входящих и исходящих соединениях всех абонентских номеров, относящихся к «номерной емкости» оператора, находившихся в непосредственной близости к месту происшествия, с указанием IMEI номеров аппаратов, базовых станций, через которые происходило соединение, вектора направления на них, с предоставлением сведений о лицах, на которых зарегистрированы абонентские номера. Постановлением Тверского районного суда города Москвы от 11 сентября 2012 г. в удовлетворении данного ходатайства было отказано.

В кассационном представлении прокурор выразил несогласие с постановлением суда, считая его незаконным, необоснованным и подлежащим отмене, при этом, ссылаясь на установленные дознанием фактические обстоятельства дела, утверждал, что дознаватель обратилась в суд с ходатайством в полном соответствии с требованиями ст. 29, 165, 23.1, 186.1 УПК РФ, в связи с необходимостью проведения следственного действия, а не оперативно-розыскного мероприятия, при наличии к тому оснований.

Выводы суда, по мнению прокурора, изложенные в постановлении, противоречат ч. 2 ст. 186.1 УК РФ, а получение информации о соединениях между неопределенным кругом абонентов и (или) абонентских устройств, не может повлечь нарушение прав граждан, установленных ст. 23 Конституции РФ и ст. 13 УПК РФ.

Судебная коллегия по уголовным делам Московского городского суда 31 октября 2012 г. нашла постановление суда законным и обоснованным, подлежащим оставлению без изменения. По мнению судей, исходя из содержания нормы, регламентированной ч. 1 ст. 186.1 УПК РФ, получение информации, о которой указывает дознаватель, «может привести к необоснованному ограничению прав неопределенного числа граждан на тайну

телефонных переговоров, что противоречит требованиям ст. 23 Конституции РФ, ст. 13 УПК РФ»[1].

Таким образом, постановление Тверского районного суда города Москвы от 11 сентября 2012 г. судебной коллегией было оставлено без изменения, а кассационное представление прокурора – без удовлетворения.

Между тем, 20 марта 2013 г. тот же судебный орган выносит апелляционное определение по уголовному делу, возбужденному по признакам преступления, предусмотренного ч. 1 ст. 105 УК РФ, которым уже отменяет постановление суда об отказе в удовлетворении ходатайства следователя о производстве следственного действия, предусмотренного ст. 186.1 УПК РФ.

Мотивируя принятое решение, судебная коллегия расценила ссылку суда первой инстанции о незаконности получения абонентской информации неопределенного круга лиц в связи с тем, что возможно несанкционированное получение сведений о телефонных соединениях лиц, в отношении которых применяется особый порядок производства по уголовным делам, несостоятельной, так как «вышеуказанные суждения, высказанные в постановлении, являлись предположениями, на которых согласно закону не может быть основано судебное решение».

В итоге, отменяя в связи с изложенным постановление суда, судебная коллегия пришла к выводу о том, что ходатайство следователя отвечает требованиям ч. 2 ст. 186.1 УПК РФ и подлежит удовлетворению, поскольку из материалов дела следует, что запрашиваемая информация имеет значение для уголовного дела и установления лица, совершившего 12 февраля 2013 г. особо тяжкое преступление, по факту которого было возбуждено данное дело[2].

Представляется, что в приведенных двух судебных решениях, наиболее верной является позиция органов предварительного следствия, которые, во-первых, основываются на нормах ч. 2 ст. 186.1 УПК, где не предусматривается конкретизация данных абонента или абонентских устройств; во-вторых, фактическим основанием производства данного следственного действия является небезосновательное предположение дознавателя (следователя) о том, что подозреваемый на момент совершения преступления может являться абонентом сотовой связи и одновременно пользователем мобильного телефона, который в процессе совершения преступления находился в его одежде, сумке или другой ручной клади.

---

[1] Кассационное определение Московского городского суда [Электронный ресурс]: от 31 октября 2012 г. по делу № 22-14801/12. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Апелляционное определение Московского городского суда [Электронный ресурс]: от 20 марта 2013 г. по делу № 10-907. Доступ из справ.-правовой системы «КонсультантПлюс».

При этом не исключено, что подозреваемый на месте совершения преступления или в непосредственной близости от него мог использовать мобильный телефон: осуществлять звонки, получать или отправлять сообщения, проверять баланс, совершать иные манипуляции, которые были отражены в информационной среде баз данных оператора сотовой связи.

Как справедливо отмечает А. Резцов, «ни Конституционный Суд, ни законодатель… не связывают возможность получения интересующих следствие сведений с установлением конкретного лица, использующего конкретный абонентский номер сотовой связи… Основанием для получения информации о соединениях между абонентами, в первую очередь, должны быть достаточные данные о том, что такая информация имеет значение для уголовного дела»[1]. Тем более что следственная практика пестрит примерами, когда правоохранительным органам удавалось раскрыть преступление «по горячим следам» благодаря именно такому поведению преступников на месте преступления и полученных об этом сведениях у операторов сотовой связи.

В соответствии с ч. 2 ст. 21 УПК РФ обязанность следователя - в каждом случае обнаружения признаков преступления принимать предусмотренные УПК РФ меры по установлению события преступления, изобличению лица или лиц, виновных в совершении преступления. При этом следователь в целях обеспечения полного и всестороннего расследования должен применить весь арсенал законных средств и методов, в том числе, используя технические возможности организаций связи. Поэтому при решении вопроса об удовлетворении или неудовлетворении ходатайства следователя о проведении следственного действия суд должен исходить из позиции приоритетности преступлений, представляющих повышенную общественную опасность, но не их исключительности.

Случаи, когда получение информация о соединениях между абонентами и (или) абонентскими устройствами необходимо, а, следовательно, обоснованно, можно подразделить на несколько групп.

К первой следует отнести случаи, когда в совершении преступного деяния принимало участие несколько лиц. Это могут быть как преступления, совершенные в соучастии, так и отдельные, но взаимосвязанные деяния (например, корыстное преступление и приобретение имущества, заведомо добытого преступным путем; несколько фактов незаконного оборота наркотических средств, совершенных «по цепочке»). Данные о соединениях между абонентами дадут возможность установить контакты обвиняемого и выделить из общей массы лиц, с которыми он контактировал, могущих иметь причастность к преступлению.

---

[1] Резцов А. Применение органами предварительного расследования ст. 186.1 УПК при получении сведений о телефонных переговорах // Законность. 2013. № 7. С. 14.

Вторая группа – это случаи, когда в процессе совершения преступления виновные общались с помощью средств связи с потерпевшими или иными лицами. Детализация соединений позволяет подтвердить сами факты контактов обвиняемых с указанными лицами (что обвиняемые, как правило, отрицают), уточнить время подготовки и непосредственного совершения преступления.

К третьей группе надо отнести случаи, когда для расследования имеет значение факт перемещения абонентского устройства от одного лица к другому или в пространстве (например, когда виновный скрылся с места совершения преступления, либо при хищении абонентских устройств). Информация о соединениях по привязке к базовой станции дает возможность установить места соединений и, следовательно, примерные места нахождения виновных лиц.

На рассматриваемое следственное действие не распространяются положения ч. 5 ст. 165 УПК РФ: оно не проводится в порядке исключения в случаях, не терпящих отлагательства, на основании постановления следователя или дознавателя, с последующим (в течение 3 суток) уведомлением судьи и прокурора. Промедление с проведением анализируемого уголовно-процессуального средства не повлечет за собой утрату доказательств.

Также следователь может определить, в какой именно суд в соответствии с требованиями ч. 2 ст. 165 УПК РФ ему следует обратиться – по месту производства предварительного следствия или по месту производства следственного действия. Определение же места производства предварительного следствия осуществляется по установленным ст. 152 УПК РФ правилам, общим для всех следственных действий.

Как показывает изучение материалов уголовных в отдельных случаях применение ч. 6 ст. 152 УПК РФ сопровождается определенными затруднениями. Так, в соответствии с данной нормой по мотивированному постановлению руководителя вышестоящего следственного органа уголовное дело может быть передано для производства предварительного расследования в вышестоящий следственный орган. Соответственно, возникает вопрос, в какой суд должен обращаться следователь в данном случае. Примечательно, что по данному поводу Конституционный Суд Российской Федерации выразил свою правовую позицию. В определении от 7 февраля 2013 г. № 132-О указывается о том, что в случае проведения расследования по уголовному делу следственным органом, занимающим положение вышестоящего по отношению к следственным органам районного уровня, ходатайства о получении разрешения на производство следственных действий подлежат рассмотрению районным судом по месту нахождения указанного вышестоящего следственного органа независимо от того, передавалось уголовное дело постановлением соответствующего руководителя от

следственного органа районного уровня или изначально было возбуждено вышестоящим следственным органом[1].

По общему правилу, установленному ч. 4 ст. 186.1 УПК РФ, получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами может быть установлено на срок до шести месяцев. Соответствующая осуществляющая услуги связи организация в течение всего срока производства данного следственного действия обязана предоставлять следователю указанную информацию по мере ее поступления, но не реже одного раза в неделю.

Назначение судебной компьютерной экспертизы. Судебная компьютерная экспертиза является самостоятельным родом экспертизы и относится к классу инженерно-технических экспертиз. Одним из важнейших характеристик экспертизы является предмет, представляющий собой сложную теоретическую и практическую конструкцию, связанную с процессом познания экспертом определенных закономерностей, которые в основном характеризуются тремя интегрируемыми элементами – объектом, задачами (целями) и методами исследования. В настоящее время выделяют следующие виды судебных компьютерных экспертиз:

1) судебная аппаратно-компьютерная экспертиза, предметом являются обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств.

2) судебная компьютерно-программная экспертиза предназначена для разрешения вопросов закономерности разработки и применения программного обеспечения, в том числе прикладного характера (программы-приложения для мобильных версий операционных систем Android, IOS, Windows, Simbian и др.).

3) судебная информационно-компьютерная экспертиза, в рамках которой исследуются закономерности, связанные с процессом ввода, поиска, передачи и использования информации с помощью компьютерных средств.

Приведенные виды судебных компьютерных экспертиз образуют классическую классификацию, данную в работе А.И. Усова, обозначение которых осуществлялось в условиях развития информационно-коммуникационных технологий в начале нового века[2].

Между тем, существенное преобразование коммуникационных технологий, повсеместное распространение корпоративных, социальных сетей, увеличение сегмента услуг «облачных» сервисов по хранению пользо-

---

[1] Об отказе в принятии к рассмотрению жалобы гражданина Ерашова Антона Сергеевича на нарушение его конституционных прав отдельными положениями статей 108, 109 и 152 УПК Российской Федерации: определение Конституционного Суда Рос. Федерации от 7 февраля 2013 г. № 132-О.

[2] Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: дис. ... д-ра юрид. наук. М., 2002. 402 с. С. 86.

вательских данных, привело к тому, что на исследование экспертам стали поступать специфичные объекты, требующие комплексного изучения.

Так, например, 21 февраля 2011 г. приговором Промышленного районного суда г. Оренбурга гр. Н. был признан виновным в совершении восьми эпизодов незаконного доступа и копирования охраняемой законом компьютерной информации в системе ЭВМ и их сети, использование вредоносных программ для ЭВМ, с целью уклонения от оплаты услуг по доступу к сети Интернет.

Следствием установлено, что Н., находясь в своём жилище с помощью своего ноутбука «ASUS K50AB», имеющего доступ к сети Интернет под собственным логином и паролем, предоставленным провайдером Оренбургского филиала ОАО «Уфанет», используя вредоносную программу «Radmin Viewer», осуществил сканирование IP-адреса, а также доступ к восьми удаленным компьютерам. После этого Н., используя вредоносную программу, скопировал сетевые реквизиты, в частности, логины и пароли, принадлежащие абонентам Оренбургского филиала ОАО «Уфанет», осуществлял неправомерный доступ в сеть Интернет[1].

В ситуациях подобного рода возникает необходимость получения экспертного заключения по результатам проведения судебной компьютерной экспертизы, которая основывается на исследовании компьютерных средств, использующих какую-либо информационную технологию.

При проведении судебной компьютерной экспертизы перед экспертом стоят следующие задачи:

1) определение характеристик программного обеспечения, посредством которого обеспечивается доступ устройства к сетевым ресурсам;

2) определение роли и предназначения исследуемого объекта в сети. Чаще всего определяется в соотношении конкретного устройства к другому, например, функциональное соотношение аппаратного средства к серверу, активному сетевому оборудованию и т.д.);

3) определение условий модификации свойств и характеристик вычислительной техники;

4) установление свойств и характеристик, архитектуры, конфигурации сети, соответствие этих характеристик для обозначения класса средств сетевой технологии, принадлежность к серверной или клиентской части приложений;

5) наличие определенных физических дефектов, исправность сетевого средства, состояние системного журнала, компонент управлением доступа;

6) определение исходного состояния вычислительной сети в целом и каждого сетевого средства в отдельности;

---

[1] Приговор Промышленного районного суда г. Оренбурга по делу 1-55/2011 от 21 февраля 2011 г.

7) установление обстоятельств события инцидента в сети по его результатам и т.д.

Особую значимость судебная компьютерная экспертиза приобретает при расследовании преступлений в сфере экономической деятельности, когда объектом исследования является целый комплекс компьютерных устройств, включающих персональные компьютеры работников, серверы организации, а также иные накопители электронной информации, образующих внутрикорпоративную виртуальную сеть. При этом исследование может осложниться наличием криптографической защиты информации, передаваемой по каналам связи такой сети[1].

Практике известны случаи, когда изъятие в ходе проведения первоначальных следственных действий (осмотра места происшествия, обыска, выемки) всего компьютерного оборудования посредством которого осуществлялись преступные действия, не приносит должного результата при проведении исследования в лабораторных условиях, так как пользователи компьютерных систем корпоративного толка могут использовать специализированные облачные шлюзы для хранения информации. Отключение компьютерного устройства от сети при изъятии может повлечь утрату аутентификационной информации, восстановление которой потребует больших временных и ресурсных затрат. Поэтому, при производстве такого рода следственных действий следует задействовать специалистов того экспертного учреждения, которому в последствии будут переданы объекты для исследования при назначении компьютерной (компьютерно-технической) экспертизы, либо предоставить возможность проведения экспертизы в месте, где установлено сетевое оборудование. К тому же участие специалиста при, например, осмотре места происшествия может способствовать получению необходимых данных для проведения дальнейшего исследования.

Вопросы, выносимые перед экспертом в постановлении о назначении компьютерной экспертизы, могут быть сформулированы следующим образом:

1. Имеются ли на предоставленном оптическом носителе марки «...» белого цвета с надписью черного цвета «...», с серийным номером вокруг посадочного кольца ..., программы (фрагменты программ), заведомо предназначенные для несанкционированного (в отсутствии волеизъявления пользователя) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации? Если да, то, какие именно, каково их функциональное назначение и сетевые возможности?

---

[1] Пропастин С.В. Оценка следователем результатов компьютерной экспертизы // Уголовный процесс. 2013. № 4. С. 32–37.

Примечание. Далее следует заменять «заведомо предназначенные» на «способные», «несанкционированного» на «скрытного от пользователя» (столь неопределенный вопрос не стоит применять к НЖМД, чем больше конкретных данных указывается (расположение, функциональные возможности, даты), тем лучше. Если эксперт не сможет установить в указанные даты инцидента искомое событие, то он сможет расширить границы поиска. В случае, если необходимо установить шифровальщика, а на ПЭВМ пользователя много иного ВПО, то эксперту придется его исследовать и описывать, что займет очень много времени, что приведет к напрасным затратам сил и средств.

2. Имеется ли на представленном на исследование носителе информации программное обеспечение, позволяющее без ведома пользователя осуществлять копирование или модификацию компьютерной информации, в частности, программы, способные выполнять без ведома пользователя сбор учетных данных, предоставлять удаленный доступ или самостоятельно, без вмешательства пользователя, взаимодействовать с системами дистанционного банковского обслуживания? Если указанные программы имеются, то каковы их функциональные возможности, расположение и даты появления на данном носителе? Если указанные программы имеются, то присутствуют ли на данном носителе следы их работы?

Примечание. Особую актуальность данный вопрос приобретает при поиске банковских троянов.

3. Содержат ли представленные на исследование компакт-диски «...1», «...2» компьютерную программу или иную компьютерную информацию, предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, если да, то для каких именно вышеуказанных функций данная программа предназначена? Присутствуют ли на представленном на исследование компакт-диске «...3» программы или их модификации, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, которые содержатся на компакт-дисках «...1», «...2».

4. Имеется ли на НЖМД представленных для проведения экспертизы ноутбуке марки «...», имеющем серийный номер: ... и системном блоке серебристого цвета с надписью «...» программное обеспечение Trojan-Banker.Win32.Metel, а также программное обеспечение способное его создавать? Если имеется, является ли оно вредоносным? Какова его классификация и предназначение?

Примечание. Постановка вопроса необходима для поиска на компьютерном устройстве подозреваемого программного обеспечения, если известно с помощью чего осуществлялась атака на компьютерное устройство жертвы.

5. Содержатся ли на НЖМД представленных для проведения экспертизы ноутбуке марки «...», имеющем серийный номер: ... и системном блоке серебристого цвета с надписью «...» сведения об обращении к доменам ... и ...?

6. Содержатся ли на НЖМД представленных для проведения экспертизы ноутбуке марки «...», имеющем серийный номер: ... и системном блоке серебристого цвета с надписью «...» сведения об использовании их пользователем сервисов мгновенного обмена сообщениями? Если содержатся, то имеются ли данные об аккаунтах пользователя?

7. Имеются ли на НЖМД, представленных для проведения экспертизы ноутбуке марки «...», имеющем серийный номер: ... и системном блоке серебристого цвета с надписью «...» сведения о контактах пользователя, а также история переписки пользователя? Если имеется, то какова вся имеющуюся история переписки?

8. Имеется ли на НЖМД представленных для проведения экспертизы ноутбуке марки «...», имеющем серийный номер: ... и системном блоке серебристого цвета с надписью «...» программное обеспечение, предназначенное для удаленного управления? Если имеется, то какое именно?

9. Присутствуют ли среди программ, содержащихся на представленном на экспертизу оптическом диске DVD, программы, позволяющие без ведома пользователя отправлять SMS-сообщения или USSD-запросы, а также скрывать от пользователя входящие SMS-сообщения? Если да, то каковы их функциональные возможности? При наличии технической информации установить, на какие номера данные программы отправляют запросы, в т.ч. платные номера, содержат ли данные программы информацию об инициаторе или авторе данных программ, какую-либо контактную информацию и т.п.? Способны ли данные программы предоставлять удаленный доступ к устройству, на котором они запущены, через сеть Интернет без ведома пользователя? Если имеются, просим Вас указать всю информацию о данном программном обеспечение: дату и время установки на устройство, информацию о предполагаемых Интернет-ресурсах (с указанием их полных данных размещения в сети «Интернет») с которых данные приложения были скопированы на устройство, указать его функциональные возможности.

10. Имеются ли на представленных на исследование электронных носителях информации программы для операционной системы Android, способные скрытно от пользователя отправлять SMS-сообщения на абонентские номера, содержащиеся в адресной книге, по команде управляющего сервера.

11. Имеются ли на представленных на исследование электронных носителях информации сведения об использовании программ, предоставляющих доступ к заданным пользователем серверам по протоколам FTP и

SSH? Если да, то к каким серверам осуществлялся доступ, а также с использованием каких учетных данных (логин и пароль)?

12. Имеются ли на представленных электронных носителях информации сведения о посещении следующих сайтов: «...», «...», «...»?

13. Имеются ли на представленном на экспертизу оптическом компакт-диске ... исходные коды компьютерных программ. Если да, то в какой операционной системе данные программы способны выполняться? (частный случай, если известно что коды представлены в виде готового проекта, иначе их очень сложно представить как программу)

14. Предназначены ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации?

15. Выводятся ли пользователю операционной системы сообщения при установке программ, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., если да, то какие?

16. Какие действия при установке производят программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., если да, то какие?

17. Производят ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., действия, которые скрыты от пользователя операционной системы, если да, то какие именно?

18. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., устанавливать скрытые от пользователя или несанкционированные сетевые соединения, если да, то какие именно?

19. Имеют ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., функции удаленного администрирования (управления), если да, то какие действия происходят при получении команд?

20. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять скрытую от пользователя операционной системы отправку коротких текстовых сообщений (смс), если да, то какие именно?

21. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять скрытое от пользователя операционной системы чтение входящих коротких текстовых сообщений (смс), если да, то каких именно?

22. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять скрытое от пользователя операционной системы блокирование входящих и

исходящих коротких текстовых сообщений (смс), если да, то каких именно?

23. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять скрытое от пользователя операционной системы удаление входящих и исходящих коротких текстовых сообщений (смс), если да, то каких именно?

24. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять сбор какой-либо технической информации об устройстве, на котором они устанавливаются, если да та какой именно информации, и производится ли скрытое копирование данной информации на иные носители, в том числе посредством информационно-телекомуникационной сети «Интернет»?

25. Предпринимают ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., какие-либо действия направленные на недопущение удаления их из операционной системы стандартными методами доступными пользователю?

26. Продолжают ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., функционировать в скрытом режиме после попытки их удаления из операционной системы?

27. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., осуществлять автозапуск при старте операционной системы без инициации данного процесса пользователем?

28. Являются ли представленные на экспертизу на оптическом компакт-диске ... файлы «...» (размер ... байт), «...» (размер ... байт), «...» компьютерными программами. Если да, то в какой операционной системе данные программы способны выполняться?

29. Имеют ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., и программы, содержащиеся в файлах «...» (размер ... байт), «...» (размер ... байт), «...» сходные функциональные возможности и алгоритмы исполнения программ?

30. Устанавливались ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске ..., на мобильный телефон ... с серийным номером ..., имеющий IMEI .... Если да, то какая программа (файл), и когда именно?

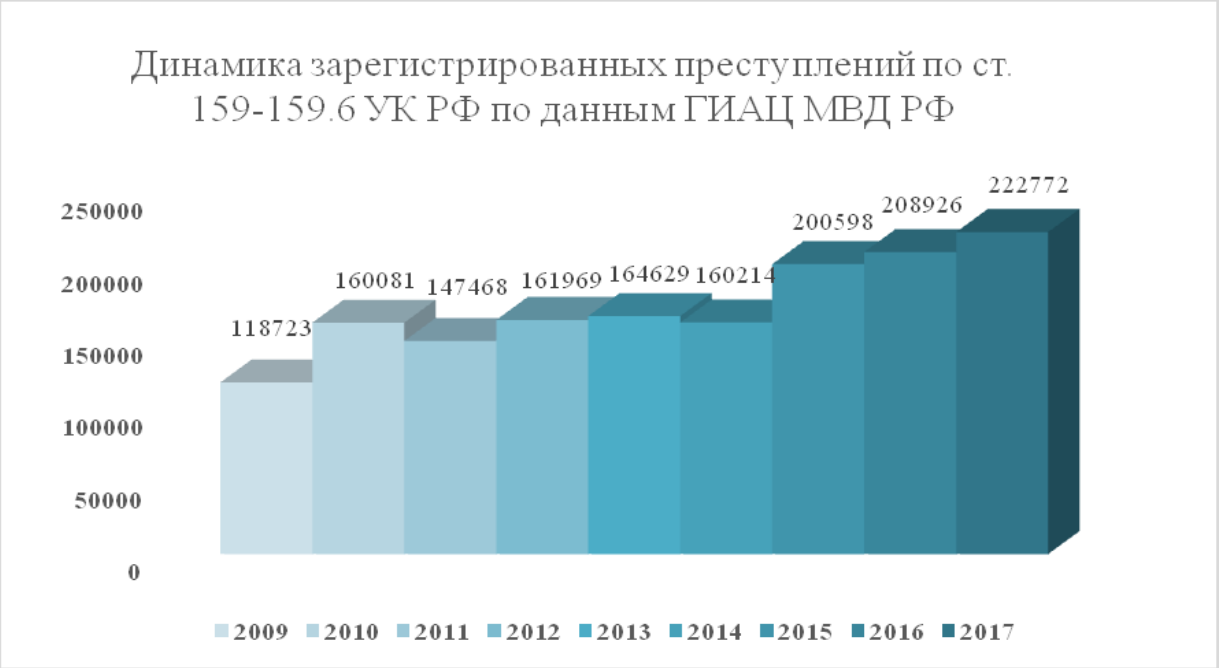
ЗАКЛЮЧЕНИЕ

Мошенничество, совершаемое с использованием компьютерной информации, следует понимать совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужих денежных средств, числящихся на банковских и иных счетах, в пользу виновного или других лиц путем применения средств хранения, обработки и (или) передачи компьютерной информации, причинившее ущерб их собственнику или иному владельцу.

Средства телекоммуникаций, вместе с новыми информационными технологиями, становятся инструментом при разработке новых банковских продуктов и механизмов их распространения, что расширяет сферу деятельности коммерческих банков и иных финансовых организаций. Электронные платежи и средства расчета в точке продажи – примеры использования новых технологий, коренным образом меняющих финансовую индустрию.

Между тем, средства телекоммуникаций и новые информационные технологии (компьютерные технологии) создают условия для подготовки, совершения и сокрытия хищений денежных средств с их использованием, к которым относятся: «виртуальный» характер дистанционных банковских операций; доступность «открытых» телекоммуникационных систем; высокая скорость выполнения транзакций; глобальный характер межсетевого операционного взаимодействия; изменения в информационном контуре банковской деятельности и появление в нём новых участников (провайдеры, сотовые операторы, аутсорсинговые и иные организации); зависимость реализации банковских операций (банковской деятельности) от надежности не только различного рода провайдеров, сотовых операторов, аутсорсинговых и других организаций, но и от аппаратно-программного обеспечения банковских операций; уязвимость программного кода банковских информационных систем.

ПРИЛОЖЕНИЯ


Динамика зарегистрированных преступлений по ст. 159-159.6 УК РФ по данным ГИАЦ МВД РФ
250000
200000
150000
100000
50000
0
118723
160081
147468
161969
164629
160214
200598
208926
222772
2009
2010
2011
2012
2013
2014
2015
2016
2017

Пример осмотра мобильного телефона классической формы с функциональной возможностью использования нескольких SIM-карт (без участия понятых)

ПРОТОКОЛ[1]
осмотра предметов (документов)

г. Энск «*3*» *мая 2014 г.*

Осмотр начат в *12* ч *00* мин
Осмотр окончен в *13* ч *32* мин

Следователь СО ОП №3 УМВД России по г. Энску лейтенант юстиции Солодов Дмитрий Андреевич с участием *специалиста криминалиста эксперта ЭКЦ УМВД России по Энской области лейтенанта полиции Барановой Алены Сергеевны* в соответствии со ст. 164, частью первой ст.176, частями первой-четвертой и шестой ст. 177 УПК РФ произвел осмотр *в кабинете 39 СО ОП № 3 УМВД России по г. Энску, расположенного по адресу: г. Орел, ул. Ленина 17, мобильного телефона «EXPLAY B240» IMEI 1 35988504811668, IMEI 2359885046811676, IMEI 3 359885046811684, о чем в соответствии со ст. 166 УПК РФ составил настоящий протокол.*

Перед началом осмотра участвующим лицам разъяснены их права, обязанности и ответственность, а также порядок производства осмотра предметов (документов).

Специалисту *Барановой Алене Сергеевне* разъяснены права, обязанность и ответственность, предусмотренные ст. 58 (57) УПК РФ.

Баранова

Лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств *цифрового фотоаппарата Canon G 225, с флеш-картой объемом памяти 8 Gb, чемодан «Криминалист».*

Осмотр производился в условиях *смешанного освещения.*

Осмотром установлено: *в присутствии специалиста-криминалиста эксперта ЭКЦ УМВД РФ по Энской области лейтенанта полиции Барановой А.С. был вскрыт прямоугольный бумажный пакет, опечатанный двумя квадратными отрезками бумаги с оттисками печати «Для пакетов». На конверте имеется рукописная надпись: «Мобильный телефон «EXPLAY B240» IMEI 1 35988504811668, IMEI 2 359885046811676, IMEI 3 359885046811684, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск ул. Ленина, 17, офис № 45 по факту тайного хищения имущества», ниже стоят подписи понятых и следователя. Конверт повреждений и разрывов не имеет; целостность оттисков печатей не нарушена.*

При вскрытии конверта в нем обнаружен мобильный телефон «EXPLAY B240» прямоугольной формы в корпусе черного цвета с серебристой окантовкой по кругу длиной 120, мм, шириной 50,1 мм, толщиной 12 мм. Мобильный телефон выполнен из полимерного материала черного цвета с серебристыми вставками по кругу на боковой панели. На момент осмотра мобильный телефон находится в выключенном состоянии.

Корпус телефона имеет мелкие потертости, более существенных повреждений на корпусе нет. На корпусе расположены:

1) на лицевой стороне – экран размером 40х51 мм, 19 клавиш с тематическими символами. Над экраном расположены отверстия для динамиков, надпись, выполненная красителем серебристого цвета латинскими символами «B240» и под экраном

[1] Каждая страница протокола подписывается участвующими лицами.

надпись, выполненная красителем серебристого цвета «EXPLAY». Центральная кнопка под экраном имеет потертость в виде белой точки. Ниже стандартная клавиатура мобильного телефона 3 клавиши вызова и клавиша сброса;

2) на верхней боковой стороне корпуса имеется разъем круглой формы для подключения дополнительного оборудования, а также фонарик.

3) на левой боковой стороне корпуса имеется разъем прямоугольной формы для подключения дополнительного оборудования.

4) на правой боковой стороне корпуса ничего не имеется.

5) оборотная сторона осматриваемого мобильного телефона состоит из крышки, выполненной из полимерного материала черного цвета, закрывающей отсек, предназначенный для аккумуляторной батареи на которой имеется текст, выполненный красителем черного цвета латинскими символами «EXPLAY». В нижней части крышки мобильного телефона имеется отверстие прямоугольной формы для динамика, в верхней части крышки - объектив фотокамеры.

При удалении крышки аккумуляторного отсека была обнаружена аккумуляторная батарея длиной 61 мм, шириной 35 мм, толщиной 5 мм, выполненная из полимера черного цвета. На лицевой части аккумуляторной батареи имеется текст, выполненный красителем черного цвета «EXPLAY», «B240», «3,7 В DC1 1000 мАч 3,7 Ватт в час. Используйте только оригинальные батареи. Перед применением ознакомьтесь с инструкцией».

При извлечении аккумуляторной батареи, в корпусе телефона обнаружена конструктивная составляющая фотокамеры круглой формы. Ниже фотокамеры расположена наклейка белого цвета на которой имеется текст: «EXPLAY модель: B240 IMEI 1 359885048116 68, IMEI 2359885046811676, IMEI 3 359885046811684», ниже расположены три пустых слота для SIM-карт.

Ниже имеется слот, в котором обнаружена флеш-карта в полимерном корпусе черного цвета «Transcend 8Gb micro SD HC», объемом памяти 8 Gb, на оборотной стороне которой имеются цифровые и буквенные обозначения, выполненные красителем белого цвета 2C4191DL LWFS140321-Q 1418 1206669445.

При нажатии клавиши мобильного телефона «включить», он не включается.

После произведенного осмотра: *мобильный телефон был собран в первоначальный вид, сфотографирован специалистом-криминалистом экспертом ЭКЦ УМВД России по Орловской области лейтенантом полиции Барановой А.С. по правилам детальной масштабной фотосъемки цифровым фотоаппаратом марки «Canon G225» с флеш-картой объемом памяти 8Gb и помещен вместе с первоначальной упаковкой в бумажный конверт, с надписью: «Мобильный телефон «EXPLAY B240» IMEI 1 359885048116 68, IMEI 2 359885046811676, IMEI 3 359885046811684, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск ул. Ленина, 17, офис № 45 по факту кражи имущества и осмотренный 3 мая 2014 года». Конверт заклеен и опечатан тремя квадратными отрезками бумаги с оттисками печати «Для пакетов». На конверте и оттисках стоят подписи специалиста и следователя.*

К протоколу осмотра прилагается *иллюстрационная таблица*.

По ходу следственного действия заявлений, замечаний на действия участников осмотра и правильность составления протокола не поступили.

Протокол предъявлен для ознакомления всем лицам, участвовавшим в следственном действии. При этом указанным лицам разъяснено их право делать, подлежащие внесению в протокол оговоренные и удостоверенные подписями этих лиц, замечания о его дополнении и уточнении. Ознакомившись с протоколом путем *личного прочтения*

по окончании осмотра от участвующих лиц заявлений, замечаний на действия участников осмотра и правильность составления протокола не поступили.

Специалист *Баранова*
Следователь *Солодов*

Иллюстрационная таблица
(приложение) к протоколу осмотра мобильного телефона «EXPLAY B240» IMEI 1 35988504811668, IMEI 2359885046811676, IMEI 3 359885046811684 от 3 мая 2014 года по уголовному делу № 33989

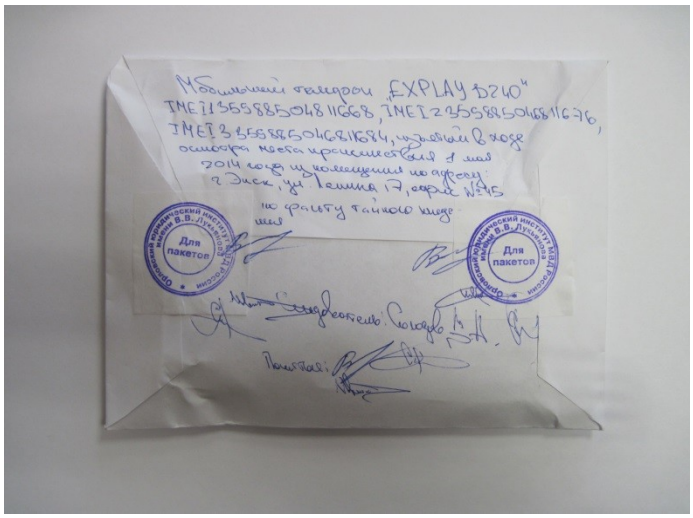


Иллюстрация 1. Конверт, при вскрытии которого был обнаружен мобильный телефон «EXPLAY B240» IMEI 1 35988504811668, IMEI 2 359885046811676, IMEI 3 35988504681168

Иллюстрация № 2. Передняя панель мобильного телефона «EXPLAY B240»

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 2

Продолжение иллюстрационной таблицы

Иллюстрация № 3. Задняя панель мобильного телефона «EXPLAY B240»

Иллюстрация № 4. Задняя панель без аккумуляторной крышки мобильного телефона «EXPLAY B240»

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 3

Продолжение иллюстрационной таблицы

Иллюстрация № 5. Общий вид оборотной стороны мобильного телефона «EXPLAY B240» без аккумуляторной батареи

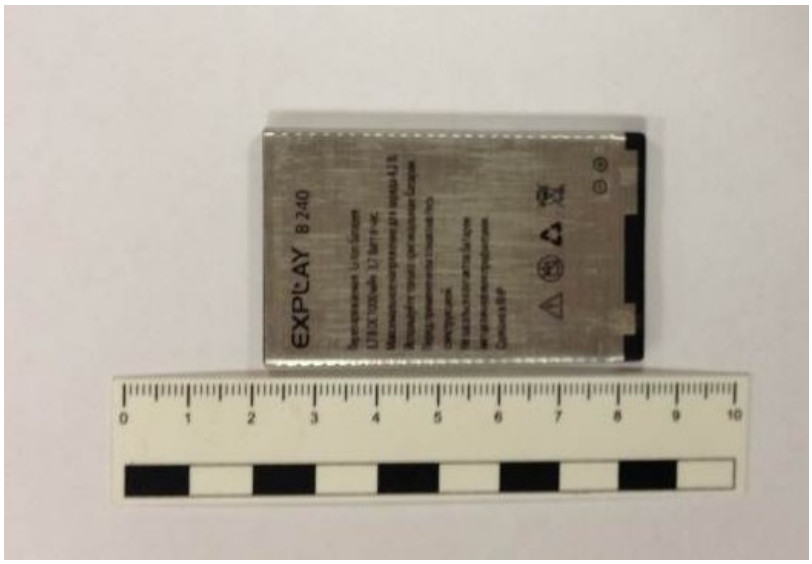


Иллюстрация № 6. Лицевая сторона аккумуляторной батареи мобильного телефона «EXPLAY B240»

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 4

Продолжение иллюстрационной таблицы

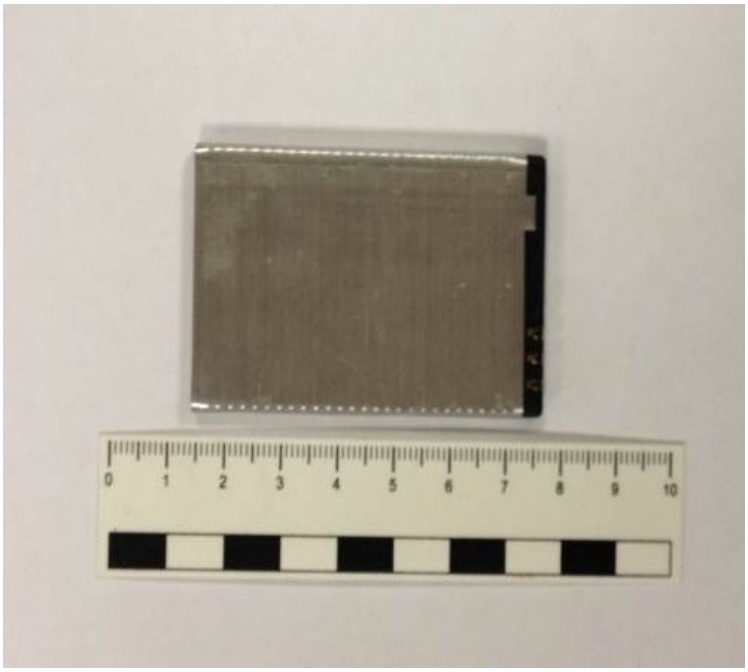


Иллюстрация № 6: Оборотная сторона аккумуляторной батареи мобильного телефона «EXPLAY B240»

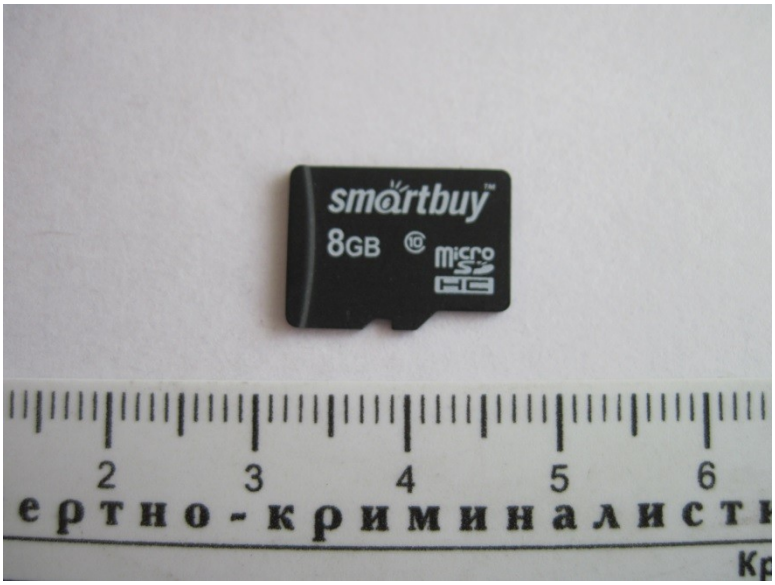


Иллюстрация № 7. Лицевая сторона флеш-карты micro-CD объемом 8 ГБ мобильного телефона «EXPLAY B240»

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 5

Продолжение иллюстрационной таблицы

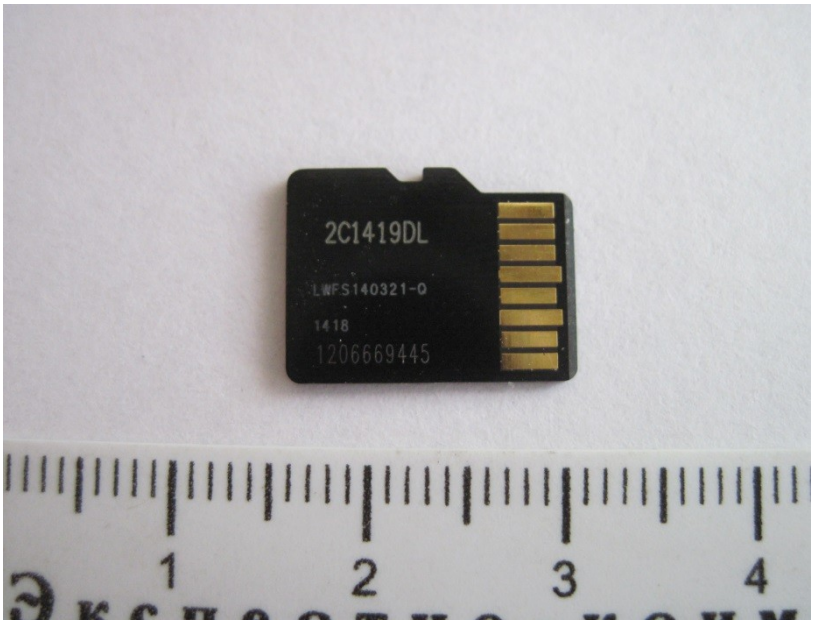


Иллюстрация № 8. Оборотная сторона флеш-карты micro-CD объемом 8 ГБ мобильного телефона «EXPLAY B240».

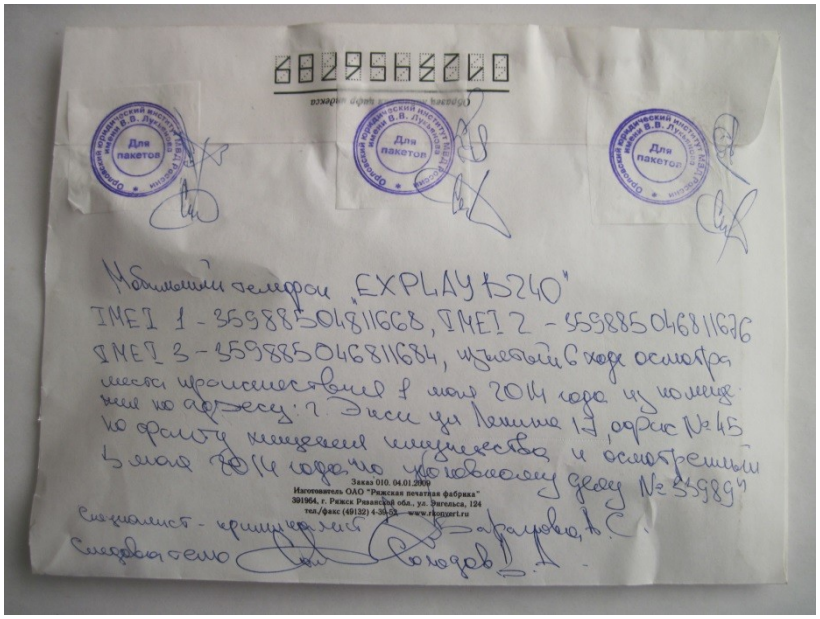


Иллюстрация № 9. Конверт, в который был помещен осмотренный мобильный телефон «EXPLAY B240» и его первоначальная упаковка.

Фотосъемку произвел и иллюстрационную таблицу составил:
специалист-криминалист эксперт ЭКЦ УМВД России
по Орловской области лейтенант полиции Место для печати Баранова А.С.

Фрагмент протокола осмотра сенсорного смартфона
(с описанием информационного содержимого)

...мобильный телефон Nokia Lumia 800 на момент осмотра упакован в бумажный конверт, который снабжен пояснительной надписью: "Приложение №3 Конверт с мобильным телефоном Nokia Lumia 800 IMEI 352826055559835, изъятого у гр. Горбушина Г.Н. по уголовному делу №111056", снабжен подписями понятых и следователя, скреплен отрезками бумаги с оттисками печати № 27 СО ОП №3 УМВД России по г. Орлу упаковка повреждений не имеет.

При вскрытии конверта в нем обнаружен мобильный телефон Nokia Lumia 800 в полимерном корпусе черного цвета. Телефон имеет следы эксплуатации (имеются царапины на корпусе и экране телефона), телефон находиться в рабочем состоянии.

Мобильный телефон Nokia Lumia 800 имеет размеры ШхВхТ 16.2x116.5x12.1 мм, тип корпуса цельный-моноблок, без открывающейся задней крышки. На верхней боковой панели телефона имеется разъем для наушников 3.5 мм и USB. На оборотной стороне корпуса телефона расположены объектив камеры и вспышка. На правой боковой панели корпуса телефона расположены кнопки регулировки громкости, блокировки\включения\выключения, кнопка фотокамеры. Тип экрана – сенсорный, емкостный, кнопки отсутствуют. У телефона отсутствует разъем для карты памяти.

*Телефон находится во включенном состоянии. При наборе комбинации *#06# появляется на экране мобильного телефона IMEI 352826055559835.*

При осмотре журнала вызовов было обнаружено: исходящий вызов, пт. 21:04 Мамуля +79192530533, входящий вызов пт. 22:31 Тема Бобров +79190003738. При осмотре сообщений на телефоне обнаружено, Мамуля пт. 17:55 "Хорошо, через 5 минут выходи, ну ты ходил?", Тема Бобров пт. 21:00 "Андрей, как твои дела?". При осмотре фотогалереии папки "Фото" телефона, обнаружен графический рисунок WP-201304404-01, на котором изображен веник молоток и савок.

При осмотре папки "Музыка+Видео" обнаружены аудиозаписи: А. Барыкин - Букет.mp3, Агата Кристи - как на войне. mp3, Агата Кристи_Би2_Люмен мы не ангелы.mp3, Алексей Королевич - Oh.mp3, Аллегрова - младший лейтенант. mp3.

При осмотре телефонной книжки папки "Контакты", были обнаруженные сохранённые номера сотовых операторов, которые записаны под именами с фамилиями: 1) Александр Сергеевич +792561234, 2) Алексей Пахомов +7896352145, 3) Алексей Туленков +7896541123, 4) Алексей Уваров +7896325641, 5) Алексей Чернокозов +7895214631, 6) Алена Шубина +78965412222.

На боковой верхней панели телефона имеется гнездо с расположенным в нем полимерным лотком черного цвета. При изъятии данного лотка из телефона, в нем обнаружена стандартная micro-SIM-карта в полимерном корпусе с маркировкой «МТС», выполненной красителем белого и красного цвета. На контактной площадке микрочипа micro-SIM-карты желтого цвета имеются три продольных параллельных друг другу потертости темно-коричневого цвета.

Все конструктивные части телефона сфотографированы по правилам детальной масштабной фотосъемки цифровым фотоаппаратом марки «Canon G225» с флеш-картой объемом памяти 8Gb. Телефон в собранном виде помещен в конверт, из которого он был извлечен в ходе осмотра, и вместе с конвертом помещен в другой бумажный конверт, снабженный пояснительной надписью: "Приложение №2 Конверт с мобильным телефоном Nokia Lumia 800 IMEI 35282 6055559835, изъятого у гр. Горбушина по уголовному делу №111056". Ниже надписи поставлены подписи понятых и следователя. Конверт скреплен отрезками бумаги с оттисками печати № 27 СО ОП №3 УМВД России по г. Орлу…

Приложение 1

Иллюстрационная таблица
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

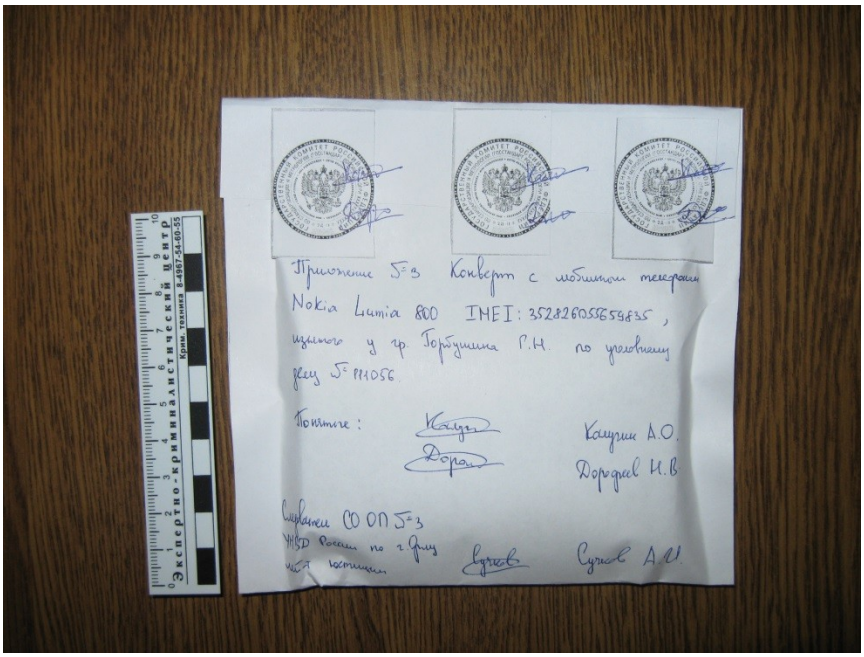


Иллюстрация № 1. Лицевая сторона упаковки телефона, изъятого по уголовному делу № 111056

Иллюстрация № 2. Оборотная сторона упаковки телефона, изъятого по уголовному делу № 111056

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 2)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

Иллюстрация № 3. Лицевая сторона корпуса м/т «Nokia Lumia 800»

Иллюстрация № 4. Оборотная сторона корпуса м/т «Nokia Lumia 800»

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 3)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

Иллюстрация № 5. Главное меню м/т «Nokia Lumia 800

Иллюстрация № 6. Продолжение главного меню м/т «Nokia Lumia 800

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 4)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

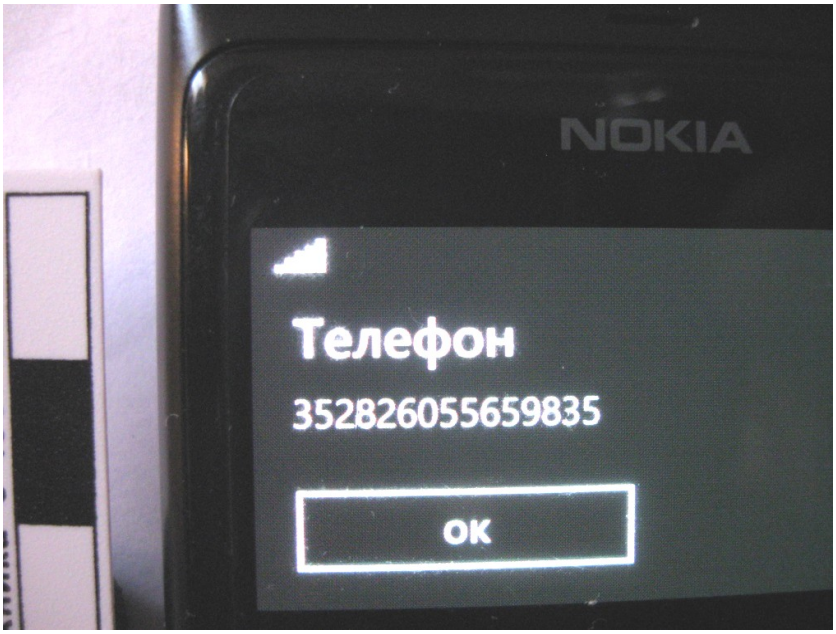


Иллюстрация № 7. Лицевая сторона м/т «Nokia Lumia 800 с IMEI кодом, при наборе комбинации *#06#

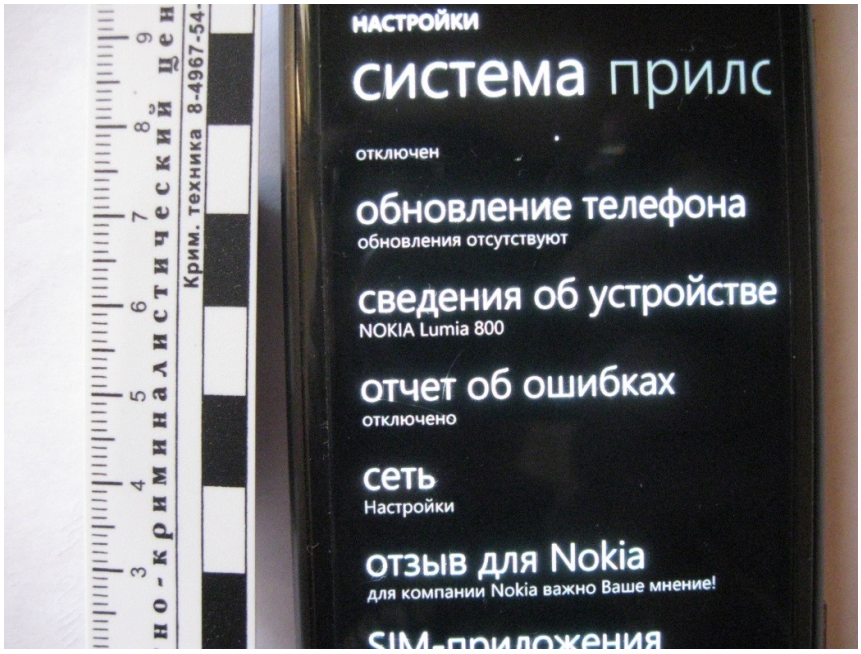


Иллюстрация № 8. Информация о телефоне на экране м/т «Nokia Lumia 800» открытого по пути:1) Главное меню - 2) Настройки - 3) Система

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 5)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI
352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

Иллюстрация № 9. Информация о телефоне на экране м/т «Nokia Lumia 800»
открытого по пути: 1) Главное меню - 2) Настройки -
3) Система - 4) Сведения об устройстве

Иллюстрация № 10. Контактный список абонентов на экране м/т «Nokia Lumia 800»
открытого по пути: 1) Главное меню - 2) Контакты

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 6)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

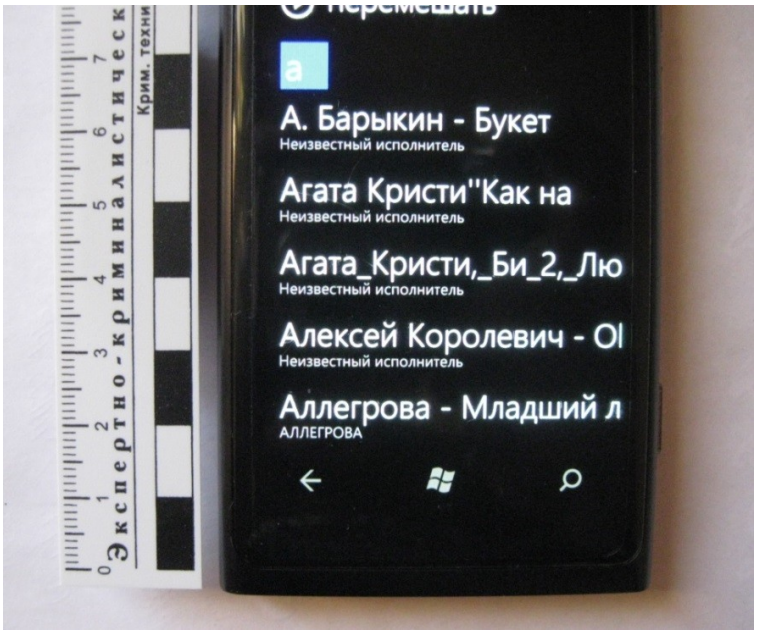


Иллюстрация № 11. Звуковые файлы на экране м/т «Nokia Lumia 800», открытого по пути:
1) Главное меню - 2) Музыка+ Видео - 3) Журнал

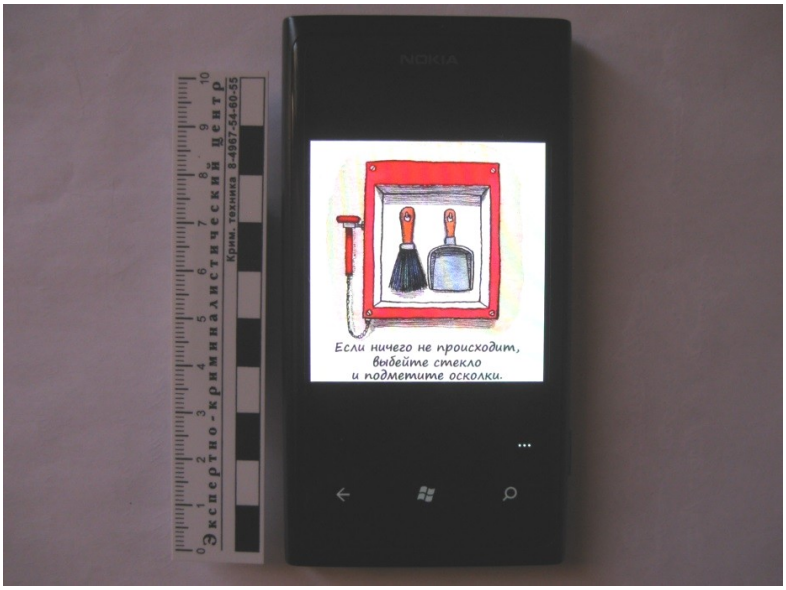


Иллюстрация № 12. Графическое изображение на экране м/т «Nokia Lumia 800», открытого по пути: 1) Главное меню - 2) Фото - 3) Сохраненные изображения

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 7)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

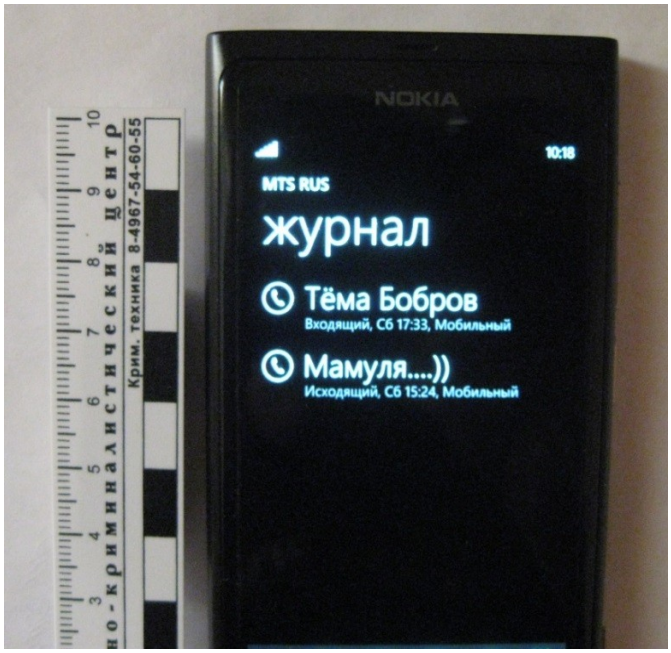


Иллюстрация № 13. Журнала вызовов на экране м\т «Nokia Lumia 800», открытого по пути: 1) Главное меню - 2) Журнал

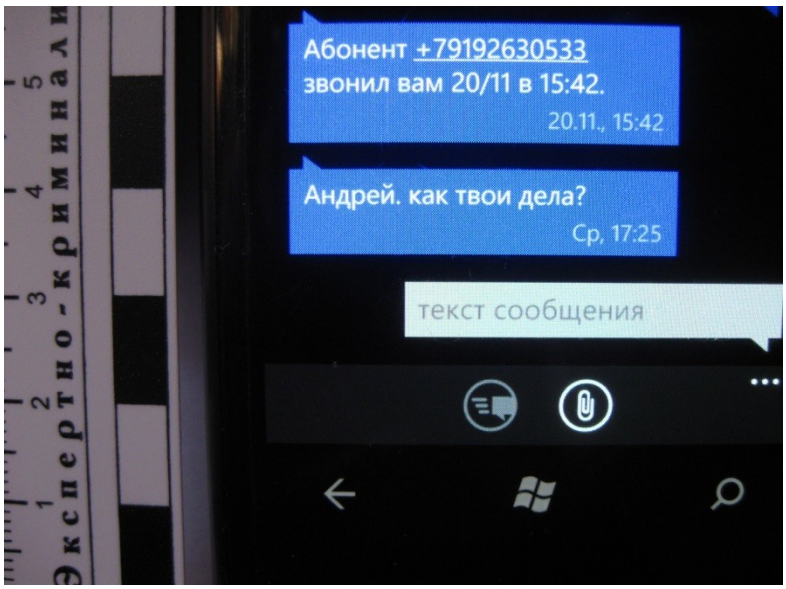


Иллюстрация №14. Текстовое сообщение от абонента +7891926356533 на экране м\т «Nokia Lumia 800», открытого по пути: 1) Главное меню - 2) Сообщения - 3) +789192636533

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 8)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

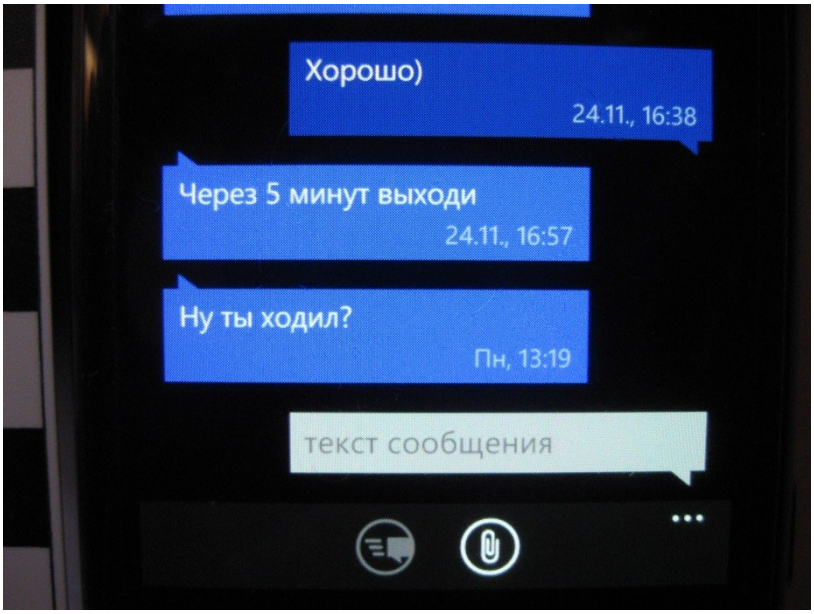


Иллюстрация №15. Текстовое сообщение от абонента +78912003637 на экране м/т «Nokia Lumia 800», открытого по пути: 1) Главное меню - 2) Сообщения - 3) +78912003637

Иллюстрация № 16. Верхняя панель корпуса м/т «Nokia Lumia 800» с гнездом, в котором размещался слот-крепление с micro-SIM картой

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 9)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

Иллюстрация № 17. Лицевая сторона слот-крепление с micro-SIM картой

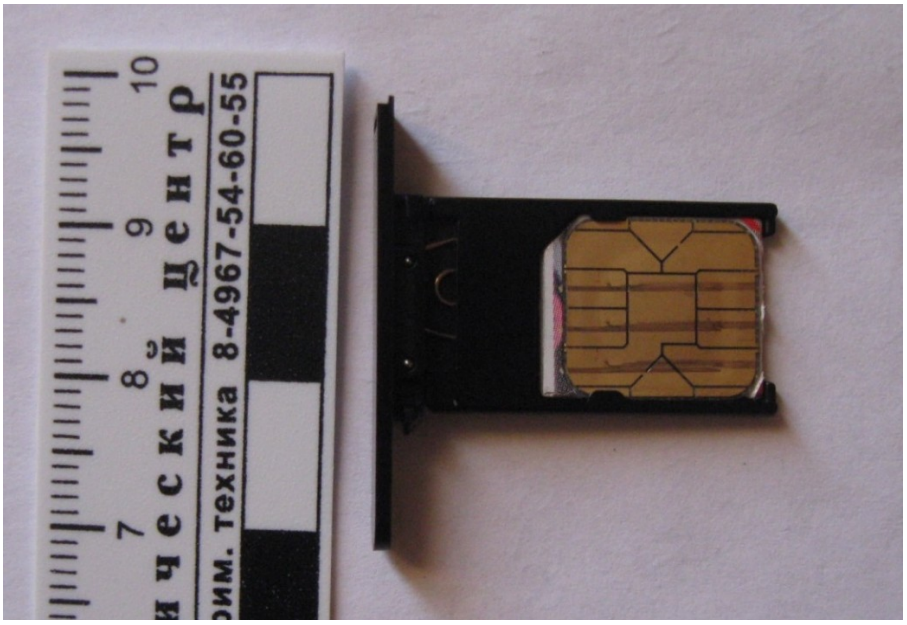


Иллюстрация № 18. Оборотная сторона слот-крепление с micro-SIM картой

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 10)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

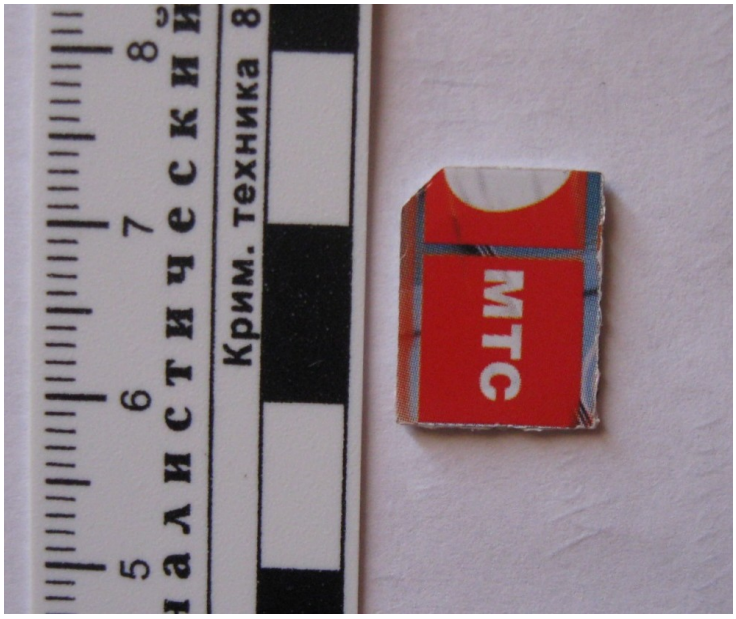


Иллюстрация № 19. Лицевая сторона micro-sim карты

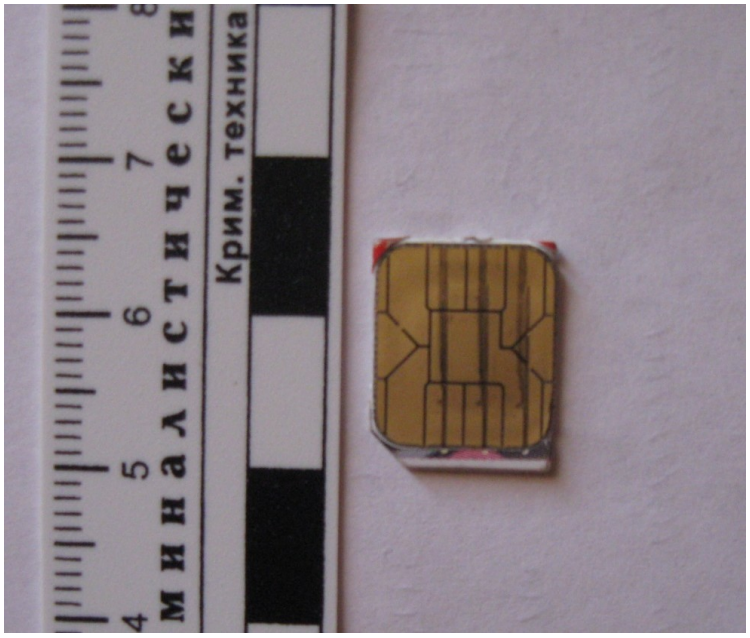


Иллюстрация № 20. Оборотная сторона micro-SIM карты

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 11)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

Иллюстрация № 21. Лицевая сторона слот-крепления для micro-sim карты

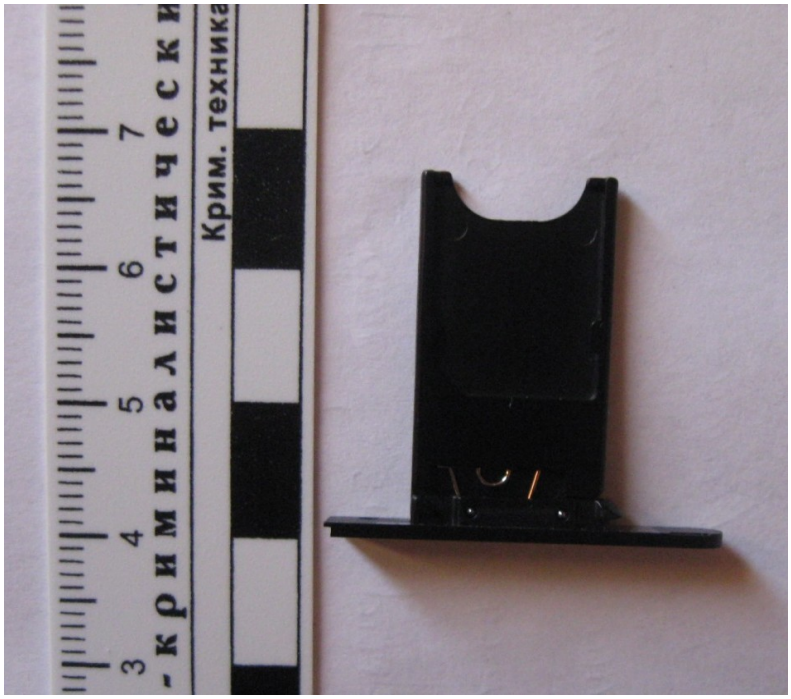


Иллюстрация №22. Оборотная сторона слот-крепления для micro-SIM карты

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

Продолжение иллюстрационной таблицы (лист 12)
к протоколу осмотра м/т «Nokia Lumia 800» с серийным номером IMEI 352826055659835 от 15 декабря 2013 года, изъятого по уголовному делу № 111056

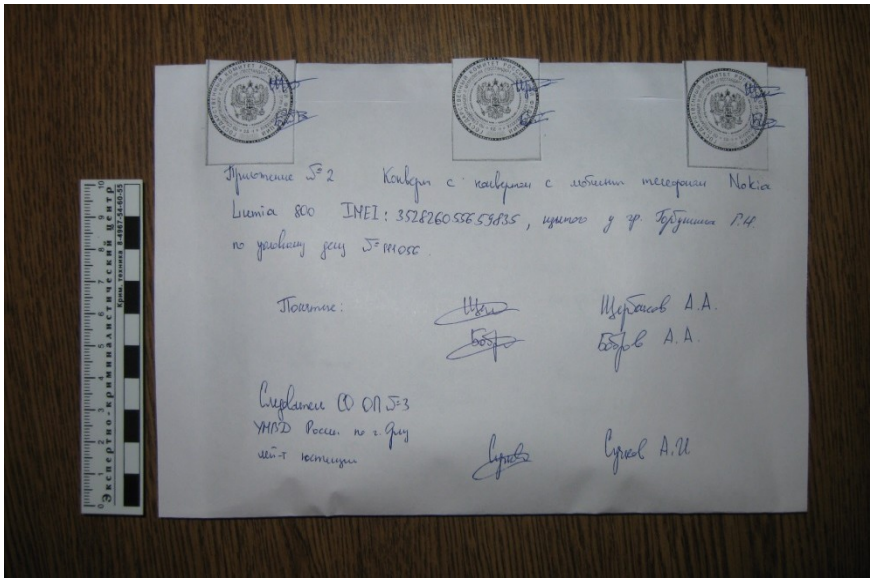


Иллюстрация № 23. Общий вид лицевой стороны упаковки телефона после его осмотра

Иллюстрация № 24. Общий вид оборотной стороны упаковки телефона после его осмотра

Следователь СО ОП № 3 УМВД России по г. Орлу
лейтенант юстиции

Место для печати

Сучков А.И.

ПРОТОКОЛ
осмотра предметов (документов)

г. Орел «*23*» *марта 2014 г.*

Осмотр начат в *15* ч *00* мин
Осмотр окончен в *15* ч *30* мин
Следователь СО ОП № 2 УМВД России по г. Орлу лейтенант юстиции Уваров Алексей Олегович
в присутствии понятых:

1. *Иванова Ивана Ивановича 1989 г.р., проживающего по адресу: г. Орел, ул. Игнатова 5, кв. 7*

2. *Петрова Петра Андреевича 1988 г.р., проживающего по адресу: г. Орел, ул. Игнатова 7, кв. 3*

с участием *специалиста криминалиста эксперта ЭКЦ УМВД России по Энской области лейтенанта полиции Торлоповой Екатерины Александровны*
в соответствии со ст. 164, частью первой ст.176, частями первой-четвертой и шестой ст. 177 УПК РФ произвел осмотр *в кабинете Г-309 Орловского юридического института им. В.В. Лукьянов, расположенного по адресу: г. Орел, ул. Игнатова 2, мобильного телефона «SonyXperia» IMEI 356179056243795, о чем в соответствии со ст. 166 УАК РФ составил настоящий протокол.*

Перед началом осмотра участвующим лицам разъяснены их права, обязанности и ответственность, а также порядок производства осмотра предметов (документов).

Понятым, кроме того, до начала осмотра разъяснены их права, обязанности и ответственность, предусмотренные ст.60 УПК РФ.

Подписи понятых

Специалисту *Торлоповой Екатерине Александровне* разъяснены права, обязанность и ответственность, предусмотренные ст. 58 (57) УПК РФ.

Подпись специалиста

Лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств *цифрового фотоаппарата Canon P350i, с флеш-картой объемом памяти 8 Gb.*

Осмотр производился в условиях *смешанного освещения.*

Осмотром установлено: *в присутствии понятых Иванова И.И. и Петрова П.А., специалиста-криминалиста эксперта ЭКЦ УМВД России по Орловской области лейтенанта полиции Торлоповой Е.А. был вскрыт бумажный пакет, опечатанный трема оттисками печати «Для пакетов». На конверте имеется надпись: «Мобильный телефон «SonyXperia» IMEI: 356179056243795, изъятый от 01 декабря 2013 года при личном обыске у подозреваемого Сидорова Сергея Сергеевича» стоят подписи понятых и следователя. Конверт повреждений и разрывов не имеет; целостность оттисков печатей не нарушена.*

При вскрытии конверта в нем оказался мобильный телефон «SonyXperia» в корпусе черного цвета с серебристой окантовкой по кругу длиной 120,4 мм, шириной 60,1 мм, толщиной 7 мм, весом 109 г, имеет прямоугольную форму. Мобильный телефон выполнен из полимерного материала черного цвета с серебристыми вставками по кругу на боковой панели.

На момент осмотра мобильный телефон находится в выключенном состоянии. Следов пальцев рук и посторонних веществ на телефоне не обнаружено.

На корпусе расположены:

1) на лицевой стороне – экран размером 90х51 мм, 3 сенсорные клавиши с тематическими символами. Над экраном расположены отверстия для динамиков, фронтальная камера и надпись, выполненная красителем серебристого цвета латинскими символами «SONY». Также на лицевой стороне имеется защитная пленка.

2) на верхней боковой стороне корпуса имеется разъем круглой формы для подключения дополнительного оборудования.

3) на левой боковой стороне корпуса имеется разъем прямоугольной формы для подключения дополнительного оборудования.

4) на правой боковой стороне корпуса имеются клавиши регулирования громкости и включения/выключения мобильного телефона.

5) оборотная сторона осматриваемого мобильного телефона состоит из:

- крышки, выполненной из полимерного материала черного цвета, закрывающей отсек, предназначенный для аккумуляторной батареи на которой имеется надпись, выполненная красителем серебристого цвета латинскими символами «XPERIA». В нижней части крышки мобильного телефона имеется отверстие прямоугольной формы для динамика, в верхней части крышки 2 отверстия круглой формы (для фотокамеры и фотовспышки).

- основной части корпуса телефона, выполненного из металла блестящего серебристого цвета, на которой имеется объектив фотокамеры круглой формы и фотовспышка круглой формы. Ниже фотокамеры и фотовспышки имеются два слота, в которых находятся SIM-карта сотовой компании «TELE2» и флеш-карта «Transcend 8GbmicroSDHC», объемом памяти 8 Gb. С лицевой стороны SIM-карта имеет надпись, выполненную из белого цвета с латинскими символами и арабскими обозначениями «TELE2».

При удалении крышки аккумуляторного отсека, обнаружена аккумуляторная батарея длиной 61 мм, шириной 55 мм, толщиной 5 мм, выполненная из полимера черного цвета. На лицевой части аккумуляторной батареи имеется надпись, выполненная красителем серебристого цвета «SONY», «BA900», а также голографическая наклейка, при просмотре которой в косопадающих лучах света читается надпись: «SONY». На оборотной стороне аккумуляторной батареи имеются следующие символы и цифры: «SONY», «Battery», «Li-Polymer», «TypeAB-0500», «1256-4166/3», «S/N 100103TWX0PS», «1700 mAh»/ Внизу расположена надпись: «MadeinChina».

При извлечении аккумуляторной батареи, на корпусе мобильного телефона обнаружена полоса бумажной ленты белого глянцевого цвета.

На полоске красителем черного цвета выполнены латинские символы, а также арабские цифры и криптографические символы. Надпись выполнена в девять параллельных строк: 1. «SONY», 2. «Type: PM-0160-BVABA», 3.«FCC iD: PY7PM-0160 «YT9», 4 «SIN: YT9108VJM6», 5. «Si 1266-0835», 6 «35617905-624379-5», 7 «СЭ 0682», 8 «Made in China», 9 «PCT MO 04».

При включении мобильного телефона отобразился фирменный логотип корпорации SONY, после чего на экране отобразилось главное меню. При нажатии на сенсорном экране на иконку "Телефон" высветились последние 5 вызовов абонента:

1) 8953251707 - входящий 9:51, 29 ноября 2013 год, продолжительностью 50 секунд;

2)89208742635 - входящий, 7:27, 30 ноября 2013 год, продолжительность 15 секунд;

3)89092086874 - отменен, время 11:02, 30 ноября 2013 год;

4)89102566874 - отменен, время 12:02, 30 ноября 2013 год;

5)89203568925 - исходящий, время 13:15, 30 ноября 2013 год, продолжительностью 1 мин 50 секунд.

При нажатии на сенсорном экране на иконку "Контакты" отобразились 5 контактов:

1) Андрей Афанютин - мобильный телефон: 89102365879, сохранен в памяти телефона;

2) Алексей Чернокозов - мобильный телефон: 89192036859, сохранен в памяти телефона;

3) Мамонтов - мобильный телефон: 89105698798, сохранен в памяти телефона;

4) Пырков - мобильный телефон: 89102896341, сохранен в памяти телефона;

5) Сестра - мобильный телефон: 89103569717, сохранен в памяти телефона.

При нажатии на эгране на иконку "Сообщения" отобразились 5 сообщений.

1) Входящее: 15:10, 30 ноября 2013 год, текст: "Привези мне документы" от абонента Пыркова;

2) Исходящее: 15:20, 30 ноября 2013 год, текст: "Сегодня вечером будут";

3) Входящее: 15:45, 30 ноября 2013 год, текст: "Поступил платеж сумма 50 рублей" от Tele2;

4) Входящее: 16:17, 30 ноября 2013 год, текст: "Заберешь когда машину?" от абонента Андрея Афанютина;

5) Исходящее: 16:20, 30 ноября 2013 год, текст: "Давай часиков в восемь!".

При нажатии на иконку "Фото" открываются 5 изображений и один видеофайл:

1) Название: приора, размер 145 кб, изображен автомобиль серебристого автомобиль;

2) Название: фотка, размер 456 кб, изображен гараж;

3) Название: Изображение 23, размер 345кб, изображена кошка;

4) Название: фото 3, размер 564 кб, изображен собака;

5) Название: фото 4, размер 564 кб, изображен елка.

Видеофайл: название Видеозапись 1, размер 1,4 Гб, формат Mp4, продолжительность 30 секунд, на видеозаписи кошка бегает по кругу за своим хвостом.

После произведенного осмотра: *мобильный телефон был сфотографирован специалистом-криминалистом экспертом ЭКЦ УМВД России по Орловской области лейтенантом полиции Торлоповой Е.А. по правилам детальной масштабной фотосъемки цифровым фотоаппаратом марки «CanonP350i» с флеш-картой объемом памяти 8Gb и помещен в бумажный конверт, с надписью: «Мобильный телефон «SonyXperia» IMEI: 356179056243795, изъятый от 01 декабря 2013 года при личном обыске у подозреваемого Сидорова Сергея Сергеевича и осмотренный 07 декабря 2013 года». Конверт заклеен и опечатан тремя оттисками печати «Для пакетов». На конверте и оттисках печати стоят подписи понятых и следователя. Подписи понятых*

К протоколу осмотра прилагается *иллюстрационная таблица*.

В ходе следственного действия заявлений, замечаний на действия участников осмотра и правильность составления протокола *не поступили.*

Подписи понятых

Протокол предъявлен для ознакомления всем лицам, участвовавшим в следственном действии. При этом указанным лицам разъяснено их право делать, подлежащие внесению в протокол оговоренные и удостоверенные подписями этих лиц, замечания о его дополнении и уточнении. Ознакомившись с протоколом путем *личного прочтения по окончании осмотра от участвующих лиц заявлений, замечаний на действия участников осмотра и правильность составления протокола не поступили.*

Подписи понятых, специалиста и следователя

Фрагмент протокола осмотра сенсорного смартфона «HTC»

в присутствии понятых и специалиста был вскрыт бумажный конверт, опечатанный тремя оттисками мастичной печати, в которой читается «Для пакетов №14». На конверте имеется надпись «Мобильный телефон «HTC Radar c110e» IMEI 358087043853162, изъятый при личном обыске у подозреваемого Сидорова Н.О. 07.12.2013.» На конверте имеются подписи понятых и следователя. Конверт повреждений и разрывов не имеет, целостность оттисков печатей на конверте не нарушена. При вскрытии конверта в нем оказался мобильный телефон «HTC Radar c110e» в чехле белого цвета. Корпус телефона серебристо-белого цвета длинной 120 мм, шириной 60 мм, толщиной 11 мм, имеет прямоугольную форму. Все углы телефона закруглены. Мобильный телефон выполнен из металла серебристого цвета с белыми вставками из пластика. На момент начала осмотра мобильный телефон находится в выключенном состоянии. Следов пальцев рук и посторонних веществ на телефоне не обнаружено. На корпусе имеются: на лицевой стороне – экран размером 50 мм на 83 мм. Над экраном расположено отверстие для динамика и текст, выполненный красителем серебристого цвета латинскими символами «htc»;на левой боковой стороне в нижней части расположен разъем для наушников; на правой боковой стороне расположена клавиши «включение камеры» и «регулятор громкости»; г) на верхней боковой стороне корпуса имеется клавиша «включение/выключение» телефона, разъем USB; на оборотной стороне корпуса осматриваемого мобильного телефона имеется надпись, выполненная из металла белого цвета латинскими символами «htc», объектив встроенной камеры.

При удалении крышки-аккумулятора и ее просмотре, обнаружена надпись «WNC-EVA 111008». На корпусе мобильного телефона обнаружена полоска клейкой бумажной ленты серого цвета. На полоске красителем черного цвета выполнены следующие надписи «IMEI 358087043853162», ниже выполнена надпись: «S/N : FA2B2VR00982». Выше указанной полоски имеется ячейка (слот) для SIM-карты. В ячейке имеется SIM-карта темно-синего цвета с логотипом компании TELE-2. На обороте корпуса SIM-карты красителем серого цвета сделано цифровое обозначение « 89701200430001481708.»

Особые приметы мобильного телефона: на верхней боковой стороне имеется скол прямоугольной формы размером 3*9 мм. Мобильный телефон был собран и принял первоначальный вид (вид до начала осмотра). Телефон при нажатии на клавишу включения/выключения включается, на экране появляется текст «HTC», затем телефон выключается.

После произведенного осмотра телефон упакован в белый бумажный конверт, который заклеен и опечатан тремя оттисками мастичной печати, в которых читается «Для пакетов №14», печати заверены подписями понятых, часть подписей находится на печати, а часть на конверте. Конверт снабжен надписью: ««Мобильный телефон «HTC Radar c110e» IMEI 358087043853162, изъятый при личном обыске у подозреваемого Сидорова Н.О. 07.12.2013.». Ниже имеются подписи понятых, специалиста и следователя.

Иллюстрационная таблица (приложение №1)
к протоколу осмотра мобильного телефона «HTC Radar c110e», IMEI 358087043853162,
изъятого при личном обыске у подозреваемого Сидорова Н.О. 07.12.2013 г.

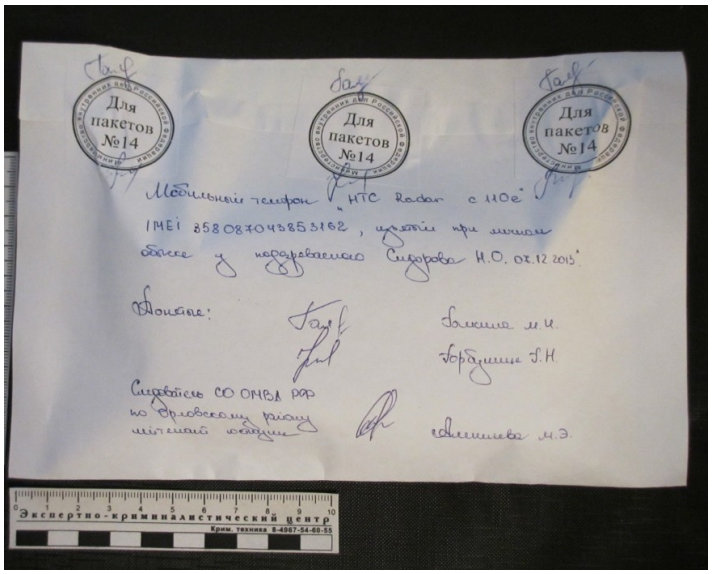


Иллюстрация № 1. Конверт с мобильным телефоном «HTC Radar c110e»

Иллюстрация № 2. Лицевая сторона мобильного телефона «HTC Radar c110e» в чехле

Фотосъемку произвел и иллюстрационную таблицу
составил специалист-криминалист эксперт
ЭКЦ УМВД России по Орловской области области

Место для печати

Сорокин М.М.

Лист 2

Продолжение иллюстрационной таблицы

Иллюстрация № 3. Оборотная сторона мобильного телефона «HTC Radar c110e» в чехле

Иллюстрация № 4. Лицевая сторона мобильного телефона «HTC Radar c110e» без чехла

Фотосъемку произвел и иллюстрационную таблицу составил специалист-криминалист эксперт ЭКЦ УМВД России по Орловской области области

Место для печати

Сорокин М.М.

Лист 3

Продолжение иллюстрационной таблицы

Иллюстрация №5. Оборотная сторона мобильного телефона «HTC Radar c110e» без чехла

Иллюстрация № 6. Оборотная сторона мобильного телефона «HTC Radar c110e» без задней крышки с SIM-картой

Фотосъемку произвел и иллюстрационную таблицу составил специалист-криминалист эксперт ЭКЦ УМВД России по Орловской области области

Место для печати

Сорокин М.М.

Лист 4

Продолжение иллюстрационной таблицы

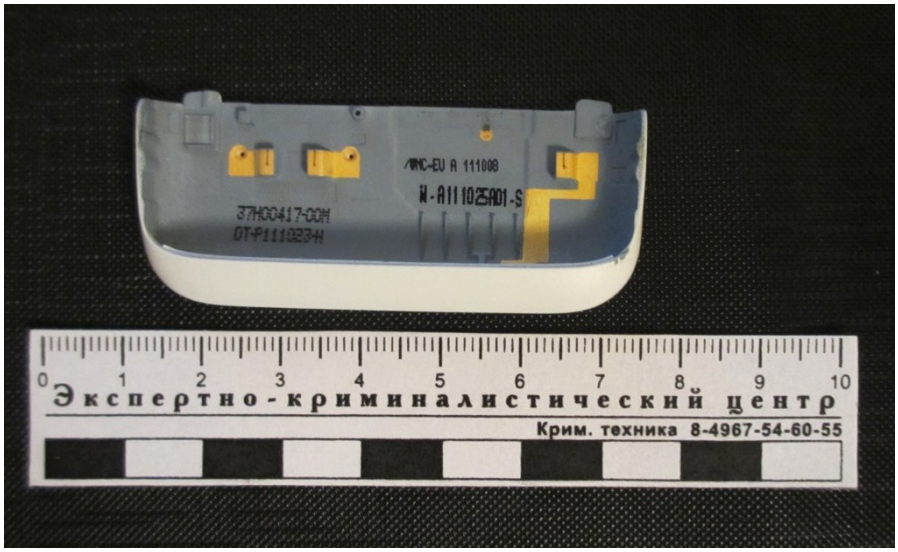


Иллюстрация № 7. Внутренняя сторона задней крышки телефона

Иллюстрация № 8. Мобильный телефон «HTC Radar c110e»
без крышки аккумулятора и SIM-карты

Фотосъемку произвел и иллюстрационную таблицу
составил специалист-криминалист эксперт
ЭКЦ УМВД России по Орловской области области

Место для печати

Сорокин М.М.

Лист 5

Продолжение иллюстрационной таблицы

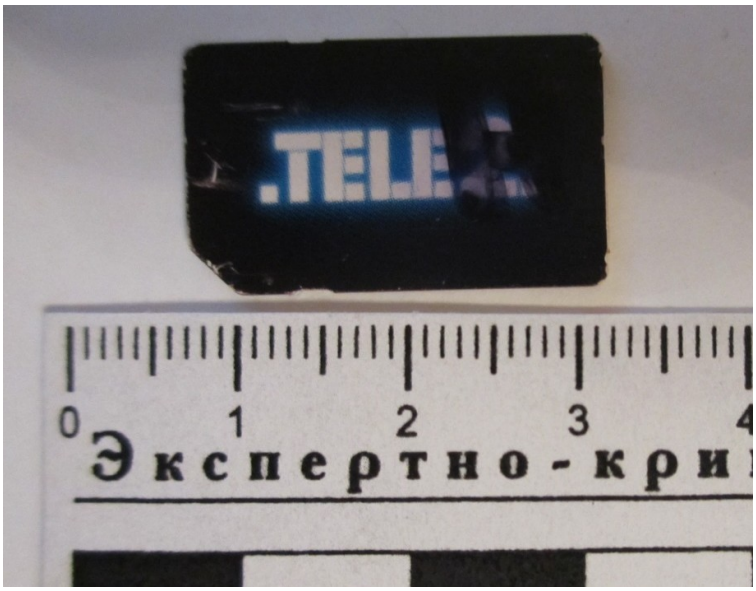


Иллюстрация № 9. Лицевая сторона SIM-карты, обнаруженной в мобильном телефоне «HTC Radar c110e»

Иллюстрация № 10. Оборотная сторона SIM-карты, обнаруженной в мобильном телефоне «HTC Radar c110e»

Фотосъемку произвел и иллюстрационную таблицу составил специалист-криминалист эксперт ЭКЦ УМВД России по Орловской области области

Место для печати

Сорокин М.М.

Лист 6

Продолжение иллюстрационной таблицы

Иллюстрация № 11. IMEI Номер мобильного телефона «HTC Radar c110e»

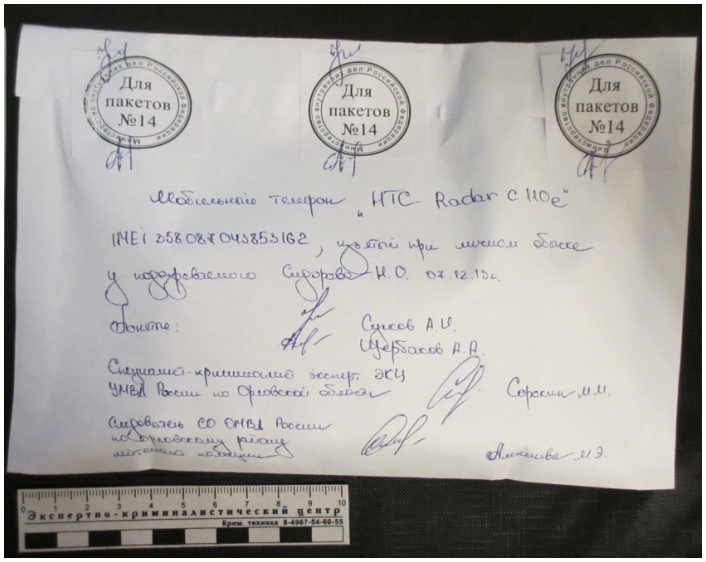


Иллюстрация № 12. Конверт с мобильным телефоном « HTC» модели « Radar c110e»

Фотосъемку произвел и иллюстрационную таблицу составил специалист-криминалист эксперт ЭКЦ УМВД России по Орловской области области Сорокин М.М.

Место для печати

Следователь Аленичева М.Э.

ПРОТОКОЛ
осмотра предметов (документов)

г. Энск «*3*» *мая 2014 г.*

Осмотр начат в *12* ч *00* мин
Осмотр окончен в *13* ч *35* мин

Следователь СО ОП №2 УМВД России по г.Энску лейтенант юстиции Петров Иван Алексеевич, с участием специалиста криминалиста эксперта ЭКЦ УМВД по Энской области, лейтенанта полиции Барановой Анны Сергеевны в соответствии со ст. 164, частью первой ст.176, частями первой-четвертой и шестой ст. 177 УПК РФ произвел осмотр в кабинете №10 СО ОП №2 УМВД России по г. Энску, расположенного по адресу: г. Энск, ул.Комсомольская 31, планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» о чем в соответствии со ст. 166 УПК РФ составил настоящий протокол.

Перед началом осмотра участвующим лицам разъяснены их права, обязанности и ответственность, а также порядок производства осмотра предметов (документов).

Специалисту *Барановой Анне Сергеевне* разъяснены права, обязанность и ответственность, предусмотренные ст. 58 (57) УПК РФ.

_____ *Баранова А.С.*

Лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств *цифрового фотоаппарата Canon EOS 650D Kit, с флеш-картой объемом памяти 16 Gb, чемодан «Криминалист».*

Осмотр производился в условиях *смешанного освещения.*

Осмотром установлено: *в присутствии специалиста-криминалиста эксперта ЭКЦ УМВД РФ по Энской области лейтенанта полиции Барановой А.С. был вскрыт прямоугольный бумажный пакет, опечатанный двумя квадратными отрезками бумаги с оттисками печати «Для пакетов». На конверте имеется рукописная надпись: «Планшетный компьютер «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества», ниже стоят подписи понятых и следователя. Конверт повреждений и разрывов не имеет; целостность оттисков печатей не нарушена.*

При вскрытии конверта в нем обнаружен планшетный компьютер «iPad Air, Space Gray, Wi-Fi + Cellular» прямоугольной формы, высотой 240 мм, шириной 169,5 мм, толщиной 7,5 мм, в корпусе черного цвета с лицевой стороны и серебристого цвета с оборотной стороны. Лицевая сторона планшетного компьютера выполнена из специального стекла черного цвета, оборотная сторона из анодированного алюминия серебристого цвета. На момент осмотра планшетный компьютер находится в включенном состоянии.

Корпус планшетного компьютера имеет мелкие потертости, более существенных повреждений на корпусе нет. На корпусе расположены:

1) на лицевой стороне – сенсорный дисплей размерами с технологией IPS 20 x 15 мм (по диагонали со светодиодной подсветкой), под дисплеем расположена кнопка «Home». Над дисплеем расположена 1.2-мегапиксельная фронтальная камера FaceTime HD с возможностью записи видео HD 720p;

2) на верхней боковой стороне корпуса имеются кнопка «Power», 3,5-мм стерео мини-Джек для наушников и микрофон;

3) на левой боковой стороне корпуса имеется пустой нано-лоток для SIM-карты;

4) на правой боковой стороне корпуса имеются кнопки регулировки громкости (+/-), переключатель беззвучного режима;

5) на оборотной стороне осматриваемого планшетного компьютера имеется 5-мегапиксельная основная камера iSight с возможностью записи видео Full HD 1080p. В нижней части оборотной стороны имеется текст, выполненный красителем черного цвета латинскими символами «iPad», ниже «Designed by Apple in California Assembled in China Model A1475 FCC ID:BCGA 1475 IC:579C-A1475 Serial: DMPLXQFJF4YF» и графические символы по эксплуатации данного планшетного компьютера;

6) на нижней боковой стороне корпуса имеются молния разъем для зарядного устройства и два встроенных динамика.

При нажатии кнопки планшетного компьютера «Power», появляется экран блокировки данного устройства. При разблокировании появилось рабочее меню данного устройства. При входе в один из имеющихся разделов – «Заметки» была обнаружена запись «Данные о переводах» со следующим содержанием: л/с 000 111 222 333 – 15:30 – 13.03.2014 года – 15 000 руб.; л/с 444 555 666 777 – 18:00 – 14.03.2014 года – 60 000 руб.; л/с 888 999 000 111 – 15:30 – 15.03.2014 года – 45 000 руб.; л/с 000 111 222 333 – 18:00 – 15.03.2014 года – 30 000 руб.».

После произведенного осмотра: *планшетный компьютер был собран в первоначальный вид, сфотографирован специалистом-криминалистом экспертом ЭКЦ УМВД по Энской области лейтенантом полиции Барановой А.С. по правилам детальной масштабной фотосъемки цифровым фотоаппаратом марки Canon EOS 650D Kit, с флеш-картой объемом памяти 16 Gb и помещен вместе с первоначальной упаковкой в прозрачный полиэтиленовый пакет и снабжен биркой с надписью: «Планшетный компьютер «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества». Пакет заклеен и опечатан отрезком бумаги с оттисками печати «Для пакетов». На конверте и оттисках стоят подписи специалиста и следователя.*

К протоколу осмотра прилагается *иллюстрационная таблица*.

По ходу следственного действия заявлений, замечаний на действия участников осмотра и правильность составления протокола не поступили.

Протокол предъявлен для ознакомления всем лицам, участвовавшим в следственном действии. При этом указанным лицам разъяснено их право делать, подлежащие внесению в протокол оговоренные и удостоверенные подписями этих лиц, замечания о его дополнении и уточнении. Ознакомившись с протоколом путем *личного прочтения по окончании осмотра от участвующих лиц заявлений, замечаний на действия участников осмотра и правильность составления протокола не поступили.*

Специалист *Баранова*
Следователь *Петров*

Иллюстрационная таблица
(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

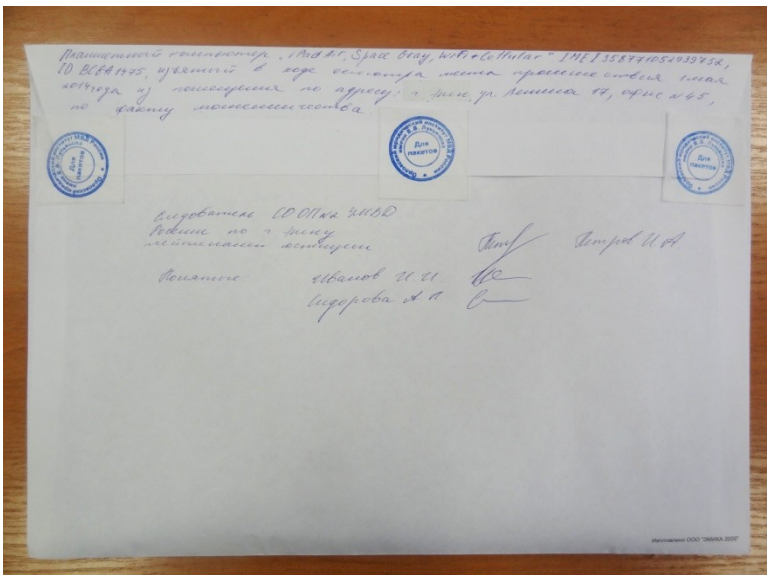


Иллюстрация № 1. Конверт, при вскрытии которого был обнаружен планшетный компьютер

Иллюстрация № 2. Общий вид конверта после вскрытия

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции Место для печати Баранова А.С.

Лист № 2

Продолжение иллюстрационной таблицы
(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

Иллюстрация № 3. Лицевая сторона планшетного компьютера

Иллюстрация № 4. Оборотная сторона планшетного компьютера

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 3

Продолжение иллюстрационной таблицы

(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

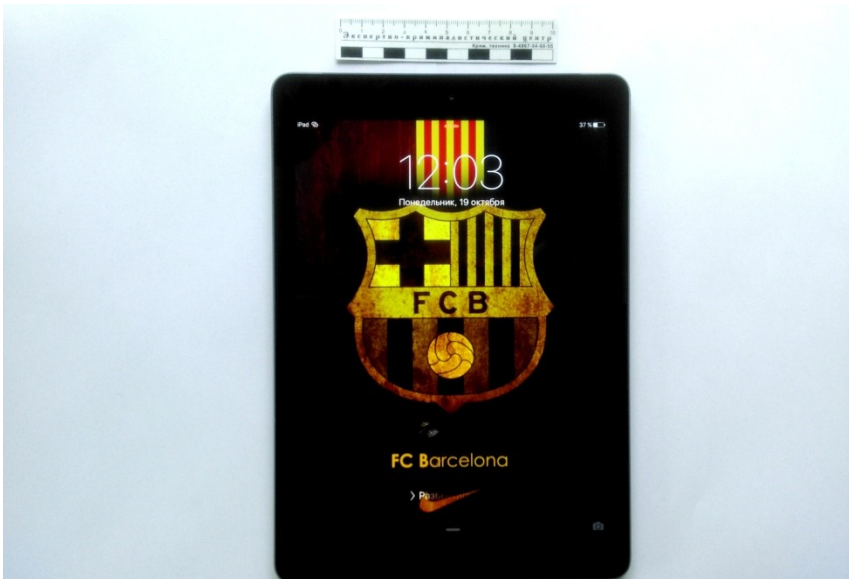


Иллюстрация № 5. Экран блокировки планшетного компьютера при нажатии кнопки «Power»

Иллюстрация № 6. Рабочее меню планшетного компьютера при разблокировании

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 4

Продолжение иллюстрационной таблицы

(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

Иллюстрация № 7. Общий вид раздела «Настройки» - «Основные»

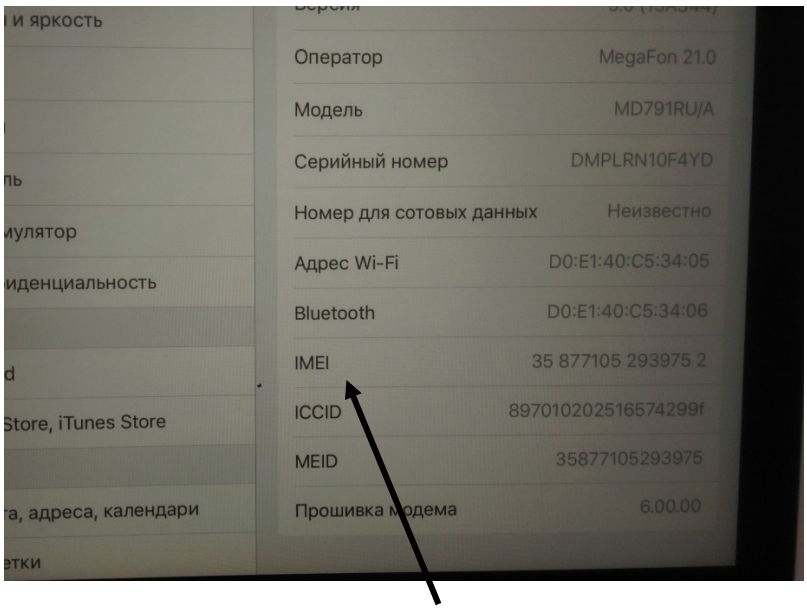


Иллюстрация № 8. IMEI планшетного компьютера

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 5

Продолжение иллюстрационной таблицы

(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

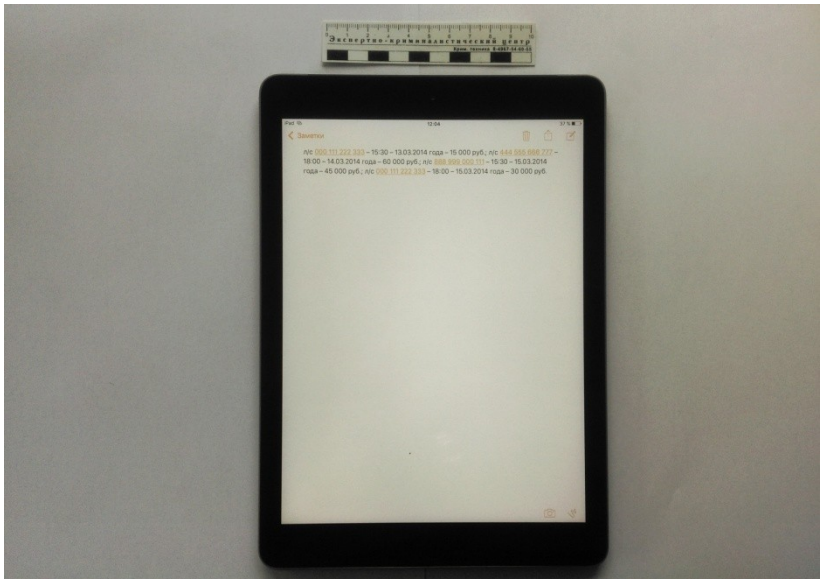


Иллюстрация № 9. Общий вид раздела «Заметки»

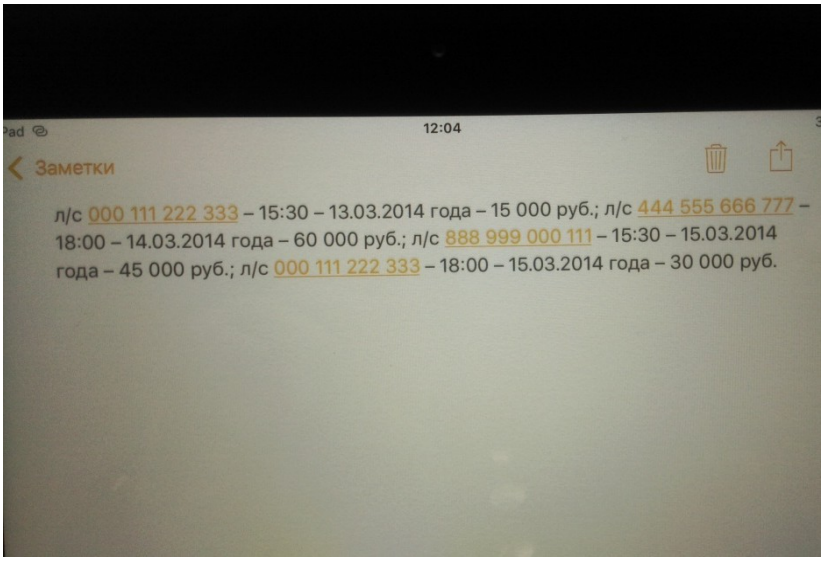


Иллюстрация № 10. Запись «Данные о переводах» в разделе «Заметки»

Специалист-криминалист эксперт ЭКЦ УМВД России по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Лист № 6

Продолжение иллюстрационной таблицы

(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

Иллюстрация № 11. Общий вид распечатанного конверта, в который был помещен осмотренный планшетный компьютер, и его первоначальная упаковка

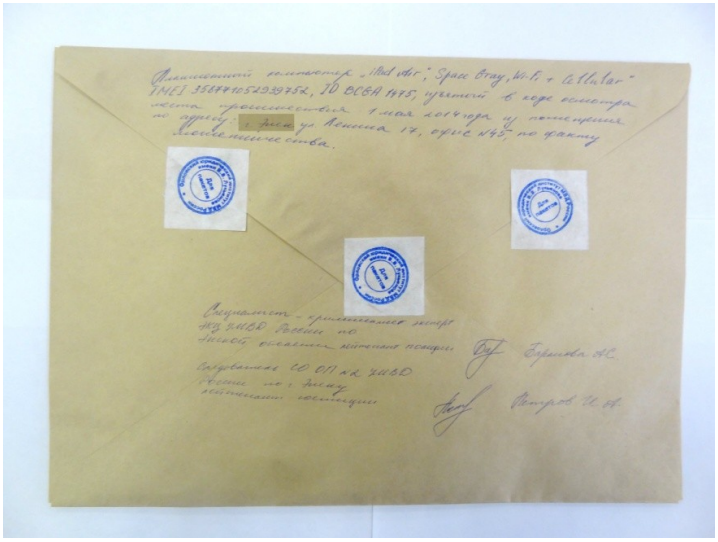


Иллюстрация № 12. Конверт, в который был помещен осмотренный планшетный компьютер, и его первоначальная упаковка

Фотосъемку произвел и иллюстрационную таблицу составил:
специалист-криминалист эксперт ЭКЦ УМВД России
по Энской области лейтенант полиции Баранова А.С.

Место для печати

Лист № 7

Продолжение иллюстрационной таблицы
(приложение) к протоколу осмотра планшетного компьютера «iPad Air, Space Gray, Wi-Fi + Cellular» IMEI 358771052939752, ID BCGA 1475, изъятый в ходе осмотра места происшествия 1 мая 2014 года из помещения по адресу: г. Энск, ул. Ленина, 17, офис № 45 по факту мошенничества

Место расположения конверта с диском CD-R №4032565678 объемом 320 Mb

Фотосъемку произвел и иллюстрационную таблицу составил:
специалист-криминалист эксперт ЭКЦ УМВД России
по Энской области лейтенант полиции

Место для печати

Баранова А.С.

Практические рекомендации

Авторский коллектив:

кандидат юридических наук, доцент
Чаплыгина Виктория Николаевна;
доктор юридических наук, доцент
Васюков Виталий Федорович;
кандидат юридических наук
Колычева Алла Николаевна

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВА

Свидетельство о государственной аккредитации
Рег. № 2660 от 02.08.2017 г.
Подписано в печать 28.12.2019 г. Формат 60x90$^{1}/_{16}$.
Усл. печ. л. – 4,81. Тираж 24 экз. Заказ № 55.

Орловский юридический институт МВД России имени В. В. Лукьянова.
302027, г. Орел, ул. Игнатова, 2.