ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

УДК 343.1:343.7

DOI: http://dx.doi.org/10.21202/1993-047X.10.2016.2.264-272

Как цитировать статью: Сергеев М. С. Критерии доказывания электронных преступлений при применении мобильных приложений. Особенности их изъятия // Актуальные проблемы экономики и права. 2016. Т. 10, № 2. С. 264–272.

М. С. СЕРГЕЕВ[1]

[1] *Казанский (Приволжский) федеральный университет, г. Казань, Россия*

КРИТЕРИИ ДОКАЗЫВАНИЯ ЭЛЕКТРОННЫХ ПРЕСТУПЛЕНИЙ ПРИ ПРИМЕНЕНИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ. ОСОБЕННОСТИ ИХ ИЗЪЯТИЯ

Цель: выявление проблем, возникающих в ходе изъятия у физических и юридических лиц сведений об электронных мобильных приложениях, которые позволяют получить доступ к личной информации, разработка решений выявленных проблем.

Методы: в целях решения поставленных задач использовались всеобщий метод познания и общенаучные методы исследования: логический метод, анализ и синтез. Кроме того, были использованы такие научные методы познания, как логико-формальный, компаративный, статистический, системного анализа.

Результаты: выработаны предложения по внесению изменений в уголовное и уголовно-процессуальное законодательство, которые позволят решить выявленные проблемы. Предложено дополнить Уголовный кодекс РФ (далее – УК РФ) разделом 8.1 «Электронные преступления», который, по нашему мнению, должен содержать пункт о мошенничестве с использованием платежных карт в сфере компьютерной информации; неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных компьютерных программ; нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Научная новизна: в исследовании рассмотрен правовой статус данных мобильных приложений, особенности процедуры выемки, необходимость выделения их в качестве отдельного вида электронных доказательств.

Практическая значимость: основные положения и выводы исследования могут быть использованы при реформировании уголовно-процессуального законодательства, а также в научной и педагогической деятельности.

Ключевые слова: уголовный процесс; электронные источники доказательства; мобильные приложения; вредоносные программы; выемка; критерии доказывания электронных преступлений

Введение

Исследователи рассматривают природу электронных доказательств в уголовном судопроизводстве в целом [1; 2, с. 76; 3, с. 192; 4 с. 53; 5 с. 6]. Бесспорно сложившееся мнение о том, что «электронное доказательство» следует рассматривать в качестве самостоятельного источника доказательства ввиду того, что сбор, хранение, а также воспроизведение электронной информации требует отличных от письменных и вещественных доказательств методов [6, с. 97]. Поддерживая данную точку зрения, следует отметить, что уголовно-процессуальное законодательство не выделяет электронные доказательства в качестве самостоятельного источника доказательства, закрепляя «электронный носитель информации» в качестве вещественного доказательства (п. 5, ч. 2, ст. 82 УПК РФ) и «иные носители информации» в качестве иных документов. В связи с этим предлагается следующее определение электронных доказательств: это сведения в электронно-цифровой форме, созданные при помощи электронно-вычислительных средств, на основании которых устанавливается наличие или отсутствие обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела.

В статье рассмотрена возможность и необходимость выделения такого вида электронного доказательства, как данные мобильных приложений. Целью работы является выявление проблем, возникающих в ходе изъятия сведений об электронных мобильных приложениях, которые позволяют получить доступ

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

к личной информации; разработка решений этих проблем.

Проведение данного исследования вызвано назревшей потребностью модернизации уголовного судопроизводства, о чем упоминается в научных трудах целого ряда исследователей: П. С. Пастухова [7, с. 16], Н. А. Зигуры [8, с. 52], Ю. А. Цветкова и О. В. Качалова [9, с. 96] и других, а также оценки необходимости выделения данных мобильных приложений в качестве отдельного вида доказательств по уголовным делам. Актуальность затронутой проблематики обусловлена тем, что с ростом рынка мобильных устройств связи ежедневно увеличивается количество приложений для таких устройств[1]. Динамика роста числа мобильных приложений на сегодняшний день следующая: за 2014 г. количество мобильных приложений в магазинах увеличилось более чем в два раза. По данным аналитической компании Appfigures, в магазине Google Play на начало 2015 г. были доступны 1,43 млн приложений, в Apple App Store – 1,21 млн, а в Amazon Appstore – 293 тысячи[2].

Существуют различные категории мобильных приложений: мультимедийные, офисные, игровые, социальные, навигационные, приложения онлайн-банкинга и др. Как правило, данные таких приложений содержат личную информацию пользователя, включающую в себя круг общения, электронную корреспонденцию, данные об истории поисковых запросов, доступ к банковским счетам, аккаунтам в различных информационных системах, сведения о фактическом местоположении, а также истории передвижения пользователя.

На сегодняшний день сложно представить себе активного члена общества, который бы не использовал мобильные устройства. По данным аналитического исследования, проведенного специалистами компании eMarketer, количество пользователей смартфонов в 2014 г. в России составило 49 млн человек, в 2015 г. – 58,2 млн человек, а к 2018 г., по прогнозам, достигнет 76,4 млн человек. Таким образом, по итогам 2015 г. Россия занимает 4-е место в мире по количеству пользователей смартфонов, лидирует в данном рейтинге Китай – 520 млн владельцев мобильных устройств, следом идут США, Индия и Япония[3]. Иными словами, с каждым днем количество пользователей мобильных устройств в России возрастает, а вместе с ними и количество лиц, использующих мобильные приложения. Этому способствуют и цены на мобильные устройства, которые являются в России самыми низкими в мире, по информации Hi-tech.Mail.ru[4]. Как правило, мобильные устройства функционируют на основе операционных систем Android, Symbian, iOS (Apple), Blackberry, Windows (Microsoft). Согласно отчету Strategy Analytics[5], наиболее популярной является операционная система Android (ее доля на рынке составляет 84,6 %), второй по популярности стала iOS (Apple) (11,9 %)[6]. Таким образом, подавляющее большинство устройств функционирует на базе двух операционных систем – Android и iOS (Apple), что позволяет сделать вывод о том, что возможна выработка общей методики сбора, анализа и хранения данных мобильных приложений.

Результаты исследования

Результатом эволюционных процессов развития электронных технических средств стали изменения в уголовном и уголовно-процессуальном законодательстве. Это ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»), ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ»), ст. 274 УК РФ («Нарушение правил экс-

[1] Мобильное приложение – это компонент, устанавливаемый на мобильное устройство, подключающийся к мобильному серверу и управляющий пользовательским интерфейсом и бизнес-логикой устройства.

[2] App Stores Growth Accelerates in 2014. URL: http://blog.appfigures.com/app-stores-growth-accelerates-in-2014 (дата обращения: 01.02.2015).

[3] Россия станет четвертым рынком смартфонов в мире // Российская газета. 2014. 15 декабря. URL: http://www.rg.ru/2014/12/15/prognoz-site-anons.html (дата обращения: 01.02.2015).

[4] Смартфоны в России стали самыми дешевыми в мире // Российская газета. 2015. 23 февраля. URL: http://www.rg.ru/2015/02/23/smartphones-russia-site.html (дата обращения: 23.02.2015).

[5] Strategy analytics – исследовательская аналитическая компания.

[6] Android Captures 84 % Share of Global Smartphone Shipments in Q3 2014. URL: http://blogs.strategyanalytics.com/WSS/post/2014/10/31/Android-Captures-84-Share-of-Global-Smartphone-Shipments-in-Q3-2014.aspx (дата обращения: 01.02.2015).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

плуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).

Статистика широкого распространения мобильных электронных устройств[7] позволяет сделать выводы о важности мобильных устройств и, в частности, содержащейся в них информации для расследования всех категорий преступлений и необходимости адаптации следственных действий к современным реалиям, в связи с тем, что мобильные приложения зачастую выступают в качестве средства совершения преступления [10, p. 43]. Все необходимые требования и разрешения к каждой программе, такие как доступ к интернет-соединению, мобильным сообщениям, звонкам, GPS и другие, указываются разработчиком в зависимости от типа программы. Однако именно это облегчает использование электронного устройства в преступных целях, таких как мошенничество, кража денежных средств, неправомерный доступ к компьютерной информации, нарушение тайны переговоров, переписки и т. д. Например, компанией AVG[8] была выявлена вредоносная программа для OS Android, которая способна сохранять работоспособность даже после выключения мобильного устройства. Получив доступ к процессу завершения работы, программа имитировала его выключение и собирала данные пользователя путем использования камеры, микрофона и интернет-соединения[9].

Доступ к личным данным владельцев мобильных устройств возможен также с использованием специальных технических устройств, работающих аналогично вышкам сотовой связи. По данным The Wall Street Journal, с 2007 г. службой судебных приставов Минюста США реализована программа по сбору данных и определению местонахождения абонентов сотовой связи при помощи технических средств, установленных на легкомоторных самолетах. Аппаратура, разработанная компанией Boeing, действуя по принципу сотовых вышек связи, позволяет собрать регистрационную информацию с большого количества мобильных устройств, включая местоположение абонентов с точностью до трех метров. Также данное оборудование позволяет блокировать сигнал мобильного устройства и осуществлять копирование данных, включая СМС-сообщения и фотографии, содержащиеся на устройствах[10].

Кроме того, личные данные пользователей могут быть получены злоумышленниками при помощи шпионских и вредоносных программ. По данным компании Lookout[11], самая высокая вероятность столкнуться с вредоносным или шпионским программным обеспечением в России и Китае – от него страдают 34,7 % пользователей[12]. По итогам 2014 г. вирусная база самого популярного российского мобильного антивируса Dr.Web пополнилась 2 867 записями для различных вредоносных, нежелательных и потенциально опасных Android-программ и включает на сегодняшний день 5 681 вредоносное приложение. Их рост, по сравнению с аналогичным периодом 2013 г., составил 102 %, а с 2010 г. их число увеличилось в 189 раз, т. е. на 18 837 %. Наиболее популярными являются приложения, связанные с отправкой платных сообщений, – 47,33 %, «шпионские» программы, собирающие конфиденциальную информацию пользователя, – 6,35 %, трояны мобильного банкинга, собирающие информацию о банковских аккаунтах, паролях, – 3,12 %, «приложения-вымогатели», блокирующие устройства и требующие оплаты за разблокировку. Рост числа обнаруженных «приложений-вымогателей» составил 6 750 % за 2014 г. и увеличился с 2 до 137 записей[13].

За создание, распространение или использование вредоносных компьютерных программ предусмотрена уголовная ответственность, установленная ст.

---

[7] Россия станет четвертым рынком смартфонов в мире // Российская газета. 2014. 15 декабря. URL: http://www.rg.ru/2014/12/15/prognoz-site-anons.html (дата обращения: 01.02.2015).

[8] AVG Technologies – чешский разработчик антивирусного программного обеспечения.

[9] Malware Is Still Spying On You Even When Your Mobile Is Off. URL: http://now.avg.com/malware-is-still-spying-on-you-after-your-mobile-is-off/ (дата обращения: 23.02.2015).

[10] США уличили в сборе данных с мобильников при помощи самолетов. URL: http://lenta.ru/news/2014/11/14/phones/ (дата обращения: 23.02.2015).

[11] Lookout – компания, специализирующаяся на решениях для мобильных устройств, обеспечивающих кибербезопасность.

[12] 6 самых вредоносных приложений для смартфонов. URL: http://www.forbes.ru/tehnologii-photogallery/internet-i-svyaz/235027-android-virus/photo/1 (дата обращения: 23.02.2015).

[13] Обзор вирусной активности для мобильных устройств за 2014 год. URL: http://news.drweb.ru/show/?i=9222&c=5&lng=ru&p=1 (дата обращения: 23.02.2015).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

273 УК РФ. Однако при расследовании преступлений с использованием компьютерной информации возникают проблемы изъятия, хранения и представления доказательств по делу. Уголовно-процессуальным кодексом изъятие электронных носителей в ходе обыска и выемки информации регламентировано ч. 9.1 ст. 182 УПК РФ и ч. 3.1 ст. 183 УПК РФ с учетом положений ч. 4 ст. 81, ч. 5 ст. 82 УПК РФ.

При изъятии данных мобильных приложений в качестве источника электронных доказательств необходимо использовать специализированный софт. Примерами таких прикладных программ являются EnCase ® Smartphone Examiner, MOBILedit! Forensic[14], Mobile Phone Examiner Plus[15] и др. Эти инструменты разработаны для сотрудников правоохранительных органов и специалистов информационной безопасности в целях сбора доказательств из мобильных устройств, они позволяют физически получать логические данные с устройств, добыть образ операционной системы, включающий файловую систему. После проведения анализа мобильных устройств возможен перенос собранной информации в специализированную программу FTK (Forensic Toolkit) для дальнейшего изучения, например, с целью восстановления удаленных файлов. Также эта интеграция позволяет произвести корреляцию улик, собранных на мобильных устройствах, с уликами, собранными на компьютерах[16].

Процедура изъятия доказательств из мобильных устройств отличается от изъятия информации из персональных компьютеров ввиду того, что мобильные электронные устройства, по сравнению с персональными компьютерами, имеют более узкие задачи, различающуюся архитектуру процессора, операционную систему и т. д. В связи с этим методы и особенности проведения процессуальных действий должны быть индивидуальными, в зависимости от технических характеристик источника доказательств [11, p. 69].

Британской ассоциацией руководителей полицейских служб (ACPO) была разработана инструкция по изъятию доказательств с мобильных устройств[17]. Согласно предложенным рекомендациям, при проведении процессуальных действий необходимо изолировать устройство от мобильного соединения путем выключения устройства либо благодаря специальным глушащим связь устройствам, все необходимые процедуры должны проводиться в специально оборудованном помещении. Устройство должно быть полностью заряженным в целях предотвращения утери информации при проведении процессуальных действий. Следует учитывать особенность оперативной (RAM) памяти устройства, для сохранения данных на которой необходимо наличие бесперебойного питания в отличие от постоянной (ROM) памяти. В целях сохранения важной информации специалист должен строго соблюдать правила, не допускать обновления приложений, так как это может повлечь уничтожение данных. Вместе с данными приложений, находящимися на мобильном устройстве, необходимо также запросить сведения, хранящиеся на серверах разработчиков приложений и данные интернет-провайдера.

Для сбора доказательств в арсенале сотрудников МВД РФ имеются специализированные технические средства, позволяющие получать с мобильных устройств необходимые для расследования преступлений сведения. Благодаря данному комплексу сотрудники правоохранительных органов имеют возможность установить точки передвижения, входящие и исходящие соединения, электронную корреспонденцию в социальных сетях и мессенджерах, фото- и видеоматериалы. При этом возможно изъятие даже удаленных данных, а также информации из защищенных хранилищ, таких как Dropbox, Google Drive, iCloud и бэкапов Android [12 p. 528]. Кроме того, специалистом может быть установлен список посещенных адресов в Интернете, пароли с идентификаторов от облачных хранилищ либо учетных записей с Android-устройства, а также данные из более 400 мобильных приложений, таких как Apple Maps, Facebook, Google+, PayPal, Viber, WhatsApp и т. п. По словам официального представителя компании-поставщика таких систем «Оксиджн Софтвер» Николая Голубева: «Комплексы бывают мобильные

[14] URL: http://www.mobiledit.com/forensic (дата обращения: 23.02.2015).

[15] URL: http://accessdata.com/product-download/digital-forensics/mpe (дата обращения: 23.02.2015).

[16] URL: http://www.forensicmall.ru/cat/accessdata/mobile-phone-examiner-plus-mpe/#tab0 (дата обращения: 23.02.2015).

[17] Good Practice and Advice Guide for Managers of e-Crime Investigation. URL: http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf (дата обращения: 23.02.2015).

Актуальные проблемы экономики и права. 2016. Т. 10, № 2
Actual Problems of Economics and Law, 2016, vol. 10, No. 2
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

и стационарные. В первом случае комплекс имеет вид кейса с дисплеем и с комплектом проводов, что позволяет сотруднику прямо на месте преступления получить все данные, находящиеся в устройстве. В стационарном варианте программное обеспечение просто устанавливают на компьютер в криминалистической лаборатории»[18].

Также сотрудниками правоохранительных органов используется современная криминалистическая техника, позволяющая в короткие сроки получить информацию из памяти мобильных устройств. Это UFED[19], «Мобильный криминалист»[20], аппаратно-программный комплекс XRY[21].

Законодатель закрепил в ст. 182 и 183 УПК РФ необходимость обязательного участия специалиста в следственных действиях – обыске и выемке, в ходе которых он производит копирование информации на электронный носитель. В связи с этим представляется, что обязательное участие специалиста связано с рядом процедурных действий: 1) обнаружение мобильного устройства (материальный носитель); 2) изъятие и его процессуальное оформление (составление протокола обыска, выемки, личного обыска, задержания); 3) обнаружение специалистом файлов; 4) фиксация изъятой информации; 5) определение допустимости применения в качестве доказательств; 6) представление в суде; 7) сопоставление полученной информации с другими полученными доказательствами. Ряд процессуалистов считает, что регламентированная процедура участия специалиста несовершенна [13, с. 155; 14; 15; 16]. В частности, отсутствует четкая регламентация понятия «электронный носитель информации», в соответствии со справкой Государственно-правового управления[22] в качестве электронных носителей информации названы компьютерные блоки, серверы, ноутбуки и карты памяти. Очевидно, что данный перечень трудно назвать исчерпывающим. Считаем справедливым утверждение А. Л. Осипенко и А. И. Гайдина о том, что перечень следует определить более четко, а также необходимо регламентировать участие специалиста при изъятии электронных носителей информации лишь в тех случаях, когда это действительно необходимо [17, с. 158].

Процедура изъятия сведений мобильных приложений с устройств регламентируется п. 3.1 ст. 183 УПК РФ («Изъятие электронных носителей информации»). Однако в зависимости от характера информации (сведения о соединениях, электронная корреспонденция и т. д.) процессуальные действия можно трактовать как «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» (ст. 185 УПК РФ) или «получение информации о соединениях между абонентами и (или) абонентскими устройствами» (ст. 186.1 УПК РФ). В соответствии с требованиями данных положений необходимые процессуальные действия производятся на основании судебного решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами или наложения ареста и выемки корреспонденции.

Сотрудники правоохранительных органов, по смыслу текста статей, запрашивают сведения о соединениях у организации, осуществляющей услуги связи, которая обязана предоставить ее на любом материальном носителе информации, а арест и выемку корреспонденции производят в учреждениях связи. Возникает вопрос о необходимости судебного решения в случае изъятия сведений мобильных приложений с помощью технических средств, описанных выше. В соответствии с определением Конституционного Суда Российской Федерации № 345-О от 02.10.2003[23], информацией, составляющей охраняемую Конституцией РФ и действующими на территории РФ законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа

[18] МВД взломает продукцию Apple с помощью спецоборудования // Известия. 2014. 1 декабря. URL: http://izvestia.ru/news/579858 (дата обращения: 05.02.2015).

[19] URL: http://www.cellebrite.com/ru/mobile-forensics/products/standalone/ufed-touch-logical (дата обращения: 23.02.2015).

[20] URL: http://www.oxygen-forensic.com/ru/ (дата обращения: 23.02.2015).

[21] URL: http://aimtech.ru/catalog/48 (дата обращения: 23.02.2015).

[22] Уточнен порядок изъятия и возвращения электронных носителей в ходе расследования уголовных дел. URL: http://www.kremlin.ru/news/16111 (дата обращения: 23.02.2015).

[23] Определение Конституционного Суда Российской Федерации № 345-О от 02.10.2003. URL: http://www.rg.ru/2003/12/10/svjaz-doc.html (дата обращения: 23.02.2015).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

к указанным сведениям органам, осуществляющим оперативно-разыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования ст. 23 (ч. 2) Конституции РФ о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения. В связи с этим в случае производства следственных действий, связанных с изъятием сведений мобильных приложений, необходимо получение решения суда. Помимо вышеперечисленного, представляет интерес предложение о выделении в качестве самостоятельного следственного действия электронного копирования [18, с. 224; 19, с. 20; 20, с. 134]. Данное предложение представляется справедливым и актуальным.

Выводы

В ходе исследования выявлены следующие проблемы, возникающие при производстве изъятия у физических и юридических лиц сведений об электронных мобильных приложениях, которые позволяют получить доступ к личной информации: 1) в уголовном и уголовно-процессуальном законодательстве отсутствуют определения электронных доказательств, электронных носителей информации, электронной информации, сведений мобильных приложений; 2) отсутствует правовая регламентация порядка изъятия, хранения, представления электронных доказательств, в частности, сведений мобильных приложений.

В результате проведенного исследования предлагается дополнить ст. 186.1 УПК РФ частью 1.1: «Изъятие информации о соединениях между абонентами и (или) абонентскими устройствами может производиться следователем с применением специализированных технических средств, при участии специалиста на основании судебного решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами».

Статью 185 УПК РФ дополнить частью 2.1: «Изъятие электронной корреспонденции из электронной памяти персональных компьютеров, мобильных устройств, а также серверов компаний, осуществляющих возможность отправки электронной корреспонденции, производится на основании судебного решения».

Дополнить ст. 5 УПК РФ пунктом 63: «Электронные доказательства – это сведения в электронно-цифровой форме, созданные при помощи электронно-вычислительных средств, на основании которых устанавливается наличие или отсутствие обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела».

Дополнить ч. 2 ст. 74 УПК РФ пунктом 7: «Электронные доказательства».

Таким образом, можно сделать вывод о необходимости выделения мобильного приложения в качества отдельного подвида электронных доказательств, который может быть как источником информации, так и средством совершения преступления.

Кроме того, УК РФ следует дополнить разделом 8.1 «Электронные преступления», который будет содержать гл. 23.1 «Преступления в сфере электронного денежного оборота», гл. 23.2 «Преступления в сфере компьютерной информации». Данный раздел с точки зрения законодательной техники, по нашему мнению, должен содержать следующие составы преступлений:

– мошенничество с использованием платежных карт;

– мошенничество в сфере компьютерной информации;

– неправомерный доступ к компьютерной информации;

– создание, использование и распространение вредоносных компьютерных программ;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

При доказывании юридически значимых фактов по уголовному делу в целях предотвращения возможности совершения электронных преступлений пользователям следует контролировать состояние мобильного программного обеспечения, использовать антивирусную программу, внимательнее относиться к источнику приложений и условиям их установки и использования. В целях безопасности не следует сохранять данные банковских счетов, аккаунтов платежных систем на мобильном устройстве.

При проведении процессуальных действий, связанных с изъятием электронной информации, необходимо учитывать техническую сложность мобильного устройства, привлекать специалиста, а также использовать необходимые специализированные технические средства сбора электронных доказательств.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Список литературы

1. Калиновский К. Б., Маркелова Т. Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6. С. 18–19.

2. Александров А. С., Кувычков С. И. О надежности «электронных доказательств» в уголовном процессе // Библиотека криминалиста. 2013. № 5. С. 76–84.

3. Пастухов П. С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств // Общество и право. 2015. № 1 (51). С. 192–196.

4. Васильев А. А., Демин К. Е. Электронные носители данных как источники получения криминалистически значимой информации: учеб. пособие. М.: МГОУ, 2009. 198 с.

5. Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике: автореф. дис. … канд. юрид. наук. Воронеж, 2003. 25 с.

6. Треушников М. К. Судебные доказательства. М.: Городец, 1999. 288 с.

7. Пастухов П. С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дис. … докт. юрид. наук. М., 2015. 64 с.

8. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. … канд. юрид. наук. Челябинск, 2010. 234 с.

9. Качалова О. В., Цветков Ю. А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2. С. 95–101.

10. Casey E., Turnbull B. Digital Evidence on Mobile Devices // Digital Evidence and Computer Crime. Third Edition. ACADEMIC PRESS, 2011. 44 p.

11. Sammons J., Brunty J. Mobile device forensics: threats, challenges and future trends // Digital Forensics: Threatscape and Best Practices. Syngress. 2015, 182 p.

12. Mason S., George E. Digital evidence and 'cloud' computing // Computer Law & Security Review. 2011. No. 27. Pp. 524–528.

13. Родивилин И. П., Шаевич А. А. Об участии специалиста при изъятии электронных носителей информации в ходе производства обыска и выемки // Криминалистика: вчера, сегодня, завтра: сб. научн. трудов. 2013. Вып. 3–4. Иркутск: ВСИ МВД России. С. 153–157.

14. Иванов А. Н. Новый порядок изъятия электронных носителей информации при производстве обыска и выемки // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2012. № 1. Саратов: Изд-во Сарат. гос. юр. акад. С. 25–26.

15. Старичков М. В. Тактика проведения обыска, связанного с изъятием носителей компьютерной информации // Криминалистика: актуальные вопросы теории и практики: сб. VII Всероссийской научно-практической конференции. Ростов н/Д: РЮИ МВД России, 2010. С. 167–169.

16. Ларин Е. Г. Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. 2012. № 2 (29). Омск: Омская академия МВД России. С. 52–53.

17. Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник ВИ МВД России. 2014. № 1. С. 156–163.

18. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.

19. Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. … канд. юрид. наук. Воронеж, 2005. 24 с.

20. Овсянников Д. В. Электронное копирование информации в системе средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. 2014. № 2 (3). С. 130–135.

Дата поступления 17.10.15
Дата принятия в печать 11.03.16

Информация об авторе

Сергеев Максим Сергеевич, аспирант кафедры уголовного процесса и криминалистики, Казанский (Приволжский) федеральный университет

Адрес: 420008, г. Казань, ул. Кремлевская, 18, каб. 308а, тел.: +7 (843) 233-71-97

E-mail: sergeev.s.maksim@gmail.com

ORCID: http://orcid.org/0000-0002-8481-0603

Researcher ID: http://www.researcherid.com/rid/L-2219-2015

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

M. S. SERGEYEV[1]

[1] *Kazan (Volga) Federal University, Kazan, Russia*

CRITERIA OF PROVING DIGITAL CRIMES WITH THE USE OF MOBILE APPLICATIONS. FEATURES OF EXEMPTION

Objective: to identify problems arising in the course of exemption from individuals and legal entities information about mobile digital applications that allow access to personal information, to develop solutions to the identified problems.

Methods: in order to solve the identified tasks, we used the universal method of cognition and general scientific research methods: logical method, analysis and synthesis. In addition were used such scientific methods of cognition, as logical-formal, comparative, statistical, system analysis.

Results: proposals have been elaborated on amendments to the criminal and criminal procedure legislation, which will allow to solve the identified problems. It is proposed to supplement the Russian Criminal Code (hereinafter CC) with the Section 8.1 "Digital crimes", which, in our opinion, should contain a paragraph on fraud with payment cards in the field of computer information systems; illegal access to computer information, creation, use and dissemination of harmful computer programs; violation of exploitation rules of storage means, processing or transmission of computer information and information-telecommunication networks.

Scientific novelty: the study examined the legal status of mobile application data, peculiarities of the process of exemption, the need to allocate them as a separate type of digital proofs.

Practical significance: the key issues and conclusions of the study can be used in reforming the criminal procedure legislation, as well as in research and teaching.

Keywords: Criminal procedure; Electronic sources of proofs; Mobile applications; Malware; Exemption; Criteria of proving the electronic crimes

References

1. Kalinovskii, K. B., Markelova, T. Yu. Dokazatel'stvennoe znachenie "elektronnoi" informatsii v rossiiskom ugolovnom protsesse (Proving significance of “digital” information in the Russian criminal procedure), *Rossiiskii sledovatel',* 2001, No. 6, pp. 18–19 (in Russ.).

2. Aleksandrov, A. S., Kuvychkov, S. I. O nadezhnosti "elektronnykh dokazatel'stv" v ugolovnom protsesse (On the reliability of “digital proofs” in the criminal procedure), *Biblioteka kriminalista*, 2013, No. 5, pp. 76–84 (in Russ.).

3. Pastukhov, P. S. "Elektronnye dokazatel'stva" v sostyazatel'noi sisteme ugolovno-protsessual'nykh dokazatel'stv (“Digital proofs” in the competitive system of criminal-procedural proofs), *Obshchestvo i pravo*, 2015, No. 1 (51), pp. 192–196 (in Russ.).

4. Vasil'ev, A. A., Demin, K. E. *Elektronnye nositeli dannykh kak istochniki polucheniya kriminalisticheski znachimoi informatsii* (Digital data carriers as a source of criminalistically relevant information), Moscow: MGOU, 2009, 198 p. (in Russ.).

5. Kukarnikova, T. E. *Elektronnyi dokument v ugolovnom protsesse i kriminalistike: dis. ... kand. yurid. nauk* (Digital document in the Russian criminal procedure and criminal studies: PhD (Law) thesis), Voronezh, 2003, 25 p. (in Russ.).

6. Treushnikov, M. K. *Sudebnye dokazatel'stva* (Court proofs), Moscow: Gorodets, 1999, 288 p. (in Russ.).

7. Pastukhov, P. S. *Modernizatsiya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva: dis. ... dokt. yurid. nauk* (Modernization of criminal-procedural proving under information society: doctoral (Law) thesis), Moscow, 2015, 64 p. (in Russ.).

8. Zigura, N. A. *Komp'yuternaya informatsiya kak vid dokazatel'stv v ugolovnom protsesse Rossii: dis. ... kand. yurid. nauk* (Computer information as a kind of proving in the Russian criminal procedure: PhD (Law) thesis), Chelyabinsk, 2010, 234 p. (in Russ.).

9. Kachalova, O. V., Tsvetkov, Yu. A. Elektronnoe ugolovnoe delo – instrument modernizatsii ugolovnogo sudoproizvodstva (Digital criminal case as a tool of modernization of criminal court procedure), *Rossiiskoe pravosudie*, 2015, No. 2, pp. 95–101 (in Russ.).

10. Casey, E., Turnbull, B. Digital Evidence on Mobile Devices, *Digital Evidence and Computer Crime,* Third Edition, Academic Press, 2011, 44 p.

11. Sammons, J., Brunty, J. Mobile device forensics: threats, challenges and future trends, *Digital Forensics: Threatscape and Best Practices*, Syngress, 2015, 182 p.

12. Mason, S., George, E. Digital evidence and ‘cloud’ computing, *Computer Law & Security Review*, 2011, No. 27, pp. 524–528.

13. Rodivilin, I. P., Shaevich, A. A. Ob uchastii spetsialista pri iz"yatii elektronnykh nositelei informatsii v khode proizvodstva obyska i vyemki (On participation of a specialists in exemption of digital data carriers during search and seizure), *Kriminalistika: vchera, segodnya, zavtra*, 2013, is. 3–4, Irkutsk: VSI MVD Rossii, pp. 153–157 (in Russ.).

14. Ivanov, A. N. Novyi poryadok iz"yatiya elektronnykh nositelei informatsii pri proizvodstve obyska i vyemki (New order of exemption of digital data carriers during search and seizure), *Problemy ugolovnogo protsessa, kriminalistiki i sudebnoi ekspertizy*, 2012, No. 1, Saratov: Izd-vo Sarat. gos. yur. akad., pp. 25–26 (in Russ.).

15. Starichkov, M. V. Taktika provedeniya obyska, svyazannogo s iz"yatiem nositelei komp'yuternoi informatsii (Tactics of search connected with the extraction of digital information carriers), *Kriminalistika: aktual'nye voprosy teorii i praktiki*: sb. VII Vserossiiskoi nauchno-prakticheskoi konferentsii (Criminal studies: topical issues of theory and practice: collection of works of the 7th All-Russia scientific-practical conference), Rostov n/D: RYuI MVD Rossii, 2010, pp. 167–169 (in Russ.).

16. Larin, E. G. Kopirovanie informatsii s elektronnykh nositelei pri proizvodstve po ugolovnomu delu (Copying information from digital carriers during the criminal procedure), *Zakonodatel'stvo i praktika*, 2012, No. 2 (29), Omsk: Omskaya akademiya MVD Rossii, pp. 52–53 (in Russ.).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

17. Osipenko, A. L., Gaidin, A. I. Pravovoe regulirovanie i takticheskie osobennosti iz"yatiya elektronnykh nositelei informatsii (Legal regulation and tactical features of exemption of digital data carriers), *Vestnik VI MVD Rossii*, 2014, No. 1, pp. 156–163 (in Russ.).

18. Volevodz, A. G. *Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva* (Counteraction to computer crimes: legal bases of international cooperation), Moscow: Yurlitinform, 2002, 496 p. (in Russ.).

19. Krasnova, L. B. *Komp'yuternye ob"ekty v ugolovnom protsesse i kriminalistike: dis. ... kand. yurid. nauk* (Computer objects in criminal procedure and criminal studies: PhD (Law) thesis), Voronezh, 2005, 24 p. (in Russ.).

20. Ovsyannikov, D. V. Elektronnoe kopirovanie informatsii v sisteme sredstv ugolovno-protsessual'nogo dokazyvaniya (Digital copying of information in the system of means of criminal-procedural proving), *Pravoporyadok: istoriya, teoriya, praktika*, 2014, No. 2 (3), pp. 130–135 (in Russ.).

Received 17.10.15
Accepted 11.03.16

Information about the author

Maksim S. Sergeyev, post-graduate student of the Chair of Criminal Procedure and Criminal Studies, Kazan (Volga) Federal University
Address: 18 Kremlyovskaya Str., Room 308a, 420008, Kazan, tel.: +7 (843) 233-71-97
E-mail: sergeev.s.maksim@gmail.com
ORCID: http://orcid.org/0000-0002-8481-0603
Researcher ID: http://www.researcherid.com/rid/L-2219-2015

For citation: Sergeyev M. S. Criteria of proving digital crimes with the use of mobile applications. Features of exemption, *Actual Problems of Economics and Law*, 2016, vol. 10, No. 2, pp. 264–272.