DOI 10.37882/2223–2974.2020.04.06

ЦИФРОВЫЕ СЛЕДЫ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО ПРИ ПОМОЩИ СРЕДСТВ СОТОВОЙ СВЯЗИ

DIGITAL FOOTPRINT IN THE INVESTIGATION OF FRAUD COMMITTED USING CELLULAR COMMUNICATIONS

Ya. Barchenkova

Summary. The article discusses the concept of digital footprint and analyzes the opinion of scientists on this issue. The author outlines the classification of digital traces of fraud committed using cellular communications.

Keywords: digital footprint, fraud, cellular communications, mobile phones, unauthorized access, electronic means, bank cards, identification number.

Барченкова Яна Владимировна
Аспирант, Российская таможенная академия
jocular16@mail.ru

Аннотация. В статье рассматривается понятие цифровой след и анализируется мнение ученых по данному вопросу и предлагается классификация цифровых следов мошенничества, совершенного при помощи средств сотовой связи.

Ключевые слова: следы, цифровые следы, мошенничество, сотовая связь, мобильные телефоны, несанкционированный доступ, электронные средства, банковские карты, идентификационный номер.

В условиях бурного развития мобильной связи происходят постоянные количественные и качественные изменения средств и услуг мобильных телекоммуникаций. Очень активно достижения в области наукоемких технологий используют современные преступники. В настоящее время практически каждое преступление сопровождается использованием преступниками мобильных телефонов. Не является исключением и такая разновидность, как мошенничество. Степень концентрации информации, имеющей важное доказательственное значение для расследования преступлений с похищением информации абонентов, находится в мобильных телефонах преступников и их соучастников, очень высокая. Это объективно предопределяет необходимость широкого использования правоохранительными органами современных достижений научно-технического прогресса в оперативно-розыскной и следственной практике, которые были бы адекватны состояния и характера преступности современности.

Вместе с тем, следственная практика показывает, что для целей раскрытия и расследования преступлений информация, находящаяся в средствах мобильной связи используется крайне мало. Недостаточно научных публикаций, посвященных данной проблеме. Поэтому целью статьи является рассмотрение возможностей использования информации, содержащейся в средствах сотовой связи при расследовании мошенничества, а также следственных действий и оперативно-розыскных мероприятий, направленных на ее получение.

В настоящее время сложно представить жизнь без информационно-компьютерных технологий. Вместе с тем с их использованием совершаются преступления и как любые преступления они оставляют следы, включающие и специфические цифровые следы.

Среди указанных преступлений, особое место занимает мошенничество, совершаемое с использованием компьютерных технологий. Причем способы его совершения значительно опережает методы и особенности расследования данных преступлений.

Значительное количество преступлений совершается путем проведения несанкционированных операций и с использованием платежных карт. Так по данным обзора ФинЦЕРТа, полученных на основе сведений от операторов по переводу денежных средств и операторов услуг платежной инфраструктуры в Банк России, объем всех несанкционированных операций, совершенных с использованием платежных карт в 2018 году составил 1384,7 млн. рублей, что на 44% больше аналогичного показателя за 2017 год (961,3 млн. рублей). Количество таких операций за отчетный период в 2018 году составило 416 933 единицы, что больше на 31,4% аналогичного показателя за 2017 год (317 178). В обзоре отмечается, что большая часть хищений со счетов физических лиц совершается через получение мошенниками несанкционированного прямого доступа к электронным средствам платежа либо побуждение владельцев средств самостоятельно совершить перевод в пользу мошенников

путем обмана или злоупотребления доверием (с использованием методов социальной инженерии) [6].

Проанализировав приговоры, вынесенные районными судами г. Москвы за 2016–2019 гг., мы пришли к выводу, что мошенники приискивают при совершении преступлений недорогие мобильные телефоны, с использованием других устройств для выхода в Интернет или установления специальных программ.

Проведенное исследование показало, что для совершения мошенничества с помощью мобильных телефонов необходимо иметь:

- мобильный телефон, который подключенный к сети сотовой связи (карту можно идентифицировать в зоне влияния определенного сотового оператора мобильной связи);
- наличие расчетных счетов в банковских организациях с привязкой к ним банковских карт и систем дистанционного управления денежными средствами, либо наличие пунктов выдачи денежных средств (личные кабинеты по работе с финансовой информацией клиентов, реестры банковских счетов и банков, кредитные истории клиентов, доступ к информации по операциями с картами клиента и т.п.);
- знание работы сотовой связи и способы шифрования и дешифрования;
- умение осуществлять операции путем коротких текстовых сообщений (например, сообщения с текстами по переводам денежных средств, меню терминалов оплаты и дополнительных услуг, сбоев работы банкоматов и т.п.).

Кроме того, преступник использует заранее подобранные и приготовленные компьютеры, ноутбуки, планшетные компьютеры с доступом в Интернет, с установленными на них специальными программами массовой рассылки SMS-сообщений[1], изменения голоса и т.п.

Большое значение в расследовании указанных преступлений играют цифровые следы. Вместе с тем нет единого определения цифровой след, так Е.Р. Россинская и И.А. Рядовский рассматривают цифровой след как «криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи». Они отмечают такое свойство цифровых следов, как: «невозможность восприятия непосредственно органами чувств, а только с помощью специальных устройств и программ; требование новых, отличных от традиционных, способов, методов и процедур по обнаружению, фиксации и обеспечению сохранности» [7]. По мнению А.И. Семикаленовой, цифровыми следами являются «дампы оперативной памяти и дампы трафиков, файлы и их обрывки, информация, создаваемая программными и аппаратным средствами их получения, служебная об этих файлах, располагающиеся на материальных носителях информации в виде цифровых кодированных последовательностей. Подобная информация доступна восприятию человеком только посредством использования специализированных программных и аппаратных средств, осуществляющих декодирование и визуализацию в привычной графической, текстовой или звуковой форме. Поэтому, ввиду своей подвижности и сложной структуры хранения, подобного рода данные могут быть получены и интерпретированы в полном объеме и без изменения содержания только с использованием специальных знаний» [8].

Проанализировав научную литературу (научные публикации Яджина Н.В., Егорова В.А. [10], Ильиных О.Н. [2], Бутенко О.С. [1]), а также следственную и судебную практику, мы считаем необходимым выделить следующие цифровые следы мошенничества, совершенного с использованием средств сотовой связи:

1. Цифровые следы, связанные с использованием непосредственно мобильного телефона с SIM-картой. Мобильный телефон имеет IMEI-код[2], содержащий 15 цифр. SIM-карта имеет идентификационный номер (IMSI[3]). Нахождение абонентов на территории отдельного региона Российской Федерации с присвоением номеров в пределах одного оператора связи называется — массивом федеральных телефонных номеров. Изменение баланса федерального телефонного номера фиксируется на лицевом счете абонента в компании сотовой связи (пополнение, перевод средств со счета) [10].

Таким образом, возникают специфические цифровые следы. Нами предлагается следующая классификация цифровым следов связанные с использованием мобильного телефона:

1.1. Цифровые следы в технических каналах сотовых сетей:

- соединения между абонентскими терминалами — это голосовая передача (включая данные о не принятых вызовах), SMS-сообщения, сред-

[1] Прим. автора: SMS (от англ. Short Message Service — «служба коротких сообщений») — технология приёма и передачи коротких текстовых сообщений с помощью сотового телефона.

[2] Прим. автора: International Mobile Equipment Identifier — международный идентификатор мобильного оборудования, 15-разрядное число, уникальное для каждого телефона, по которому контролируется работа аппарата в GSM сети. См.: Жуков С. Хакинг мобильных телефонов. М. Бук-пресс, 2006. с. 9.

[3] IMSI — International Mobile Subscriber Identity — международный идентификатор мобильного абонента (индивидуальный номер абонента).

ства информационного обмена, модемы (Интернет-соединения, Wi-Fi соединения и др.);
- сведения об используемом оконечном оборудовании, о серийных номерах терминалов (IMEI), справочная информация об абонентах (номер SIM-карты, номер телефона абонента), сведения о приемопередающем сетевом оборудовании;
- сведения о пространственно-временных данных — расположение базовых станций и периодах соединений (время и продолжительность соединений), также о перемещение абонента в прошлом (подобная информация хранится от 60 дней до 7 лет в зависимости от оператора).

1.2. Цифровые следы на мобильном телефоне с SIM-картой:
- IMEI-код, содержащий 15 цифр, идентификационный номер SIM-карты;
- сведения о телефонных соединениях, отправленных сообщениях;
- данные из прикладных приложений Viber, Skype, WhatsApp, Facebook, Vkontakte и др.;
- сведения об используемых контактах, фотографиях, аудиозаписях, видеозаписях,
- наличие программ по записи и изменению голоса, по изменению (перепрошивки[1]) IMEI-кода телефона, специальное программное обеспечение для проведения банковских операций.

2. Цифровые следы, связанные с использованием банковской карты (банковского счета):
- файл, содержащий сведения о произведенных банковских операциях (транзакции через банкоматы, CNP-транзакции[2] и др.), и хранящийся в банковских учреждениях, в том числе о времени и месте;
- сведения о движении средств на счете в платежной системе;
- сведения о счете держателя банковской карты;
- сведения из электронного журнала терминала или банкомата;
- задокументированные записи изображения с камер терминала или банкомата, хранящиеся на сервере банковских учреждений.

3. Аудиофонограммы — задокументированные записи разговоров между мошенником и потерпевшим.

4. Цифровые следы, связанные с использованием мошенниками компьютеров, ноутбуков, планшетов:
- наличие баз данных с контактами потенциальных потерпевших;
- сведения об используемых контактах, фотографиях, аудиозаписях, видеозаписях;
- наличие программ, позволяющих совершать мошеннические действия при помощи интернет-технологий, в том числе вредоносные программы.

Чтобы выявить такие «цифровые следы» необходимо обратится к экспертизе профессиональных специалистов в следственных органах. В настоящее время развивается новый род инженерно-технических экспертиз — экспертиза телекоммуникационных систем и средств.

К основным вопросам, относящимся к решениям эксперта, относятся:
- какая существует в наличии информация в памяти аппарата мобильной связи (данные о соединении, звуко-видеозаписи, фотоизображения, текстовые сообщения и др.);
- содержание удаленной информации на сменных носителях и SIM-карте.

Экспертное исследование перечисленных объектов позволяет установить обстоятельства преступления: время и продолжительность использования мобильного телефона; содержание сообщений; список абонентов и др.

Рассмотрим способы обнаружения и получения информации с мобильных телефонов и у операторов сотовых систем связи. Прежде всего, необходимо различать данный случай изъятия информации, которая обнаруживается в средствах сотовой связи, от снятия информации с каналов связи как следственного действия.

Во-первых, в рамках снятия информации с каналов связи речь идет лишь о передаче устной речи человека. Несмотря на то, что сведения, передаваемые с помощью, например, SMS, MMS-сообщений, несомненно, могут содержать интересующую следствие информацию, они, однако, не являются объектом этого действия. Мы поддерживаем позицию, что весьма эффективно для целей расследования может использоваться информация о обстоятельства, сопутствующие звонке, имея в виду, в частности, детализацию телефонных переговоров.

Во-вторых, общим для снятия информации с каналов связи в следственной и оперативно-розыскной деятельности является использования технического контроля информации, которая непосредственно передается техническими каналами мобильной связи. Снятие ин-

[1] Прим. автора: IMEI «прошивается» в GSM телефон при его производстве. IMEI GSM телефона можно посмотреть на наклейке под аккумулятором телефона или в самом телефоне, набрав на телефоне #06#. См. Жуков С. Хакинг мобильных телефонов. М. Бук-пресс, 2006. с. 9.

[2] Прим. автора: Транзакция типа «Card Not Present» — операция, осуществленная в сети Интернет с использованием реквизитов платежной карты (без предъявления ее материального носителя)

формации с каналов связи производится в автоматическом режиме непрерывно в течение определенного следователем промежутка времени. В отличие от этого из средств мобильной связи вытягивается уже имеющаяся и хранимая в них информация.

В-третьих, познавательное значение при производстве снятия информации с каналов связи может иметь не только содержание информации, но и ее эмоциональная окраска, фоновая и другая информация, которая может сопровождать язык и быть зафиксирована, например, звукозаписывающими устройствами. Информация, содержащаяся в средствах мобильной связи такого свойства не имеет.

При расследовании мошенничества часто возникает необходимость не столько в получении и исследовании не столько содержания разговоров, передаваемых по сетям мобильной связи, в реальном масштабе времени, сколько в установке и дальнейшему изъятию информации при наличии достаточных оснований полагать, что она имеет существенное значение для установлении обстоятельств преступления.

Исследование информации с мобильных телефонов, SIM-, флеш-карт и той, что содержится в детализации телефонных соединений абонента мобильного телефона, способствует не только установлению обстоятельств, подлежащих доказыванию при мошенничестве, но и решению ряда других криминалистических задач, а именно: построению и выдвижению следственных версий; установлению местонахождения разыскиваемого лица; выявлению дополнительных эпизодов преступной деятельности; розыску финансовых махинаций; преодолению противодействия расследованию; проведению тактических комбинаций и операций; установление соучастников преступной деятельности и установлению их связей; раскрытие преступления «по горячим следам».

ЛИТЕРАТУРА

1. Бутенко О. С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // Lex Russica. М.: МГЮА, 2016. № 4 (113). С. 49–60.
2. Егоров В.А., Ильиных О. Н. Особенности назначения и производства судебных экспертиз по делам о преступлениях, связанных с использованием средств сотовой связи // Концепт. 2014. Спецвыпуск № 29. ART 14837. URL: http://e-koncept.ru/2014/14837.htm.
3. Жуков С. Хакинг мобильных телефонов. М. Бук-пресс, 2006. С. 9.
4. Ковтун Ю.А., Рудов Д. Н. Проблемные аспекты расследования мошенничеств, совершаемых с использованием мобильной связи // Проблемы правоохранительной деятельности. 2013. № 2. С. 61–63.
5. Максимович А. Б. Средства сотовой связи как объект криминалистического исследования: Дис. канд. юрид. наук:12.00.12, Москва: 2018. 238 с.
6. Обзор несанкционированных переводов денежных средств за 2018 год // Департамент информационной безопасности Банка России. URL: https://cbr.ru/Content/Document/File/62930/ gubzi_18.pdf
7. Россинская Е.Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6–8.
8. Семикаленова А. И. Цифровые следы: назначение и производство экспертиз // Вестник университета имени О. Е. Кутафина. 2019. № 5. С. 115–120
9. Семикаленова А.И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 178–185
10. Яджин Н.В., Егоров В. А. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи // Концепт. 2014. Спецвыпуск № 29. ART 14848. URL: http://e-koncept.ru/2014/14848.htm.

Журнал «Современная наука: актуальные проблемы теории и практики»