ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ЗАКРЕПЛЕНИЯ СЛЕДОВ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО ПРИ ПОМОЩИ СРЕДСТВ СОТОВОЙ СВЯЗИ

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

Аннотация. В статье рассматривается особенности собирания следов мошенничества совершенного с использованием средств сотовой связи. Определенное внимание уделяется особенностям собирания следов мошенничества с использованием сотовых телефонов.

Ключевые слова: следы, мошенничество, собирание следов, сотовая связь, мобильные телефоны, электронные средства, электронные носители, следственные действия, микрообъекты.

PECULIARITIES OF UNCOVERING AND DOCUMENTING THE INDICATIONS OF FRAUD COMMITTED WITH THE AID OF CELLULAR

Ya. Barchenkova

Summary. The article discusses the feature of removing electronic media and mobile devices and analyzes the opinion of scientists on this issue. The author outlines the method of fixing traces of fraud committed using cellular communications. The author also focuses on the electronic form of displaying these traces.

Keywords: traces, fraud, the gathering of traces, cellular communications, mobile phones, electronic means, electronic media, investigative actions, micro-objects.

Развитие электронных технологий и телекоммуникационных сетей в современном информационном обществе создал предпосылки для появления принципиально нового вида преступлений — получение незаконной прибыли от использования ресурсов телекоммуникационных сетей, проще говоря, мошенничество или «телекоммуникационное мошенничество», под которым Г.В. Семенов понимает неправомерную деятельность, связанную с несанкционированным пользованием услугами связи [13, с. 100].

По прогнозам отечественных и зарубежных специалистов в XXI в. количество преступлений в области информационно-телекоммуникационных технологий будет неуклонно увеличиваться, поскольку, во-первых — эти деяния приносят колоссальные прибыли; во-вторых — организованные преступные группы стали предоставлять довольно важное значение получению конфиденциальной информации о деятельности государственных и частных коммерческих структур для реализации своих преступных намерений и обеспечения собственной безопасности [6, с. 7].

Такие противоправные действия, как использование информационных ресурсов с корыстной целью влекут значительные убытки государству и операторам связи. Поэтому не случайно вопросу защиты отрасли связи сегодня уделяется особое значение. Ведь преступность в отрасли связи имеет каскадный эффект, влечет за собой недополучение прибылей, перегрузки сетей, недовольство абонентов, нарушения безопасности и др. Так, по данным «Международного союза телекоммуникаций» (ITU), убытки от мобильных преступлений в мировой сотовой индустрии составляют ежегодно порядком $25 млрд. или от 3 до 7% от общей суммы доходов.

Подсчитано, что финансовые убытки от этих преступлений, увеличиваются на 12% ежегодно. Много компаний, как правило, не афишируют свои потери. Тому борьба с мошенничеством, кражами трафика и контроль пропуска трафика по скрытым схемам требует дополнительных материальных затрат и административных мер [10, с. 4].

Из вышеприведенного можно сделать вывод о высокой степени латентности таких деяний, несовершенство законодательства, прежде всего уголовного, отсутствие надлежащих механизмов, сил и средств, которые можно было бы использовать для предотвращения «телеком-

муникационным преступлений», а также для их выявления, расследования и раскрытие [3].

Юридические дефиниции понятия «телекоммуникационное мошенничество», «телекоммуникационный преступление» на сегодняшний день российское законодательство еще не разработало в полной мере, а некоторые его нормы, предусматривающие ответственность за действия, связанные с использованием телекоммуникационного оборудование, далеки от совершенства и не полностью охватывают те действия, которые можно считать уголовно опасными для общественных отношений.

С появлением в 1990-х годах в России средств мобильной связи органы предварительного расследования ежедневно сталкиваются с фактами совершения мошенничества, среди которых существенное место занимает мошенничество, совершенное с использованием средств сотовой связи.

Так в январе–ноябре 2019 года зарегистрировано свыше 260 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий, кражи, мошенничества, грабежи, разбои[1] [14].

В зависимости от уровня подготовки и возможностей, преступников в сфере мобильных коммуникаций разделяют на группы по «специальностям»:

а) фродистеры — злостные неплательщики, которых разделяют на две группы: криминальные элементы и недобросовестные клиенты (первые, имея контракт с компанией, используют поддельные документы, а вторые пользуются настоящими, но платить не желают и попадают в категорию безнадежных должников); четкого предела между ними нет. Ежегодно около 1,5 млн. владельцев мобильных телефонов всеми правдами и неправдами пытаются уклониться от уплаты счетов за пользование. Средний размер ущерба от мошенничества этого типа (по данным зарубежных операторов) оценивается примерно в $600 млн.

б) фрикеры — телефонные пираты, усилия которых сначала сосредоточивались на создании оборудования, обманывающих АТС с целью получения бесплатных звонков (однако технологии развиваются, и в поле зрения фрикеров оказалась мобильная связь, где можно заниматься тем же, с меньшим риском); будучи профессионально подготовленными специалистами, фрикеры представляют серьезную угрозу для будущего сетей мобильной связи. Ведь уже сам факт организации бесплатного роуминга, а также услуг и переконфигурирование форм оплаты и тем более перепрограммирование сетевого оборудования являются опасным для абонентов и операторов связи;

в) хакеры, которые из сети Интернет успешно перешли к мобильной; их главная цель — атаки на сетевые инфраструктуры для проникновения в базы данных операторских компаний. Если раньше для хакеров это было в основном развлечением, то в последнее время, получая большие счета за услуги мобильной связи, они ищут обходные пути, продавая свои услуги;

г) вирусописатели, или вирусологи (virus-maker) еще опаснее чем «интернетовские». Вирусы, созданные ими, способны потенциально разрушить базы данных операторов, уничтожить деньги в мобильных банкоматах и нанести сети другого вреда;

д) кракеры. Это разновидность хакеров, специализирующаяся в сфере программного обеспечения и занимается взломом защиты программного обеспечение телекоммуникаций, кроме того, они разрабатывают программы, проникают в сеть и создают пути доступа к конфиденциальной информации, имеющей большую ликвидность в денежном выражении;

е) кардеры — это те, кто подделывает пластиковые карты и именно сегодня эти преступления считаются одними из самых серьезных в сфере высоких технологий. Их деятельность граничит с хакерской, особенно если нужно взломать карточную базу данных оператора связи. Наиболее уязвимое место в схеме — prepaid-карты, а точнее, спрятан в ней цифровой код. Способов его считывания многие, в частности, это профессиональное удаление защитного слоя на карте с следующим его восстановлением или заменой на новый код, считывание с другого карты (так называемый метод shave & paste — «сбрить и наклеить»).

ж) инсайдеры — это сотрудники передают преступникам информацию о путях проникновения в телекоммуникационную сеть оператора. Иногда они и сами занимаются этим. Утечка информации, или так называемое внутреннее мошенничество, всегда был большой угрозой для безопасности телекоммуникационных сетей. Доля потерь операторов от внутреннего мошенничества превышает 20% общей прибыли. Инсайдеру, как никому другому, известны все «тонкости» работы сети и процедуры добавления новых абонентов.

з) просто воры, поскольку уголовный доступ к сотовой связи с помощью похищенных или утерянных мобильных телефонов получает все большее распространение. В совершении разного рода преступлений похищенные телефоны, оказывается,

[1] Прим. автора — состояние преступности в России за январь-ноябрь 2019. Министерство внутренних дел Российской Федерации ФКУ «Главной информационно-аналитический центр»

играют не последнюю роль. Преступники используют их так же, как угнанные автомобили. Однако похищенный мобильный телефон действует лишь небольшой отрезок времени (пока обладатель не сообщит о похищении), в течение которого воры успевают анонимно совершить преступление или совершить множество дорогих звонков. Рекорд был зафиксирован, когда за один день преступниками с помощью похищенного телефона был нанесен ущерб на сумму около 15 тыс. фунтов стерлингов [12, с. 54].

Одним из разновидностей «телекоммуникационного мошенничества» является несанкционированная маршрутизация входящего международного трафика в телефонную сеть общего пользования.

Серьезным шагом в формировании нормативной базы, регулирующей отношения, связанные с развитием и функционированием мобильной связи в Российской Федерации, стало соответствующее правовое закрепление ответственности за совершение общественно опасных действий уголовного характера. Ведь в итоге быстрого развития отрасли мобильной связи в нашей стране и высоких тарифах на оплату услуг этой отрасли, пользование средствами мобильного связи стало привлекательным объектом для преступной деятельности, в частности, прослушивание переговоров, определение местоположения абонента и его передвижений (характерные для убийств, совершенных на заказ), блокировка соединений, умышленно создаваемыми препятствиями и тому другое [4].

Наиболее ярким примером использования мобильной связи в преступных целях появились действия по доступу и пользованию его ресурсами без их надлежащей оплаты. По данным Ассоциации борьбы с мошенничеством в области связи (CFCA) ежегодные убытки операторов и абонентов от мошеннических действий оцениваются более чем в 12 млрд. долларов. В среднем, потери оператора связи от мошенничества составляют от 3 до 5% от общей суммы прибыли.

Указанная проблема была предметом непосредственного обсуждения на заседаниях Юридической комиссии в Палате представителей и Сенате США. Как отмечалось в одном из докладов, если не принять срочных мер, то затраты на компенсацию ущерба от преступлений в этой области будут расти ежегодно на 40% [1].

Уголовное законодательство многих зарубежных стран содержит специальные нормы и нормативно правовые акты, предусматривающие уголовную ответственность за неправомерный доступ к сферам мобильной связи и пользование их ресурсами (Великобритания: Закон «О телекоммуникациях» Telecommunication Act) 1984 г., Закон «О мошенничестве в телекоммуникациях» (Telecommunication (Fraud) Act) 1997 г.; Закон Венгрии «О защите информации о лице и использовании информации, имеющей общественный интерес», 1992 г.; Нидерланды: ст. 138a, 55 Уголовного кодекса Нидерландов; Италия: ст. 615-ter Уголовного кодекса Италии; Испания: статья 248.2 Уголовного кодекса Испании и тому прочее.) [5, С. 5–9; 16, 7; 8].

Защита информации (предотвращение свободного доступа к информации, устранение технических каналов ее утечки и т.п.) В ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях и сетях электросвязи обеспечивается комплексом организационных, программных и технических мероприятий. Преодоление защиты может проявляться во взломе паролей, кодов доступа и тому подобное. Способ преодоления указанных мер безопасности не будет значение для квалификации, конечно, если же оно не будет содержать признаков другого состава преступления (например, уничтожение программных или технических средств) [11].

Если лицо имеет право доступа к информации, которая обрабатывается в ЭВМ, автоматизированных системах, компьютерных сетях или сетях электросвязи, то ее действия квалифицируются по УК РФ «Несанкционированные действия с информацией, которая обрабатывается в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к нему» в другой статье УК РФ «Нарушение, правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или правил защиты информации, которая в них обрабатывается» [15].

Субъективная сторона преступления характеризуется умышленной формой вины.

Преступные действия при преодолении программного и технической защиты для получения несанкционированного доступа могут быть совершены только с прямым умыслом.

Человек, способный вмешаться в работу ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи имеет соответствующие знания, умения и навыки. Бесспорно, преступник осознает социальную опасность несанкционированного вмешательства, его противоправность; предусматривает последствия в виде утечки, потери, подделки, блокировка информации, искажение процесса обработки информации или нарушение установленного порядка ее маршрутизации; желает или сознательно допускает

наступления этих последствий, относится к их наступлению безразлично. Мотив преимущественно корыстный, или возможны — месть, хулиганство, подрыв репутации, сокрытие другого преступления и т.п. [9, С. 156].

Итак, термин «преступления, связанные с вмешательством в работу сетей мобильной связи» можно рассматривать как преступную деятельность, в которую включаются не только уголовные действия по пользованию ресурсами (услугами) системы мобильной связи, а и уголовные действия по доступу к данной системы, предусмотренные самостоятельными составами УК РФ.

Как и любые рассматриваемые деяния, данные преступления оставляют следы. Как правило, они отображаются в электронной форме. Для их собирания необходимы специальные познания и навыки, а также специализированное оборудование. В этой связи для обнаружения, фиксации и изъятия указанных следов, следует привлекать специалистов. Практика показывает, что они помогут установить:

- следы на электронных носителях, содержащих сведения о соединениях между абонентами, о произведенных финансовых операциях, системе сотовой связи и иных обстоятельствах, хранящихся у сотовых операторов либо на компьютерах;
- следы на мобильных устройствах в виде информации о проведенных финансовых операциях, реальном ущербе от совершенного преступления, местах обналичивания денежных средств, круге лиц, причастных к совершению преступления и т.д.

Кроме того указанные следы способствуют установить местонахождение преступников, лиц с которыми они контактировали включая и потерпевших от их действий, а также расшить круг свидетелей и определить IMEI-номера используемых телефонных аппаратов;

- следы на мобильном устройстве, содержащих сведения об абонентской книге телефона, соединениях абонентов сетей сотовой связи (журнал звонков, сообщения формата SMS[1], MMS[2]), произведенных финансовых операциях, системе сотовой связи, специальных программных средств для «прошивки» мобильных телефонов, SIM-карт, из имеющихся на устройстве приложений, таких как Viber, Skype, WhatsApp, Facebook, Telegram, Vkontakte, Одноклассники и т.д. Они могут содержать данные о пользователях мобильных телефонов, используемых телефонных номеров, фотографиях и видеозаписях, а также следы пальцев рук, микрообъекты;
- следы на SIM-карте[3], содержащих сведения в виде абонентской книги, журнал звонков, текстовые сообщения. Наличие указанной информации, способствует установлению членов преступной группы, определению круга потерпевших и свидетелей, установлению временных промежутков совершенных преступлений.

При производстве следственных действий, связанных с изъятием средств сотовой связи и электронных носителей, следует соблюдать следующие правила:

- по прибытию следственно-оперативной группы на место производства следственных действий, принять меры к обеспечению сохранности информации, содержащейся на мобильных устройствах, компьютерах, электронных носителях и т.д.;
- запретить присутствующим лицам прикасаться к работающим устройствам;
- исключить возможное влияние на подлежащие изъятию устройства, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов;
- при транспортировке в иное помещение не производить какие-либо манипуляции с устройствами, если результат заранее не известен;
- у владельца изымаемого устройства выяснить пароли;
- произвести копирование информации, содержащейся на электронном носителе информации в соответствии с нормами ч. 3 ст. 164. 1 УПК РФ [15];
- зафиксировать обнаруженные мобильные телефоны и электронные носители, включая их конфигурацию;
- упаковать мобильный телефон и иные электронные носители, с тем, чтобы их можно было использовать при производстве экспертизы.

Таким образом, выделяя отдельные виды мобильного мошенничества как преступления, а также зная порядок выявления и раскрытия деяния, можно разработать ряд упреждающих мероприятий для повышения эффективности расследований по делам, связанным с преступлениями с использованием мобильных средств связи и прочих коммуникационных технологий.

[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: MMS — (от англ. Multimedia Messaging Service — «Служба мультимедийных сообщений» — система передачи мультимедийных сообщений (изображений, мелодий, видео) в сетях сотовой связи.

[3] Прим. автора: SIM-карта (англ. Subscriber Identification Module — модуль идентификации абонента) — идентификационный модуль абонента, применяемый в мобильной связи.

ЛИТЕРАТУРА

1. Jos Dumortier, Mark Hyland, Diana Alonso Blas. Legal aspects of fraud detection.— Leuven, 2014.— P. 5–9.
2. Архипова Н.А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений: Сб. мат-лов криминалист. чтений. Барнаул: Барнаульский юрид. институт МВД России, 2014. № 10.
3. Борьба с телефонным пиратством: [методы, схемы, рекомендации] / И. Н. Балахничев, А. В. Дрык, А. И. Крупа.— Минск, 2018. 322 с.
4. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.
5. Европейское законодательство по телекоммуникациям: [аналитический материал; сравнительный анализ]. Спб., 2019. 225 с.
6. 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.
7. Закон Великобритании «О телекоммуникациях» (Telecommunication Act) и «О защите данных» от 12.07.84. URL: http:// www.pdp.org.ua/index. php?option= com_content& view= article& id= 887: 212–3- visnyk-& catid= 44:— i& Itemid= 120.
8. Закон Венгрии «О защите информации о лице и доступе к информации, представляющей общественный интерес» от 06.11.1992. URL: http://www.pdp.org.ua/index.php?option=com_content&view=article&id=887:212–3-visnyk-&catid=44:—i&Itemid=118.
9. Иванов П. Досье на телефонного мошенника // Сети. 2010. № 12. С. 52–61.
10. Ковтун Ю.А., Рудов Д. Н. Проблемные аспекты расследования мошенничеств, совершаемых с использованием мобильной связи // Проблемы правоохранительной деятельности. 2013. № 2. С. 61–63.
11. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N195-ФЗ (ред. от 01.03.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_34661.
12. Максимович А. Б. Средства сотовой связи как объект криминалистического исследования: Дис. канд. юрид. наук:12.00.12, Москва: 2018. 238 с.
13. Семенов Г. В. Расследование преступлений в сфере мобильных телекоммуникаций: Автореф. дис. канд. юрид. наук. Воронеж, 2003. 17 с.
14. Состояние преступности в России за январь-ноябрь 2019. Министерство внутренних дел Российской Федерации ФКУ «Главной информационно-аналитический центр».
15. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N174-ФЗ (ред. от 04.11.2019) СПС «КонсультантПлюс», 2020.
16. 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»

Российская таможенная академия