ВАДИМ ВИКТОРОВИЧ СУЩИК,
старший оперуполномоченный 37 отдела
Управления «К» БСТМ МВД России

СОВЕРШЕНСТВОВАНИЕ АДМИНИСТРАТИВНО-ПРАВОВЫХ МЕР ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ В ОБЛАСТИ СВЯЗИ

Представлен авторский подход к совершенствованию административно-правовых мер противодействия правонарушениям в области связи. С учетом вновь возникающих административных деликтов в области связи предложены дополнения в Кодекс Российской Федерации об административных правонарушениях.

Ключевые слова: Интернет, мобильная связь, телекоммуникации, административно-правовое регулирование, клонирование SIM-карты, модификация IMEI-кода, компьютерная информация, сотовый «фрод».

V. V. Sushchik, Senior Police Operative, Department «K», Russia MI Bureau of Special Technical Actions; **e-mail: ncp-ruc@mvd.ru, tel.: 8 (495) 623-49-82.**

Improving administrative and legal means for combating offences in the sphere of communication.

An author's approach to improving administrative and legal means of combating offences in the sphere of communication is presented. In view of new administrative torts in the sphere of communication, supplements to the Russian Federation Administrative Offences Code are suggested.

Key words: Internet, mobile communication, telecommunication, administrative and legal regulation, cloning SIM-card, IMEI-code modification, computer data, cell «fraud».

Исследование различных аспектов противоправной деятельности, связанной с совершением правонарушений в сфере информационных технологий, показывает, что защита от противоправных действий, объектами которых являются средства вычислительной техники и средства связи, а также информация, содержащаяся в них, есть сложный и многогранный процесс, организация которого определяется множеством факторов, формирующих специфику данной деятельности.

Одним из таких факторов выступает проблематика установления справедливой ответственности за правонарушения в области связи. В настоящее время нельзя однозначно утверждать, что среди ученых, законодателей и правоприменителей выработан однозначный подход к данному вопросу. Это обусловлено непродолжительным периодом существования исследуемых правоотношений и неспособностью юридической науки и практики к быстрому осмыслению происходящих процессов и реагированию на технологический прогресс, способствующий окончательному становлению информационного общества. Как справедливо отмечает Е. Смыслина, «...юрисдикционые органы оказались в довольно сложном положении: возникла совершенно новая система общественных отношений, связанная с совершенно новыми технологиями, и чтобы применить к ним нормы существующего законодательства, нужно как минимум понимать сущность и содержание этих отношений»[1].

С середины 90-х годов прошлого века на рынке оказания услуг связи отмечен рост числа правонарушений, связанных с неправомерным использованием возрастающих возможностей сотовой связи. Этот вид преступлений стал настолько распространен, что получил собственное название - «фрод»[2]. Это - мошенничество с контрактами и счетами за услуги сотовой связи, хищения и клонирование сотовых телефонов, а также изощренные способы обмана сотовых компаний[3]. Иными словами, под «фродом» подразумевается вся совокупность фактов незаконного использования ресурсов сотовой связи.

В то же время следует иметь в виду, что «... эти понятия заимствованы из зарубежного законодательства, а понятие „мошенничество" традиционно используется в нашей стране для обозначения несколько иного преступления»[4].

Вместе с тем, с развитием технологий правонарушения в области связи не ограничились только лишь сотовым или мобильным «фродом». Сюда также с уверенностью можно отнести следующие противоправные действия:

незаконное оказание телематических услуг;

незаконный доступ к ресурсам проводной связи;

незаконный доступ к услугам кабельного телевидения;

копирование информации SIM-карт мобильных телефонов;

правонарушения в сфере платежей за телематические услуги;

заключение договоров на оказание телематических услуг по подложным документам и иные.

Таким образом, с течением времени правонарушения в области связи на порядок увеличились и стали более разнообразными.

Ущерб, причиняемый операторам связи только от сотового «фрода», в мировых масштабах, по некоторым данным, доходит до 13,6% от общего числа доходов[5]. Следует согласиться с А. Борейко, что «...прибыль от этого вида мошенничества не меньше, чем в наркоторговле, а риск значительно ниже, поскольку во многих странах законодательство не содержит адекватных мер по борьбе с ним»[6]. Действительно, все правонарушения в области связи, в том числе сотовой, а также в телекоммуникационных сетях квалифицируются, как правило, семью статьями Уголовного кодекса Российской Федерации, а именно: ст. 159 (мошенничество), ст. 160 (присвоение или растрата), ст. 165 (причинение имущественного ущерба без признаков хищения), ст. 171 (незаконное предпринимательство), ст. 272 (неправомерный доступ к компьютерной информации) и ст. 273 (создание, использование и распространение вредоносных компьютерных программ)[7].

Основными причинами, снижающими эффективность противодействия правонарушениям в области связи и телекоммуникаций, можно назвать следующие:

многообразие видов противоправных действий, постоянное появление новых форм и способов их совершения;

несовершенство законодательной базы, в которой нет единой трактовки совершаемых деяний, в связи с чем однотипные правонарушения квалифицируются по разным статьям Уголовного кодекса Российской Федерации;

отсутствие у сотрудников следственных органов достаточного опыта в расследовании уголовных дел, возбужденных по фактам совершения преступлений в области связи и телекоммуникаций. Это обстоятельство выражается прежде всего в том, что для возбуждения уголовного дела в разных субъектах Российской Федерации требуется разный объем материалов, которые содержат достаточные данные, свидетельствующие о наличии признаков состава преступления.

В связи с этим необходимо обратить внимание на основания привлечения за отдельные правонарушения в области связи и телекоммуникаций виновных лиц к административной ответственности. В пользу административного наказания выступают оперативность его осуществления и отсутствие трудоемких оперативно-розыскных и следственных действий при раскрытии и расследовании уголовно наказуемого деяния.

Несмотря на наличие в главе 13 Кодекса Российской Федерации об административных правонарушениях[8] 28 составов административных правонарушений, ни одно из них не устанавливает ответственности за противоправные действия в области связи и телекоммуникаций. Между тем анализ законодательства Российской Федерации в указанной сфере позволяет сделать вывод о наличии оснований для привлечения к административной ответственности за некоторые из них.

Проанализируем такие противоправные действия.

Оказывая своим абонентам услуги подвижной связи, управляющие центры системы сотовой телефонной связи оператора постоянно отслеживают местонахождение абонента для организации сеанса связи в случае вызова этого абонента. Мобильный телефон периодически отсылает регистрационный сигнал на базовую станцию той местности, в которой он находится. В свою очередь полученный сигнал транслируется в управляющий центр системы. Таким образом, принцип определения местоположения абонента заложен в алгоритм работы сотовой телефонной сети. Относительно недавно ведущие операторы связи стали предлагать своим абонентам данную возможность в качестве одной из услуг. Обнаружить местоположение абонента можно только с его согласия посредством разрешения на контроль местоположения. Одновременно с этим в случае, если злоумышленнику телефонный аппарат станет доступным хотя бы на короткий промежуток времени, он может осуществить регистрацию двух аппаратов сотовой связи без ведома контролируемого абонента. Несмотря на то, что оператор связи должен гарантировать каждому абоненту возможность запрета определения своего местоположения в любой момент, абонент также вправе знать свое проверяемое положение. Однако функция запроса своего контролируемого состояния не всегда может быть предусмотрена, поэтому в случае оказания оператором сотовой связи услуги дистанционного предоставления информации о местонахождении абонента необходимо обязать оператора предоставлять контролируемому абоненту возможность получения сведений о произведенных в его отношении запросах и под-

ключенных сервисах. В случае непредоставления указанных сведений оператора сотовой связи следует привлекать к административной ответственности за нарушение тайны личной жизни абонента.

В соответствии с ч. 2 ст. 62 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[9] пользователь услугами связи имеет право на получение необходимой информации об услугах связи. Непредоставление полной и необходимой информации абоненту оператором связи о возможных негативных последствиях при оказании услуг может повлечь за собой, в частности, необеспечение защиты конфиденциальности данных о нем. Так, например, ряд современных моделей телефонов, оснащенных передатчиком «Bluetooth», позволяют злоумышленникам скрытно получить доступ к телефону и выполнить с ним произвольные действия. Проблема состоит в том, что для некоторых телефонов «Bluetooth»-гарнитура не должна проходить авторизацию, для того чтобы воспользоваться телефоном. Производители гарнитур стремятся снизить стоимость устройств за счет отсутствия аппаратной реализации данной процедуры. Производители же мобильных телефонов, зная об этом, упраздняют механизм проверки для обеспечения совместимости с большим количеством гарнитур. Обычно поиск гарнитуры инициируется самим мобильным телефоном, так как гарнитура для снижения стоимости не снабжается функционалом, позволяющим осуществлять поиск устройств. Это означает, что гарнитура сама не может найти мобильный телефон и не может определить, по какому «Bluetoothw-каналу взаимодействовать с ним. По этой причине разработчики телефонов пренебрегают функциями авторизации.

В связи с этим на ряде мобильных телефонов существуют открытые порты «Bluetooth», по которым можно обратиться к телефону, имитируя поведение беспроводной гарнитуры. Для уязвимых телефонов номер профиля беспроводной гарнитуры точно известен. При этом подключенная к телефону гарнитура обладает правами ROOT. Злоумышленник, подключившись к телефону, может получить доступ к любым данным, включая SMS-сообщения и данные контактов. Он может как беспрепятственно скопировать эти данные, так и записать в память телефона компрометирующие данные[10].

Помимо незаконного доступа к данным, имеющимся на телефонном аппарате, абонент также может стать объектом «заражения» сотового устройства вредоносным программным обеспечением при использовании услуги доступа к сети Интернет. Кроме того, сведения, характеризующие личность абонента или его активность в сети Интернет, могут стать достоянием посторонних лиц с помощью файла «cookies». В «cookies» могут быть сохранены данные, которые пользователь оставил о себе в сети Интернет (логин, пароль, Ф.И.О., e-mail, почтовые настройки). Даже если пользователь в сети Интернет при просмотре электронного ресурса не оставляет «следов» о себе, в распоряжении сервера остается информация об IP-адресе посетителя, с помощью которого можно определить узел связи, который используется для доступа к сети Интернет

Таким образом, в целях защиты абонентов от претерпевания неблагоприятных последствий при предоставлении им услуг связи необходимо внесение изменений в ФЗ «О связи» в части, предусматривающей при заключении договора об оказании услуг связи со стороны оператора связи предоставление исчерпывающих гарантий обеспечения конфиденциальности хранящейся в телефонном аппарате охраняемой законом информации. Неисполнение указанной обязанности должно караться привлечением соответствующего оператора связи к административной ответственности.

Также, на взгляд автора, заслуживает внимания с точки зрения установления административной ответственности такое противоправное деяние, как блокирование канала связи абонента, что стало возможным с появлением автоматических систем связи и программируемых аппаратов связи. Поставив на автодозвон телефонные номера «нужных» абонентов, злоумышленник надежно лишает его коммутационного канала. В случае, когда основой бизнеса являются информационные услуги, дискредитация коммутационного канала даже в течение непродолжительного времени может поставить крест на бизнесе субъекта.

Сложность рассматриваемой ситуации заключается в том, что определить внешнее блокирование может только оператор связи, в биллинговой системе которого зафиксированы все попытки доступа к номеру абонента[11].

Стоит отметить, что наличие административной санкции в этой ситуации будет эффективным, если причиненный имущественный ущерб не достигнет предела, при наступлении которого виновное лицо должно привлекаться к уголовной ответственности, а также в случае отсутствия признаков уголовно наказуемого деяния в целом.

Особое значение для сетей сотовой связи имеет вопрос, связанный со сменой IMEI-кодов телефонных аппаратов и созданием дубликата (клона) SIM-карты. Относительно клонирования SIM-карт в большинстве случаев возбуждаются уголовные дела по ст. 272 или ст. 165 УК РФ[12].

С вопросом о привлечении к юридической ответственности за изменение IMEI-кодов не все так однозначно.

Не существует двух легальных телефонов с одинаковыми IMEI-кодами. Фиксация IMEI-кода в базе данных оператора сотовой связи позволяет последнему контролировать оконечную аппаратуру пользователя - модель телефонного аппарата, легальность его приобретения, миграцию аппаратов между абонентами.

Изменение идентификатора является неправомерным и должно вызывать соответствующие санкции, однако и в административном, и в уголовном законодательстве конкретная норма, которая бы устанавливала ответственность за указанное действие, отсутствует, что ведет к сложностям правоприменения в данной сфере. Известно, что на практике за изменение IMEI-кода возбуждались уголовные дела по ст. 272 или ст. 273 УК РФ[13]. В то же время в проекте федерального закона от 11 апреля 2005 г. № 159989-4, предусматривавшего внесение изменений в отдельные законодательные акты, Уголовный кодекс Российской Федерации предлагалось дополнить ст. 181.1, в которой устанавливалась бы ответственность за несанкционированное изменение международного идентификатора мобильного телефона, установленного его производителем, а равно его подделку, совершенные из корыстной или иной личной заинтересованности. Верховный Суд Российской Федерации в официальном отзыве от 7 июля 2005 г. № 1088-5/общ. не поддержал данный законопроект, мотивируя это тем, что «Общая часть Уголовного кодекса Российской Федерации позволяет решить вопрос об ответственности лиц, которые помогают сбывать краденые сотовые телефоны, в том числе путем изменения или подделки международного идентификатора мобильного телефона».

Известные случаи квалификации изменения IMEI-кода на практике небесспорны. Применение ст. 272 УК РФ возможно при условии непосредственного отнесения IMEI-кода к охраняемой законом компьютерной информации, т.е. данным, представленным в форме электрических сигналов, доступ к которым ограничен федеральным законом. Международный идентификатор мобильного оборудования представляет собой уникальный серийный номер каждого телефона GSM, состоящий из 15 цифр. Он указан на коробке с телефоном под штрих-кодом и на корпусе телефона под аккумулятором. Сверить его можно, набрав на клавиатуре комбинацию клавиш *#06#. Пятнадцать цифр номера IMEI означают сочетание [TAC] [FAC] [SNR] [SP], где TAC (Type Approval code) - 6 цифр - код конкретной модели телефона, FAC (Final Assembly Code) - 2 цифры - код страны-производителя сотового телефона, SNR (Serial number) - 6 цифр - серийный номер телефона, SP (Spare), последняя цифра - запасной идентификатор, вычисляемый по специальному алгоритму на основе предыдущих цифр. Таким образом, весьма неочевидным представляется отнесение IMEI-кода к охраняемой законом компьютерной информации.

Более реалистичным выглядит вариант привлечения к ответственности за модификацию IMEI-кода по ст. 273 УК РФ. При изменении IMEI перепрограммируемая память, в которой он прописан, выступает в качестве носителя информации, а сам IMEI может рассматриваться в качестве компьютерной информации, но при условии, что под компьютерной будет подразумеваться информация в форме, доступной для восприятия ЭВМ, или передающаяся по каналам связи[14], так как в настоящее время отсутствует дефиниция «информация, предоставленная в форме электрических сигналов». На данный факт указывало правовое управление Государственной Думы ФС РФ в отзыве на законопроект «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[15].

Альтернативная возможность решения проблемы заключается в применении ст. 13.6 КоАП РФ («Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи»). Данное решение вытекает из ч. 2, 3 ст. 41 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» - «Подтверждение соответствия средств связи и услуг связи» - в которых установлена обязательная сертификация радиоэлектронных средств связи. Из нормы ст. 25 ФЗ «О техническом регулировании», устанавливающей, что «сертификат соответствия включает в себя информацию об объекте сертификации, позволяющую идентифицировать этот объект», следует обязательное наличие собственного сертификата для каждого сотового телефонного аппарата. Идентификатором каждого аппарата, по которому производится сертификация изделия, является IMEI[16].

Представляется, что только законодательное установление дефиниции «изменение (модификация) IMEI» позволит ответить на возникающие вопросы в процессе квалификации деяния, связанного с использованием сотового телефонного аппарата с измененным (поддельным) IMEI-кодом. На взгляд автора, установление административной санкции выглядит предпочтительнее в свете ранее неудачных попыток закрепления уголовной ответственности.

В заключение необходимо отметить, что с развитием информационных технологий не стоит на месте развитие связи и телекоммуникаций. К сожалению, часто результаты этого развития направлены в русло корыстного обогащения и не всегда могут трактоваться как действия, совершаемые в рамках правового поля.

Возрастающее число разнообразных деяний, направленных на неправомерное получение охраняемой законом информации, извлечение доходов от различных манипуляций с устройствами сотовой связи, а также совершение иных противоправных действий в области связи и телекоммуникаций заставляют правоохранительные органы не только адекватно реагировать на них путем привлечения к ответственности за совершение деяния, содержащего признаки преступления или административного правонарушения, но и проявлять изобретательство в случае, если за совершенное противоправное действие законодатель не установил ни административной, ни уголовной ответственности. Однако попытки «подбора» существующих статей, особенно уголовных, на взгляд автора, не должны иметь места. Совершается ряд противоправных действий, объективно требующих привлечения к административной ответственности даже при отсутствии признаков общественной опасности. Одним из таких примеров может быть модификация IMEI-кода.

В то же время нельзя признать удачной главу 13 КоАП РФ. Ни одной, по мнению автора, актуальной статьи, предусматривающей административную ответственность за правонарушение в области связи и информации, хотя потерпевшим здесь потенциально может стать каждый второй обладатель смартфона, коммуникатора или просто телефонного аппарата, который может хранить, обрабатывать и передавать компьютерную информацию, в этом Кодексе не содержится. Однако, как отмечено, в пользу применения административного наказания выступает оперативность его осуществления и отсутствие трудоемких оперативно-розыскных и следственных действий при раскрытии и расследовании уголовно наказуемого деяния.

Таким образом, представляется наиболее оптимальным вариант развития событий, при котором за противоправные деяния в области связи необходимо установление административной санкции.

[1] Смыслина Е. Борьба с пиратской вольницей в мировой паутине // Российская юстиция. 2001. № 6. С. 62.

[2] Трофимов Ю.И. Правовая охрана баз данных операторов электросвязи: Дис. ... канд. юрид. наук. - Омск, 2008.

[3] Там же.

[4] Семенов Г.В., Бирюков П.Н Ответственность за мошенничество в сетях сотовой связи: Учеб. пособие. - Воронеж: Воронежский гос. ун-т, 2002. С. 41.

[5] URL: http://www.lawcabinet.ru/news/497.html

[6] Борейко А. Многоликий фрод // Ведомости. 2002. 29 марта.

[7] Материалы совещания-семинара экспертов внутренних дел (полиции) государств - участников СНГ по борьбе с преступлениями в сфере информационных технологий. - Домодедово: ВИПК МВД России, 2007. С. 60.

[8] Собрание законодательства РФ. 2002. № 1 (ч. 1) Ст 1.

[9] Собрание законодательства РФ. 2003. № 28. Ст. 2895.

[10] Жуков И.Ю., Михайлов Д.М. Исследование уязвимостей «Bluetooth» - передатчика мобильных телефонов // Право и безопасность: Журнал. 2010. № 56.

[12] Собрание законодательства РФ. 1996. № 25. Ст. 2954

[13] Материалы совещания-семинара экспертов внутренних дел (полиции) государств - участников СНГ по борьбе с преступлениями в сфере информационных технологий. - Домодедово: ВИПК МВД России, 2007. С. 63.

[14] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Бюллетень международных договоров. 2009. № 6. Июнь.

[15] Федеральный закон от 7 декабря 2011 г. № 420-ФЗ -О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 2011. № 278. 9 дек.

[16] Трофимов Ю.И. Указ. соч.