*Д. В. Соколов*

# ПОНЯТИЕ «МОШЕННИЧЕСТВО». СОТРУДНИЧЕСТВО РОССИЙСКИХ ОПЕРАТОРОВ СВЯЗИ В СФЕРЕ БОРЬБЫ СО ЗЛОУМЫШЛЕННИКАМИ

В отечественных и зарубежных изданиях и публикациях, названиях международных организаций и специализированного софта по борьбе с преступниками в сетях операторов связи всесторонне используется термин «мошенничество» («fraud») для обозначения действий в сетях операторов связи, которые направлены на получение прибыли злоумышленниками. Но ни в России, ни за ее пределами нет единой точки зрения, что же такое мошенничество в телекоммуникационной среде, что приводит к затруднениям при общении специалистов по противодействию злоупотреблениям в сети, адаптации международных стандартов в российских телекоммуникационных компаниях, наказании злоумышленников за противоправные действия.

Злоупотребления в сетях связи (мошенничество) имеют следующие последствия:

- снижение доходов компании;
- снижение лояльности абонентов;
- отрицательное влияние на имидж компании;
- снижение лояльности акционеров, инвесторов;
- снижение финансовой устойчивости бизнеса.

В России юридически значимое определение мошенничества дано в статье 159 Уголовного кодекса Российской Федерации: «мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» [1].

Упрощенно «мошенничество» можно определить как «неправомочную деятельность, которая позволяет абонентам-нарушителям получать услуги связи бесплатно» [2]. Но под данное определение не подпадает большой круг потенциальных злоумышленников, которые также наносят ущерб операторам связи, например посредники или другие операторы связи. Да и целью может быть не бесплатное получение услуги, а другие финансовые интересы.

Поэтому для определения мошенничества больше подходит следующее: «Мошенничество — это неправомочная деятельность юридических и физических лиц, наносящая ущерб мобильной связи» [2]. Но и это определение не отражает всей полноты понятия, так как нацелено только на операторов сотовой связи. В общем случае: мошенничество — это неправомочная деятельность юридических и физических лиц, наносящая ущерб операторам связи. В этом определении расширен круг лиц, но под него подпадают и обычные хулиганы-вандалы. Значит, и оно все-таки неадекватно отражает понятие «мошенник».

Компания МТС определяет мошенничество как «умышленную деятельность лиц на сетях связи, в т. ч. мошенническую, по неправомерному получению услуг и использованию ресурсов оператора связи, без надлежащей их оплаты, неправомерному доступу к служебной информации оператора, в том числе с целью извлечения дохода, а также иные действия, направленные на причинение убытков или иного вреда оператору». Также, согласно МТС, «мошенник — физическое или юридическое лицо, получившее несанкционированный доступ к услугам связи, а также пользующийся услугами в режиме неправомерного доступа, в том числе с целью извлечения дохода, являющееся абонентом, сотрудником, партнером оператора или третьим лицом, действия которого направлены на причинение убытков или иного вреда оператору связи», а мошенническая атака — «массовые действия фродстеров (злоумышленников) в течение непродолжительного времени (всплеск активности), направленные на получение существенной материальной выгоды, причинение убытков или иного вреда оператору связи. Например: генерация фродстером (злоумышленником) контент-трафика в роуминге в

течение 1–2 суток с использованием аппаратно-программного обеспечения и большого количества (более 100) SIM-карт на фиктивных контрактах в целях получения бонуса. Оператор в этом случае несет существенные материальные потери в виде невозвратной дебиторской задолженности». В этом определении также имеется слабое место: «в течение непродолжительного времени», тогда как известно немало видов злоупотреблений, которые происходят в течение длительного времени (например, физическое подключение к телефонной линии абонента).

В зарубежных источниках также можно найти попытки дать определение мошенничеству в сетях операторов связи. За границей, с точки зрения промышленности, этот термин обычно используется для описания воровства, обмана или преднамеренного неправильного использования услуг связи, предлагаемых операторами связи. Американский научно-исследовательский институт прокуроров (American Prosecutors Research Institute) определяет этот тип нарушения как использование телекоммуникационного оборудования для преднамеренного обмана или преступного управления человеком в целях получения финансовой выгоды.

Томас Суоцци (Thomas R. Suozzi) и Джеймс Лоренс (James H. Lawrence) в статье «Телекоммуникационное мошенничество» пишут: «Телекоммуникационное мошенничество — воровство телекоммуникационных сервисов (телефонов, сотовых телефонов, компьютеров и т. д.) или использование телекоммуникационных сервисов для реализации других форм мошенничества. Жертвами выступают потребители, фирмы и сервис-провайдеры».

Более подробный анализ нормативно-правовых документов зарубежных стран по вопросам мошенничества в области телекоммуникаций и правовой ответственности за НСД можно посмотреть в отчете о НИР [3]. В нем приведены определения, имеющие юридически значимую силу, предназначенные для преследования злоумышленников с целью наказания и возмещения ущерба.

Из вышесказанного видно, что четного понимания, что такое мошенничество, ни в России, ни за ее пределами нет. На данный момент у каждой страны и организации есть свое понимание мошенничества в телекоммуникационной среде. Первым этапом в стандартизации борьбы с злоупотреблениями в сетях операторов связи должно стать однозначное определение понятия «мошенничество» на международном уровне. Но стоит иметь в виду, что в области обеспечения защиты информации нет понятия «мошенничество». Оно взято из обыденной жизни и юридических документов. Технические специалисты используют понятие «угроза» информации. Для юридической и организационной защиты информации определение «мошенничество» допустимо, но для технической защиты необходимо использовать понятие «угроза».

Существуют несколько организаций, в число задач которых входит изучение проблем несанкционированного доступа в сетях операторов связи. Одной из этих организаций является «Ассоциация документальной электросвязи».

В российском общественно-государственном объединении «Ассоциация документальной электросвязи» (АДЭ) (образована в 2000 г.) представлено более ста компаний из десяти городов России. Среди самых известных и наиболее весомых операторов связи можно выделить ВГТРК, «ВымпелКом», «Компания ТрансТелеКом», МГТС, «Ростелеком», РТКомм.РУ, «Связьинвест», Центральный телеграф, «ЦентрТелеком», «Газпром космические системы». Также в списках членов организации есть государственные органы: МВД России, Минкомсвязь России, Минфин России, ФСО России, ФТС России, ФСБ России, ФСКН России, ФСТЭК России.

Задачей ассоциации является реализация потребностей граждан, бизнеса и органов государственной власти в инфокоммуникационных технологиях и технологиях информационной безопасности. Это объединение является правопреемником общественного объединения «Ассоциация документальной электросвязи», созданного 30 августа 1994 г. по инициативе Минсвязи России.

В 2005 г. по решению исполкома АДЭ был создан Координационный совет по информационной безопасности инфокоммуникационных сетей и систем. Цель создания — формирование единой, совместимой и защищенной информационно-телекоммуникационной инфраструктуры Российской Федерации, координация деятельности организаций и предприятий по созданию систем обеспечения сетевой и информационной безопасности.

Основные направления деятельности Координационного совета:

- участие в разработке проектов нормативных правовых актов в области сетевой и информационной безопасности, экспертиза этих актов;
- содействие совершенствованию правоприменительной практики в сфере обеспечения сетевой и информационной безопасности;
- разработка практических рекомендаций по обеспечению сетевой и информационной безопасности;
- содействие совершенствованию систем лицензирования и сертификации в области информатизации и связи;
- организация разработки и реализации учебных программ переподготовки и повышения квалификации специалистов в области обеспечения сетевой и информационной безопасности.

Другой организацией, которая занимается вопросами безопасности в сети, является международный Форум противодействия международному противоправному сетевому доступу.

В Форуме противодействия международному противоправному сетевому доступу (Forum for International Irregular Network Access, FIINA), который основан в 1987 г. как организация, представляющая права международных операторов связи на собственную защиту, защиту предоставляемых услуг связи и собственных клиентов от несанкционированного доступа, злоупотреблений и других противоправных действий, представлено всего две российские компании. Этими компаниями являются МТТ и ТТК (стала членом организации в 2006 г.). ТТК в октябре 2009 г. в Москве провела двадцать вторую ежегодную конференцию FIINA, которая впервые в истории организации состоялась на территории Восточной Европы. Но стоит отметить, что участниками форума могут стать операторы связи, предоставляющие международные услуги связи и имеющие соответствующие лицензии на данную деятельность, а при приеме требуется ходатайство двух участников форума. Участники форума имеют равные права, которые не зависят от статуса компании на рынке, от того, управляется компания государственными или частными активами.

Основными целями форума FIINA являются:

- предоставление операторам связи возможности обсуждать и обмениваться информацией о случаях противоправного сетевого доступа;
- выявление новых случаев противоправного сетевого доступа, используемые при этом средства;
- координация усилий в противостоянии противоправному сетевому доступу;
- ежегодное проведение заседаний форума для поддержки и объединения усилий в противостоянии противоправному международному сетевому доступу на должном уровне.

В состав руководства форума FIINA входят такие известные в телекоммуникационном мире специалисты, как Luis Cardoso (президент форума, компания Portugal Telecom), Rui Fortes (председатель форума, компания Cape Verde Telecom), Fabian Pivato (экс-председатель форума, компания Telmex — мексиканская телекоммуникационная компания), Gerhard Schroede (глава технического комитета — компания Deutsche Telekom), Peter Coulter (глава правового комитета, AT&T), протоколы заседаний ведут Greg Maggs (компания Telstra) и Peter Hoath (компания BT).

Еще одной известной международной организацией является Ассоциация по борьбе с мошенничеством в телекоммуникациях (Communications Fraud Control Association, CFCA), которая основана в 1985 г. Головной офис расположен в Розеланде, штат Нью-Джерси, США. В этой ассоциации состоят те же российские компании: МТТ и ТТК.

Основными целями организации являются:

- укрепление и развитие сотрудничества между компаниями, связанного с выявлением фактов мошенничества как внутри, так и вне коммуникационной отрасли;
- выявление, предупреждение и контроль инцидентов мошенничества;
- содействие развитию интересов членов ассоциации, связанных с защитой и эффективностью профессиональной деятельности этих организаций.

К задачам ассоциации относятся информирование компаний и организаций с целью развития знаний о мошенничестве на телекоммуникационном рынке услуг, осуществление правовой защиты компаний при контроле над мошенничеством в отрасли телекоммуникаций.

Любая корпорация, чей бизнес имеет непосредственное отношение к отрасли связи, может подать заявку на членство в ассоциации. Членом ассоциации может быть назначен тот, кто непосредственно отвечает за обнаружение, пресечение деятельности или судебное преследование правонарушителей.

Членами ассоциации являются представители 27 стран мира, шесть из которых (Россия, США, Великобритания, Германия, Италия и Канада) входят в «большую восьмерку».

Из вышесказанного следует вывод, что российские операторы связи активно ведут диалог на внутренней арене, но в то же время на международной арене в сфере информационной безопасности российские операторы связи представлены слабо: мало предложений и рекомендаций по совершенствованию правовых и технологических процессов.

Как мы видим, единого и полного определения мошенничества в сетях оператора связи на данный момент не существует не только в юридически значимой плоскости, но и на уровне международных стандартов. В этой ситуации каждая страна обособленно решает проблему через введение определений в свой уголовный кодекс (чаще всего эти определения охватывают весь спектр возможных мошенничеств, а не только аспекты, касающиеся ЭВМ). Но необходимо понимать, что в области обеспечения защиты информации нет понятия «мошенничество» — оно взято из обыденной жизни и юридических документов. Технические специалисты используют понятие «угроза» информации (активам, ресурсам), которое, в свою очередь, описывается через понятия источника угрозы, предполагаемого метода нападения, уязвимостей (которые являются предпосылкой для нападения) и идентификации активов (которые являются целью нападения). Для юридической и организационной защиты информации определение «мошенничество» допустимо, но так как предполагается разработать техническое решение защиты информации в сетях оператора связи, то для удобства и единства понятийного аппарата в дальнейшей работе будет использоваться понятие «угроза», а вместо термина «мошенник» — термины «нарушитель», «злоумышленник».

Не стоит забывать, что любое нарушение функционирования систем при оказании услуг связи, которое вызвано ошибками сотрудников, несовершенством используемых технологий и бизнес-процессов, может привести к возникновению злоумышленных действий правонарушителей, что повлияет на стабильность и рентабельность бизнеса.

## СПИСОК ЛИТЕРАТУРЫ:

1. Статья 159 Уголовного кодекса РФ «Мошенничество».
2. *Максименко В. Н., Афанасьев В. В., Волков Н. В.* Защита информации в сетях сотовой подвижной связи. М.: Горячая линия — Телеком, 2007.
3. *Волков Н. В., Демчишин В. И. и др.* Разработка модели защиты сети GSM от НСД с учетом методов борьбы с мошенничеством. Отчет о НИР ООО «Современные Телекоммуникации». 2004 г.