Д. В. Соколов

УГРОЗА АКТИВАМ В СЕТЯХ ОПЕРАТОРОВ СВЯЗИ: ТИПЫ УГРОЗ И ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ

С широким развитием телекоммуникаций, и в частности различных услуг для юридических лиц и конечных пользователей, все актуальнее и очевиднее становится проблема незаконного использования технологических возможностей операторов связи отдельными лицами и (или) организациями для своего обогащения за счет оператора.

Операторы связи не разглашают информацию об убытках, которые связаны с несанкционированным доступом к сетям связи, но, проанализировав имеющуюся в открытом доступе информацию, можно определить порядок этих цифр. Согласно данным Всемирной ассоциации по борьбе с мошенничеством в телекоммуникациях (Communications Fraud Control Association, CFCA), в 2005 г. операторы связи понесли убытки в размере $ 54,4–60 млрд от действий злоумышленников. Средние потери поставщика услуг составляют 3–8 % (по другим сведениям 10 %) его дохода, но эти потери неоднородны – в странах Африки они достигают 35 %. Нет точных данных и по России, по неподтвержденным сообщениям, потери составляют 10 % от дохода. Например, МГТС опубликовала подсчеты, согласно которым потери дохода только в Москве составляют $ 100-200 тысяч в год. Но это приблизительные данные. «Результаты исследования свидетельствуют, что мошенничество в телекоммуникациях – более прибыльный преступный бизнес, чем мы первоначально думали. И эта проблема растет с каждым годом», – подчеркивает сотрудник CFCA Джон Левандовски [1].

В России работу операторов связи регулирует закон «О связи». В нем дается определение сети связи: «Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи», в соответствии со статьей 2 Федерального закона «О связи» [2]. Этим законом устанавливаются правовые основы деятельности в области связи на территории РФ и на находящихся под юрисдикцией РФ территориях, определяются полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в деятельности или пользующихся услугами связи. Также в этом законе даны такие ключевые определения для телекоммуникационных операторов, как:

- «оператор связи – юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии»;
- «пользователь услугами связи – лицо, заказывающее и (или) использующее услуги связи»;
- «трафик – нагрузка, создаваемая потоком вызовов, сообщений и сигналов, поступающих на средства связи»;
- «услуга связи – деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений»;
- «универсальные услуги связи – услуги связи, оказание которых любому пользователю услугами связи на всей территории Российской Федерации в заданный срок, с установленным качеством и по доступной цене является обязательным для операторов универсального обслуживания»;
- «управление сетью связи – совокупность организационно-технических мероприятий, направленных на обеспечение функционирования сети связи, в том числе регулирование трафика».

Вторым документом, который регулирует отношения между телекоммуникационными операторами и их абонентами и пользователями, а также форму и порядок расчетов за оказание услуг, является постановление правительства «Об утверждении правил оказания телематических услуг связи». В нем дано ключевое определение: «абонент – пользователь телематическими

услугами связи, с которым заключен возмездный договор об оказании телематических услуг связи с выделением уникального кода идентификации» [3]. В этом документе также даны определения:
- «абонентская линия — линия связи, соединяющая пользовательское (оконечное) оборудование с узлом связи сети передачи данных»;
- «карта оплаты — средство, позволяющее абоненту и (или) пользователю использовать телематические услуги связи, идентифицировав абонента и (или) пользователя для оператора связи как плательщиков»;
- «пользователь телематическими услугами связи — лицо, заказывающее и (или) использующее телематические услуги связи»;
- «информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»;
- «тарифный план — совокупность ценовых условий, при которых оператор связи предлагает пользоваться одной либо несколькими телематическими услугами связи»;
- «телематическое электронное сообщение — одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом»;
- «техническая возможность предоставления доступа к сети передачи данных — одновременное наличие незадействованной монтированной емкости узла связи, в зоне действия которого запрашивается подключение пользовательского (оконечного) оборудования к сети передачи данных, и незадействованных линий связи, позволяющих сформировать абонентскую линию связи между узлом связи и пользовательским (оконечным) оборудованием»,

также даны определения вредоносного программного обеспечения и спама.

Для обнаружения незаконных действий существуют различные программно-аппаратные средства, но после детектирования несанкционированного доступа возникает вопрос: как юридически наказать злоумышленника, привлечь его к ответственности? В России существует, как минимум, три статьи, которые можно применить к незаконопослушному пользователю.

Если рассматривать телефон или модем как элементы компьютерной сети, то некоторые действия можно классифицировать по статье 272 УК РФ «Неправомерный доступ к компьютерной информации»: «1. Неправомерный доступ к охраняемой законом компьютерной информации… если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда… либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет. 2. То же деяние, совершенное группой лиц… либо лицом с использованием своего служебного положения… наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда… либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет». Эта статья применима к уничтожению, блокированию, модификации, копированию информации либо нарушению работы ЭВМ, но в ней нет упоминания о получении преступниками незаконного дохода. И наказание за такое преступление невелико, в зависимости от тяжести преступления — от штрафа в размере двухсот минимальных размеров оплаты труда до лишения свободы на срок до пяти лет.

При подделке преступником карт предоплаты услуг оператора связи его действия подпадают под статью 187 УК РФ «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов»: «1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами…

2. Те же деяния, совершенные организованной группой, — наказываются лишением свободы на срок от четырех до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового». В этой статье наказание более серьезное — лишение свободы на срок от двух до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет в зависимости от тяжести совершенного преступления.

Третья применяемая статья: получение незаконного доступа к сетям оператора связи может быть квалифицированно по статье 159 УК РФ «Мошенничество»: «1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием... 2. Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину... 3. Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере... 4. Мошенничество, совершенное организованной группой либо в особо крупном размере....». Груз ответственности — от штрафа в размере ста двадцать тысяч рублей до десяти лет лишения свободы в зависимости от тяжести преступления. Но собрать доказательства по этому виду преступлений крайне сложно.

Широкой публике известны единичные случаи, когда операторы связи «выносили мусор из избы» и дела о потере доходов от несанкционированного доступа доходили до суда. Абсолютное большинство поставщиков услуг связи предпочитают умалчивать о таких случаях, боясь отрицательных маркетинговых последствий такой «рекламы», и списывают потери как «непредвиденные расходы». Также поступают и пострадавшие абоненты, предпочитая не тратить свои нервы и время, выясняя, куда пропали 100 рублей со счета.

Наиболее распространены следующие типы угроз сети оператора (по данным компании Subex):

• Внутренние угрозы: инсайдеры, пожалуй, самые опасные преступники, они имеют доступ ко многим системам оператора связи, знают в деталях сеть передачи данных, и при этом их трудно вычислить. Например: злоумышленник может совершить продажу кодов карт оплаты услуг, сделать переактивацию заранее оплаченных номеров, удалить записи из биллинговых систем, удалить/изменить значение флагов и параметров аккаунта клиента и т. д.

• Подписные угрозы: в момент подписки на услугу клиент-мошенник намеренно предоставляет ложные данные. В этом случае подписчик пользуется дорогостоящими услугами без намерения их оплатить, а оператор не может собрать деньги с клиента-мошенника (схема реализуема, если счет клиента является постоплатным).

• Клонирование: в этом случае злоумышленник техническими средствами клонирует аппарат передачи данных (в аналоговых сетях это дублирование MIN/ESN, в GSM-сетях это клонирование SIM-карт). В результате создается эффект, что в сети функционируют два аппарата с одним номером: один принадлежит легальному владельцу, второй — злоумышленнику. Злоумышленник пользуется различными услугами, а легальный клиент их оплачивает.

• Продажа услуг: в этом случае абонент пользуется услугами оператора-мошенника, у которого заключен договор с вышестоящим оператором на предоставление услуг (оператор-мошенник является реселлером услуг). Злоумышленники собирают деньги с клиентов, но не оплачивают счета вышестоящего оператора, следовательно, эти деньги являются недополученным доходом для оператора. Потери могут быть очень высокими за короткий период времени.

• Злоупотребления с PRS (premium rate service, звонки с добавочной стоимостью): злоумышленник пользуется услугами PRS через оператора связи. У PRS увеличивается число соединений, и таким образом сетевой провайдер должен будет заплатить больше денег PRS-

провайдеру. При попытке оператора связи взять с клиента заплаченную сумму выясняется, что сделать это невозможно по различным причинам: неточности в договоре, поддельные документы клиента и т. п. Злоумышленник находится в сговоре с PRS.

• Коробочный маркетинг: некоторые операторы продают услуги связи в комплекте с оборудованием (например, с сотовым телефоном) для более быстрого проникновения оборудования на рынок. В этом случае злоумышленник покупает по заниженной цене комплект «оборудование + услуга», тем или иным способом отказывается от услуги и продает оборудование по более высокой стоимости. В результате оператор не получает дохода от того, что клиент пользуется услугой, и теряет деньги на субсидировании оборудования.

• SMS-злоупотребление: этот вид угроз становится все более популярным. Злоумышленники организуют sms Doc-атаки клиентов операторов сотовой связи, в которых пишут, что обладатель телефона что-то выиграл или с ближайшим родственником случилась какая-либо беда. После отправки обратного sms или звонка по указанному номеру со счета клиента снимается большая сумма.

• Угрозы, связанные с голосовой почтой: это может произойти по сценарию «счет на третьего». Злоумышленник взламывает голосовую почту законного пользователя и производит настройки, разрешая оплату звонков, сделанных злоумышленником. В данном случае пользователь будет оплачивать звонки преступника.

• Злоупотребление в роуминге: у сотового оператора мало возможностей контролировать в реальном времени клиентов в роуминге. Злоумышленники используют эту уязвимость для совершения звонков без намерения их оплатить.

• «Прикрепленное» злоупотребление основано на физическом присоединении к аппаратуре сервисов для совершения несанкционированных звонков.

• Дилер и торговый посредник: нечестные посредники между клиентами и операторами также большая проблема для последних.

• Угрозы с кредитными картами: в этом классе угроз злоумышленник использует для оплаты услуг украденную кредитную карту. Часто банк впоследствии отменяет транзакцию, деньги возвращаются законному владельцу, а оператор несет потери от неоплаченных услуг.

На данный момент не существует единой модели классификации видов угроз для операторов связи, предпринимаются только попытки ее создания на международном уровне.

Успешная борьба со злоупотреблениями в телекоммуникационной среде возможна только при комплексном подходе: решения должны пресекать саму возможность возникновения злоупотребления (интеллектуальные и превентивные решения управления), а если злоупотребление все же произошло, то помогать в расследовании инцидента и сборе доказательной базы для правоохранительных органов.

СПИСОК ЛИТЕРАТУРЫ:

1. Корпоративный журнал «Сеть ТТК». 2008. № 4 (10). URL: http://ttk.pp.ru/www/nsf/site.nsf/files/set_4_08.pdf/$FILE/set_4_08.pdf.

2. Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ (с изменениями, внесенными Федеральным законом от 23декабря 2003 г. № 186-ФЗ).

3. Постановление Правительства Российской Федерации «Об утверждении правил оказания телематических услуг связи» от 10 сентября 2007 г. № 575 (в ред. Постановления Правительства РФ от 16февраля 2008 г. № 93).