# Содержание

Введение 2

Техническое мошенничество 3

Контрактное мошенничество 4

Процедурное мошенничество 5

Сотовые мошенники в Интернете 6

Секретные коды для бесплатных звонков 7

Специальные прошивки телефона 7

Генераторы карт оплаты 8

Шпионы 9

Заключение 11

Литература 12

# Введение

Главная забота сотовых операторов, помимо конкуренции друг с другом, – это борьба с разными видами фрода (от английского fraud, мошенничество). Это махинации с контрактами и счетами, хищения и клонирование сотовых телефонов, а также всевозможные изощренные способы обмана сотовых компаний. По оценкам специалистов, общемировые потери операторов от мошенничества составляют $20-25 млрд. в год.

Ни для кого не секрет, что борьба с мошенничеством является на сегодняшний день одной из самых актуальных задач для операторов сотовой связи. Потери от действий различных злоумышленников достигают очень значительных сумм. Согласно статистике, в общем трафике телефонных переговоров на долю мошенников приходится от 2 до 6%. Европейские операторы сотовой связи ежегодно заявляют об убытках, исчисляющихся миллионами евро. И при этом учитываются только потери компаний. Между тем многие способы мошенничества наносят ущерб конечным пользователям. Поэтому нет ничего удивительного в том, что вопросы сотового мошенничества и защиты от него в последнее время приобрели большую актуальность. Но, для того чтобы бороться со злоумышленниками, необходимо разобраться в приемах, которыми они пользуются. И здесь не обойтись без классифицирования способов обмана как операторов сотовой связи, так и их клиентов. Именно этим мы с вами, уважаемые читатели, сейчас и займемся.

# Техническое мошенничество

Под техническим мошенничеством обычно понимают все виды атак на различные участки системы сотовой связи. Так, например, злоумышленник или злоумышленники могут попробовать получить доступ к компьютерам, обеспечивающим деятельность сотовой сети. В случае удачи они получат возможность внести в действующее программное обеспечение определенные изменения, которые позволят им бесплатно пользоваться услугами компании. Правда, для этого нужно быть высококлассным специалистом. Впрочем, существуют и более уязвимые для атаки элементы, например, существующие в системе базы данных. Именно в них хранится вся информация по пользователям и их SIM-картам. Так что доступ к этим базам хакеров был бы катастрофой для оператора сотовой связи. Но, естественно, компании понимают всю опасность подобной ситуации, а поэтому надежно защищают компьютеры, использующиеся в системе.

Более распространенным видом технического мошенничества являются различные атаки на устройства конечных пользователей, самой опасной из которых, конечно же, является клонирование. Для ее осуществления злоумышленники должны получить телефон-жертву на несколько часов в свое пользование. Сделав это (украв его у владельца, просто найдя потерянный аппарат), они с помощью специального оборудования создают его двойник, имеющий точно такие же идентификационные номера. Таким образом, оборудование сотовой сети будет воспринимать клон в качестве оригинала и списывать деньги за разговоры со счета его владельца, который и является в данной ситуации пострадавшим.

Отдельно хочется отметить возможность внутрикорпоративного технического мошенничества. Речь идет о внесении несанкционированных изменений в данные или программное обеспечение людьми, имеющими доступ к компьютерам системы по долгу службы. Нечистоплотные сотрудники операторов сотовой связи вполне могут изменить информацию в служебных базах или биллинговой системе таким образом, чтобы пользоваться услугами компании по сниженным ценам или вообще бесплатно.

# Контрактное мошенничество

Все виды мошенничества, относящиеся к этой группе, характеризуются одной общей чертой. В них абоненты системы сотовой связи своими действиями наносят ущерб компании-оператору. В остальном же мошеннические действия в каждом конкретном случае могут очень сильно отличаться друг от друга. Наиболее распространенным является использование злоумышленниками рекламных предложений операторов сотовой связи. Рассмотрим такой пример. Допустим, оператор сотовой связи начинает работу в каком-то городе. И, для того чтобы привлечь к себе внимание потенциальных клиентов, проводит специальную акцию – зачисляет на счет каждого подключившегося до определенного числа человека 500 рублей. Естественно, узнав об этом, находятся люди, которые заключают договор с оператором и начинают пользоваться его услугами. Но при этом они не платят деньги, а тратят подаренные 500 рублей, после чего уходят. То есть фактически получается, что эти люди заключили договор без намерения пользоваться услугами данного оператора.

Естественно, рассмотренный нами пример один из самых простых. На самом деле некоторые мошенники умудряются проворачивать достаточно хитрые схемы, позволяющие им бесплатно или по сниженным ценам пользоваться услугами оператора сотовой связи. Кстати, некоторые компании пытаются защититься от этой опасности. Так, например, клиентам МТС, для того чтобы воспользоваться специальными предложениями своего оператора, необходимо заключить дополнительное соглашение, подтверждающее их намерение в дальнейшем пользоваться услугами фирмы и оплачивать их.

# Процедурное мошенничество

К процедурным видам мошенничества относятся все виды атак на бизнес-процедуры, используемые в сотовой связи. Наиболее уязвимым в этом плане является роуминг. Например, нарушитель уехал куда-то за пределы области действия его оператора. При этом он может осуществлять звонки со своего телефона, пользуясь услугами другой компании. Однако в этом случае нередко возникают задержки в биллинговых операциях. Таким образом, человек, который «проговорил» все деньги со своего счета, некоторое время еще может делать звонки, поскольку система, в которой он находится в данный момент, пока не знает об этом. Естественно, это только один пример процедурной уязвимости роуминга. На самом деле существует еще несколько возможностей осуществлять разговоры мошенническим способом.

Другим видом процедурного мошенничества является неправомерное использование карт оплаты. Причем способы реализации этого действия могут быть различными. Так, например, известны случаи, когда в некоторых системах сотовой связи промежуток между пополнением счета с карты и выводом последней из обращения составлял несколько секунд. Этим успешно пользовались некоторые злоумышленники. Для этого они одновременно активировали со своих телефонов одну и ту же карту. В этом случае система пополняла сначала один счет. А потом, до вывода карты из обращения, успевала прокредитовать еще и другой.

Вторым способом неправомерного использования карт оплаты являются слабые места в процессе их производства и распределения. Для примера можно рассмотреть такой случай. В любом производстве существует определенная вероятность возникновения брака. Естественно, бракованные карты не поступают в продажу, но они содержат все необходимые реквизиты для пополнения счета. Таким образом, получив к ним доступ, злоумышленник может совершенно бесплатно пользоваться услугами сотовой связи. Правда, операторы достаточно строго следят за процессом производства, поэтому достать бракованные карты оплаты очень непросто.

Ну и, наконец, третьим распространенным способом процедурного мошенничества является использование фальшивых карт и генераторов PIN-кодов. Правда, нужно сразу отметить, что до сих пор нет официального подтверждения работоспособности предлагаемых злоумышленниками программ. Существует очень большая вероятность того, что это всего-навсего уловка, которая помогает мошенникам выманивать деньги у доверчивых людей.

# Сотовые мошенники в Интернете

Не так давно в интернете появилось множество сайтов, предлагающих посетителям приобрести различные технологии для совершения бесплатных звонков в сетях мобильной связи стандарта GSM. На первый взгляд кажется, что и говорить-то здесь совершенно не о чем – очевидно, что это самое обычное мошенничество, тем не менее, в нашей стране постоянно находятся желающие получить возможность разговаривать по сотовому телефону «просто так».

Рассматривать подобные «предложения» мошенников будем на конкретных примерах. Необходимо учитывать, что их сайты очень часть переезжают с одного места на другое, т. к. речь идет о прямом нарушении законодательства. А это значит, что как только модераторы какого-либо хостинг-провайдера найдут на своем сервере подобный сайт, то сразу же удалят его. Правда, мошенника это не останавливает – он тут же переходит на использование другого сервиса. Поэтому нет ничего удивительного в том, что веб-страницы вскоре могут стать недоступными.

## Секретные коды для бесплатных звонков

Суть этого предложения очень проста. Якобы, специально для сотрудников высшего звена сотовых компаний существуют секретные коды, позволяющие делать бесплатные исходящие звонки. Пользоваться ими нужно так. Сначала набираешь нужный тебе номер телефона, а потом, без всяких перерывов, секретный код. Придумано это было для того, чтобы руководители компаний могли в любое время пользоваться сотовыми телефонами «независимо от состояния своего счета».

Ну а теперь давайте немного подумаем. У всех операторов сотовой связи есть безлимитные тарифные планы. Неужели вы думаете, что руководитель высшего звена не может себе позволить заплатить за свои разговоры? Тем более что он может легко и быстро оформить договор по безлимитному тарифу на саму компанию, после чего беседовать по мобильному сколько угодно. Таким образом, существование системы секретных кодов не имеет абсолютно никакого смысла. Да ее и нет. Это всего лишь выдумка мошенников с целью получения денег от жертв «за воздух».

## Специальные прошивки телефона

Обычно, люди, предлагающие прошивки для телефона, делающие все разговоры по нему бесплатными, представляются бывшими сотрудниками операторов сотовой связи. Мол, проработав инженером 1, 3, 5… лет обнаружил уязвимость. Она позволяет разговаривать по мобильнику бесплатно, только для этого нужно телефон перепрограммировать. Заплатите мне, и я вышлю вам нужную прошивку. Привлекательное предложение? Еще бы. А ведь многие мошенники, чтобы показать свои «знания», вовсю «сыплют» реальными терминами технологий сотовой связи. И как тут не поверить, когда обещают «по значению RAND и ответа SRES калькулировать ключ идентификации Ki»?

А верить-то и нельзя. Вообще, любой человек, знакомый с технологией сотовой связи, сразу поймет, что имеет дело с мошенником. Дело в том, что простое и, зачастую, беспорядочное использование технических терминов может «запудрить» мозги только тем, кто вообще с этим не встречался. Поэтому люди, соблазненные предложением мошенников, и заплатившие им, получают следующее. В лучшем случае, это будет программа, которая только имитирует деятельность по перепрошивке телефона. Но последствия могут быть и серьезней. Так, например, полученная утилита действительно может попытаться изменить прошивку вашего телефона, но нет никакой гарантии, что после этого он вообще будет работать. Ну и, наконец, вместо программы можно легко получить троянского коня, который, в довершении всего, попытается выкрасть ваши пароли для доступа к Интернету.

## Генераторы карт оплаты

На сегодняшний день это самое распространенное мошенничество. «Стопроцентно реально работающие генераторы карт оплаты сотовой связи!». Такие предложения можно встретить на десятках разных сайтах, в форумах и на досках объявлений. Тут же описывается и история их создания. Оказывается, автор программы почти год работал в одной из компаний сотовой связи, познакомился там с алгоритмом генерации номеров карт оплаты, после чего и написал генератор, который он готов передать любому лицу за определенное вознаграждение.

Все предложения, касающиеся генераторов номеров карт оплаты, можно разделить на две группы. В первой продаже подлежит сама программа. Обычно она «универсальна» и может «работать» со всеми операторами сотовой связи «от Москвы и до Находки». Что, честно говоря, уже странно, поскольку у большинства из них существуют различные алгоритмы генерации. И даже проработав год у одного оператора, невозможно узнать, какие принципы используют другие. Кроме того, не забывайте, что большинство операторов сотовой связи блокируют телефоны (точнее, sim-карты), с которых три раза набирался неправильный номер или код активации карты оплаты. Таким образом, вы, уважаемые читатели, рискуете не только просто потерять свои деньги, отданные мошенникам, но и вообще лишиться связи.

Вторая группа предложений заключается в следующем. Мошенник утверждает, что для генерации номеров карт оплаты ему нужна одна настоящая, но еще не активированная карточка. И поэтому он предлагает жертве выслать ее данные ему. Взамен мошенник обещает предоставить четыре сгенерированных номера карт большего номинала, оставив себе один «в уплату». И, что самое смешное, есть люди, которые «клюют» на это. На первый взгляд кажется, что мошенник не ищет для себя особой выгоды – он всего лишь хочет бесплатно пользоваться сотовой связью. И он действительно достигает своей цели. За счет номеров карт оплаты, которые он получает от доверчивых интернетчиков. Ну а после получения желаемого, он тут же перестает общаться с жертвой или отправляет ей четыре номера, взятых «с потолка».

## Шпионы

Иногда в Интернете встречаются предложения приобрести программы, предназначенные для подслушивания разговоров по сотовому телефону. Якобы они рассчитаны на коммерсантов, которых наверняка интересуют происки конкурентов, мужей и жен, подозревающих своих благоверных в измене и т.д. Стоимость таких программ достигает сотен долларов, что внушает к ним определенное уважение. Наверное, поэтому нет-нет, да и находятся люди, желающие ее приобрести.

Но любой человек, хотя бы поверхностно знакомый с основами сотовых технологий, никогда не попадется на эту «удочку». Мы уже писали о безопасности сотовой связи. И выяснили, что получить на свой сотовый телефон «разговор», предназначенный не тебе, невозможно из-за надежной процедуры аутентификации. Единственной возможностью «подслушать» является радиоперехват. Но он возможен только с помощью специального оборудования, естественно, не поставляемого вместе с программой.

Но и «поймать волну» – это еще не все. Вся информация по радиоканалу передается в зашифрованном виде. Конечно, шифр можно взломать. Но для этого опять же потребуется специальное обеспечение, не один компьютер и целая куча времени. В общем, эффективное оборудование и программное обеспечения для прослушивания сотовых телефонов, если оно действительно существует, будет стоить не меньше нескольких сотен тысяч долларов. Да и для его работы необходимо постоянно находиться хотя бы в пределах одной соты с объектом слежки.

# Заключение

Итак, как мы видим, существует множество самых разнообразных способов мошенничества, связанных с системами сотовой связи. Некоторые из них наносят ущерб операторам, другие – их клиентам. Но в любом случае проблема сотового мошенничества очень серьезна. Впрочем, в последнее время борьба с ним ведется на всех уровнях. Государство готово обеспечить правовую защиту как операторов сотовой связи, так и их клиентов. Правоохранительные органы серьезно (и чаще всего успешно) занимаются расследованием случаев сотового мошенничества. Операторы сотовой связи и компании, выпускающие различное оборудование и мобильные телефоны, постоянно разрабатывают новые способы защиты от злоумышленников. Да и простые пользователи систем мобильной связи стали менее доверчивыми. Так что будем надеяться, что сотовое мошенничество хоть и не удастся искоренить полностью (наверное, это невозможно), но хотя бы получится свести потери от него к минимуму.

Ну а напоследок давайте еще раз вспомним, как можно обезопасить себя и свои деньги от «сотовых» мошенников в Интернете. В принципе, достаточно всего лишь соблюдать основные правила безопасного поведения в Сети. Также необходимо помнить, что реальных способов обеспечения бесплатной сотовой связи не так уж и много, и ни один из них не имеет ничего общего с предложениями, размещенными на разных сайтах. И пусть даже в форумах оставлено большое число благодарственных сообщений и подтверждений работоспособности кодов, программ и прошивок. Все они пишутся самими же преступниками, только под разными именами. Ну а, кроме того, помните, что даже если вам повезет, и вы действительно найдете способ совершать бесплатные звонки по сотовому телефону, то это деяние будет уголовным преступлением. И рано или поздно вас вычислят (не зря же операторы держат у себя приличную службу безопасности), найдут и примерно, чтобы другим неповадно было, накажут.

# Литература

1. Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий. – М., 2002, – С. 18
2. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. – Воронеж, 2001. – С. 25
3. Угрозы в сфере ИБ // Виды сотового мошенничества // 11.11.2004
4. Угрозы в сфере ИБ // Сотовые мошенники в Интернете // 19.07.2004