УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА

УДК 343.98

Д.С. АЛПАТОВ,

старший преподаватель

Набережночелнинский филиал Института экономики, управления и права (г. Казань)

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НОВЫХ СПОСОБОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ СОТОВОЙ СВЯЗИ

Статья посвящена вопросам криминалистической характеристики способов совершения преступлений в сфере сотовой связи, как «традиционных», так и появившихся относительно недавно, в 2008–2010 гг. В данной статье автором предложены основные направления противодействия подобного рода преступлениям.

Огромная, на пол-экрана рабочего стола Windows, заставка порнографического характера программы-блокиратора с требованием отправить два смс-сообщения, сообщение с поздравлением в выигрыше миллиона рублей и предложением дальнейшего участия в розыгрыше и звонок «родственника» попавшего в беду с мольбами помочь и т.д. – эти знакомые многим ситуации объединяют два факта – все они являются преступлениями и в каждом из этих случаев для достижения преступных целей используется сотовый телефон.

Вообще, сотовая связь настолько глубоко внедрилась в наш быт, что уже сложно представить современного человека без мобильного телефона. Тем более что сотовый представляет собой не только средство передачи голосовых данных, а, по сути, небольшой компьютер со встроенным периферийным оборудованием – видеокамерой, плейером, игровой приставкой и тому подобными гаджетами для выхода во всемирную сеть Интернет.

Мобильная связь начала развиваться в 70-х гг. XX века. Обусловлено это было объективной необходимостью в доступности телефонной связи для населения и перспективностью экономически выгодного проекта на основе достижений науки для будущих производителей.

Первые известные стандарты сотовой связи – NMT и AMPS (позднее – DAMPS, от первой буквы «D» в слове «Digital» – цифровой) появились в 1981 г. Второе поколение, так называемое 2G, появилось позднее, после решения Европейской Конференции Администрации Почт и Электросвязи, в связи с необходимостью введения единого стандарта цифровой сотовой связи. Результатом развития данного направления стало внедрение знакомого всем стандарта GSM (Global System for Mobile Communications). Появившись в Германии в 1992 г., сейчас этот стандарт все еще является основным для большинства абонентов в мире [1].

Стремительное развитие средств мобильной связи и иных достижений науки и техники породили пласт новых видов преступлений, где данные средства используются в качестве орудия или способа совершения преступлений.

Рассмотрим, какие же преступления совершаются в сфере предоставления услуг сотовой связи. Существует несколько типовых схем совершения преступных посягательств.

1. Переадресация звонков**.** Преступник становится клиентом компании мобильной связи, покупает телефон, а затем дает объявление в газету о предоставлении услуг дешевой связи с любой точкой мира. Связавшийся с ним клиент называет номер, на который он хочет позвонить. Затем мошенник кладет трубку, устанавливает переадресацию на указанный номер и связь осуществляется в обход по транку, через коммутатор. При этом номер преступника не занят и может использоваться снова. Благодаря этому можно одновременно обслужить множество международных вызовов, получить за них денежную сумму и скрыться.

2. Мошенничество с абонентом. Для этого преступник абонирует сотовую связь на имя другого лица, без ведома последнего, затем использует телефон в операциях по «торговле телефонными звонками», то есть предлагает своим клиентам анонимно звонить по любому номеру в мире по низкому тарифу. Если счет остается неоплаченным, телефон отключается, а мошенник подключается к очередному чужому номеру. В результате компании сотовой связи вынуждены возмещать компаниям междугородной связи стоимость таких звонков.

3. Перепрограммирование**.** Преступник приобретает сотовый телефонный аппарат законным способом и заменяет микросхему либо же нелегально приобретает телефон с уже перепрограммированным программным запоминающим устройством. При помощи перепрограммированного аппарата преступник получает доступ к коммутационному оборудованию телефонных компаний, и его вызовы обрабатываются, как и любые другие, с той лишь разницей, что отсутствует абонент для предъявления счета. Поскольку поставщик услуг сотовой связи не может установить личность клиента, она вынуждена оплатить счета по стоимости междугородной части таких вызовов.

4. Клонирование (использование чужого идентификационного номера (другими словами – счета) в корыстных интересах). Преступник перехватывает идентифицирующий сигнал чужого телефона и выделяет из него идентификационные номера MIN и ESN. Потенциальный преступник может перехватить эту электронную информацию при помощи радиосканера либо так называемого сотового кэш-бокса – комбинации сканера, компьютера и сотового телефона. Он легко выявляет и запоминает номера MIN и ESN и автоматически перепрограммирует себя на них. Использовав пару MIN/ESN один раз, он стирает ее из памяти и выбирает другую. Такой аппарат делает выявление мошенника практически невозможным. Преступник перепрограммирует свой телефон так, чтобы пользоваться электронным серийным номером и телефонным номером этого абонента. Перепрограммирование осуществляется путем перенесения информации с помощью компьютера на микросхему, которая вставляется в сотовый телефон. Таким телефоном можно пользоваться до тех пор, пока несанкционированные вызовы не будут обнаружены. Стоимость разговора с этого аппарата заносится на счет того абонента, у которого эти номера были украдены. Если абонент докажет, что звонки произведены не им, то он может опротестовать счета и добиться их отмены. В таких случаях компания сотовой связи вынуждена оплатить междугородную часть таких вызовов. Преступник же выходит на номер любого другого абонента и снова возвращается к своему незаконному бизнесу [2].

Вышеописанные способы совершения преступных посягательств являются, можно сказать, уже традиционными. Но в последнее время появляются и новые способы совершения мошеннических действий. Новыми мы их называем весьма условно, поскольку все они основаны на старых схемах, рассчитанных на доверие и склонность к «халяве» наших граждан. Какие же это способы? Рассмотрим наиболее популярные.

Одним из распространенных способов является звонок от популярного теле- или радиоведущего, где жертве сообщается о проводимой, например, одной из радиостанций акции, в которой номер абонента участвовал в розыгрыше призов и одержал победу. Выигрыш, например сотовый телефон, можно забрать в офисе радиостанции, осталось оплатить НДС. Для этого необходимо активировать несколько карт оплаты на определенный номер. По словам представителя Управления «К» А. Грабленского, были случаи, когда такие «розыгрыши» производились из мест лишения свободы. Например, один мошенник, отбывая 13-летний срок заключения во Владимирском централе, с помощью сотового телефона

проводил «лотереи» в московской области, представляясь от имени крупных сотовых компаний или радиостанций и обещая крупные выигрыши. Обманутые перечисляли деньги, а соучастники преступника, находившиеся на свободе, снимали деньги со счетов. Как вариант, используется следующий способ. Также сообщается о выигрыше, но для получения приза необходимо сообщить свой пин-код и данные паспорта. Это необходимо было преступникам, чтобы снять деньги со счета абонента и подделать документы. Данный способ кажется невероятным в исполнении, но в мае 2009 г. в Москве была задержана семейная пара, совершавшая мошенничества, на счету которой оказались около 10 тысяч жертв по всей России, а ущерб от их деятельности составлял свыше 100 млн рублей.

Схожим с предыдущим является следующий способ. Условно назовем его «Звонок от оператора». Жертве звонит мошенник, представляющийся сотрудником службы технической поддержки компании сотовой связи. Затем он предлагает подключить новую услугу либо предлагает перерегистрацию во избежание сбоя мобильной связи или наоборот улучшения качества и тому подобное, после чего диктует жертве код, который он должен набрать на телефоне. Данный код является средством для перевода денег со счета абонента на счет мошенника. Или другой вариант. «Оператор» звонит абоненту и налагает штрафные санкции по причине неоповещения оператора о смене тарифного плана, пользования услугами роуминга без предупреждения и тому подобное, в результате чего «жертве» необходимо активировать карты оплаты на определенный номер [3].

Весьма распространены такие способы, когда жертве приходит смс с незнакомого номера, например, с таким с текстом: «У меня проблемы. Я в больнице. Срочно позвони. Если не берут, положи на этот номер 300 рублей». Применяя нехитрые методы социальной инженерии, преступники в накладе не остаются, ведь у всех есть родные и близкие, и если из десяти абонентов 1–2 положат небольшую сумму (а она, как правило, небольшая – 100–300 рублей), значит, цель достигнута. Более сложный способ связан с непосредственным общением с жертвой. Мошенник, представляясь знакомым, сослуживцем родственника (иногда – сотрудником правоохранительных органов) сообщает поднявшему трубку (конечно, жертва здесь не случайна) о беде, произошедшей с близким, например, что он стал виновником ДТП или задержан милицией по подозрению в совершении преступления. Объясняя, что нужна необходимая сумма для того, чтобы «уладить дело», жертве назначается встреча для передачи денег.

Существуют и иные способы совершения преступлений в сфере сотовой связи. На электронный почтовый ящик клиента приходит письмо с предложением купить программу, которая может подобрать секретный код карт оплаты. Для этого абоненту необходимо активировать карту стоимостью 5 долларов, и он получит взамен код карты на 20 долларов и приз – 1000 смс. Также объявлялись акции «Позвони на номер такой-то и получи 5 долларов на счет». Абоненты звонили и получали 5 долларов на счет, правда, с их счета снимали 15 долларов. Или еще один способ под названием «Один звонок». Мошенник набирает номер и разъединяется. Если абонент перезванивает на незнакомый номер, то с его счета списывается крупная сумма денег, ведь стоимость входящих преступник определяет сам.

Казалось бы, невероятно, как такие случаи вообще возможны, поскольку они постоянно упоминаются в СМИ и обсуждаются многими людьми, в том числе и в кругу будущих жертв. Но тем не менее ряды потерпевших постоянно пополняются в силу упомянутых выше причин.

Мы рассмотрели лишь немногие из способов совершений таких преступлений. Существуют также и внедренные со спамом троянские программы-блокираторы рабочего стола и Интернета, с требованием отправить 2 смс для разблокировки стоимостью (по словам потерпевших) около полутора тысяч рублей. Существуют и «акции», рекламирующие скидки при покупке жилья, для получения которых необходимо участвовать в смс-голосовании. Ко всему прочему, мошенники устраивают смс-знакомство с «симпатичной девушкой», роль которой исполняет программа-робот, более или менее по смыслу отвечающая на входящие смс. Суть всех этих действий одна – при помощи сотового телефона необходимо принудить жертву добровольно отдать деньги. И если эти схемы перестанут работать, преступники вскоре разработают новые.

Вообще, интересен следующий факт. При подготовке данной статьи нами было опрошено 378 граждан г. Набережные Челны. Из опрошенных 82 респондента указали, что они сами либо их родственники или знакомые являлись жертвами таких преступных действий. В правоохранительные органы обратился 1 человек.

Сейчас сфера коммуникаций постоянно развивается. С 2003 г. активно внедряется стандарт 3G с поддержкой видеозвонков и многим другим. Компании МТС, Билайн и Мегафон запускают данный стандарт в тестовом и уже коммерческом режимах. Кроме того, в мире ведутся разработки стандарта 4G. Несомненно, это откроет новый уровень возможностей, в том числе и для преступников.

На наш взгляд, однозначного решения проблемы нет. По мере развития сферы высоких технологий будут развиваться и новые способы совершения преступных посягательств. Сдерживающим фактором, на наш взгляд, будут являться меры законодательного и организационного характера. Уже давно возникла объективная необходимость пристального внимания к законодательному регулированию вопросов уголовно-правового характера в сфере высоких технологий. Кроме того, необходимо тесное сотрудничество правоохранительных органов и служб безопасности крупных компаний-поставщиков услуг на рынке сотовой связи. К тому же, нельзя не принимать во внимание опыт правоохранительных органов зарубежных стран по борьбе с преступлениями в данной сфере, поскольку данные преступные действия уже давно приобрели транснациональный характер.

Владельцам же сотовых телефонов, потенциальным жертвам мошеннических действий, можно дать несколько практических советов:

– никогда не передавайте сотовый телефон и конфиденциальную информацию третьим лицам;

– необходимо чаще менять поставщика услуг сотовой связи;

– сообщать о каждом инциденте поставщику услуг и правоохранительным органам;

– использовать две и более единицы антивирусной программной продукции;

– не поддаваться на провокации мошенников.

Список литературы

1. Наука и техника: технология и промышленность. – URL: http: // www.krugosvet.ru/enc/nauka_i_tehnika/tehnologiya_i_promyshlennost

2. Преступность в сфере сотовой связи. – URL: http:// www.imc.org.ua/index4.php?a=prot705a (дата обращения: 14.03.2010).

3. Советы о том, как избежать некоторых видов телефонного мошенничества. – URL: http://www.gadjievo.ru/forum/showthread.php?t=1884 (дата обращения: 14.03.2010)

В редакцию материал поступил 27.10.11

Ключевые слова: сотовая связь, компании-поставщики услуг сотовой связи, пользователи сотовой связью, мошеннические посягательства на денежные средства компаний-поставщиков услуг сотовой связи и их пользователей.