А.А. Лабутин
(группа по Республике Татарстан
филиала по ПФО ФГКУ «ВНИИ МВД России»)

«МОБИЛЬНЫЕ» МОШЕННИЧЕСТВА: ОСНОВНЫЕ СПОСОБЫ СОВЕРШЕНИЯ

В статье раскрываются наиболее распространенные в криминальной среде схемы совершения мошенничества с использованием средств сотовой связи и основные способы изъятия денежных средств у потерпевших от таких преступлений.

Ключевые слова: средства сотовой связи, телефон, мошенничество, схемы и способы совершения

In article the schemes of commission of fraud most widespread in the criminal environment with use of means of cellular communication and the main ways of withdrawal of money at victims from such crimes reveal.

Key words: means of cellular communication, phone, fraud, schemes and ways of commission

Корыстную преступность можно назвать криминальным феноменом. Её доля превышает 90% от общего количества зарегистрированных преступлений в странах с развитой экономикой и более 60% в развивающихся странах [1]. При этом каждый третий вид преступления, преследуемого по Уголовному кодексу Российской Федерации, входит в число преступлений, где корыстная мотивация выступает характерным признаком.

Наиболее распространенными преступлениями из числа корыстных являются преступления против собственности, совершаемые посредством различных форм хищений чужого имущества. Их общественная опасность определяется тем, что в своем большинстве они вносят дезорганизацию в экономическую жизнь страны, создают возможности для паразитического обогащения одних за счет других.

При этом одной из «самых популярных» у преступников форм хищений чужого имущества является мошенничество, «вирус» которого проник практически во все сферы человеческой деятельности.

Интенсивное развитие телекоммуникаций и компьютерных технологий является главной чертой нашего времени. Возникшие в 80-х гг. прошлого века беспроводные (мобильные) системы связи, благодаря своим функциональным возможностям, приобрели огромную популярность и распространились по всему земному шару. На сегодняшний день количество абонентов сотовых сетей в мире превысило 2,5 миллиарда человек [2].

Едва появившись, телефон стал высокодоходным орудием криминалитета, а сотовый (или мобильный) – в особенности: вместе со свободным оборотом на рынке сотовых телефонов появились и различные виды и схемы мошенничества, связанные с ним.

Злоумышленники всегда ищут способ «примоститься» к кормушке любого высокодоходного бизнеса. Как и в любой другой отрасли, способы мошенничества в сфере сотовой связи разнятся как по степени изощренности мошенников, так и по степени общественной опасности их деяний, при этом арсенал так называемых «мобильных кидал» постоянно пополняется и совершенствуется.

Как свидетельствует международная статистика, ежегодные совокупные потери

операторов связи и абонентов от телефонного мошенничества составляют примерно $10-40 млрд. Точно подсчитать невозможно – операторы информацией о своих потерях делятся неохотно, а абоненты, «кинутые» на 100-500-900 руб., зачастую никуда не обращаются [3]. Вместе с тем, по данным МВД России, каждый пятый из ста обладателей сотовых телефонов становился жертвой мошенничества [4].

Так, сравнительно недавно (по оценкам специалистов МВД России, с 2008 года), на территории нашего государства появились и начали массово проявляться так называемые «мобильные» мошенничества, где в качестве главного «орудия» совершения преступления выступают средства сотовой телефонной связи. Главной причиной популярности у криминалитета такого способа отъема чужого имущества у граждан – денежных средств – является широкая распространенность и относительная доступность для большинства населения услуг сотовой связи и средств общения внутри нее. Жертвами «мобильных» мошенников становятся все без исключения – это и бизнесмены, и чиновники, и звезды шоу-бизнеса, и обычные граждане.

Для общения с потенциальной жертвой «мобильные» мошенники используют:

1) телефонный звонок – позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом;

2) SMS-сообщения – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – в надежде на доверчивого получателя.

Основная цель «мобильных мошенников» – заставить потерпевшего добровольно передать свои денежные средства. Для этого используются различные схемы.

По данным Управления «К» МВД России, в настоящее время наиболее «популярными» в криминальной среде схемами телефонного мошенничества являются:

1) ***обман по телефону:*** требование выкупа или взятки за освобождение якобы из отделения полиции родственника или знакомого. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (совершил ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и др.). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас так делать нельзя, так как он боится потерять погоны. Деньги необходимо привезти в определенное место, передать какому-либо человеку или перевести на определенный счет. Общественная опасность подобных преступлений заключается в том, что, помимо причинения материального ущерба потерпевшим, дискредитируются правоохранительные органы, в частности полиция;

2) ***SMS-просьба о помощи:*** требование перевести определённую сумму на указанный номер (как правило, используется обращение «мама», «друг», «сынок» и т.п.). Абонент получает на мобильный телефон SMS-сообщение: «У меня проблемы, позвони по такому-то номеру, если номер недоступен, положи на него определенную сумму и перезвони» [5];

3) ***телефонный номер (ссылка) – «грабитель»:*** платный номер или интернет-ссылка, за один звонок или выход на которые со счёта списывается денежная сумма. Например, абоненту приходит SMS-сообщение о необходимости найти редкую группу крови для спасения ребенка. В сообщении указывается контактный номер телефона, звонки на который автоматически снимают денежные средства со счета звонящего. Или абоненту приходит SMS-сообщение, содержащее объявление с предложением стабильной работы с жильем и высокой зарплатой. Для получения информации о работе в них предлагается отправить SMS или позвонить на короткий номер (повышенная стоимость SMS или платный автоответчик). Или абонент получает от мошенников SMS-сообщение, оповещающее его о том, что он может посмотреть присланную ему поздравительную открытку со своего сотового телефона, пройдя по указанной ссылке. После перехода по ссылке абонент автоматически

подписывается на один из платных сервисов или «цепляет» вирус, в результате чего в последующем происходит ежедневное списание средств с его телефонного счета. Или абоненту приходит SMS-сообщение: «Вам отправлена MMS-открытка или получен MMS-подарок от, например, «Катя» для абонента с номером +7...». И далее абонент видит свой номер и ссылку для скачивания. При нажатии на ссылку на телефон скачивается и автоматически запускается java-приложение, содержащее вредоносное программное обеспечение, которое отсылает SMS с переводом средств на номера мошенников;

4) ***выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи:*** потерпевшего просят приобрести карты экспресс-оплаты и сообщить коды либо перевести определенную, как правило, крупную денежную сумму на свой счёт, а потом ввести специальный код. На мобильный телефон абонента звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем (телефон, ноутбук и др.) в лотерее, организованной радиостанцией и оператором мобильной связи. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения; грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.); спрашивает, может ли абонент активировать на свой номер карты экспресс-оплаты на определенную денежную сумму; объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер; поясняет порядок последующих действий для получения приза. Если по каким-то причинам абонент не сможет в течение часа найти карты экспресс-оплаты на определенную денежную сумму, то все равно должен позвонить для согласования дальнейших действий. Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора – сообщить свои коды. Оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего присваивает ему персональный номер «победителя», с которым гражданин должен ехать за призом. Предложение самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании не принимается, таковы правила рекламной акции;

5) ***простой код от оператора связи:*** предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства со счёта. Поступает звонок якобы от сотрудника службы технической поддержки оператора сотовой связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников;

6) ***штрафные санкции и угроза отключения номера:*** якобы за нарушение договора с оператором сотовой связи. Мошенник представляется сотрудником службы технической поддержки оператора сотовой связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения), и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды;

7) ***ошибочный перевод средств:*** просят вернуть деньги, а потом дополнительно снимают сумму по чеку. Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «мобильный перевод». Сразу после этого поступает звонок от мошенника, который сообщает, что ошибочно перевел деньги на его счет и просит вер-

нуть их обратно тем же «мобильным переводом»;

8) ***услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека:*** зная склонность некоторых граждан «пошпионить» за близкими и знакомыми, злоумышленники придумали очередной способ мошенничества в Интернете. Пользователю предлагается изучить содержание SMS-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того, как пользователь отправляет SMS, с его счета списывается сумма гораздо большая той, что была указана мошенниками, – до 500 руб., а интересующая информация так и не поступает;

9) ***SMS-сообщение о блокировании банковской карты:*** абоненту приходит SMS-сообщение о том, что его банковская карта заблокирована, и ему предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда владелец карты звонит по указанному телефону, ему сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и PIN-код для ее перерегистрации. Получив реквизиты пластиковой карты, мошенники переводят денежные средства на свой телефон, а затем снимают их со счета;

10) ***SMS-сообщение о выигрыше автомобиля:*** абоненту сотовой связи, как правило, в ночное время приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления необходимых документов) счастливому обладателю новенького автомобиля необходимо перечислить на счет своего сотового телефона определенную денежную сумму, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации». Как только жертва завершает указанные манипуляции, счет обнуляется.

По результатам проведенного нами анализа материалов уголовных дел и судебно-следственной практики по преступлениям рассматриваемой категории считаем необходимым выделить и такую нередко используемую мошенниками схему, как ***заказ на приготовление и доставку готовых блюд и продуктов.*** Так, в целях реализации своего преступного умысла, мошенники осуществляют по сотовому телефону звонок в различные регионы России и оставляют заказ на приготовление и последующую доставку на домашний адрес готовых блюд и продуктов в предоставляющие такие услуги организации (рестораны, кафе и т.д.) [6]. Затем, когда преступникам сообщают о готовности их заказа, мошенники просят контактный телефон курьера, осуществляющего доставку, и в процессе разговора с курьером под любым предлогом убеждают последнего во время доставки внести через платежный терминал денежные суммы на счета абонентских номеров «своих» сотовых телефонов. После поступления денежных средств мошенники просто отключают сотовый телефон [7].

Новая схема мошенничества с использованием средств сотовой связи совсем недавно выявлена в Вологодской области, где сотрудниками уголовного розыска областного УМВД России в результате оперативно-розыскных мероприятий были задержаны два жителя Республики Украина, подозреваемые в совершении мошеннических действий. Преступная схема основывалась на отзывчивости граждан. Жертвами злоумышленников в основном становились пожилые люди. Заходя в подъезд или частный дом, неизвестный интересовался у жителей, не находил ли кто видеокассету или компакт диск с очень ценной информацией. Отзывчивые граждане, особенно пенсионеры, проникались сочувствием и

помогали опрашивать соседей. После безрезультатных поисков подозреваемый оставлял свой контактный номер и просил обязательно перезвонить в случае обнаружения пропажи, обещая приличное вознаграждение. Затем появлялся второй злоумышленник и приносил кассету (диск), которую он якобы только что нашел, и требовал вознаграждение. Граждане звонили «потерявшему», который говорил, что подъедет в скором времени и просил рассчитаться с человеком, обнаружившим искомую кассету или диск. Все пострадавшие, в основном – люди преклонного возраста, до последнего верили, что делают благое дело, помогают человеку, потерявшему ценную вещь. И только спустя время понимали, что их обманули [8].

И отметим еще один недавний случай, связанный с очередным способом совершения мошенничества с использованием средств сотовой связи. Сотрудники УЭБиПК ГУ МВД России по г. Москве совместно с ГСУ ГУ МВД России по г. Москве и службой безопасности Сбербанка России при поддержке СОБР ЦСН ГУ МВД России по г. Москве провели крупномасштабную операцию по пресечению деятельности группы мошенников и задержанию организаторов и участников организованной преступной группы. Жертвами злоумышленников становились, как правило, люди преклонного возраста – пенсионеры, инвалиды и ветераны Великой Отечественной войны. Аферисты звонили им по телефону и, представляясь работниками различных государственных органов – МВД России, ФНС, Центробанка, Счетной палаты и других, предлагали получить компенсацию за ранее приобретенные биологически активные добавки. Они просили пожилых людей оплатить издержки по оформлению документов, якобы необходимых для получения компенсации. После осуществления первого денежного перевода на счета подконтрольных им частных лиц злоумышленники звонили снова и под различными предлогами требовали дополнительных платежей. Например, говорили о возможности предоставления большего размера компенсации, ссылались на неправильное зачисление денежных средств и прочее. Впоследствии они обналичивали деньги через банкоматы. По предварительным данным, от действий аферистов пострадало более 150 человек. Ущерб в каждом из эпизодов составил от 100 тысяч до 1,5 млн рублей. Среди пострадавших – жители не только Москвы и Подмосковья, но и других регионов России. Полицейские установили, что лидер группы ранее осуществлял мошенническую деятельность в области реализации биологически активных добавок. Собранная таким образом база данных покупателей использовалась для повторного совершения хищений «по схеме компенсаций» [9].

Изъятие денежных средств может проходить также разными способами. Наиболее популярны у «мобильных» мошенников следующие схемы получения денежных средств от потерпевших:

- передать деньги из рук в руки или оставить в условленном месте;
- приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;
- перевести деньги на свой счёт и ввести специальный код;
- перевести деньги на указанный счёт;
- позвонить на специальный телефонный номер, который окажется платным, и со счёта потерпевшего будут списаны средства.

В качестве примеров приведены далеко не все схемы «мобильных» мошенничеств, арсенал преступников постоянно совершенствуется и пополняется, при этом все чаще в своих мошеннических схемах криминальные аферисты используют возможности Интернет-ресурсов.

ЛИТЕРАТУРА

1. См.: Лунеев В.В. Преступность XX века. Мировой криминологический анализ. М., 1997. С. 234.
2. См.: Лазарева И.В. Расследование преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи: автореф. дис. … канд. юрид. наук. Хабаровск, 2007.
3. См.: http://aferizm.ru.
4. См.: http://znakkachestva.ru.
5. Прим. автора. «Мобильные» мошенники придумали очередной способ обмануть доверчивых владельцев сотовых телефонов. Их SMS теперь маскируются под знакомые абонентам номера – теперь просьбы о финансовой помощи могут прийти от якобы знакомых людей, тех, чьи имена занесены в контакты абонента. То есть кибер-преступники научились подделывать имя отправителя (по материалам сайта: http://news.mail.ru).
6. Прим. автора. Данные по реальным домашним адресам и организациям, выполняющим заказы на приготовление и последующую доставку на домашний адрес готовых блюд и продуктов, мошенники получают, как правило, через Интернет.
7. См., например, материалы уголовного дела №2694, возбужденного в отношении Джабуа А.А. по признакам составов преступлений, предусмотренных ч. 2 ст. 159 УК РФ (7 эпизодов). Архив ОМВД России по Зубово-Полянскому муниципальному району Республики Мордовия. У/д №2694, 2011.
8. См.: http://mvd.ru.
9. См.: http://petrovka38.ru.