УДК 343.72 С. 40—45

О НЕКОТОРЫХ ПРИКЛАДНЫХ АСПЕКТАХ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Коробов А. А.
Орловский юридический институт
МВД России им. В. В. Лукьянова
E-mail: konvar2012@mail.ru.

С развитием научно-технического прогресса информационная среда неизбежно расширяется и постепенно начинает охватывать практически все области жизни современного человека, включая товарно-денежные отношения, рыночную экономику.

В настоящее время все чаще сделки оплачиваются сторонами депозитными или кредитными пластиковыми картами, либо бесконтактным способом оплаты, а равно с помощью мобильных устройств с заранее установленным программным обеспечением. Например, на операционных система Android и IOS для смартфонов, планшетов и часов, устанавливается программное обеспечение, позволяющее путем поднесения мобильного устройства к считывающему кассовому прибору для оплаты товаров и услуг.

При этом, важно отметить, что и мошеннические действия, с использованием электронных средств платежа, не остаются в стороне, стараясь развиваться и успевать за информационно-вычислительной средой современного, всестороннего развитого общества.

Последней тенденцией современного общества выступает усовершенствование форм и видов хищений, предметом которых являются банковские карты, электронные кошельки и иные электронные платежные системы, среди которых лидерство принадлежит мошенничеству.

В последнее время Банк России зафиксировал резкий подъем несанкционированных операций со счетами клиентов банков. В подавляющем большинстве случаев они происходят через подменные телефонные номера с использованием социальной инженерии. Поэтому актуальной на сегодняшний день проблемой пока остается проблема личной безопасности и защиты индивидуальных данных.

В мошеннических схемах оказывается задействованными все большее количество людей, растет количество потерпевших из числа менее защищенных слоев населения — пенсионеры. Данный вопрос давно является дискуссионным в научных кругах и как следствие требует дальнейшего исследования.

Ключевые слова: подменный номер, мошенничество, несанкционированное списание денежных средств, социальная инженерия, электронное средство платежа, транзакция, конфиденциальные данные.

ABOUT SOME APPLIED ASPECTS OF FRAUD USING ELECTRONIC MEANS OF PAYMENT

Korobov A. A.
Lukyanov Orel Law Institute
of the Ministry of the Interior of Russia
E-mail: konvar2012@mail.ru.

With the development of scientific and technological progress, the information environment inevitably expands and gradually begins to cover almost all areas of modern life, including commodity-money relations, and the market economy.

Currently, more and more transactions are paid by the parties with Deposit or credit cards, or contactless payment method, as well as using mobile devices with pre-installed software. For

example, on the Android and IOS operating systems for smartphones, tablets and watches, software is installed that allows you to bring your mobile device to the cash register reader to pay for goods and services.

At the same time, it is important to note that fraudulent actions using electronic means of payment do not remain on the sidelines, trying to develop and keep up with the information and computing environment of a modern, all-round developed society.

The latest trend in modern society is the improvement of forms and types of theft, the subject of which are Bankcards, e-wallets and other electronic payment systems, among which the leadership belongs to fraud.

Recently, the Bank of Russia has recorded a sharp rise in unauthorized transactions with Bank customers ' accounts. In the vast majority of cases, they occur through spoofed phone numbers using social engineering. Therefore, the problem of personal security and protection of individual data remains an urgent problem today.

An increasing number of people are involved in fraudulent schemes, and the number of victims from less protected segments of the population — pensioners-is growing. This issue has long been debated in scientific circles and as a result requires further research.

Keywords: fake number, fraud, unauthorized debiting of funds, social engineering, electronic means of payment, transaction, confidential data.

Введение

Еще в 2018 году ФинЦЕРТ (подразделение ЦБ РФ, отвечает за кибербезопасность) отметил резкий всплеск хищений средств с карт физических лиц. Общая сумма составила 1,4 млрд руб., что в 1,4 раза больше показателя 2017 года. При этом около трети хищений пришлась на четвертый квартал и 97 % атак были проведены с использованием социальной инженерии.

Описание исследования

В начале 2019 года тренд усилился, причем злоумышленники при звонках потенциальным жертвам стали чаще использовать технологию подмены телефонного номера банка (так называемый А-номер) при использовании звонков через Интернет. При таких звонках на экране телефона жертвы высвечивается реальный номер банка, а клиенту сообщают о попытке несанкционированного списания средств, называют его ФИО, номер паспорта, остаток по счету и даже последние трансакции.

Для защиты средств клиенту предлагают перевести их на специальный счет, сообщить полную информацию по карте, кодовое слово или данные из SMS. Нередко клиент, сбитый с толку информацией, которую может знать только банк, рассказывает неизвестным собеседникам по телефону всю запрашиваемую информацию,после чего происходит хищение всех денежных средств.

Для совершения подобных звонков злоумышленники используют IP-телефонию. Применяя один из протоколов такой связи (SIP-протокол), звонки можно проводить с помощью компьютера, установив специальную программу; через сети Wi-Fi или 3G/4G с помощью SIP-программ для планшетов и мобильных телефонов; используя специальный стационарный SIP-телефон, который включаются в роутер; через обычный телефон, подключив его к VoIP-шлюзу, а сам шлюз — к роутеру. Технология широко используется в обычной жизни для правомерных действий, например, соединение по SIP-протоколу позволяет организации с несколькими колл-центрами звонить своим клиентам с одного указанного на сайте номера телефона.

Есть и технические решения, которые позволяют совершать звонок с номера, просто похожего на номер банка. Например, международные звонки с номера +880 (0) 555-57-77, который похож на номер колл-центра Сбербанка 8 (800) 555-57-77, но на самом деле совершается из Бангладеш. Или же звонки с иных номеров 8-800, которые операторы IP-телефонии могут сдать в аренду на срок от одного дня. Тем более, что сегодня программы и АТС, позволяющие совершать звонки с подменой А-номера, стали намного доступнее и дешевле, чем ранее.

При этом, если ранее, в 2018 году, злоумышленникам было сложно выдать себя за сотрудников службы безопасности банка, то уже в начале 2019 года преступникам были известны паспортные данные клиентов и остатки по их счетам благодаря доступу злоумышленников к банковской тайне. Причем источником информации могли служить не только недобросовестные сотрудники банка, но и «пробивка» данных по конкретному человеку по номеру телефона или полному имени владельца

карты, которая стала доступна сегодня на черном рынке за сравнительно небольшие деньги, и которая позволяет получить информацию о счетах клиентов и трансакциях по ним.

Один из Telegram-каналов предлагал подобную услугу по базам Промсвязьбанка, Бинбанка, Сбербанка и ВТБ, а также активно призывал к сотрудничеству желающих продавать информационные базы из других банков. Причем на смену ликвидируемым с помощью правоохранительных органов неизбежно и оперативно приходят новые, предлагающие такие же или подобные услуги.

Ярким примером является появление в открытом доступе информации по заемщикам банков Южного, Уральского и Приволжского федеральных округов, — по косвенным признакам база принадлежала брокеру на рынке POS-кредитования. В данной базе содержались данные по 294 тыс. заемщикам (полный пакет документов, включая фото), данные о кредитах и т. д.

Информацию об остатке на счете клиента и последних транзакциях мошенники могут выяснить, в том числе позвонив под видом клиента (с использованием той же технологии подмены А-номера) на автоинформатор банка. Подменный номер телефона клиента во многих банках позволяет пройти первичную идентификацию при звонке и получить доступ к конфиденциальной информации.

Исходя из пресс-релизов и информационных обзоров Сбербанка, Юникредитбанка, Райффайзенбанка и т. д.), и на сегодняшний день данная проблема не утратила актуальности, при этом банки активно и последовательно выступают за разделение ответственности с операторами связи.

Например, специалисты по IT-безопасности Сбербанка говорят о том, что оператор связи, допускает нарушение п. 9 ст. 46 закона «О связи» передавая сомнительные вызовы, в части невыполнения обязанности по передаче абонентского номера в исходном виде. Кроме того, оператор в случае выявления подобных нарушений обязан, согласно п. 10 этой же статьи, прервать трафик любых данных через свою сеть. Вместе с тем, за совершение вызовов с использованием подменного номера в российском законодательстве ответственность прямо не предусмотрена. Отсюда в целях скорейшего превентивного реагирования на рост преступлений, использующих подобные алгоритмы, целесообразно форсировать процесс по разработке и интегрированию соответствующих изменений в законодательство, которые бы детально регламентировали установление ответственности лиц, совершающих мошеннические действия, с одной стороны и не соблюдающих возложенные на них обязанности операторов связи — с другой. Наряду с этим необходимо реализовывать технический потенциал

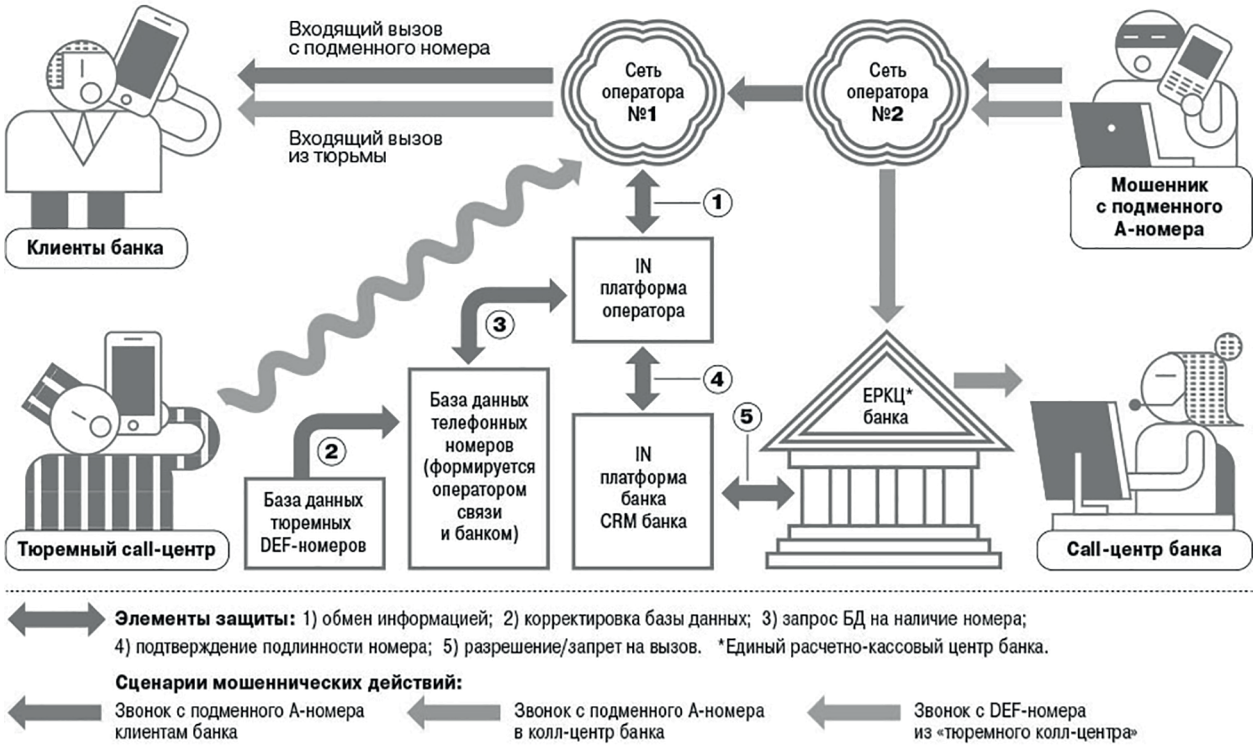

Рис. 1. Одна из примерных технологий хищения денежных средств при помощи социальной инженерии (источник: фотоархив ИД «Коммерсантъ»)

операторов сотовой связи по проверке любого подставного А-номера или случаев фейковой переадресации.

Дополнительным фактором безопасности способна стать идентификация номеров, начинающихся с цифр 8-800, данный номер должен быть закреплен за строго идентифицированным абонентом. Данный критерий должен быть одним из определяющим при допуске к трафику и находить отражение в нормативных актах Минкомсвязи.

Законодателем уже предприняты попытки правовой дефиниции мошенничества с использованием электронных средств платежа.

До недавнего времени ст. 159.3 УК РФ устанавливала ответственность за мошенничество с использованием платежных карт. Однако 23 апреля 2018 года ряд депутатов Государственной Думы РФ и членов Совета Федерации РФ посчитали необходимым внести следующие коррективы в нормы уголовного законодательства, предложив федеральный закон № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»: изменить наименование ст. 159.3 УК РФ и изложить ее в следующей редакции «Мошенничество с использованием электронных средств платежа».

Обратимся к действующему законодательству в части определения термина «электронное средство платежа». В соответствии со ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» под электронным средством платежа следует понимать средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств [2; 3].

При этом, несмотря на вышеуказанное определение «электронное средство платежа», законодатель посчитал нужным выделить такой состав, как «мошенничество, совершенное с использованием электронных средств платежа», закрепив его в примечании ст. 159.3 УК РФ в следующей дефиниции: «хищение чужого имущества, совершенное с использованием поддельного или принадлежащего другому лицу электронного средства платежа, в том числе кредитной, расчетной или иной платежной карты, путем обмана уполномоченного работника кредитной, торговой или иной организации» [1; 2].

Подобная новелла имеет следующие обоснование. Зачастую совершению преступления предшествует длительная и тщательная подготовка, включающая ряд трудно доказуемых и сложно выявляемых преступных деяний. Вместе с тем существенно усиливает степень общественной опасности данных деяний и специфика способа совершения преступления — использование средств удаленного доступа к банковскому счету, либо электронному кошельку при помощи современных технических решений (например, глобальная сеть Интернет предоставляет значительные возможности удаленного доступа к банковским счетам, электронным кошелькам и конфиденциальным данным пользователей, причем как в рамках совершения легитимных, так и противозаконных операций [1].

К вопросу о санкции за подобные деяния отечественный законодатель также отнесся очень внимательно, предложив ужесточить наказание с ареста до лишения свободы: в ч. 1 ст. 159.3 УК РФ слова «арестом на срок до четырех месяцев» заменить словами «лишением свободы на срок до трех лет».

Следует в числе прочего отметить, что части 2 и 3 ст. 159.3 УК РФ также подверглись ужесточению: в июле 2016 года федеральным законом № 325-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» [2; 3; 4] верхний предел санкции абз. 2 ч. 2 с четырех лет лишения свободы изменился до пяти лет, а в абз. 2 ч. 3 с пяти лет лишения свободы срок увеличили до шести лет. Таким образом, законодательство, предусматривающее ответственность за мошенничество с использованием электронных средств платежа, последовательно идет по пути ужесточения санкций за данный вид правонарушений.

Данное ужесточение следует признать обоснованным в свете стремительного роста данной группы правонарушений и усложнения способа их совершения. Данная тенденция служит основным стимулом ужесточения ответственности за мошеннические действия, особенно совершенные с использованием современных информационных технологий. При этом подобное ужесточение ответственности со стороны законодателя аргументируются как ответ на угрозы и вызовы криминального характера, неизбежно возникающие при возникновении и использовании новых форм банковского обслуживания. К числу названных угроз и вызовов можно отнести высокотехнологические формы хакерских атак, а также методы социальной инженерии, в результате

использования которых непосредственно владелец счета осуществляет перевод денежных средств злоумышленникам, либо сам сообщает им свои индивидуальные данные и конфиденциальную информацию [1].

Достаточно важно отметить, и тот факт, что изменению подверглась и сумма ущерба, которая позволяет признать мошенничество, совершенное с использованием электронных средств платежа, в крупном и особо крупном размерах — примечание к ст. 158 УК РФ. Так, крупным размером считается хищение, превышающее 250 тысяч рублей, а в особо крупным — 1 миллион рублей (ранее крупным размером признавалось более 1,5 миллионов рублей, а особо крупным — более 6 миллионов рублей). В этой связи становится очевидным вести речь об увеличении частоты применения данной законодательной нормы, поскольку нижний порог признание деяний преступными и совершенные с квалифицирующими признаками (в крупном и особо крупных размерах) является вполне реальным и достаточно распространенным.

Вместе с тем, помимо непосредственного хищения денежных средств с электронных средств платежа огромный пласт правонарушений составляют сбор, аккумулирование в электронных базах личных конфиденциальных данных граждан (номера счетов, адресные данные, доступ к аккаунтам в соцсетях, базам ГИБДД и т. д.) с последующей продажей злоумышленникам. Варианты и способы дальнейшего использования полученных преступниками конфиденциальных данных многовариантны и сложно прогнозируемы. Это может быть и описанная выше схема хищения средств при помощи социальной инженерии, и использование чужого аккаунта под предлогом сбора средств для помощи больным родственникам, использование чужого счета для транзита денежных средств при запутывании следов транзакции и т. п.

Все больше усложняются и используемые ранее схемы. Например, на сегодняшний момент появилась еще одна схема мошенничества: держателю карты звонят мошенники, представляясь сотрудниками службы безопасности банка, разговор идет со знанием технической терминологии и специфики работы службы безопасности банка. Звонок проходит с номера с московским кодом (не сотовым), номер телефона симметричный с нулями. Звонящий говорит приблизительно так: «Здравствуйте. Мы зафиксировали запрос на вывод средств с карты такому гражданину… на сумму… Это ваш запрос?».

Держатель карты данную информацию опровергает. Дальше мошенник предлагает блокировать карту, предупреждая о возможном мошенничестве, и приглашает в офис банка-эмитента, чтобы заблокировать карты и защитить свои деньги. Личных данных при этом не спрашивают.

В конце первого этапа мошенничества задаётся вопрос: «Картами каких банков вы ещё пользуетесь?». Владелец карты сообщает банки, картами которых он пользуется, на что мошенник отвечает следующей фразой: «Спасибо. Мы передадим информацию их службе безопасности, они с вами свяжутся».

Далее, буквально через минуту, поступает звонок якобы от службы безопасности второго банка, озвученного владельцем карты с номера, незначительно (часто даже на одну цифру) отличающегося от телефона колл-центра безопасности банка. Примерные вопросы, которые задают злоумышленники «Что Вас смущает?», «Вы хотите, чтобы мы проверили транзакции по Вашему счету?». Владелец карты объясняет, что ему звонили из другого банка, были какие-то мошеннические попытки, и сотрудники службы безопасности банка заблокировали их.

На это мнимый сотрудник службы безопасности второго банка говорит: «Мы сейчас проверим. Оставайтесь на линии» — и в телефоне включается музыка режима ожидания.

«Спасибо за ожидание. Мы проверили, у вас за последние полтора часа было несколько попыток списания средств на такие-то суммы, мы блокируем эти попытки. Надо будет посмотреть, где произошло списание, оставайтесь на линии» — опять ожидание с музыкой.

«Спасибо за ожидание. Вы подключались к общественным сетям — кафе, аэропорт, что-то такое?»

Собственник карты отвечает, «Да, подключался к общественному Wi-fi, например, в кафе».

На это ему отвечают: «Вот оттуда и прошло списание. Считывающее устройство, люди украли ваши персональные данные и попытались списать средства», далее создается видимость проверки данных, и мнимый сотрудник службы безопасности говорит: «У вас произошла утечка данных с телефона. Давайте мы сейчас вашу карту заблокируем и проведём проверку безопасности телефона. Заблокированную карту мы направим на перевыпуск и вы придёте в офис нашего банка с паспортом, заберёте свою карту и будете в безопасности. В какое отделение банка вам удобнее будет подойти?».

Человек указывает, в какое отделение банка ему будет удобнее подойти. Все реально, все соответствует настоящему банку, сленг и слова и действия — всё указывает на то, что это на самом деле служба безопасности банка.

Третьим этапом мошенничества является, как правило, предложение зайти в плеймаркет и установить приложение техподдержки якобы от банка, чью службу безопасности якобы представляет мошенник. И вот тут под видом проверки безопасности телефона предлагают установить приложение удаленного доступа к телефону. Например, тимвьювер или аналогичное. Как правило, подобное предложение происходит в середине разговора, после 10 или более минут переговоров как бы со службами безопасности нескольких банков в атмосфере полной аутентичности. К тому же, ради обеспечения безопасности человека, которому позвонили. Поверить, не усомниться и установить приложение в этих условиях очень легко.

Если приложение устанавливается — финал предсказуем: человек своими руками даёт удаленный доступ к своему телефону, в котором установлено какое-либо приложение онлайн-банка. Перевод денег с привязанной к телефону/приложению карты становится делом буквально пары секунд.

Отдельной группой правонарушений является использование скимминговых технологий и цифровых сканеров в людных местах с непосредственным снятием денежных средств либо с выпуском карты-двойника.

Заключение

Резюмируя вышеизложенное можно прийти к выводу о давно назревшей необходимости изменения законодательной позиции в отношении мошенничества, с использованием электронных средств платежа. Это позволит всесторонне подойти к вопросу финансовой глобализации в современном обществе, законному управлению информацией с использованием современного электронно-программного обеспечения.

Список литературы

1. Баранчикова, М. В. Использование официального документа как способ совершения мошенничества при получении выплат / М. В. Баранчикова // Уголовное право в эволюционирующем обществе : сб. науч. статей по мат. VII Межд. науч.-практ. конф. — Курск : Юго-Западный государственный университет, 2017. — С. 172—175.

2. Баранчикова, М. В. Использование служебного положения как способ совершения специальных видов мошенничества / М. В. Баранчикова // Закон и право. — 2018. — № 10. — С. 78—80.

3. Баранчикова, М. В. Особенности квалификации служебного мошенничества и его разграничение с коррупционными преступлениями / М. В. Баранчикова // Эволюция государства и права: история и современность : сб. науч. статей II Международной научно-практической конференции, посвященной 25-летию юридического факультета Юго-Западного государственного университета ; отв. ред. С. Г. Емельянов. — Курск, 2017. — С. 254—257.

4. Хисамова, З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа З. И. Хисамова // Государство и право. — 2015. — № 3 (33). — С. 127—132.

References

1. Baranchikova, M. V. Ispolzovanie ofitsialnogo dokumenta kak sposob sovershеniya moshennichestva pri poluchenii vyplat / M. V. Baranchikova // Ugolovnoe pravo v evolyutsioniruyushchem obshchestve : sb. nauch. statey po mat. VII Mezhd. nauch.-prakt. konf. — Kursk : Yugo-Zapadnyy gosudarstvennyy universitet, 2017. — S. 172—175.

2. Baranchikova, M. V. Ispolzovanie sluzhebnogo polozheniya kak sposob sovershеniya spetsialnykh vidov moshennichestva / M. V. Baranchikova // Zakon i pravo. — 2018. — № 10. — S. 78—80.

3. Baranchikova, M. V. Osobennosti kvalifikatsii sluzhebnogo moshennichestva i ego razgranichenie s korruptsionnymi prestupleniyami / M. V. Baranchikova // Evolyutsiya gosudarstva i prava: istoriya i sovremennost : sb. nauch. statey II Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy 25-letiyu yuridicheskogo fakulteta Yugo-Zapadnogo gosudarstvennogo universiteta ; otv. red. S. G. Yemelyanov. — Kursk, 2017. — S. 254—257.

4. Khisamova, Z. I. Kvalifikatsiya posyagatelstv, sovershennykh s ispolzovaniem elektronnykh sredstv platezha Z. I. Khisamova // Gosudarstvo i pravo. — 2015. — № 3 (33). — S. 127—132.

Дата поступления статьи в редакцию: 23.03.2020.