УДК 338.31

ОСОБЕННОСТИ ПРЕСТУПЛЕНИЙ В СФЕРЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

FEATURES OF CRIMES IN THE SPHERE OF NON-CASH PAYMENTS USING BANK CARDS

©Кашина Ю. А.,
Красноярский государственный аграрный университет,
г. Красноярск, Россия
©Kashina Yu.,
Krasnoyarsk State Agricultural University,
Krasnoyarsk, Russia

Аннотация. В работе показаны некоторые аспекты совершения преступлений в сфере электронной коммерции посредством банковских карт и показаны пути нормализации криминогенной ситуации. Одной из проблем современной платежной системы является мошенничество в сфере безналичных расчетов с использованием банковских карт. Решение проблемы должно начинаться с законодательного уровня. В частности, важно внести соответствие криминалистической и криминологической характеристик в законодательное определение мошенничества в данной сфере. Это будет способствовать четкой квалификации подобных преступлений.

Abstract. The paper shows some aspects of committing crimes in the field of electronic commerce through bank cards and shows the ways to normalize the criminal situation. One of the problems of the modern payment system is fraud in the sphere of cashless payments using bank cards. The solution of the problem should begin with a legislative level. In particular, it is important to bring the forensic and criminological characteristics in line with the legislative definition of fraud in this area. This will facilitate a clear qualification of such crimes.

Ключевые слова: электронная коммерция, банковский карты, экономические преступления, расследования, уголовное право, мошенничество.

Keywords: e-commerce, bank cards, economic crimes, investigations, criminal law, fraud.

За последние годы платежная индустрия России добилась впечатляющих результатов. На современном российском рынке электронных платежей заложен фундамент для дальнейшего динамичного развития, что имеет большое значение для отечественной экономики. Несмотря на стабильный и постоянный рост объемов электронных платежей, который сопутствует общему развитию российской экономики, сохраняется и целый ряд проблем, таких как ограниченный опыт обращения к банковским услугам у значительной части населения, внушительный объем «серого» рынка и общая ориентация экономики на использование наличных денежных средств. Как показывает практика, электронные системы платежей способствуют стимулированию потребительских расходов. Еще одна проблема заключается в том, что в связи с развитием рыночных отношений, резким увеличением количества банковских учреждений и предприятий различных форм собственности,

расширением объемов финансовых операций, в том числе расчетов с использованием банковских карт, значительно увеличилось и число преступлений в сфере экономики [1].

В последние годы этому бизнесу уделяют пристальное внимание как банки, стремящиеся активно развивать платежные сервисы для физических лиц, так и регуляторы рынка финансовых услуг [2, с. 44]. Связано это с наибольшим удобством для населения и соответственно увеличением скорости проведения транзакций. Электронные платежные системы и платежные терминалы стали привычным атрибутом повседневной жизни россиян.

В 2015 году в мире убытки от махинаций с банковскими картами выросли до 21 млрд долларов (для примера, в 2010-м они составляли около 8 млрд). К 2020 году, как ожидается, эта цифра может составить 31 млрд долларов. В эти убытки включены, помимо прочего, выплаты банков и кредитных компаний пострадавшим от мошенничества. Что заставляет кредитные организации вкладывать большие деньги в разработку технологий, защищающих от мошенничества (1).

Продавцы тоже несут убытки от киберпреступности. Система платежей на их сайтах должна соответствовать высоким стандартам безопасности. Если же нет - кредитные компании могут наложить на них штраф на сумму, которую клиент потерял, став жертвой мошенников.

Процессы криминализации электронных платежей тормозят развитие многих интеграционных процессов в экономике, которые в условиях кризиса являются инструментами выживания компаний и перехода их на новый качественный уровень. Это связано с тем, что денежная система пронизывает всю экономику, и проблемы в ней существенно влияют на эффективность в целом [3, с. 680-689]. Сегодня состояние платежных систем является фактором, влияющим на оценку динамики развития экономических систем. Существуют критерии развития региональных экономик, которые основываются на состояние их денежной системы, в том числе уровне развития электронной коммерции [4, с. 152-156]. Это является обоснованным, так как уровень развития электронных платежных систем — это качество и культура ведения бизнеса и комфортность развития предпринимательской среды в целом.

Наибольшую общественную опасность представляют не сами экономические преступления, а переход экономической преступности в совершенно новое качество, обусловливающее криминализацию экономической системы. Такое криминальное экономическое поведение субъектов хозяйствования становится условием их успешного функционирования. Преступления, совершаемые в сфере проведения безналичных расчетов с использованием банковских карт, относятся к качественно новому виду корыстной преступности в банковской сфере, которая непосредственно связана с модернизацией экономических отношений в обществе. В связи с этим изучаемая группа преступлений, получивших в статистических материалах название «преступления экономической направленности», может посягать как на собственность и другие экономические интересы государства, отдельных групп граждан (потребителей, партнеров, конкурентов), так и на порядок управления экономической деятельностью в целях извлечения наживы.

В Российской Федерации уровень потерь по картам оценить сложно, поскольку такая статистика не ведется ни Центральным банком, ни правоохранительными органами, ни какой-либо иной официальной и уполномоченной организацией, что существенно дискредитирует стандарты социальной защиты населения от подобного рода мошенничеств [5, с. 28-32]. По данным интернет-сайтов в 2016-м году мошенники украли из банкоматов 5 млрд рублей — вдвое больше, чем годом ранее. Ущерб увеличился из-за того, что в 2017-м

широкое распространение получили новые виды атак на устройства самообслуживания: заражение вирусами-шпионами и беспроводной скимминг, то есть размещение хакерского оборудования рядом с банкоматом (2).

Потребители все чаще стали оплачивать сервисы связи, такие как мобильную связь, доступ в интернет, платное ТВ и другие, либо с помощью мобильных приложений, либо на сайте оператора.

Наиболее крупные и устойчивые платежные сети в России – компания ОСМП (розничный бренд QIWI), ОАО «Киберплат», «Рапида», «ComePay», «Contact». Сервисы электронных платежей постоянно развиваются, предлагая все новые и новые виды услуг. Если в начале 2000-х годов основная часть платежей приходилась на оплату услуг операторов связи и интернет, то теперь лидеры рынка предлагают широкий спектр услуг — от традиционной оплаты услуг сотовых операторов, интернет - провайдеров, коммерческого телевидения, IP-телефонии до платежей в системах электронных денег, таких как WebMoney, PayPal, Яндекс. Через данные системы проходят денежные переводы, платежи по банковским кредитам, оплаты услуг ЖКХ, штрафов ГИБДД и техосмотра и др.

Любой из компонентов системы электронных платежей потенциально имеет уязвимости, вызванные как ошибками в настройке систем, не умением или нежеланием использовать более безопасные технологии и протоколы, так и ошибками в реализации механизмов защиты. В результате мошенники могут использовать эти слабые места для получения контроля над объектами систем электронных платежей.

Основными объектами «интереса» мошенников становятся платежные терминалы, серверы участников платежных систем — операторов и агентов, шлюзы в смежные платежные системы — банковские, системы электронных денег, денежных переводов.

Считывание секретной информации, хранящейся на карте, может производиться разными способами. Наиболее распространенный из них — это сговор мошенников с сотрудниками магазинов, отелей, ресторанов, других торговых и развлекательных предприятий (осуществление скимминга). Через такие компании проходит большое количество трансакций с пластиковыми картами, информация о которых сохраняется в компьютерных базах, данных компании или на слипах (бумажных документах, подтверждающих факт осуществления платежа). В результате информация о реквизитах карточек передается представителям криминальных структур. При этом платежную карту пропускают через специальное устройство (скимер) и считывают данные, которые хранятся на ее магнитной полосе. Мошенники получают своеобразный оттиск карты, и им уже ничего не стоит вписать в него необходимую сумму, подделать подпись, а все расчеты за операцию переадресовать на законного владельца карты [6, с. 24-26].

Бывает, что представители криминальных структур организуют собственные магазины. Цель их существования — получить как можно больше данных о пластиковых картах клиентов. Часто для этого используются и интернет-сайты. Защита от подобного рода угроз достигается традиционными методами: установка антивирусов, регулярные проверки, своевременное обновление, использование защищенных протоколов для удаленного управления, сетевая фильтрация, настройка конфигураций в соответствии с рекомендациями по безопасности для операционных систем, настройка журналов регистрации и их мониторинг. Канал связи между терминалом и платежной сетью необходимо шифровать и, кроме того, обеспечить аутентификацию при установлении сетевого соединения, как терминала, так и сервера, с которым он осуществляет взаимодействие.

В 2017 году мошенники придумали новый способ заработка – они звонят гражданам и представляются сотрудниками ФНС, сообщают о вымышленной задолженности и предлагают «решить вопрос» малыми средствами. Пострадавших от этого уже около 4 тысяч россиян (3).

Значительная доля мошеннических трансакций происходит через POS-терминалы, на втором месте – банкоматы, на третьем – электронная коммерция. Вместе с тем объем потерь через электронную коммерцию постоянно увеличивается: банки все активнее начинают заниматься интернет-эквайрингом. Большинство случаев мошенничества через банкоматы приходится на считывание данных, и передача информации преступникам (скимминг). За ним следуют физические атаки на банкомат (взлом или хищение) и установка вредоносного программного обеспечения.

Одной из существенных причин нападений на банкоматы может статься снижение затрат на охрану — банки снизили эту расходную статью в 2017 г. в связи с кризисом. Не исключено, что это приведет к дальнейшему увеличению количеств преступлений в сфере электронной коммерции.

Изучение географических особенностей преступлений, связанных с использованием банковских карт, показало, что традиционно самые высокие показатели по количеству скимминговых трансакций регистрируются в Москве и Санкт-Петербурге, где происходит более 50% случаев мошенничества.

Наличие данной криминологической особенности объясняется развитой инфраструктурой и большим количеством банкоматов. Сравнение аналогичного показателя с мировой практикой показывает, что удельный вес преступлений, связанных с незаконным снятием денежных средств в банкоматах, составляет лишь 5% всех эпизодов мошенничества. В остальных случаях целью преступников становятся покупки в магазинах и через сеть интернет. Это наносит существенный удар по сфере бизнесе. Особенно в российской экономике, в которой пока не проработаны методы защиты от подобных угроз [7, с. 43].

Говоря об угрозах в отношении платежных терминалов, важно помнить, что они включают в себя обычный, хоть и специальным образом защищенный и настроенный компьютер — чаще всего под управлением Windows или одной из версий Linux. Традиционные для обычных персональных компьютеров угрозы заражения вирусами актуальны и для платежных терминалов. В последнее время в банковской среде активно обсуждаются участившиеся случаи кражи секретных ключей клиентов интернет-банкинга с использованием троянских программ и последующие хищения денег клиентов. Очевидно, что терминалы как устройства для проведения платежей, достоверность которых также подтверждается цифровой подписью, являются приманкой для мошенников.

Также актуальна и угроза получения удаленного контроля над терминалом — анализируя внутреннюю логику установленного программного обеспечения, мошенники могут проводить платежи, создавать новых получателей платежей, вносить изменения в реквизиты получателей платежей или менять пользовательский интерфейс таким образом, что плательщик сам переведет деньги туда, куда нужно мошенникам, не подозревая об этом. Заражение терминала происходит и традиционными методами: через ручное обновление программного обеспечения, «флэшку», заражение базы обновлений на сервере и через локальную сеть в случае проводного подключения терминала.

Еще одним объектом внимания злоумышленников могут стать каналы связи между терминалами и сетью оператора платежной системы — как правило, это GPRS-каналы, проводные и WiFi-линии, связывающие терминалы с платежной сетью через Интернет. Если

канал связи недостаточно защищен, мошенники могут читать информацию о платежах, проводить повторные платежи за счет внедрения в канал связи скопированных кусков трафика или его повторения, изменять реквизиты совершаемых платежей и терминала.

С расширением спектра предлагаемых услуг, со сращиванием традиционных сервисов платежных систем с банковскими услугами, с увеличением сумм, проходящих через платежные системы, встал вопрос контроля за рисками при проведении подобных операций и обеспечением криминологической безопасности держателей банковских карт. В зависимости от условий, способствующих совершению рассматриваемых общественно опасных деяний в сфере проведения безналичных расчетов, производимых с использованием банковских карт, можно выделить две группы преступлений:

1) обусловленных технологическими рисками, связанными непосредственно со слабостями и уязвимостями используемых информационных систем и технологий;

2) имеющих своей причиной недостатки контрольной среды, обеспечивающей достоверность, надежность и корректность платежных операций. Любая система электронных платежей представляет собой совокупность вычислительных комплексов компьютеров, серверов, взаимодействующих посредством приложений и протоколов, связанных между собой через сети связи, нередко общедоступные, например, интернет.

В последние годы государство предприняло несколько последовательных шагов для урегулирования электронных платежей и банковских карт. С 2011 года действует федеральный закон *«О национальной платежной системе»,* который защищает в первую очередь физических лиц (4). Если у банка нет доказательств, что клиент нарушил правила использования электронного средства платежа, он должен возместить суммы, перечисленные со счета по несанкционированной транзакции. Кроме того, финансовые институты обязаны информировать клиентов о совершении каждой операции, иначе деньги придется вернуть вне зависимости от того, кто виноват в их утере. Со своей стороны, пострадавший гражданин для защиты своих прав обязан в течение суток после сомнительного списания уведомить кредитную организацию, что карта используется без согласия ее держателя.

Что касается юридических лиц, то в скором будущем банки смогут по простому заявлению *блокировать* на пять дней транзакции, совершенные без согласия плательщика. За это время получатель платежа должен предоставить его обоснование — копию договора или акт о выполненной работе.

Еще один *пакет поправок* к Уголовному кодексу РФ включает введение уголовного наказания за хищение денег с банковских карт и электронных кошельков. В настоящий момент статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации» предусматривает максимальное наказание за подобное преступление в виде ареста на четыре месяца. Поправки дополнят статью понятием «хищение средств с банковского счета и электронных денежных средств», введут ответственность за мошенничество с использованием электронных средств платежа, в том числе поддельных или украденных пластиковых карт. Максимальной мерой наказания за подобные преступления станет лишение свободы на три года. Одновременно предлагается ввести уголовную ответственность за получение обманным путем доступа к коммерческой, налоговой или банковской тайне. Среди прочего, это и код доступа к интернет-банку, который доверчивые граждане сообщают мошенникам по телефону.

В 2018 году Госдума приняла во втором чтении законопроект об усилении уголовного наказания за хищение средств с банковских карт. Согласно тексту пояснительной записки к законопроекту, он направлен на повышение уголовно-правовой защиты граждан и организаций за счет усиления уголовной ответственности за хищение чужого имущества, совершенное с банковского счета, а также электронных денежных средств посредством дополнения статьи «Кража» УК РФ. В документе также отмечается, что поправки к закону закрепляют уголовную ответственность за хищение чужого имущества с использованием поддельного или чужого электронного средства платежа, включая кредитную, расчетную или иную платежную карту путем обмана работника кредитной, торговой или иной организации. Санкция дополняется наказанием в виде лишения свободы сроком до трех лет.

Подавляющее число преступлений в сфере проведения безналичных расчетов, с использованием банковских карт связано с совершением мошеннических действий. Однако классическое уголовно-правовое понятие мошенничества не совпадает с его криминологическим аналогом, то есть понятие мошенничества, используемым в банковской сфере при эксплуатации международных платежных систем. Если в описательной диспозиции ст. 159 УК РФ под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, то криминологическое понятие «мошенничество в сфере проведения безналичных расчетов с использованием банковских карт» имеет несколько иное, более узкое значение (5). Так, платежные системы под мошенничеством понимают любые потери в результате каких-либо противоправных действий, так как, с их точки зрения, мошенническая операция – это операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная держателем. Использование чужой платежной карты — это не всегда следствие злоупотребления доверием. Гораздо чаще завладение картой другого держателя происходит другими способами. В 2012 году была введена специальная статья 159.3, отражающая мошенничество с банковскими картами. Согласно данной статье «мошенничество с использованием платежных карт - это есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации». Однако данное определение не в полной мере отражает криминологический характер мошенничества с банковскими картами. Ведь указанное мошенничество может осуществляться не только путем обмана банка, но и посредством введения в заблуждение самого держателя. Кроме того, возникают ситуации, когда держатель под воздействием мошеннического обмана подтвердил какое-либо действие, а затем объявил о том, что оно совершено без его согласия. Словом, исследования видов мошенничеств, то есть выявление криминологического состава является основой для ввода или корректировки специальных статей Уголовного кодекса.

В УК РФ также отсутствуют специальные нормы, предусматривающие уголовную ответственность за такие распространенные в настоящее время виды карточного мошенничества, как скимминг, фишинг и др.

В связи с этим в целях привлечения виновных лиц к уголовной ответственности и назначения справедливого уголовного наказания за противоправные деяния в области платежных карт необходимо не столько оперировать терминологией платежных систем, сколько суметь квалифицировать указанные деяния с точки зрения УК РФ.

Немаловажную роль в расследовании таких преступлений должна занимать судебная экспертиза, которая должна быть дополнена новыми направлениями — расследования и криминологическая экспертиза преступлений в сфере цифровой экономики [8, с. 425-428]. Сегодня остро встает вопрос как о классифицировании преступлений в области цифровой экономики, так и о подготовке специалистов в этом новом направлении, для которого пока не выделено отдельного направления в образовательных программах [9, с. 311-313].

Многочисленные случаи мошенничества существенно подрывают доверие к системам электронных платежей, поэтому дальнейшее успешное развитие национальной платежной системы невозможно без разработки и внедрения эффективных приемов и методов предупреждения этих преступлений как общими, так и специальными субъектами, что требует комплексного подхода к решению указанных проблем и обусловливает необходимость исследования вопросов, связанных с совершенствованием противодействия преступлениям, совершаемым в сфере проведения безналичных расчетов с использованием банковских карт.

Источники:

(1). Как не стать жертвой мошенничества с кредитными картами. URL: https://clck.ru/DLKuj (дата обращения: 09.04.2018).

(2). Мошенники атаковали российские банкоматы 5 тыс раз в 2017 году. URL: https://clck.ru/DLK7s. (дата обращения: 09.04.2018).

(3). Мошенники в 2016 году украли с банковских карт россиян 650 млн рублей. URL: https://clck.ru/DLK9H (дата обращения: 09.04.2018).

(4). Федеральный закон «О национальной платежной системе» от 27.06.2011 N 161-ФЗ (Редакция от 18.07.2017).

(5). Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 19.02.2018).

Sources:

(1). How not to become a victim of credit card fraud. URL: https://clck.ru/DLKuj (reference date: 04/09/2018).

(2). Scammers attacked Russian ATMs 5 thousand times in 2017. URL: https://clck.ru/DLK7s. (date of circulation: 04/09/2018).

(3). Scammers in 2016 stole 650 million rubles from Russian bank cards. URL: https://clck.ru/DLK9H (reference date: 04/09/2018).

(4). Federal Law "On the National Payment System" of 27.06.2011 N 161-FZ (Revision of 18.07.2017).

(5). The Criminal Code of the Russian Federation of June 13, 1996, No. 63-FZ (as amended on 19.02.2018).

Список литературы:

1. Айснер Л. Ю., Ерошина А. А., Жулаева А. С., Лущаева Г. М., Иванова Н. Г., Коренева В. В., Король Л. Г., Малимонов И. В., Сторожева А. Н., Дадаян Е. В., Трашкова С. М., Шепелева Ю. С., Щебляков Е. С., Рахинский Д. В., Синьковская И. Г. Актуальные психолого-педагогические, философские, экономические и юридические проблемы современного российского общества. Ульяновск, 2017.

2. Ерещенко М. А., Холопов А. А., Сочнева Е. Н. Транснационализация экономики России // Постулат. 2017. №5-1 (19). С. 44.

3. Сочнева Е. Н., Воронин Е. А., Зябликов Д. В. Социально-экономическая политика Красноярского края как региона инновационного развития // Сибирский журнал науки и технологий. 2017. Т. 18. №3. С. 680-689.

4. Сочнева Е. Н., Белякова Г. Я. Классификационные признаки регионов сырьевой направленности // Конкурентоспособность в глобальном мире: экономика, наука, технологии. 2017. №3-1 (32). С. 152-156.

5. Сочнева Е. Н., Федотов В. М. Внедрение международных стандартов в России // The Newman in Foreign Policy. 2016. №33 (77). С. 28-32.

6. Савельев С. Д. Ответственность за преступления в совершенные с помощью сети «Интернет» // Российская юстиция. 2016. №1. С. 24-26.

7. Ерещенко М. А., Холопов А. А., Сочнева Е. Н. Сравнительный анализ поддержки малого и среднего бизнеса в России и экономически-развитых странах Европейского союза // Постулат. 2017. №5-1 (19). С. 43.

8. Цугленок Н. Н., Дадаян Е. В., Сторожева А. Н. К вопросу о перспективах развития кафедр международного института судебных экспертиз и права // В сб.: Наука и образование: опыт, проблемы, перспективы развития Материалы международной научно-практической конференции. 2012. С. 425-428.

9. Рахинский Д. В., Король Л. Г., Малимонов И. В., Шепелева Ю. С. Процесс обучения и современные информационные технологии // В сб.: Проблемы современной аграрной науки. Материалы международной заочной научной конференции. 2010. С. 311-313.

References:

1. Eisner, L. Yu., Eroshina, A. A., Zhulaeva, A. S., Lushchaeva, G. M., Ivanova, N. G., Koreneva, V. V., Korol, L. G., Malimonov, I. V., Storozheva, A. N., Dadayan, E. V., Trashkova, S. M., Shepeleva, Yu. S., Shcheblyakov, E. S., Rakhinsky, D. V., & Sinkovskaya, I. G. (2017).Topical psycho-pedagogical, philosophical, economic and legal problems of modern Russian society. Ulyanovsk.

2. Ereshchenko, M. A., Kholopov, A. A., & Sochneva, E. N. (2017).Transnationalization of the Russian economy. *Postulate,* 5-1 (19). 44.

3. Sochneva, E. N., Voronin, E. A., & Zyablikov, D. V. (2017). Socio-economic policy of the Krasnoyarsk Territory as a region of innovative development. *Siberian Journal of Science and Technology, 18* (3). 680-689.

4. Sochneva, E. N., & Belyakova, G. Ya. (2017). Classification attributes of the regions of raw materials orientation. *Competitiveness in the global world: economics, science, technology, 3-1* (32). 152-156.

5. Sochneva, E. N., & Fedotov, V. M. (2016). Introduction of international standards in Russia. *The Newman in Foreign Policy, 33* (77). 28-32.

6. Savelyev, S. D. (2016). Responsibility for crimes committed with the help of the Internet network. *Russian Justice,* (1). 24-26.

7. Ereshchenko, M. A., Kholopov, A. A., & Sochneva, Ye. N. (2017). Comparative analysis of support of small and medium business in Russia and the economically-developed countries of the European Union. *Postulate, 5-1* (19). 43.

8. Tsuglenok, N. N., Dadayan, Ye. V., & Storozheva A. N. (2012). On the issue of perspectives for the development of the departments of the international institute of forensic

examinations and law. *In: Science and Education: Experience, Problems, Development Prospects practical conference,* 425-428.

9. Rakhinsky, D. V., Korol, L. G., Malimonov, I. V., & Shepeleva, Yu. S. (2010). The learning process and modern information technologies. In: *Problems of modern agrarian science. Materials of the international correspondence scientific conference,* 311-313.

Работа поступила
в редакцию 19.04.2018 г.

Принята к публикации
23.04.2018 г.

Ссылка для цитирования:

Кашина Ю. А. Особенности преступлений в сфере безналичных расчетов с использованием банковских карт // Бюллетень науки и практики. 2018. Т. 4. №5. С. 574-582. Режим доступа: http://www.bulletennauki.com/kashina (дата обращения 15.05.2018).

Cite as (APA):

Kashina, Yu. (2018). Features of crimes in the sphere of non-cash payments using bank cards. *Bulletin of Science and Practice, 4*(5), 574-582.