**ЗАЩИТА ОТ СКИММИНГА И ДРУГИХ ФОРМ БЕСКОНТАКТНОГО МОШЕННИЧЕСТВА**

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| Введение | 3 |
| 1. Механизм преступлений с пластиковыми картами: понятие и виды | 5 |
| 2. Обстановка в сфере обращения банковских пластиковых карт в России | 8 |
| 3. Обстановка в сфере обращения банковских пластиковых карт в зарубежных странах | 14 |
| 4. Меры по предотвращению мошенничества с пластиковыми картами | 17 |
| 5 Регистрация и использование электронных средств платежа, а также противодействие мошенничеству и краже | 19 |
| Заключение | 27 |
| Список использованных источников | 30 |

**Введение**

В наши дни, в отличие от последних нескольких лет, меньше людей хранят большие деньги дома или переносят их в сумку или карманы, потому что они боятся, что их квартира будет ограблена или они вырвут сумку на улице. Поэтому больше людей, для обеспечения безопасности своих сбережений и удобства использования средств, все чаще прибегают к банковским услугам. Сегодня банки могут предоставлять широкий спектр услуг для долгосрочных и краткосрочных депозитов наличными, открывая счета. Банковские карты пользуются большой популярностью. В современном обществе почти каждый человек имеет одну или несколько банковских карт определенного банка. Это связано с удобством их использования: легко снимать и вкладывать деньги на такую карту, оплачивать дорогостоящую карту в магазине и при необходимости переводить деньги на другую карту.

Развитие платежных систем является характерной чертой современного мира. В настоящее время коммерческие организации не могут быть представлены без выпуска, внедрения и обслуживания банковских карт. Однако, несмотря на то, что иностранные банки уже давно используют карточную систему, этот инструмент недавно вышел на первый план. Тем не менее, банковские карты являются неотъемлемой частью не только нашей жизни, но и удобным инструментом в области мошенничества.

Это оправдывается тем фактом, что в этой области есть возможность действовать, не только не привлекая внимания, но часто даже не выходя из собственного дома. Мошенникам не нужно обладать определенными навыками, достаточно просто найти информацию в Интернете, которая есть огромная сумма, или купить необходимое оборудование и специальные программы.

В мире развитых технологий, человечеству с каждым днём становится всё труднее отказаться от появления новых сервисов дистанционного банковского обслуживания. Многочисленные компании каждый год разрабатывают и вводят новые системы защиты, а представители криминального мира пытаются найти способы, чтобы обойти эту защиту.

Конечно, если проявить упорство, можно найти средство борьбы с любой системой защиты, но, обычно, на это требуется много затрат. Намного легче ввести в заблуждение человека, не следящего за развитием современных технологий и не знающего всех тонкостей этой сложной системы.

Но мошенники тоже идут в ногу со временем. Количество людей, желающих украсть деньги с таких счетов, безусловно, велико. Мошенники пытаются узнать данные вашей карты и ее пароль, чтобы завладеть деньгами, лежащими на карте. Так появился скимминг.

Скимминг – (от англ. skim – снимать сливки) – это кража данных карт при помощи специального считывающего устройства (скиммера). Злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код), узнать ПИН-код можно с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах. Так же скимминг трактуют как установку на банкоматы нештатного оборудования, которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковский карты и вводимый ПИН-код) для последующего хищения денежных средств со счета банковской карты.

Стать жертвой скимминга можно не только снимая наличные, но и оплачивая покупки в торговых точках.

При развитии информационных систем и технологий возрастает уровень преступлений в данной сфере. В условиях роста объема эмиссии банковскиих карт и количества банкоматов актуализируются проблемы обеспечения безопасности последних. Среди наиболее распространенных методов, с помощью которых мошенники пытаются добыть наличность из банкоматов, выделяются такие, как:

- «мошеннический ПИН-ПАД»,

- «фишинг»,

- «щипачество»,

- «Ливанская петля» («траппинг»),

- «кардинг»,

- «кибератака»,

- «скимминг» и др.

Целью работы является изучение скимминга и других форм мошенничества с банковскими картами в Российской Федерации, а также способов борьбы с данным видом преступления.

Для достижения поставленной цели следует решить такие задачи, как:

- определить понятие «скимминг» «траппинг» «Ливанская петля» и др.;

- охарактеризовать виды мошенничества с банковскими картами;

- дать характеристику данному составу преступления;

- выявить проблемы в национальном законодательстве;

- выработать предложения по усовершенствованию законодательства в области обеспечения безопасности банкоматов и банковских карт.

**1 Механизм преступлений с пластиковыми картами: понятие и виды**

Сегодня как в России, так и в западных странах нам более распространенным способом компрометации банковских карт в банкоматах является «скимминг» – разновидность ATM-преступлений с пластиковыми картами. Скимминг карты – это действия, направленные на похищение информации путём ее считывания с пластиковых карт, в момент, когда жертва расплачивается либо обналичивает денежные средства.

Происходит данное понятие от слова скиммер. Скиммером, называют гаджет, созданный из электромагнитных материалов и вмонтированный в устройство для считывания информации с карт с магнитной полосой. Подобные гаджеты нередко появлялись и раньше у мошенников. Причины скимминга заключаются в большом росте оплаты через банковские карты. Из-за него возрастает и количество различных денежных терминалов. Модели таких устройств не являются совершенными в плане безопасности и часто попадают в поле зрения хакеров. Все эти действия и методы, направленные на кражу информации с банковских карточек, называются фишинг. Устройства самостоятельно изготавливаются злоумышленниками из магнитных считывателей, батареи питания и небольшой микросхемы. Внешне такие гаджеты маскируют под деталь банкомата.

Среди разновидностей скимминга следует выделить наиболее распространенные: фиктивные пункты выдачи денежных средств; проникновение через сеть в процессинговые центры; подключение к POS-терминалам в торговых точках; накладки на клавиатуре банкоматов, мини-камеры и т.д.

Действительность такова, что жертвой скимминга может стать практически любой участник денежных отношений, который пользуется банковской картой. Чаще всего скиммер имитирует накладку для прорези, куда вставляется банковская карта. После того, как ничего не подозревающий гражданин решит обналичить средства и вставит в такой «заражённый» банкомат карточку, сначала сработает считывающие устройство злоумышленника.

После того, как все операции будут завершены, и владелец получит назад свою карту, считанные данные попадут на флэшку мошенника. Обработав всю считанную информацию, её наносят на магнитную полоску, наклеенную на кусок пластика, то есть делается дубликат карты. Но этого порой недостаточно для кражи денег с карты. Любая информация, а уж тем более доступ к личному счёту охраняются паролем. Для банковских карт это пин-код, состоящий из четырёх цифр. Для того, чтобы его похитить, злоумышленникам нужны дополнительные скимминг устройства. Обычно, они представляют собой накладку на клавиатуру банкомата либо миниатюрные камеры.

Поэтому целесообразно выделить основные причины и особенности скимминга:

1) наблюдаемый рост скимминг-атак на банкоматы коррелирует с «техническими» причинами, среди которых выделяют: относительно невысокую степень защищенности банковских карт, которые оснащены магнитной полосой (по оценкам экспертов, их количество на рынке пластиковых карт составляет порядка 80% от общей массы).

Поэтому наиболее предпочтительны карты со встроенными чипами, способными обеспечить более высокий уровень защиты и др. «Знаковым в этом отношении событием стало решение Сбербанка России перейти с 1 июля 2013 г. к эмиссии банковских карт, оснащенных исключительно чипами, существенно повышающими безопасность электронных средств платежа»;

2) рассматриваемая разновидность преступлений стала относительно новым и не до конца изученным явлением, поэтому при выявлении и расследовании уголовного дела по факту скримминг-атаки возникают определенные сложности.

Это обусловлено рядом объективных обстоятельств: значительный временной промежутком между обнаружением владельца карты и факта совершенного посягательства, проведения проверочных мероприятий по ситуации, изложенной в заявлении, принятием решения о возбуждении уголовного дела и его расследованием с одной стороны, и довольно оперативными действиями мошенников;

3) высокий уровень технической подготовки злоумышленников. Для подделки пластиковой банковской карты и получения ее PIN-кода, как правило, мошенники используют следующие высокотехнологичные устройства: эмбоссер, при помощи которого возможно нанести надпись на пластиковую основу банковской карты; тайпер – устройство, позволяющее «впаивать» магнитную пленку на пластиковую заготовку карты; энкодер, через который можно записать полученные сведения на банковскую карту; скиммер – устройство, позволяющее считывать информацию, в дальнейшем заносимую на ЭВМ для последующей обработки.

Кроме скимминга выделяют также и другие механизмы для совершения преступлений с банковскими картами, например фишинг.

Фишингом является [атака](https://ssd.eff.org/ru/glossary/%D0%B0%D1%82%D0%B0%D0%BA%D0%B0), при которой [злоумышленник](https://ssd.eff.org/ru/glossary/%D0%B7%D0%BB%D0%BE%D1%83%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA) отправляет на первый взгляд безобидное электронное письмо или ссылку, являющуюся на самом деле вредоносной. Фишинговые атаки являются распространённой формой заражения компьютеров вредоносными программами, то есть программами, которые скрывают своё присутствие на компьютере и могут быть использованы удалённо для управления заражённым компьютером, кражи информации или слежки за пользователем.

Злоумышленник, как правило, составляет фишинговое сообщение так, чтобы мотивировать вас открыть ссылку или вложенный файл, которые могут содержать [вредоносный код](https://ssd.eff.org/ru/glossary/%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D0%B5-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B). Для фишинга может также использоваться интернет-чат. Поэтому важно проверять ссылки, получаемые по электронной почте или в чате.

Веб-адреса в электронных письмах могут быть обманчивыми. Представленный в письме веб-адрес может содержать ссылку на совершенно другой веб-сайт. Для того, чтобы увидеть настоящий прописанный в ссылке адрес, на неё необходимо навести курсор.

Некоторые злоумышленники используют доменные имена, похожие на веб-адреса популярных сервисов, чтобы вас «одурачить»: <http://wwwcnn.com/> и <http://www.cnn.com/> – это не одно и то же!  Многие используют сокращение URL для создания коротких ссылок, но это позволяет маскировать заражённые адреса. Если вы получили сокращённый URL, например созданный t.co на Твиттер, попробуйте проверить его реальный адрес при помощи сервиса <http://www.checkshorturl.com/>.

Существует ещё один способ обмана, при котором вы получаете ссылку на файл, якобы расположенный на таком сервисе, как Google Docs или Dropbox. При переходе по ссылке на экране вы видите аналог страницы входа на соответствующий сервис, предлагающий вам ввести своё имя пользователя и пароль. Но вполне возможно, что ссылка увела вас на поддельный сайт, содержащий копию страницы входа.

Таким образом, если вы перешли по ссылке, прежде чем вводить пароль, проверьте адресную строку вашего веб-браузера. Она отображает реальный адрес страницы.

Наиболее интересным видом мошенничества является «Траппинг». Trapping – «ливанская петля» – мошенничество, которое предполагает изъятие карты у владельца весьма бесхитростным способом. Если большинство вариантов мошенничества с банковскими картами имеют цель лишь получить их реквизиты при помощи различных программно-аппаратных ухищрений для последующего опустошения счетов, то цель этого способа – получение самой пластиковой карты.

Этот экзотичный метод был изобретен в Ливане, отсюда и его название.

В картридер банкомата мошенник помещает так называемую «ливанскую петлю», которая представляет собой блокиратор из фотопленки (что-то вроде ловушки). Пользователь банковских услуг, вставляя карту в банкомат, в реальности вставляет ее в заранее подготовленный «конверт» из пленки, в котором она «благополучно» застревает.

Естественно, владелец застрявшей карточки начинает переживать и пребывать в легкой панике.

Как правило, в этот момент «неравнодушный человек» находится рядом (возможно, он даже будет переодет в форму сотрудников банка) и предлагает проделать ряд операций для спасения карточки, в том числе повторить ввод пин-кода.

Естественная паника клиента банка, «квалифицированный советчик», который «случайно» оказывается рядом и активно пытается помочь – все ведет к тому, что в определенный момент, клиент банка набирает пин-код при мошеннике. Результат: банковская карта находится в заранее установленной «ловушке», а пин-код становится известен мошеннику. После всех манипуляций мошенник советует составить заявление о возврате карты в отделении банка. Как только владелец карты уходит от банкомата, мошенник оперативно извлекает карту вместе со своим «конвертом» из пленки. Несколько минут – и карта оказывается полностью пустой.

Если в момент манипуляций с картой у банкомата пин-код не удалось узнать, мошенник все равно забирает карту и тратит средства с нее в любой торговой сети.

Следующим приёмом злоумышленников является «вишинг». Вишинг (англ. vishing) - относительно новый вид мошенничества - голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию, такую как номера карт и счетов.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию: автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции - перезвонить по определенному номеру немедленно. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, часто представляется вымышленным именем от лица финансовой организации; когда по этому номеру перезванивают, на другом конце провода отвечает типично компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона; как только номер введен, вишер становится обладателем всей необходимой информации (номер телефона, полное имя, адрес), чтобы, к примеру, обложить карту штрафом; затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как PIN-код, срок действия карты, дата рождения, номер банковского счета и т.п.

В конце 2012 - начале 2013 гг. мошенники несколько усовершенствовали этот способ, правда это «усовершенствование» направлено на самых доверчивых людей. Состоит он в следующем:

Используя базы данных компаний мобильной связи, жулики массово рассылают SMS примерно следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру...». Естественно, указывается номер телефона мошенника. Некоторые граждане, вместо того, что бы сразу обратиться в ближайший офис своего банка для проверки поступившей информации, либо позвонить в службу клиентской поддержки, перезванивают по указанному в SMS номеру. Мошенник представляется «сотрудником банка» или «отдела безопасности банковской системы платежей и переводов».

Под предлогом разблокирования карты, злоумышленник выясняет у гражданина, подключена ли к его счету услуга «Мобильный банк» и, если такая услуга подключена, мошенник обманным путем выясняет у владельца номер банковской карты, срок ее действия и персональный код. Затем под предлогом разблокирования получает согласие от потерпевшего на осуществление операций по карте, и через Интернет похищает деньги с его счета путем безналичного перевода на другие счета.

Если же услуга «Мобильный банк» не подключена, мошенник в ходе телефонного разговора предлагает гражданину подойти к ближайшему банкомату и осуществить ряд неких операций, вводя его в заблуждение и переводя деньги на абонентские номера телефонов сотовой связи либо на другие банковские счета. Такое жульничество становится возможным только из-за простой неосведомленности держателей карт о том, что ни одна организация, включая банк, не вправе требовать ПИН-код или реквизиты банковской карты.

Но совершенству, как известно, предела нет: в 2015-2016 гг. злоумышленники стали применять для получения данных карт банковских клиентов так называемые внешние интерактивные голосовые ответы (IVR).

В рамках этой схемы гражданам звонят не сами мошенники, а запрограммированные ими роботы, которые представляются сотрудниками банков и выуживают необходимую информацию. Схема работает, так как автоматизированные программы вызывают доверие у населения. По данным компании Zecurion, специализирующейся на вопросах безопасности дистанционного банковского обслуживания, за год — с апреля 2015 года по апрель 2016-го — с помощью IVR мошенники украли с банковских карт россиян 6 млн рублей.

Как правило, мошенники запускают роботизированные программы в облачных дата-центрах — чтобы cкрыть следы (по IP-адресам злоумышленников вычислить проще), а чтобы у собеседников не возникло подозрений, системы направляют их и на живых «сотрудников».

**2 Обстановка в сфере обращения банковских пластиковых карт в России**

Практика изучения мошенничества показывает, что наибольшей популярностью у преступников пользуется скиммер. Перед ридером банкомата монтируется устройство, считывающее информацию с магнитной полосы карты при ее введении в банкомат.

Мошенники используют скиммер – устройство для считывания данных карты с магнитной дорожки платежной карты. Для данной мошеннической схемы используется целый набор скимминговых устройств:

- устройство для считывания магнитной дорожки пластиковой карты, которое устанавливается в картоприемник или в картридер, находящейся при входе в зону обслуживания помещения банка для клиентов;

- мини-камера, установленная на банкомате, направленная на клавиатуру ввода.

Обобщая сказанное, следует отметить, что основная цель установки накладных клавиатур, мини видеокамер и скиммеров заключается в том, чтобы считать закодированную на магнитной полосе информацию и персональный код владельца пластиковой банковской карты. Похищенная таким несанкционированным способом информация, как правило, наносится на другие карты и используется вместе с соответствующими персональными идентификационными номерами для получения наличных в банкоматах.

Первые модели банкоматных скимминг-устройств были достаточно примитивны. Изготавливалось всё вручную, поэтому внимательно присмотревшись, можно было сразу определить, что на картоприёмнике установлена накладка. Нередко, первые скиммеры вызывали затруднения в работе самих банкоматов.

Сегодня, с общим развитием технологий, устройства считывания достаточно прогрессировали. Найденные образцы техники, тоньше картонного листа, а миниатюрный лазерный скимминг-считыватель информации с магнитных полос позволяет размещать его внутри картоприёмника.

Банкоматный скимминг – более распространённый тип кражи информации в странах третьего мира. Это связано с тем, что подделать детали на терминалах и установить их достаточно просто и быстро, а население практически не использует никаких средств защиты.

В связи с переходом коммерческих банков в РФ на международный стандарт микропроцессорных чиповых карт EMV количество случаев скимминга в нашей стране начиная начало постепенно сокращаться.

Анализ судебно-следственной практики показывает, что скимминг выступает начальным этапом в общей цепи последовательных преступных деяний по получению денежных средств с банковской карты, в силу чего в действиях преступников зачастую обнаруживаются признаки составов преступлений, предусмотренных ст. 183 УК РФ и ст. 187 УК РФ [1]. Преступная схема может быть представлена в виде триады деяний: сбор информации о банковской карте – изготовление поддельного платежного инструмента на основе полученных сведений – хищение денежных средств.

Современная правоприменительная практика рассматривает скимминг лишь как сопутствующее явление более тяжких преступлений, в результате чего происходит недооценка общественной опасности деяния, что делает данную разновидность преступлений одной из самых популярных. Поэтому лишь правильная квалификация и своевременное выявление способны существенно повлиять на уровень преступлений в сфере безналичных расчетов, в связи с чем, представляется необходимым выделение нескольких вопросов квалификации рассматриваемого явления.

Сейчас существует процесс оплаты бесконтактной банковской картой. Не нужно ничего никуда засовывать, вспоминать PIN-код, корябать чеки плохо пишущей ручкой, не говоря уже о том, чтобы отсчитывать купюры и копаться по карманам в поисках мелочи. Приложил — и готово, свободен! Только вот простота совершения покупки заставляет задуматься: а что, украсть деньги с карты так же просто? Провел ридером по карману — и привет, средства, нажитые непосильным трудом?

Бесконтактные банковские карты используют для передачи данных технологию NFC, разновидность RFID. На карте размещены чип и антенна, которые «откликаются» на запрос платежного терминала на радиочастоте 13,56 МГц. Разные платежные системы используют собственные стандарты: Visa payWave, MasterCard PayPass, American Express ExpressPay и так далее. Но устроены они похожим образом.

Дальность передачи данных через NFC составляет несколько сантиметров. Поэтому первый барьер защиты — физический. Считыватель, по сути, необходимо приложить вплотную к карте, что довольно сложно сделать незаметно.

Зато можно сделать нестандартный ридер, который работает на большей дистанции. Например, исследователи из британского Университета Суррей продемонстрировали возможность считывания по NFC данных на расстоянии до 80 см с помощью компактного сканера.

Такое устройство вполне может незаметно «опрашивать» бесконтактные карты в общественном транспорте, торговых центрах, аэропортах и тому подобных местах скопления людей. Благо в некоторых странах подходящие карты лежат в бумажнике уже у каждого второго гражданина.

Впрочем, можно пойти еще дальше и обойтись вовсе без сканера и личного присутствия. Еще одно оригинальное решение проблемы расстояния предложили испанские хакеры Рикардо Родригес и Хосе Вилла, представившие доклад на недавней конференции Hack In The Box. Большинство современных Android-смартфонов оснащены модулем NFC. При этом смартфоны нередко оказываются физически рядом с бумажником — например, в одной сумке. Родригес и Вилла создали концепт Android-троянца, который превращает смартфон жертвы во что-то вроде ретранслятора NFC-сигнала.

Как только зараженный телефон оказывается возле бесконтактной карты, он отправляет через Интернет злоумышленникам сигнал о доступности транзакции. Мошенники активируют обычный платежный терминал, подносят к нему свой NFC-смартфон. Таким образом создается «мост» через Интернет между NFC-карточкой и NFC-терминалом, удаленными друг от друга на любое расстояние.

Троянец может распространяться стандартным способом, например в комплекте со «взломанным» платным приложением. Все, что требуется, — это версия Android 4.4 и выше. Root-доступ необязателен, хотя и желателен для того, чтобы троянец мог работать и после блокировки экрана.

Так что же, получается, что мошенническая NFC-транзакция неизбежно будет задержана банком или платежной системой? Скорее всего, да, если в этой схеме не задействованы недобросовестные работники на стороне банка.

Но есть и еще одна неприятная возможность. Через NFC можно украсть не «саму транзакцию», а информацию о банковской карте.

Стандарт EMV допускает хранение определенных данных в незашифрованном виде в памяти чипа карты. К таким данным могут относиться номер карты, несколько последних совершенных операций и так далее (какая именно информация и как хранится в чипе, определяют банк-эмитент и платежная система). Эти данные можно считать с помощью NFC-смартфона, установив на него вполне легальное приложение (например, Banking card reader NFC — можете сами поэкспериментировать со своими картами).

До сих пор считалось, что эта открытая информация не ставит под угрозу безопасность карты. Однако авторитетное британское издание для потребителей «Which?» выступило с неожиданным опровержением этого тезиса.

На сегодняшний день в России используется две технологии бесконтактной оплаты — PayWave от VISA и PayPass от MasterCard. Карты по технологии MasterCard выпускает 43 крупных российских банка, 16 банков используют ноу-хау от Visa. Картами с бесконтактной технологией оплаты товаров пользуется около двух миллионов россиян.

Суть данной мошеннической схемы схожа с технологией сканирования сигналов электрозамков автоугонщиками. Как сообщили рассказали «Ридусу» в Zecurion, средства с карт PayPass и PayWave списываются мошенниками с помощью самодельных ридеров, способных сканировать банковские карты с чипами RFID. По сути, это аналоги обычных бесконтактных PoS-терминалов: RFID-ридеров, посылающих электромагнитные сигналы.

Современную платежную систему России можно представить в виде совокупности инструментов и механизмов, используемых организациями при предоставлении своим клиентам платежных услуг. Указанные инструменты и механизмы видоизменяются и совершенствуются, что неизбежно ведет, в свою очередь, к росту объема и разновидности преступлений в указанной сфере.

Так, при анализе статистических данных МВД России за последние 10 лет примерно в 8 раз выросло количество преступлений, совершенных с использованием платежных карт. Обращает на себя внимание и количество статей Уголовного кодекса РФ, по которым квалифицируют указанные общественно опасные деяния.

В июле 2017 г. Президентом России В.В. Путиным подписан Закон, ужесточающий ответственность за неправомерные действия в сфере компьютерной информации.

Платежная карта - это электронное средство платежа, «инструмент» национальной платежной системы, законодательно регламентированный, соответствующий международным стандартам, охраняемый в том числе и нормами уголовного законодательства.

В соответствии с Национальным законодательством по целевому назначению представлены: расчетная (дебетовая) карта; кредитная карта; предоплаченная карта.

В зависимости от модификации уровня и степени защиты выделяют следующие виды банковских карт: карта с магнитной полосой, карта с микропроцессором, скрэтч-карта, карта в электронном виде и прочие.

В настоящее время самыми распространенными являются карты с чипом и магнитной полосой, последние в Российской Федерации постепенно выводят из оборота.

Магнитная полоса - носитель информации с ограниченным объемом памяти.

По цвету магнитные полосы различаются следующим образом: HiCo - полоса черного цвета, LoCo - полоса коричневого цвета.

На магнитной полосе находятся три дорожки, по которым можно нанести ту или иную информацию. Все три дорожки магнитной полосы используются, как правило, в крупных банковских платежных системах (например, VISA).

Существует ряд международных стандартов, определяющих практически все свойства пластиковых карточек, начиная от физических свойств пластика, размеров карточки и заканчивая содержанием информации, размещаемой на карточке тем или иным способом.

ISO-7810 «Идентификационные карты - физические характеристики» - геометрические размеры пластиковых карт должны соответствовать: ширина - 85,595 + 0,125 мм; высота - 53,975 + 0,055 мм; толщина - 0,76 + 0,80 мм; радиус окружности в углах - 3,18 мм.

Печать на картах может производиться офсетным, цифровым, сублимационным способами. Может выполняться горячее тиснение фольгой, типпинг фольгой, установка голограмм, высечка отверстий, имплантация микросхемы (чипа), сублимация скретч-панели и панели для подписи.

ISO-7811 «Идентификационные карты - методы записи»;

ISO-7812 «Идентификационные карты - система нумерации и процедура регистрации идентификаторов эмитентов» (5 частей);

ISO-7813 «Идентификационные карты - карты для финансовых транзакций»;

ISO-4909 «Банковские карты - содержание третьей дорожки магнитной полосы»;

ISO-7816 «Идентификационные карты - карты с микросхемой с контактами» (6 частей).

Эмбоссирование - один из способов персонализации пластиковых карточек, при котором на готовой ламинированной карточке выдавливаются символы (выпуклые буквы, выпуклый шрифт). После этой операции верхушки рельефных символов покрываются фольгой (золотом, серебром), такая операция называется типированием. Эмбоссирование символов возможно только при горизонтальной ориентации карточки. Эмбоссирование осуществляется двумя видами шрифтов: высотой 4,5 мм - большой (Farrington OCR); высотой 3 мм - малый (Standart Gothic и Cyrillic). Большой шрифт может содержать только цифры: 0123456789. При эмбоссировании следует учитывать месторасположение таких элементов, как магнитная полоса и подписная панель. При этом зона эмбоссирования уменьшается, так как от края расположения этих элементов необходимо делать отступ не менее 3 мм.

При совершении транзакций карты с чипом и магнитной полосой задействуется именно информация с чипа. Он обладает большим объемом памяти, и информация на нем подвергается более сложному типу шифрования.

Каждая транзакция микропроцессорной карты подтверждается специально сформированным для нее кодом, и для каждой последующей операции требуется новый код, сделать дубликат фактически невозможно. В настоящее время чипы умеют читать практически все устройства, принимающие банковские пластиковые карты.

Если банкомат провел операцию с использование лишь данных с магнитной полосы, то данную транзакцию можно оспорить и банк (владелец устаревшего банкомата) обязан возместить ущерб, причиненный держателю карты.

Так, следствием установлено, что в период времени, предшествующий 3 января 2014 г., неустановленный организатор приискал скимминговое устройство, изготовленное самодельным образом, являющееся приспособлением для получения информации, вводимой пользователем банкомата с клавиатуры, в том числе и информации о пин-кодах пластиковых платежных карт, которое необходимо было закрепить над клавиатурой банкомата таким образом, чтобы клавиатура попадала «в поле зрения» камеры видеорекордера, и устройство для считывания магнитной полосы платежной карты, являющееся приспособлением для получения (перехвата) информации с магнитной полосы пластиковых платежных карт, которое необходимо было установить перед картоприемником банкомата, а также ноутбук марки; зарядное устройство от ноутбука; компьютерную мышь и два USB-модема для обработки полученной информации, после чего при неустановленных обстоятельствах неустановленный организатор через неустановленное следствием лицо передал Кока и Коваленко, которым была отведена роль, заключающаяся в тайной установке скиммингового оборудования на банкоматы, принадлежащие ОАО, заранее выбранные неустановленным организатором на территории г. Москвы. Незаметно от клиентов отделения указанного ОАО и третьих лиц Кока и Коваленко установили вышеуказанное скимминговое оборудование на неустановленные банкоматы, принадлежащие ОАО, расположенные на территории г. Москвы, тем самым скомпрометировав 23 карты клиентов ОАО. После получения информации о пин-кодах неустановленное следствием лицо изготовило дубликаты платежных пластиковых карт в количестве 23 штук, скопировав на них вышеуказанную информацию. Однако подысканные в качестве исполнителей Кока и Коваленко, следуя вышеуказанному плану, развозили на автомобиле скимминговое оборудование, а также 23 пластиковые карты, которые могли быть восприняты в технологии функционирования платежных систем в качестве расчетных, задержаны сотрудниками полиции в 21.10 3 января 2014 г., в связи с чем не смогли довести свой преступный умысел до конца по независящим от них обстоятельствам.

В научной литературе получило развитие такое понятие, как кардинг. Однако, основываясь на практике квалификации деяний по национальному уголовному законодательству, данный термин не в полной мере охватывает виды и способы завладения информацией, а как следствие, и денежными средствами со счета платежной карты.

Все способы хищения условно можно разделить на пять категорий:

1. Интернет/телефон, т.е. похищение персональных данных посредством интернет-рассылок, запуск вредоносных программ, выяснение данных у держателей карт посредством телефонных переговоров с последними. Противоправное деяние совершается в несколько этапов: получение персонифицированных данных платежной карты; изготовление поддельной пластиковой карты (белый пластик) или приобретение пластиковых карт с погашенным сроком годности; сбыт поддельных карт; обналичивание денежных средств через банкоматы и интернет-магазины.

2. Подделка карт (белый пластик, использование б/у карт).

3. Перехват информации с пластиковых карт:

- посредством так называемых «хакерских ридеров», способных сканировать банковские карты с чипами RFID (аналоги легальных бесконтактных PoS-терминалов: RFID-ридеров, посылающих электромагнитные сигналы);

- кража денег «по воздуху» - смартфоны, оснащенные чипами NFC (NFC - разновидность RFID). Принцип примерно тот же, что и в магнитных проездных, пропусках и пластиковых картах MasterCard PayPass и VISA payWave. Сигналы с таких банковских карт преступники «по воздуху» перехватывают с помощью кустарно сделанных считывателей. Хакерам для вывода средств с карты необходимо лишь узнать ее полный номер и месяц/год окончания обслуживания.

4. Кража персональных данных - хищение посредством «специальных расширений» - плагинов, устанавливаемых на смартфоны и ПК:

- скимминг, кардинг, траппинг, поддельные банкоматы.

5. Кражи/потери банковских пластиковых карт.

Так, основываясь на примерах судебной практики, хищение, совершенное с использованием кредитных или расчетных карт при одних и тех же обстоятельствах, может признаваться судами и мошенничеством, и кражей.

Обман - информационное воздействие на держателя или владельца платежной карты, при котором он вводится в заблуждение; цель воздействия - заставить передать виновному денежные средства или право на них.

Как мошенничество квалифицируется безвозмездное обращение лицом в свою пользу или в пользу других лиц денежных средств, находящихся на счетах в банках, совершенное с корыстной целью путем обмана или злоупотребления доверием.

В случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по ст. 159 УК РФ, а также, в зависимости от обстоятельств дела, по ст. ст. 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать по соответствующей части ст. 158 УК РФ.

Хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной или поддельной кредитной либо расчетной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя).

Изготовление в целях сбыта или сбыт поддельных кредитных или расчетных банковских карт квалифицируется по ст. 187 УК РФ. Изготовление лицом поддельных банковских расчетных либо кредитных карт для использования в целях совершения этим же лицом преступлений, предусмотренных ч. 3 или ч. 4 ст. 159 УК РФ, следует квалифицировать как приготовление к мошенничеству.

Если лицо использовало похищенную или поддельную кредитную либо расчетную карту, но по независящим от него обстоятельствам ему не удалось обратить в свою пользу или в пользу других лиц чужие денежные средства, содеянное в зависимости от способа хищения следует квалифицировать как покушение на кражу или мошенничество по ч. 3 ст. 30 УК РФ и соответствующей части ст. 158 или ст. 159 УК РФ.

Сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, заведомо непригодных к использованию, образует состав мошенничества и подлежит квалификации по соответствующей части ст. 159 УК РФ.

В случае, когда лицо изготовило с целью сбыта поддельные кредитные либо расчетные карты, заведомо непригодные к использованию, однако по независящим от него обстоятельствам не смогло их сбыть, содеянное должно быть квалифицировано в соответствии с ч. 1 ст. 30 УК РФ как приготовление к мошенничеству, если обстоятельства дела свидетельствуют о том, что эти действия были направлены на совершение преступлений, предусмотренных ч. ч. 3 или 4 ст. 159 УК РФ.

**3 Обстановка в сфере обращения банковских пластиковых карточек в зарубежных странах**

В ходе анализа мошеннических действий, связанных с получением и использованием данных банковских карт за рубежом было установлено, что зарубежное законодательство при рассмотрении уголовно правовой нормы об ответственности за незаконное осуществление банковских операций преподносит более точные и понятные формулировки законов, касательно банковской деятельности, что считается в их пользу огромным плюсом и должно учитываться отечественным законодателем в случае изменения или дополнения уголовно-правовой нормы о незаконной банковской деятельности».

В наше время актуальным и немало важным вопросом является огромное количество совершения преступлений с помощью банковских карт и компьютерной сети Internet, они взаимосвязаны. Об этом пишут многие журналисты, приводя в примеры реальные факты того, что подобные преступления за рубежом расследуются годами, какие то из них раскрываются и преступников наказывают, а какие-то до сих пор в процессе.

Наикрупнейшее преступление с использованием банковских карт было совершено в США в 2011 году. Мошенники изготавливали дубликаты пластиковых карт, все данные они получали с карт клиентов, предоставляемых ими в ресторанах и других предприятиях обслуживания, расположенных в Африке, Азии, Европе и на Ближнем Востоке. Всего группировке удалось потратить почти 13 миллионов долларов чужих средств.

Заготовки для фальшивых карт поступали из России, Ливии, Ливана и Китая. В некоторых случаях к картам печатались и водительские удостоверения с соответствующими данными. Представитель полиции Нью-Йорка охарактеризовал воображение злоумышленников и преступные схемы как «поразительные».

Обвинения были предъявлены 111 участникам преступной группы, из них 86, на тот момент, находятся уже под стражей. Есть ли среди них россияне или выходцы из России было неизвестно.

Таким же образом действовала и другая преступная группировка, только немного другим способом. Их не могли нейтрализовать около девяти лет. За это время, предполагается, что мошенники скопировали 15 тысяч кредитных карт и обналичили счета их владельцев на общую сумму около 50 миллионов евро.

Данные для копирования карт с магнитной полосой мошенники получали, когда небрежный обладатель кредитки пытался использовать фальшивый банкомат, установленный бандитами специально для этой цели. Машина денег не выдавала, но копировала все данные карты "клиента", включая его пин-код. После этого мошенники изготавливали дубликат карты и снимали с нее средства [ИС; 6].

«Резкий всплеск преступлений в интернете в США в последнее время имеет один плюс. Грабить банки становится все менее выгодно по сравнению с махинациями с банковскими картами. Налетчики видят, что можно получить больший куш, не рискуя жизнью и не прибегая к насилию. Поэтому количество ограблений банков в Соединенных Штатах стремительно снижается, а количество финансовых преступлений в интернете наоборот стремительно растет.

За последние десять лет количество ограблений банков сократилось почти вдвое - до 5,1 на 100 американских банков в 2011 году. Уровень преступности в США снижается, но сокращение количества банковских ограблений, согласно данным ФБР, намного превышает это снижение. Предварительные данные показывают, что в 2012 году были ограблены 3870 американских банков, тогда как в прошлом эта цифра превышала 5000. Так редко банки в США не грабили уже несколько десятилетий. Всплеск же пришелся на начало 90-х годов прошлого века. В 1991 году налетчики наведывались почти в 9400 банков.

Специалисты по безопасности банков и бывшие агенты ФБР объясняют тенденцию усилением банковской защиты и ужесточением законодательства. В 1987 году в законодательство были внесены поправки, позволяющие судьям сажать налетчиков на значительно более долгие сроки, чем раньше. Есть и еще одно объяснение: в последние годы все больше преступников приходят к выводу, что ограбления банков являются очень рискованным делом, а выгоды они приносят относительно немного. Такой вывод приводит к переквалификации большого количества банковских грабителей в киперпреступников.

Вместе с общим снижением количества ограблений банков снижается количество пострадавших. В 2011 году в результате налетов на банки пострадали 88 человек и 13 погибли. Это примерно на 40% ниже, чем цифры по 2003 году - году, когда ФБР начало вести подобную статистику.

Число финансовых преступлений в интернете стремительно растет. В 2011 году их было совершено 314 000, что примерно в пять раз больше, чем в 2001 году. По данным Ассоциации банкиров США, аферы с банковскими картами принесли преступникам в 2010 году 1,8 млрд. долларов. Ограбления банков же в 2012 году дали только 29,5 млн. долларов, или 7,6 тыс. в среднем за ограбление. В 1997 году эти цифры были значительно выше: 107 млн. долларов и 12,4 тыс. соответственно».

Ввиду всего этого оптимальным будет привести реальный пример, произошедший относительно недавно. Совершенное в 2013 году, точнее в этом году преступление было раскрыто, а вот сам процесс, хищения денежных средств с банковских карт с помощью интернета, длился с 2007 года. В данной незаконной операции участвовали 11 человек. Среди задержанных фигурируют граждане США, Великобритании и Вьетнама. Сумма ущерба, причиненная злоумышленниками, оценивается в 200 млн долларов.

За 6 лет им удалось похитить данные более чем миллиона кредитных карт, взломав сайты интернет-магазинов, и перепродали их сомнительным клиентам.

На сегодняшний день из всех видов мошенничества "лидирует" подделка карточек. Как правило, на их заготовки наносится логотип эмитента, поле для проставления подписи и в точности воспроизводятся все признаки защиты (используются подлинные реквизиты реально существующих карточек). На международном рынке в изготовлении поддельных карточек первенство держат представители Юго-Восточной Азии, откуда осуществляется большинство "пластиковых" афер. Выявлены и филиалы преступных сообществ в Испании, Италии и Великобритании.

В Европе азиатских мошенников напористо теснят выходцы из Африки. Африканцы обычно используют поддельные карты для получения наличных денег непосредственно в банках. При этом удостоверяют свою личность с помощью украденных идентификационных документов. Африканцы осуществляют полную подделку пластиковых карт, чаще всего в США.

Другой распространенный вид преступлений - незаконное использование подлинных карточек. Сюда относятся операции с украденной или утерянной карточкой, изготовление продавцом дополнительных копий платежных квитанций, которые в дальнейшем используются для снятия денег со счетов.

Известны случаи, когда недобросовестные работники банков или предприятий, занятые изготовлением карточек, пользуются задержкой между открытием счета и доставкой карточки владельцу для совершения по ней операций. Иногда владельцы карточек сами делают ложные заявления о происшедшей якобы краже и потере карточек. Пока процессинговый центр включит номер карточки в стоп-лист и известит торговые точки, проходит несколько дней За это время владелец проводит с карточкой максимальное число операций, а затем предъявляет банку свои претензии В практике нередко наблюдаются частичные подделки карточек, когда злоумышленник (чаще всего владелец карточки) изменяет либо номер, либо фамилию. Это делается механическим путем: надпись срезается и наклеивается. Особый интерес для преступников представляют банковские пластиковые карточки, пересылаемые по почте. Кража обнаруживается с большим опозданием, в результате отсутствует возможность немедленного блокирования счета; к моменту кражи карточки, как правило, не подписаны, а, значит, злоумышленник может поставить свою подпись и легально использовать карточку по своему усмотрению. Выявлены случаи, когда преступники специально устраивались работать на почту или в частные службы доставки, чтобы иметь возможность изымать конверты с пластиковыми банковскими карточками.

 Распространена схема мошенничества, получившая название «белого пластика» Такие карточки не имеют опознавательных знаков банка эмитента, платежной системы и голограммы. На совершенно чистый пластиковый бланк наносятся данные уже существующих карточек и предъявляются для оплаты. Правда, такими карточками могут в сговоре воспользоваться только их владельцы и служащие предприятий торговли или сервиса, поскольку фальшивку можно определить на глаз. Дальше производится «замывание» ложных квитанций среди подлинных. В результате невозможно установить, какая карточка была предъявлена настоящая или поддельная Для совершения мошеннических действий с «белым пластиком» нередко создаются целые фирмы.

**4 Меры по предотвращению мошенничества с пластиковыми картами**

Поначалу банки не знали, как бороться со скиммингом, так как атаки приобретали массовый характер и постоянной улучшались. Так и сейчас происходит постоянные соревнования между хакерами и специалистами банковской безопасности.

В борьбе со скиммингом, банки обычно используют три технологии - физический мониторинг, пассивный антискимминг и активный антискимминг.

**Физический мониторинг банкоматов.**

Включает в себя периодический осмотр банкомата сотрудниками банка, инкассаторами, либо специалистами сервисной службы на аутсерсинге. Осмотр обычно производится по граффику с заполнением специального журнала проверок, чтобы в случае нахождения инородного устройства выявить промежуток времени в течение которого был риск компрометации карт. Физический мониторинг может казаться самым дешевым, однако в пересчете на потраченное время сотрудников и вероятность мошенничества между проверками, по факту оказывается самым ненадежным и дорогим способом борьбы со скиммингом.

**Пассивный антискимминг.**

Банк устанавливает на щель картоприемника специальные антискимминговые накладки, препятствующие установке посторонних устройств. Накладка может быть подключена к специальному датчику, который срабатывает в случае попытки мошенника снять антискиммер с банкомата. Датчик может состоять из обычных проводов, которые рвутся при снятии антискиммера с банкомата, либо пары магнит+геркон (при котором контакты геркона реагируют на удаление антискимминговой накладки со встроенным магнитом). При этом, в процессе удаления антискиммера, наличие герконовой пары мошенник может не заметить, что повышает шансы его поимки.

Недостаток пассивного антискимминга в том, что многие держатели карт, начитавшись и насмотревшись страшилок про банкоматное мошенничество, увидев постороннее устройство боятся (и кстати вполне оправданно) пользоваться таким банкоматом.

Частично успокоить держателей карт удается разместив на экране банкомата, или на специальной наклейке под картоприемником изображения правильного вида картоприемника. К сожалению не все держатели карт бдительны, а технологии, применяемые мошенниками позволяют изготавливать скиммеры настолько высогого качества, что отличить скиммер от антискиммера порой не могут даже сотрудники банков. Пассивный антискимминг - это бюджетный, компромисный, но не лучший вариант борьбы со скиммингом.

**Активный антискимминг.**

Это самый дорогой, но эффективный способ борьбы со скиммингом. Устройство устанавливается внутри банкомата и незаметно снаружи.  Активный антискиммер контролирует пространство перед банкоматом и позволяет моментально выявить несанкционированную установку на него посторонних устройств. Антискиммер может также создавать радиопомехи в области щели картоприемника, препятствующие работе посторонних электронных устройств.

Датчики антискиммера позволяют анализировать электромагнитное поле в зоне размещения картридера, ПИН-клавиатуры и монитора и в случае резкого изменения напряженности поля (включения излучающих устройств при радиопередаче, установка постороннего оборудования), устройство подает команду на управляющий блок банкомата, который выводит банкомат из режима обслуживания клиентов и может выполнять дополнительные действия (отправка команды, SMS, оповещение службы охраны и мониторинга и т.д.).

Уязвимость бесконтактных карт можно снизить с помощью «шапочки из фольги», точнее, кошелька. Условно говоря, если вы положите карту в фольгированный пакет, специальный радиоэкранированный кошелек или металлическую коробочку, транзакцию провести будет нельзя. Впрочем, специалист по компьютерной безопасности предлагает другой способ защиты капиталов.

Самый надежный и радикальный метод — это отказаться от использования подобных бесконтактных карт. Для большинства пользователей он будет самым предпочтительным. Когда вы получаете карту, уже тогда надо задуматься, нужны вам бесконтактные платежи или нет, потому что сценарии использования бесконтактных карт очень специфичны и, если вы не планируете их использовать, от данной возможности стоит отказаться.

Уголовная ответственность за незаконное использование банковских карт указана в статье 187 УК РФ. Данная статья предусматривает наказание в виде принудительных работ на срок до пяти лет либо лишением свободы на срок до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

**5 Регистрация и использование электронных средств платежа, а также противодействие мошенничеству и краже**

Значение электронных платежей в современных геополитических условиях переоценить трудно, поскольку они позволяют обеспечивать перемещение капитала по всему миру, осуществлять взаиморасчеты между хозяйствующими субъектами в режиме on-line, способствуя увеличению объемов платежного оборота, снижению стоимости переводов и т.д.

Именно поэтому 3 июня 2017 г. на Петербургском международном экономическом форуме в качестве приоритетного направления деятельности Банка России был обозначен переход на безналичное денежное обращение, предполагающее изменение устоявшейся модели финансового поведения субъектов гражданского оборота, а также усиление контроля за техническим исполнением требований информационной безопасности.

В экономической теории под средствами платежа часто подразумевают не сами деньги, как это следовало бы ожидать, а их функцию, вследствие чего употребление названного термина стало провоцировать смешение понятий «электронные средства платежа» («электронные деньги») и «технико-электронные средства» (средства ведения безналичных взаиморасчетов), что всерьез осложняет исследование вопросов, вынесенных в заголовок настоящей статьи.

Известно, что впервые понятие ЭСП было легализовано в п. 3 ст. 847 ГК РФ, провозгласившем, что договором может быть удостоверено право распоряжения денежными суммами, находящимися на счете, ЭСП и другими документами с использованием в них аналогов собственноручной подписи (п. 2 ст. 160 ГК РФ), кодов, паролей и иных средств, подтверждающих факт дачи распоряжения уполномоченным на то лицом.

Буквальное толкование указанной нормы под ЭСП позволяло понимать расчетный (платежный) документ, составленный в соответствующей (электронной) форме (электронный платежный документ).

В п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» электронный документ определяется как документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Часть 1 ст. 11.1 Закона № 149-ФЗ гласит, что органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

В настоящее время основным нормативным правовым актом, регламентирующим порядок использования ЭСП во взаиморасчетах, является Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

В части, касающейся регистрации ЭСП, положения Закона № 161-ФЗ детализированы в указании Банка России от 14.09.2011 № 2694-У «О порядке уведомления Банка России оператором электронных денежных средств о начале деятельности по осуществлению перевода электронных денежных средств», в пункте 3 которого продекларировано, что оператор электронных денежных средств, осуществляющий деятельность по переводу электронных денежных средств, обязан направить в Банк России (Департамент регулирования расчетов) почтовым отправлением с уведомлением о вручении или нарочным через Экспедицию Банка России письменное уведомление о начале деятельности по осуществлению перевода ЭДС не позднее 10 рабочих дней со дня первого увеличения остатка ЭДС.

Впоследствии требование о регистрации ЭСП было закреплено в п. 2.1 Положения № 383-П «О правилах осуществления перевода денежных средств», утвержденного Банком России 19 июня 2012 г., где провозглашалось, что процедуры приема к исполнению распоряжений включают: удостоверение права распоряжения денежными средствами (удостоверение права использования ЭСП), контроль целостности распоряжений, структурный контроль распоряжений, контроль значений реквизитов распоряжений, контроль достаточности денежных средств.

В этой же норме оговаривалось, что:

- процедуры приема к исполнению распоряжения плательщика, требующего в соответствии с федеральным законом согласия третьего лица на распоряжение денежными средствами плательщика, включают контроль наличия такого согласия третьего лица;

- процедуры приема к исполнению распоряжения получателя средств, требующего акцепта плательщика, включают контроль наличия заранее данного акцепта плательщика или получение акцепта плательщика;

- банки могут дополнительно устанавливать, в том числе в договорах, иные процедуры приема к исполнению распоряжений, включая регистрацию распоряжений, контроль дублирования распоряжений, получение согласия кредитной организации плательщика на операцию с использованием ЭСП.

Квинтэссенцией Закона № 161-ФЗ является следующее. Клиент (юридическое лицо или индивидуальный предприниматель) предоставляет денежные средства ОЭДС с использованием своего банковского счета, который учитывает их посредством формирования записи, отражающей размер обязательств оператора перед клиентом в сумме предоставленных денежных средств. Использование ЭСП осуществляется на основании договора, заключаемого оператором по переводу денежных средств, с клиентом, а также договоров между взаимодействующими операторами. До этого ОПДС обязан информировать клиента об условиях использования ЭСП, в том числе о любых ограничениях способов и мест, случаях повышенного риска и проч.

Интенсивное развитие информационных технологий в сфере безналичных расчетов, свойственных главным образом кредитно-банковской отрасли российской экономики, рост числа интернет-платежей, расчетов, производимых с использованием банковских карт, на фоне недостаточного нормативного правового их регулирования явились предпосылкой к более широкому пониманию ЭСП. Учеными и специалистами-практиками стало признаваться, что распоряжение денежными средствами может осуществляться как с помощью электронных расчетных документов, так и документов, удостоверенных ЭСП, а также с применением банковских карт, иных технических устройств и средств связи.

Диспозиция п. 3 ст. 847 ГК РФ изначально не исключала возможности отнесения банковской карты, равно как и других ЭСП, к разновидности документов, поскольку банковская карта представляла (и представляет) собой документ, выдаваемый кредитной организацией в подтверждение факта размещения на соответствующем банковском счете денежных средств в договорной валюте. На основании этого держатель карты приобретал (приобретает) возможность многократного распоряжения наличными денежными средствами, находящимися на ней.

Подобная дефиниция банковской карты формально не противоречила требованиям п. 3 ст. 847 ГК РФ. Вместе с тем в отличие от понятия ЭСП как средства оформления платежного документа, понятие ЭСП как документа в описываемых ситуациях нисколько не отражало истинного назначения рассматриваемого устройства.

Оценке банковских карт как платежных документов способствовала также диспозиция ст. 187 УК РФ, предусматривающая ответственность за изготовление, приобретение, хранение, транспортировку в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (оцениваемых в качестве платежных документов), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

В настоящее время в Российской Федерации кроме расчетов банковскими картами в обиход входят и другие инновационные способы безналичных расчетов, в частности, мобильный банкинг, то есть удаленное управление банковским счетом с помощью планшетного компьютера, смартфона или обычного телефона.

Электронные деньги - термин, употребляющийся во многих значениях, связанных с использованием компьютерных сетей и систем хранимой стоимости для передачи (хранения) денежных средств. По обычаю под ними подразумеваются системы хранения и передачи как традиционных, так и негосударственных (частных) валют. Обращение электронных денег осуществляется по правилам, установленным (согласованным с) Банком России и по собственным правилам негосударственных платежных систем.

Технические устройства (мобильные телефоны, компьютеры, терминалы, банкоматы), используемые в этих целях, в отличие от дебетовых банковских карт, даже теоретически не могли рассматриваться в качестве документов в силу присущих им физических свойств и функционального предназначения.

В то же время понятие ЭСП, предложенное ГК РФ, если игнорировать не очень корректную формулировку, представленную в п. 3 ст. 847 ГК РФ, достаточно точно определяло функцию технических устройств при осуществлении электронных платежей.

Некоторые виды ЭСП, например, расчетные и предоплаченные банковские карты, в техническом аспекте представляют собой неотъемлемый атрибут технологии платежного инструмента - формы безналичных расчетов. Часть электронных устройств (терминалы, банкоматы) - особая группа ЭСП - используется только по месту их установки.

Другие виды ЭСП (компьютеры, мобильные телефоны) в большинстве своем не предназначены для использования в качестве платежных инструментов, но в совокупности с дополнительными устройствами (программным обеспечением) в состоянии выступать в качестве физических носителей определенного их вида (например, ЭДС), либо обеспечивать доступ к подобным инструментам через интерфейс платежной системы (операционный сайт банка).

С течением времени некоторые из электронных устройств, использовавшихся для управления банковским счетом, начали употребляться для оказания платежных услуг организациями, не являющимися кредитными. Однако содержащееся в ГК РФ понятие ЭСП как средства распоряжения денежными суммами на банковском счете, формально не могло прилагаться к безналичным платежам, проводимым вне банковской системы.

Учитывая растущий объем электронных платежей в стране, а также важную роль ЭСП в осуществлении безналичных расчетов в электронной форме, понятие ЭСП, закрепленное в ГК РФ, нуждалось в более точном нормативном правовом урегулировании.

При подготовке проекта закона о национальной платежной системе Банк России предусмотрел более широкое определение ЭСП, позволявшее учесть как существующие средства и способы передачи распоряжений об осуществлении переводов денежных средств в электронном виде, так и перспективные.

В п. 19 ст. 3 Закона № 161-ФЗ ЭСП определяется как средство и (или) способ, позволяющие клиенту ОПДС 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. Данной дефиницией ЭСП охватываются все существующие ныне устройства и способы, а также их комбинации, предоставляемые оператором платежных услуг на основании договора клиенту и позволяющие ему осуществлять денежные переводы как с использованием, так и без использования банковских счетов.

Следует отметить, что такой подход не позволяет рассматривать платежный документ в электронной форме, использующийся в системах дистанционного банковского обслуживания кредитных организаций, как ЭСП, несмотря на то, что указанному понятию и правилам его использования законодатель придал системообразующий характер в части, касающейся всех применявшихся в стране форм безналичных расчетов, включая расчеты ЭДС. Это выражается в том, что при оказании платежной услуги в электронной форме независимо от выбранной формы безналичных расчетов действуют единообразные правила использования ЭСП, а также распределения рисков при несанкционированных операциях, связанные с уведомительными процедурами клиента и ОПДС. Данные императивные требования не зависят от правового статуса оператора платежной системы и технических характеристик ЭСП.

В то же время не все установленные императивные правила использования ЭСП могут быть применимы на практике. Так, ч. 3 ст. 9 Закона № 161-ФЗ обязывает ОПДС до заключения с клиентом договора об использовании ЭСП информировать его, в частности, о случаях повышенного риска, а также о любых ограничениях способов и мест такового. Требования об обязательном предоставлении вышеуказанной информации в целом адекватны целям защиты прав потребителей при заключении договоров, предусматривающих возможность длительного использования ЭСП для многократных платежей. Когда же потребителю приходится совершать разовый перевод денежных средств через банкомат с функцией cash i№ или другие, аналогичные по функционалу устройства, охватываемые понятием ЭСП, то предоставление по инициативе ОПДС такой информации клиенту лишается всякого смысла.

Это же можно сказать в отношении установленной Законом обязанности ОПДС направлять клиенту уведомление о факте совершения каждой операции с использованием ЭСП, носящей публично-правовой характер. Обусловлено сказанное тем, что клиент лично присутствует в месте платежа и ввиду получения в его подтверждение кассового чека не нуждается в каком-либо дополнительном уведомлении о факте таковой операции.

Неприменимыми оказываются и положения Закона № 161-ФЗ об уведомлении клиентом оператора об утрате или использовании ЭСП без согласия клиента, так как в подобных случаях невозможно ни то, ни другое.

Таким образом, при переводе денежных средств посредством банкоматов или платежных терминалов некоторые установленные Законом императивные правила в отношении уведомительных процедур при использовании ЭСП в практической плоскости не срабатывают.

Ввиду изложенного, во избежание формального нарушения требований Закона № 161-ФЗ, неприменимых к отдельным видам ЭСП, целесообразно предусмотреть дополнительную дифференциацию технических устройств с детализацией видов ЭСП, на которые указанные требования не распространяются.

В последние годы в Российской Федерации прослеживается устойчивая тенденция к росту числа несанкционированных операций с использованием систем дистанционного банковского обслуживания. По информации Банка России, в 2014 г. их было совершено более 300 тыс. на общую сумму более 3,5 млрд руб., из которых 1,58 млрд руб. приходилось на несанкционированные операции с использованием платежных карт, эмитированных кредитными организациями. Количество таких операций на протяжении 2015 - 2016 гг. постоянно увеличивалось. В то же время объем несанкционированных операций, совершенных с использованием платежных карт, эмитированных на территории Российской Федерации, в 2016 г. составил 1,08 млрд руб., что меньше аналогичного показателя за 2015 г. на 6,1%.

При постепенном сокращении доли несанкционированных операций, осуществляемых с использованием банкоматов и платежных терминалов, наблюдается некоторый прирост числа несанкционированных транзакций, осуществленных посредством сети Интернет, а также средств мобильной связи.

В целях защиты клиентов банков и платежных систем от хищений Банк России подготовил поправки к Положению о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств, которыми введены дополнительные требования к банкам и иным организациям, проводящим платежи.

В платежной индустрии разработаны технологические решения, способствующие защите денежных потоков от противоправных посягательств. Одно из них - токенизация операций, позволяющая обезопасить ЭСП с помощью надежной системы шифрования данных. Расплачиваясь картой, покупатель не передает продавцу свои платежные реквизиты, вся карточная информация шифруется и превращается в так называемый токен, выглядящий как случайная комбинация некоей группы символов. Когда токен попадает в терминал продавца, а потом транслируется по сети в банк для подтверждения платежа, он становится бесполезным для мошенников, поскольку не отражает какой-либо значимой информации.

Вместе с тем у злоумышленников остается возможность использовать схемы, в которых зачисление денежных средств на счет получателя производится весьма быстро. В этой связи целесообразно переработать положения ст. 9 Закона № 161-ФЗ и ряда норм других законодательных актов в целях формирования реально работающей системы остановки и возврата платежей. Для этого Банку России в масштабах национальной платежной системы следует нормативно урегулировать такое понятие, как запрос отмены перевода. Подобные запросы должны быть стандартными и производиться в режиме реального времени, обрабатываясь всеми участниками рынка переводов.

Кроме того, в условиях высокой скорости проведения расчетов, многообразия форм ЭСП, значимого уровня технической оснащенности преступников актуализируется реальная потребность в создании правового механизма приостановления перевода денежных средств.

Негативная ситуация с защитой прав граждан в области регистрации и использования ЭСП усугубляется еще и тем, что существующая система судебного порядка удостоверения фактов несанкционированного списания денежных средств всерьез осложняет работу органов правосудия, которые не в состоянии оперативно рассматривать большое количество связанных с этим дел. По существу, суды должны быть последней инстанцией при разрешении споров, связанных с несанкционированными списаниями денежных средств, если не сработали иные (претензионные) механизмы их урегулирования.

Часть 11 ст. 9 Закона № 161-ФЗ устанавливает весьма ограниченный срок для опротестования операций по переводу денежных средств (один день), в то время как клиенты банков могут находиться вне зоны действия мобильной связи или за границей без подключения услуг международного роуминга.

Когда клиент обращается в банк с жалобой на несанкционированное списание денежных средств, служащие последнего в большинстве случаев отказывают ему в ее удовлетворении, мотивируя это введением верных паролей. Исходят они из признания того, что перевод денежных средств не мог быть осуществлен никем иным, кроме как законным владельцем карты. Однако при этом упускается из виду, что преступники могли использовать «инновационные» уловки, открывающие им доступ к счетам клиентов банка, в частности скимминг.

Отказывая клиенту в возмещении похищенных денежных средств, служащие банков нередко апеллируют также к тому, что клиент совершил перевод денег через личный кабинет на сайте банка, хотя тот пароль ни разу не получал, а то и вовсе не имел доступа к Интернету. Отсутствие же должных оповещений по телефону служащие банков сплошь и рядом списывают на зараженность телефона клиента всевозможными вирусами. Причем для того, чтобы сделать подобные утверждения, они не утруждают себя просьбами предъявить «зараженный» телефон, всячески игнорируя представляемые клиентом справки об отсутствии в нем вредоносных программ.

Сопутствующие данному вопросу рекомендации о необходимости обращения клиента за защитой своих прав в правоохранительные органы носят преимущественно бюрократический характер, поскольку последние крайне нежелательно берут на себя какие-либо обязательства по проведению соответствующих процессуальных проверок в виду их сложности и бесперспективности в плане установления фактов несанкционированных транзакций денежных средств.

В то же время именно банк, как ОПДС, имеет возможность провести проверку транзакции и при возникновении сомнений уведомить об этом клиента. Понятно, что подобные обязательства для него дополнительная нагрузка, однако именно такой подход в состоянии повысить деловую репутацию кредитной организации.

Банком России разработан ряд стандартов по обеспечению информационной безопасности банковской системы, нарушение которых может влечь различные виды ответственности. Это, однако, не умаляет актуальности разработки мер по усилению контроля за регистрацией и использованием ЭСП, для повышения эффективности которого целесообразно осуществить ряд мероприятий.

1. В Законе № 161-ФЗ следует урегулировать понятия национальной платежной системы, платежной системы и значимой платежной системы, а также уточнить перечень федеральных органов исполнительной власти, полномочных осуществлять их нормативное правовое регулирование.

2. В целях создания механизма приостановления перевода денежных средств необходимо:

- закрепить право, а в ряде случаев обязанность ОПДС на приостановление переводов денежных средств при выявлении признаков их совершения без согласия плательщика;

- установить обязанность клиента незамедлительно уведомлять ОПДС о ставшем ему известным факте несанкционированного получения третьими лицами информации, необходимой для получения доступа к ЭСП;

- определить порядок возврата денежных средств при доказанности факта их перевода без согласия клиента;

- предусмотреть полномочия Банка России по установлению для кредитных и некредитных финансовых организаций обязательных требований к обеспечению защиты информации при осуществлении банковской деятельности (деятельности в сфере финансовых рынков).

3. В целях изменения ситуации с несанкционированными списаниями денежных средств со счетов клиентов кредитных организаций Банку России в масштабах национальной платежной системы следует нормативно урегулировать такое понятие, как запрос отмены перевода.

4. Для более оперативного и качественного предотвращения (пресечения) фактов несанкционированных списаний денежных средств со счетов клиентов кредитных организаций нужно законодательно закрепить право ОПДС, обслуживающего получателя и уже зачислившего денежные средства на его счет, при получении от ОПДС, обслуживающего плательщика, уведомления блокировать денежные средства на счете получателя в пределах указанной в уведомлении суммы денежных средств (при условии их достаточности на счете). При этом во избежание умножения споров с физическими лицами на сей предмет желательно предусмотреть возможность снятия заблокированных денежных средств при личном обращении получателя (физического лица) в кредитную организацию и предоставлении документов, позволяющих его идентифицировать.

5. В Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» надо внести дополнение о том, что при установлении вины кредитной организации, не обеспечившей предусмотренных мер защиты денежных средств и вкладов, и допустившей их хищение, ущерб клиенту (вкладчику) возмещается в полном объеме за ее счет. В гл 3

6. С целью защиты денежных средств клиентов финансовых организаций в ч. 11 ст. 9 Закона № 161-ФЗ целесообразно внести изменения, связанные с увеличением срока оспаривания рассматриваемых транзакций (операций) с одного до трех дней.

Эту же норму желательно дополнить абзацем следующего содержания: «После получения оператором информации о переводе денежных средств без согласия клиента оператор обязан уведомить об этом правоохранительные органы».

7. Для повышения ответственности кредитных организаций, не обеспечивающих предусмотренных мер защиты денежных средств и вкладов и допустивших их хищение, ч. 2 ст. 74 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» необходимо изложить в следующей редакции: «В случаях нарушения кредитной организацией федеральных законов, издаваемых в соответствии с ними нормативных актов и предписаний Банка России, непредставления информации, представления неполной или недостоверной информации о своей деятельности и аудиторского заключения по ней, необеспечения безопасности по защите денежных средств и вкладов и допущения их хищения, Банк России...» (далее по тексту).

Статью 19 Закона № 395-1 следует дополнить нормой, декларирующей меры Банка России, применяемые им в порядке надзора в случае нарушения кредитной организацией федеральных законов и нормативных актов Банка России, а также нарушений в деятельности банковской группы.

8. Целесообразно рекомендовать Банку России внести дополнение в Инструкцию «О применении к кредитным организациям мер воздействия за нарушения пруденциальных норм деятельности», введенную в действие Приказом от 31.03.1997 № 02-139, в части установления принудительных мер воздействия к кредитной организации за необеспечение мер безопасности по защите денежных средств, создающих реальную угрозу интересам клиентов и (или) кредиторов (вкладчиков).

9. Следует расширить полномочия Банка России по установлению стандартов информационной безопасности и осуществления контроля их исполнения организациями, привлекаемыми для обеспечения безопасности, хранения, обработки, передачи компьютерной информации кредитных организаций и субъектов национальной платежной системы.

10. В целях установления обязанности руководителей кредитных организаций информировать правоохранительные органы и Банк России о фактах посягательств на их сетевые ресурсы желательно внести соответствующие изменения в федеральное законодательство, а также предусмотреть санкции за непринятие банками надлежащих мер по защите денежных вкладов.

**ЗАКЛЮЧЕНИЕ**

Развитие платежных систем является характерной чертой современного мира. В настоящее время коммерческие организации не могут быть представлены без выпуска, внедрения и обслуживания банковских карт.

Однако, несмотря на то, что иностранные банки уже давно используют карточную систему, этот инструмент недавно вышел на первый план.

Тем не менее, банковские карты являются неотъемлемой частью не только нашей жизни, но и удобным инструментом в области мошенничества.

Это оправдывается тем фактом, что в этой области есть возможность действовать, не только не привлекая внимания, но часто даже не выходя из собственного дома.

Мошенникам не нужно обладать определенными навыками, достаточно просто найти информацию в Интернете, которая есть огромная сумма, или купить необходимое оборудование и специальные программы.

В мире развитых технологий, человечеству с каждым днём становится всё труднее отказаться от появления новых сервисов дистанционного банковского обслуживания. Многочисленные компании каждый год разрабатывают и вводят новые системы защиты, а представители криминального мира пытаются найти способы, чтобы обойти эту защиту.

Конечно, если проявить упорство, можно найти средство борьбы с любой системой защиты, но, обычно, на это требуется много затрат. Намного легче ввести в заблуждение человека, не следящего за развитием современных технологий и не знающего всех тонкостей этой сложной системы.

При развитии информационных систем и технологий возрастает уровень преступлений в данной сфере. В условиях роста объема эмиссии банковскиих карт и количества банкоматов актуализируются проблемы обеспечения безопасности последних.

Среди наиболее распространенных методов, с помощью которых мошенники пытаются добыть наличность из банкоматов, выделяются такие, как:

- «мошеннический ПИН-ПАД»,

- «фишинг»,

- щипачество»,

- «Ливанская петля» («траппинг»),

- «кардинг»,

- «кибератака»,

- «скимминг» и др.

Как правило, осуществление мошенничества с использованием банковских карт или их реквизитов редко носит одиночный характер.

Объединить все схожие случаи можно, проанализировав список транзакций и выделив общие из списка транзакций жертв. В случае если найдены соответствия, то следующим шагом может стать локализация и определение типа устройства, с помощью которого был осуществлен несанкционированный доступ к банковской карте. Тут возможны несколько вариантов развития событий:

1. утечка данных из базы данных онлайн-магазинов и сервисов, в том числе использование злоумышленником вредоносного программного обеспечения и фишинговых атак;
2. скимминговая атака на один из банкоматов;
3. осуществление НСД к карте лица, проводящего платежи через торговые и платежные терминалы, находящегося в сговоре со злоумышленником;
4. разглашение данных сотрудниками организации-эмитента. Действительность такова, что жертвой скимминга может стать практически любой участник денежных отношений, который пользуется банковской картой. Поэтому целесообразно выделить основные причины и особенности скимминга:

1) наблюдаемый рост скимминг-атак на банкоматы коррелирует с «техническими» причинами, среди которых выделяют: относительно невысокую степень защищенности банковских карт, которые оснащены магнитной полосой (по оценкам экспертов, их количество на рынке пластиковых карт составляет порядка 80% от общей массы).

Поэтому наиболее предпочтительны карты со встроенными чипами, способными обеспечить более высокий уровень защиты и др. «Знаковым в этом отношении событием стало решение Сбербанка России перейти с 1 июля 2013 г. к эмиссии банковских карт, оснащенных исключительно чипами, существенно повышающими безопасность электронных средств платежа»;

2) рассматриваемая разновидность преступлений стала относительно новым и не до конца изученным явлением, поэтому при выявлении и расследовании уголовного дела по факту скримминг-атаки возникают определенные сложности.

Это обусловлено рядом объективных обстоятельств: значительный временной промежутком между обнаружением владельца карты и факта совершенного посягательства, проведения проверочных мероприятий по ситуации, изложенной в заявлении, принятием решения о возбуждении уголовного дела и его расследованием с одной стороны, и довольно оперативными действиями мошенников;

3) высокий уровень технической подготовки злоумышленников.

Для подделки пластиковой банковской карты и получения ее PIN-кода, как правило, мошенники используют следующие высокотехнологичные устройства:

- эмбоссер, при помощи которого возможно нанести надпись на пластиковую основу банковской карты;

- тайпер – устройство, позволяющее «впаивать» магнитную пленку на пластиковую заготовку карты;

- энкодер, через который можно записать полученные сведения на банковскую карту;

- скиммер – устройство, позволяющее считывать информацию, в дальнейшем заносимую на ЭВМ для последующей обработки.

В связи с вышесказанным можно сделать вывод о том, что обеспечение безопасности банковской системы в России зависит от эффективности работы службы безопасности кредитных организаций и сотрудников правоохранительных органов, которые занимаются предупреждением и выявлением мошенничества.

Кроме того, на наш взгляд, следует оборудовать банкоматы специальными антискимминговыми устройствами.

Практика изучения мошенничества показывает, что наибольшей популярностью у преступников пользуется скиммер.

Перед ридером банкомата монтируется устройство, считывающее информацию с магнитной полосы карты при ее введении в банкомат.

Развитие системы безналичных расчетов породило множество вопросов, к разрешению которых правоприменитель оказался не готов, в результате чего скимминг фактически остается безнаказанным, злоумышленникам зачастую назначается наказание в виде штрафа, размеры которого, как показал анализ судебной практики, явно не соответствуют угрозе деяния.

Становится очевидным, что проблема скимминг-атак переходит на качественно новый уровень и приобретает комплексный межотраслевой характер, требующий адекватного реагирования в целях противодействия хищениям с использованием поддельных банковских карт.

Самый надежный и радикальный метод — это отказаться от использования подобных бесконтактных карт.

Для большинства пользователей он будет самым предпочтительным.

Когда вы получаете карту, уже тогда надо задуматься, нужны вам бесконтактные платежи или нет, потому что сценарии использования бесконтактных карт очень специфичны и, если вы не планируете их использовать, от данной возможности стоит отказаться.

Уголовная ответственность за незаконное использование банковских карт указана в статье 187 УК РФ [3].

Данная статья предусматривает наказание в виде принудительных работ на срок до пяти лет либо лишением свободы на срок до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Уголовный кодекс Российской Федерации: [принят Государственной Думой РФ 24 мая 1996г., одобрен Советом Федерации 5 июня 1996, с изменениями и дополнениями по состоянию на 24.11.2014] // Собрание законодательства РФ – 1996. – № 25. – Ст. 2954.
2. Сизоненко А. Б., Стукалов В. В. Выявление и раскрытие преступлений, совершаемых с использованием пластиковых карт и их реквизитов: Методические рекомендации. – Краснодар: КрУ МВД России, 2013.– С. 41-44.
3. Безопасные финансы – полезные советы [Электронный ресурс]. – Режим доступа: http: //arb.ru/b2b/trends/bezopasnye\_finansy\_poleznye\_sovety-9908113/.
4. Как бороться со скиммингом [Электронный ресурс]. – Режим доступа: http://arb.ru/b2b/trends/kak\_borotsya\_so\_skimmingom-9894729/#5172.
5. Мошенники – серьезная проблема для банков во всем мире [Электронный ресурс]. – Режим доступа: http://arb.ru/b2b/trends/9903646/?source=mail.
6. Популярность мобильных платежей продолжает расти [Электронный ресурс]. – Режим доступа: http://static.androidiani.com/.
7. Современные методы защиты финансовой безопасности [Электронный ресурс]. – Режим доступа: http://cdni.wired.co.uk/.