Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 9, Is. 3, pp. 121-128, 2016

DOI: 10.13187/vesp.2016.9.121
www.ejournal21.com

Technical Means

UDC 004.056.5

Bank Cards and the Safety

Yuri F. Katorin [a,*]

[a] State university of the sea and river fleet of the name of the Admiral S.O. Makarov, Russian Federation

Abstract

This article is dedicated to questions of providing safety of cash resources, with the use of bank cards, since the financial operations of this type were since olden times the object of the increased attention from the side of individual dishonest personalities, the special features of cards with the magnetic strip and cards with the chip are described, and the enumeration of the basic tricks of criminals, used for the unsanctioned output of money, so is given, uses and servicing of bank maps are given to recommendation regarding providing of safety of operations.

Keywords: plastic bank card, swindle, the unsanctioned output of money, safety of cash resources, with the use of the bank cards.

1. Введение

Все больше людей пользуются пластиковыми банковскими картами. Лишь немногие знают, чем одна карта отличается от другой (Visa от MasterCard, карта с чипом от обычной карты с магнитной полосой). Многие хранят деньги на пластиковой карте, так как считают, что там они более защищены от воровства. Обеспечение безопасности денежных средств при использовании банковских карт сегодня является одной из важнейших задач. Финансовые операции всякого рода издавна являлись объектом повышенного внимания со стороны отдельных нечестных личностей. Банковские карты и взаимосвязанный с ними интернет-банкинг не исключение. Наряду со значительным количеством преимуществ, банковские карты имеют и некоторые недостатки, самым важным из которых являются небезопасность безналичных расчетов и высокая степень возникновения риска мошенничества по банковским картам (Абдеев, 1994).

Банковская карта является ключом доступа к банковскому счету и этим обусловливает огромный интерес к данному платежному инструменту со стороны мошенников, так как они со своей стороны также могут получить возможность доступа к средствам, размещенным на банковских счетах. Проявляя недюжинную изобретательность и смекалку, мошенники всех сортов активно охотятся за денежными средствами граждан на счетах кредитных карт. Нам,

* Corresponding author
E-mail addresses: katorin@mail.ru (Yu.F. Katorin)

впрочем, следует лишь помнить, что их действия не принесут никакого вреда, если соблюдать все рекомендации банковских специалистов по безопасности. Разумеется, неплохо при этом ознакомиться с наиболее распространенными способами компрометации пластиковых карт (Лаврушин, 2001).

2. Материалы и методы

Основными методами, используемыми в исследовании, являются методы научного познания: наблюдение, сравнительный и логический анализ, комплексный и системный подход к изучению оцениваемых показателей, методы экспертных оценок и структурного анализа сложных процессов.

Методологической основой исследования послужили работы отечественных и зарубежных экономистов, специалистов в области банковского дела, управления рисками, информационных систем, материалы научно-практических конференций, а также аналитические и тематические публикации по исследуемой проблеме.

В качестве материалов для исследования использованы законодательные и нормативные акты, регулирующие банковскую деятельность, официально опубликованные данные международных платежных систем MasterCard Worldwide и Visa International, Центрального Банка Российской Федерации, статистические данные нескольких крупных российских и зарубежных банков по мошенничеству и разработанные ими стратегические меры противодействия, различные аналитические материалы, отражающие реальное развитие технологий противодействия.

3. Обсуждение

Одна из уловок преступников, достаточно часто применяемая для несанкционированного съема денег с банковских карт – так называемый фишинг. Это способ получения реквизитов карты посредством мошеннического обмана ее владельца. Обычно держателям пластика рассылаются СМС якобы от работников банка, в тексте которых предлагается позвонить по указанному телефону, якобы в банк. При разговоре, под благовидным предлогом, у владельца счета выманиваются данные карты необходимые для снятия денег или покупок в интернет-магазинах. Распространен также фишинг с использованием рассылок по электронной почте. Владелец счета получает письмо, якобы из банка, где ему предлагается пройти по указанной ссылке. На специально созданном сайте, интерфейс которого, скорее всего, будет очень похож на настоящий банковский, его уже ждет подробная инструкция и окошечки для ввода конфиденциальной информации. При этом мошенники просят назвать пин-код или реквизиты карты для какой-нибудь системной проверки или подтверждения личности владельца (Аляев, 2010а).

Еще одна уловка мошенников – считывание данных с карты с помощью специальных приспособлений, устанавливаемых непосредственно на банкомат. Подобный способ называется скиммингом и используется главным образом на уличных банкоматах в нелюдных или затемненных местах. К устройству может быть прикреплена мини-видеокамера для «подглядывания» за набором пин-кода, а к отверстию для карт крепится специальная накладка для считывания данных – скиммер. Разновидность скимминга – шимминг, при котором в щель устройства внедряется тонкая и гибкая, практически незаметная пользователю электронная плата для фиксации реквизитов карты. На основе полученных данных умельцы изготавливают поддельные карточки и спокойно снимают по ним денежные средства со счета (Аляев, 2010а).

Ну и совсем уже примитивный, но действенный способ обмана, когда в отверстие банкомата вставляется специальное устройство, не позволяющее извлечь карту. «Случайно» оказавшийся рядом прохожий начинает активно помогать, давая советы и в «благих целях» выманивает у растерявшегося владельца пин-код. Карту, естественно, достать не удается, а после того, как обескураженный клиент уходит разбираться с банком, мошенник извлекает пластик и благополучно снимает деньги (Аляев, 2010а).

Таким образом, для того чтобы украсть деньги с пластиковой карты, мошенники должны получить какой-нибудь из этих четырех компонентов:

- сама пластиковая карта;

- данные о держателе карты – номер, имя владельца, дата окончания срока действия, защитный код CVC, расположенный на обратной стороне карты;
- копию магнитной полосы карты;
- PIN-код карты.

Различные комбинации этих компонентов позволяют мошенникам осуществлять разные виды мошенничества, например:

- если у мошенников есть сама пластиковая карта, но нет PIN-кода, тогда мошенник может выдать себя за законного держателя карты и расплатиться ею в магазине или в сети Интернет. Такая ситуация чаще всего встречается в случае утери или кражи пластиковой карты;
- если у мошенников есть пластиковая карта и PIN-код, то они могут снять с карты всю наличность, которая там есть, через любой банкомат. Если у мошенников есть копия магнитной полосы карты и PIN-код, то они сами могут изготовить копию карты и действовать так же, как и в предыдущем случае;
- если у мошенников есть только данные о держателе карты, то они могут использовать ее для оплаты товаров и услуг через Интернет или по каталогам, где это возможно (Аляев, 2010а).

Внимание банков к проблеме безопасности операций использования и обслуживания таких платежных инструментов, как банковские карты, связано с тем, что увеличение количества действующих карт, развитие инфраструктуры рынка услуг на основе банковских карт и значительный рост объема операций сопровождаются увеличением потерь от действий, мошенников. Помимо прямых финансовых потерь банки несут также и косвенные потери, связанные со снижением уровня доверия, снижением качества обслуживания, потерей существующих и потенциальных клиентов. Наличие прямых потерь от мошеннических операций и значительные косвенные потери вызывают необходимость принятия эффективных мер по обеспечению безопасности операций с банковскими картами и качеству обслуживания держателей карт (Положение об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт, 24.12.2004; Аляев, 2010б).

4. Результаты

Для борьбы с мошенничеством такого рода применяются различные подходы. Платежные системы разрабатывают стандарты безопасности, применение которых снижает риски мошенничества (такие, как PCI DSS, PA DSS, PCI PED и др.), и обязывают все компании их исполнять. Это касается торгово-сервисных организаций, непосредственно принимающих пластиковые карты к оплате, а также банков, процессинговых центров, платежных шлюзов и других организаций, через которые проходят платежи по пластиковым картам. Не забыты и разработчики программного обеспечения для обработки и проведения платежей по картам, а также разработчики устройств ввода PIN-кода, для которых недавно были приняты новые стандарты безопасности (Аляев, 2010б).

Банки, которые авторизуют платежи, и те банки, которые выпускают сами карты, также активно работают над снижением рисков: они внедряют системы мониторинга платежей, позволяющие выявить мошеннические транзакции, разрабатывают правила проведения платежей для торговых точек, предоставляют сервис мгновенного оповещения держателя карты о снятии у него средств по SMS и т.п. (Печникова, Маркова, Стародубцева, 2007).

На сегодняшний день в обиходе самыми распространенными являются карты с магнитной полосой и карты с чипом. Второй вариант в чистом виде в России почти не используется — в качестве его альтернативы используют гибридный вариант (чип + магнитная полоса) (Печникова, Маркова, Стародубцева, 2007).

Для данного типа карты информация заносится на магнитную полосу. Карты с магнитной полосой бывают трёх форматов: ID-1, ID-2, ID-3 (наиболее распространен формат ID-1). Магнитная полоса содержит 3 дорожки (чаще всего используют только 2), на которые в закодированном виде записывают номер карты, срок ее действия, фамилию держателя карты и тому подобные данные. Наиболее полно и точно карты с магнитной полосой описаны в стандартах:

ISO-7810 «Идентификационные карты — физические характеристики»;

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).

Большинство видов пластиковых карт имеют размер, определённый стандартом ISO 7810 ID-1. Какие же средства защиты (помимо магнитной полосы, на которую заносится информация о владельце) позволяют отличить данную карту среди многих других? Подобная информация так же заносится в штрих код. Например, у «Связного банка» при переводе денег на счет достаточно знать именно штрих-код. Идентифицировать владельца так же можно при помощи образца его личной подписи на обратной стороне. Так же все карты имеют идентификационный номер, срок действия и специальный код CVV2 или CVC2 на обороте. Этих данных достаточно, чтобы совершать платежи через Интернет. Многие банки так же наносят на свои карты голографические знаки. В отличие от карт с магнитной полосой, при совершении транзакций задействуется именно информация с чипа. Чип обладает большим объемом памяти, и информация на нем подвергается более сложному типу шифрования. При осуществлении транзакции картой с магнитной полосой, она всегда имеет одинаковые идентифицирующие карту данные, которые передаются в банк. Поэтому их можно скопировать и изготовить поддельную карту. Микропроцессорная карта работает иначе: каждая транзакция подтверждается специально сформированным для нее кодом, и для каждой последующей операции требуется новый код, сделать дубликат фактически невозможно. Гибридный вариант прижился ввиду сложного перехода техники принимающей карты на новый тип данных. Сейчас чипы умеют читать практически все устройства принимающие 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 (Печникова, Маркова, Стародубцева, 2007).

Вернемся к тому, как же так получилось, что с карты (находящейся всегда у владельца при себе) были сняты все накопления. Я могу только догадываться, т.к. все что у меня есть это образование в сфере ИТ и Интернет (который знает все). Злосчастная карта относилась к самому дешевому в обслуживании типу карт. Обычная карта с магнитной полосой (даже не именная). Какие меры защиты присутствовали на карте:

Визуальная. Каждый финансовый документ имеет определенный размер и создана из определенной толщины пластика. На карте имеется информация — это ФИО владельца, номер, срок действия, дополнительные сведения. Есть логотип, например, Visa. Также присутствует специальное поле с подписью владельца.

Магнитная полоса с информацией о владельце. Она играет роль своеобразного жёсткого диска. На ней хранятся сведении о счёте и самом владельце. Именно с помощью полосы происходят все денежные операции. С ее помощью открывается доступ к счёту. Эта самая не защищённая часть на карточке.

СМС-информирование о транзакциях

Пин-код

Штрих-код

Чип. На карте одновременно может быть и чип, и полоса. Маленький процессор защищает карту, если вы расплачиваетесь ею в торговых точках. Вся информация зашифрованная. Чтобы узнать сведения на чипе необходимо знать специальный код. Это одна из надежных систем защиты (Печникова, Маркова, Стародубцева, 2007).

Магнитная полоса удачно копируется специальным устройством — скиммером. После чего изготавливается дубликат карты и все что остается это узнать пин-код карты. Для этого обычно в паре со скиммером используется скрытая видеокамера или же если это сам злоумышленник в лице официанта или продавца, то он старается подсмотреть пин-код. Еще более технологичный вариант, когда к устройству ввода подключается считыватель вводимых данных (Аляев, 2010а).

Так же для получения данных у владельцев используются фишинговые сайты или рассылки где владельцев карт просят ввести их секретную информацию (номер карты CVV2 или CVC2 и т.п.).

Довольно распространенные случаи, когда злоумышленники портят считыватель карт, так чтобы карта там застряла. Если владелец уходит, то появляется злоумышленник и завладевает картой (Аляев, 2010а).

Существует разновидность другого метода — кардинга (англ. carding – прочесывание). В этом случае злоумышленник завладевает базой интернет-магазина или какого-нибудь онлайн банка и снимает деньги с карт, к которым удается получить доступ.

Сейчас набирает обороты более сложный вариант скимминга — шимминг (от англ. тонкая прокладка). Эти устройства, в отличие от скиммеров, незаметны: тонкая гибкая плата толщиной около 1 мм вставляется через щель картридера и считывает данные введенных карт, позволяя похитить номер карты и ее пин-код. Эксперты успокаивают, что до России такой вид мошенничества пока не дошел, так как это довольно дорого и трудноосуществимо. (На мой взгляд, мне попался именно этот вариант, так что эксперты могут брать себе на заметку) (Аляев, 2010а; Печникова, Маркова, Стародубцева, 2007).

Подпись на обратной стороне. Данный тип защиты вообще абсурден, если карта как в моем случае неименная, ибо владельцем может быть любой, кто нанесет подпись. В случае с дубликатом ничего не мешает нанести свою подпись и свои имя, фамилию на изготовленную копию. По своему опыту — проходил пол года с картой, где стерлась подпись на обороте и только потом мне указали на это и заставили при них оставить автограф (что еще абсурднее) (Печникова, Маркова, Стародубцева, 2007).

Голограмма с логотипом банка. Как способ подтвердить, что у вас не поддельная карта на руках вполне может быть, но не более того.

Очень полезная вещь СМС-информирование, вы всегда будете видеть, как утекают ваши деньги. Мои утекли за 2 минуты. На то чтобы дождаться ответа от оператора в банке после череды автоответчиков и переадресаций ушло около 1,5 минут. Надо заметить, что телефон вообще можно оставить дома или он может разрядиться или не быть доступа в сеть, да и много всего еще. Так что как способ защиты очень сомнителен. Тем более как подсказали пользователи @MyHabrahabr и @SpiritOfVox есть способ вообще блокировать телефон жертвы на момент «потрошения» ее карты (Печникова, Маркова, Стародубцева, 2007).

Как бы это ни было печально, но законодательной базы регламентирующей ответственность банков при осуществлении мошеннических действий с пластиковыми картами в России пока нет. Как показывает практика, это не гарантирует возврата денег или процесс может затянуться на долгое время. Все случаи рассматриваются каждым банком в отдельности. Они проводят свое собственное расследование и, как правило, если вы нарушили хоть один пункт договора по использованию пластиковой карты (передали третьим лицам, хранили пин-код в доступном для других месте, сообщали информацию о сроке службы, номере карты или cv1/cv2 коды третьим лицам), то в возврате средств будет отказано. Для того чтобы иметь основания и написать заявление в банк — нужно дождаться подтверждения прохождения транзакции (около 3-х дней). До этого момента деньги еще фактически находятся на вашем счету, и оснований для обжалования транзакции нет. Обычно, для того чтобы вернуть похищенные мошенниками деньги, клиенту российского банка нужно выполнить ряд условий, но в первую очередь своевременно заблокировать карту и в нужный срок написать заявление. Если злоумышленнику удастся получить копию вашей карты без чипа и пин-код, то, скорее всего, такие операции не отличить от совершенных вами лично и тут тоже напрашивается отказ (Постановление Правительства РФ «Положение об осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт без применения контрольно-кассовой техники», 31.03.2005; Федеральный закон «О банках и банковской деятельности», 02.12.1990; Федеральный Закон «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт», 22.05.2003).

5. Выводы

Всех описанных выше неприятностей можно легко избежать, если придерживаться золотого правила: никогда, никому и ни под каким предлогом не сообщать реквизиты банковской карты. Следует помнить, что ни один работник банка не попросит клиента сообщить ему коды, пароли и прочие подобные данные. Специалисты банков делают все от них зависящее, чтобы обезопасить карты и счета своих клиентов. Буквально до каждого доводятся подробные инструкции по обеспечению безопасности, главное правило которых – никогда не терять бдительность, а в случае утери пластика или его компрометации немедленно блокировать карту и связаться со специалистами. Действенная мера безопасности – подключение услуги СМС-оповещения об операциях по карте. Полученная вовремя информация о несанкционированном доступе к счету позволит оперативно принять меры (Корнев, Костюченко, 2006).

Несколько практических советов:

1) Если у вас все еще обычная карта с магнитной полосой — поменяйте ее на карту с чипом (не настолько она дороже, зато деньги целее будут).

2) Никогда не пишите PIN-код на карте. Это все равно, что оставить открытую машину с ключами в замке зажигания, так же не храните записанный PIN-код вместе с картой. Безопаснее всего, если вы выучите код наизусть и вообще не будете его хранить в письменном виде.

3) Никогда не выпускайте карту из поля зрения. Это доступ к вашим деньгам. Представьте, что вместо карты вы даете кассиру или официанту все деньги, которые у вас есть на счете и просите его взять сколько нужно.

4) Установите лимит на снятие денежных средств в течение суток. При включенном СМС-информировании это позволит с меньшими потерями успеть заблокировать карту.

5) Блокируйте карту сразу, как появится подозрительная транзакция, многие банки позволяют производить блокировку/разблокировку карты по телефону.

6) Внимательно смотрите на устройства, в которые вставляете карту и не передавайте ее третьим лицам.

7) Не ошибайтесь при вводе PIN-кода больше двух раз. После трех ошибочных вводов кода банкомат может задержать вашу карту или в лучшем случае заблокировать дальнейшие операции по ней.

8) Если карта застряла в банкомате — сначала блокируйте ее, потом можно и бросить, если нет времени или нет возможности найти лицо уполномоченное извлечь карту из банкомата (Балабанов, 2001; Ивлев, Попова, 2002).

Пользователям интернет-банкинга настоятельно советуется по возможности не проводить финансовые операции с компьютеров посторонних лиц, а на своем установить пакет программ безопасности. Не используйте для оплаты в Интернете карты, на которых у вас находятся крупные суммы денег. Лучше вообще завести для таких целей специальную отдельную карту для расчетов в Интернете и переводить туда деньги по мере необходимости. Покупки в интернет магазинах и прочих интернет-сервисах следует проводить осторожно, а предпочтение отдавать проверенным сайтам с солидной репутацией и системой безопасности. Обязательно установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения (Аляев, 2011).

Ну и самое простое: прежде чем снять деньги в уличном банкомате, неплохо его осмотреть, а при малейших подозрениях или сомнениях лучше отложить операцию. Наиболее безопасны в использовании банкоматы в фойе банков, крупных магазинах или в других охраняемых местах. Обеспечить безопасность банковских карт и интернет-банкинга не так сложно, нужно лишь установить для себя ряд разумных правил поведения и никогда от них не отступать.

Примечания

Абдеев, 1994 - *Абдеев П.Ф.* Философия информационной цивилизации. М.: Владос, 1994. 203 с.

Аляев, 2010а - *Аляев Д.А.* Актуальные категории карточного мошенничества и механизмы его предотвращения. Социально-экономические проблемы кооперативного сектора экономики. Материалы III Международной научно-практической конференции молодых ученых-преподавателей, сотрудников, аспирантов и соискателей. М.: Российский университет кооперации, 2010. с. 25-28.

Аляев, 2010б - *Аляев Д.А.* Банковские риски при операциях с кредитными картами. // Российское предпринимательство, 2010. №9 (2), с. 99-104.

Аляев, 2011 - *Аляев Д.А.* Практические аспекты функционирования систем мониторинга транзакций по банковским картам. // *Финансы и кредит*, 2011. №19 (451), с. 42-45.

Балабанов, 2001 - *Балабанов И.Т.* Электронная коммерция. СПб.: Питер, 2001.

Ивлев, Попова, 2002 - *Ивлев В., Попова Т.* Balanced ScoreCard – альтернативные модели. // *Банки и технологии*. 2002. №4.

Корнев, Костюченко, 2006 - *Корнев В.С., Костюченко А.С.* Автоматизация моделей рыночной экономики (на примере модели системы безналичных расчетов с применением пластиковых карт). М.: Спутник, 2006.

Лаврушин, 2001 - *Лаврушин О.И.* Банковское дело: Учебник 2-е изд., перераб. и доп. М.: Финансы и статистика, 2001.

Печникова и др., 2007 - *Печникова А.В., Маркова О.М., Стародубцева Е.Б.* Банковские операции. М.: ИНФРА-М, 2007. 366 с.

Положение об эмиссии..., 2004 - Положение об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт (24.12.2004). N 266-П, утв. ЦБ РФ.

Постановление Правительства РФ, 2005 - Постановление Правительства РФ «Положение об осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт без применения контрольно-кассовой техники» от 31.03.2005 N 171.

Федеральный закон «О банках...», 1990 - Федеральный закон «О банках и банковской деятельности» от 02.12.1990 N 395-1.

Федеральный закон «О применении...», 2003 - Федеральный Закон «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт» от 22.05.2003. N 54.

References

Abdeev, 1994 - Abdeev P.F. (1994). Filosofiya informatsionnoi tsivilizatsii. M.: Vlados, 203 s.

Alyaev, 2010a - Alyaev D.A. (2010). Aktual'nye kategorii kartochnogo moshennichestva i mekhanizmy ego predotvrashcheniya. Sotsial'no-ekonomicheskie problemy kooperativnogo sektora ekonomiki. Materialy III Mezhdunarodnoi nauchno-prakticheskoi konferentsii molodykh uchenykh-prepodavatelei, sotrudnikov, aspirantov i soiskatelei. M.: Rossiiskii universitet kooperatsii, s. 25-28.

Alyaev, 2010b - Alyaev D.A. (2010). Bankovskie riski pri operatsiyakh s kreditnymi kartami. Rossiiskoe predprinimatel'stvo, №9 (2), s. 99-104.

Alyaev, 2011 - Alyaev D.A. (2011). Prakticheskie aspekty funktsionirovaniya sistem monitoringa tranzaktsii po bankovskim kartam. Finansy i kredit, №19 (451), s. 42-45.

Balabanov, 2001 - Balabanov I.T. (2001). Elektronnaya kommertsiya. SPb.: Piter.

Ivlev, Popova, 2002 - Ivlev V., Popova T. (2002). Balanced ScoreCard – al'ternativnye modeli. Banki i tekhnologii. №4.

Kornev, Kostyuchenko, 2006 - Kornev B.C., Kostyuchenko A.C. (2006). Avtomatizatsiya modelei rynochnoi ekonomiki (na primere modeli sistemy beznalichnykh raschetov s primeneniem plastikovykh kart). M.: Sputnik.

Lavrushin, 2001 - Lavrushin O.I. (2001). Bankovskoe delo: Uchebnik 2-e izd., pererab. i dop. M.: Finansy i statistika.

Pechnikova i dr., 2007 - Pechnikova A.B., Markova O.M., Starodubtseva E.B. (2007). Bankovskie operatsii. M.: INFRA-M, 366 s.

Polozhenie ob emissii..., 2004 - Polozhenie ob emissii bankovskikh kart i ob operatsiyakh, sovershaemykh s ispol'zovaniem platezhnykh kart (24.12.2004). N 266-P, utv. TsB RF.

Postanovlenie Pravitel'stva RF, 2005 - Postanovlenie Pravitel'stva RF «Polozhenie ob osushchestvlenii nalichnykh denezhnykh raschetov i (ili) raschetov s ispol'zovaniem platezhnykh kart bez primeneniya kontrol'no-kassovoi tekhniki» ot 31.03.2005 N 171.

Federal'nyi zakon «O bankakh...», 1990 - Federal'nyi zakon «O bankakh i bankovskoi deyatel'nosti» ot 02.12.1990 N 395-1.

Federal'nyi zakon «O primenenii...», 2003 - Federal'nyi Zakon «O primenenii kontrol'no-kassovoi tekhniki pri osushchestvlenii nalichnykh denezhnykh raschetov i (ili) raschetov s ispol'zovaniem platezhnykh kart» ot 22.05.2003. N 54.

УДК 004.056.5

Банковские карты и безопасность

Юрий Федорович Каторин [a, *]

[a] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Российская Федерация

Аннотация. Данная статья посвящена вопросам обеспечения безопасности денежных средств, при использовании банковских карт, ибо финансовые операции такого рода издавна являлись объектом повышенного внимания со стороны отдельных нечестных личностей, описываются особенности карт с магнитной полосой и карты с чипом, а так же приводится перечень основных уловок преступников, применяемых для несанкционированного съема денег, даются рекомендации по обеспечению безопасности операций использования и обслуживания банковских карт.

Ключевые слова: пластиковая банковская карта, мошенничество, несанкционированный съем денег, безопасность денежных средств, использование банковских карт.

* Корреспондирующий автор
E-mail addresses: katorin@mail.ru (Ю.Ф. Каторин)