

достоверная отчетность, а также ее прозрачность может стать залогом формирования качественного рынка банковских услуг - рынка покупателя, который свободен самостоятельно принимать решения.

**Список литературы:**

1. О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации. Указание ЦБ РФ от 12.11.2009г. №2332-У [Электронный ресурс]– Режим доступа: <http://base.consultant.ru>. Дата обращения: 09.05.2013г.
2. Об опубликовании и представлении информации о деятельности кредитных организаций Указание ЦБ РФ от 20.01.2009 N 2172-У [Электронный ресурс] – Режим доступа: <http://base.consultant.ru>. Дата обращения: 09.05.2013г.
3. О представлении и опубликовании кредитными организациями годовой финансовой отчетности, составленной в соответствии с МСФО. Указание ЦБ РФ от 16.01.2013г. №2964-У [Электронный ресурс] – Режим доступа: <http://base.consultant.ru>. Дата обращения: 09.05.2013г.
4. Лаврушин, О.И. Банковское дело [Текст]: учебник / О.И. Лаврушина. - М.: Финансы и статистика, 2011.- 768 с.

**Рыкова Ирина Анатольевна,**  
к.э.н., доцент кафедры финансов и кредита  
Орловского государственного института экономики и торговли  
e-mail: [olegnashevce-orel@yandex.ru](mailto:olegnashevce-orel@yandex.ru)

**Борякова Наталия Михайловна**  
студентка финансово-экономического факультета  
Орловского государственного института экономики и торговли  
e-mail: [olegnashevce-orel@yandex.ru](mailto:olegnashevce-orel@yandex.ru)

**УДК 336.717.1**

**О.А. Степанова, Е.П. Артеменко, В.М. Якушенко**

**ОБЕСПЕЧЕНИЕ РАСЧЕТОВ ПЛАСТИКОВЫМИ КАРТАМИ**

*Внедрение пластиковых карточек является важнейшей тенденцией развития технологий безналичного оборота в банковской деятельности. Как финансовый инструмент карточки постоянно совершенствуются, растет сфера их применения, расширяется комплекс оказываемых услуг. Банковские пластиковые карты давно стали мишенью для преступных посягательств, как и всякий высокодоходный бизнес в сфере безналичного оборота.*

*Ключевые слова: банковская пластиковая карта, дебетовые карты, кредитные карты, денежный оборот, безналичный расчет, скимминг, фишинг, эквайринг.*

Современные этапы развития банковского сектора характеризуется расширением объема и структуры денежного оборота, осложнением расчетов, необходимостью уменьшения финансовых рисков и налаживанием действенного контроля за системой денежного оборота. Выполнение таких сложных задач

может быть обеспечено существенным расширением безналичных расчетов, новых банковских услуг.

Одной из таких банковских услуг является создание системы массовых электронных платежей с помощью банковских платежных пластиковых карточек.

Банковская карта (BC, VCard, BankCard) – пластиковая карта, привязанная к одному или нескольким расчётным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных. Карты бывают дебетовые и кредитные. Дебетовые карты используются для распоряжения собственными деньгами, находящимися на расчетном счете в банке. Кредитные карты используются в качестве альтернативы кредитам, т.е. этими картами клиент расплачивается деньгами банка, которые необходимо будет вернуть банку, но уже на более лояльных условиях, нежели кредит.

Система безналичного расчёта была создана в США во времена «торгового бума» (1940 – 1950-е годы). В большинстве своём она заменила чековые книжки. В процессе своего развития происходила техническая модернизация карт. Сначала это был просто кусочек картона, затем он стал работать по принципу перфокарты, в начале 1970-х была разработана магнитная полоска, а в конце 1990-х в кредитные карты стали интегрироваться чипы.

Первая универсальная кредитная карта (DinersClub) появилась в 1950 г. [4].

Безналичный расчёт в современных условиях играет ведущую роль. В некоторых странах, таких как США, безналичные расчеты составляют около 90%. В России же доля безналичных расчетов постепенно растет на 10-15% и за I квартал 2013 г. составила 52%, в то время как в 2012 г. этот показатель составлял 42% [3].

Пластиковые карточки по своему экономическому смыслу предназначены для сокращения части наличности в обороте, ускорения расчётов и для расширения объемов доступных клиентам услуг.

По данным Банка России, количество банковских карт, выпущенных в России для физических лиц, по состоянию на 1 января 2011 г. составило 144 млн. 112 тыс. штук против 125 млн. 787 тыс. карт на начало 2010 г.. Активно растет и суммарный объем операций по банковским картам: по информации AnalyticResearchGroup, в прошлом г. он достиг 12094,1 млрд. руб., увеличившись за год на 27,7%, в то время как в 2009 г. рост составлял лишь 8%. Однако, по сути, граждане карточками и не пользуются вовсе, а лишь снимают наличные [2].

Наряду с развитием безналичного оборота, а именно пластиковых карт, развивались способы злоупотребления пластиковыми картами. Тогда же появились и первые подделки.

Основными видами мошенничества с пластиковыми картами являются скимминг и фишинг. Менее распространено такое понятие, как «трапинг» - когда в картоприемник банкомата вставляется фото пленка, удерживающая карту в определенном положении. Далее злоумышленник под видом сотрудника бан-

ка или просто желающего помочь предлагает ввести ПИН-код якобы для того, чтобы извлечь карту из банкомата. Когда же жертва отчаивается и уходит разбираться с банком, злоумышленник извлекает карту и при помощи подсмотренного ПИН-кода тут же снимает с неё денежные средства.

Иногда деньги пропадают с карточных счетов в результате кражи кошелька. Происходит это, как правило, потому, что держатели карт пренебрегают правилами пользования платежной картой и хранят карты вместе с ПИН-кодом или же пишут его прямо на карте.

Известны также случаи подмены карт – когда у владельца берут карту для расчета, скажем, в ресторане – и возвращают, но уже не его карту. Не заметивший подмены клиент в ближайшее время узнает о пропаже денег со своего карточного счета.

Банки не меньше держателей карт заинтересованы в решении данной проблемы, так как прослеживается тенденция роста потерь банков из-за действий мошенников. Поэтому банки вынуждены обращать большое внимание на обеспечение безопасности этих операций.

Для обеспечения безопасности транзакций по банковским картам банки либо самостоятельно разрабатывают всевозможные программы защиты, либо прибегают к помощи компаний по защите информации.

Система контроля операций с пластиковыми картами, исходя из возможных рисков, обычно включает в себя 2 направления:

1. Служба внешнего (со стороны банка) контроля за операциями с пластиковыми картами.

Это направление обеспечивается сотрудниками общепанковской системы безопасности, в их задачи входит:

- проверка клиентов перед принятием решения о выдаче карточки;
- проверка торговых фирм перед заключением договора эквайринга;
- в тех случаях, когда факт мошенничества налицо, принятие мер по розыску владельца карты и, по возможности, сокращению потерь банка;
- выезды в торговые точки по сигналу о попытке использовать поддельную или украденную карту.

2. Служба обеспечения безопасности расчетов непосредственно в Департаменте пластиковых карт.

Выделение такого подразделения обосновано требованиями большого объема специальных знаний и навыков:

- особенности работы с пластиковыми картами на каждом этапе их изготовления и использования;
- доступ к информации по карточкам и транзакциям по ним;
- требования платежных систем по обеспечению безопасности;
- правила решения спорных вопросов с другими банками-участниками;
- участие в разработке договоров, инструкций;
- поддержание контактов со службами безопасности платежных систем и других банков участников.

Для работы в этой группе требуется хороший английский для оперативного решения вопросов с другими банками и службами платежных систем.

Основные направления обеспечения безопасности:

- обеспечение физической и технологической безопасности процесса производства карточек, процессирования транзакций и процесса авторизации;
- обеспечение проверки персональных данных потенциальных владельцев карт;
- обеспечение информационно-аналитической деятельности по раннему выявлению мошеннических действий с пластиковыми картами;
- обеспечение физической и технологической безопасности. Как правило, подразделение банка, занимающееся пластиковыми картами, состоит из трех основных технологических модулей:
  - а) прием и обработка заявлений на выпуск карт;
  - б) персонализация карт и печать ПИН-конвертов;
  - в) модуль обеспечения авторизации и обмена финансовой информацией с платежными системами.

Основная задача - исключить возможность исчезновения заготовок карточек, изготовленных карточек и ПИН-конвертов, расходных материалов (слипы и прочее), а также информации в любом виде о параметрах выпускаемых карт (номер, срок действия, имя владельца, лимиты, информация с магнитной полосы).

Новые технологии позволяют сегодня распознавать мошеннические операции в режиме реального времени. Это круглосуточный мониторинг операций по картам клиентов с возможностью распознавания мошеннических операций в режиме реального времени. При первом же подозрении на несанкционированность операции карта блокируется. Также одним из эффективных методов борьбы является сотрудничество с другими банками и правоохранительными органами при выявлении мошеннического использования платежных карт.

Все банки всегда предлагают клиенту подключить услугу SMS-банкинга, которая позволяет контролировать доступ к средствам на счете и получать отчет о любой только что проведенной операции. В банках работают круглосуточные службы поддержки (Контакт – центр), куда можно и нужно обращаться в случае кражи или утери карты, а также при обнаружении несанкционированных операций. Своевременное обращение в службу поддержки, как правило, почти всегда позволяет избежать нежелательного развития событий.

Если расследование, проведенное банком, указало на непричастность клиента к проведению операции по платежной карте и доказало, что клиент пострадал от действия мошенников, убытки клиенту банк компенсирует в полном объеме.

В Европе лидером по темпам роста мошенничества с банковскими картами является Россия. За 2012 г. ущерб от мошенничества увеличился на 35%. Совокупные убытки от противоправных действий с банковскими картами в Европе в 2012 г. выросли на 6%, по сравнению с 2011 г. Франция, Россия и Вели-

кобритания обеспечили 80% этого роста [1].

В России рост мошенничества по операциям с картами прежде всего связан с ростом карточного кредитования. В 2012 г. его объемы выросли более чем на 100%.

Средний размер займа, полученного с помощью кредитной карты, - 51,1 тыс. рублей. При этом на 1 мая 2013 г. количество кредитов, по которым не было ни одного платежа (то есть с признаками мошенничества), составило 679 тыс., что на 43% больше, чем год назад [5].

Для борьбы с «скиммингом» применяются самые разнообразные методы. При этом одними из самых активных «борцов» являются производители банкоматов, которые в стремлении защитить свою продукцию изобретают различные приспособления, препятствующие установке несанкционированного оборудования, с помощью которого скиммеры похищают информацию о картах.

Антискимминговый модуль безопасности, устанавливаемый на банкомат, оборудован специальными датчиками для контроля области картоприемника, позволяющими выявлять несанкционированную установку на банкомат любых посторонних устройств. При подозрении на подобное подключение модуль подает сигнал оповещения в соответствующие службы, ответственные за обеспечение безопасности банкоматов, одновременно останавливая работу банкомата, подвергнувшегося атаке.

Некоторые производители стараются заложить средства и механизмы обеспечения безопасности в самой основе конструкции банкоматов. Например, устройство считывания пластиковых карт имеет специальное исполнение наружной части – закругленная форма участка передней панели банкоматов вокруг картоприемника делает практически невозможной установку скиммера. Кроме того, устройство считывания пластиковых карт оснащается механизмом вибрации, который встряхивает карту во время загрузки – меняет скорость движения карты и использует серию быстрых остановок и пусков. Подобный эффект тряски препятствует точному считыванию данных с карты с помощью скиммера, установленного преступником.

Одним из средств борьбы со скиммингом является эмиссия банком платежных карт с использованием микрочипа. Данные с такой карты считать гораздо сложнее, кроме того, в случае если это получится – существует возможность возврата похищенных денежных средств.

Большая роль в борьбе со скиммерами принадлежит бдительности держателей платежных карт. Поэтому необходимо помнить о тех элементарных мерах безопасности, к которым нас призывает банк:

- не хранить пластиковую карту рядом с ПИН-кодом, не записывать ПИН-код на самой карте;
- не передавать карту третьим лицам;
- не расплачиваться за покупки в интернете с незнакомых или подозрительных сайтов;

- при оплате с карты ставьте подпись только в тех чеках, в которых верно указана сумма совершенной вами покупки;
- регулярно (не реже одного раза в месяц) проверяйте выписки по банковскому счету;
- в случае потери или кражи карты немедленно обращаться в банк;
- при получении любых запросов (по электронной почте, телефону и иным способом) с просьбой подтверждения персональных данных и сведений о Вашей карте не передавайте информацию по Вашей карте (ПИН-код, номер карты, срок окончания действия карты, CVC2/CVV2 – код безопасности), так как данные сообщения используются злоумышленниками в целях получения конфиденциальной информации для последующего использования в мошеннических целях.

Похищенные деньги вернут держателю карты в случае, если доказана вина сотрудников банка или же найден мошенник. Если же в результате проверки выявлено, что деньги похищены вследствие несоблюдения держателем пластиковой карты правил её использования, то банк может помочь только в плане предоставления информации о движениях на карточном счете.

В России до сих пор не принят закон, который бы защищал держателей карт от незаконного списания средств. В 2013 г. предполагалось ввести поправки, обязывающие банки возвращать клиентам незаконно списанные средства с их карт еще до окончания расследования, но их принятие отложили еще на год.

#### **Список литературы:**

1. Официальный сайт Национального агентства финансовых исследований (НАФИ) [Электронный ресурс]. - Режим доступа: <http://banki.ru>. Дата обращения: 20.05.13.
2. Официальный сайт газеты «Новые известия» [Электронный ресурс]. - Режим доступа: <http://www.newizv.ru>. Дата обращения: 20.05.13.
3. Рынок. Финансы. Недвижимость. [Электронный ресурс]. - Режим доступа: <http://sia.ru>. Дата обращения: 19.05.13.
4. Википедия [Электронный ресурс]. - Режим доступа: <http://ru.m.wikipedia.org/wiki/>. Дата обращения: 19.05.13.
5. Экономика [Электронный ресурс]. - Режим доступа: <http://www.newsru.com/>. Дата обращения: 22.09.13.

**Степанова Оксана Александровна**

*к.э.н., доцент кафедры финансов и кредита*

*Орловского государственного института экономики и торговли*

*e-mail:artemenko.alla@inbox.ru*

**Артеменко Екатерина Петровна**

*студентка инженерно-технологического факультета*

*Орловского государственного института экономики и торговли*

*e-mail:artemenko.alla@inbox.ru*

**Якушенко Валентина Михайловна**

*студентка финансово-экономического факультета*

*Орловского государственного института экономики и торговли*

*e-mail:artemenko.alla@inbox.ru*