9. Цитаты Владимира Владимировича Путина О запуске масштабной системной программы развития цифровой экономики [Электронный ресурс] TADVISER – Режим доступа: http://www.tadviser.ru/index.php

УДК 004

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Е.В. Ильинская, А.О. Курбанов
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В статье проведен анализ видов банковских карт в России, выделены основные группы риска при дистанционном банковском обслуживании, рассмотрен перечень мер, которые позволят предотвратить рассмотренные риски.

Ключевые слова: *дистанционное банковское обслуживание, банковские карты, риски при использовании банковских карт, снижение риска мошеннических операций.*

INFORMATION SECURITY AT REMOTE BANKING SERVICE

E.V. Ilinskaja, A.O. Kurbanov
Belgorod, Russia
Belgorod state national research University

The article analyzes the types of Bank cards in Russia, identifies the main risk groups in remote banking, considers a list of measures that will prevent the risks.

Keywords: *remote banking, Bank cards, risks when using Bank cards, reducing the risk of fraudulent transactions.*

Конкуренция, а также необходимость привлекать новых клиентов вынудили банки использовать дистанционное банковское обслуживание. Это обеспечивает повышение конкурентоспособности банка и позволяет привлекать новых клиентов. Дистанционное банковское обслуживание неразрывно связано с информационными технологиями. Несмотря на разнообразие и надежность современных средств безопасности, они не гарантируют отсутствие риска при совершении банковских операций.

Известными формами ДБО являются операции с банковскими картами. Одной точки зрения относительно понятия «банковская карта» не существует. Банковскую карту можно определить как средство управления или распоряжения денежными средствами ее держателя в целях оплаты товаров и услуг, а также для получения наличных денег и валюты [1, с. 266]. Благодаря универсальности и удобству использования, банковские карты используются повсеместно – в сферах розничных услуг, банковской и бюджетной.

В России существуют следующие виды банковских карт:

1. Расчетная (дебетовая). Предназначена для операций с средствами держателя карты на его банковском счете.
2. Кредитная. Используется для совершения операций с денежными средствами, предоставленными кредитной организацией держателю карты.
3. Предоплаченная. Предназначена для совершения операций с электронными деньгами [2].

Следует отметить, что банковские карты не поддерживают операции с электронными деньгами, а представляют собой инструмент управления банковским счетом, то есть дают возможность распоряжаться только обычными деньгами, имеющие безналичную форму [3, с. 194].

В последние годы заметна тенденция к увеличению количества эмитента (выпуска) банковских карт. Так, количество расчетных и кредитных карт, эмитированных кредитными организациями, выросло с 100 млн единиц в 2008 году до более чем 270 млн в 2019 году, то есть, более, чем вдвое. При этом большую долю из них приходится на расчетные карты – около 87%, на кредитные же – 12,9% [4]. Главными причинами этого являются удобство пользования картами для клиентов (например, получение нецелевого кредита), развитие технологической инфраструктуры, расширение функциональных возможностей банкоматов и прибыль для банков – банки взимают процент или комиссию от суммы денежных средств при проведении различных операций с картой (например, при обслуживании клиента другого банка с помощью банкомата).

Для совершения операций с банковской картой используется соответствующее оборудование – банкоматы, терминалы для безналичной оплаты – и программное обеспечение. Очевидно, что существует риск поломки оборудования, возникновения сбоя, а также мошенничество. В этом случае пользователь карты может потерять собственные деньги, в то время как банк может столкнуться со снижением деловой репутации [5, с. 100].

Поэтому условно можно выделить следующие группы риска при использовании банковских карт:

1. Риски, связанные с обслуживанием банковских карт с помощью соответствующего оборудования и программного обеспечения.
2. Риски, связанные с деятельностью банка-эмитента карты.
3. Риски, связанные с деятельностью мошенников.

Первая группа охватывает такие риски, как:

- выход из строя (поломка) оборудования, обслуживающего банковскую карту;
- сбой или отказ в работе банковской информационной системы;
- ошибки пользователя при работе с оборудованием;
- сбой в работе систем связи.

Это риски, связанные в основном с отказом или прекращением обслуживания клиента по техническим причинам или же причинам, связанным с человеческим фактором, то есть ошибками самого клиента. Проявлением ошибок клиента при работе с оборудованием может служить блокирование карты и средств, размещенных на ней, при неправильном многократном наборе ПИН-кода и незнании кодового слов. Такого рода проблемы, как правило, клиент решает путем обращения к сотрудникам банка.

Ко второй группе рисков можно отнести:

- преднамеренное сокрытие фактов совершения операций и сделок;
- нарушение договора об использовании банковской карты;
- неадекватная организация информационной системы банка;
- применение неэффективных средств безопасности.

Подобные риски наиболее часто возникают при пользовании услугами небольших банков, которые либо не имеют средств для приобретения надежных и безопасных информационных систем, либо занимаются нелегальной деятельностью в целях получения прибыли или обслуживания интересов конкретных физически лиц или организаций. Большое количество подобных банков стало причиной начала так называемой «чистки банковского сектора» Центральным Баном РФ. Данные мероприятия привели к уменьшению общего числа банков, работающих в РФ, с 2013 по 2019 год примерно вдвое [6].

К третьей группе рисков относятся действия мошенников, направленные, в основном, на получение конфиденциальной информации о жертве, которая обычно использоваться для кражи денежных средств с банковской карты. Наиболее часто мошенничество осуществляется при помощи банкоматов.

В свою очередь, риски третьей группы можно разбить на две подгруппы – социальные и технологические.

Первая подгруппа включает в себя виды мошенничества, основанные на использовании человеческого фактора. Все виды этой группы мошенничества связаны с введением в заблуждение жертвы, в результате чего жертва выдает конфиденциальную информацию. К видам социального мошенничества относятся:

1. Мошенничество по телефону. Осуществляется путем установления контакта с потенциальной жертвой при помощи мобильной связи, то есть, с помощью телефонного звонка или SMS. Мошенник выдает себя за банковского служащего или служащего другой организации и под различными предлогами пытаются вынудить жертву получить конфиденциальную информацию или совершить перевод денежных средств на банковский счет или номер мобильного телефона.

2. Фишинг. Характеризуется созданием в интернете сайтов, внешне напоминающие официальные сайты банков или других организаций. Одновременно они различными способами, например, массовой рассылкой писем по электронной почте писем и сообщений в социальных сетях, распространяют ссылки на данный сайт. В сообщениях запрашивается конфиденциальная информация. Фишинг имеет разновидности:

– spearphishing – мошенники заранее выбирают себе определенную группу людей по какому-либо признаку и атакуют эту группу;

– twinphishing – рассылаются поддельные письма, которые внещне схожи с настоящими письмами банков;

– smishing – характеризуется попыткой получить информацию с помощью SMS;

– vishing – характеризуется попыткой получить информацию с помощью эмуляции звонка из колл-центра банка;

– whalephishing – потенциальными жертвами являются менеджеры высшего звена и/или руководство компаний. Перед каждой атакой мошенники собирают большой объем личной информации о потенциальной жертве, что повышает вероятность успеха фишинга.

К второй подгруппе относятся мошеннические операции с использованием специальных технических средств и программ. К ним относятся:

3. «Ливанская петля». Мошенники устанавливают в картоприемник банкомата или платежный терминал техническое устройство, которую часто называют «ливанской петлей», блокирующее вставляемую карту, тем самым делая невозможным её извлечение после окончания сеанса обслуживания. С помощью обмана или заранее установленных других устройств (например, накладная пластина на клавиатуру, микрокамера и пр.) у законного владельца узнается ПИН-код. Как только владелец карты уходит от банкомата или платежного терминала, мошенники вынимают устройство из банкомата вместе с зажатой в нем картой.

4. Скимминг. Заключается в использовании нескольких устройств для получения конфиденциальной информации. В число данных устройств может входить: скиммер – устройство для чтения данных с магнитной полосы банковской карты, поддельная клавиатура для ввода ПИН-кода жертвой, скрытая камера – для фиксации вводимого ПИН-кода. Также может применяться вредоносная программа, встроенная в банкомат. Выделяют следующие виды скримминга:

– мошенничество с использованием банкомата, платежного терминала или дверного замка при входе в круглосуточную зону самообслуживания для клиентов;

– мошенничество в организациях, работающих в сфере торговли или услуг. В данном случае с помощью специального оборудования сотрудники данных организаций в целях совершения мошеннических действий копируют данные с магнитной полосы карты клиента, когда принимают её у клиента для оплаты товаров (услуг), добиваясь отсутствия карты в поле зрения владельца [7].

Теперь рассмотрим перечень мер, которые позволят предотвратить рассмотренные риски. Эти меры предназначены для соблюдения как банками, так и их клиентами.

Чтобы минимизировать риски первой группы, руководству банка следует обращать пристальное внимание на подбор сотрудников в ИТ-отдел. Это способствует снижению количества уязвимостей в информационной системе, поскольку высококвалифицированные, опытные сотрудники реже ошибаются. Также необходимо покупать качественное современное оборудование, чтобы снизить вероятность поломки за определенный временной период. Наличие сотрудников, которые будут учить клиентов пользоваться оборудованием, минимизирует риск возникновения ошибок при работе с ним.

Чтобы не столкнуться с неблагоприятными последствиями незаконной или нежелательной для клиента деятельности банка, клиенту следует пользоваться услугами крупных банков. Для этого нужно ознакомиться с такой информацией, как: рейтинг ЦБ надежных банков, оценки рейтинговых агенств банка, отзывы клиентов, величина собственного капитала банка, количество клиентов.

Мерами для снижения риска мошеннических операций со стороны банка являются:

– Разработка и соблюдение стратегии информационной безопасности;

– Непрерывное совершенствование существующих систем безопасности и управления рисками;

– Следование рекомендациям международных платежных систем в области риск-менеджмента;

– Информирование клиентов о схемах мошенничества.

– Мерами для снижения риска мошеннических операций со стороны клиента являются:

– Следование всем рекомендациям банка при пользовании банковскими услугами;

– Не разглашение конфиденциальной информации о банковской карте;

– Обеспечение условий хранения банковской карты, которые исключают возможность ее потери или попадания в руки посторонних;

– Визуальный осмотр банковского оборудования на предмет наличия посторонних устройств.

Развитие информационных технологий привело к созданию дистанционного банковского обслуживания. Банковские карты прочно вошли в нашу жизнь, но это породило множество рисков и проблем, связанных с их использованием. Во избежание возникновения вышеперечисленных рисков необходимо предпринимать меры по их минимизации. При этом меры необходимо предпринимать и банкам, и их клиентам.

ЛИТЕРАТУРА

1. Тарасенко О.А., Хоменко Е.Г. Банковское право. Теория и практика применения банковского законодательства: учебник. – М.: Проспект, 2016 – 368 с.

2. Положение ЦБР от 24 декабря 2004 г. № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» (с изменениями и дополнениями).

3. Количество платежных карт, эмитированных кредитными организациями, по типам карт // Официальный сайт Банка России [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm (дат

4. Давыдова, Л. В. Тенденции развития национальной денежной системы: теория и практика [Текст] : монография / Л. В. Давыдова, Н. В. Тулайков ; М-во образования и науки Российской Федерации, Гос. образовательное учреждение высш. проф. образования «Орловская региональная акад. гос. службы». – Орел : Изд-во ОРАГС, 2010. – 194 с.;

5. Риски по банковским и платежным картам в России и их минимизация [Электронный ресурс]

6. Сведения о количестве действующих кредитных организаций и их филиалов в территориальном разрезе // Официальный сайт Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/statistics/bank_system_new/cr_inst_branch_01021

УДК 004.056

БЕЗОПАСНЫЙ ОБМЕН ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Е.В. Ильинская, К.А. Павленко
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В статье рассматриваются меры сохранению безопасности электронного документооборота в области экономической безопасности предприятия. А именно использование электронной подписи, сжатия и шифрования документа тремя методами: симметричное, асимметричное и комбинированное шифрование.

Ключевые слова: *экономическая безопасность предприятия; безопасный документооборот; шифрование документа; электронная подпись, сжатие электронного документа.*

SECURE EXCHANGE OF ELECTRONIC DOCUMENTS AS A FACTOR OF ECONOMIC SECURITY OF ENTERPRISE

E.V. Ilinskaja, K.A. Pavlenko
Belgorod, Russia Belgorod state national research University

The article deals with measures to preserve the security of electronic document management in the field of economic security of the enterprise. Namely, the use of electronic signature, compression and encryption of the document by three methods: symmetric, asymmetric and combined encryption.

Key words: *economic security of the enterprise; secure document flow; document encryption; electronic signature, electronic document compression.*

На сегодняшний день нет официальных документов Российской Федерации, регламентирующих понятие экономической безопасности предприятия или организации. В Законе РФ «О безопасности» даны определения безопасности и угрозы безопасности. Безопасность – состояние защищенности жизненно важных интересов личности, общества, и государства от внутренних и внешних угроз. Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [3]. Оба эти определения так же можно отнести к деятельности предприятия.