БЕЗОПАСНОСТЬ СИСТЕМЫ «КЛИЕНТ БАНК» ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

Е.Ю. Залецкая
(г. Томск, Томский политехнический университет)
E-mail: ZaletskayaLiza@mail.ru

THE SAFETY OF THE REMOTE BANKING FOR INDIVIDUALS

E.U. Zaletskaya
(Tomsk, Tomsk Polytechnik University)

It's difficult to imagine our lives without computer technologies. They are particularly useful in the banking sector. There are many types of remote control systems – remote banking is one of them. This article deals with weak, unprotected sides of this system, with methods of fraud. Several recommendations for safety usage of remote banking are also given.

Remote Banking, security, fraud, database,

Безопасность системы «клиент-банк» для физических лиц. Большое влияние на современный мир оказывают компьютерные коммуникации. Они заменяют нам привычный бумажный носитель, тем самым облегчая и сокращая работу. Но, к сожалению, какие бы инновации не были изобретены, люди всегда находили варианты мошенничества. Сейчас этот обман заключается в киберпреступлениях. По данным МВД в 2014 году было зарегистрировано 11 000 компьютерных преступлений. Опрошенные «Ведомостями» эксперты рассказывают, что вести учёт подобных преступлений непросто, но общее их количество во много раз превышает данные из статистики МВД. Так, в 2013 г. киберпреступники заработали в России и СНГ $2,5 млрд. [1]

Целью данной статьи является рассмотрение проблем безопасности систем «клиент-банк», способы мошенничества, а так же рекомендации по защите информации в системе.

Самой популярной целью мошенничества в киберпространстве являются системы дистанционного банковского обслуживания (ДБО). Одной из этих целей является система «банк-клиент». Данная система представляет собой программный комплекс, позволяющий клиенту совершать операции по счёту, обмениваться информацией и документами с банками, физически не посещая его. Достаточно лишь установить данное программное обеспечение на электронный носитель и все операции можно производить с помощью телефона или компьютера.

Система «банк-клиент» имеет свои технологические особенности, среди них можно отметить поддержку работы многофилиальных банков, развитую систему администрирования прав работников банка и клиента, а также отсутствие записей в системном реестре при инсталляции клиентской подсистемы. Существует множество видов данной системы, каждый банк разрабатывает свою, уникальную.

Проникновение на компьютер клиента банка вируса, в целях которого хищение ключа ЭПЦ и перехват логина и пароля учетной записи. Как правило, применяется универсальное вредоносное программное обеспечение. [2] Существует множество вариантов их проникновения, самые распространённые из них приведены в табл. 1 «векторы атаки и способы защиты клиент банка»

Таблица 1

Популярные уязвимости в системе «клиент-банк»

№	Уязвимость	Содержание
1	Рассылка по электронной почте, где указывается ссылка на файл, который предлагается скачать или на PDF-документ.	Подобные уязвимости могут возникать при покупке банком уже готового ПО.
2	Cross-Site Scripting (XSS)	XSS – самый популярный класс уязвимостей. Он позволяет злоумышленнику влиять на содержание web-страницы тем самым использовать ресурс банка для атаки на клиента.

Окончание табл. 1

№	Уязвимость	Содержание
3	SQL-инъекции	Возможность SQL-инъекции позволяет мошенникам использовать базу данных системы «клиент-банк», что может привести к утечке или изменению базы клиентов, их счетов, номеров пластиковых карт и т. п.
4	Ошибки бизнес-логики системы	Приводят к нарушению её функционирования, а иногда и к прямым денежным потерям.

Возвращаясь к самому распространённому способу нарушителя (хищение логина и пароля) хотелось бы добавить, что такие способы защиты информации, как одноразовые пароли на каждую операцию или различные дополнительные устройства – Universal Serial Bus USB-токены, криптокалькуляторы широкого распространения не получили. В табл. 2 представлены системы защиты ДБО в крупнейших российских банках для физических лиц [3].

Таблица 2

Системы защиты ДБО в крупнейших российских банках для физических лиц

№	Название банка	Уникальный номер клиента	Виртуальная клавиатура	Одноразовые пароли для каждой операции		Используется ли USB-токен
1	Сбербанк	есть	–	есть	На распечатке из банкомата или по SMS (можно отключить)	–
2	ВТБ 24	есть	–	есть	На скретч-карте	–
3	Альфа банк	есть	есть	есть	Высылается на мобильный телефон по SMS	–
4	Газпромбанк	есть	–	есть	Распечатка из банкомата, SMS или специальное приложение на телефоне	Есть
5	Россельхозбанк	есть	–	есть	На скретч-карте	–

Приведённые в таблице способы защиты системы банк-клиент сокращает возможности хищения денежных средств со счёта клиента. Хочется акцентировать внимание на том, что данные способы не полостью исключают возможность мошенничества, а лишь сокращают её. Безопасность информации заключается не только в защите банком обслуживания, но и в самих клиентах. У каждого банка существует инструкция о мерах защиты информации при использовании системы «Банк-клиент». Самые распространённые советы представлены ниже:

1) смена пароля, данного в банке на свой собственный при первом входе в систему;
2) регулярная смена пароля не реже 1 раза в 50 дней (банки рекомендуют использовать сложные пароли, не использовать в качестве него собственное имя или фамилию);
3) не разглашения собственного пароля от системы «клиент-банк»;
4) ключевая информация должна размещаться на сменном накопителе (дискета, USB-накопитель или USB-токен);
5) сменный носитель с ключевой информацией должен использоваться только владельцем сертификата ключевой информации;
6) с целью исходящего и входящего подозрительного трафика компьютер с установленной системой «клиент-банк» должен быть защищён от внешнего доступа программным или аппаратным средством межсетевого экранирования;
7) в случае утери телефона, привязанного к системе, немедля сообщить в банк.

Итак, мы рассмотрели, что такое система «клиент-банк», какие уязвимости могут быть у неё, как действуют мошенники для хищения информации и денежных средств клиента, а также были разработаны советы для безопасной работы с данной системой.

Список литературы

1. Е. Разумный / газета «Ведомости». Киберпреступники в списках не значатся. Электронный ресурс: http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya // Дата обращения: 07.04.2015 г.
2. Синцов А. / Электронный журнал консалтинговой компании в области информационной безопасности Digital Security. Безопасность банк-клиентов. Электронный ресурс: http://dsec.ru/ipm-research-center/article/bezopasnost_bank_klientov// Дата обращения: 07.04.2015 г.
3. Проект по защите информации от утечек. Риски дистанционного обслуживания. Системы защиты ДБО в крупнейших российских банках для физических лиц. Электронный ресурс: http://www.zecurion.ru/press/smi/CNEWS_60_DBO_Zecurion.pdf // Дата обращения: 30.04.2015 г.

ФОРМИРОВАНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ РФ ПО ПЛАСТИКОВЫМ КАРТАМ

И.О. Казина
(Томский политехнический университет, г. Томск)
E-mail: ina.kazina@mail.ru

FORMING A NATIONAL SYSTEM OF THE RUSSIAN FEDERATION ON PLASTIC CARDS

I.O. Kazina
(Tomsk Polytechnic University, Tomsk)

Abstract: The article is devoted to the formation of national system of bank cards in Russian Federation, it's structure and qualities.

В условиях устойчивого экономического развития России, обусловленного высоким уровнем цен на энергоресурсы на международных рынках, особую значимость приобретает эффективная национальная платежная система, которая необходима для обеспечения бесперебойности расчетов между субъектами экономики России.

Цель статьи: Рассмотреть формирование национальной системы РФ по банковским картам.

Для реализации указанной цели были поставлены и решены следующие задачи:

- Изучены структура и основные элементы национальной платежной системы;
- Описан процесс проведения платежей до перехода на НСПК;
- Описаны этапы формирования платежной системы России и их характеристика;
- Рассмотрен процесс проведения платежей после перехода РФ на НСПК;

Национальная платежная система (НПС) является одним из основных компонентов денежно-кредитной и финансовой системы страны и, следовательно, важным фактором ее экономического развития. Национальная платежная система включает в себя все формы институционального и инфраструктурного взаимодействия в финансовой системе при переводе денежных средств от плательщика к получателю (см. рис. 1.)

Для принятия мер по развитию НПС необходимо охарактеризовать ее устройство. Элементы национальной платежной системы, которые в их взаимодействии и определяют направления ее развития (см. рис. 1):

1. Платежные инструменты, используемые для инициирования и направления перевода денежных средств со счетов плательщиков на счета получателей в финансовых учреждениях.
2. Платежные инфраструктуры для инициирования и клиринга платежных инструментов, обработки и передачи платежной информации, а также перевода денежных средств между учреждениями-плательщиками и получателями.