

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТ-БАНКИНГА

К.И. Логутенко

(г. Томск, Томский политехнический университет)

INFORMATION SECURITY WHEN USING INTERNET BANKING

K.I. Logutenko

(Tomsk, National Research Tomsk Polytechnic University)

Безопасное использование услуг интернет-банкинга является ключевым вопросом для клиентов, предпочитающих выполнение операций с финансами в Интернете. Большинство потребителей таких услуг ощущают страх быть обманутыми, что провоцируется периодическими сообщениями СМИ о всевозможных атаках хакеров, однако немалая часть вины в большинстве случаев лежит на самих клиентах. Банки отчётливо понимают важность обеспечения безопасности предоставляемых услуг, и то какой урон могут нанести сообщения о компрометации работы системы интернет-банкинга. В связи с этим каждый банк прикладывает всевозможные усилия, для того чтобы попытаться предотвратить попытки взлома. В наши дни тема информационной безопасности при использовании услуг интернет-банкинга является достаточно актуальной, так как большинство операций с финансами осуществляется в Интернете.

Цель данной статьи – рассмотрение основных методов обеспечения информационной безопасности при использовании услуг интернет-банкинга, а также выявление самых уязвимых операций и разработка рекомендаций по их защите.

Сегодня практически всеми банками, предоставляющими услуги интернет-банкинга, используются SSL-шифрование данных, в систему банка от компьютера пользователя и обратно. Клиенту выдаются цифровые сертификаты и электронная цифровая подпись (ЭЦП), которая позволяет идентифицировать пользователя. Для полноценной защиты своих счетов этого не достаточно.

Более инновационные банки предлагают к использованию токены – usb-ключи, внешне похожие на флешку и позволяющие безопасно хранить: цифровые сертификаты, ключи ЭЦП и другую авторизационную информацию. Совсем недавно появились ключи, с помощью которых можно формировать ЭЦП аппаратно, т. е. внутри самого токена. Например, устройство eToken PRO (Java), на борту которого пользователи сами формируют ЭЦП согласно ГОСТ Р 34.10–2001, за счёт этого сертификат ЭЦП никогда не покидает токен, и следовательно перехват информации невозможен. Ещё один из методов обеспечения безопасности – пин-код, осуществляющий неприступность лицевого счёта, в случае потери или хищения токена. В данной ситуации токен выступает в роли «замка», который запирает «дверь» к счёту клиента.

Самыми незащищенными от несанкционированных действий мошенников являются автоматические групповые операции, счета и сумма на которых, как правило, не подлежат достаточному контролю. Операции такого рода и возможные меры по предотвращению рассмотрены в табл. 1.

Помимо перечисленных выше незащищенных операций интернет-банкинг не застрахован от других возможных рисков. Например, возникновение технического сбоя во время проведения операции, но подобный риск не в силах нанести большой вред владельцу счёта. Система интернет-банкинга, как и другие системы обработки данных, устроена таким образом, что при возникновении программного или технического сбоя в процессе транзакции документы не будут приняты системой банка. Если неверная операция всё-таки была проведена, необходимо немедленно обратиться в банк для того чтобы исправить ошибку, и банк возвратит денежные средства на счет клиента в кратчайшие сроки.

Главная задача банка – демонстрация надежности своей системы безопасности интернет-банкинга. Большим плюсом является наличие стандартов в области информационной безопасности, например PCI DSS, Стандарт Банка России и другие. После прохождения аудита на соответствие требованиям этим стандартам, банк доказывает свою способность защищать данные своих клиентов. К несчастью, на сегодня не каждое кредитное учреждение может заявить о своём полном соответствии стандартам, касающимся информационной безопасности.

Таблица 1.

Операции, подверженные большому риску и меры предосторожности

№	Наименование операции/источника опасности	Меры предосторожности
1	Изменение внешнего получателя платежа	Ввод запрета на редактирование информации после прохождения стадий контроля и до электронной подписи отправляемого рейса
2	Начисление процентов счета до востребования и расчётные счета	Создание в рамках службы безопасности специализированной службы, для контроля автоматических операций по закрытым для остальных сотрудников методикам
3	Хищение денежных средств через систему клиент-банк	Ограничение для каждого клиента максимального ежедневного объема платежей, совершаемых по системе клиент-банк и регламентация обязательного ежедневного контроля выписки клиентом даже при отсутствии платежей
4	Разрушение системы автоматизации или ее отдельного модуля	Регулярное создание резервных копий, введение запрета на доступ сотрудника в информационную систему после уведомления его об увольнении

Чтобы обеспечить конфиденциальность личных данных и сохранность денег, необходимо придерживаться следующих правил безопасности:

- не сообщать никому свой пароль и пин-код (даже сотрудникам банка, т. к. они ни при каких обстоятельствах не имеют право запрашивать пароли пользователей);
- пользоваться одним компьютером (не допускать смены паролей и проведение платежей с малознакомых компьютеров, к которым имеет доступ множество пользователей);
- при работе на чужом компьютере, ни в коем случае не сохранять ключ электронной цифровой подписи;
- если существуют подозрения о том, что кто-то подсмотрел пароль, обратиться в банк и заблокировать доступ в систему;
- в случае хищения личных данных или денежных средств со счетов проинформировать банк о случившемся и подать заявление.

Придерживаясь данных рекомендаций можно избежать вероятности хищения личной информации и средств клиента, пользующегося услугами интернет-банкинга.

Можно сделать вывод о том, что обеспечение достоверности и конфиденциальности информации, передаваемой между банком и клиентом – один из самых важных аспектов дистанционного банковского обслуживания. Также не стоит забывать, что безопасное использование услуг интернет-банкинга по большей части зависит от самих клиентов банка. И для предотвращения негативных инцидентов необходимо развивать культуру безопасного пользования дистанционными услугами банка.

Список литературы

1. Банковский менеджмент: учебник / под ред. Е.Ф. Жукова. – 4-е изд., перераб. и доп. – Москва: ЮНИТИ, 2014. – 319 с.: ил. – Библиогр.: с. 313.
2. Банки и банковское дело: учебное пособие для бакалавров / под ред. В.А. Боровковой. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2014. – 623 с.: ил. – Бакалавр. Базовый курс. – Библиогр.: С. 622–623. – Глоссарий: С. 590–621.
3. Тепман Л.Н. Управление рисками в условиях финансового кризиса: учебное пособие для вузов / Л.Н. Тепман, Н.Д. Эриашвили. – Москва: ЮНИТИ-ДАНА, 2011. – 295 с.: ил. – Библиогр.: С. 291–292.
4. Ермаков С.Л. Основы организации деятельности коммерческого банка: учебник для вузов / С.Л. Ермаков, Ю.Н. Юденков; Академия народного хозяйства при Правительстве Российской Федерации (АНХ), Факультет финансов и банковского дела. – Москва: КноРус, 2011. – 645 с.: ил. – Библиогр.: С. 639–645.