Секция «Юриспруденция»

Обеспечение информационной безопасности в системе интернет-банкинга.

Дементьева Юлия Павловна
Аспирант
Саратовская государственная юридическая академия, , Саратов, Россия
E-mail: dementeva-yuliya@yandex.ru

На протяжении последних 15 лет системы дистанционного банковского обслуживания (ДБО) стали широко применяться в российских кредитных организациях.

Наиболее востребованным видом ДБО у клиентов является интернет-банкинг, который позволяет управлять своими банковскими счетами и картами через сеть Интернет в онлайн-режиме. Помимо уже перечисленных выше достоинств систем ДБО, к достоинствам интернет-банкинга можно добавить то, что работа с этой системой не имеет привязки к месту - достаточно иметь доступ к сети Интернет и веб-браузер [1].

Многие потенциальные пользователи банковских интернет-услуг сомневаются в безопасности электронных расчетов. Начиная с 2008 г. количество злоупотреблений и мошенничества в сфере ДБО начало неуклонно возрастать, и стало понятно, что в обеспечении безопасности электронных платежей необходимо что-то менять. Как утверждают эксперты Академии биржевой торговли Masterforex-V, главным минусом использования Интернет-банкинга является риск мошеннического взлома и, как следствие, несанкционированный доступ к денежным средствам, находящимся на счетах [4].

Выделяют три основных типа угроз:

- фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков (Ситибанк, Альфа-банк), сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте, Одноклассники.ru) [3];

- кража логина, пароля, закрытых ключей - на компьютере клиента внедряются вредоносные программы, так называемые "черви"и "трояны которые воруют (переписывают, копируют) идентификационные данные клиента;

- выполнение мошеннических операций непосредственно с рабочего компьютера клиента – в память компьютера загружается вирус, который подключает его к серверу, управляемому хакером. После этого с сервера можно отдавать команды по выполнению определенных действий на компьютере, в том числе и операций в системе интернет-банкинга [2].

В этой связи перед Интернет-банкингом стоит целый ряд проблем и задач, требующих решения:

· Кредитной организации необходимо разработать план оперативных действий при возникновении «конфликтных» ситуаций (сбор доказательной базы, переход на резервные каналы). Это необходимо для того, чтобы минимизировать риски нарушения информационной безопасности в ДБО, вернуть клиентам уверенность, а также стабилизировать положение банка в таких условиях.

· Проводить работу по информированию клиентов и персонала о важности мероприятий информационной безопасности. Ведь зачастую пренебрежение даже самых про-

стых правил соблюдения безопасности (защита от вредоносных программ, хранение ключей ЭЦП в незащищенном месте, ведет к негативным последствиям, а именно – потерей денежных средств клиентом.

Для обеспечения наивысшего уровня безопасности электронных операций, швейцарские ученые решили эту проблему иным образом, а именно, представили новейшую технологию безусловной аутентификации доступа и подтверждения транзакций, получившей название биометрическая идентификационная AGSES-карта. Это персональное мобильное устройство размером с банковскую карточку оснащено сканером отпечатка пальца и хранит идентификатор личности владельца в виде биометрических моделей. Карта имеет уникальный номер и предназначена для подтверждения доступа и электронных операций путем сверки отпечатков пальцев владельца, при этом в небезопасную компьютерную среду не попадают идентификационные данные пользователя. AGSES-карта активно используется в европейских странах, действуют программы налогового, страхового, социального, банковского обслуживания, запланировано применение в качестве платежного инструмента, а также инструмента физического доступа. Ряд российских банков приступил к интеграции AGSES-карты в качестве устройства аутентификации клиентов.

Технический прогресс не стоит на месте, и способы защиты, которые еще вчера давали 100-процентную гарантию от взлома интернет-банкинга, сегодня уже не имеют такой надежности. Будущее информационной безопасности в системах класса "интернет-банк"представляется как некая "гонка вооружений". На каждый ход мошенников будут следовать ответные действия банков и разработчиков систем ДБО. Конечно же, клиенты должны понять, что больше закрывать глаза на проблемы информационной безопасности вряд ли получится. Только в случае неукоснительного соблюдения необходимых мер безопасности можно свести риск потери своих же денег к минимуму [2].

Литература

1. Письмо ЦБ РФ от 31.03.2008 N 36-Т "О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга". "Вестник Банка России N 16, 09.04.2008.

2. Илюхин О. Интернет-банкинг: безопасность превыше всего // Справочно-правовая система «Консультант Плюс». 2010. № 5.

3. Материал из Википедии — свободной энциклопедии: http://ru.wikipedia.org/wiki

4. Интернет-банкинг в России: экономия времени и денег: http://free-forex-ua.blogspot.ru/2011

Слова благодарности

С Уважением, Юлия Дементьева.