УДК 004

Минимизация рисков участников дистанционного банковского обслуживания

В. А. Конявский, д-р техн. наук
Национальный исследовательский университет Высшая школа экономики,
Московский физико-технический институт (государственный университет),
Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Рассмотрена наиболее злободневная проблема информационной безопасности — риски, связанные с дистанционным банковским обслуживанием (ДБО), и их минимизация. Предложен подход, основанный на введении в процесс взаимодействия Банка и Клиента дополнительного участника. Определены основные виды дополнительных участников.

Ключевые слова: дистанционное банковское обслуживание, доверенная среда, недоверенная среда, дополнительный участник.

В ДБО участвуют две стороны — Банк и Клиент.

Банк

Функция обеспечения защиты информации, идентификации и аутентификации клиентов не свойственна банку. Но банк вынужден это делать в силу особенностей законодательства. Конечно, он делает это плохо. Более того, плохое исполнение этих функций выгодно банку. В этом случае, имитируя защиту, банк всегда может обвинить клиента в недостаточно полном следовании правилам ИБ. Именно поэтому, даже глубоко понимая основы ИБ, специалисты банка не предлагают клиенту действительно надежных механизмов защиты. Запутать клиента, не говоря ему неправды, — очень несложно. Хорошие СЗИ и СКЗИ дорогие и очень сложные. Клиент никогда не сможет правильно их настроить и все время эксплуатации поддерживать достаточный уровень безопасности. Значит, если ему предложат, купит что-то ненадежное, но дешевенькое — "Я сам обманываться рад". Конечно, забудет обновить антивирус или установит новое программное обеспечение, нарушающее изолированность среды, например, скачает новую игрушку — вот и "Сам виноват".

Ситуацию усугубил ФЗ 161 — риски банка сильно возросли. Банк спит и видит, кому бы передать несвойственные функции, конечно, вместе с рисками. Самостоятельно банк в общем случае не может корректно обеспечить защищенность клиента, и поэтому хотя и не занимается этим, зато повышает стоимость услуг.

Клиент

Клиент (хозяйствующий субъект) приходит в банк, потому что другого способа управлять своими деньгами у него нет. Он исходит из того, что банк его не обманет, и рекомендации банка по ИБ воспринимает как диктуемое ему условие, выполнение которого (или имитация выполнения) необходимо для получения услуги от банка. Но нельзя хорошо сделать то, что не умеешь. Естественно, рекомендации выполняются формально, тем более что они непонятны и невнятны. В своем большинстве непонятные требования выглядят убедительными для клиента (он же не профессионал по ИБ), и клиент уверен, что в случае утраты денег банк их ему вернет. При этом клиент хорошо понимает, что он не специалист по ИБ, наслышан об активности хакерских группировок, надеется, что конкретно его это не коснется, но хочет эти риски передать кому угодно. В цепочке взаимодействия Клиент-Банк нет третьего, поэтому клиент хочет риски передать банку, и даже не сделав это, верит, что так и есть.

При этом позиция клиента противоположна позиции банка – банк предлагает использовать ЭП в недоверенной среде для того, чтобы при необходимости списать все потери на клиента, клиент же считает ЭП достаточным механизмом защиты, не понимая, что должен обеспечить СФК. Противоречие между позициями клиента и банка в данной конструкции неразрешимо.

Конявский Валерий Аркадьевич, профессор, зав. кафедрой «Защита информации»
E-mail: 001@pvti.ru

Статья поступила в редакцию 14 июня 2014 г.

При наступлении нештатной ситуации в стресс попадают обе стороны информационного взаимодействия, так как клиент бесправен и никогда ни за что не сможет доказать, что деньги украли не у него, а у банка, а банк должен компенсировать утраченные деньги, конечно, за счет клиента, который рядом, а не за счет хакера, которого еще надо разыскать. В результате реализуются самые сильные репутационные риски для банка и финансовые риски для клиента.

Разрешение данного противоречия возможно путем введения в цепочку информационного взаимодействия дополнительных участников (ДУ). Конечно, такие изменения повлекут также изменения нормативной и нормативно-правовой базы, перераспределение рисков и ответственности.

В идеале:

У клиента

- рисков ИБ быть не должно вообще;
- финансовая нагрузка, связанная с ИБ, минимизируется.

У банка

- могут быть только внутренние риски ИБ, "косяки" остальных участников взаимодействия не касаются банка;
- финансовые риски, связанные с ДБО, компенсируются.

"Идеальные" требования могут быть реализованы за счет "идеальных" механизмов:

– у клиента — ненастраиваемые СЗИ и СКЗИ, требований по обеспечению доверенности среды функционирования клиенту не предъявляются, требования по безопасности отчуждаются от клиента к ДУ;

– исполнение процедур идентификации и аутентификации отчуждается от банка к ДУ;

– финансовые риски компенсируются ДУ.

Итак, появляются ДУ, которые принимают на себя риски клиента и банка в области ИБ, и компенсируют финансовые риски, т. е в общем случае нужен как минимум один технический оператор (ТО) и один финансовый оператор (ФО).

Все клиенты взаимодействуют с ТО, а он взаимодействует с Банком.

Далее важный момент. Неразумно принимать риски ИБ, не принимая ответственности за процессы взаимодействия (и, соответственно, управления этими процессами), т. е. ТО обеспечивает исполнение процессов взаимодействия и управление ими с учетом обеспечения достаточного уровня защищенности процессов. Стала понятна базовая функция ТО — это ЦОД. Конечно, ЦОД, предоставляющий услуги в защищенном виде.

В этом случае легко, так как риски сосредоточены в одной точке, определяется место и функция ФО — это страховая компания, взаимодействующая с ТО, т. е. ЦОДом.

В настоящее время имеется техническая реализация такого подхода. Особенностью является то, что описанная структура взаимодействия не полностью соответствует структуре, предусмотренной ФЗ-161. Требует изменения и вся структура договоров. Сейчас разработка проектов таких документов ведется в ВШЭ. Требуется вмешательство регулятора и в определение обязательного состава клиентского договора.

Наибольшие трудности, тем не менее, представляет собой организация страхования информационных рисков. На первом этапе развития страхование будет невозможно без перестрахования рисков. Для перестрахования необходимо, чтобы оценка рисков велась в терминах зарубежных страховых компаний. В этом случае сертификация и аттестация по российским правилам будет иметь важный, но лишь справочный характер. Такого опыта сегодня у нас нет. Создать систему, при которой учет требований зарубежных страховщиков не подменил бы оценки наших регуляторов, а дополнил бы их в требуемом разрезе, — важная задача, и за ее решение могла бы взяться наша Ассоциация защиты информации.

Remote banking participants risks minimization

V. A. Konyavsky
National Research University Higher School of Economics, Moscow Institute of Physics and Technology (State University), National Research Nuclear University “MEPhI”, Moscow, Russia

The article is devoted to the most vivid information security problem of the day — the remote banking risks and their reducing. The approach based on incorporation the additional participant into the process of the Bank and the Client cooperation.

Keywords: remote banking, trusted environment, untrusted environment, additional participant.

Received June 14, 2014