XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VIII: С.33-34, 2003.

УДК 388.2(075.8)

Н.С. Сабурина (4 курс, каф. СМ), В.И. Чуркин, к.т.н., доц.

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ INTERNET-BANKING В РОССИИ

Начиная с середины 1990-х годов, все большее число финансовых институтов для предоставления своих услуг используют возможности сети Интернет. Первыми, кто представил свои услуги в Интернете, были банки. В 1995 году западные банковские организации предоставили своим клиентам прямой доступ к своим счетам, позволяющий управлять ими из любой точки мира, где есть Интернет. Такой доступ к счету через Сеть получил название Internet banking. On-line banking – e-banking – Internet banking (IB) – предоставление банковских услуг через электронные каналы передачи информации, в том числе через Интернет. Сетевой банк (Net-only bank) – банк, осуществляющий свою деятельность исключительно через Интернет, не имеющий фактических представительств, за исключением юридического адреса. Самым первым виртуальным банком считается американский Security First Network Bank, открывшийся 18 октября 1995 года. В Европе первым виртуальным банком был Advance Bank, дочерняя структура Дрезденской банковской группы (Германия). Подразделение появилось в 1996 году.

Однако открытость Интернет оборачивается для банков проблемой обеспечения безопасности обмена информацией. Один из подходов к решению вопроса о безопасности в сети Интернет был предложен компанией Netscape Communicatios Corp. Ею был разработан протокол защищенного обмена информацией между клиентом и сервером – SSL (Secure Socket Layer), обеспечивающий защиту данных между сервисными протоколами (такими как HTTP, FTP и т.д.) и транспортными протоколами (TCP/IP).

Протокол SSL в настоящее время является наиболее распространенным для защиты данных в Интернет и предназначен для решения традиционных задач обеспечения защиты информационного воздействия. Протокол SSL включает два этапа взаимодействия сторон защищаемого соединения: установление SSL сессии и защита потока данных.

На первом этапе осуществляется аутентификация сервера и (опционально) клиента, стороны договариваются об используемых криптографических алгоритмах и формируют общий «секрет», на основе которых создаются общие сеансовые криптографические ключи для последующей защиты соединения. Этот этап называется также процедурой «рукопожатия».

На втором этапе конфиденциальность информации обеспечивается путем шифрования потока данных на сформированном общем ключе с использованием симметричных криптографических алгоритмов, а контроль целостности передаваемых блоков данных осуществляется за счет использования кодов аутентификации сообщений.

Для аутентификации и формировании общих секретных сеансовых ключей в SSL используются методы асимметричной (двухключевой) криптографии, предполагающей наличие у каждой аутентифицируемой стороны двух ключей – секретного и открытого для кодирования/декодирования информации. Секретный ключ доступен только самому владельцу и хранится в тайне, а открытый ключ может распространяться свободно в составе сертификата и должен быть известен той стороне, которая выполняет процедуру аутентификации. В качестве двухключевого алгоритма для аутентификации сторон и формирования совместных секретных сеансовых ключей протокол SSL чаще всего использует алгоритм RSA (RSA Data Security Inc.) Для распространения открытых ключей используется специальная форма-сертификат, которая состоит из следующих частей:

- имя центра сертификации, имя владельца сертификата;

- открытый ключ владельца сертификата;
- идентификатор и параметры алгоритма криптообработки;
- цифровую подпись центра сертификации, заверяющую все данные в составе сертификата, период действия сертификата.

Одной из причин, препятствующих созданию российскими разработчиками систем защищенного электронного документооборота на основе Web-приложений является наличие экспортных ограничений на средства криптографии: практически все существующие продукты, поддерживающие протокол SSL, реализованы в США и из-за экспортных ограничений доступны лишь в усеченном варианте. Они позволяют работать с криптографическими ключами только ограниченной длины (например, Netscape Navigator, Internet Explorer, в экспортном варианте своих продуктов реализуют алгоритмы шифрования с длиной ключа 40 бит и алгоритм RSA с параметром 512 бит), что, безусловно, недостаточно для организации надежного уровня защиты. Кроме того, эти ограничения не позволяют создавать национальные центры сертификации, а использование зарубежных центов юридически сложно. Решение проблемы было предложено известной компанией «Сигнал-КОМ», созданной в 1990 г., и реализовано в программном продукте «Inter-Pro», предназначенном для защиты Web-приложений на базе расширенного протокола SSL, обладающего следующими свойствами:

- используемые протоколом зарубежные криптографические алгоритмы свободны от экспортных ограничений на длину ключей;
- протокол дополнен отечественными криптографическими алгоритмами (ГОСТ 28147-89);
- в рамках SSL реализована возможность формирования и проверки в режиме on-line цифровой подписи пользователя под электронной HTML-формой, заполняемой им в процессе взаимодействия с Web-сервером.

В настоящее время некоторые российские банки стремятся идти в ногу со временем и предлагают своим клиентам воспользоваться новой системой "Интернет-Банк":

- Система "Интернет-банк" состоит из двух частей – клиентской и банковской.
- В "клиентской части" используются стандартная платформа Windows 95/98/NT и стандартные программы просмотра вебстраниц Интернета (рекомендуется Microsoft Internet Explorer 4.0 и выше).
- В "банковской части" системы используется интерактивный сайт банка.

Для совершения операций клиент посещает специально выделенный ВЕБ-сайт Банка и производит все операции со своим расчетным счетом в Банке.

Для подключения к системе "Интернет-банк" необходимо:

- иметь расчетный счет в банке, предоставляющем интернет- услуги;
- заключить договор на обслуживание счета посредством "Интернет-банка";
- получить дискету с комплектом установки системы криптозащиты, имя и пароль, сертификат открытого ключа Банка;
- иметь компьютер с выходом в Интернет.

Функции системы "Интернет-банк":

- отправка платежных поручений в Банк, получение информации об их исполнении;
- получение информации об остатках на лицевых счетах;
- получение в электронном виде выписок по лицевым счетам за требуемый период;
- перевод средств на любой счет в другом банке;
- осуществление коммунальных платежей, оплата счетов за связь и пр.;
- получение кредита.

По данным исследования на 1 января 2002 в российских банках установлено 323 Интернет-системы (с учетом систем, находящихся в опытной эксплуатации), причем это только те банки, которые имеют системы с полноценным применением Интернет-технологий. Реально же функционирующих полноценных систем Internet banking (IB) на рынке намного меньше.