

Руководство по установке
ПБЗИ «Агава-С 5.0»
и СКЗИ «Крипто-КОМ 3.2»
клиентом банка

Содержание

Механизмы защиты в системе «iBank 2»	2
Инструкция пользователю средств криптографической защиты информации.	2
Использование USB-токена «iBank 2 Key» в системе «iBank 2»	3
Установка криптобиблиотек для Windows	5
Установка криптобиблиотек для Unix	5

Механизмы защиты в системе «iBank 2»

Система «iBank 2» относится к классу систем защищенного электронного документооборота. Обмен электронными документами в модулях РС-Банкинг, Internet-Банкинг, Web-Банкинг и Mobile-Банкинг происходит между банком и клиентом.

Электронный документ, отправленный клиентом и полученный банком, является основанием для совершения банком финансовых операций.

Для обеспечения аутентичности (доказательство авторства) и целостности документа в Internet-Банкинге, РС-Банкинге и Mobile-Банкинге, а также в дополнительных сервисах системы «iBank 2» используется механизм электронной цифровой подписи (ЭЦП) под электронными документами.

Именно электронный документ с ЭЦП является основанием для совершения финансовых операций и доказательной базой при разрешении конфликтной ситуации.

Для криптографической защиты информации в систему «iBank 2» встроены и поставляются в составе системы взаимно совместимые сертифицированные ФСБ РФ многоплатформенные криптобиблиотеки:

- ПБЗИ «Агава-С 5.0» компании «Р-Альфа»;
- СКЗИ «Крипто-КОМ 3.2» компании «Сигнал-КОМ».

Сертификаты соответствия ФСБ РФ:

- рег. № СФ/114-1171 от 01.09.2008г. на Агава-С 5.0;
- рег. № СФ/124-1070 от 07.11.2007г. на Крипто-КОМ 3.2;
- рег. № СФ/114-1069 от 07.11.2007г. на Крипто-КОМ 3.2;
- рег. № СФ/114-1068 от 07.11.2007г. на Крипто-КОМ 3.2;
- рег. № СФ/114-1170 от 15.07.2008г. на Крипто-КОМ 3.2.

Криптобиблиотеки представлены в виде динамических библиотек (DLL для Win32, SO для UNIX) и механизм их использования встроен в клиентские Java-апплеты, в клиентские и серверные Java-приложения.

Криптобиблиотеки предназначены для обеспечения защиты конфиденциальной информации, которая не является государственной тайной, от угроз нарушения конфиденциальности и целостности при помощи использования криптографических процедур, встроенных в прикладные программы.

Инструкция пользователю средств криптографической защиты информации.

При работе со средствами криптографической защиты информации (СКЗИ) необходимо соблюдать следующие правила:

- Криптобиблиотеки не входят в состав дистрибутива клиентской части системы «iBank 2». Диск с криптобиблиотеками должен быть получен в службе безопасности банка под роспись в журнале учета СКЗИ.

- Рабочие места, на которые устанавливаются СКЗИ, должны быть проверены на отсутствие программных закладок (трояны, кейлогеры и т.д.) и аппаратных закладок (аппаратный кейлогер для клавиатуры и т.д.).
- На технических средствах, предназначенных для работы с СКЗИ, разрешено использовать только лицензионное программное обеспечение фирм-изготовителей.
- СКЗИ устанавливаются с диска, полученного в службе безопасности банка под роспись в журнале учета СКЗИ.
- На ЭВМ с СКЗИ не должны устанавливаться средства разработки и отладки ПО.
- Системный блок и разъемы ЭВМ с СКЗИ должны опечатываться сотрудником службы безопасности компании, при каждом включении ЭВМ должна проверяться их целостность.
- В случае обнаружения "посторонних" (незарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках все работы на данном рабочем месте должны быть прекращены.

Пользователю СКЗИ запрещается:

- запускать на исполнение программы, не разрешенные администратором безопасности;
- обрабатывать предоставленными СКЗИ информацию, содержащую государственную тайну;
- подключать к ЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- осуществлять несанкционированное вскрытие системных блоков ЭВМ;
- приносить и использовать в помещении, где установлены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер);
- производить несанкционированное копирование СКЗИ.

Использование USB-токена «iBank 2 Key» в системе «iBank 2»

Для безопасного хранения и использования ЭЦП клиентов при работе в системе «iBank 2» используется USB-токен «iBank 2 Key».

USB-токен «iBank 2 Key» — это аппаратное USB-устройство (см. [рис. 1](#)). Его основу составляет микроконтроллер, который выполняет криптографическое преобразование данных, и память, в которой хранятся данные пользователя (пароли, сертификаты, ключи шифрования и т. д.).



Рис. 1. USB-токен «iBank 2 Key»

В USB-токенах «iBank 2 Key» реализованы все российские криптоалгоритмы и имеется защищенная область памяти, позволяющая хранить до 63-х секретных ключей ЭЦП одного или нескольких клиентов.

В USB-токене «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей ЭЦП;
- формирование и проверка ЭЦП по ГОСТ Р34.10-2001 (эллиптические кривые);
- генерация ключей шифрования;
- шифрование и расшифрование в соответствии с ГОСТ 28147-89;
- формирование и проверка имитовставки (последовательности данных фиксированной длины, получаемой по определенному правилу из открытых данных и секретного ключа и добавляемой к данным для обеспечения имитозащиты) в соответствии с ГОСТ 28147-89;
- вычисление хеш-функции в соответствии с ГОСТ Р34.11-94.

Формирование ЭЦП клиента в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри токена: на вход токен принимает электронный документ, на выходе выдает ЭЦП под данным документом. При этом время формирования токеном ЭЦП приблизительно равно 0,5 сек.

Секретный ключ ЭЦП генерируется самим токеном, хранится в защищенной памяти токена и никогда, никем и ни при каких условиях не может быть считан из токена.

Для использования функций криптографической защиты в «iBank 2 Key» системы электронного банкинга «iBank 2» встроена поддержка криптобиблиотеки СКЗИ «Криптомодуль-С» компании «Терна СБ», сертифицированных ФСБ (сертификат соответствия рег. № СФ/114-1009 от 14 мая 2007 года, действителен до 9 марта 2010 года).

Установка криптобиблиотек для Windows

Криптобиблиотеки ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2» устанавливаются путем копирования файлов библиотек в каталог, доступный через переменную окружения PATH, например, C:\Windows или C:\Windows\System32.

- Для установки ПБЗИ «Агава-С 5.0» скопируйте файл `ibank2agava.dll`.
- Для установки СКЗИ «Крипто-КОМ 3.2» скопируйте файл `ibank2ccom.dll`.

Для получения файлов криптобиблиотек обратитесь в Ваш банк.

Установка криптобиблиотек для Unix

Криптобиблиотеки ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2» устанавливаются путем копирования файлов библиотек в каталог, определяемый следующим образом:

1. Войдите на стартовую страницу систему «iBank 2» и запустите любой из java-апплетов (например, «Internet-Банкинг для корпоративных клиентов»).
2. Откройте в браузере окно Java консоли и, находясь в нем, нажмите S.
3. В консоли появится список переменных. Путь к требуемому каталогу - любое значение переменной `java.library.path`.

Файлы библиотек, которые необходимо скопировать:

- Для установки ПБЗИ «Агава-С 5.0» файл `libibank2agava.so`.
- Для установки СКЗИ «Крипто-КОМ 3.2» файл `libibank2ccom.so`.

Информация о типе используемой криптографии отображается в Java-консоли при запуске Java-апплета.

Для получения файлов криптобиблиотек обратитесь в Ваш банк.