ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
КОММЕРЧЕСКИЙ ИНВЕСТИЦИОННЫЙ
БАНК ЕВРОАЛЬЯНС

Генеральная Лицензия Банка России № 1781 от 10.10.2006 г.

УСЛУГИ ЮРИДИЧЕСКИМ ЛИЦАМ

СИСТЕМА «Банк-Клиент».

Новое в использовании и хранении ключей ЭЦП

Банк «ЕВРОАЛЬЯНС» предлагает своим клиентам, использующим систему «Банк-Клиент», ознакомиться с техническими новшествами, которые призваны обеспечить защиту их денежных средств.

Данное информационное сообщение составлено в профилактических целях. Оно содержит информацию о том, как обезопасить денежные средства на счетах клиентов, использующих системы дистанционного банковского обслуживания (*далее – системы ДБО*).

Не секрет, что в настоящее время сеть Интернет не является безопасной средой. Вредоносные программы постоянно модифицируются. Безусловно, использование антивирусов, персональных межсетевых экранов и средств защиты от несанкционированного доступа, снижает возможность вредоносного вторжения. Однако эти механизмы не гарантируют стопроцентной защиты персонального компьютера и данных клиента.

Используя уязвимости в операционных системах, Web-браузерах и почтовых программах, злоумышленники заражают компьютеры клиентов вредоносными программами (троянами) и дистанционно похищают файлы с секретными ключами ЭЦП клиентов и пароли, вводимые с клавиатуры. Далее злоумышленники по системе дистанционного банковского обслуживания «Банк-Клиент» от имени корпоративного клиента подключаются к банку, отслеживают поступления средств и в нужный момент направляют в банк платежные поручения с корректными ЭЦП клиента. Большая часть платежей, направляемых злоумышленниками, не вызывает подозрений у банка. Такие документы имеют корректную ЭЦП, обычные реквизиты получателей и типовое назначение платежа для данного клиента. Исполнение банком таких платежей приводит к хищению денежных средств с расчетного счета корпоративного клиента.

КАК БОРОТЬСЯ

Есть только один действенный метод борьбы с вредоносными программами, похищающими секретные ключи ЭЦП клиентов – исключить все операции с секретными ключами на компьютере клиента. *Секретный ключ ЭЦП клиента не должен попадать в персональный компьютер.*

Вся работа с секретными ключами ЭЦП клиента, все криптографические процедуры *должны быть вынесены* с компьютера клиента *в отдельную компактную доверенную среду.*

Такой *доверенной средой* является ***персональный аппаратный криптопровайдер***, который обеспечивает невозможность считывания (неизвлекаемость) секретного ключа ЭЦП клиента.

Использование персональных аппаратных криптопровайдеров в системах ДБО *обеспечивает гарантированную защиту секретных ключей ЭЦП клиентов* от хищений вредоносными программами.

О ПЕРСОНАЛЬНЫХ АППАРАТНЫХ КРИПТОПРОВАЙДЕРАХ

Персональный аппаратный криптопровайдер представлен в двух формах – в виде ***смарт-карты*** и ***USB-токена***, и имеет следующие достоинства:

1) *защищенное хранение и неизвлекаемость секретного ключа ЭЦП клиента*. Ни разработчик, ни производитель, ни владелец, ни злоумышленник не могут никакими способами считать секретный ключ ЭЦП клиента из устройства. Секретный ключ ЭЦП генерируется только внутри персонального аппаратного криптопровайдера и не может быть импортирован в устройство.

2) *формирование ЭЦП клиента* по российскому криптографическому алгоритму ГОСТ Р34.10-2001 *непосредственно внутри самого устройства*. На вход персональному аппаратному криптопровайдеру передается электронный документ (например, платежное поручение), а на выходе устройства – ЭЦП под данным документом. При этом доступ ко всем криптографическим функциям устройства предоставляется *только после ввода корректного пароля*.

USB-ТОКЕН «IBank2 Key»

Персональный аппаратный криптопровайдер USB-токен «iBank 2 Key» (разработан компанией «БИФИТ») предназначен для защиты секретных ключей ЭЦП клиентов от хищений. Это устройство объединяет в компактном пластиковом корпусе *USB-картридер и карточный криптографический микроконтроллер ST19NR66* производства компании STMicroelectronics.


СЕРТИФИКАТ СООТВЕТСТВИЯ

В криптографическом микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» российского разработчика «Терна СИС». В составе карточной операционной системы содержится средство криптографической защиты информации «Криптомодуль-С» российского разработчика «Терна СБ», сертифицированное ФСБ РФ по классу КС2. Сертификат соответствия рег. № СФ/114-1009 от 14.05.2007г.

Главное достоинство USB-токена «iBank 2 Key» - защищенное хранение (неизвлекаемость) секретного ключа ЭЦП клиента и формирование ЭЦП клиента под электронным документом непосредственно внутри устройства по российскому криптографическому алгоритму ГОСТ Р34.10-2001. На вход USB-токена передается электронный документ, на выходе устройства – ЭЦП под документом.

Исполнение «А»

Исполнение «М»

При этом *секретный ключ ЭЦП генерируется самим USB-токеном при инициализации, хранится в защищенной памяти токена и никогда, никем и ни при каких условиях не может быть считан из токена*.

СМАРТ-КАРТА «IBank 2 Key»

Персональный аппаратный криптопровайдер смарт-карта «iBank 2 Key» представляет собой *карточный криптографический микроконтроллер ST19NR66* производства компании STMicroelectronics, *имплантированный на пластиковую карту* и полностью соответствующий спецификациям ISO 7816.

Как и в USB-токене «iBank 2 Key», в криптографическом микроконтроллере смарт-карты «прошита» карточная операционная система «Магистра» со встроенным СКЗИ «Криптомодупь-С», сертифицированным ФСБ РФ по классу КС2.

Функционально смарт-карта «iBank 2 Key» полностью аналогична USB-токену «iBank 2 Key» за исключением электрического интерфейса.

Для работы со смарт-картами «iBank 2 Key» клиенты системы ДБО «iBank 2» должны иметь CCID-совместимый картридер.

Главные достоинства персонального аппаратного криптопровайдера «iBank2 Key» в форме смарт-карты – это компактность, удобство использования и хранения.

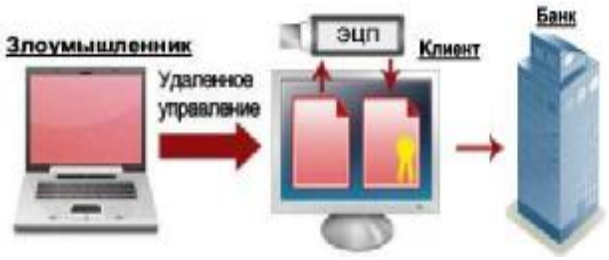
РАБОТА ПЕРСОНАЛЬНОГО АППАРТАНОГО КРИПТОПРОВАЙДЕРА «iBank 2 Key» в виде USB-токенов и смарт-карт обеспечена для всего спектра настольных платформ -Windows XP/2003/Vista/2008, Linux и Mac OS X.

Поддержка персонального аппаратного криптопровайдера «iBank 2 Key» встроена в клиентские модули Web-Банкинга, Internet-Банкинга, PC-Банкинга, Центра финансового контроля Онлайн и Офлайн, Корпоративного автоклиента.

Обеспечивается одновременная работа сразу с несколькими подключенными к компьютеру USB-токенами и смарт-картами (актуально при работе в ЦФК).

В одном персональном аппаратном криптопровайдере «iBank 2 Key» могут храниться до 64-х секретных ключей ЭЦП клиентов, поддерживается хранение и работа секретных ключей ЭЦП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы ДБО «iBank2».

ВАЖНО!



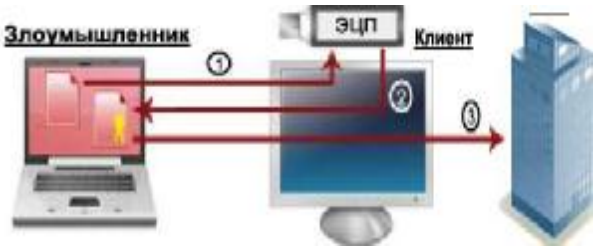
Нельзя оставлять USB-токен «iBank 2 Key» подключенным к компьютеру с доступом в Интернет *постоянно (круглосуточно) и бесконтрольно*, т.к. с помощью вредоносных программ злоумышленники могут удаленно подключиться к компьютеру клиента, запустить программу «Клиент-Банк» и, перехватив ЭЦП с постоянно подключенного USB-токена «iBank 2 Key», создать платежные поручения от имени клиента, которые затем отправляют в банк.

Для сведения:

В настоящее время в нескольких российских банках были зафиксированы попытки хищений в онлайне. Во всех выявленных случаях злоумышленники пользовались халатностью клиентов, оставляющих USB-токен «iBank 2 Key» постоянно (круглосуточно) и бесконтрольно подключенным к компьютеру с доступом в Интернет. С помощью вредоносных программ (троянов) со встроенным механизмом удаленного управления злоумышленники удаленно подключались к зараженному компьютеру корпоративного клиента, запускали программу Клиент-Банк. Далее с использованием ранее перехваченного долговременного пароля и постоянно подключенного USB-токена «iBank 2 Key» злоумышленники от имени клиента заходили в систему «Клиент-Банк», создавали платежные поручения, подписывали ЭЦП и отправляли в банк.

В ряде случаев корпоративным клиентам удавалось наблюдать процесс создания и подписи злоумышленниками платежных поручений у себя на мониторе. Одновременно были зафиксированы попытки хищений с использованием троянов со встроенным механизмом удаленного доступа к USB-портам компьютера клиента. При этом программа «Банк-Клиент» загружалась и исполнялась на компьютере злоумышленника, а для входа в систему «Банк-Клиент» и формирования ЭЦП клиента под платежными документами использовался удаленный доступ к USB-портам компьютера клиента с постоянно подключенным USB-токеном.

КАК БОРОТЬСЯ



Для борьбы с такого рода угрозами рекомендуется строго соблюдать порядок работы в системе «Банк-Клиент», в том числе недопустимо постоянно и бесконтрольно держать подключенным к компьютеру USB-токен или смарт-карту «iBank 2 Key»

Для преодоления механизма контроля доступа клиента с заданных IP-адресов злоумышленники осуществляют туннелирование трафика с компьютера злоумышленника до компьютера клиента и перенаправление трафика злоумышленника через компьютер клиента в банк.

Новые разновидности троянов не являются специфичными для системы «Банк-Клиент» - удаленный доступ к USB-портам или удаленное управление компьютером клиента упрощают злоумышленникам задачу хищений в онлайне при работе клиентов с любыми системами ДБО.

Важно отметить, что ни в одном из инцидентов секретный ключ ЭЦП клиента не был похищен из USB-токена «iBank 2 Key». Благодаря применению USB-токенов и смарт-карт «iBank 2 Key» возможности злоумышленников по хищению средств сильно ограничены.

Более подробные консультации по вопросам использования и хранения ключей ЭЦП можно получить по телефонам **(4932) 41-25-79, 41-15-69, 47-15-30**.

www.euroalliance.ru