

**Хищения по системам
дистанционного банковского
обслуживания ?**



**Внедряйте персональные
аппаратные криптопровайдеры**

О хищениях

В начале 2008 года в российских банках начался лавинообразный рост хищений денежных средств со счетов корпоративных клиентов с использованием систем дистанционного банковского обслуживания (далее ДБО).

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 ДБО от имени корпоративного клиента подключаются к банку, отслеживают поступления средств и в нужный момент направляют в банк платежные поручения с корректными ЭЦП клиента.

Успешно прошедшие проверку ЭЦП, но при этом подозрительные, абсолютно не свойственные данному клиенту платежные поручения пресекаются банковскими операционистами на этапе принятия решения об исполнении документов.

Большая же 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.

При этом вся ответственность за убытки безусловно и полностью возлагается на клиента как единственного владельца секретных ключей ЭЦП.

О причинах

Для обеспечения аутентичности (целостности и авторства) электронных финансовых документов во всех системах ДБО используется механизм ЭЦП на базе российского криптографического алгоритма ГОСТ Р34.10-2001. Длина секретного ключа ЭЦП - 256 бит. Это 10^{78} вариантов. Подобрать или угадать секретный ключ ЭЦП невозможно-атомов во Вселенной меньше.

В банке секретного ключа ЭЦП клиента нет. В банке есть только открытый ключ ЭЦП клиента, с помощью которого банковский сервер проверяет подпись клиента под электронными документами. Восстановить из открытого ключа ЭЦП секретный ключ ЭЦП технически невозможно.

Именно поэтому все действия злоумышленников направлены на хищение (копирование) секретного ключа ЭЦП у его единственного владельца - клиента.

Анализ выявленных вредоносных программ показывает, что злоумышленники эксплуатируют фундаментальную проблему - неспособность массового пользователя обеспечивать доверенную среду на своем компьютере.

Угрозе хищений секретных ключей ЭЦП клиентов подвержены все системы ДБО, в которых секретные ключи хранятся в копируемых файлах вне зависимости от типа носителя-дискета, жесткий диск, флешка, USB-токен или смарт-карта.

Как бороться

Сегодня уже нельзя считать компьютер клиента доверенной средой. Особенно компьютер, подключенный к Интернету.

Антивирусы, персональные межсетевые экраны и средства защиты от несанкционированного доступа безусловно должны использоваться и своевременно обновляться на компьютере клиента. Но все эти механизмы не гарантируют защиту персонального компьютера клиента от постоянно модифицируемых вредоносных программ.

Есть только один радикальный и 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 криптопро-вайдер, реализованный в виде смарт-карты или USB-токена и обеспечивающий **неизвлекаемость** (невозможность считывания) секретного ключа ЭЦП клиента.

О персональных аппаратных криптопровайдерах

Главное достоинство персонального аппаратного криптопровайдера -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 навязан или импортирован в устройство.

Еще одно важное достоинство персонального аппаратного криптопровайдера -это 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.

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

О USB-токене «iBank2 Key»

Для защиты секретных ключей ЭЦП клиентов от хищений компания «БИФИТ» предлагает банкам использовать в системах ДБО персональный аппаратный криптопровайдер USB-токен «iBank2 Key».

Устройство объединяет в компактном пластиковом корпусе USB-картридер и карточный криптографический микроконтроллер ST19NR66 производства компании STMicroelectronics.

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.



Исполнение «М»

Главное достоинство USB-токена «iBank 2 Key» - защищенное хранение (неизвлекаемость) секретного ключа ЭЦП клиента и формирование ЭЦП клиента под электронным документом по российскому криптографическому алгоритму ГОСТ Р 34.10-2001 непосредственно внутри устройства. На вход USB-токена передается электронный документ, на выходе устройства - ЭЦП под документом.

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

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».