

eToken на защите систем дистанционного банковского обслуживания

В рамках мероприятий по повышению уровня информационной безопасности финансовых операций, совершаемых в системе дистанционного банковского обслуживания, в соответствии с рекомендациями Центрального Банка Российской Федерации (письмо ЦБ РФ № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам по информационной безопасности при использовании систем интернет-банкинга») СДМ-БАНК принял решение о внедрении с 05.04.2010 года нового носителя ключей ЭЦП – сертифицированного электронного USB-ключа eToken PRO (сертификат ФСТЭК России №1883 от 11.08.2009 г.), позволяющего значительно снизить риск несанкционированного использования секретного ключа ЭЦП.

Дистанционное банковское обслуживание – это динамично развивающийся банковский сервис. Число пользователей услуг ДБО стремительно растет.

Как следствие – в последнее время на мировом и российском рынках таких услуг наблюдается рост мошенничеств, связанных с несанкционированным переводом денежных средств со счетов клиентов, пользующихся дистанционными банковскими услугами.

Анализ ситуации показывает, что в целях хищения денежных средств в основном используется атака, направленная на получение доступа к секретным данным пользователей (паролям и закрытым (секретным) ключам электронной цифровой подписи). Затем, с помощью систем «Интернет-Клиент» или «Банк-Клиент», злоумышленники совершают несанкционированные переводы от лица легальных пользователей систем на сторонние счета.

Основными причинами, по которым подобные действия злоумышленников становятся возможны и могут нанести значительный ущерб пользователям систем ДБО, являются:

- слабая антивирусная защита рабочего места пользователя, позволяющая специально разработанным программам-шпионам осуществить хищение конфиденциальных данных: паролей и секретных ключей ЭЦП;
- «фишинговые» атаки, основанные на методах социальной инженерии, итогом которых также является хищение конфиденциальных данных: паролей и секретных ключей ЭЦП;
- низкий уровень защиты доступа к компьютеру. Этот фактор также делает незащищенными конфиденциальные данные, и атака злоумышленника с целью хищения закрытых ключей ЭЦП увенчается успехом;
- хранение секретных ключей на незащищенных носителях, среди которых flash-накопители, дискеты, жесткие диски компьютеров, карты памяти. Незащищенные носители являются легкой мишенью для злоумышленников и позволяют легко скопировать секретные ключи пользователей систем ДБО.

Как мы видим, во всех случаях единственной целью мошенников является получение **секретных ключей электронных цифровых подписей**, которую злоумышленники с легкостью и достигают.

Как снизить риски мошенничества?

Очевидно, что для исключения случаев мошенничества при использовании удаленного доступа к счетам пользователей необходимо обеспечить надежное и безопасное хранение секретных ключей ЭЦП. Для этого необходимо обеспечить хранение секретных ключей ЭЦП только на специализированных защищенных носителях.

Единственным защищенным носителем на сегодняшний день является **USB-ключ eToken PRO**.

eToken PRO разработан специально для безопасного хранения секретного ключа ЭЦП, обеспечивая высокий уровень защиты, подтвержденный много численными международными сертификатами безопасности, в частности: ITSEC Level E4, FIPS 140-1-Level 2,3. Секретные ключи ЭЦП, находящиеся в закрытой памяти устройства, не могут быть из нее извлечены.

Что дает пользователю eToken PRO?

- ◆ безопасность применения – воспользоваться им может только его владелец, знающий PIN-код устройства;
- ◆ надежность хранения информации – качественная микросхема и прочный герметичный корпус существенно уменьшают риск выхода устройства из строя;
- ◆ мобильность – минимальные требования к установке ПО на новом рабочем месте;
- ◆ удобство работы – ключ выполнен в виде брелока со световой индикацией, напрямую подключается к компьютеру через USB-порт и не требует дополнительных устройств (проводов, блоков питания и т.п.).

На сегодняшний день на рынке дистанционного обслуживания не зарегистрировано ни одного случая несанкционированного доступа к системам ДБО, использующим eToken.

eToken – ключ к безопасному использованию дистанционных банковских услуг!

Уделяя особое внимание информационной безопасности финансовых операций, совершаемых в системе дистанционного банковского обслуживания, КБ «СДМ-БАНК» (ОАО) настоятельно рекомендует Вам перейти на использование eToken PRO.

По всем вопросам, связанным с переходом на использование eToken PRO, Вы можете проконсультироваться по телефонам (495) – 956 – 79 – 01.