Защищенный доступ
на примере ДБО

Андрей ШПАКОВ,
ведущий инженер-консультант,
ЗАО «С-Терра СиЭсПи»

Сегодня большинство людей, не отторгающих новые технологии, ощутили все преимущества систем дистанционного банковского обслуживания (ДБО). Помните ли вы, как приходилось выстаивать очереди для оплаты услуг ЖКХ или осуществления денежного перевода, а пенсионеры вынуждены были часами сидеть в отделениях банка за пенсией? Сейчас же дети и внуки могут избавить их от этой необходимости.

Польза ДБО для юридических лиц еще более очевидна. Рабочее время бухгалтерии оптимизируется за счет отсутствия бумажного документооборота. Нет необходимости в хранении десятков, а иногда и сотен килограммов бумажных документов.

Основным двигателем ДБО выступают сами банки, получая экономическую выгоду за счет снижения стоимости обслуживания клиента. Причем срок окупаемости системы заметно сокращается с ростом количества клиентов, для привлечения которых банк создает различные каналы ДБО, такие как: «толстый» или «тонкий» клиенты, мобильный клиент и др.

Подобное разнообразие решений порождает большое количество потенциальных уязвимостей. Более того, на текущий момент, до ввода «Национальной платежной системы» (№ ФЗ-161), если система «Клиент-Банк» была взломана на стороне пользователя – банк не несет ответственности.

Атака на базы данных банка является сложной задачей, поэтому злоумышленники зачастую пользуются отсутствием бдительности клиента. Наибольшее распространение получили специализированные программы, которые можно «подхватить» в Интернете. Например, программы типа keylogger перехватывают комбинацию логин-пароль и отсылают ее злоумышленнику, приложения-аналоги Team Viewer или Radmin передают изображение с монитора, троян может подменить реквизиты отправленного поручения, предложив пользователю подписать документ с неверными сведениями. Уже существует вредоносное ПО, способное заражать BIOS, CMOS и компрометировать систему на уровне «железа», не оставляя каких-либо следов на жестком диске компьютера.

Универсальным решением в данном случае является создание изолированной среды функционирования операционной системы клиента, т. е. среды, полностью защищенной от любого неразрешенного вмешательства.

С этой функцией идеально справляется продукт СПДС «ПОСТ» компании «С-Терра СиЭсПи», в основе которого лежит концепция построения среды доверенного сеанса. Выполнено устройство в виде USB-носителя.

Автоматизированное рабочее место (АРМ) загружается с СПДС «ПОСТ» только в случае успешного ввода PIN-кода, эталон которого хранится на защищенной и сертифицированной смарт-карте ведущих российских производителей. По результатам проверки PIN-кода определяются права пользователя, предоставляется доступ к предусмотренным правами разделам USB-носителя, выполняется проверка целостности операционной системы и загрузка ее с СПДС «ПОСТ». По окончании загрузки и выбора профиля сетевых настроек устанавливается IPSec-туннель до сервера банка. При этом, как правило, все остальные соединения запрещаются (в соответствии с политикой администратора).

Целевое программное обеспечение (например, «Клиент-Банк») запускается уже в изолированной среде. При этом ключи для электронной подписи могут храниться как на смарт-карте, встроенной в СПДС «ПОСТ», так и на внешнем токене, а также в реестре терминальной машины, доступ к которой защищен VPN.

Наличие терминальной и браузерной версии продукта позволяет применять различные варианты исполнений системы «Клиент-Банк».

В итоге в созданной изолированной среде функционирования АРМ невозможно запустить стороннее ПО, подключить запрещенные политикой администратора внешние носители, нельзя подключиться к ней по сети. Для повышения степени защиты в конструкции USB-носителя предусмотрены меры защиты против физического воздействия на элементы устройства.

Таким образом, устройство СПДС «ПОСТ» компании «С-Терра СиЭсПи» обеспечивает двухфакторную аутентификацию, изолированную среду функционирования, защищенный канал между клиентом и сервером банка, иными словами, полностью защищает АРМ пользователя. Продукт сертифицирован ФСБ России как СКЗИ по классу КС2, полностью удовлетворяет требованиям приложения ЦБ РФ и может позволить банкам ранжировать спектр предоставляемых средств безопасности для клиента в зависимости от ожидаемых рисков. ■