# Удаленный доступ под надежной защитой

**Глеб Клименко,** *менеджер по работе с заказчиками ЗАО "С-Терра СиЭсПи"*

Современный бизнес мобилен и динамичен, деловой человек должен постоянно находиться на связи, более того, иметь доступ не просто в Интернет, но и к корпоративной информационной среде. Все чаще руководители компаний задумываются о повышении производительности бизнес-процессов за счет организации удаленных рабочих мест для сотрудников, банки и страховые организации предлагают все более широкий спектр интернет-услуг, информационные технологии все глубже внедряются в медицину и образование.

В этих условиях нельзя упускать из виду вопросы обеспечения безопасности передаваемой информации. Защищенный удаленный доступ в корпоративную сеть снижает риски и угрозы потери конфиденциальной информации, вторжения в информационную систему, которые могут привести к значительным убыткам и репутационным потерям компании. Очевидно, что одних организационных методов для снижения рисков недостаточно. Необходимы современные технические средства и адекватные новым угрозам технологии защиты, такие как технология создания среды построения доверенного сеанса (СПДС).

## Применение СПДС "ПОСТ"

Особенностью этого продукта является простота инсталляции и использования, отсутствие необходимости доработки, сложной настройки оборудования, а также дополнительной подготовки или повышения квалификации персонала. Следует отметить, что в состав СПДС "ПОСТ" входят контролируемый встроенный неизымаемый токен производства ведущей российской компании-разработчика, а также высокопроизводительная память стандарта eMMC. Конструкция продукта гарантирует целостность используемого на нем ПО и надежное хранение ключевой информации.

Применение СПДС "ПОСТ" может обеспечить весьма существенные преимущества в сравнении с существующими технологиями защиты. Доверенный сеанс не требует использования антивирусного ПО, обеспечивает удаление любых следов работы пользователя в системе, что исключает риск утечки важной информации даже в случае работы с недоверенного рабочего места. Кроме того, пользователь лишен возможности выполнять несанкционированные действия, так как в среде функционирования ему предоставляется доступ исключительно к целевым приложениям.

Применение СПДС в банковской сфере позволяет, например, гарантированно защитить сеанс связи пользователей ДБО с сервером обслуживания, независимо от защищенности компьютера, с которого осуществляется доступ. Таким образом обеспечивается надежная безопасность наиболее уязвимого места в системе ДБО – рабочего места клиента.

Использование данной технологии в здравоохранении открывает широкие возможности для повышения эффективности использования медицинских информационных систем (МИС). Медицинский работник может в защищенном режиме обрабатывать персональные данные пациента и обмениваться информацией с МИС на любом рабочем месте, загрузив индивидуальную целостную среду функционирования с СЗН, закрепленного за ним. Кроме того, врач имеет возможность безопасно использовать свою электронную подпись с любого рабочего места без риска быть скомпрометированным.

Внедрение технологии СПДС в страховую сферу дает возможность страховому агенту удаленно в режиме доверенного сеанса обращаться в центральную информационную базу страховой компании для получения или передачи информации.

В ряде случаев удобнее использовать комплексное решение для построения доверенного сеанса, включающее не только СЗН, но и бездисковую рабочую станцию (тонкий клиент), настроенную на совместную работу. Например, комплект доверенного сеанса (КДС) от компании "С-Терра", в состав которого входит СПДС "ПОСТ". КДС идеально подходит для организации работы в компаниях, в которых осуществляется посменная работа на одних и тех же рабочих местах. Важно отметить, что в случае использования КДС от "С-Терра" загрузка рабочей станции возможна только при наличии СЗН у сотрудника. При этом достигается персонализация рабочего места каждого сотрудника, снижаются риски утечки данных, предотвращается несанкционированный доступ к конфиденциальной информации, повышается экономическая эффективность использования каждого рабочего места.

Разумеется, невозможно подобрать универсальное решение для всех сценариев обеспечения защищенного удаленного доступа, но при выборе оптимального варианта следует учитывать в первую очередь функциональность, надежность, простоту в исполнении и использовании предлагаемых средств, и конечно, нельзя забывать об экономической эффективности и соответствии требованиям российского законодательства. ●

На российском рынке уже появляются как отдельные устройства, так и комплексные решения отечественных и западных вендоров, предназначенные для построения СПДС. Самый компактный, удобный, надежный и недорогой вариант такого устройства основан на использовании специального загрузочного носителя (СЗН), с которого обеспечивается строгая двухфакторная аутентификация пользователя, доверенная загрузка эталонной среды функционирования, строится защищенное соединение с ресурсами корпоративной сети. При этом используется рекомендованная ФСБ России криптография. В качестве примера такого устройства можно привести СПДС "ПОСТ" – продукт компании "С-Терра", который соответствует требованиям ФСБ России к СКЗИ по классу КС2. Это дает возможность использовать его в информационных системах с повышенными требованиями к защите данных, например в банковских или медицинских ИС.


см. стр. 60