Мобильность и доверенность

Р.Ю. Кобцев, *руководитель группы по связям с общественностью*
В.Ю. Максимов, *PR-менеджер*
В.Н. Зорин, *системный аналитик*

ДАННАЯ ПРОБЛЕМА назревала уже давно. Наконец стало ясно: для повышения эффективности бизнеса важно обеспечить мобильность передачи данных. Это подразумевает возможность использования ноутбука вне корпоративного периметра, т.е. в среде с высоким уровнем угроз по отношению к информационным ресурсам – как непосредственно компьютера, так и всей корпоративной информационной системы (КИС) в целом.

Требовалось решение, гарантирующее необходимый уровень безопасности пользователю и организации при беспроводном обмене данными. Уровень, при котором в случае попыток реализации угроз вероятность ущерба была бы минимальной, а возможный риск не превышал бы допустимых пределов. Было необходимо комплексное решение, обеспечивающее выполнение всех механизмов защиты. И такое решение оказалось возможным только путем объединения целого ряда технологий нескольких производителей в единый комплекс.

Выход есть

Базовый доверенный модуль (БДМ) «Мобильный клиент» предназначен для защиты сотрудников, работающих с корпоративными информационными ресурсами вне и внутри периметра КИС. При правильной корпоративной политике информационной безопасности базовым доверенным модулем способен выступать компьютер сотрудника, клиента, посредника, поставщика, а также других лиц, участвующих в бизнес-процессах организации и обладающих правом доступа к конфиденциальным информационным ресурсам.

Благодаря применению новой технологии защиты БДМ «Мобильный клиент» снижает риски угроз при работе мобильного сотрудника с ресурсами КИС. Основой для нового решения служат встроенная в ноутбук ThinkPad система безопасности ESS и разработанный компанией «Элвис Плюс» продукт FW/VPN-агент «Застава-SC».

«Застава-SC» использует возможности встроенной системы безопасности IBM, что гарантирует дополнительные преимущества.

Вот наиболее ощутимые из них: хранилище ключей, паролей, локальной политики агента и сертификатов защищено на аппаратном уровне; закрытый ключ и пароль базы данных не выходят за границы чипа; закрытый ключ и сертификат открытого ключа пользователя доверительно привязаны к аппаратному ключу компьютера; пароль базы данных агента соответствует паролю пользователя, хранимому в чипе; операции с использованием закрытых ключей и паролей не выходят за границы чипа.

БДМ «Мобильный клиент» обеспечивает выполнение следующих функций: защищенное на аппаратном уровне хранение критически важных данных; идентификация и аутентификация пользователя независимо от ОС; генерация паролей в соответствии с корпоративной политикой безопасности; блокирование атак прямого перебора паролей (атак типа Brute-Force); аппаратная изолированность операций с использованием закрытых ключей; генерация ключей; защита файлов и каталогов; сетевое экранирование БДМ, управляемое корпоративной политикой; формирование VPN-каналов, управляемое корпоративной политикой безопасности; проверка целостности (BIOS, событийных протоколов и т.п.); антивирусная защита.

Многофункциональность – основа БДМ

Для защиты от сетевых атак БДМ «Мобильный клиент» применяется управляемый персональный брандмауэр. Управляемость означает перспективу его динамического конфигурирования в соответствии с требованиями корпоративной политики безопасности. В частности, при доступе в Интернет локальная политика безопасности должна блокировать возможность работы пользователя с подозрительными Web-серверами и порталами. Исходя из потенциальной опасности Интернет-среды, функционирование БДМ будет основано на принципе: запрещены соединения со всеми источниками, кроме доверенных.

Такая политика реализуется как часть корпоративного подхода с помощью центра управления (ЦУ) «Застава». После трансляции в локальные политики для всех «Мобильных клиентов» она загружается в ноутбуки сотрудников по защищенному протоколу. Последний обеспечивает конфиденциальность и целостность локальной политики, причем встроенная подсистема безопасности, установленная на клиенте, гарантирует надежное хранение закрытых ключей.

Продукт «Застава-SC», как FW/VPN-агент, позволяет: формировать защищенные VPN-соединения с КИС посредством протокола ESP (IPSec); аутентифицировать стороны сетевого взаимодействия на основе сертификатов пользователей, хостов, групп с помощью протокола IKE; поддерживать целостность IP-пакетов по протоколу AH (IPSec).

Таким образом, продукт поддерживает все три базовых свойства безопасности информации – конфиденциальность, целостность и доступность.

Одна из самых актуальных задач, стоящих перед пользователем, которую удалось решить базовым доверенным модулем «Мобильный клиент», – минимизация расходов на формирование единой системы безопасности. Экономия осуществляется за счет использования встроенных сервисов безопасности аппаратной платформы и операционной системы.

Продукт сертифицирован – сертификат ФСТЭК России № 1000. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ
ОАО «Элвис Плюс»
см. стр. 48