СКВОЗНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ КАНАЛОВ НА ЛОКАЛЬНОЙ СЕТИ

М.П. РЕВОТЮК, К.Е. КОЛОТЫГИН

Прикладные системы, построенные на основе распределенных архитектур, могут нуждаться в организации надежной защиты логических каналов обмена данными на локальной сети. Например, ввод пароля для доступа к СУБД с рабочей станции, использование низкоуровневых интерфейсов доступа к данным могут порождать угрозу перехвата. Система ответственного назначения не должна становиться уязвимой из-за ошибочных или преднамеренных действий административного или технического персонала корпоративной сети, а также недостаточной защищенности ее компонент.

Надежный метод предвосхищения подобных угроз – сквозная защита критической по безопасности информации, базирующаяся на созда-

нии канала VPN (Virtual Privacy Network) по инициативе конечных пользователей. VPN поддерживается Windows 2000/XP/2003. Однако в последнее время доступны несимметричные криптосистемы с аппаратным хранением ключей или даже программ криптоядра на персональных носителях, например, отечественные разработки “CryptoKey 2001”, “EnigmaCrypt” ООО “Энигма”, практически не нуждающиеся в администрировании.

Объект рассмотрения – каналы VPN на основе персональных аппаратных устройств, обеспечивающие независимость уровня скрытия информации от настроек операционной системы, а также физического канала. Для образования защищенного канала на рабочих станциях абонентов должен быть установлен сервис, реализующий дуплексный обмен с шифрованием трафика по выбранному, из соображений технической реализуемости, открытому протоколу транспортного уровня, например, TCP/IP. Такой сервис играет роль локального прокси-сервера между прикладной программой и внешней средой, активизируемого только после предъявления аппаратных устройств абонентами.

Применение несимметричной криптосистемы обеспечивает гарантированную взаимную аутентификацию абонентов канала и снимает проблему управления ключами. После взаимной аутентификации с целью повышения быстродействия шифрования возможен управляемый переход на режим использования симметричного ключа.

Рассмотренный прием использован для построения защиты эксплуатируемых комплексов, соединяемых по открытым интерфейсам RPC (Remote Procedure Call).