ПРОТОКОЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ VPN-СОЕДИНЕНИЯ

А. Э. АФАНАСЕНКО

Virtual Private Network (виртуальная частная сеть) – технология, которая была разработана для создания надежно защищенных сетей на базе имеющейся и функционирующей инфраструктуры какой-либо глобальной сети. Технология VPN может использоваться для объединения нескольких локальных сетей в одну существующую инфраструктуру, а также для связи одного компьютера с сетью. Объединение сетей происходит с помощью VPN-туннелей, "проложенных" в Интернете. Для их создания и поддержания в рабочем состоянии необходимы специальные протоколы, программное обеспечение, специфическое оборудование. Важно позаботится о защите корпоративной информации (среди которой могут быть и секретные данные), которая будет передаваться по туннелям. Для создания VPN могут использоваться различные протоколы. Тем не менее, на практике почти всегда применяются только два из них: SocketSecure-Layer и IPSec. Большинство же разработчиков выбирают именно второй вариант.

Протокол IPSec включает два протокола: Authentication Header (AH) и Encapsulating Secure Payload (ESP). Первый создает конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений. С его помощью аутентифицируется каждый пакет. Протокол ESP обеспечивает конфиденциальность данных. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов.

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса. С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. IPSec поддерживает не-

сколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее.