16 Безопасность Беспроводных компьютерных систем .

Для обеспечения безопасности в беспроводных сетях используется несколько **средств:**

Контроль за подключением к точке доступа на основе MAC-адресов и имени сети

Шифрование на основе протокола WEP (RC4)

Контроль за доступом к среде передачи на основе протокола 802.1x

Поддержка нового протокола WPA

Настройка VPN поверх беспроводного соединения

Вынос беспроводной сети за межсетевой экран, как сети с низким доверием.

Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Несмотря на то, что новые устройства поддерживают более совершенный протокол шифрования данных WPA и WPA2, многие старые точки доступа не поддерживают его и требуют замены. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало доступной более безопасную схему, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифро - буквенные пароли для того, чтобы максимально усложнить задачу подбора пароля.