Содержание

Изм	*Лист*	*№ докум.*	*Подп.*	*Дата*			
Разраб.					*Лит.*	*Лист*	*Листов*
Пров.						*1*	*4*
Н. контр.							
Утв.							

1 Способы передачи данных

1.1 При выборе физической среды передачи данных учитываются следующие показатели:

- Стоимость оборудования, монтажа и обслуживания;
- Максимальная скорость передачи информации;
- Ограничения на максимальную длину кабеля;
- Безопасность и надежность функционирования сети.

1.2 Для подключения компьютеров между собой будет использоваться стандарт беспроводной локальной связи Wi-Fi 4[1)] на частоте 2.4 ГГц, его характеристики:

- Максимальная скорость передачи данных 300 Мбит/с;
- Максимальное расстояние от передатчика 150 метров на открытой местности;
- Легкость монтажа и наращивания ЛВС;
- Низкая стоимость.

1.3 Способы передачи данных

Непосредственно главным моментом в проектировании сети является выбор способов передачи данных. Способ передачи определяется сетевой технологией, на основе которой построена ЛВС. Оптимальным решением для данной сети являются технологии Fast Ethernet[2)] и Wi-Fi. Они полностью подходят для данной ЛВС по скорости передачи данных, безопасности передачи информации, обратной совместимости с предшествующим им технологиям. Для построения сети достаточно иметь по одному сетевому адаптеру поддерживающие стандарты Wi-Fi для каждого компьютера и один маршрутизатор. Данные технологии позволяют иметь ЛВС хорошую расширяемость, низкую стоимость, простота настройки

[1)] IEEE 802.11n — версия стандарта 802.11 для сетей Wi-Fi, появившаяся в 2009 году.

[2)] Fast Ethernet (FE) — общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с.

и эксплуатации. Работа стандартов Wi-Fi основана на передаче идентификатора сети SSID с помощью пакетов на скорости 0,1 Мбит/с каждые 100 мс. Потому 0,1 Мбит/с — наименьшая скорость передачи данных Wi-Fi. С помощью SSID клиент может выяснить о возможности подключения к точке доступа. Защита канала передачи данных с помощью Wi-Fi основана на методах шифрования:

- WEP[1)] — это первый стандарт защиты Wi-Fi, на самом деле не дает защиты по сравнению с проводными сетями, так как имеет множество уязвимостей и взламывается множеством разных способов, что из-за расстояния покрываемого передатчиком, делает данные более уязвимыми. Данный протокол обеспечивает защиту канала передачи данных только на короткое время, спустя которое любую передачу данных можно взломать вне зависимости от сложности пароля — пароли в WEP либо 40 либо 104 бита, что есть крайне короткая комбинация. Все эти недостатки имеются из-за времени создания WEP — конец 90-х годов и потому IEEE[2)] в 2004 году обьявили WEP устаревшим.
- WPA[3)] — второе поколение защищенных протоколов Wi-Fi. Совершенно иной уровень защиты каналов данных в сравнении с WEP. Длина пароля произвольная, от 8 до 63 байт. Поддерживает различные алгоритмы шифрования данных после авторизации в сети. WPA в главной степени отличается от WEP тем, что шифрует данные каждого клиента по отдельности — после авторизации генерируется временный ключ PTK который используется для кодирования передачи данных конкретного клиента.
- WPS[4)] — протокол, позволяющий для авторизации вместо пароля использовать кнопку на роутере для подключения. При выпуске этого протокола была фундаментальная уязвимость — WPS позволяет под-

---

[1)] Wired Equaivalent Privacy

[2)] Институт инженеров электротехники и электроники — IEEE (англ. Institute of Electrical and Electronics Engineers) (I triple E — «Ай трипл и») — международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей.

[3)] Wi-Fi Protected Access

[4)] Wi-Fi Protected Setup

ключиться к точке доступа по 8-ми символьному коду, состоящему из цифр. Но из-за ошибки нужно подобрать всего лишь 4 из них.