СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Беспроводные технологии

СПбГЭТУ «ЛЭТИ», 2021 г.

8. БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

8.1 Теоретические основы построения и архитектура беспроводных сетей

Беспроводные технологии— подкласс технологий для передачи информации на расстояние между двумя и более точками для передачи данных между которыми используется инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

В настоящее время существует множество беспроводных технологий, наиболее часто применяемыми из которых являются, Wi-Fi, WiMAX, Bluetooth, GPRS,CDMA, 3-5G (рис 8.1).

Рис. 8.1

Каждая из технологий обладает определёнными характеристиками, которые определяют её область применения (табл 8.1).

Таблица 8.1

	PAN	*LAN*	*MAN*	*WAN*
Стандарты	Bluetooth	IEEE 802.11 a/g/n	802.16 MMDS,LMDS	GPRS,CDMA, 3-5G
Скорость	< 48 Мбит/с	54-300 Мбит/с	40Мбит/с- 1 Гбит/с	10-25 Гбит/с
Диапазон	Короткий	Средний	Длинный	Длинный
Область применения	Точка-Точка	Сеть	Доступ последней мили	Мобильные устройства

Существуют различные подходы к классификации беспроводных технологий.

По дальности действия:

- беспроводные персональные сети (WPAN— Wireless Personal Area Networks). Примеры технологий— Bluetooth;
- беспроводные локальные сети (WLAN— Wireless Local Area Networks). Примеры технологий— Wi-Fi;

- беспроводные сети масштаба города (WMAN— Wireless Metropolitan Area Networks). Примеры технологий — WiMAX;
- беспроводные глобальные сети (WWAN — Wireless Wide Area Network). Примеры технологий— CSD, GPRS, EDGE, EV-DO, HSPA;

Стандарт IEEE 802.11. Технология передачи данных Wi-Fi разработана консорциумом Wi-Fi Alliance на базе стандартов IEEE 802.11, является набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6; 5 и 60 ГГц. IEEE определяет четыре основных стандарта WLAN 802.11: 802.11a, 802.11b, 802.11g и 802.11n (табл 8.2), которые не требуют лицензирования.

Таблица 8.2

	802.11a	802.11b	802.11g	802.11n
Год принятия	1999	1999	2003	2009
Скорость	54 Мбит/с	11 Мбит/с	54 Мбит/с	До 600 Мбит/с
Полоса частот	5 ГГц	2.4 ГГц	2,4 ГГц	2,4-2,5 или 5 ГГц
Количество каналов	23	3	3	9

Применение технологии позволяет обеспечить защиту от помех и коллизий за счет применения дополнительных механизмов обеспечения помехоустойчивости в том числе на (рис 8.2):

- уровень MAC – способ доступа к общей среде выполняет следующие функции: доступ к разделяемой среде; обеспечение перехода станции между базовыми станциями; обеспечение безопасности передачи данных;
- уровень LLC – передача данных

Рис. 8.2

Сеть Wi-Fi может использоваться как самостоятельная сеть, либо в составе более сложной сети, с подключением к проводным сегментам сети.

Рассмотрим ***основные элементы,*** необходимые для построения сети:

Для построения беспроводной сети используются Wi-Fi адаптеры и точки доступа.

Независимые базовые зоны обслуживания (IBSS) - представляют группу работающих станций, связывающихся непосредственно одна с другой (ad-hoc сетью) без использования отдельной точки доступа (рис 8.3).

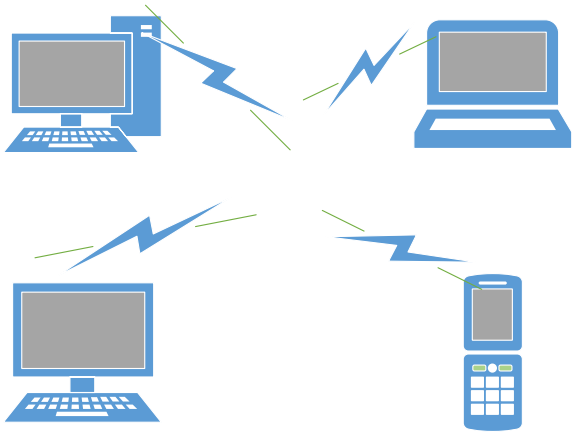

Рис. 8.3

Станции непосредственно устанавливают соединения друг с другом, в результате чего создается только одна базовая зона обслуживания (BSS), не имеющая интерфейса для подключения к проводной локальной сети. Алгоритм передачи данных:

1. При инициации передачи данных станция задает сигнальный (маячковый) интервал для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT) и синхронизации времени.

2. При завершении передачи маячкового сигнала каждая станция приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего TBTT, определяет новую случайную задержку.
3. Если маячковый сигнал не поступает до окончания случайной задержки, посылает маячковый сигнал и возобновляет работу приостановленных таймеров задержки.

К недостаткам данной технологии передачи данных можно отнести:

- передаваемый сигнал намного мощнее принимаемого;
- проблемы «скрытой» и «засвеченной» станции;
- сигнал о коллизии может не дойти до всех компьютеров;
- при отсутствии подтверждения кадр пересылается повторно;

Коллизия обходится очень дорого:

- обнаруживается по отсутствию подтверждения;
- временные затраты: передача кадра, тайм-аут ожидания подтверждения.

Проблема «скрытой станции» возникает, когда не все станции могут получить «маячковый сигнал» друг от друга, например сигнал может быть не воспринят станцией, находящейся в другой части сети:

- Хост B планирует осуществить передачу данных A, контроль канала показал, что он свободен.
- В этот же момент времени хост C тоже решил передать данные хосту A, поскольку зона действия беспроводной среды C свободна.

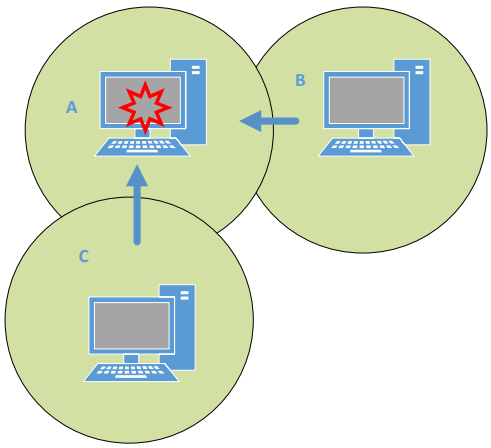

Рис. 8.4

- Однако, когда эти данные дошли до хоста A, они столкнулись с теми данными, которые передавал хост B, произошла коллизия и хост A не может принять данные, не от одного элемента сети.

Проблема «засвеченной станции» возникает, когда хост D находится вне зоны действия передатчика хоста B, поэтому хост C может смело передавать данные хосту D, однако сам хост C находится в зоне действия передатчика хоста B, поэтому он считает, что среда занята и ждет, когда хост B закончит передачу (рис 8.5).

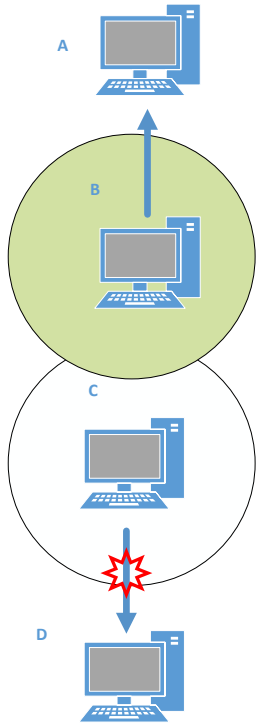

Рис. 8.5

Базовая зона обслуживания (Basic Service Set - BSS) - группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется точкой доступа (access point) (рис 8.6)

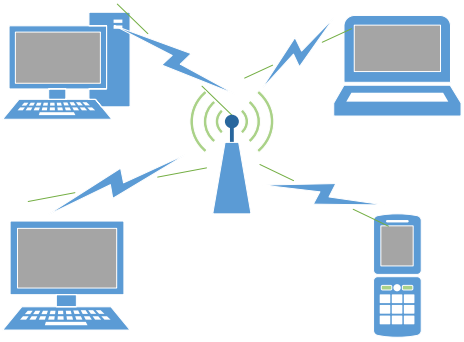

Рис. 8.6

Использование данной технологии позволяет реализовать возможность подключения достаточно большого количества пользователей и обладает более высокой помехоустойчивостью. Точка доступа может работать как по прямому назначению, так и в составе проводной сети и служить в качестве моста между проводным и беспроводным сегментами сети.

Расширенные зоны обслуживания Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа с целью построения распределенной сети (Wireless Distributed System - WDS). Это режимы беспроводного моста "точка-точка" и "точка - много точек", беспроводной клиент и повторитель (рис 8.7).

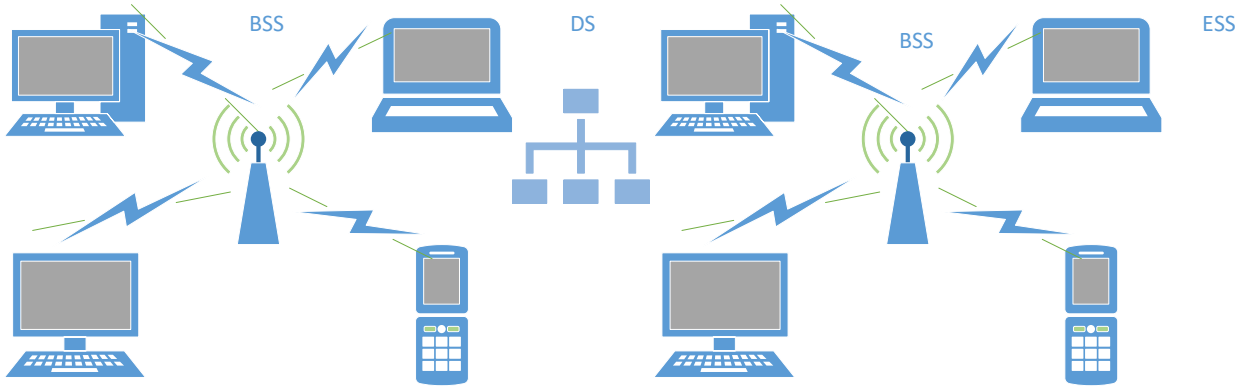

Рис. 8.7

В этом случае расширенные зоны обслуживания можно рассмотреть, как сети, включающие:

- сеть с базовым набором услуг (Basic Service Set - BSS) –единица сети, состоит из нескольких станций, реализующих протокол MAC. Соединяется с распределительной системой (Distribution System - DS) через точку доступа или кабельное соединение. Станция-

приемник использует идентификатор зоны обслуживания (Service Set IDentifier - SSID) для фильтрации получаемых сигналов и выделения того, который ей нужен;

- сеть с расширенным набором услуг (Extended Service Set - EES) – состоит из нескольких BSS объединенных распределительной системой DSS;
- служба распределенной системы (Distributed System Service - DSS) обеспечивает передачу пакетов между станциями, которые не могут взаимодействовать непосредственно. DSS бразуется базовыми станциями и распределительной системой DS. DS может быть основана на проводной или беспроводной среде.

Доступ к сети обеспечивается путем передачи широковещательных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций.

Режимы коллективного доступа к среде. Для борьбы с коллизиями в 802.11 использует типа коллективного доступа к среде передачи данных, с использованием:

- функции распределенной координации (Distributed Coordination Function, DCF)
- функции централизованной координации (Point Coordination function, PCF).

Протокол Multiple Access with Collision Avoidance (MACA) позволяет осуществить реализацию вышеуказанных функций и:

- может использоваться в Wi-Fi (не обязательно);
- применяется в основном в произвольном режиме (Ad-hoc).

Режим DCF. DCF – подуровень для эпизодического обмена равноправных станций – каждая станция может захватить среду. Эта функция основана на методе коллективного доступа с обнаружением несущей и механизмом избегания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA):

1. Каждый хост, прежде чем начать передачу, «прослушивает» среду, пытаясь обнаружить несущий сигнал, и только при условии, что среда свободна, может начать передачу данных.

2. Если среда занята, то хост устанавливает таймер ожидания = время резервации канала (время, необходимое на полную передачу сообщения) + время передачи кадра + короткий межкадровый интервал + время передачи подтверждения. После этого повторяется попытка передачи кадра.

3. Если получатель принял кадр неискаженным, то он подтверждает получение, посылая служебный кадр ACK - квитанцию о доставке.

4. Если передающая станция не получила пакет ACK, то предполагается, что произошла коллизия, и через случайный промежуток времени кадр передаётся снова.

Пример пересылки кадров в режиме DCF (рис 8.8):

1. A посылает B кадр RTS, запрашивая разрешение на передачу.

2. B подтверждает возможность передачи кадром CTS (+размер сообщения).

3. A запускает таймер ACK и начинает передачу данных.

4. В случае корректного приема, B генерирует кадр ACK, сообщающий станции A о конце передачи. Если интервал времени таймера на станции A истекает прежде, чем получен ACK, весь алгоритм работы протокола повторяется с самого начала. Механизм выставления NAV удерживает станции от передачи.

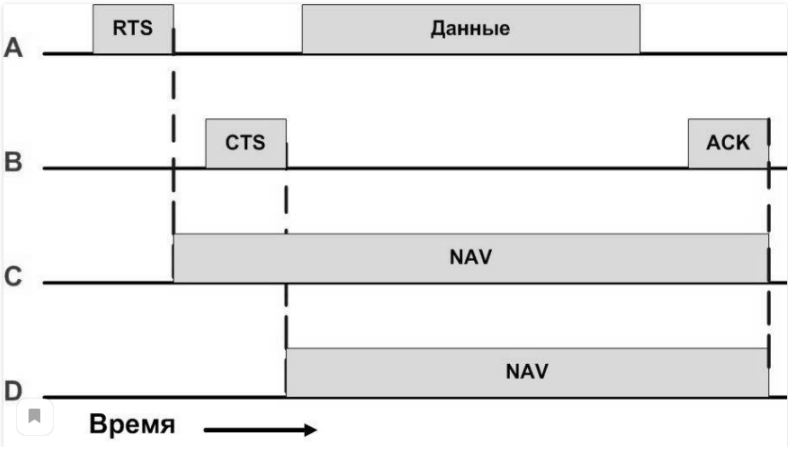

Рис. 8.8

Недостаток: конфликтный принцип, асинхронная передача.

Режим DCF с фрагментацией пакетов. *Фрагментация* повышает надежность передачи путем принудительной повторной пересылки коротких отрезков кадров, в которых произошла ошибка, а не кадров целиком.

1. Осуществляется разбиение кадров на небольшие отрезки, каждый из которых содержит собственную контрольную сумму.

2. Фрагменты нумеруются и подтверждаются индивидуально с использованием протокола с ожиданием и передаются по сети.

3. Подтверждение принудительной повторной пересылки коротких отрезков кадров, в которых произошла ошибка, а не кадров целиком

4. Механизм выставления NAV удерживает станции от передачи.

Пример пересылки кадров в режиме DCF с фрагментацией (рис 8.9):

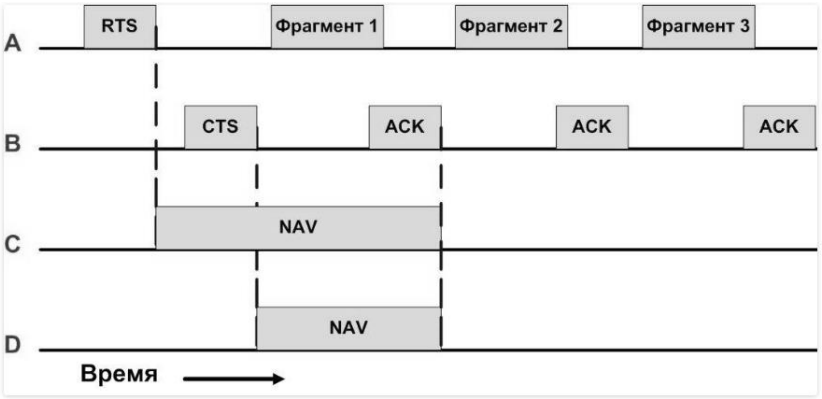

Рис. 8.9

Недостаток – уменьшение пропускной способности сети

Режим DCF решение проблемы скрытой станции (рис 8.10).

1. Хост В инициирует передачу данных с хостом В сообщением RTS

2. Хост А в ответ передает управляющее сообщение CTS и это сообщение получает не только *хост В*, но и *С*, который находятся вне зоны действия передатчика *компьютера В*.

3. Хост С понимает, что сейчас *В*, сигнал от которого он не видит, будет передавать данные размером 1500 байт, поэтому он ждет, когда передача закончиться.

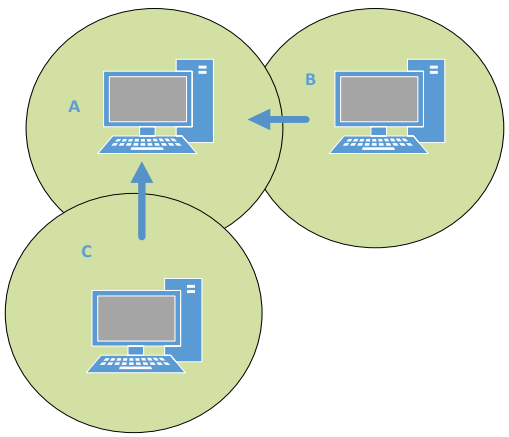

Рис. 8.10

Режим PCF. Режим PCF применяется в тех случаях, когда необходимо приоритезировать чувствительный к задержкам трафик. Использует интервалы коллективного доступа:

- пересылка приоритетного трафика (Short IFS);
- PIFS – D(CF)IFS – процедура организации приоритетного синхротрафика;
- DIFS – процедура организации неприоритетного асинхронного трафика.

Приоритеты интервалов:

- Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.
- Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период.
- Захват среды возможен, когда среда свободна в течение времени, равного или большего, чем DIFS.

Механизм PCF является опциональным и применяется в сетях с точкой доступа, выступающей в виде центра координации (Point Coordinator, PC, рис 9.11)

1. Каждый хост может работать в режиме PCF, для этого он должен подписаться на эту услугу при присоединении к сети.
2. Координатор циклически опрашивает станции с приоритетным трафиком используя процедуру опроса, для реализации права хостов на использование среды, направляя им специальный кадр.
3. Хост, получив такой кадр, подтверждает прием специального кадра и одновременно передает данные к адресату в интервале SIFS-PIFS.
4. При отсутствии подтверждения координатор опрашивает следующую станцию в интервале PIFS-DIFS.
5. После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.

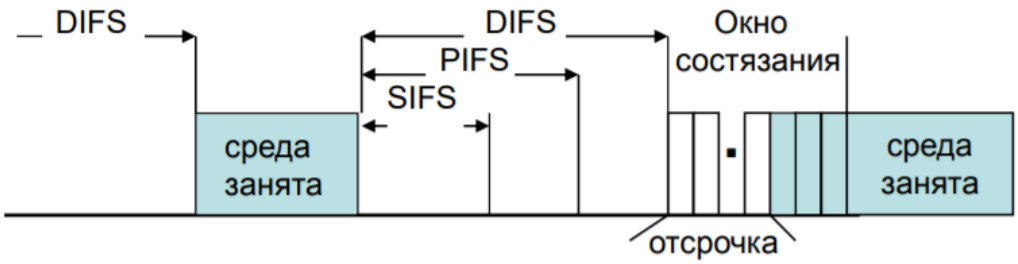

Рис. 8.11

8.2 Безопасность передачи данных в беспроводных технологиях

При всех своих достоинствах развертывания средств передачи данных в беспроводных сетях, технология имеет ряд проблем при обеспечении безопасности сетевого взаимодействия.

Возможные атаки на беспроводные технологии представлены на рис. 8.11.

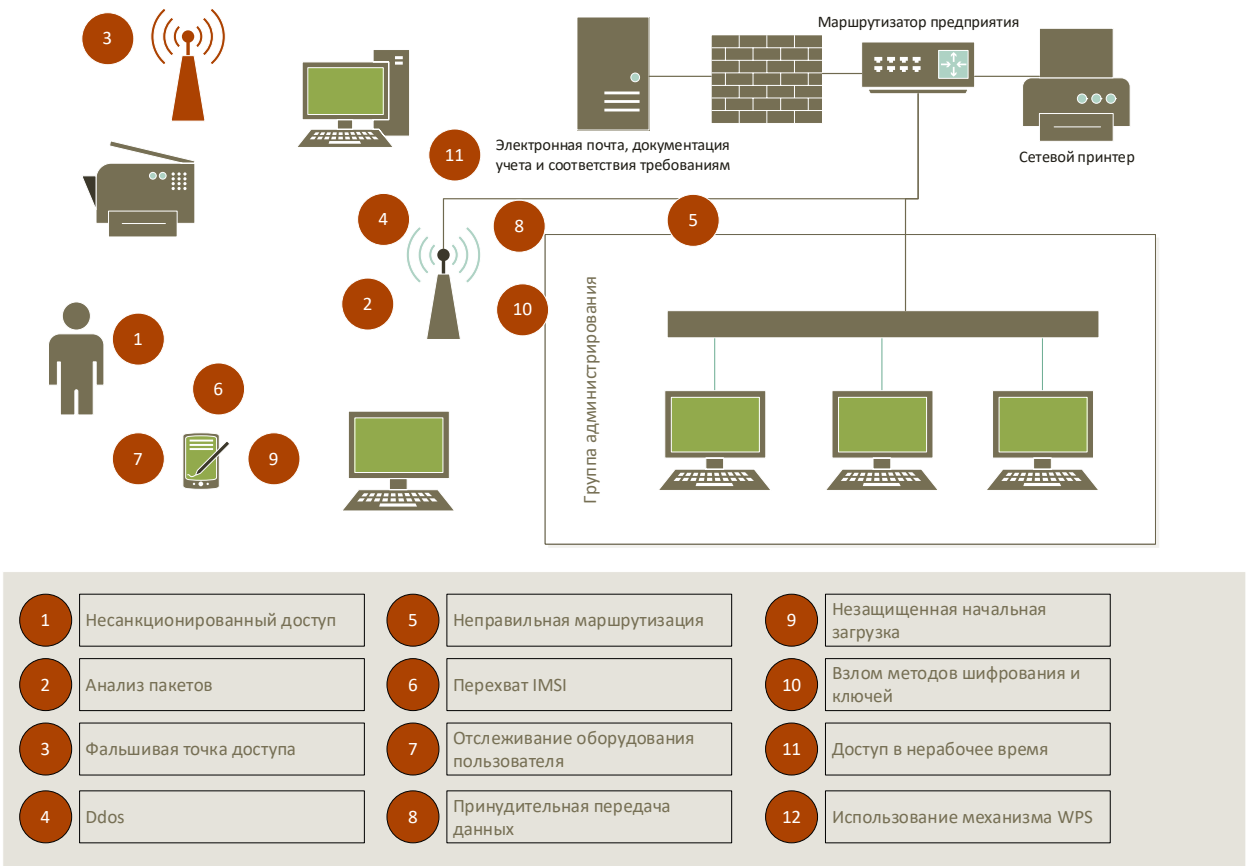

Рис. 8.22

Выделяют несколько основных видов атак, направленных на беспроводные сети.

Атаки напрямую на сеть:

- *анализ* пакетов -осуществляется путем перехвата сигнала при помощи станции с Wi-Fi-адаптером. Подключенный сетевой сниффер пакетов

позволяет отображать все данные, передаваемые по сети (включая логины и пароли, а также посещенные страницы и передаваемые данные);

- реализация атаки Ddos - злоумышленник создает устройство, заполняющее весь спектр на частоте 2.4 Ггц помехами и нелегальным трафиком. При этом достаточно трудно доказать сам факт проведения DDos атаки на физическом уровне в беспроводной сети.

Выделяют два вида DDoS-атак: нападение на физический и программный уровни системы. Атаки первого вида рассчитаны на простое исчерпание ресурсов жертвы, они переполняют систему запросами на ресурсы (пропускную способность, процессорное время, дисковое пространство и т. п.). Атаки второго вида основаны на использовании уязвимостей в программном обеспечении атакуемого ресурса и через него сформировать атаку.

*Организация поддельных точек доступа -з*адача сводится к «созданию» двойника сети, который будет дублировать имя настоящей точки, и к которому у потенциальной жертвы может быть сконфигурирован доступ (как с зашитой, так и без). Также, при наличии рядом легитимной точки доступа, злоумышленник может попытаться ее «погасить», чтобы перенаправить клиентов на свою точку доступа. В этом случае устройство злоумышленника будет не просто подслушивающим устройством, а непосредственным интернет-шлюзом для доступа в Интернет, что дает возможность перехватывать любые отправляемые или получаемые данные.

Избыточное покрытие сети позволяет осуществить подключение сторонних лиц за пределами контролируемого периметра сети.

Проблемы идентификатора беспроводной ЛВС. Идентификатор SSID регулярно передается точками радиодоступа в специальных фреймах beacon. По нему атакующий может определить SSID с помощью анализатора трафика, например Sniffer Pro Wireless.

Уязвимость аутентификации по MAC-адресу. При аутентификации по MAC-адресу, атакующий может обмануть метод аутентификации путем подмены своего MAC-адреса легитимным. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться

анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

Уязвимость открытой аутентификации. Открытая аутентификация не позволяет определять легитимность пользователя, в связи с этим рекомендуется использовать WEP. Или использовать методы аутентификации более высокого уровня.

Использование механизма WPS позволяет получить доступ к беспроводной сети на уровне администратора сети.

Атака реализованная путем проникновения через гостевой доступ позволяет подключиться к гостевой сети и осуществить анализ трафика, сотрудников, случайно подключенных к данной сети.

Атаки на сетевое оборудование использование неправильно сконфигурированные точки доступа или устройства, для доступа к атакам на сетевое оборудование.

Вероятность реализации указанных повышается, если:

- используются протоколы WEP/PEP;
- у пользователя настроено автоматическое подключение к сети;

Подобные атаки реализуются не только в незащищенных беспроводных сетях, где все данные передаются в незашифрованном виде. Злоумышленники могут подобрать пароль сети методом перебора и подключиться к закрытой беспроводной сети.

8.3 Реализация безопасности беспроводных сетей

Борьба с атаками в беспроводных сетях имеет ряд особенностей, связанных с мобильностью атакующих, поскольку невозможно ни отследить их физическое местоположение, ни изолировать их от сети.

Наиболее распространенные механизмы защиты представлены на рис. 8.12

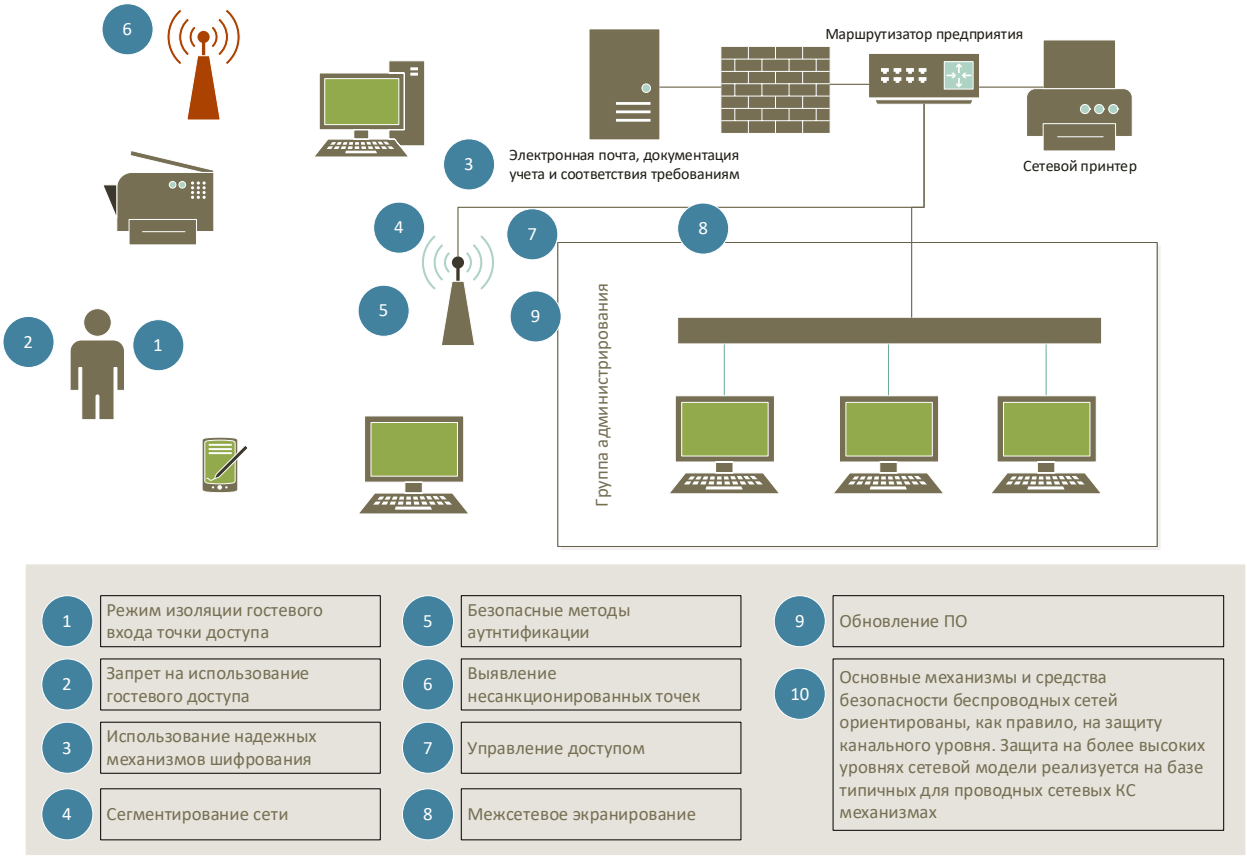

Рис. 8.12

К ним относят:

- обеспечение физической защиты точки доступа от использования механизма WPS и изменения пароля, установленного по умолчанию;
- отключение трансляции SSID сети;
- ограничение числа компьютеров с доступом в Интернет, запрет на использование сотрудниками гостевого доступа;
- фильтрация доступа по MAC-адресам;
- использование механизмов аутентификации и шифрования данных;
- использование механизмов межсетевого экранирования;
- оценка диаграмм направленности сети для снижения мощности сигнала и-перемещения оборудование (центр, другие помещения);
- настройка передающих устройств таким образом, чтобы вход в систему управления был разрешен только для проводного соединения, когда точка доступа напрямую подключена к компьютеру через сетевой кабель.
- Технология Wi-Fi предусматривает два механизма аутентификации беспроводных абонентов:

Процессы аутентификации состоит из следующих этапов:

1. Пользователь посылает фрейм Probe Request во все радиоканалы, чтобы найти все точки радиодоступа с необходимыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена.
2. Точки радиодоступа, находящиеся в радиусе действия сигнала отвечают фреймом Probe Response, содержащим синхронизирующую информацию и данные о текущей загрузке точки радиодоступа.
3. Пользователь определяет, с какой точкой доступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).
4. Точка радиодоступа посылает подтверждение аутентификации (Authentication Reply).
5. В случае успешной аутентификации пользователь посылает точке радиодоступа фрейм ассоциации (Association Request).
6. Точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response).
7. Осуществляется обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP:

1. Пользователь посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка радиодоступа посылает подтверждение аутентификации, содержащее Challenge Text.
3. Абонент шифрует Challenge Text своим статическим WEP-ключом и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем Challenge Text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

Аутентификация по MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования

для беспроводных сетей. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации

Механизм шифрования WEP (Wired Equivalent Privacy). В технологии применяется симметричные криптоалгоритмы - RC4. К особенностям WEP-протокола относят:

- устойчивость к атакам, связанным с простым перебором ключей шифрования;
- использование самосинхронизации для каждого сообщения (позволяет уменьшить число искаженных и потерянных пакетов);
- легкость в реализации;
- открытость;
- проблемы управления статическими WEP-ключами, поэтому утрата абонентского адаптера, точки радиодоступа или собственно секретного ключа представляют опасность для системы безопасности беспроводной локальной сети.

Алгоритм реализации. Поля Кадр WEP включает в себя следующие поля: незашифрованная часть; вектор инициализации; идентификатор ключа; зашифрованная часть; данные; контрольная сумма. Для шифрования:

1. Каждый участник устанавливает у себя общий секретный ключ (в 802.11 предусмотрено наличие до четырех секретных ключей). Размер секретного ключа может быть установлен равным 40 или 104 битам.
2. Вектор инициализации размером 24 бита, добавляется к секретному ключу со стороны младших байтов и формирует ключ шифрования данного пакета (размером 64 или 128 бит) (рис 8.13).
3. Использование алгоритма RC4 и полученного ключа шифрования позволяет зашифровать данные с использованием псевдослучайной последовательностью. Отправитель добавляет IV и идентификатор ключа в соответствующее поле в заголовке пакета и устанавливает битовый флаг, сообщающий об использовании WEP. Пакет отправляется получателю.

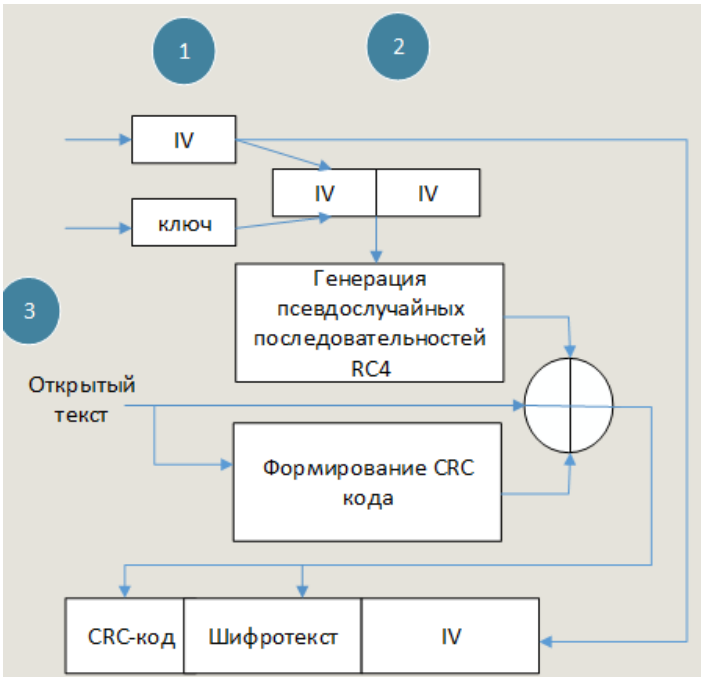

Рис. 8.33

Для расшифрования:

1. Получатель извлекает IV из заголовка пакета, добавляет его к своему секретному ключу и формирует ключ шифрования (рис 8.14).
2. На основе полученного ключа шифрования в соответствии с алгоритмом RC4 формируется ПСП, размер которой равен размеру зашифрованных данных в пакете. Получатель выполняет сложение ПСП с шифротекстом и таким образом восстанавливает открытый текст.
3. Получатель сравнивает эталонный CRC-код, содержащийся в пакете, с CRC-кодом, вычисленным для расшифрованного открытого текста. При отрицательном результате сравнения пакет считается некорректным и отбрасывается.

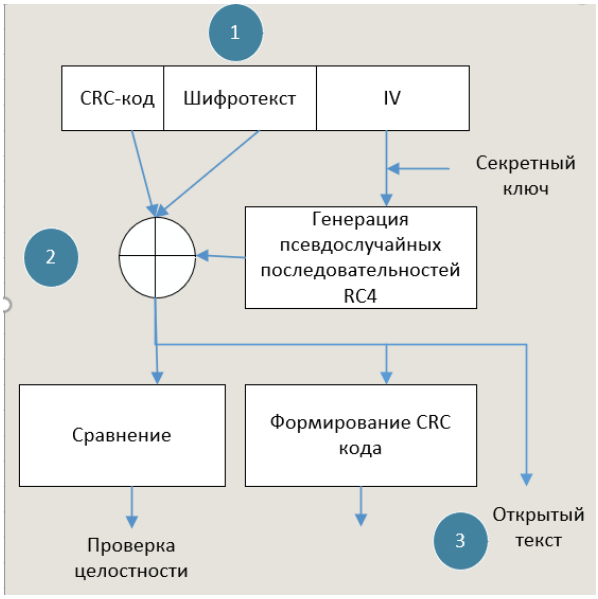

Рис. 8.44

Уязвимость шифрования WEP. Секретный ключ шифрования WEP может быть выделен с использованием определенных фреймов, собранных в при передаче в сети с использованием статистического анализа.

Повторное использование вектора инициализации, позволяет вычислить ключ для этого [4]:

1. Осуществляется отправка абоненту беспроводной локальной сети сообщение известного содержания последующим сбором фреймов, предположительно содержащие шифрованное сообщение.

2. Поиск ключевой последовательности, путем использования функции XOR к предполагаемому шифрованному и известному нешифрованному сообщениям, для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.

3. Формирование фрейма с сообщением ICMP на основании полученной на ш. 2 ключевой последовательности, один байт длиннее, чем длина уже известной ключевой последовательности, байт выбирается случайным образом из 256 возможных ASCII-символов.

4. Итерация шага 3 до тех пор, пока не будет подобрана ключевая последовательность нужной длины.

Основное отличие ***спецификация WPA (Wi-Fi Protected Access)*** от WEP заключается в использовании временного протокола целостности ключа (Temporal Key Integrity Protocol, TKIP), который позволяет осуществить:

- пофреймовое изменение ключей шифрования. WEP-ключ быстро изменяется, и для каждого фрейма он другой используется для того, чтобы атакующий не смог накопить фреймы в количестве, достаточном для вывода битов ключа;
- усовершенствованный механизм управления ключами TKIP.
- контроль целостности сообщения MIC.

Механизм защиты состоит из следующих шагов:

1. *Пофреймовое изменение ключей шифрования*. Помимо увеличения 24-разрядный вектор инициализации до 48-разрядного IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV. При этом 48-разрядный IV разбивается на части для использования при пофреймовом изменении ключа (рис 8.14), [5].

1.1 Устройство инициализирует IV, присваивая ему значение 0.

1.2 Базовый WEP-ключ (например, имеющим 128-разрядное значение) перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0-4 294 967 295) и MAC-адресом передатчика (имеющим 48-разрядное значение). Результат этого действия называется ключ 1-й фазы (80-разрядное значение). Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ.

1.3 Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика для выработки значения 128-разрядного пофреймового ключа, первые 16 разрядов которого представляют собой значение IV (16 нулей).

1.4 Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит (в стандартном 24-битовом IV) представляют собой фиксированное значение, используемое как заполнитель.

1.5 Пофреймовый ключ применяется для WEP-шифрования фрейма данных.

1.6 Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. После того как пофреймовые возможности IV будут исчерпаны, IV 1-й фазы (32 бита) увеличивается на 1 (он теперь будет состоять из 31 нуля и одной единицы, 00000000000000000000000000000001) и т. д.

1.7 Значение пофреймового ключа вычисляется заново, как на этапе 2.

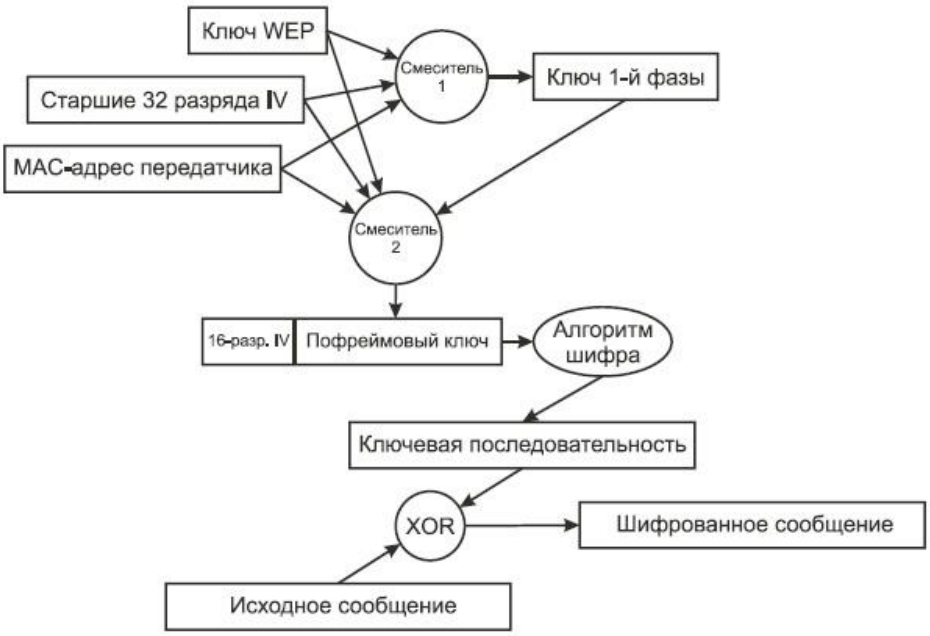

Рис. 8.15 [5]

2. *Использование контроля целостности сообщения (MIC)* устраняет проведение атак с использованием поддельных фреймов и манипуляции битами. Для этого MIC формируются уникальный ключ, отличающийся от ключа, используемого для шифрования фреймов данных, перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма (рис 8.16).

Рис. 8.16 [5]

3. Механизм шифрования TKIP осуществляется следующим образом (рис 8.17):
4. С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ.
5. Алгоритм MIC генерирует MIC для фрейма в целом.
6. Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
7. Фрагменты фрейма шифруются с помощью пофреймового ключа.
8. Осуществляется передача зашифрованных фрагментов.

Рис. 8.17 [5]

Аналогично процессу шифрования по алгоритму TKIP, процесс расшифрования (рис 8.18):

1. Предварительно вычисляется ключ 1-й фазы.

2. На основании IV, полученного из входящего фрагмента фрейма WEP, вычисляется пофреймовый ключ 2-й фазы.

3. Если полученный IV не тот, какой нужно, фрейм отбрасывается.

4. Фрагмент фрейма расшифровывается, и осуществляется проверка признака целостности (ICV).

5. Если контроль признака целостности дает отрицательный результат, такой фрейм отбрасывается.

6. Расшифрованные фрагменты фрейма собираются, чтобы получить исходный фрейм данных.

7. Приемник вычисляет значение MIC и сравнивает его со значением, находящимся в поле MIC фрейма.

8. Если эти значения совпадают, фрейм обрабатывается приемником.

9. Если эти значения не совпадают, значит, фрейм имеет ошибку MIC, и приемник принимает меры противодействия MIC.

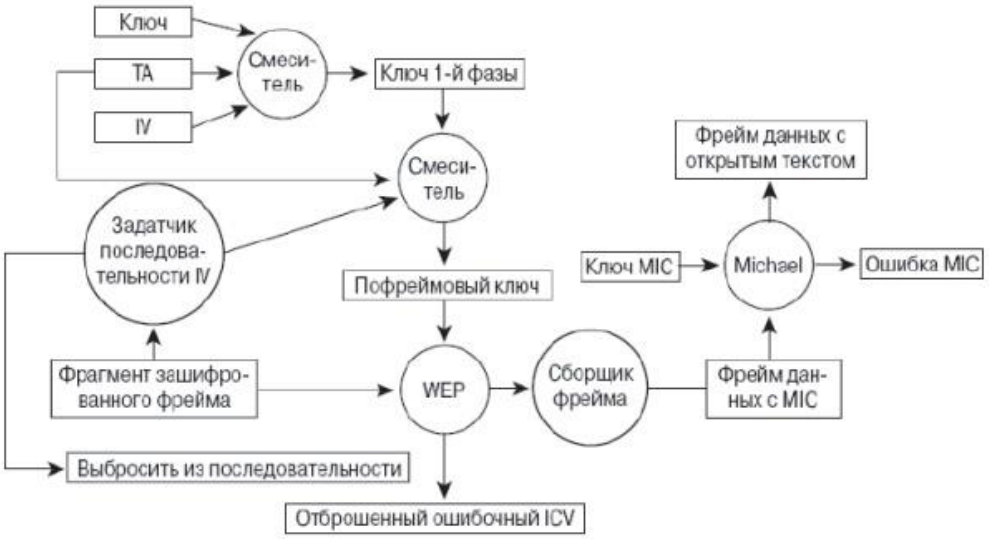

Рис. 8.18[5]

Меры противодействия MIC состоят в выполнении приемником следующих задач:

- Приемник удаляет существующий ключ на ассоциирование.
- Приемник регистрирует проблему как относящуюся к безопасности сети.

- Ассоциированный клиент, от которого был получен ложный фрейм, не может быть ассоциирован и аутентифицирован в течение 60 секунд, чтобы замедлить атаку.

Клиент запрашивает новый ключ.

WPA может работать в двух режимах (табл 8.3):

- Pre-Shared Key (персональный) при котором применение WPA осуществляется всеми категориями пользователей беспроводных сетей с единым паролем на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). Подобный подход уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами WEP, заменяя их целостной и четкой системой на основе цифро-буквенного пароля.
- Enterprise (корпоративный), где хранение базы данных и проверка аутентичности осуществляются специальным сервером, чаще всего RADIUS.

- Таблица 8.3

Технология	*Статический WEP*	*Динамический WEP*	*WPA*	*WPA 2 (Enterprise)*	*WPA 3*
Год принятия	1999	1999	2003	2004	2018
Аутентификация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ	Технология SEA
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES	SHA, BIP-GMAC-256
Шифрование	Статический ключ 40 бит	Сессионный ключ	129	CCMP (AES) 40 бит	CCMP (AES) 128 бит, 198 бит
Распределение ключей	Однократное, вручную	Сегмент Pair-wise Master Key (PMK)	Производное от PMK	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)	48-битный вектор инициализации

Алгоритм шифрования	RC4	RC4	RC4	AES	AES
Длина ключа, бит	64/128	64/128	128	до 256	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS	RADIUS

В WPA3-Personal обеспечена надёжная защита за счет:

1. Ограничения на число попыток ***аутентификации*** в рамках одной сессии рукопожатия. Вместо PSK (Pre-Shared Key) ключа в WPA3 реализована технология SAE (Simultaneous Authentication of Equals), основывающиая на протоколе обмена ключами Диффи — Хеллмана с использованием конечных цикличных групп.
2. Результирующий сессионный ключ, который получает каждая сторона соединения для аутентификации сеанса, вырабатывается на основе информации из пароля, ключей каждой системы и MAC-адресов обеих сторон. Компрометация закрытого ключа одной из сторон не приводит к компрометации сессионного ключа, т.е. даже узнав пароль атакующий не сможет расшифровать ранее перехваченный трафик.

В WPA3-Enterprise применяется:

-шифрование на основе как минимум 192-разрядных ключей, соответствующих требованиям CNSA (Commercial National Security Algorithm);

- для аутентифицированного шифрования рекомендовано применение 256-разрядных ключей GCMP-256 (Galois/Counter Mode Protocol);

-для передачи и подтверждения ключей используется HMAC с хэшами SHA-384 (HMAC-SHA384);

для согласования ключей и аутентификации используются ECDH (Elliptic Curve Diffie-Hellman) и ECDSA (Elliptic Curve Digital Signature Algorithm) с 384-разрядными эллиптическими кривыми,

- для защиты целостности кадров применяется протокол BIP-GMAC-256 (Broadcast/Multicast Integrity Protocol Galois Message Authentication Code).

8.4 Bluetooth

Bluetooth —спецификация IEEE 802.15.1 беспроводных персональных сетей WPAN, обеспечивающая обмен информацией между оконечными пользовательскими устройствами, такими как персональные компьютеры,

мобильные телефоны, принтеры, цифровые фотоаппараты, устройства ввода, наушники, гарнитуры на радиочастоте для ближней связи.

Топология сети. Обмен информацией в сети может осуществляться только между ведущим (master) и подчинённым (slave) устройствами, организация связи между которыми, представлена на рис.8.19:

- пикосеть точка-точка;
- пикосеть звезда;
- рассеянная пикосеть;

Подчинённое устройство может сообщаться только с ведущим, причём только тогда, когда это разрешает ведущее устройство [6]. В каждый момент времени обмен данными может идти только между двумя устройствами в одном направлении.

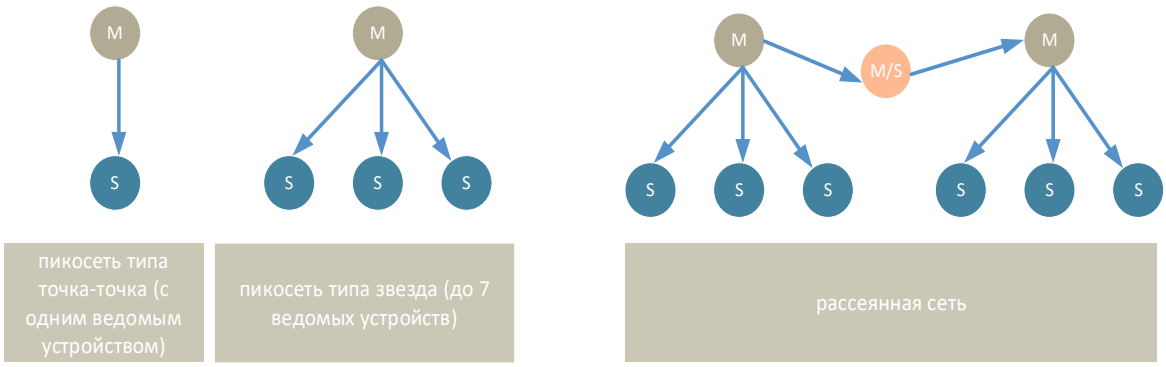

Рис. 8.19

Стек протоколов используется для обеспечения сетевого взаимодействия и построения профиля (набора возможностей). К протоколам, используемым в относят Bluetooth [7]:

LMP (Link Management Protocol)— используется для установления и управления радиосоединением между двумя устройствами. Реализуется контроллером Bluetooth.

HCI (Host/controller interface)— определяет связь между стеком хоста (то есть компьютера или мобильного устройства) и контроллером Bluetooth.

L2CAP (logical Link Control and Adaptation Protocol)— используется для мультиплексирования локальных соединений между двумя устройствами, использующими различные протоколы более высокого уровня. Позволяет фрагментировать и пересобирать пакеты.

SDP (Service Discovery Protocol)— позволяет обнаруживать услуги, предоставляемые другими устройствами, и определять их параметры.

RFCOMM (Radio Frequency Communications)— протокол замены кабеля, создаёт виртуальный последовательный поток данных и эмулирует управляющие сигналы RS-232.

BNEP (Bluetooth Network Encapsulation Protocol)— используется для передачи данных из других стеков протоколов через канал L2CAP. Применяется для передачи IP-пакетов в профиле Personal Area Networking.

AVCTP (Audio/Video Control Transport Protocol)— используется в профиле Audio/Video Remote Control для передачи команд по каналу L2CAP.

AVDTP (Audio/Video Distribution Transport Protocol)— используется в профиле Advanced Audio Distribution для передачи стереозвука по каналу L2CAP.

TCS (Telephony Control Protocol — Binary) — протокол, определяющий сигналы управления вызовом для установления голосовых соединений и соединений для передачи данных между устройствами Bluetooth. Используется только в профиле Cordless Telephony.

Применение стека протоколов позволяет сформировать модель использования набора протоколов, реализующих конкретный профиль, на базе которого сформировано приложение на основе Bluetooth. (рис 8.20)

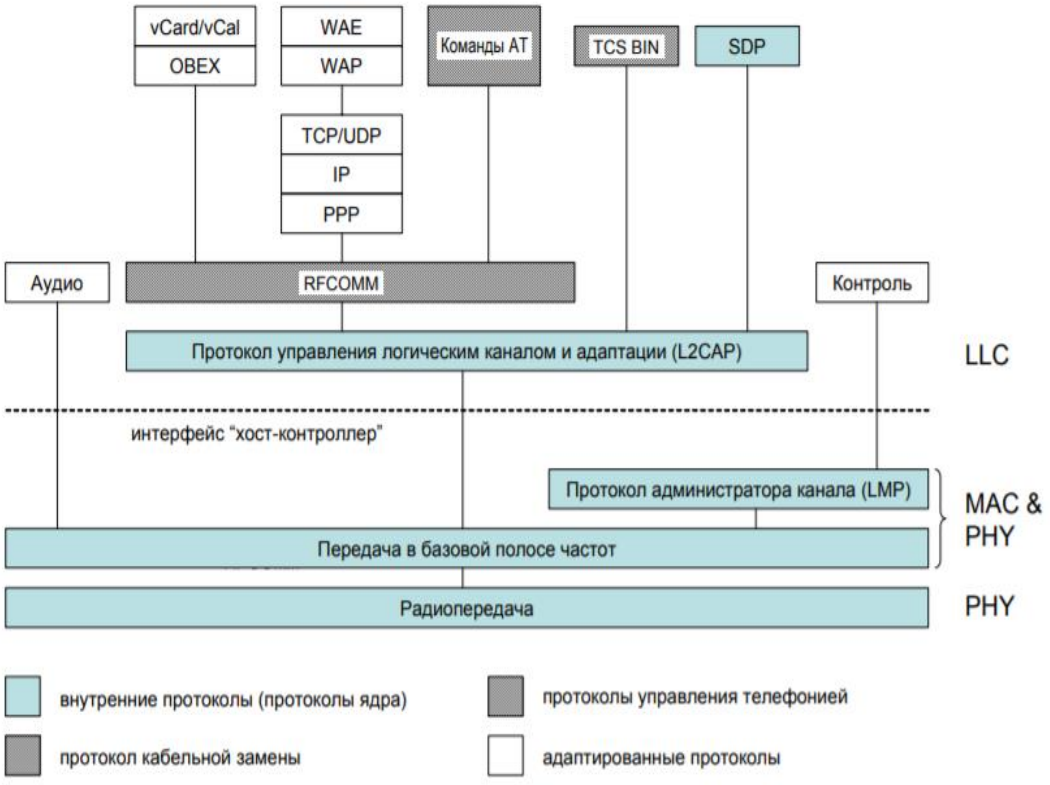

Рис. 8.20 [6]

Соединение. В пикосети реализован принцип централизованного управления. Ведущее устройство периодически инициирует опрос на разных частотах из заданного набора. Ведомые устройства находятся в режиме ожидания, включаясь по заданному режиму. После «пробуждения» приемник осуществляет поиск несущей частоты, периодически излучаемой ведущим устройством. Если сигнал обнаруживается, то ведомое устройство автоматически переходит из режима ожидания в рабочее состояние (рис 8.20).

Сопряжение ведущего и ведомого устройства завершается успешно, если излучаемые и принимаемые частоты совпадают, код доступа принят правильно и поступила квитанция. Лишь тогда вызывное устройство передает пакет, содержащий идентификационные параметры и текущий номинал генератора опорной частоты. На этом процедура вхождения в связь завершается.

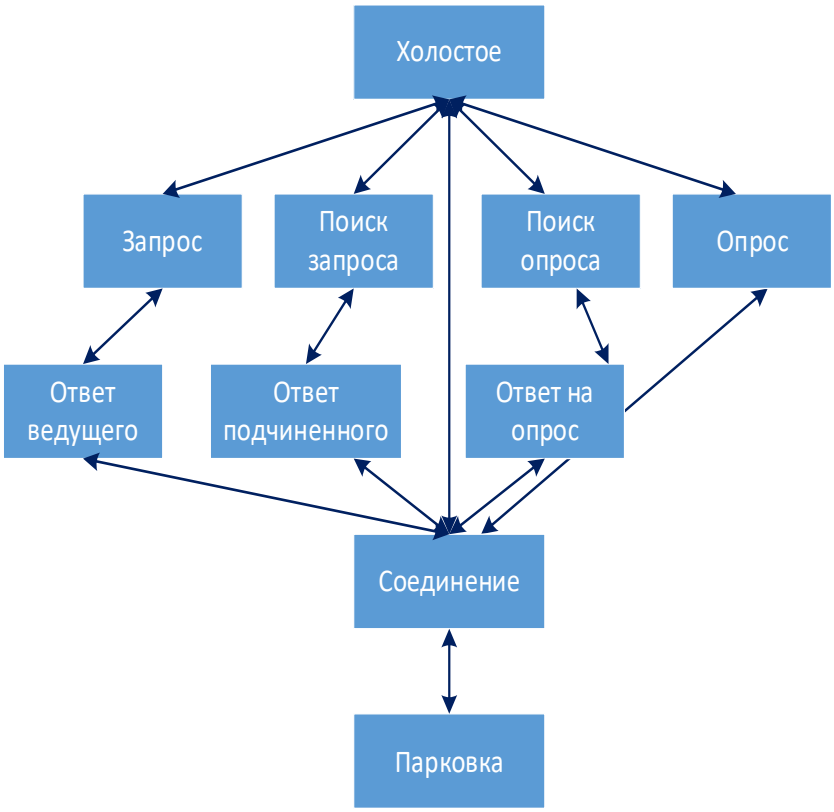

Рис. 8.21[6]

Основные состояния:

холостое состояние – низкое энергопотребление, работают только часы устройства

состояние соединения – устройство подключено к пикосети

состояние парковки – состояние подчинённого устройства, от которого не требуется участия в работе пикосети, но которое должно оставаться её частью

Промежуточные состояния:

опрос – определение устройством наличия других устройств в пределах его досягаемости

поиск опроса – ожидание устройством опроса

ответ на опрос – устройство, получившее опрос, отвечает на него

запрос – посылается одним устройством другому для установления с ним соединения (запрашивающее устройство становится ведущим, запрашиваемое – подчинённым)

поиск запроса – устройство ожидает запрос

ответ подчинённого устройства – подчинённое устройство отвечает на запрос ведущего

ответ ведущего устройства – ведущее устройство отвечает подчинённому после получения от него ответа на запрос

Обеспечение безопасности. Bluetooth может работать в одном из трех режимов безопасности.

Режим 1 - незащищенный (no security).

В этом режиме не работает ни шифрование, ни аутентификация, а само устройство работает в неразборчивом - широковещательном режиме (promiscuous).

Режим 2 - защищенный на уровне приложения/службы (application/service based (L2CAP)). В таком режиме после установки соединения менеджер безопасности (Security Manager) осуществляет аутентификацию, что позволяет ограничить доступ к устройству.

Режим 3 - защищенный на уровне канала связи (link-layer PIN authentification/ MAC address encryption).

Модель безопасности Bluetooth состоит из пяти этапов [8]:

1. Создание одного или нескольких общих секретных ключей в процессе сопряжения устройств.

2. Хранение ключей, созданных во время сопряжения, для использования в последующих соединениях и создания достоверной пары устройств.

3. Аутентификация устройства.

4. Шифрование данных.

5. Обеспечение целостности сообщений.

Основные характеристики, обеспечивающие защищенность Bluetooth представлены в табл. 8.4.

Таблица 8.3

Характеристика	*Bluetooth BR/EDR*		*Bluetooth Low Energy*	
	До версии 4.1	*Версия 4.1 и новее*	*До версии 4.1*	*Версия 4.1 и новее*
Физические радио каналы	79 каналов с шагом в 1 МГц		40 каналов с шагом в 2 МГц	
Обнаружение / соединение	Опрос (inquiry) / разбиение (paging)		Оповещение (advertising)	
Конфиденциальность адреса устройства	Отсутствует		Присутствует	
Максимальная скорость данных	1-3 Мбит/с		1 Мбит/с через GFSK-модуляцию	
Алгоритм сопряжения	До версии 2.1: E21/E22/SAFER+ Версия 2.1-4.0: Elliptic Curve P-192, HMAC-SHA-256	P-256 Elliptic Curve, HMAC-SHA-256	AES-128	P-256 Elliptic Curve, AES-CMAC
Алгоритм аутентификации устройства	E1/SAFER	HMAC-SHA-256	AES-CCM	
Алгоритм шифрования	E0/SAFER+	AES-CCM	AES-CCM	
Стандартный радиус действия	30 метров		50 метров	
Максимальная выходная мощность	100 мВ (20 дБ)		10 мВ (10 дБ) / 100 мВ (20 дБ)	

Список литературы

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
2. ГОСТ Р 59162-2020. Национальный стандарт Российской Федерации.
3. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей.
4. Варлатая С. К., Рогова О. С., Юрьев Д. Р. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником // Молодой ученый. — 2015. — №1. — С. 36-37.
5. Протоколы беспроводной передачи данных https://intuit.ru/studies/courses/1004/202/lecture/5250?page=3
6. Лекция 1. Обзор архитектуры Bluetooth Версия 2.0 + EDR https://wl.unn.ru/materials/courses/wlnet/Lect/6_Lect_1.pdf
7. Интернет-энциклопедия https://ru.wikipedia.org/wiki/Bluetooth
8. Эксплуатация достоверного Bluetooth-соединения https://www.securitylab.ru/analytics/495788.php