СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Интернет вещей

Фрагмент конспекта

СПбГЭТУ «ЛЭТИ», 2021 г.

3 БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

3.1 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.1).

Рис. 1

Каждая из технологий обладает определёнными характеристиками, которые определяют её область применения (Таблица 1).

Таблица 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 (Таблица 2), которые не требуют лицензирования.

Таблица 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 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. 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. 3).

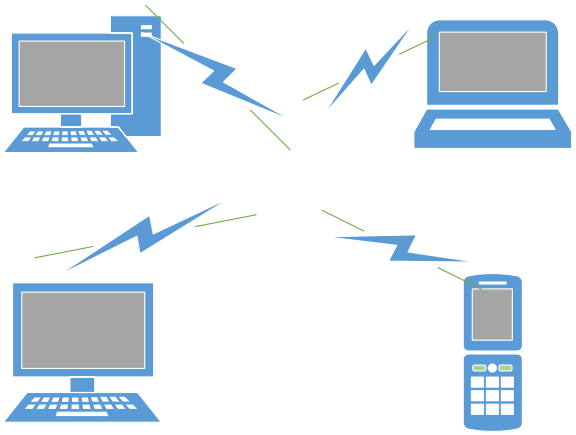

Рис. 3

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 (Рис. 4):

- 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.

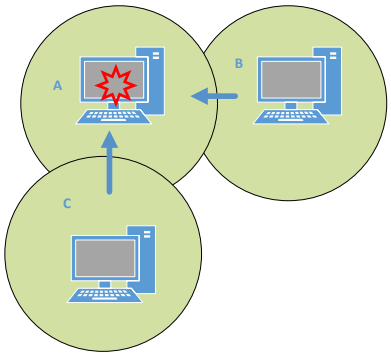

Рис. 4

- 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 5).

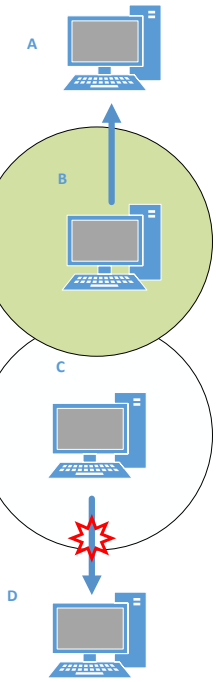

Рис. 5

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. 6)

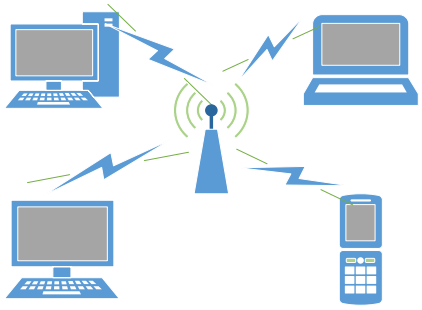

Рис. 6

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).

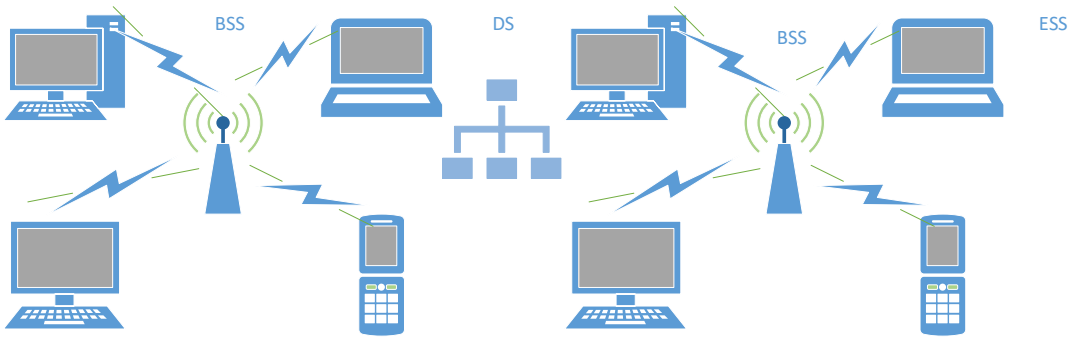

Рис. 7

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.

Режим DCF решение проблемы скрытой станции (Рис 8)**.**

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.

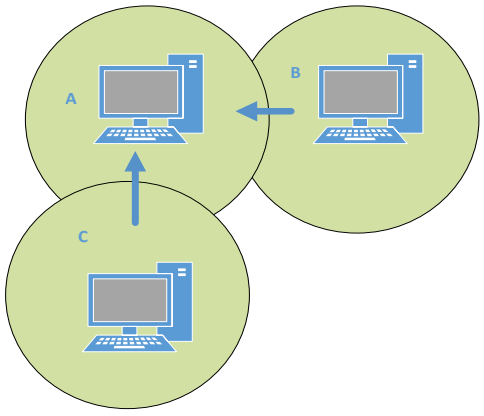

Рис. 8

3.2 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. 9.

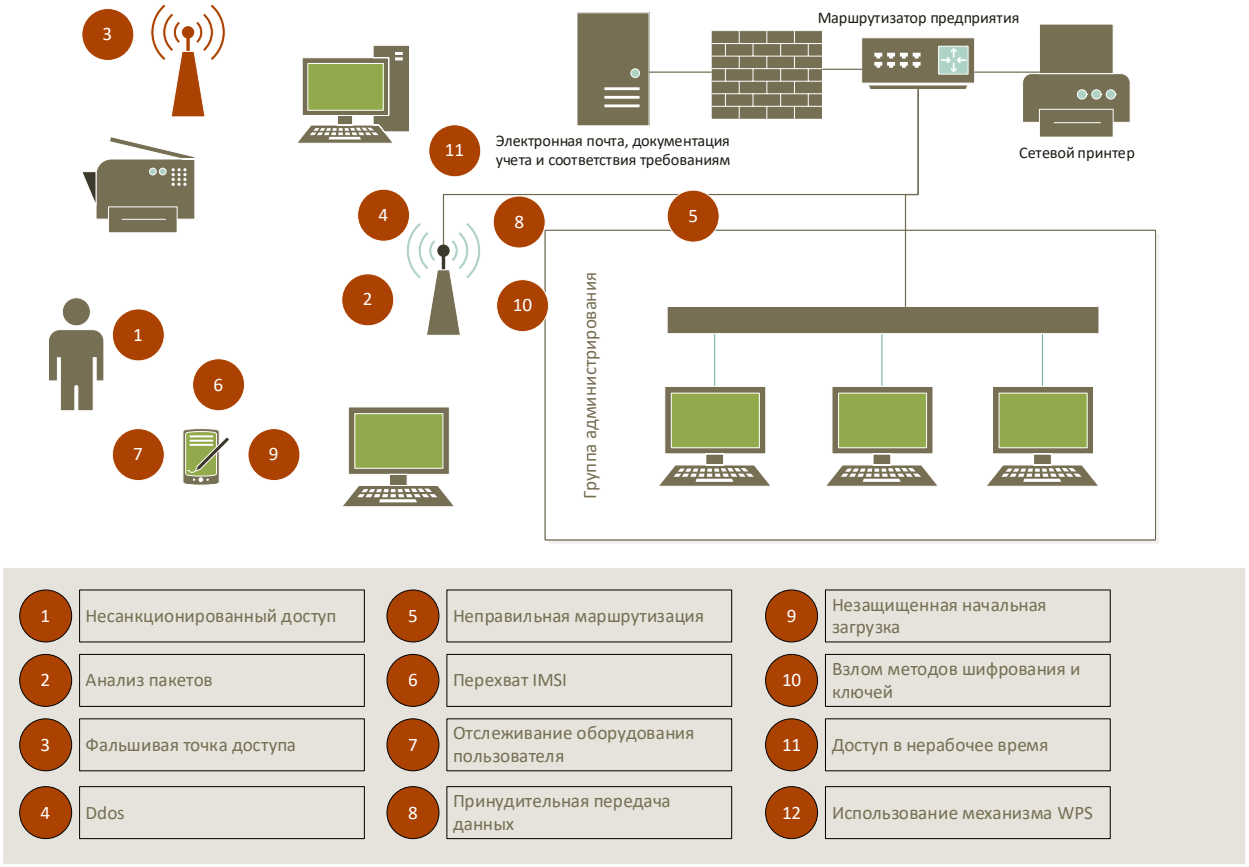

Рис. 9

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.

3.3 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.

К наиболее распространенные механизмы 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. 10).
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.

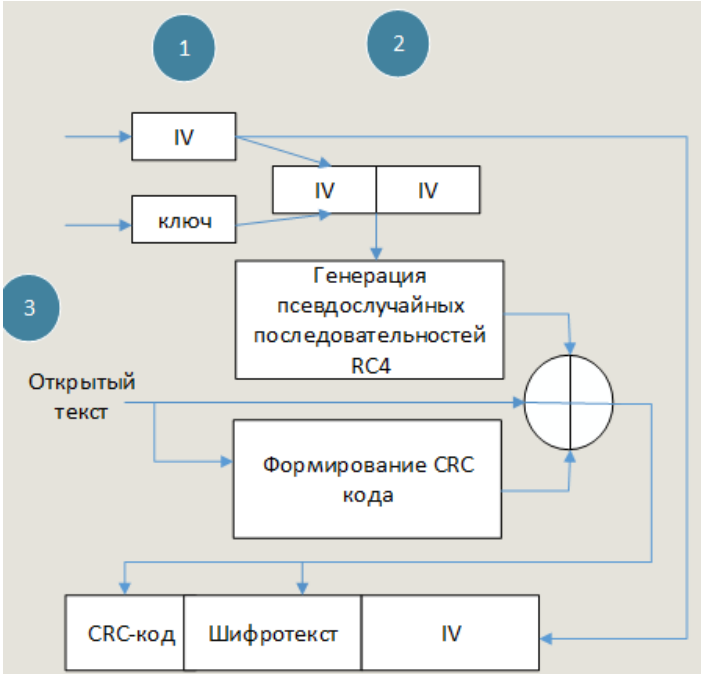

Рис. 20

Для расшифрования:

1. Получатель извлекает IV из заголовка пакета, добавляет его к своему секретному ключу и формирует ключ шифрования (Рис 11).
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.

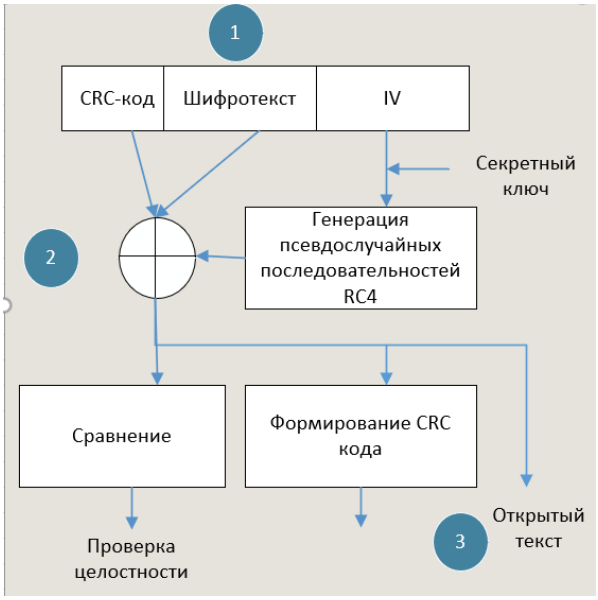

Рис. 31

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.

WPA может работать в двух режимах:

- 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.

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).

3.4 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. 12:

- 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.

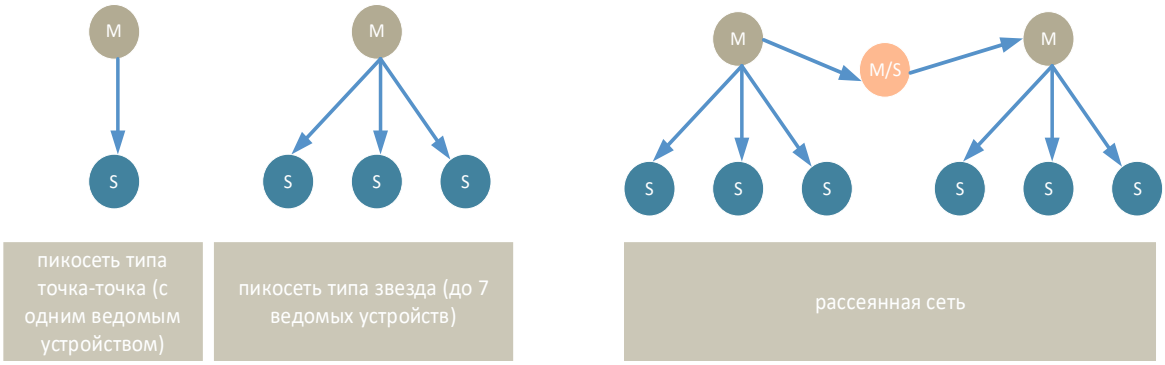

Рис. 12

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. 13)

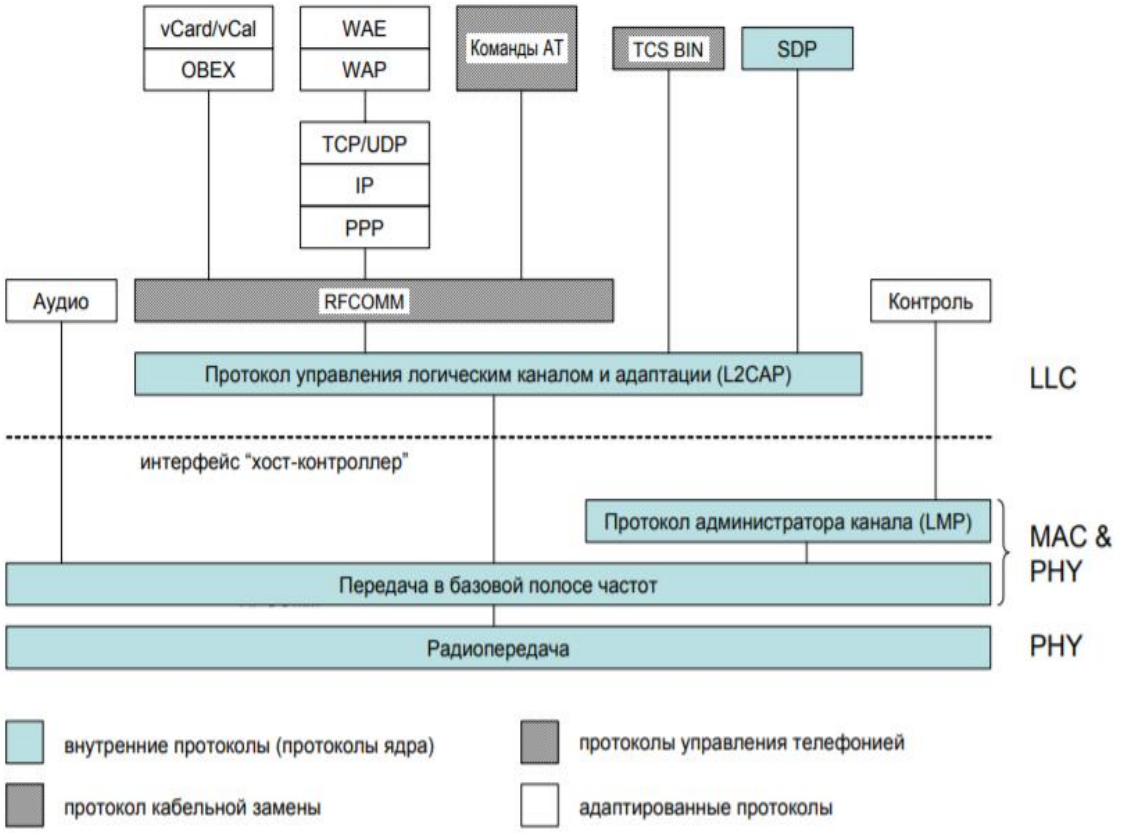

Рис. 43 [6]

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 14).

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.

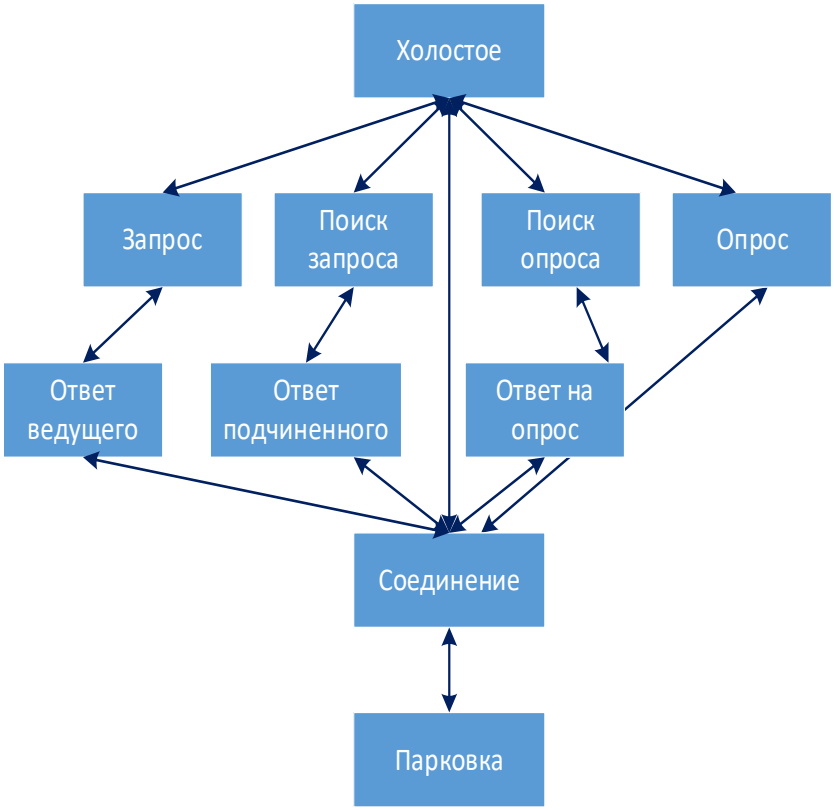

Рис. 54

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.

3.5 Стек протокола TCP/IP

Основу транспортных средств стека TCP/IP составляют протоколы межсетевого и транспортного уровней, определяющие маршрут, передачу данных от отправителя к получателю, а также, гарантируют надежность доставки пакетов. Прикладной уровень стека поддерживает интерфейс с пользователем и приложением, а уровень сетевых интерфейсов — интерфейс с технологиями составляющих сетей (Рис.15).

Назначение протокола IP — протокола межсетевого взаимодействия (Internet Protocol, IP) —передача пакетов между сетями. Протокол IP относится к протоколам без установления соединения и обрабатывает каждый пакет как независимую единицу, не имеющую связи с другими пакетами.

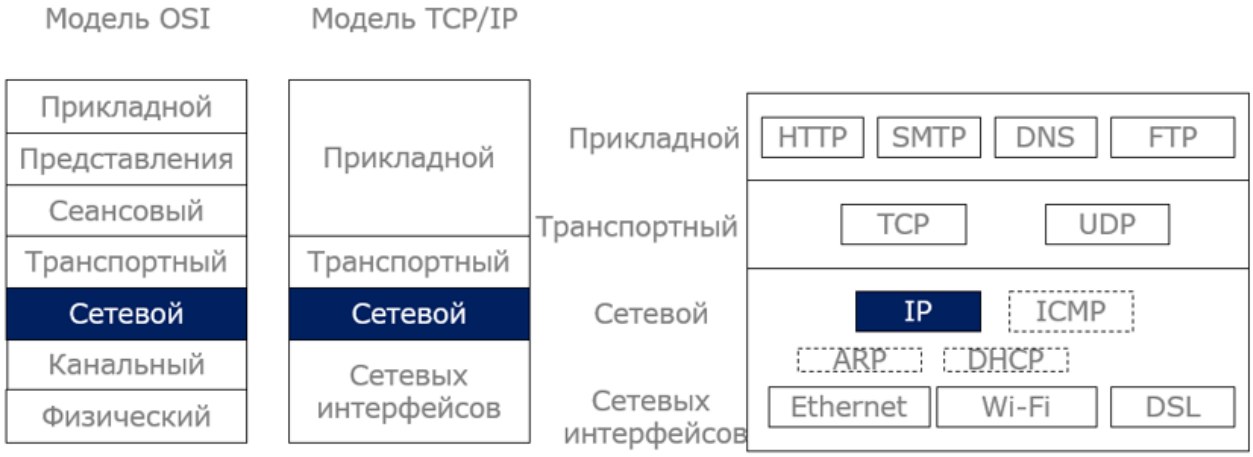

Рис. 65

Единицей данных, передаваемых по протоколу IP, является дейтограмма, состоящая из заголовка и поля данных. Наибольший интерес представляет заголовок дейтограммы, длинной 20 байт (Рис. 16).

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина
16 бит Идентификатор пакета		3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни	8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя			
32 бита IP-адрес получателя			
Опции и выравнивание (не обязательно)			

Рис. 76

- К функциям IP- протокола относят:
- передач пакетов по сети;
- динамическую фрагментацию пакетов при передаче между сетями с различными значениями поля данных кадров;
- перенос между сетями различных типов адресной информации в унифицированной форме.

В стеке протоколов TCP/IP протокол TCP (Transmission Control Protocol) работает на транспортном уровне, обеспечивая надежную транспортировку данных между прикладными процессами путем установления логического соединения.

Единицей данных протокола TCP является сегмент. Информация, поступающая к протоколу TCP в рамках логического соединения от протоколов более высокого уровня, рассматривается протоколом TCP как неструктурированный поток байт. Поступающие данные буферизуются средствами TCP. Для передачи на сетевой уровень из буфера "вырезается" некоторая непрерывная часть данных, называемая сегментом, состоящая из заголовка и блока данных. Заголовок сегмента имеет следующие поля, представленные на Рис 17. Все поля заголовка можно использовать для различного вида атак.

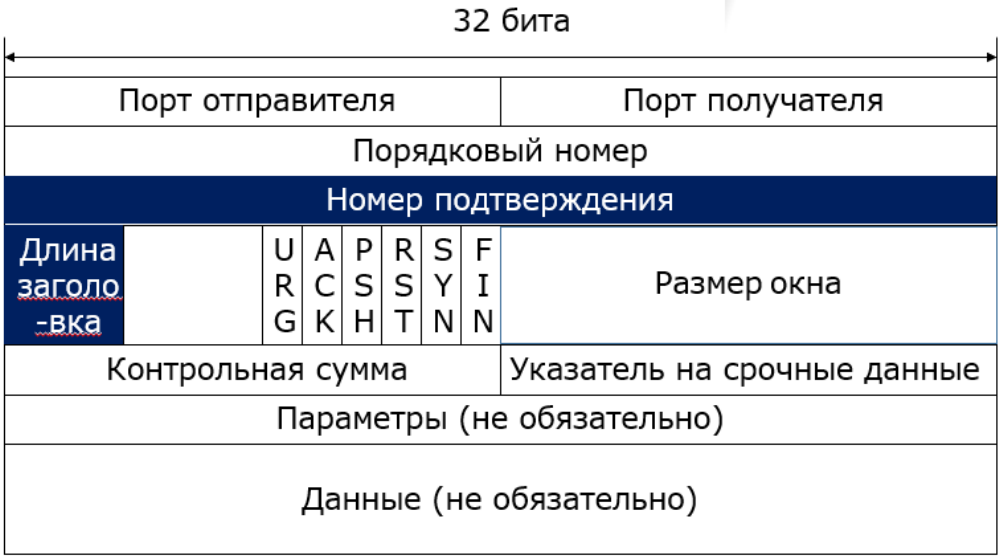

Рис. 87

К функциям TCP относят:

получение и передача потока данных от вышестоящего уровня IP-модулю;

- обеспечение полнодуплексной передачи данных;
- обеспечение защиты от повреждения, потери, дублирования;
- обеспечение работы нескольких соединений;
- управление потоком данных (с помощью механизмов перегрузки окна).

Для организации надежной передачи данных предусматривается установление логического соединения между двумя прикладными процессами. В рамках соединения осуществляется обязательное подтверждение правильности приема для всех переданных сообщений, и при необходимости выполняется повторная передача. Соединение в TCP позволяет вести передачу данных одновременно в обе стороны, то есть полнодуплексную передачу.

Соединение в протоколе TCP идентифицируется парой полных адресов обоих взаимодействующих процессов, включающих IP-адрес (номер сети и номер компьютера) и номер порта. Портам присваиваются стандартные,

зарезервированные номера (например, номер 21 закреплен за сервисом FTP, 23 - за TELNET), или произвольно выбранными локальными номерами.

Установление соединения выполняется в следующей последовательности (Рис. 18):

1. Узел А в сообщении TCP, посылаемому узлу В устанавливает флаг SYN и начальный порядковый номер ISN с которого будут нумероваться отправляемые данные.

Рис. 98

2. Для подтверждения приема сообщения, узел В откликается посылкой TCP сегмента с установленным флагом ACK. Но вследствие того, что протокол TCP обеспечивает полнодуплексную передачу, узел В может в свою очередь запросить соединение на передачу данных с узлом А посылкой флага SYN и начального порядкового номера своих сообщений ISN.
3. Узел А, подтверждает получение сообщение от узла В. Так как сеанс связи можно считать установившимся, то узел А может включить свои данные, нумерация которых начинается с ISN (A)+1 в это сообщения.
4. Происходит передача данных между узлами А и В.

5. Сеанс обмена данными заканчивается процедурой закрытия, которая в заголовке последнего сегмента использует флаг FIN. Аварийный разрыв соединения происходит посылкой сообщение с битом RST, при этом все недопоставленные данные уничтожаются.

В рамках соединения правильность передачи каждого сегмента должна подтверждаться квитанцией получателя. Квитирование - один из традиционных методов обеспечения надежной связи. Идея квитирования состоит в следующем.

Для организации повторной передачи искаженных данных отправитель нумерует отправляемые кадры и ожидает от приемника *положительную квитанцию* - служебное сообщение, извещающее о том, что исходный кадр был получен и данные в нем оказались корректными. Существуют два подхода к организации процесса обмена квитанциями: с простоями и с организацией "окна".

Метод с простоями требует, чтобы узел, посылал очередной кадр, после получения квитанции (положительной или отрицательной) от получателя. Производительность обмена данными в этом методе незначительна, так как передающий узел и мог бы послать следующий кадр сразу же после отправки предыдущего, однако он обязан ждать прихода квитанции, что особенно заметно на низкоскоростных каналах связи, то есть в территориальных сетях.

В *методе с организацией "окна"* отправителю разрешается передать некоторое количество кадров в непрерывном режиме, без получения на эти кадры ответных квитанций. Количество кадров, которые возможно передать таким образом, называется размером окна W. При отправке кадра с номером 1 отправителю разрешается передать еще (W-1) кадров до получения квитанции на первый кадр. Если квитанция на кадр 1 не получена, то процесс передачи приостанавливается, и по истечению некоторого тайм-аута кадр 1 считается утерянным и передача его осуществляется снова. Выбор времени

ожидания (тайм-аута) очередной квитанции является важной задачей, при которой необходимо учитывать скорость и надежность линий связи, их протяженность и т.д. В протоколе TCP при каждой передаче засекается время от момента отправки сегмента до прихода квитанции о его приеме. Получаемые значения усредняются с весовыми коэффициентами, возрастающими от предыдущего замера к последующему. В качестве тайм-аута выбирается среднее время оборота, умноженное на некоторый коэффициент.

Описанный алгоритм называется *алгоритмом скользящего окна* (при каждом получении квитанции окно перемещается (скользит), захватывая новые данные, которые разрешается передавать без подтверждения).

В протоколе TCP квитанцией (ASK SN) подтверждается правильный прием данных, отсутствие квитанции говорит о приеме искаженного сегмента, потере сегмента или квитанции. В качестве квитанции получатель отсылает сообщение (сегмент), в которое помещает число, на единицу превышающее максимальный номер байта в полученном сегменте. Если размер окна равен W, а последняя квитанция содержала значение n, то отправитель может посылать новые сегменты до тех пор, пока в очередной сегмент не попадет байт с номером n+W. Этот сегмент выходит за рамки окна, и передачу в таком случае необходимо приостановить до прихода следующей квитанции.

Изменяя величину окна, возможно, повлиять на загрузку сети. Чем больше окно, тем большую порцию неподтвержденных данных можно послать в сеть. Если сеть не справляется с нагрузкой, то протокол TCP, отправляя квитанцию, помещает в нее новый, уменьшенный размер окна. Если узел совсем отказывается от приема, то в квитанции указывается окно нулевого размера. После приема квитанции с нулевым значением окна отправитель время от времени делает контрольные попытки продолжить обмен данными. Если протокол-приемник уже готов принимать информацию, то в ответ на контрольный запрос он посылает квитанцию с указанием ненулевого размера окна.

3.6 Безопасность протокола TCP/IP

Основным недостатком протокола TCP/IP является отсутствие встроенных функций защиты, криптографического закрытия пакетов сообщений, контроля подлинности, а также аутентификация участников обмена. Поэтому пакеты сообщений доступны для анализа и модификации.

В случае пассивных атак на протоколы TCP/IP, возникает трудность обнаружения нарушителя, все несанкционированные действия которого сводятся к наблюдению за циркулирующими в сети пакетами. При активных атаках на TCP/IP нарушитель модифицирует и/или фильтрует содержимое пакетов сообщений для обмана получателя или нарушения работоспособности принимающего узла.

- Действия нарушителя, направленные против какого-либо узла или сети, и содержат:
- несанкционированное подключение и прослушивание сети, с последующим анализом потока информации;
- прерывание передачи сообщений;
- перехват, модификация данных, передаваемых через сеть;
- выдача себя за другой узел, для использования его привилегий;
- несанкционированная передача данных (обход правил фильтрации IP трафика в сетях);
- отказ в обслуживании- приведение узла в состояние, когда он не может нормально функционировать, принимать и передавать данные.

3.7 Протокол HTTP

HTTP-прикладной клиент-серверный протокол, работающий поверх TCP, без сохранения состояния. То есть запрос от клиента является абсолютно самостоятельной единицей, не связанной ни с запросами этого или других клиентов. Рассмотрим стандартный запрос клиента к серверу:

Передача и прием запроса от клиента к серверу (Рис.19):

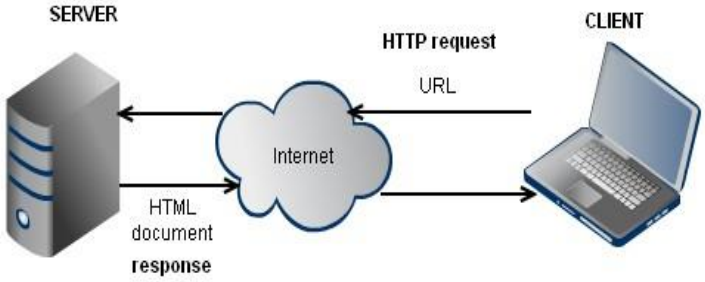

Рис. 109

1. Разбор URI, определение имени запрошенного файла, виртуальный путь преобразуется в реальный.
2. Разбор заголовков HTTP-запроса.
3. Осуществление контроля доступа путем анализа параметров запроса, которые могут применяться с дополнительными модулями:

-аутентификация – установление пользователя, от чьего имени HTTP-браузер произвел запрос;

-авторизация— определение, имеет ли право пользователь, прошедший аутентификацию производить данный запрос

4. Определение типа запрашиваемого документа (файл, подлежащий просмотру, CGI-программа, файл с директивами SSI, файл со встроенным кодом и т., а также язык документа, кодировка символов).
5. Генерация ответа. На этой стадии извлекаются или генерируются в результате работы программы файлы или процедуры-обработчика. Формируемый HTTP-ответ возвращается клиенту. Если запрос не может быть обслужен, сервер возвращает клиенту ответ с кодом ошибки.
6. Протоколирование. На этой стадии в журналы аудита заносятся записи об обслуживании запроса.
7. Освобождение ресурсов: памяти и файлов и т. п.

В процессе TCP соединения сервер и клиент обмениваются запросами-HTTP- сообщениями, состоящими из текстовых заголовков, пустой строкой, отделяемой данные от заголовка и собственно данных.

Проблемы безопасности, связанные с использованием HTTP, можно разделить на группы:

- проблемы, связанные с передачей данных;
- уязвимости клиентских приложений;
- уязвимости серверного программного обеспечения:
- уязвимости серверов (Apache, nginx);
- уязвимости в серверных сценариях.

Для защиты информации и уменьшения риска указанных атак используют расширение протокола HTTP с использованием криптографического закрытия данных. HTTPS обеспечивает защиту от атак, основанных на прослушивании, при условии, что сертификат сервера проверен и используется шифрование.

- В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.
- Для организации сеанса HTTPS используются серверные сертификаты и, редко, клиентские сертификаты, которые позволяют реализовать взаимную аутентификацию.

Протокол HTTPS позволяет осуществлять идентификацию как сервера, так и клиента.

Идентификация сервера

1. После установления соединение, сервер посылает клиенту свой сертификат, чтобы клиент идентифицировал его. Это позволяет предотвратить атаку посредника. В сертификате указывается URI сервера.
2. Если имя сервера не совпадает с указанным в сертификате, то пользовательские программы, например браузеры, сообщают об этом

пользователю. В основном, браузеры предоставляют пользователю выбор: продолжить незащищённое соединение или прервать его.

Идентификация клиента

Обычно сервер не располагает информацией о клиенте, достаточной для его идентификации. Однако для обеспечения повышенной защищённости соединения используется так называемая двухсторонняя аутентификация. При этом сервер после подтверждения его сертификата клиентом также запрашивает сертификат. Таким образом, схема подтверждения клиента аналогична идентификации сервера.

3.9 Обеспечение защиты за счет межсетевого экранирования

Межсетевой экран (брандмауэр или firewall, МСЭ)- специализированный комплекс защиты, позволяющий разделить среду передачи на 2 и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными из одной части в другую.

Первоначально термин МСЭ описывал аппаратное устройство, которое блокировало нежелательный трафик и пропуская полезный. Затем появились высоконадежные программные средства, которые относительно просто инсталлируются и эффективно используются.

Первые МСЭ появились в начале 90гг. и представляли собой программные или программно-аппаратные устройства, осуществляющие IP-маршрутизации с установленными правилами фильтрации. Недостаток этих МСЭ заключался в том, что трудно было сформулировать приемлемые правила фильтрации и ограничивать сервисы прикладного уровня (Telnet, FTP, SMTP). В 1994 году компания Check Point ввела графический интерфейс конфигурирования и управления. В 1996 г. Вышел межсетевой экран для ОС Windows NT, с помощью которого администраторы могли сконфигурировать надежную защиту без знания UNIX.

К основным функциям межсетевого экрана можно отнести:

- ограничение доступа внешних пользователей к серверам защищаемым межсетевым экраном;

- разграничение доступа внутренних пользователей к внешним ресурсам;
- фильтрация трафика;
- сигнализация и аудит.

Современные МСЭ обеспечивают высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP и характеризуются прозрачностью для пользователей, большим быстродействием и высокой эффективностью.

Основной тенденцией развития средств сетевой защиты является интеграция, в частности, межсетевых экранов с криптографическими и антивирусными средствами, а также средствами анализа уровня обеспечения безопасности.

Классификация межсетевых экранов По уровням протоколов:

- пакетный фильтр (экранирующий маршрутизатор-screening router);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз (application gateway);
- шлюз экспертного уровня (stateful inspection), инспектор состояний.

По исполнению:

- аппаратный (в виде специализированного устройства, достоинством данного исполнения является простота ввода в эксплуатацию, за счет наличия типовых шаблонов настройки, а к недостаткам можно отнести меньшую по сравнению с программными аналогами масштабируемость и трудность обеспечения взаимодействия с программными продуктами сторонних фирм);

- программно-аппаратный (в виде модуля к маршрутизатору или коммутатору, или специально выделенного сервера).

- программный (в виде программного приложения или усеченной ОС, недостатком программного исполнение, является потребления ресурсов, а также уязвимость самих ОС).

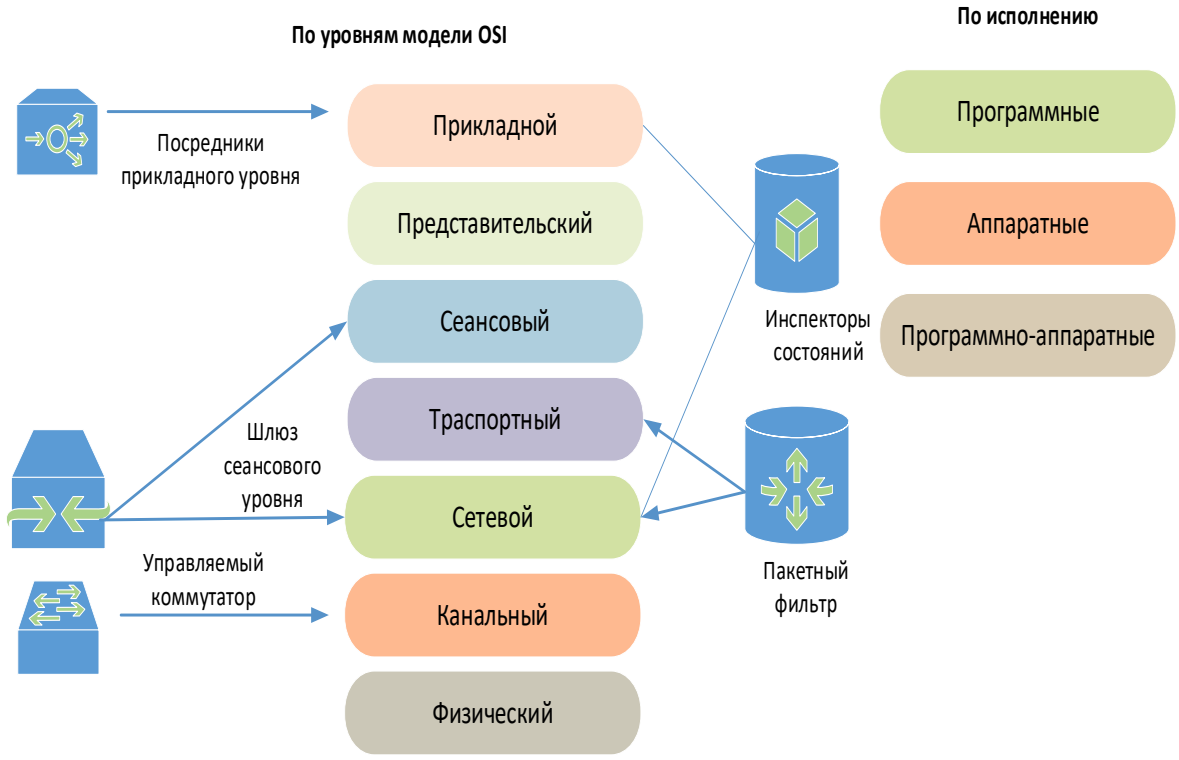

Рис. 119

Пакетные фильтры. Пакетный фильтр- маршрутизатор, обрабатывающий пакеты (сетей TCP/IP и IPX/SPX) на основании информации, содержащейся в заголовках пакетов, для этого:

- используется статическая фильтрация (заданная администратором для каждого уникального типа пакета, требующего обработки).
- для многоканальных соединений требуется учитывать дуплексность соединений.

Технология реализована в пограничных маршрутизаторах, операционных системах, персональные межсетевые экраны. МСЭ предназначен для фильтрации трафика, на основе набора предварительно загруженных в экран правил, соответствующих политике безопасности. Для описания правил прохождения пакетов составляются правила фильтрации с основными параметрами (Рис. 20).

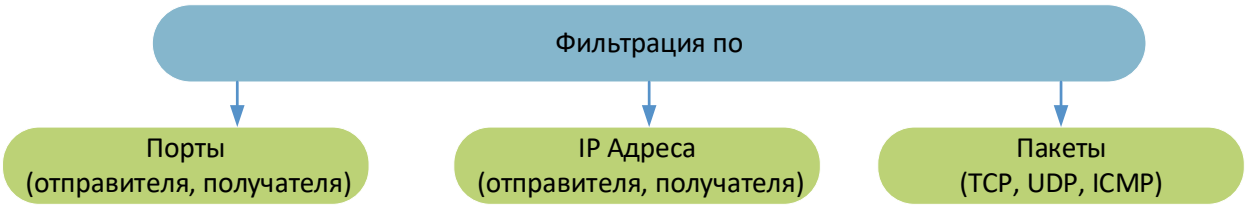

Рис. 20

При этом сетевой трафик может проходит не через один фильтр, а через ряд фильтров, следующих друг за другом. Для этого анализируются заголовки IP, TCP и UDP пакетов (адрес получателя, отправителя, порт и др.) и осуществляется поиск правилах фильтрации, с которым согласуются все проверяемые поля

Пакетные фильтры реализованы как аппаратно (может быть использован обычный маршрутизатор) так и в виде программного обеспечения установленного на сервере.

Достоинства: простота реализации, высокая производительность, прозрачность для программных приложений, малая цена.

Недостатки:

- проверяя только заголовки пакетов, пакетный фильтр не обеспечивает ряд важных функций (аутентификация, проверка подлинности, целостности и др.). Отсутствует возможность анализа пакетов прикладного уровня;
- отсутствует защита от подмены адреса;
- сложность настройки и администрирования;
- при увеличении числа правил возможно снижение производительности;
- требуется детальное знание сетевых услуг и протоколов;
- нет контроля состояния соединения;
- трудность функционирования в сетях с динамическим распределением адресов.

Шлюзы сеансового уровня. К функциям шлюза сеансового уровня относят:

1. динамическую фильтрацию в сетевых фильтрах;
2. фильтрацию фрагментированных пакетов;
3. трансляция IP- адресов.

Рассмотрим процедуру фильтрации фрагментированных пакетов, с функцией защиты от Ddos атак, которая состоит из следующих этапов (Рис 21):

1. МСЭ получает пакет SYN от компьютера А.
2. МСЭ передает полученный пакет на сервер В.
3. Сервер В передает пакет SYN/ACK на компьютер А, но МСЭ его перехватывает.
4. МСЭ пересылает полученный пакет на компьютер А, кроме того, МСЭ от имени компьютера А посылает пакет ACK на сервер В
5. Если же МСЭ не получит пакета ACK или кончится тайм-аут на установление соединения, то он вышлет в адрес сервера В пакет RST, отменяющий соединение.

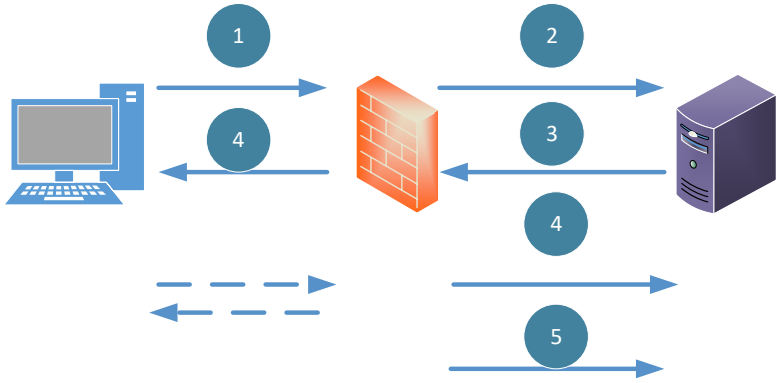

Рис. 21

Экранирующий транспорт осуществляет контроль виртуальных соединений и трансляцию IP-адресов при взаимодействии с внешней средой.

Для установки виртуального соединения принимая запрос от рабочей станции на связь с внешней сетью, шлюз (Рис 22):

1. Проверяет, удовлетворяет ли он базовым критериям фильтрации.
2. Если условия фильтрации приемлемы, то шлюз от имени рабочей станции отправляет пакет, помеченный флагом SYN (запрос на соединение) и ISN (начальный порядковый номер) компьютеру внешней среды.
3. Компьютер- получатель откликается посылкой пакета с установленным флагом ASK, подтверждающем прием пакета, а также флагами SYN, ISN, обозначающих возможность передачи данных к шлюзу.

4. Шлюз в свою очередь подтверждает запрос на соединение отсылкой пакета с установленным флагом ASK и номером очередного пакета ISN.

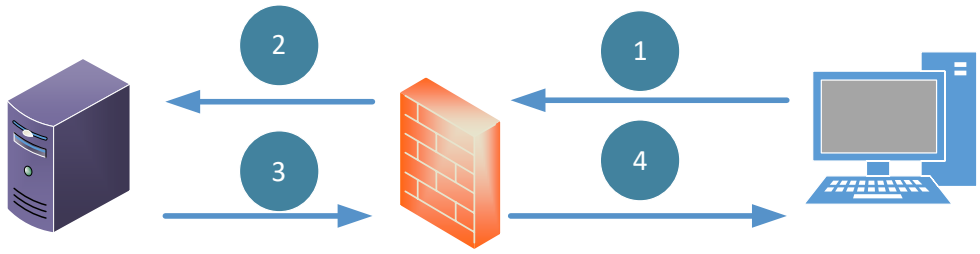

Рис. 22

5. Для передачи данных между рабочей станцией и компьютером внешней среды шлюз помещает в специальную таблицу данные о соединении (адрес получателя, отправителя, состояния соединения и т.д.), на основании которых шлюз передает пакеты из внешней среды рабочей станции (Таблица 3).

Таблица 3

Внутренний IP	*Внутренний порт*	*Внешний IP*	*Внешний порт*
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

В случае закрытия сессии шлюз удаляет соответствующую строку из таблицы и разрывает цепь, использовавшуюся в данном соединении.

Преимущества:

- Позволяет преодолеть нехватку адресов IPv4 и осуществить сокрытие внутренней структуры сети.
- Применение технологии позволяет динамически задавать правила фильтрации трафика.
- Учет, ограничение и разграничение работы пользователей с ресурсами с помощью механизмов аутентификации, а также механизм трансляции внутренних адресов позволяют ограничить доступ к информации как внутренних, так и внешних пользователей.

Недостатки:

- Отсутствие единого стандарта NAT.
- Отсутствие возможности проверки содержания поля данных.
- Невозможность регулирования передачи информации на прикладном уровне.
- Использование ненадежной системы идентификации и аутентификации, основанную на IP-адресах отправителя/получателя.

Посредники прикладного уровня. К функция прикладного шлюза относят:

-установку виртуального соединения между рабочей станцией и внешней сетью;

-проверку подлинности передаваемых данных (контроль цифровых подписей);

-фильтрацию (по названию сервиса, допустимому временному диапазону, ограничению на содержимое сообщений);

-преобразование потока сообщений (например, прозрачное шифрование);

-разграничение доступа к внешней/внутренней средам (аутентификация и идентификация при обращении к межсетевому экрану, разрешение доступа только заданным адресам, блокировка поиска информации по нежелательным ключевым словам ит.д.);

-кэширование данных, запрашиваемых из внешней среды;

-администрирование, регистрация событий и генерация отчетов.

Прикладной шлюз осуществляет контроль виртуальных соединений, однако в отличие от шлюза сеансового уровня, для каждого прикладного протокола TCP/IP функционируют свои программы посредники (например, для протокола FTP- посредник FTP, который пропускает только ftp-пакеты).

- Достоинства:
- Анализ на прикладном ровне и возможность реализации дополнительных механизмов защиты (например, анализ содержимого).
- Исключение прямого взаимодействия между двумя узлами.

- Высокий уровень защищенности.
- Контроль состояния соединения. Осуществляя фильтрацию пакетов на прикладном уровне, то есть производя проверку содержимого пакета, обеспечивают высокий уровень защиты внутренней среды.
- Недостатки:
- высокая стоимость;
- большие затраты времени и ресурсов на анализ каждого пакета
- невозможность автоматического подключения поддержки новых сетевых приложений и протоколов, так как для каждого из них необходим свой агент.

Инспекторы состояния. Термин «инспектор состояния» был введен компанией Check Point. Осуществляют фильтрацию пакетов с контролем состояния соединения, сочетая в себе элементы экранирующих маршрутизаторов и прикладных шлюзов. На сетевом и транспортном уровнях обеспечивают фильтрацию пакетов по содержимому их заголовков, на прикладном уровне осуществляют фильтрацию пакетов в соответствии с заданной политикой безопасности. Инспекторы состояния оперируют на трех уровнях: прикладном, сеансовом и сетевом и позволяют контролировать:

- каждое приложение— на основе разработанных посредников;
- каждую сессию — на основе таблицы состояний;
- каждый передаваемый пакет — на основе таблицы правил.

При получении пакета данных содержимое этого пакета сравнивается с некими шаблонами, специфическими для соответствующего протокола прикладного уровня. Осуществляется выполнение следующих действий:

- пропуск пакета;
- удаление пакета и сессии;
- регистрация пакета и сессии и передача на механизмы фильтрации.
- Преимущества механизма управления сессиями:

- контроль хода TCP-соединения. Автоматическое открытие клиентских портов, необходимых для текущего соединения;
- контроль данных прикладных протоколов;
- блокировка атак, связанных с некорректной установкой флагов TCP;

Основные параметры сессии, хранящаяся в таблице сессий:

- интерфейсы, MAC-, IP-адреса и порты взаимодействующих сторон;
- номера родительской и дочерней сессий;
- текущее состояние сессии;
- протокол транспортного и прикладного уровней4
- информация о контексте прикладного протокола;
- номера TCP-последовательностей для последнего принятого пакета;
- имя пользователя, которому принадлежит данная сессия;
- время начала, время последней активности и значение таймаута неактивности сессии;
- количество пакетов и байт, прошедших от клиента к серверу и обратно;
- параметры подсчета интенсивности пакетов в сессии;
- номер порта трансляции при использовании режима NAT.

Преимущества:

- Прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения.
- Высокая скорость обработки информационных потоков.
- Не изменяют IP-адресов проходящих через них пакетов (любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программами).

К недостаткам можно отнести прямое соединение между авторизованным клиентом и компьютером внешней сети.

Демилитаризованная зона (DMZ - Demilitarized Zone) - сеть, которая добавляется между защищенной сетью и сетью, которая имеет меньший уровень безопасности, для создания дополнительного уровня безопасности.

В зависимости от условий функционирования, а также количества сетевых интерфейсов межсетевых экранов существуют различные схемы подключения к внешней сети:

- схема единой защиты локальной сети (Без выделения DMZ);
- схема с одной DMZ (с защищаемой закрытой и не защищаемой открытой подсетями);
- схема с Service-log DMZ (с раздельной защитой закрытой и открытой подсетей для одного МЭ с 3 сетевыми интерфейсами);
- схема с двумя DMZ (с раздельной защитой закрытой и открытой подсетей для двух МЭ с двумя сетевыми интерфейсами).

Межсетевые экраны с одним сетевым интерфейсом недостаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а соответственно не могут обеспечивать надежную защиту межсетевых взаимодействий. В связи с этим рационально рассмотреть схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами:

- единая защита локальной сети;
- с защищаемой закрытой и не защищаемой открытой подсетями;
- с раздельной защитой закрытой и открытой подсетей.

Недостатки межсетевых экранов. К общим недостаткам межсетевых экранов можно отнести сложность администрирования. К наиболее частым атакам и уязвимостям, которым подвергаются межсетевые экраны целесообразно отнести (Рис. 23):

1. Обход защиты межсетевого экранирования. Межсетевые экраны не могут защитить ресурсы внутренней сети в случае неконтролируемого

использования в ней модемов. Доступ в сеть через модем по протоколам SLIP или PPP в обход межсетевого экрана делает сеть практически незащищенной. Поэтому необходимо контролировать все имеющиеся в сети точки удаленного доступа. Для этих целей возможно применение как организационных, так и технических мер.

Рис. 23

2. Использование злоумышленником или персоналом разрешенных портов. Правила предусматривают соответствующую проверку с целью определения того, разрешен или нет конкретный протокол (например, если открыты порты 25 и 80, то тем самым разрешается пропуск во внутреннюю сеть почтового (SMTP) и Web (HTTP) трафика). Вся несанкционированная деятельность осуществляется в рамках разрешенного протокола, создавая тем самым в нем туннель, по которому злоумышленник и реализует атаку. Самый простой пример, применения туннелей - Internet-черви и макровирусы, заносимые в корпоративную сеть в виде вложений.

3. Наиболее очевидный недостаток межсетевых экранов - невозможность защиты от авторизованных пользователей, выполняющих несанкционированные действия. Для устранения этого недостатка возможно использование систем обнаружения атак (intrusion detection systems). Данные средства, обнаруживают и блокируют несанкционированную деятельность в сети независимо от того, кто ее реализует - авторизованный пользователь (в т.ч. и администратор) или злоумышленник. Такие средства могут работать как самостоятельно, так и совместно с межсетевым экраном. Например, система RealSecure обладает возможностью автоматической реконфигурации межсетевого экрана CheckPoint Firewall-1 путем изменения правил, запрещая тем самым доступ к ресурсам корпоративной сети с атакуемого узла.

4. Отсутствие встроенных механизмов защиты от вирусов, апплетов и др.

5. Подмена IP адреса.

6. Подбор пароля.

7. Отсутствие защиты новых сетевых сервисов. Межсетевые экраны разграничивают доступ по широко распространенным протоколам, таким как HTTP, Telnet, SMTP, FTP и ряд других. При появлении нового протокола или сервиса встает вопрос о создании нового посредника.

Для эффективной защиты межсетевого взаимодействия необходимо использовать все возможные методы– пакетная фильтрация, технология посредничества, а также фильтрация экспертного уровня. Использование одной из перечисленных технологий по отдельности приводит к специфическим недостаткам межсетевых экранов:

пакетная фильтрация, основанная на анализе служебных полей IP, ICMP, UDP и TCP-пакетов уязвима из-за возможности подмены IP-адресов.

- Программы-посредники без использования пакетных фильтров подвержены атакам «отказ в обслуживании», а без фильтрации экспертного уровня характеризуются более высокими затратами компьютерных ресурсов.
- Фильтрация экспертного уровня, без использования программ-посредников не обеспечивает аутентификацию взаимодействующих сторон, трансляцию сетевых адресов и ряд других важных функций

защиты, например криптографическое преобразование трафика и антивирусную защиту.

Поэтому межсетевые экраны, поддерживающие все ранее перечисленные методы защиты, обеспечивают наиболее высокую безопасность корпоративной сети при ее подключении к Internet.

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