МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
Институт «Высшая школа электроники и компьютерных наук»
Кафедра «Информационно-аналитическое обеспечение управления в социально-экономических системах»

РАБОТА ПРОВЕРЕНА
Рецензент

_____/_____/
«____» _____2017 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
д.т.н., профессор
_____/О.В. Логиновский /
«____» _____2017 г.

ИЗУЧЕНИЕ УЯЗВИМОСТЕЙ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА IEEE 802.x

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ ЮУрГУ-09.03.01.2017.180. ПЗ ВКР

Руководитель ВКР,
к.т.н., доцент
_____/А.Н. Шурыгин/
«____» _____ 2017 г.

Автор ВКР,
Студент группы КЭ-443
_____/А.С. Самуйлов/
«____» _____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____/В.Н. Любицын/
«____» _____ 2017 г.

Челябинск 2017

АННОТАЦИЯ

Самуйлов А.С. Изучение уязвимостей беспроводных сетей стандарта 802.x. – Челябинск: ЮУрГУ, ВШ ЭКН; 2017, 138 с., 4 ил., 1 таблица, библиогр. список - 28 наим.

Было проведено изучение современных беспроводных сетей на канальном, сетевом, транспортном и прикладном уровнях. Возможности и способы их применения, а также их способность сохранять конфиденциальность, целостность и непротиворечивость, передаваемой ими информации. В результате анализа уязвимостей в практической части работы были представлены два способа повысить защищенность информации, при передаче её через беспроводные локальные сети, а также через сеть интернет.

					ЮУрГУ–09.03.01.2017.180 ПЗ ВКР		
Изм.	Лист	№ докум.	Подпись	Дата			
Разраб.		Самуйлов А.С.			*Изучение уязвимостей беспроводных сетей стандарта IEEE 802.x*	Лит.	Лист 6 / Листов 138
Провер.		Шурыгин А.Н.					
Реценз.		Баринов А.Е.					
Н. Контр.		Любицын В.Н.					ЮУрГУ Кафедра ИАОУ
Утверд.		Логиновский О.В.					

ОГЛАВЛЕНИЕ

Определения и сокращения

Сетевая модель OSI (англ. *open systems interconnection basic reference model* — базовая эталонная модель взаимодействия открытых систем, сокр. **ЭМВОС**; 1978 год) — сетевая модель стека сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99).

Сеть Ad-hoc — в такой сети отсутствует точка доступа, управляющая подключением устройств. Устройства сети Ad-hoc могут обмениваться данными только с другими устройствами Ad-hoc. Они не могут соединяться с устройствами, подключенными к беспроводной сети в режиме инфраструктуры, или устройствами, подключенными к проводной сети. Кроме того, безопасность режима Ad-hoc менее надёжна по сравнению с режимом инфраструктуры.

Частотный диапазон ISM - та часть радиочастотного спектра общего назначения, которая может быть использована без лицензирования. Единственное требование для разрабатываемых продуктов в ISM-диапазоне — это соответствие нормам, которые устанавливаются регулирующими органами для данной части частотного спектра.

DSSS (Direct Sequence Spread Spectrum, расширение спектра методом прямой последовательности) – один из основных методов модуляции сигнала, используемый в беспроводных локальных сетях. Данный метод применяется для преобразования исходного сигнала и передачи его одновременно по нескольким каналам связи определенной ширины.

Ethernét (эзернет, от лат. aether — эфир) — пакетная технология компьютерных сетей, преимущественно локальных. Технология Ethernet, рожденная как технология локальных сетей, сегодня используется при решении самых разных задач: от подключения разнообразных терминальных устройств и базовых станций сотовой связи до организации суперскоростных магистралей. Технологические и экономические вопросы проектирования, построения и обслуживания сетей на базе Ethernet приходится решать при создании и эксплуатации любой современной коммуникационной инфраструктуры.

FHSS (Frequency Hopping Spread Spectrum, псевдослучайное изменение рабочей частоты) – метод обработки сигнала с целью расширения его спектра, используемый в беспроводных локальных сетях.

LAN, **Локальная вычислительная сеть** (**ЛВС**, *локальная сеть*; англ. *Local Area Network, LAN*) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

MAC-адрес (от англ. *Media Access Control* — управление доступом к среде, также **Hardware Address**) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

MAN, Городская вычислительная сеть (Metropolitan area network, MAN) (от англ. *«сеть крупного города»*) — объединяет компьютеры в пределах города, представляет собой сеть по размерам меньшую чем WAN, но большую, чем LAN.

Power over Ethernet (PoE)-технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными, через стандартную витую пару в сети Ethernet. Для передачи питания используют специальные сетевые коммутаторы поддерживающие эту технологию.

Qos (англ. Quality of Service — качество обслуживания) - способность сетевой инфраструктуры предоставлять улучшенное обслуживание определенному виду передаваемого трафика при помощи различных технологий.
Качество обслуживания на втором уровне модели OSI (канальном) в пределах одного сетевого элемента обеспечивается за счет использования модели дифференцированного обслуживания (Differentiated Service – DiffServ) и обеспечивается: Классификацией и разметкой трафика; Управлением перегрузками (механизмы очередей).

Secure Shell (SSH) - это сетевой протокол, который позволяет двум компьютерам обмениваться данными по безопасному каналу. Шифрование обеспечивает конфиденциальность и неприкосновенность информации. SSH использует шифрование с открытым ключом для проверки подлинности удаленного компьютера и

предоставляет ему аутентификацию пользователя, если это необходимо. Обычно SSH используется для подключения (входа) к удаленной машине и выполнения команд, но он также поддерживает туннелирование (tunneling), проброс TCP-портов и передачу сеанса X11; передача файлов может быть осуществлена с использованием протоколов SFTP или SCP. По умолчанию сервер SSH "прослушивает" стандартный порт TCP номер 22. Программа-клиент SSH обычно используется для установления связи с демоном *sshd*, который принимает удаленные подключения. И сервер, и клиент, как правило, присутствуют в современных операционных системах, в том числе в Mac OS X, GNU/Linux, Solaris и OpenVMS. Существуют проприетарные, freeware и open source (с открытым исходным кодом) версии различных уровней сложности и завершенности.

STP (англ. Spanning Tree Protocol) - сетевой протокол, работающий на втором уровне модели OSI. Основан на одноименном алгоритме, разработчиком которого является «Мама Интернета» — Радья Перлман (англ. Radia Perlman). Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Происходит это путем автоматического блокирования ненужных в данный момент для полной связности портов. Протокол описан в стандарте IEEE 802.1D.

VPN - это обобщенное название сети или соединения, которое создано внутри или поверх другой сети, например сети Интернет. Как правило, так называют созданную защищенную сеть или туннель внутри незащищенной сети Интернета. В самом простом виде VPN представляет собой туннель из VPN клиента, установленного на компьютере пользователя и VPN сервера. Внутри этого туннеля, средствами VPN, осуществляется защита, шифрование и изменение данных, которыми обменивается компьютер пользователя и веб-сайты или веб-сервисы в сети Интернет

VLANs – это виртуальные сети, которые существуют на втором уровне модели OSI. То есть, вилан можно настроить на коммутаторе второго уровня. Если смотреть на вилан, абстрагируясь от понятия «виртуальные сети», то можно сказать, что VLAN – это просто метка в кадре, который передается по сети. Метка содержит номер вилана (его называют VLAN ID или VID), – на который отводится 12 бит, то есть, вилан может нумероваться от 0 до 4095. Первый и последний номера зарезервированы, их использовать нельзя.

WAN, Глобальная вычислительная сеть, ГВС (англ. *Wide Area Network,* WAN) — компьютерная сеть, охватывающая большие территории и включающая большое число узлов. Глобальные вычислительные сети связывают компьютеры, рассредоточенные на расстоянии сотен и тысяч километров. Часто используются уже существующие не очень качественные линии связи. Более низкие, чем в локальных сетях, скорости передачи данных (десятки килобит в секунду) ограничивают набор услуг передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты. Для стойкой передачи дискретных данных применяются более сложные методы и оборудование, чем в локальных сетях.

Введение

Беспроводная вычислительная сеть — вычислительная сеть, основанная на беспроводном (без использования кабельной проводки) принципе, полностью соответствующая стандартам для обычных проводных сетей (например, Ethernet). В качестве носителя информации в таких сетях могут выступать радиоволны СВЧ-диапазона.

Существует два основных направления применения беспроводных компьютерных сетей:

- Работа в замкнутом объеме (офис, выставочный зал и т. п.);
- Соединение удаленных локальных сетей (или удаленных сегментов локальной сети).

Для организации беспроводной сети в замкнутом пространстве применяются передатчики со всенаправленными антеннами. Стандарт IEEE 802.11 определяет два режима работы сети — Ad-hoc и клиент-сервер. Режим Ad-hoc (иначе называемый «точка-точка») — это простая сеть, в которой связь между станциями (клиентами) устанавливается напрямую, без использования специальной точки доступа. В режиме клиент-сервер беспроводная сеть состоит, как минимум, из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций. Поскольку в большинстве сетей необходимо обеспечить доступ к файловым серверам, принтерам и другим устройствам, подключенным к проводной локальной сети, чаще всего используется режим клиент-сервер. Без подключения дополнительной антенны устойчивая связь для оборудования IEEE 802.11b достигается в среднем на следующих расстояниях: открытое пространство — 500 м, комната, разделенная перегородками из неметаллического материала — 100 м, офис из нескольких комнат — 30 м. Следует иметь в виду, что через стены с большим содержанием металлической арматуры (в железобетонных зданиях таковыми являются несущие стены) радиоволны диапазона 2,4 ГГц иногда могут вообще не проходить, поэтому в комнатах, разделенных подобной стеной, придется ставить свои точки доступа.

Для соединения удаленных локальных сетей (или удаленных сегментов локальной сети) используется оборудование с направленными антеннами, что позволяет увеличить дальность связи до 20 км (а при использовании специальных усилителей и большой высоте размещения антенн — до 50 км). Причем в качестве подобного оборудования могут выступать и устройства Wi-Fi, нужно лишь добавить к ним

специальные антенны (конечно, если это допускается конструкцией). Комплексы для объединения локальных сетей по топологии делятся на «точку-точку» и «звезду». При топологии «точка-точка» (режим Ad-hoc в IEEE 802.11) организуется радиомост между двумя удаленными сегментами сети. При топологии «звезда» одна из станций является центральной и взаимодействует с другими удаленными станциями. При этом центральная станция имеет всенаправленную антенну, а другие удаленные станции — однонаправленные антенны. Применение всенаправленной антенны в центральной станции ограничивает дальность связи дистанцией примерно 7 км. Поэтому, если требуется соединить между собой сегменты локальной сети, удаленные друг от друга на расстояние более 7 км, приходится соединять их по принципу «точка-точка». При этом организуется беспроводная сеть с кольцевой или иной, более сложной топологией.

Мощность, излучаемая передатчиком точки доступа или же клиентской станции, работающей по стандарту IEEE 802.11, не превышает 0,1 Вт, но многие производители беспроводных точек доступа ограничивают мощность лишь программным путём, и достаточно просто поднять мощность до 0,2-0,5 Вт. Для сравнения — мощность, излучаемая мобильным телефоном, на порядок больше(в момент звонка - до 2 Вт). Поскольку, в отличие от мобильного телефона, элементы сети расположены далеко от головы, в целом можно считать, что беспроводные компьютерные сети более безопасны с точки зрения здоровья, чем мобильные телефоны.

Если беспроводная сеть используется для объединения сегментов локальной сети, удаленных на большие расстояния, антенны, как правило, размещаются за пределами помещения и на большой высоте.

Продукты для беспроводных сетей, соответствующие стандарту IEEE 802.11, предлагают четыре уровня средств безопасности: физический, идентификатор набора служб (SSID — Service Set Identifier), идентификатор управления доступом к среде (MAC ID — Media Access Control ID) и шифрование.

Технология DSSS для передачи данных в частотном диапазоне 2,4 ГГц за последние 50 лет нашла широкое применение в военной связи для улучшения безопасности беспроводных передач. В рамках схемы DSSS поток требующих передачи данных «разворачивается» по каналу шириной 20 МГц в рамках диапазона ISM с помощью схемы ключей дополнительного кода (Complementary Code Keying, CCK). Для декодирования принятых данных получатель должен установить правильный частотный канал и использовать ту же самую схему CCK. Таким обра-

зом, технология на базе DSSS обеспечивает первую линию обороны от нежелательного доступа к передаваемым данным. Кроме того, DSSS представляет собой «тихий» интерфейс, так что практически все подслушивающие устройства будут отфильтровывать его как «белый шум».

Идентификатор SSID позволяет различать отдельные беспроводные сети, которые могут действовать в одном и том же месте или области. Он представляет собой уникальное имя сети, включаемое в заголовок пакетов данных и управления IEEE 802.11. Беспроводные клиенты и точки доступа используют его, чтобы проводить фильтрацию и принимать только те запросы, которые относятся к их SSID. Таким образом, пользователь не сможет обратиться к точке доступа, если только ему не предоставлен правильный SSID.

Возможность принятия или отклонения запроса к сети может зависеть также от значения идентификатора MAC ID — это уникальное число, присваиваемое в процессе производства каждой сетевой карте. Когда клиентский ПК пытается получить доступ к беспроводной сети, точка доступа должна сначала проверить адрес MAC для клиента. Точно так же и клиентский ПК должен знать имя точки доступа.

Механизм Wired Equivalency Privacy (WEP), определенный в стандарте IEEE 802.11, обеспечивает еще один уровень безопасности. Он опирается на алгоритм шифрования RC4 компании RSA Data Security с 40- или 128-разрядными ключами. Несмотря на то, что использование WEP несколько снижает пропускную способность, эта технология заслуживает более пристального внимания. Дополнительные функции WEP затрагивают процессы сетевой аутентификации и шифрования данных. Процесс аутентификации с разделяемым ключом для получения доступа к беспроводной сети использует 64-разрядный ключ — 40-разрядный ключ WEP выступает как секретный, а 24-разрядный вектор инициализации (Initialization Vector) — как разделяемый. Если конфигурация точки доступа позволяет принимать только обращения с разделяемым ключом, она будет направлять клиенту случайную строку вызова длиной 128 октетов. Клиент должен зашифровать строку вызова и вернуть зашифрованное значение точке доступа. Далее точка доступа расшифровывает полученную от клиента строку и сравнивает её с исходной строкой вызова. Наконец, право клиента на доступ к сети определяется в зависимости от того, прошел ли он проверку шифрованием. Процесс расшифровки данных, закодированных с помощью WEP, заключается в выполнении логической операции «исключающее ИЛИ» (XOR) над ключевым потоком и при-

нятой информацией. Процесс аутентификации с разделяемым ключом не допускает передачи реального 40-разрядного ключа WEP, поэтому этот ключ практически нельзя получить путём контроля за сетевым трафиком. Ключ WEP рекомендуется периодически менять, чтобы гарантировать целостность системы безопасности.

Еще одно преимущество беспроводной сети связано с тем, что физические характеристики сети делают её локализованной. В результате дальность действия сети ограничивается лишь определенной зоной покрытия. Для подслушивания потенциальный злоумышленник должен будет находиться в непосредственной физической близости, а значит, привлекать к себе внимание. В этом преимущество беспроводных сетей с точки зрения безопасности. Беспроводные сети имеют также уникальную особенность: их можно отключить или модифицировать их параметры, если безопасность зоны вызывает сомнения.

Для вторжения в сеть необходимо к ней подключиться. В случае проводной сети требуется электрическое соединение, беспроводной — достаточно оказаться в зоне радиовидимости сети с оборудованием того же типа, на котором построена сеть.

В проводных сетях основное средство защиты на физическом и MAC-уровнях — административный контроль доступа к оборудованию, недопущение злоумышленника к кабельной сети. В сетях, построенных на управляемых коммутаторах, доступ может дополнительно ограничиваться по MAC-адресам сетевых устройств.

В беспроводных сетях для снижения вероятности несанкционированного доступа предусмотрен контроль доступа по MAC-адресам устройств и тот же самый WEP. Поскольку контроль доступа реализуется с помощью точки доступа, он возможен только при инфраструктурной топологии сети. Механизм контроля подразумевает заблаговременное составление таблицы MAC-адресов разрешенных пользователей в точке доступа и обеспечивает передачу только между зарегистрированными беспроводными адаптерами. При топологии «ad-hoc» (каждый с каждым) контроль доступа на уровне радиосети не предусмотрен.

Для проникновения в беспроводную сеть злоумышленник должен:

•Иметь оборудование для беспроводных сетей, совместимое с используемым в сети (применительно к стандартному оборудованию — соответствующей технологии беспроводных сетей — DSSS или FHSS);

•При использовании в оборудовании FHSS нестандартных последовательностей скачков частоты узнать их;

•Знать идентификатор сети, закрывающий инфраструктуру и единый для всей логической сети (SSID);

•Знать (в случае с DSSS), на какой из 14 возможных частот работает сеть, или включить режим автосканирования;

•Быть занесенным в таблицу разрешенных MAC-адресов в точке доступа при инфраструктурной топологии сети;

•Знать ключ WPA или WEP в случае, если в беспроводной сети ведется шифрованная передача.

Решить все это практически невозможно, поэтому вероятность несанкционированного вхождения в беспроводную сеть, в которой приняты предусмотренные стандартом меры безопасности, можно считать очень низкой. Информация устарела. На 2010 год, принимая во внимания уязвимости WEP, защищенной можно считать сеть, с ключом 128разрядным AES/WPA2 от 20 символов.

1. БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ СЕТИ

1.1 Определение стандарта IEEE 802

IEEE 802 — группа стандартов семейства IEEE, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN).

В частности, стандарты IEEE 802 ограничены сетями с пакетами переменной длины. Число 802 являлось следующим свободным номером для стандарта, хотя часто ассоциируется с датой принятия стандарта — февраль 1980 года.

Службы и протоколы, указанные в IEEE 802, находятся на двух нижних уровнях (канальный и физический) семиуровневой сетевой модели OSI. Фактически IEEE 802 разделяет канальный уровень OSI на два подуровня — Media Access Control (MAC) и Logical Link Control (LLC). Таким образом, уровни располагаются в следующем виде:

-Канальный уровень (подуровень LLC, подуровень MAC)

-Физический уровень

Семейство стандартов IEEE 802 поддерживается комитетом по стандартам IEEE 802 LAN/MAN Standards Committee (LMSC). Наиболее часто используются для семейства Ethernet, Token Ring, беспроводной LAN, мостов и сетей с виртуальными мостами (Virtual Bridged LANs). Каждая отдельная рабочая группа работает в своей области стандарта.

Рабочие группы IEEE 802:

- IEEE 802.1 - Управление сетевыми устройствами и их взаимодействие
- IEEE 802.1b - Управление локальной сетью
- IEEE 802.1D - Описание Алгоритма прозрачного моста, STP, QoS
- IEEE 802.1d - Логика работы коммутатора, исключение петли избыточных связей (STP)
- IEEE 802.1e - Протокол загрузки системы
- IEEE 802.1f
- IEEE 802.1G - Удалённый MAC-мост
- IEEE 802.1h - Транслирующий мост между разными технологиями
- IEEE 802.1p - дополнение к логике, обеспечивающее приоритетизацию трафика и динамическую фильтрацию IGMP
- IEEE 802.1Q - Спецификация параметров и требований мостовой передачи виртуальных сетей. Описание VLAN

- IEEE 802.1r - Проприетарный протокол регистрации атрибутов GARP (GPRP)
- IEEE 802.1s - *Multiple Spanning Trees* (расширение STP для многих VLAN)
- IEEE 802.1v - Классификация VLAN по протоколам и портам
- IEEE 802.1w - Быстрый STP (*Rapid STP*)
- IEEE 802.1X - Контроль доступа к сети, основанный на RADIUS
- IEEE 802.1AB - Link Layer Discovery Protocol (LLDP)
- IEEE 802.1ad - Провайдерские мосты
- IEEE 802.1ah - Мост опорных операторских сетей (PBB)
- IEEE 802.1AE - Безопасность MAC
- IEEE 802.1af - KeySec
- IEEE 802.1ag - Управление ошибками соединения
- IEEE 802.1aq - Shortest Path Bridging (SPB)
- IEEE 802.1ak - *Multiple Registration Protocol*
- IEEE 802.2 - Logical Link Control (LLC)
- IEEE 802.3 - Технология Ethernet
- IEEE 802.3a - 10BASE2, «Тонкий Ethernet» (англ. *thinnet*): 10 Мбит/с (1,25 Мбайт/с) через коаксиальный кабель RG-58 (диаметр 5 мм)
- IEEE 802.3b - 10BROAD36
- IEEE 802.3c - 10 Мбит/с (1,25 Мбайт/с), спецификации повторителя
- IEEE 802.3d - FOIRL(англ. *Fiber-Optic Inter-Repeater Link*, волоконно-оптическая связь между повторителями)
- IEEE 802.3e - 1BASE5 (StarLAN): 1 Мбит/с через витую пару
- IEEE 802.3i - 10BASE-T: 10 Мбит/с (1,25 Мбайт/с) через витую пару
- IEEE 802.3j - 10BASE-F: 10 Мбит/с (1,25 Мбайт/с) через оптическое волокно
- IEEE 802.3u - 100BASE-TX, 100BASE-T4, 100BASE-FX, *Fast Ethernet*: 100 Мбит/с (12,5 Мбайт/с), автосогласование(совместимость с IEEE 802.3i)
- IEEE 802.3x - поддержка полнодуплексной связи; совместимость с DIX
- IEEE 802.3y - 100BASE-T2: 100 Мбит/с (12,5 Мбайт/с) через витую пару 3-й категории (две пары медных проводов)
- IEEE 802.3z - 1000BASE-X, *Gigabit Ethernet*: 1 Гбит/с (125 Мбайт/с) через волоконно-оптический кабель
- IEEE 802.3-1998 - Версия, включающая в себя все предыдущие стандарты с исправленными ошибками
- IEEE 802.3ab - 1000BASE-T, *Gigabit Ethernet*: 1 Гбит/с (125 Мбайт/с) по витой паре 5-й категории

- IEEE 802.3ac - Увеличение максимального размера фрейма до 1522 байт (для поддержки информации о VLAN стандарта IEEE 802.1Q и приоритета стандарта IEEE 802.1p)
- IEEE 802.3ad - Агрегирование каналов
- IEEE 802.3-2002 - Версия, включающая в себя все предыдущие стандарты с исправленными ошибками
- IEEE 802.3ae - 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW, *10 Gigabit Ethernet*: 10 Гбит/с (1,25 Гбайт/с) через оптическое волокно
- IEEE 802.3af - PoE (Power over Ethernet) — электропитание через Ethernet
- IEEE 802.3ah - Ethernet in the First Mile (EFM, «первая миля» Ethernet)
- IEEE 802.3ak - 10GBASE-CX4 10 Гбит/с (1,25 Гбайт/с) через твинаксиальный кабель
- IEEE 802.3-2005 - Ревизия основного стандарта, включающая четыре предшествующих изменения
- IEEE 802.3an - 10GBASE-T, *10 Gigabit Ethernet*: 10 Гбит/с (1,25 Гбайт/с) по витой паре 6-й или 7-й категории
- IEEE 802.3ap - 1 и 10 Гбит/с (125 и 1250 Мбайт/с) по печатной кросс-плате
- IEEE 802.3aq - 10GBASE-LRM: 10 Гбит/с (1,25 Гбайт/с) по многомодовому оптическому волокну
- IEEE 802.3ar - Управление перегрузкой
- IEEE 802.3as - Расширение формата кадров
- IEEE 802.3at - Питание через Ethernet оконечных устройств повышенной мощности (более 24 Вт)
- IEEE 802.3au - Требования изоляции для питания через Ethernet (опубликован как 802.3-2005/Cor 1)
- IEEE 802.3av - 10 Гбит/с, *10 Gigabit Ethernet PON*
- IEEE 802.3aw - Исправлена ошибка в описании 10GBASE-T (опубликован как 802.3-2005/Cor 2)
- IEEE 802.3ax - Агрегирование каналов; этап формального перевода протокола 802.3ad в подгруппу 802.1 (опубликован как 802.1AX)
- IEEE 802.3ay - Этап ревизии стандарта 802.3-2005
- IEEE 802.3az - *Ethernet* с энергосберегающим режимом (снижение потребляемой мощности сетевой карты в периоды низкой сетевой активности примерно до 89 мВт вместо типичного значения около 476 мВ)

- IEEE 802.3ba - *100 Gigabit Ethernet* через 10 м жгута медных кабелей (4x25 Гбит или 10x10 Гбит) либо 100 м многомодового оптоволокна (MM) либо 40 км одномодового оптоволокна (SM)
- IEEE 802.3-2008/Cor 1 - Увеличение таймингов Pause Reaction Delay которых было недостаточно для 10 Gbit/s (имя рабочей группы было 802.3bb)
- IEEE 802.3bc - Move and update Ethernet related TLVs (type, length, values), previously specified in Annex F of IEEE 802.1AB (LLDP) to 802.3
- IEEE 802.3bd - Priority-based Flow Control. An amendment by the IEEE 802.1 Data Center Bridging Task Group (802.1Qbb) to develop an amendment to IEEE Std 802.3 to add a MAC Control Frame to support IEEE 802.1Qbb Priority-based Flow Control
- IEEE 802.3.1 - MIB definitions for Ethernet. It consolidates the Ethernet related MIBs present in Annex 30A&B, various IETF RFCs, and 802.1AB annex F into one master document with a machine readable extract. (workgroup name was P802.3be)
- IEEE 802.3bf - Provide an accurate indication of the transmission and reception initiation times of certain packets as required to support IEEE P802.1AS
- IEEE 802.3bg - Provide a 40 Gbit/s PMD which is optically compatible with existing carrier SMF 40 Gbit/s client interfaces (OTU3/STM-256/OC-768/40G POS)
- IEEE 802.3-2012 - A revision of base standard incorporating the 802.3at/av/az/ba/bc/bd/bf/bg amendments, a corrigenda and errata
- IEEE 802.3bj - Define a 4-lane 100 Gbit/s backplane PHY for operation over links consistent with copper traces on “improved FR-4” (as defined by IEEE P802.3ap or better materials to be defined by the Task Force) with lengths up to at least 1 m and a 4-lane 100 Gbit/s PHY for operation over links consistent with copper twinaxial cables with lengths up to at least 5 m
- IEEE 802.3bk - This amendment to IEEE Std 802.3 defines the physical layer specifications and management parameters for EPON operation on point-to-multipoint passive optical networks supporting extended power budget classes of PX30, PX40, PRX40, and PR40 PMDs
- IEEE 802.3bm - 100G/40G Ethernet for optical fiber
- IEEE 802.3bp - 1000BASE-T1 – Gigabit Ethernet over a single twisted pair, automotive & industrial environments
- IEEE 802.3bq - 25G/40GBASE-T for 4-pair balanced twisted-pair cabling with 2 connectors over 30 m distances
- IEEE 802.3bs - 400 Gbit/s Ethernet over optical fiber using multiple 25G/50G lanes
- IEEE 802.3bt - Power over Ethernet enhancements up to 100 W using all 4 pairs balanced twisted-pair cabling, lower standby power and specific enhancements to support IoT applications (e.g. Lighting, sensors, building automation)

- IEEE 802.3bw - 100BASE-T1 – 100 Mbit/s Ethernet over a single twisted pair for automotive applications
- IEEE 802.3-2015 - 802.3bx – a new consolidated revision of the 802.3 standard including amendments 802.2bk/bj/bm
- IEEE 802.3by - Optical fiber, twinax and backplane 25 Gigabit Ethernet
- IEEE 802.3bz - 2.5 Gigabit and 5 Gigabit Ethernet over Cat-5/Cat-6 twisted pair – 2.5GBASE-T and 5GBASE-T
- IEEE 802.3cd - Media Access Control Parameters for 50 Gb/s and Physical Layers and Management Parameters for 50 Gb/s, 100 Gb/s, and 200 Gb/s Operation
- IEEE 802.4 - Маркерная шина Token bus
- IEEE 802.5 - Определяет MAC-уровень для маркерного кольца
- IEEE 802.6 - Городские сети (MAN)
- IEEE 802.7 - Широкополосная передача по коаксиальному кабелю
- IEEE 802.8 - Волоконно-оптические сети
- IEEE 802.9 - Интегрированные сети передачи речевых сообщений и данных
- IEEE 802.10 - Сетевая безопасность
- IEEE 802.11 - Беспроводные локальные сети
- IEEE 802.11a - 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)
- IEEE 802.11b - улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
- IEEE 802.11c - процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001)
- IEEE 802.11d - интернациональные роуминговые расширения (2001)
- IEEE 802.11e - улучшения: QoS, пакетный режим (packet bursting) (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
- IEEE 802.11h - распределённый по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
- IEEE 802.11i - улучшенная безопасность (2004)
- IEEE 802.11j - расширения для Японии (2004)
- IEEE 802.11k - улучшения измерения радиоресурсов
- IEEE 802.11l - зарезервирован
- IEEE 802.11m - поправки и исправления для всей группы стандартов 802.11
- IEEE 802.11n - увеличение скорости передачи данных (600 Мбит/с). 2,4-2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g (сентябрь 2009)
- IEEE 802.11o - зарезервирован
- IEEE 802.11p - WAVE — Wireless Access for the Vehicular Environment (беспроводной доступ для среды транспортного средства)

- IEEE 802.11q - зарезервирован, иногда его путают с 802.1Q
- IEEE 802.11r - быстрый роуминг
- IEEE 802.11s - ESS Wireless mesh network (Extended Service Set — расширенный набор служб; Mesh Network — многосвязная сеть)
- IEEE 802.11T - Wireless Performance Prediction (WPP, предсказание производительности беспроводного оборудования) — методы тестов и измерений
- IEEE 802.11u - взаимодействие с не-802 сетями (например, сотовыми)
- IEEE 802.11v - управление беспроводными сетями
- IEEE 802.11w - Protected Management Frames (защищенные управляющие фреймы)
- IEEE 802.11x - зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.**1X**
- IEEE 802.11y - дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве
- IEEE 802.11ac - новый стандарт IEEE. Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утвержден в январе 2014 года
- IEEE 802.11ad - новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с
- IEEE 802.12 - 100BaseVG
- IEEE 802.13 - Не используется
- IEEE 802.14 - Кабельный модем
- IEEE 802.15 - Wireless PAN
- IEEE 802.15.1 - Bluetooth certification
- IEEE 802.15.2 - IEEE 802.15 and IEEE 802.11 coexistence
- IEEE 802.15.3 - High-Rate wireless PAN (e.g., UWB, etc)
- IEEE 802.15.4 - Физический уровень и управление доступом к среде для беспроводных персональных сетей с низким уровнем скорости (Low-rate WPAN)
- IEEE 802.15.5 - Mesh networking для WPAN
- IEEE 802.15.6 - Body area network
- IEEE 802.16 - Беспроводная городская сеть (WiMAX-сертификация)
- IEEE 802.16e - (Мобильные) Широковещательные беспроводные сети
- IEEE 802.16.1 - Служба местного многоточечного распределения
- IEEE 802.17 - Эластичное кольцо пакетов
- IEEE 802.18 - Радиорегулирование
- IEEE 802.19 - Сосуществование сетей
- IEEE 802.20 - Мобильный широковещательный беспроводной доступ

- IEEE 802.21 - Media Independent Handoff
- IEEE 802.22 - Местные беспроводные сети
- IEEE 802.23 - Рабочая группа чрезвычайных сервисов
- IEEE 802.24 - Smart Grid TAG
- IEEE 802.25 - Omni-Range Area Network

1.2 Определение беспроводной локальной сети

Беспроводная сетевая технология используется для соединения двух или более устройств и обеспечивает связь через точки доступа для передачи сигналов. Беспроводная локальная сеть — это не что иное, как сеть, которая объединяет несколько компьютеров для отправления и получения данных. Компьютеры при этом должны иметь беспроводные сетевые адаптеры, чтобы связаться с точками доступа. Настройка беспроводной сети обеспечивает передачу данных, которая осуществляется через радиоэфир, а объединение устройств происходит без использования кабельных соединений. Термин «беспроводной» охватывает не только многократно рассмотренный уже на данном сайте Wi-Fi, но и все виды беспроводных технологий и устройств, в том числе сотовую связь и BlueTooth. Объединить все устройства, снабженные беспроводным модулем — компьютеры с беспроводными адаптерами, компьютерные аксессуары (беспроводные мыши, беспроводная клавиатура, пульты дистанционного управления, беспроводные маршрутизаторы, беспроводные сетевые карты), телевизор, планшет, ноутбук, смартфон, веб-камера и т. д.

Беспроводные соединения осуществляются по воздуху с помощью электромагнитных волн (радиочастоты, инфракрасные, спутниковые). Все современные устройства, работающие с популярными операционными системами, такими как Windows XP, Windows 7, Mac OS, Linux, работают с беспроводными сетями.

Существуют различные способы настройки беспроводной сети, называемые «топологией» или «архитектурой» и четыре основных типа стандартов радиочастот для беспроводных сетей: 802.11, 802.11a, 802.11b, 802.11g. Основные различия между ними — скорость соединения (802.11 и 802.11b являются самыми медленными в 1-2 Мбит и 5,5-11 Мбит в секунду соответственно). Фактическая скорость передачи данных зависит от количества и размера физических барьеров внутри сети и возможных помех при радиопередачах.

По масштабам охватываемой территории беспроводные сети подразделяются на четыре основных типа.

Беспроводные персональные сети (PAN). Это маленькие сети, как правило соединяющие между собой два устройства, например, два смартфона, телефон и гарнитуру или смартфон и ноутбук. Примером является Bluetooth.

Беспроводные локальные сети (WLAN). WLAN обеспечивают беспроводную связь на относительно небольшой территории или в небольшой группе зданий (предприятия) с помощью радиоволн или инфракрасных сигналов. Сети подключают и связывают неограниченное количество компьютеров и ноутбуков, а это связывает людей, использующих эти компьютеры. Лица внутри рабочей группы соединены через локальные сети. Примером такой сети является Wi-Fi, обеспечивающая доступ в Интернет. Существуют беспроводные локальные сети, узлы которых находятся на расстояния более 12500 км (космические станции и орбитальные центры). Эти сети также относят к локальным.

Беспроводные городские сети (MAN) Это уже не одна, а целый ряд локальных сетей, связанных вместе). Примером MAN являются Wimax (Yota). Многие локальные сети в связаны между собой в

Глобальные сети WAN (Wide Area Network), которые облегчают общение между людьми посредством электронной почты. Сегодня электронная почта стала самым простым, дешевым способом передачи информации между пользователями. Беспроводные глобальные сети связи охватывает большие географические зоны (самая популярная — Интернет.

1.3 Wi-Fi

Wi-Fi — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Wi-Fi был создан в 1998 году в лаборатории радиоастрономии CSIRO (Commonwealth Scientific and Industrial Research Organisation) в Канберре, Австралия. Создателем беспроводного протокола обмена данными является инженер Джон О'Салливан (John O'Sullivan).

История

Стандарт IEEE 802.11n был утверждён 11 сентября 2009 года. Его применение позволяет повысить скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. С 2011 по 2013 разрабатывался стандарт IEEE 802.11ac, стандарт принят в январе 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства, поддерживающие данный стандарт.

27 июля 2011 года Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволяют принимать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намёком» на Hi-Fi (англ. *High Fidelity* — высокая точность). Несмотря на то, что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается.

Принцип работы

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID (англ.)русск.) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- Автономные точки доступа (называются также самостоятельные, децентрализованные, умные)
- Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные)
- Бесконтроллерные, но не автономные (управляемые без контроллера)

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- Со статическими настройками радиоканалов
- С динамическими (адаптивными) настройками радиоканалов
- Со «слоистой» или многослойной структурой радиоканалов

Преимущества Wi-Fi

- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.

•Позволяет иметь доступ к сети мобильным устройствам.

•Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.

•Мобильность. Вы больше не привязаны к одному месту и можете пользоваться Интернетом в комфортной для вас обстановке.

•В пределах Wi-Fi зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.

•Излучение от Wi-Fi устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона.

Недостатки Wi-Fi

•В диапазоне 2,4 GHz работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшает электромагнитную совместимость.

•Производителями оборудования указывается скорость на L1 (OSI), в результате чего создаётся иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

•Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; В Японии есть ещё один канал в верхней части диапазона, а другие страны, например Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например Россия, Беларусь и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора.

•Как было упомянуто выше — в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

•Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным

применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифро-буквенные пароли для того, чтобы максимально усложнить задачу подбора пароля.

•В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только легковзламываемый WEP.

Беспроводные технологии в промышленности

Для использования в промышленности технологии Wi-Fi предлагаются пока ограниченным числом поставщиков. Так Siemens Automation & Drives предлагает Wi-Fi-решения для своих контроллеров SIMATIC в соответствии со стандартом IEEE 802.11g в свободном ISM-диапазоне 2,4 ГГц и обеспечивающим максимальную скорость передачи 54 Мбит/с. Данные технологии применяются для управления движущимися объектами и в складской логистике, а также в тех случаях, когда по какой-либо причине невозможно прокладывать проводные сети Ethernet. Использование Wi-Fi устройств на предприятиях обусловлено высокой помехоустойчивостью, что обуславливает их применение на предприятиях с множеством металлических конструкций. В свою очередь Wi-Fi приборы не создают существенных помех для узкополосных радиосигналов. В настоящее время технология находит широкое применение на удаленном или опасном производстве, там где нахождение оперативного персонала связано с повышенной опасностью или вовсе затруднительно. К примеру, для задач телеметрии на нефтегазодобывающих предприятиях, а также для контроля за перемещением персонала и транспортных средств в шахтах и рудниках, для определения нахождения персонала в аварийных ситуациях.

Некоммерческое использование Wi-Fi

Пока коммерческие сервисы пытаются использовать существующие бизнес-модели для Wi-Fi, многие группы, сообщества, города и частные лица строят свободные сети Wi-Fi, часто используя общее пиринговое соглашение для того, чтобы сети могли свободно взаимодействовать друг с другом.

Многие муниципалитеты объединяются с локальными сообществами, чтобы расширить свободные Wi-Fi-сети. Некоторые группы строят свои Wi-Fi-сети, полностью основанные на добровольной помощи и пожертвованиях.

Для получения более подробной информации смотрите раздел совместные беспроводные сети, где можно также найти список свободных сетей Wi-Fi, расположенных по всему миру (см. также Бесплатные точки доступа Wi-Fi в Москве).

OLSR (en) — один из протоколов, используемых для создания свободных сетей. Некоторые сети используют статическую маршрутизацию, другие полностью полагаются на OSPF. В Израиле разрабатывается протокол WiPeer для создания бесплатных P2P-сетей на основе Wi-Fi.

В Wireless Leiden разработали собственное программное обеспечение для маршрутизации под названием LVrouteD для объединения Wi-Fi-сетей, построенных на полностью беспроводной основе. Бóльшая часть сетей построена на основе ПО с открытым кодом, или публикуют свою схему под открытой лицензией. (превращает любой ноутбук с установленным Wi-Fi-модулем в открытый узел Wi-Fi-сети). Также следует обратить внимание на netsukuku — Разработка всемирной бесплатной mesh-сети.

Некоторые небольшие страны и муниципалитеты уже обеспечивают свободный доступ к хот-спотам Wi-Fi и доступ к Интернету через Wi-Fi по месту жительства для всех. Например, Королевство Тонга и Эстония, которые имеют большое количество свободных хот-спотов Wi-Fi по всей территории страны. В Париже OzoneParis предоставляет свободный доступ в Интернет неограниченно всем, кто способствует развитию Pervasive Network, предоставляя крышу своего дома для монтажа оборудования Wi-Fi. Unwire Jerusalem — это проект установки свободных точек доступа Wi-Fi в крупных торговых центрах Иерусалима. Многие университеты обеспечивают свободный доступ к Интернет через Wi-Fi для своих студентов, посетителей и всех, кто находится на территории университета.

Некоторые коммерческие организации, такие как Panera Bread, предоставляют свободный доступ к Wi-Fi постоянным клиентам. Заведения McDonald’s Corporation тоже предоставляют доступ к Wi-Fi под брендом McInternet. Этот сервис был запущен в ресторане в Оук-Брук, Иллинойс; он также доступен во многих ресторанах в Лондоне, Москве.

Тем не менее, есть и третья подкатегория сетей, созданных сообществами и организациями, такими как университеты, где свободный доступ предоставляется членам сообщества, а тем, кто в него не входит, доступ предоставляется на платной

основе. Пример такого сервиса — сеть Sparknet в Финляндии. Sparknet также поддерживает OpenSparknet — проект, в котором люди могут делать свои собственные точки доступа частью сети Sparknet, получая от этого определённую выгоду.

В последнее время коммерческие Wi-Fi-провайдеры строят свободные хот-споты Wi-Fi и хот-зоны. Они считают, что свободный Wi-Fi-доступ привлечёт новых клиентов и инвестиции вернутся.

Бесплатный доступ к Интернету через Wi-Fi

Независимо от исходных целей (привлечение клиентов, создание дополнительного удобства или чистый альтруизм) во всём мире и в России, в том числе, растёт количество бесплатных хот-спотов, где можно получить доступ к наиболее популярной глобальной сети (Интернет) совершенно бесплатно. Это могут быть и крупные транспортные узлы (такие хот-спот зоны, например, уже находятся на станциях метро в различных городах мира, таких как: Лондон, Париж, Нью-Йорк, Токио, Сеул, Сингапур, Гонконг, Москва), где подключиться можно самостоятельно в автоматическом режиме, и места общественного питания, где для подключения необходимо попросить карточку доступа с паролем у персонала, и даже просто территории городского ландшафта, являющиеся местом постоянного скопления людей.

Стандартами Wi-Fi не предусмотрено шифрование передаваемых данных в открытых сетях. Это значит, что все данные, которые передаются по открытому беспроводному соединению, могут быть прослушаны злоумышленниками при помощи программ-снифферов. К таким данным могут относиться пары логин/пароль, номера банковских счетов, пластиковых карт, конфиденциальная переписка. Поэтому, при использовании бесплатных хот-спотов не следует передавать в Интернет подобные данные.

Первые хот- зоны в Московском метрополитене, охватывающие поезда Кольцевой линии, были запущены совместно с оператором сотовой связи «МТС» 23 марта 2012 года. Первые месяцы интернет работал в тестовом режиме со скоростью 7,2 Мбит/с. В 2013 году московский метрополитен провел конкурс при поддержке Правительства Москвы на установку Wi-Fi соединения на всех станциях метрополитена. Конкурс выиграла компания ЗАО «Максима Телеком» и вложила в создание беспроводной сети в метрополитене 1,8 млрд рублей. Эта Wi-Fi сеть называется MosMetro_free. Ежедневно этой сетью пользуется 1,2 млн человек. В начале 2015 года к сети Wi-Fi в метро подключилось более 55 млн уникальных

пользователей. Поезда Московского метрополитена, в отличие от других стран мира, где точки доступа в интернет находятся только на станциях или в туннелях, оснащены индивидуальным Wi-Fi роутером. В 2015 году Wi-Fi стал появляться не только в вагонах электропоездов, но и на эскалаторах, переходах и в вестибюлях станций метро. В 2015 году хот-зоны длительностью сессии интернет — соединения в 25 минут появились на более чем 100 остановках общественного транспорта в Москве. Сеть подключения называется Mosgortrans_Free. Скорость интернет — соединения составляет 10 Мбит/с. За 2015 год на остановках вышло в сеть более 70 тысяч уникальных пользователей. После принятия ФЗ-№ 97 от 5 мая 2014 года для подключения к Wi-Fi на остановках общественного транспорта или в метрополитене нужно пройти авторизацию с помощью SMS. На конец 2015 года было оборудовано ещё 300 остановок беспроводным интернетом.

1.4 Методы аутентификации в Wi-Fi сетях

1. **Открытая аутентификация (англ. *Open Authentication*):**
Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, то есть по сути это защита беспроводной Wi-Fi сети на основе ограничения доступа, что не безопасно.
Используемые шифры: без шифрования, статический WEP, CKIP.

2. **Аутентификация с общим ключом (англ. *Shared Key Authentication*):**
Необходимо настроить статический ключ шифрования алгоритма WEP (англ. *Wired Equivalent Privacy*). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети.
Схема аутентификации с общим ключом уязвима к атакам «Man in the middle». Алгоритм шифрования WEP — это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа.
Используемые шифры: без шифрования, динамический WEP, CKIP.

3. **Аутентификация по MAC-адресу:**
Данный метод не предусмотрен в IEEE 802.11, но поддерживается большинством производителей оборудования, например D-Link и Cisco. Происходит сравнение MAC-адреса клиента с таблицей разрешённых MAC-адресов, хранящейся на точке доступа, либо используется внешний сервер аутентификации. Используется как дополнительная мера защиты.
IEEE начал разработки нового стандарта IEEE 802.11i, но из-за трудностей утверждения, организация WECA (англ. *Wi-Fi Alliance*) совместно с IEEE анонсировали стандарт WPA (англ. *Wi-Fi Protected Access*). В WPA используется TKIP (англ. *Temporal Key Integrity Protocol*, протокол проверки целостности ключа), который

использует усовершенствованный способ управления ключами и покадровое изменение ключа.

4. **Wi-Fi Protected Access (WPA)**

После первых успешных атак на WEP было принято разработать новый стандарт 801.11i. Но до него был выпущен «промежуточный» стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1x и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS сервера(WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK)
Используемые шифры: TKIP (стандарт), AES-CCMP (расширение), WEP (в качестве обратной совместимости).

5. **WI-FI Protected Access2 (WPA2, 801.11I)**

WPA2 или стандарт 801.11i — это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом.
Используемые шифры: AES-CCMP (стандарт), TKIP (в качестве обратной совместимости).

6**.. Cisco Centralized Key Managment (CCKM)**

Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа. Клиент один раз проходит аутентификацию на RADIUS-сервере, после чего может переключаться между точками доступа.
Используемые шифры: WEP, CKIP, TKIP, AES-CCMP

1.5 Методы шифрования в Wi-Fi сетях

WEP-шифрование (*Wired Equivalent Privacy*)

Аналог шифрования трафика в проводных сетях. Используется симметричный потоковый шифр RC4 (англ. *Rivest Cipher 4*), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими. Есть два основных протокола WEP:

- 40-битный WEP (длина ключа 64 бита, 24 из которых — это вектор инициализации, который передается открытым текстом);
- 104-битный WEP (длина ключа 128 бит, 24 из которых — это тоже вектор инициализации); Вектор инициализации используется алгоритмом RC4. Увеличение длины ключа не приводит к увеличению надежности алгоритма.

Основные недостатки:

- использование для шифрования непосредственно пароля, введенного пользователем;
- недостаточная длина ключа шифрования;
- использование функции CRC32 для контроля целостности пакетов;
- повторное использование векторов инициализации и др.

TKIP-шифрование (англ. *Temporal Key Integrity Protocol*)

Используется тот же симметричный потоковый шифр RC4, но является более криптостойким. Вектор инициализации составляет 48 бит. Учтены основные атаки на WEP. Используется протокол Message Integrity Check для проверки целостности сообщений, который блокирует станцию на 60 секунд, если были посланы в течение 60 секунд два сообщения не прошедших проверку целостности. С учётом всех доработок и усовершенствований TKIP все равно не считается криптостойким.

CKIP-шифрование (англ. *Cisco Key Integrity Protocol*)

Имеет сходства с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. *Cisco Message Integrity Check*) для проверки целостности сообщений.

WPA-шифрование

Вместо уязвимого RC4, используется криптостойкий алгоритм шифрования AES (англ. *Advanced Encryption Standard*). Возможно использование EAP (англ. *Extensible Authentication Protocol*, расширяемый протокол аутентификации). Есть два режима:

- Pre-Shared Key (WPA-PSK) — каждый узел вводит пароль для доступа к сети;
- Enterprise — проверка осуществляется серверами RADIUS;

WPA2-шифрование (IEEE 802.11i)

Принят в 2004 году, с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi оборудование. В данном протоколе применяется RSN (англ. *Robust Security Network*, сеть с повышенной безопасностью). Изначально в WPA2 используется протокол CCMP (англ. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. *Extensible Authentication Protocol*) с некоторыми его дополнениями. Как и в WPA есть два режима работы: Pre-Shared Key и Enterprise.

WPA и WPA2 имеют следующие преимущества:

- ключи шифрования генерируются во время соединения, а не распределяются статически.
- для контроля целостности передаваемых сообщений используется алгоритм Michael.
- используется вектор инициализации существенно большей длины.

1.6 Атаки на Wi-Fi сети

Разведка

Большинство атак начинаются с разведки, в ходе которой производится сканирование сети (NetStumbler, Wellenreiter), сбор и анализ пакетов — многие служебные пакеты в сети Wi-Fi передаются в открытом виде. При этом крайне проблематично выяснить, кто легальный пользователь, пытающийся подключиться к сети, а кто собирает информацию. После разведки принимаются решения о дальнейших шагах атаки.

Защита сети с помощью отключения ответа на широковещательный запрос ESSID и скрытия название сети в служебных пакетах Beacon frame является недостаточной, так как сеть всё равно видна на определённом радиоканале и атакующий просто ждёт авторизованного подключения к сети, так как при этом в незашифрованном виде передаётся ESSID. На этом защитная мера теряет смысл. Хуже того, некоторые системы (например WinXp Sp2) непрерывно рассылают имя сети в эфир, пытаясь подключиться. Это также является интересной атакой, так как в таком случае можно пересадить пользователя на свою точку доступа и получать всю информацию, что он передаёт по сети.

Можно уменьшить подверженность разведке, разместив точку доступа так, чтобы она обеспечивала необходимое покрытие, и это покрытие минимально выходило за контролируемую территорию. Нужно регулировать мощность точки доступа и использовать специальные инструменты для контроля распространения сигнала. Также можно полностью экранировать помещение с точкой доступа для полной невидимости сети извне.

Hardware

В случае анализа небольшой территории подойдёт встроенный Wi-Fi адаптер ноутбука, но на большее не хватит. Нужен более мощный адаптер с разъёмом для внешней антенны. Многие используют такие, как Alfa networks AWUS036H, Ubiquiti SRC, Linksys WUSB54GC.

Антенна

Существуют антенны направленные и всенаправленные. Первые имеют большую дальность при таком же коэффициенте усиления, но меньший угол работы и больше подходят для изучения ограниченной территории. Вторые имеют худшие

характеристики, но больше подходят для сбора информации с обширной территории. Для целей сбора информации подойдут антенны с коэффициентом усиления 7-9 dbi.

GPS

При сборе информации будет нелишним наносить на карту координаты найденных и изучаемых точках доступа. Для этого потребуется GPS, неважно, подключаемые ли к компьютеру внешние GPS-приёмники или смартфон с встроенным GPS. Важно лишь чтобы такой девайс мог передавать данные по протоколу nmea или garmin.

Программное обеспечение

В Linux-подобных системах настроить работу адаптера на приём всех пакетов, а не только тех, которые предназначены именно ему проще, чем на Windows. В некоторых драйверах такой режим поддерживается изначально, другие нужно изменять.
Наиболее распространённые программы для сбора информации — это Kismet и Aircrack-ng suite.
Kismet может не только перехватывать пакеты и обнаруживать скрытые сети, это также и инструмент для мониторинга и отладки сети, причём не только Wi-Fi, программа может работать с телефонными и Bluetooth сетями.
Aircrack-NG представляет собой набор инструментов для аудита беспроводных сетей. А ещё в эта программа реализует стандартную атаку FMS наряду с некоторыми оптимизациями KoreK’a, также новую PTW-атаку, которая ещё сильнее уменьшает время на взлом WEP.
Другие программы: Dwepcrack (улучшенная FMS атака), AirSnot (FMS), WepLab (улучшенная FMS атака, атака Koreka).

Атаки на сети с WEP-шифрованием

Объясняются уязвимостью RC4, в любой из такого рода атак, необходимо получить какое-то количество пакетов из сети.
1. **FMS-атака (Fluhrer, Martin, Shamir)** — самая первая атака на сети с WEP-шифрованием, появилась в 2001 году. Основана на анализе передаваемых векторов инициализации и требует, чтобы пакеты содержали «слабые» инициализационные вектора (Weak IV). Для проведения атаки нужно как минимум полмиллиона пакетов. После обновления протокола эта атака неуспешна.

2. **Атака KOREK'A (ник хакера, придумавшего атаку).** Количество требуемых уникальных IV — несколько сотен тысяч, для ключа длиной 128 бит. Главное требование — чтобы IV не совпадали между собой. Абсолютно не важно наличие слабых IV. Атака была предложена в 2004 году.
3. **PTW-атака (Pyshkin, Tews, Weinmann).** В основе лежит прослушивание большого количества ARP-пакетов (англ. *Address Resolution Protocol*). Достаточно 10000-100000 пакетов. Самая эффективная атака на сеть с WEP-шифрованием. Данную атаку можно вычислить по большому количеству ARP-пакетов, которые генерируются в сеть. Единственный минус — почти всегда требуется проводить активную атаку на беспроводную сеть, так как ARP-запросы при нормальном функционировании сети никогда не сыпятся как из «рога изобилия».
Атаки на протокол WEP условно можно разделить на активные и пассивные.

Пассивные сетевые атаки
В 2001 году криптоаналитики Флурер (Fluhrer), Мантин (Mantin) и Шамир (Shamir) показали, что можно вычислить секретный ключ на основе определённых кадров, собранных в сети. Причина — уязвимость метода планирования ключей (Key Scheduling Algorithm — KSA) алгоритма шифрования RC4. Слабые векторы инициализации позволяют с помощью статистического анализа восстановить секретный ключ. Требуется собрать около 4 миллионов кадров, это около 4 часов работы сети. Взломаны как 40-битные, так и 104-битные ключи, причём защищённость ключа не возросла.

Активные сетевые атаки
Нарушитель воздействует на сеть для получения определенной информации для индуктивного вычисления секретного ключа. В основе активной атаки WEP лежит то, что при потоковом шифровании происходит XOR первоначального сообщения и ключа для вычисления зашифрованного сообщения.
Индуктивное вычисление ключа эффективно в силу отсутствия хорошего метода контроля целостности сообщений. Значение идентификатора ключа (ICV), завершающего кадр WEP, вычисляется с помощью функции CRC32 (циклический избыточный 32-битный код), подверженной атакам с манипуляцией битами. В итоге существуют атаки, основанные на повторном использовании вектора инициализации (IV Replay) и манипуляции битами (Bit-Flipping).

Повторное использование вектора инициализации (Initialization Vector Replay Attacks)

1.Злоумышленник многократно посылает клиенту Wi-Fi сети по проводной сети сообщение известного содержания (IP-пакет, письмо по электронной почте и т. п.).
2.Злоумышленник пассивно прослушивает радиоканал связи абонента с точкой доступа и собирает кадры, вероятно содержащие шифрованное сообщение.
3.Злоумышленник вычисляет ключевую последовательность, применяя XOR к предполагаемому шифрованному и известному нешифрованному сообщениям.
4.Далее злоумышленник «выращивает» ключевую последовательность для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.
Пара вектора инициализации и секретного ключа, а следовательно и порождаемая ими ключевая последовательность может использоваться повторно.

После того, как ключевая последовательность вычислена для кадров некоторой длины, её можно «вырастить» до любого размера:

1.Злоумышленник генерирует кадр на один байт длиннее, чем длина уже известной ключевой последовательности. Пакеты ICMP (Internet Control Message Protocol), посылаемые командой ping, отлично подходят для этого, так как точка доступа вынуждена на них отвечать.
2.Злоумышленник увеличивает длину ключевой последовательности на один байт.
3.Значение дополнительного байта выбирается случайным образом из 256 возможных ASCII-символов.
4.Если предполагаемое значение дополнительного байта ключевой последовательности верно, то будет получен ожидаемый ответ от точки доступа (ICMP в случае ping’a)
5.Процесс повторяется до тех пор, пока не будет подобрана ключевая последовательность нужной длины.

Манипуляция битами (Bit-Flipping Attacks)

Преследуется та же цель, что и при использовании вектора инициализации. Идея в том, что многое служебные поля и их положение в кадре не меняются. Злоумышленник меняет биты пользовательских данных в кадре на канальном уровне (модель OSI), тем самым изменяя пакеты на сетевом уровне.

1.Злоумышленник пассивно собирает кадры Wi-Fi-сети анализаторами трафика.
2.Злоумышленник захватывает кадр и произвольно изменяет биты в поле данных протокола 3-го уровня.
3.Злоумышленник модифицирует значение вектора контроля целостности кадра ICV (описано ниже).
4.Злоумышленник передает модифицированный кадр в Wi-Fi-сеть.
5.Принимающая сторона (абонент либо точка доступа) вычисляет значение вектора контроля целостности кадра ICV для полученного модифицированного кадра.

6.Принимающая сторона сравнивает вычисленное значение вектора ICV с имеющимся в полученном модифицированном кадре.
7.Если значения ICV совпадают, кадр считается неискаженным и не отбрасывается.
8.Принимающая сторона деинкапсулирует содержимое кадра и обрабатывает заголовки сетевого уровня.
9.Поскольку манипуляция битами происходила на канальном уровне, контрольная сумма пакета сетевого уровня оказывается неверной.
10.Стек протокола сетевого уровня на принимающей стороне генерирует предсказуемое сообщение об ошибке.
11.Злоумышленник наблюдает за сетью в ожидании зашифрованного кадра с сообщением об ошибке.
12.Злоумышленник захватывает кадр, содержащий зашифрованное сообщение об ошибке, и вычисляет ключевую последовательность, как же как в случае атаки с повторным использованием вектора инициализации.

Манипуляция с ICV

Процедура манипуляции с ICV, расположенного в зашифрованной части кадра, для обеспечения его корректности для модифицированного кадра.

1.Исходный кадр F1 имеет вектор C1.
2.Создается кадр F2 такой же длины, что и F1, служащий маской для модификации битов кадра F1.
3.Создается кадр F3 путём выполнения двоичной функции XOR над кадрами F1 и F2.
4.Вычисляется промежуточный вектор C2 для кадра F3.
5.Вектор C3 для кадра F3 вычисляется путём выполнения двоичной функции XOR над C1 и C2.

Проблемы управления статическими WEP-ключами

Ещё один недостаток — нельзя управлять ключами шифрования. В WEP поддерживаются только статические ключи, и их нужно заранее распространять между клиентами и точками доступа. Протокол 802.11 аутентифицирует не пользователя, а его устройство, и потеря последнего, или разглашение ключа приводит к том, что нужно менять ключи у всех абонентов и на всех точках доступа в сети. Вручную. В небольшой локальной сети это ещё реально, но не более. Требуется тщательно следить за оборудованием сети и не допускать утечек ключей.

Атаки на сети с WPA/WPA2-шифрованием

WPA обычно использует алгоритм шифрования TKIP. WPA2 в обязательном порядке использует алгоритм шифрования AES-CCMP, который более мощный и

надежный по сравнению с TKIP. Считается, что взлом WPA2 практически неосуществим.

WPA и WPA2 позволяют использовать либо EAP-based аутентификацию (RADIUS Server «Enterprise») или Pre-Shared Key (PSK) «Personal»-based аутентификацию.

Были проведены только атаки на аутентификацию обоих методов шифрования, после чего методом грубой силы можно подобрать PSK-ключ. Скорость перебора можно увеличить, если заранее вычислить необходимые данные и составить таблицы для перебора. Однако, если для аутентификации используется технология WPS, использующая PIN-код, то атака сводится к перебору всех возможных кодов.

6 ноября 2008 года на конференции PacSec было показано, как взломать ключ TKIP, используемый в WPA, за 12-15 минут. Этот метод позволяет прочитать данные, передаваемые от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. Ещё одним условием успешной атаки было включение QoS на маршрутизаторе.

В 2009 году сотрудниками Университета Хиросимы и Университета Кобе, Тосихиру Оигаси и Масакату Мории был разработан и успешно реализован на практике новый метод атаки, который позволяет взломать любое WPA соединение без ограничений, причём, в лучшем случае, время взлома составляет 1 минуту.

WPA с включённым AES и WPA2 не подвержены этим атакам.

23 июля 2010 года была опубликована информация об уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ. Никакого взлома ключей или брут-форса не требуется.

На сегодня основными методами взлома WPA2 PSK являются атака по словарю и метод грубой силы.

Атака по словарю на WPA/WPA2 PSK

WPA/WPA2 PSK работает следующим образом: он вытекает из ключа предварительной сессии, которая называется Pairwise Transient Key (PTK). PTK, в свою очередь использует Pre-Shared Key и пять других параметров — SSID, Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адрес точки доступа) и Suppliant MAC-address (MAC-адрес wifi-клиента). Этот ключ в дальнейшем использует шифрование между точкой доступа (AP) и WiFi-клиентом.

Злоумышленник, который в этот момент времени прослушивает эфир, может перехватить все пять параметров. Единственной вещью, которой не владеет злодей это — Pre-Shared key. Pre-Shared key получается благодаря использованию парольной

фразы WPA-PSK, которую отправляет пользователь, вместе с SSID. Комбинация этих двух параметров пересылается через Password Based Key Derivation Function (PBKDF2), которая выводит 256-bit'овый общий ключ. В обычной WPA/WPA2 PSK атаке по словарю, злоумышленник будет использовать ПО, которое выводит 256-битный Pre-Shared Key для каждой парольной фразы и будет использует её с другими параметрами, которые были описаны в создании PTK. PTK будет использоваться для проверки Message Integrity Check (MIC) в одном из пакетов handshake. Если они совпадут, то парольная фраза в словаре будет верной. При этом используются уязвимости протокола аутентификации пользователей — открытая передача ANounce, SNounce, MAC-адреса точки доступа и MAC-адреса WiFi-клиента. Если при воспроизведении алгоритма аутентификации произойдет «успешная авторизация пользователя», значит выбранный из словаря пароль является истинным и атака привела к успешному взлому сети.

Сообщения 4 стороннего рукопожатия (4 кадра канального уровня) содержат в себе информационные поля следующего содержимого:

1.MAC-адрес точки доступа;
2.MAC-адрес клиента;
3.Случайное 32-байтное число, генерируемое точкой доступа при установлении соединения (Anonce) — кадр I;
4.Случайное 32-байтное число, генерируемое клиентом (Snonce) — кадр II;
5.Размер текущего кадра аутентификации (без канального заголовка) — кадр II или III или IV;
6.Содержимое кадра аутентификации (без канального заголовка) — обязательно тот же, кадр, что выбран в предыдущем пункте;
7.Ключ целостности сообщения (MIC) — обязательно тот же, кадр, что выбран в предыдущем пункте;
8.Версия протокола защиты данных (WPA или WPA2) — фрейм II или III или IV.

1.7 WiMAX

WiMAX (англ. *Worldwide Interoperability for Microwave Access*) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN и был согласован).

Название «WiMAX» было создано WiMAX Forum — организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным телефонным линиям и DSL». Максимальная скорость — до 1 Гбит/сек на ячейку.

Область использования

WiMAX подходит для решения следующих задач:

- Соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета.
- Обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и DSL.
- Предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг.
- Создания точек доступа, не привязанных к географическому положению.
- Создания систем удалённого мониторинга (monitoring системы), как это имеет место в системе SCADA.

WiMAX позволяет осуществлять доступ в Интернет на высоких скоростях, с гораздо большим покрытием, чем у Wi-Fi-сетей. Это позволяет использовать технологию в качестве «магистральных каналов», продолжением которых выступают традиционные DSL- и выделенные линии, а также локальные сети. В результате подобный подход позволяет создавать масштабируемые высокоскоростные сети в рамках городов.

Целесообразность использования WiMAX как технологии доступа

Проблема последней мили всегда была актуальной задачей для связистов. К настоящему времени появилось множество технологий последней мили, и перед любым оператором связи стоит задача выбора технологии, оптимально решающей задачу

доставки любого вида трафика своим абонентам. Универсального решения этой задачи не существует, у каждой технологии есть своя область применения, свои преимущества и недостатки. На выбор того или иного технологического решения влияет ряд факторов, в том числе:

- стратегия оператора, целевая аудитория, предлагаемые в настоящее время и планируемые к предоставлению услуги,
- размер инвестиций в развитие сети и срок их окупаемости,
- уже имеющаяся сетевая инфраструктура, ресурсы для её поддержания в работоспособном состоянии,
- время, необходимое для запуска сети и начала оказания услуг.

У каждого из этих факторов есть свой вес, и выбор той или иной технологии принимается с учётом всех их в совокупности.

Фиксированный и мобильный вариант WiMAX

Набор преимуществ присущ всему семейству WiMAX, однако его версии существенно отличаются друг от друга. Разработчики стандарта искали оптимальные решения как для фиксированного, так и для мобильного применения, но совместить все требования в рамках одного стандарта не удалось. Хотя ряд базовых требований совпадает, нацеленность технологий на разные рыночные ниши привела к созданию двух отдельных версий стандарта (вернее, их можно считать двумя разными стандартами). Каждая из спецификаций WiMAX определяет свои рабочие диапазоны частот, ширину полосы пропускания, мощность излучения, методы передачи и доступа, способы кодирования и модуляции сигнала, принципы повторного использования радиочастот и прочие показатели. А потому WiMAX-системы, основанные на версиях стандарта IEEE 802.16 e и d, практически несовместимы. Краткие характеристики каждой из версий приведены ниже.

802.16-2004 (известен также как 802.16d, фиксированный WiMAX и WiMAXpre). Спецификация утверждена в 2004 году. Используется ортогональное частотное мультиплексирование (OFDM), поддерживается фиксированный доступ в зонах с наличием либо отсутствием прямой видимости. Пользовательские устройства представляют собой стационарные модемы для установки вне и внутри помещений, а также PCMCIA-карты для ноутбуков. В большинстве стран под эту технологию отведены диапазоны 3,5 и 5 ГГц. По сведениям WiMAX Forum, насчитывается уже порядка 175 внедрений фиксированной версии. Многие аналитики видят в ней конкурирующую или взаимодополняющую технологию проводного широкополосного доступа DSL.

802.16-2005 (известен также как 802.16e и мобильный WiMAX). Спецификация утверждена в 2005 году. Это — новый виток развития технологии фиксированного доступа (802.16d). Оптимизированная для поддержки мобильных пользователей версия поддерживает ряд специфических функций, таких как хэндовер, *idle mode* и роуминг. Применяется масштабируемый OFDM-доступ (SOFDMA), возможна работа при наличии либо отсутствии прямой видимости. Планируемые частотные диапазоны для сетей Mobile WiMAX таковы: 2,3-2,5; 2,5-2,7; 3,4-3,8 ГГц. В мире реализованы несколько пилотных проектов, в том числе первым в России свою сеть развернул «Скартел». В Казахстане реализован проект FlyNet (flynet.kz). Конкурентами 802.16e являются все мобильные технологии третьего поколения (например, EV-DO, HSDPA).

Основное различие двух технологий состоит в том, что фиксированный WiMAX позволяет обслуживать только «статичных» абонентов, а мобильный ориентирован на работу с пользователями, передвигающимися со скоростью до 150 км/ч. Мобильность означает наличие функций роуминга и «бесшовного» переключения между базовыми станциями при передвижении абонента (как происходит в сетях сотовой связи). В частном случае мобильный WiMAX может применяться и для обслуживания фиксированных пользователей.

Широкополосный доступ

Многие телекоммуникационные компании делают большие ставки на использование WiMAX для предоставления услуг высокоскоростной связи. И тому есть несколько причин.

Во-первых, технологии семейства 802.16 позволят экономически более эффективно (по сравнению с проводными технологиями) не только предоставлять доступ в сеть новым клиентам, но и расширять спектр услуг и охватывать новые труднодоступные территории.

Во-вторых, беспроводные технологии многим более просты в использовании, чем традиционные проводные каналы. WiMAX и Wi-Fi сети просты в развёртывании и по мере необходимости легко масштабируемы. Этот фактор оказывается очень полезным, когда необходимо развернуть большую сеть в кратчайшие сроки. К примеру, WiMAX был использован для того, чтобы предоставить доступ в Сеть выжившим после цунами, произошедшего в декабре 2004 года в Индонезии (Aceh). Вся коммуникационная инфраструктура области была выведена из строя и требовалось оперативное восстановление услуг связи для всего региона.

В сумме все эти преимущества позволят снизить цены на предоставление услуг высокоскоростного доступа в Интернет как для бизнес-структур, так и для частных лиц.

Пользовательское оборудование

Оборудование для использования сетей WiMAX поставляется несколькими производителями и может быть установлено как в помещении (устройства размером с обычный DSL-модем), так и вне его. Следует заметить, что оборудование, рассчитанное на размещение внутри помещений и не требующее профессиональных навыков, при установке, конечно, более удобно, однако способно работать на значительно меньших расстояниях от базовой станции, чем профессионально установленные внешние устройства. Поэтому оборудование, установленное внутри помещений, требует намного больших инвестиций в развитие инфраструктуры сети, так как подразумевает использование намного большего числа точек доступа.

С изобретением мобильного WiMAX всё больший акцент делается на разработке мобильных устройств. В том числе специальных телефонных трубок (похожих на обычный мобильный смартфон), и компьютерной периферии (USB радиомодулей и PC card).

1.8 Принцип работы WiMAX

Основные понятия

В общем виде WiMAX сети состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом.

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется обеспечения прямой видимости между базовой станцией и приёмником.

Как уже говорилось выше, WiMAX применяется как для решения проблемы «последней мили», так и для предоставления доступа в сеть офисным и районным сетям.

Между базовыми станциями устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 140 Мбит/с. При этом, по крайней мере одна базовая станция подключается к сети провайдера с использованием классических проводных соединений. Однако, чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надёжность сети в целом.

Структура сетей семейства стандартов IEEE 802.16 имеет схожесть с традиционными GSM сетями (базовые станции действуют на расстояниях до десятков километров, для их установки не обязательно строить вышки — допускается установка на крышах домов при соблюдении условия прямой видимости между станциями).

MAC / канальный уровень

В Wi-Fi сетях все пользовательские станции, которые хотят передать информацию через точку доступа (AP), соревнуются за «внимание» последней. Такой подход может вызвать ситуацию, при которой связь для более удалённых станций будет постоянно обрываться в пользу более близких станций. Подобное положение вещей делает затруднительным использование таких сервисов, как Voice over IP (VoIP), которые очень сильно зависят от непрерывного соединения.

Что же касается сетей 802.16, в них MAC использует алгоритм планирования. Любой пользовательской станции стоит лишь подключиться к точке доступа, для неё будет создан выделенный слот на точке доступа, недоступный другим пользователям.

Архитектура

WiMAX Forum разработал архитектуру, которая определяет множество аспектов работы WiMAX сетей: взаимодействия с другими сетями, распределение сетевых адресов, аутентификация и многое другое.

- SS/MS: (the Subscriber Station/Mobile Station)
- ASN: (the Access Service Network)
- BS: (Base station), базовая станция, часть ASN
- ASN-GW: (the ASN Gateway), шлюз, часть ASN
- CSN: (the Connectivity Service Network)
- HA: (Home Agent, часть CSN)
- NAP:(a Network Access Provider)
- NSP: (a Network Service Provider)

ASN (Access Service Network) — сеть доступа.
ASN Gateway — предназначен для объединения трафика и сообщений сигнализации от базовых станций и дальнейшей их передачи в сеть CSN.
BS (Base Station) — базовая станция. Основной задачей является установление, поддержание и разъединение радиосоединений. Кроме того, выполняет обработку сигнализации, а также распределение ресурсов среди абонентов.
CSN (Connectivity Service Network) — сеть обеспечения услуг.
HA (Home Agent) — элемент сети, отвечающий за возможность роуминга. Кроме того, обеспечивает обмен данными между сетями различных операторов.
Следует заметить, что архитектура сетей WiMax не привязана к какой-либо определённой конфигурации, обладает высокой гибкостью и масштабируемостью.

1.9 Bluetooth

Bluetooth - это технология беспроводной связи. То есть передача данных осуществляется по радиоканалам. Блютуз позволяет создавать беспроводное соединение между устройствами, благодаря которому вы можете передавать абсолютно любую информацию. Более того, данная технология позволяет удаленно управлять устройствами и создавать голосовую связь. Это позволяет использовать беспроводные наушники, гарнитуру, а также удаленно управлять принтерами, сканерами и так далее.

Принцип действия Bluetooth

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (англ. *Industry, Science and Medicine*), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4-2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (англ. *Frequency Hopping Spread Spectrum, FHSS*). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорогое.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приёмнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «point-to-point», но и соединение «point-to-multipoint».

1.10 Спецификации Bluetooth

Bluetooth 1.0
Первая версия несла множество недостатков в плане совместимости устройств разных производителей. К тому же была обязательна передача адреса устройства (**BD_ADDR**), которая ставила под угрозу анонимность и безопасность.

Bluetooth 1.1
Добавлена поддержка не шифрованных каналов и **RSSI** (индикация уровня сигнала).

Bluetooth 2.0
Представлен в **начале 2007** года
Основным нововведением была опциональная поддержка **EDR** (*Enhanced Data Rate*), для увеличения скорости передачи данных (в среднем **2.0-2.3 Мбит/сек**). Так же было добавлено несколько улучшений увеличивающих стабильность передачи данных, безопасность и совместимость.

Bluetooth 2.1
Представлен в **августе 2007** года
Добавлена энергосберегающая технология (*Sniff Subrating*) уменьшающая энергопотребление в несколько раз. Улучшена безопасность и скорость идентификации устройств. Также появилась возможность обновления ключа шифрования без разрыва соединения.

Bluetooth 3.0 + HS
Представлен в **Апреле 2009** года
Появилась **AMP** (*Asymmetry Multiprocessing Programming*) — высокоскоростное дополнение к **802.11**Скорость передачи данных увеличилась вплоть до **24Мбит/сек**. Является отдельной технологией, которая потребляет больше энергии. Поэтому производители ставят на свои устройства 2 стандарта (2.0 для нетребовательных к скорости операций и **3.0** для больших объёмов).

Bluetooth 4.0
Представлен в **декабре 2009** года
Главной особенностью является очень маленького потребление энергии, благодаря непостоянной передаче сигнала. Приёмник находится наготове и включается

только тогда, когда ему подаётся сигнал с другого устройства, в остальное время он бездействует. Скорость установлений соединения – **5мс**, расстояние до **100м**, скорость ~ **1Мбит**, отличную безопасность благодаря шифрованию **128 бит AES**. Активно рекламируется для спортивного оборудования, всевозможных датчиков.

1.11 Профили Bluetooth

Профиль — набор функций или возможностей, доступных для определённого устройства Bluetooth. Для совместной работы Bluetooth-устройств необходимо, чтобы все они поддерживали общий профиль.

Нижеуказанные профили определены и одобрены группой разработки Bluetooth SIG:

- *Advanced Audio Distribution Profile* (A2DP) — разработан для передачи двухканального стерео аудиопотока, например, музыки, к беспроводной гарнитуре или любому другому устройству. Профиль полностью поддерживает низкокомпрессированный кодек Sub_Band_Codec (SBC) и опционально поддерживает MPEG-1,2 аудио, MPEG-2,4 AAC и ATRAC, способен поддерживать кодеки, определённые производителем.
- *Audio / Video Remote Control Profile* (AVRCP) — разработан для управления стандартными функциями телевизоров, Hi-Fi оборудования и прочего. То есть позволяет создавать устройства с функциями дистанционного управления. Может использоваться в связке с профилями A2DP или VDPT.
- *Basic Imaging Profile* (BIP) — разработан для пересылки изображений между устройствами и включает возможность изменения размера изображения и конвертирование в поддерживаемый формат принимающего устройства.
- *Basic Printing Profile* (BPP) — позволяет пересылать текст, сообщения электронной почты, vCard и другие элементы на принтер. Профиль не требует от принтера специфических драйверов, что выгодно отличает его от HCRP.
- *Common ISDN Access Profile* (CIP) — для доступа устройств к ISDN.
- *Cordless Telephony Profile* (CTP) — профиль беспроводной телефонии.
- *Device ID Profile* (DIP) — позволяет идентифицировать класс устройства, производителя, версию продукта.
- *Dial-up Networking Profile* (DUN) — протокол предоставляет стандартный доступ к Интернету или другому телефонному сервису через Bluetooth. Базируется на SPP, включает в себя команды PPP и AT, определённые в спецификации ETSI 07.07.
- *Fax Profile* (FAX) — предоставляет интерфейс между мобильным или стационарным телефоном и ПК, на котором установлено программное обеспечение для факсов. Поддерживает набор AT-команд в стиле ITU T.31 и/или ITU T.32. Голосовой звонок или передача данных профилем не поддерживается.

- *File Transfer Profile* (FTP_profile) — обеспечивает доступ к файловой системе устройства. Включает стандартный набор команд FTP, позволяющий получать список директорий, изменения директорий, получать, передавать и удалять файлы. В качестве транспорта используется OBEX, базируется на GOEP.
- *General Audio / Video Distribution Profile* (GAVDP) — база для A2DP и VDP.
- Generic Access Profile (GAP) — база для всех остальных профилей.
- *Generic Object Exchange Profile* (GOEP) — база для других профилей передачи данных, базируется на OBEX.
- *Hard Copy Cable Replacement Profile* (HCRP) — предоставляет простую альтернативу кабельного соединения между устройством и принтером. Минус профиля в том, что для принтера необходимы специфичные драйвера, что делает профиль неуниверсальным.
- *Hands-Free Profile* (HFP) — используется для соединения беспроводной гарнитуры и телефона, передаёт монозвук в одном канале.
- *Human Interface Device Profile* (HID) — обеспечивает поддержку устройств с HID (Human Interface Device), таких как мыши, джойстики, клавиатуры и проч. Использует медленный канал, работает на пониженной мощности.
- *Headset Profile* (HSP) — используется для соединения беспроводной гарнитуры (Headset) и телефона. Поддерживает минимальный набор AT-команд спецификации GSM 07.07 для обеспечения возможности совершать звонки, отвечать на звонки, завершать звонок, настраивать громкость. Через профиль Headset, при наличии Bluetooth 1.2 и выше, можно выводить на гарнитуру всё звуковое сопровождение работы телефона. Например, прослушивать на гарнитуре все сигналы подтверждения операций, mp3-музыку из плеера, мелодии звонка, звуковой ряд видеороликов. Гарнитуры, поддерживающие такой профиль, имеют возможность передачи стереозвука, в отличие от моделей, которые поддерживают только профиль Hands-Free.
- *Intercom Profile* (ICP) — обеспечивает голосовые звонки между Bluetooth-совместимыми устройствами.
- *LAN Access Profile* (LAP) — обеспечивает доступ Bluetooth-устройствам к вычислительным сетям LAN, WAN или Интернет посредством другого Bluetooth-устройства, которое имеет физическое подключение к этим сетям. Bluetooth-устройство использует PPP поверх RFCOMM для установки соединения. LAP также допускает создание ad-hoc Bluetooth-сетей.
- *Object Push Profile* (OPP) — базовый профиль для пересылки «объектов», таких как изображения, виртуальные визитные карточки и др. Передачу данных инициирует отправляющее устройство (клиент), а не приёмное (сервер).

- *Personal Area Networking Profile* (PAN) — позволяет использовать протокол Bluetooth Network Encapsulation в качестве транспорта через Bluetooth-соединение.
- *Phone Book Access Profile* (PBAP) — позволяет обмениваться записями телефонных книг между устройствами.
- *Serial Port Profile* (SPP) — базируется на спецификации ETSI TS07.10 и использует протокол RFCOMM. Профиль эмулирует последовательный порт, предоставляя возможность замены стандартного RS-232 беспроводным соединением. Является базовым для профилей DUN, FAX, HSP и AVRCP.
- *Service Discovery Application Profile* (SDAP) — используется для предоставления информации о профилях, которые использует устройство-сервер.
- *SIM Access Profile* (SAP, SIM) — позволяет получить доступ к SIM-карте телефона, что позволяет использовать одну SIM-карту для нескольких устройств.
- *Synchronisation Profile* (SYNCH) — позволяет синхронизировать персональные данные (PIM). Профиль заимствован из спецификации инфракрасной связи и адаптирован группой Bluetooth SIG.
- *Video Distribution Profile* (VDP) — позволяет передавать потоковое видео. Поддерживает H.263, стандарты MPEG-4 Visual Simple Profile, H.263 profiles 3, profile 8 поддерживаются опционально и не содержатся в спецификации.
- *Wireless Application Protocol Bearer* (WAPB) — протокол для организации P-to-P (Point-to-Point) соединения через Bluetooth.

1.12 Атаки на Bluetooth

BlueBug

Данный вид атаки позволяет получить доступ к выполнению AT-команд на сотовом телефоне, что может привести к чтению и отправке СМС, полному доступу к телефонной книге, и многому другому. Возможности атаки почти ничем не ограничены. Так например, у автора, в образовательных целях естественно, получилось скачать с одного из телефонов всю записную книгу, все смс, установить на нём переадресацию входящих вызовов и заставить набрать номер телефона техподдержки оператора.

Полный список всех возможностей этого вида атаки займёт не один килобайт текста и ограничен лишь фантазией и познаниями атакующего.

BlueSmack

Принцип этой атаки стар как windows 95. Неудивительно, ведь в те времена эта атака называлась Ping of Death и предназначалась <счастливым> пользователям windows 95. С тех пор много воды утекло, однако принцип атаки остался. В результате если отправить длинный пакет, например с помощью утилиты l2ping, входящей в состав пакета BlueZ, то целевое устройство может <повиснуть> или самопроизвольно перезагрузиться.

Как защититься

Пользователям старых устройств опять же поможет смена ОС, современные устройства к атаке невосприимчивы.

BlueSnarf

Пожалуй, самая популярная атака на устройства bluetooth.

В этой атаке, впервые представленной публике в 2003 году, используется сервис OPP (OBEX Push Profile), который используется для упрощенного обмена <визитками> и прочими файлами, и при нормальных обстоятельствах работает вполне стабильно. Однако чаще всего для доступа к этому сервису не требутся авторизация, что, кстати тоже не является проблемой. Главная проблема состоит в том, что если прошивка написана не совсем верно, атакующий может скачать любой существующий файл командой GET, а это может быть например '/telecom/pb.vcf' (в этом файле хранится телефонная книга устройства).

Bluesnarf++

Развитие идеи bluesnarf, позволяющее получить полный (RW) доступ к файловой системе устройства, включая карты памяти, виртуальные и RAM диски и т.п. Вместо малофункционального OPP используется OBEX FTP (со всеми возможностями протокола FTP), к которому можно подключиться без авторизации.

Уязвимые устройства
Многие Siemens, Samsung, SonyEricsson, и т.п. Nokia не восприимчивы к этой атаке.

Как защититься
Авторизация, не принимать подозрительные соединения, обновить прошивку.

HeloMoto

Как можно понять из названия, атака затрагивает телефоны Motorola. Суть в следующем: атакующий соединяется с сервисом OPP жертвы (не требуется авторизация), имитирует посылку <визитки> и разрывает соединение, не закончив его. В результате, в списке <доверенных устройств> жертвы появляется телефон атакующего, что даёт возможность соединиться с сервисом гарнитуры (Headset) и выполнять AT-команды (Атака BlueBug).

Поскольку на телефонах Motorola максимальная длительность нахождения Bluetooth в режиме обнаружения составляет всего 60 секунд, владельцам можно не беспокоиться. Шанса встретить хакера в момент уязвимости телефона практически нет.

BlueDump (Re-Pairing attack)

Эта достаточно серьёзная атака основана на методе <подделки> BT-MAC адреса с целью получить привелегии настоящего обладателя MAC. Лучше всего пояснить на примере.

Допустим, есть 3 устройсва с Bluetooth - 2 из них находятся в доверительных отношениях, третье - устройство злоумышленика. Если злоумышленик знает MAC адреса прервых двух устройств, ему достаточно дождаться выхода одного из устройств из зоны действия, присвоить себе его MAC и инициировать повторное <спаривание> с оставшимся устройством. Это становится возможным из-за того, что одно из устройств может <забыть> link key, которым шифруется передача данных и запросить его повторную генерацию.

Уязвимые устройства
Все устройства bluetooth.

Как защититься
Никак. На данный момент эта уязвимость неизлечима. Однако, не всё так плохо - ведь без знания адреса доверенного устройства злоумышленик не сможет ничего сделать - перебрать все возможные адреса за небольшой промежуток времени невозможно.

CarWhisperer

Атака на автомобильные магнитолы с bluetooth, которая становится возможной из-за использования производителем стандартного и, как правило, неизменяемого pin-кода вроде 0000 или 1234.

Соединение происходит совершенно прозрачно для владельца автомобиля, после чего телефон(кпк/ноутбук:) работает с магнитолой как с обычной гарнитурой.

DoS атаки с использованием bss (bluetooth stack smasher)

Этот тип атак использует неправильно сформированные L2CAP пакеты для выключения/зависания/перезагрузки атакуемого устройства. С различными параметрами уязвимы следующие устройства: Nokia N70, SonyEricsson T68i, W800i, K600i и другие модели.
Защититься от такой атаки пока невозможно, в будущем скорее всего поможет смена прошивки.

1.13 UWB

UWB (англ. *Ultra-Wide Band*, сверхширокая полоса) — это беспроводная технология связи на малых расстояниях при низких затратах энергии, использующая в качестве несущей сверхширокополосные сигналы с крайне низкой спектральной плотностью мощности.

Для безлицензионного использования сверхширокополосных сигналов в Российской Федерации выделены диапазоны от 2,85—10,6 ГГц[1], в США 3,1—10,6 ГГц, в Евросоюзе 6—8 ГГц. При этом спектральная плотность мощности СШП приемопередатчика при работе в помещении не должна превышать −47…−45 дБм/МГц (−41,3 дБм/МГц в США и Евросоюзе).

Использование сверхширокой полосы частот (не менее 500 МГц) позволяет UWB достичь скорости передачи до 480 Мбит/с на расстоянии до 3 м. На расстояниях до 10 м технология позволяет достичь лишь 110 Мбит/с.

Особенности технологии UWB:

- Большая скорость передачи информации;
- Высокая помехозащищенность;
- Высокая электромагнитная совместимость;
- Устойчивость связи в условиях многолучевого распространения радиоволн;
- Высокая степень защиты связи от перехвата;
- Способность легко проникать через препятствия;
- Техническая простота аппаратуры и ее дешевизна.

1.14 Использование UWB в системе RealTrac

RealTrac PDS (Proximity Detection System) – это система предотвращения сближения с небезопасными объектами и выдачи предупреждения персоналу о возникновении опасных ситуаций.

Созданное решение может быть использовано в строительстве, производстве, горной добыче и других областях: везде, где используется крупногабаритная техника с ограниченными условиями обзора или другие опасные для сближения объекты.

Конструктивно система RealTrac PDS состоит из двух компонент:

1) **RealTrac Vehicle Tag** (метка, устанавливаемая на опасный для сближения объект)
Метка обеспечивает определение местоположения транспорта или другого небезопасного для сближения объекта и передачу координат на сервер.

2) **RealTrac Tag** (метка, носимая персоналом).
Мобильное радио-устройство, обеспечивающее измерение расстояний до стационарных и мобильных объектов, и позволяющее определять местонахождение человека.

Система производит измерение расстояний с использованием двух радиостандартов:

1. IEEE 802.15.4a CSS (Chirp Spread Spectrum), 2,4 ГГц, на расстояниях от 20 до 400 метров, точность измерения расстояний – 1-3 метра
2. IEEE 802.15.4a UWB (Ultra Wide Band), 6.0 – 7.0 ГГц, на расстояниях до 25 метров, точность измерения расстояний 0.5 – 1 метра.

Использование двух радиостандартов на базе устройств обусловлено тем, что технология CSS используется в качестве канала передачи данных и для интеграции в систему локального позиционирования RealTrac; UWB выбран в качестве технологии, позволяющей получить наибольшую точность замеров для данной задачи.

Принцип работы
Vehicle Tag устанавливается на объекте, небезопасном для сближения, и программно конфигурируется согласно специфике решаемой проблемы.

На данный момент Vehicle Tag имеет функциональность, позволяющую хранить в энергонезависимой памяти списки, содержащие информацию относительно политики нахождения определенных меток в запрещенной зоне, размеров этой зоны для каждой метки, состояния внешних интерфейсов подключения и многих других параметров, характерных для каждой задачи.

Устройства Realtrac Tag раздаются персоналу.

По специализированному радиоканалу происходит измерение расстояния между Vehicle Tag и Realtrac Tag, и в случае пересечения опасной зоны, формируется сигнал тревоги: включается сирена, прожектора, производятся различные предупреждения и т.д.

Система может функционировать как автономно, так и в составе системы локального позиционирования RealTrac.

1.5 Использование UWB в технологии Wireless USB

Wireless USB (беспроводной USB) — стандарт беспроводной передачи данных, который разрабатывается группой Wireless USB Promoter Group.

История

В 2005 году анонсирована первая версия Wireless USB, которая предусматривала возможность беспроводного обмена информацией между устройствами на скорости до 480 Мбит/с в радиусе трех метров. При увеличении расстояния до десяти метров, пропускная способность канала связи снижается до 110 Мбит/с.

В 2007 году на рынок вышли первые продукты.

В сентябре 2010 года завершена спецификация Wireless USB 1.1. Предполагает повышение скорости передачи данных, а также поддержку более высоких частот — до 6 ГГц и выше. При разработке большое внимание уделялось повышению энергетической эффективности. Устройства, выполненные в соответствии со спецификацией 1.1, тратят меньше энергии в режиме простоя. Wireless USB 1.1 предусматривает поддержку технологии Near Field Communication (NFC), что упрощает настройку и эксплуатацию Wireless USB-устройств. Сохранена обратная совместимость с существующим оборудованием.

Использование

Wireless USB предназначен в качестве замены для традиционных проводных USB. К типичным подключаемым устройствам относятся: клавиатура, мышь, камера, принтер, внешние накопители и т.д. Wireless USB также может использоваться для простого совместного использования принтеров, которые не имеют стандартный сетевой интерфейс или подключение к серверу печати. Принтер, подключенный к Wireless USB, ведет себя таким образом, как будто он подключен с помощью USB непосредственно к обычному компьютеру. Технология не предназначена для создания компьютерных сетей (хотя теоретически это возможно).

Передача данных

Параметры передачи соответствуют параметрам стандартного USB версии 2.0, но пропускная способность зависит от расстояния между взаимодействующими устройствами. На расстоянии до 3 метров, скорость передачи данных может теоретически достигать 480 Мбит/с (обычной для USB-стандарта). На отдалении в 10

метров — только до 110 Мбит/с (в оптимальных условиях). Wireless USB предназначен для работы в диапазоне частот от 3,1 ГГц до 10,6 ГГц. Передача данных шифруется с помощью AES-128/CCM.

Физический перенос данных основан на беспроводной технологии UWB, разработанной альянсом WiMedia. Эта же технология используется другими стандартами беспроводной передачи данных (Bluetooth, WiNET, ZigBee).

1.16 ZigBee

ZigBee — спецификация сетевых протоколов верхнего уровня — уровня приложений APS (англ. *application support sublayer*) и сетевого уровня NWK, — использующих сервисы нижних уровней — уровня управления доступом к среде MAC и физического уровня PHY, регламентированных стандартом IEEE 802.15.4. ZigBee и IEEE 802.15.4 описывают беспроводные персональные вычислительные сети (WPAN). Спецификация ZigBee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация ZigBee содержит возможность выбора алгоритма маршрутизации, в зависимости от требований приложения и состояния сети, механизм стандартизации приложений — профили приложений, библиотека стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации.

Области применения

Основными областями применения технологии ZigBee являются беспроводные сенсорные сети, автоматизация жилья («Умный дом» и «Интеллектуальное здание»), медицинское оборудование, системы промышленного мониторинга и управления, а также бытовая электроника и «периферия» персональных компьютеров.

Способность к самоорганизации и самовосстановлению, ячеистая (mesh-) топология, защищённость, высокая помехоустойчивость, низкое энергопотребление и отсутствие необходимости получения частотного разрешения делают ZigBee-сеть подходящей основой для беспроводной инфраструктуры систем позиционирования в режиме реального времени (RTLS).

1.17 Описание ZigBee

ZigBee — стандарт для набора высокоуровневых протоколов связи, использующих небольшие, маломощные цифровые трансиверы, основанный на стандарте IEEE 802.15.4-2006 для беспроводных персональных сетей, таких как, например, беспроводные наушники, соединённые с мобильными телефонами посредством радиоволн коротковолнового диапазона. Технология определяется спецификацией ZigBee, разработанной с намерением быть проще и дешевле, чем остальные персональные сети, такие как Bluetooth. ZigBee предназначен для радиочастотных устройств, где необходима длительная работа от батареек и безопасность передачи данных по сети.

Альянс ZigBee является органом, обеспечивающим и публикующим стандарты ZigBee, он также публикует профили приложений, что позволяет производителям изначальной комплектации создавать совместимые продукты. Текущий список профилей приложений, опубликованных, или уже находящихся в работе:

- Домашняя автоматизация
- Рациональное использование энергии (ZigBee Smart Energy 1.0/2.0)
- Автоматизация коммерческого строительства
- Телекоммуникационные приложения
- Персональный, домашний и больничный уход
- Игрушки

Сотрудничество между IEEE 802.15.4 и ZigBee подобно тому, что было между IEEE 802.11 и альянсом Wi-Fi. Спецификация ZigBee 1.0 была ратифицирована 14 декабря 2004 и доступна для членов альянса ZigBee. 30 октября 2007 г., была размещена спецификация ZigBee 2007. О первом профиле приложения — «Домашняя автоматизация» ZigBee, было объявлено 2 ноября 2007. ZigBee работает в промышленных, научных и медицинских (ISM-диапазон) радиодиапазонах: 868 МГц в Европе, 915 МГц в США и в Австралии, и 2.4 ГГц в большинстве стран в мире (под большинством юрисдикций стран мира). Как правило, в продаже имеются чипы ZigBee, являющиеся объединёнными радио- и микроконтроллерами с размером Flash-памяти от 60K до 128K таких производителей, как Jennic JN5148, Freescale MC13213, Ember EM250, Texas Instruments CC2430, Samsung Electro-Mechanics ZBS240 и Atmel ATmega128RFA1. Радиомодуль также можно использовать отдельно с любым процессором и микроконтроллером. Как правило, производители радиомодулей предлагают также стек программного обеспечения ZigBee, хотя доступны и другие независимые стеки.

Так как ZigBee может активироваться (то есть переходить от спящего режима к активному) за 15 миллисекунд или меньше, задержка отклика устройства может быть очень низкой, особенно по сравнению с Bluetooth, для которого задержка, образующаяся при переходе от спящего режима к активному, обычно достигает трёх секунд. Так как ZigBee большую часть времени находится в спящем режиме, уровень потребления энергии может быть очень низким, благодаря чему достигается длительная работа от батарей.

Первый выпуск стека сейчас известен под названием ZigBee 2004. Второй выпуск стека называется ZigBee 2006, и, в основном, заменяет структуру MSG/KVP, использующуюся в ZigBee 2004 вместе с «библиотекой кластеров». Стек 2004 года сейчас более или менее вышел из употребления. Реализация ZigBee 2007 в настоящее время является текущей, она содержит два профиля стека, профиль стека № 1 (который называют просто ZigBee) для домашнего и мелкого коммерческого использования, и профиль стека № 2 (который называют ZigBee Pro). ZigBee Pro предлагает больше функций, таких как широковещание, маршрутизацию вида «многие-к-одному» и высокую безопасность с использованием симметричного ключа (SKKE), в то время как ZigBee (профиль стека № 1) занимает меньше места в оперативной и Flash-памяти. Оба профиля позволяют развернуть полномасштабную сеть с ячеистой топологией и работают со всеми профилями приложений ZigBee.

ZigBee 2007 полностью совместим с устройствами ZigBee 2006. Устройство ZigBee 2007 может подключаться и работать с сетью ZigBee 2006, и наоборот. В связи с наличием различий в опциях маршрутизации, устройства ZigBee Pro могут быть только конечными устройствами (ZEDs) сетей ZigBee 2006, и наоборот, устройства ZigBee 2006 и ZigBee 2007 могут быть только конечными устройствами в сети ZigBee Pro. При этом приложения, которые запускаются на устройствах, работают одинаково, независимо от реализации профиля стека.

1.18 Приложения ZigBee

Протоколы ZigBee разработаны для использования во встроенных приложениях, требующих низкую скорость передачи данных и низкое энергопотребление. Цель ZigBee — это создание недорогой, самоорганизующейся сети с ячеистой топологией предназначенной для решения широкого круга задач. Сеть может использоваться в промышленном контроле, встроенных датчиках, сборе медицинских данных, оповещении о вторжении или задымлении, строительной и домашней автоматизации и т. д. Созданная в итоге сеть потребляет очень мало энергии — индивидуальные устройства согласно данным сертификации ZigBee позволяют энергобатареям работать два года.

Типовые области приложения:

- Домашние развлечения и контроль — рациональное освещение, продвинутый температурный контроль, охрана и безопасность, фильмы и музыка.
- Домашнее оповещение — датчики воды и энергии, мониторинг энергии, датчики задымления и пожара, рациональные датчики доступа и переговоров.
- Мобильные службы — мобильные оплата, мониторинг и контроль, охрана и контроль доступа, охрана здоровья и телепомощь.
- Коммерческое строительство — мониторинг энергии, HVAC, света, контроль доступа.
- Промышленное оборудование — контроль процессов, промышленных устройств, управление энергией и имуществом.

Существуют три различных типа устройств ZigBee.

- Координатор ZigBee (ZC) — наиболее ответственное устройство, формирует пути древа сети и может связываться с другими сетями. В каждой сети есть один координатор ZigBee. Он и запускает сеть от начала. Он хранит информацию о сети, выступает как доверенный центр и хранит ключи безопасности.
- Маршрутизатор ZigBee (ZR) — Маршрутизатор может выступать в качестве промежуточного маршрутизатора, передавая данные с других устройств. Он также может запускать функцию приложения.
- Конечное устройство ZigBee (ZED) — его функциональная нагруженность позволяет ему обмениваться информацией с материнским узлом (или координатором, или с маршрутизатором), он не может передавать данные с других устройств. Такое отношение позволяет узлу львиную часть времени пребывать в спящем состоянии,

что позволяет экономить энергоресурс батарей. ZED требует минимальное количество памяти, и поэтому может быть дешевле в производстве, чем ZR или ZC.

1.19 Протоколы ZigBee

Протоколы построены на недавно разработанном алгоритме AODV (протокол динамической маршрутизации для мобильных ad-hoc сетей (MANET) и других беспроводных сетей) и NeuRFon предназначенными для образования ad-hoc сетей (децентрализованная беспроводная сеть, образованная случайными абонентами) или узлов. В большинстве случаев сеть является скоплением скоплений. Она также может принимать форму сети или одиночного скопления. Текущие профили получаются из протоколов ZigBee поддерживают сети со включёнными или с отключёнными маячками.

В сетях с отключёнными маячками (где порядок маячков составляет 15) используется механизм доступа к каналам. В этом типе сети маршрутизаторы ZigBee обычно поддерживают свои приёмники включёнными продолжительно, что требует более мощной энергоподдержки. Однако это позволяет разнородным сетям, в которых некоторые устройства продолжительно принимают, пока другие только передают, в то время, когда определяются внешние сигналы. Типичный пример разнородной сети — это беспроводной ламповый выключатель. Узел ZigBee в лампе может принимать постоянно, с того времени как он подключён к общему питанию, в то время как ключ, соединяющий лампу с батареей, остаётся в спящем режиме, пока выключатель отключён. Затем ключ переходит в активный режим, посылает лампе команду, ожидая подтверждения, и возвращается в спящее состояние. В таких сетях узел лампы должен быть, по меньшей мере, маршрутизатором ZigBee, если не координатором, узел ключа, обычно, это конечное устройство ZigBee.

В сетях с маячками специальные узлы сети, маршрутизаторы ZigBee, передают периодические маячки, чтобы подтвердить своё присутствие на других узлах сети. Узлы могут находиться в спящем состоянии между маячками, что снижает их скважность и увеличивает жизнь батареек. Интервалы маячков могут различаться от 15.36 мс до 15.36 мс * 214 = 251.65824 с для скорости в 250 kbit/s, от 24 мс до 24 мс * 214 = 393.216 с для скорости в 40 kbit/s и от 48 мс до 48 мс * 214 = 786.432 с для 20 kbit/s. Однако низкая скважность операций (сигналов) вместе с длинными интервалами маячков требует точного распределения времени, что может войти в противоречие с требованием низкой стоимости изделия.

В общем, протоколы ZigBee снижают время включения радиопередатчиков и сокращают энергопотребление. В маячковых сетях узлы должны быть активными только во время осуществления маячком передачи. В безмаячковых сетях расход энергии решительно асимметричен, некоторые устройства всегда активны, в то время как другие проводят большую часть своего времени в спящем режиме. Устройства ZigBee должны быть совместимы со стандартом IEEE 802.15.4-2003 беспроводных персональных сетей (исключая профиль 2.0 «рационального использования энергии»). Стандарт определяет нижние слои протокола — физический слой (PHY), и контроль доступа (MAC) часть ссылки на слой данных (DLL). Этот стандарт определяет работу на частотах 2.4 ГГц (в мире, не лицензированная частота), 915 МГц (Американский континент) и 868 МГц (Европа) диапазон ISM. На частоте 2.4 ГГц есть 16 каналов ZigBee, каждый канал требует ширины диапазона в 5 МГц. Основная частота для каждого канала может быть рассчитана как FC = (2405 + 5 * (ch — 11)) МГц, где ch = 11, 12, …, 26.

Радио используют широкополосную модуляцию с прямым расширением спектра которая управляется цифровым потоком в модуляторе. Двоичная фазовая манипуляция используется на полосах в 868 и 915 МГц, а офсетная квадратурная фазовая манипуляция передающая по 2 бита в символе используется на полосе 2,4 ГГц. В чистом виде, при передаче через воздух скорость передачи данных составляет 250 кбит/с для каждого канала в диапазоне 2.4 ГГц, 40 кбит/с для каждого канала в диапазоне 915 МГц и 20 кбит/с в диапазоне 868 МГц. Расстояние передачи от 10 до 75 метров и свыше 1500 метров для Zigbee pro, хотя оно сильно зависит от отдельного оборудования. Максимальная выходная мощность радио в основном составляет 0 дБм (1 мВт).

Базовый режим доступа к каналу «контроль несущей частоты, многократный доступ/избежание коллизий кадров» (CSMA/CA- вероятностный сетевой протокол канального (MAC) уровня). То есть перед тем как узлы начинают передачу по пути обмена информацией для людей, они кратко проверяются, что ни один из них не ведёт передачу перед началом общей работы. Существуют три знаменитые исключения для работы CSMA. Маячки посылаются за предусмотренный промежуток времени и CSMA не используется. Подтверждения посланий также не используют CSMA. Наконец устройства в маячковых ориентированных сетях, которые имеют низкую скрытность в требованиях режима реального времени могут также использовать слоты гарантированного времени., которые по определению не используют CSMA.

1.20 Лицензирование и государственное регулирование ZigBee

Спецификация ZigBee доступна для широкой публики при условиях некоммерческого использования. Входной уровень членства в альянсе ZigBee, называемый Adopter, обеспечивает доступ к ещё не опубликованным спецификациям и разрешает создавать продукты для коммерческого использования спецификации. Регистрация в ходе использования спецификации ZigBee требует от коммерческого разработчика присоединения к альянсу ZigBee. «Ни одна часть этой спецификации не может быть использована для производства продуктов или продажи без членства в альянсе ZigBee.» Происходят ежегодные конфликты по поводу оплаты с общей публичной лицензией GNU. Согласно пункту 2-b: «Вы должны быть уверены в том, что любая работа, которую вы распространяете или публикуете, если вся эта работа или её часть содержит программу или извлечёна из программы или из любой её части, вся эта работа должна быть лицензирована как целое без передачи третьим лицам, согласно условиям данной лицензии». С тех пор как лицензия GPL не делает различий между коммерческим и некоммерческим использованием невозможно выполнить лицензирование стека ZigBee согласно GPL или совместить выполнение ZigBee с лицензионным кодом GPL. Требование к разработчику присоединиться к альянсу ZigBee также вступает в конфликт с другими лицензиями свободного программного обеспечения.

Применение сетей ZigBee в Российской Федерации в частотном диапазоне 2400-2483,5 МГц не требует получения частотных разрешений и дополнительных согласований (Решение ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001), решения ГКРЧ постоянно обновляются, решение от 07.05.2007 № 07-20-03-001 давно претерпело несколько раз изменения, однако смысл остается близко подобным.

Выводы по главе один

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11ac	WLAN	до 1 Гбит/с	до 300 метров	5 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбит/с	до 300 метров	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбит/с	до 300 метров	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбит/с (в перспективе до 600 Мбит/с)	до 300 метров	2,4 — 2,5 или 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбит/с	25-80 км	1,5-11 ГГц
WiMax	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2,3-13,6 ГГц
WiMax 2	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	120-150 км (стандарт в разработке)	До 11 ГГц
Bluetooth v.1.1	802.15.1	WPAN	до 1 Мбит/с	до 10 метров	2,4 ГГц
Bluetooth v.2.0	802.15.3	WPAN	до 2,1 Мбит/с	до 100 метров	2,4 ГГц
Bluetooth v.3.0	802.11	WPAN	от 3 Мбит/с до 24 Мбит/с	до 100 метров	2,4 ГГц
UWB	802.15.3a	WPAN	110-480 Мбит/с	до 10 метров	7,5 ГГц
ZigBee	802.15.4	WPAN	от 20 до 250 кбит/с	1-100 м	2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал)

Беспроводные сети опоясывают своими невидимыми "нитями" весь мир. Им не мешают ни границы, ни суша, ни вода, ни строения.

Будущие перспективы очевидны. Миниатюрные устройства постепенно обретут возможность обмена данными при помощи стандарта Bluetooth (или его схожей замены). Расширится диапазон беспроводной гарнитуры, а включать свет в комнате с пульта позволит ZigBee.

Объединять периферию в рамках комнаты призван Wireless USB. Для домашнего кинотеатра предназначен WirelessHD. Перспективная технология, которая может со временем вытеснить современные проводные подключения.

На уровне квартиры или даже нескольких квартир, либо для объединения проводных локальных сетей между домами будет использоваться Wi-Fi. Он для этого создан и это удобнее. Куда дешевле установить маленькую точку доступа в квартире или в кафе (для посетителей), чем дорогостоящее WiMAX оборудование, для которого требуется сложный процесс настройки.

Что касается WiMAX, то этот стандарт хорошо подходит прежде всего для интернет-провайдеров. С его помощью они можно довести интернет в самые отдаленные части планеты.

2. ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации является органичным компонентом государственной политики развития национального сектора применения информационных технологий. Среди основных документов, определяющих на сегодняшний
день фундаментальные подходы к обеспечению информационной безопасности в Российской Федерации, можно выделить, в первую очередь,
следующие:

- Закон Российской Федерации 27.07.2006 No 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года;
- Доктрина информационной безопасности Российской Федерации;
- Стратегия развития информационного общества в Российской Федерации.

Указанные, а также сопутствующие им ведомственные нормативные документы (в первую очередь это документы ФСТЭК России) на сегодняшний день формируют комплексную систему требований по обеспечению информационной безопасности для информационных систем различного уровня. В то же время вопрос уточнения специфики киберпространства, а также соответствующих угроз и механизмов защиты, безусловно, заслуживает отдельного рассмотрения.

Из современных правовых документов в области безопасности киберпространства следует особо отметить следующие:

- Концептуальные взгляды на деятельность Вооруженных сил РФ в информационном пространстве;
- Проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Указ Президента России 2013г. No 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Однако, на сегодняшний день в Российской Федерации документом, определяющим наиболее фундаментальные подходы к обеспечению кибербезопасности, является Концепция стратегии кибербезопасности Российской Федерации. Документ определяет киберпространство как сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а кибербезопасность, в свою очередь, как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Тем самым, понятие «кибербезопасность» является по определению более узким, чем понятие «информационная безопасность». Следует обратить внимание, что указанное определение отличается и от общепринятых в отдельных отраслях определений понятия «кибербезопасности».

Общая структура направлений деятельности, предложенная в Концепции стратегии кибербезопасности Российской Федерации:
- Общесистемные меры (в т.ч. оценка защищенности, стандартизация, антикризисное планирование)
- Совершенствование нормативно-правовой базы и правовых мер
- Проведение научных исследований в области кибербезопасности
- Создание условий для разработки, производства и применения средств обеспечения кибербезопасности
- Совершенствование кадрового обеспечения и организационных мер
- Организация внутреннего и международного взаимодействия действующих лиц по обеспечению кибербезопасности
- Формирование и развитие культуры безопасного поведения в киберпространстве

Нетрудно видеть, что предложенные механизмы должны сформировать логичную и целостную систему, однако для практической их реализации необходима колоссальная работа по подготовке нормативных документов, регламентирующих отдельные аспекты соответствующей деятельности.

На этом этапе может быть полезен международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (ISO/IEC 27032 Information

technology. Security techniques. Guidelines for cybersecurity), разработанный подкомитетом SC 27 «Информационные методы обеспечения безопасности» технического комитета ISO/TC «Информационные технологии». Понятие киберпространства в данном документе носит более прикладной характер: оно рассматривается как комплексная среда, возникающая в результате взаимодействия людей, программного обеспечения и удаленных
сервисов с использованием информационных и телекоммуникационных технологий. Принципиально важным при этом является вопрос взаимодействия между различными организациями, обеспечивающими существование киберпространства как единого целого: по мнению разработчиков стандарта тот факт, что каждая из организаций решает вопросы обеспечения информационной безопасности самостоятельно, создает предпосылки для реализации принципиально новых угроз информационной безопасности.

Тем самым, кибербезопасность реализуется на стыке следующих трех компонентов системы обеспечения информационной безопасности:
- безопасность приложений;
- сетевая безопасность;
- безопасность сети интернет.

Выделяются две основных категории участников информационного взаимодействия: провайдеры и потребители.
Провайдеры могут предоставлять как доступ к среде информационного взаимодействия, так и доступ к тем или иным сервисом. В качестве потребителей могут выступать физические лица и организации.

По сути, в содержательной части стандарт представляет собой набор рекомендаций для провайдеров и потребителей по обеспечению кибербезопасности. Если для физических лиц рекомендации сводятся в основном к выполнению рекомендаций провайдеров, то провайдеры должны реализовывать полноценную систему управления информационной безопасности в соответствии с требованиями стандарта ISO/IEC 27001. Подчеркивается важность анализа рисков и управления рисками согласно ISO/IEC 27005.

Категории механизмов безопасности, предлагаемые для киберпространства, включают следующие аспекты:
- Безопасность приложений

- Защиту серверов
- Защиту конечных пользователей
- Защита от атак, связанных с использованием методов социальной инженерии.

На мой взгляд, акцент на организацию межсистемного взаимодействия, характерный для стандарта, нельзя назвать в полной мере обоснованным – тем самым, принятие аутентичного перевода ISO/IEC 27032 в качестве стандарта
ГОСТ Р вряд ли целесообразно. В то же время, отдельные положения стандарта вполне могут быть задействованы при разработке аналогичного отечественного нормативного документа (например, в статусе документа Минобороны или ФСТЭК России).

2.1 Федеральный закон "О связи" от 07.07.2003 N 126 ФЗ (последняя редакция)

Настоящий Федеральный закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Целями настоящего Федерального закона являются:

- создание условий для оказания услуг связи на всей территории Российской Федерации;
- содействие внедрению перспективных технологий;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российскими радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

Сфера действия настоящего Федерального закона:

- Настоящий Федеральный закон регулирует отношения, связанные с созданием и эксплуатацией всех сетей связи и сооружений связи, использованием радиочастотного спектра, оказанием услуг электросвязи и почтовой связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях.
- В отношении операторов связи, осуществляющих свою деятельность за пределами Российской Федерации в соответствии с правом иностранных государств, настоящий Федеральный закон применяется только в части регулирования порядка выполнения работ и оказания ими услуг связи на находящихся под юрисдикцией Российской Федерации территориях.

- Отношения в области связи, не урегулированные настоящим Федеральным законом, регулируются другими федеральными законами и иными нормативными правовыми актами Российской Федерации в области связи.

2.2 Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149 ФЗ (последняя редакция)

Сфера действия настоящего Федерального закона:

1. Настоящий Федеральный закон регулирует отношения, возникающие при:
- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:
- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если

только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2.3 Национальный стандарт РФ ГОСТ Р 56498-2015/IEC/PAS 62443-3:2008 "Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2015 г. N 775-ст)

Использование методик и стандартов IT-безопасности стало обычным явлением в офисной среде и выражено в форме повсеместного свода правил для управления информационной безопасностью (ИСО/МЭК 27002, ранее известный как ИСО/МЭК 17799), для эксплуатационной безопасности, а также в форме критериев оценки IT-безопасности (ИСО/МЭК 15408) при разработке продуктов.

Интернет и беспроводные сети уже появились на производстве. Проблемы безопасности автоматизированных систем все больше находят отражение в заголовках специализированных изданий. Однако общепризнанная практика и соответствующие стандарты запаздывают и это несмотря на повышенный интерес в сфере автоматизированных систем. Это чревато возможными материальными производственными убытками и ущербом для здоровья, человеческой жизни и окружающей среды.

По аналогии тому, как ранее были предусмотрены методологические принципы для эксплуатационной безопасности в офисной среде, настоящий стандарт - это начальная попытка предусмотреть методологические принципы для безопасности эксплуатации автоматизированных систем.

Однако методики и стандарты из офисной среды не могут быть непосредственно применены к автоматизированным системам. Исследование, проведенное EWICS [15] показало, что широко применяемый ИСО/МЭК 27002 необходимо значительно расширить, чтобы он был применим к системам управления, используемым в промышленности. Несмотря на то, что 189-и пунктам в указанном исследовании была дана оценка от применимых до абсолютно применимых, 85% или 45% были признаны как требующие дополнительной методологической основы.

Настоящий стандарт содержит рекомендуемые нормы, установленные специалистами-практиками на основе практического опыта, но разработанные независимо от ИСО/МЭК 27002.

Примечание - Несмотря на то, что желательно было бы согласовать структуру и терминологию настоящего стандарта с ИСО/МЭК 27002, на данный момент этого не сделано.

Предполагается, что настоящий стандарт заполнит существующий в настоящее время пробел, пока планируются дальнейшие действия по укреплению методологической основы в последующем издании МЭК 62443, как отмечено в приложении А.

Соответствие политике настоящего стандарта - вопрос частный. Это соответствие может быть указано в качестве примечания ко всем положениям политики ICS или к некоторым из них или к ее специальной версии.

Некоторые меры, описанные в настоящей политике, могут быть не применимы одновременно в конкретный момент времени для конкретной конфигурации в конкретном контексте безопасности. Политика допускает такое блочное исполнение и адаптацию.

Также, в зависимости от конкретной ICS, может быть признано необходимым или желательным, например, с точки зрения компромисса между риском и затратами, не реализовывать определенные меры, регламентированные настоящей политикой. В зависимости от характера безопасности это может быть сделано лишь временно во исполнение политики ICS, с использованием ее положений по управлению ошибками.

Выводы по главе два

Кибербезопасность – область информационных технологий, занимающаяся защитой сетей, компьютеров, программ, устройств от атак, повреждения или несанкционированного доступа.

История развития и создания

На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. С развитием технологий и разрастанием сетей связи выросло и значение обеспечения безопасности. История кибербезопасности начинается с появления первых атак на компьютеры. В 1989 году Робертом Моррисом был создан первый компьютерный червь – самораспространяющийся вирус. Конечно, атаки и вирусы существовали и до этого времени, но именно червь Морриса был первой масштабной и широко распространенной DoS атакой (англ. Denial of Service – «отказ в обслуживании») в сети ARPANET – предшественник Интернета.
В 1990-х годах в США был создан Консорциум по исследованиям в области информационной безопасности, в рамках которого разработали предложение по Международной конвенции по борьбе с киберпреступностью и терроризмом. В сентябре 1997 года был опубликован документ RFC 2196, который представлял собой руководство по разработке политики в области компьютерной безопасности в рамках интернет-сообщества. В 2014 году Европейским институтом стандартизации электросвязи (ETSI) был создан технический комитет Cyber Security, отвечающий за стандартизацию кибербезопасности на международном уровне.
В настоящее время кибербезопасность приобретает все большее значение в связи с растущим влиянием компьютерных систем и Интернета на все сферы жизни, развитием беспроводных сетей (например, на базе Bluetooth и Wi-Fi), а также ростом «умных» устройств, смартфонов, телевизоров как части Интернета вещей.

Технические характеристики

Ранее действия по обеспечению кибербезопасности выполнялись вручную, теперь же преимущественно при помощи компьютеров. Основу кибербезопасности составляют три процесса:

- предотвращение угрозы

- обнаружение угрозы
- реагирование

Сегодня распространены следующие виды атак: бэкдор (от англ. back door – «чёрный ход»), атаки типа отказ в обслуживании, атаки прямого доступа, подслушивание, подмена данных, фальсификация, фишинг (от англ. fishing – выуживание), кликджекинг (англ. Clickjacking) и др.

Основной профилактической мерой сегодня является использование межсетевых экранов, так называемых «брандмауэров», которые фильтруют поступающие пакеты. Немаловажной мерой безопасности является применение криптографии для защиты файлов, процедуры аутентификации для доступа к данным (простейший способ – введение пароля, биометрические проверки). Современные операционные системы снабжены алгоритмами проверки и сканирования на наличие возможных угроз.

Кейсы применения

Защита различных устройств, подключенных к сети связи, начиная от компьютеров, серверов, транспортных средств, заканчивая носимой электроникой (часы, очки, браслеты и т.д.), имплантируемыми медицинскими устройствами, такими как кардиостимуляторы, в будущем – имплантируемые таблетки с обратной связью и др.

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая *Политика информационной безопасности* или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) (англ. *Organizational security policy*) — совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (англ. *ICT security policy*) — правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:
- Защита объектов информационной системы;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.), включая защиту информации в локальных сетях;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:
- Определение информационных и технических ресурсов, подлежащих защите;
- Выявление полного множества потенциально возможных угроз и каналов утечки информации;
- Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- Определение требований к системе защиты;
- Осуществление выбора средств защиты информации и их характеристик;
- Внедрение и организация использования выбранных мер, способов и средств защиты;
- Осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.
Документы верхнего уровня Политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. Подобные документы могут называться «Концепция ИБ», «Регламент управления ИБ», «Политика ИБ», «Технический стандарт ИБ» и т. п. Область распространения документов верхнего уровня обычно не ограничивается, однако данные документы могут выпускаться и в двух редакциях — для внешнего и внутреннего использования.

Согласно ГОСТ Р ИСО/МЭК 17799—2005, на верхнем уровне Политики информационной безопасности должны быть оформлены следующие документы: «Концепция обеспечения ИБ», «Правила допустимого использования ресурсов информационной системы», «План обеспечения непрерывности бизнеса».

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации. Например: Безопасности данных, Безопасности коммуникаций, Использования средств криптографической защиты, Контентная фильтрация и т. п. Подобные документы обычно издаются в виде внутренних технических и организационных политик (стандартов) организации. Все документы среднего уровня политики информационной безопасности конфиденциальны.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

3.ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ БЕСПРОВОДНЫХ СЕТЕЙ

3.1 Определение VPN

VPN (англ. *Virtual Private Network* — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).
В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: *узел-узел*, *узел-сеть* и *сеть-сеть*.

Виртуальные частные сети (VPN) представляют собой подключения типа «точка-точка» в частной или публичной сети, например в Интернете. VPN-клиент использует для виртуального обращения на виртуальный порт VPN-сервера специальные протоколы на основе TCP/IP, которые называются туннельными протоколами. При обычной реализации VPN клиент инициирует по Интернету виртуальное подключение типа «точка-точка» к серверу удаленного доступа. Сервер удаленного доступа отвечает на вызов, выполняет проверку подлинности вызывающей стороны и передает данные между VPN-клиентом и частной сетью организации.

Для эмуляции канала типа «точка-точка» к данным добавляется заголовок (выполняется инкапсуляция). Этот заголовок содержит сведения маршрутизации, которые обеспечивают прохождение данных по общей или публичной сети до конечного пункта. Для эмуляции частного канала и сохранения конфиденциальности передаваемые данные шифруются. Пакеты, перехваченные в общей или публичной сети,

невозможно расшифровать без ключей шифрования. Такой канал, по которому частные данные передаются в инкапсулированном и зашифрованном виде, и называется VPN-подключением.
VPN-подключения типа «сеть-сеть» (также называются VPN-подключения типа «маршрутизатор-маршрутизатор») позволяют организациям устанавливать маршрутизируемые подключения между отдельным офисами (или между другими организациями) по публичной сети, при этом обеспечивая безопасность связи. Маршрутизируемое VPN-подключение по Интернету логически подобно выделенному каналу глобальной сети (WAN). В случае, когда сети соединены по Интернету, как показано на следующем рисунке, маршрутизатор переадресует пакеты другому маршрутизатору через VPN-подключение. С точки зрения маршрутизаторов VPN-подключение работает как канал уровня передачи данных.

VPN-подключение типа «сеть-сеть» связывает два сегмента частной сети. VPN-сервер обеспечивает маршрутизируемое подключение к сети, к которой прикреплен VPN-сервер. Вызывающий маршрутизатор (VPN-клиент) проходит проверку подлинности на отвечающем маршрутизаторе (VPN-сервере) и, в целях взаимной проверки подлинности, отвечающий маршрутизатор проходит проверку подлинности на вызывающем маршрутизаторе. При VPN-подключении типа «сеть-сеть» пакеты, отсылаемые с любого из маршрутизаторов через VPN-подключение, обычно формируются не на маршрутизаторах.

Уровни реализации

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).
Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — PPTP, причём используемую зачастую *не* для создания частных сетей.
Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP — Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

Структура VPN

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

Классификация VPN

По степени защищенности используемой среды: защищённые; доверительные.

По способу реализации: в виде специального программно-аппаратного обеспечения; в виде программного решения; интегрированное решение.

По назначению: Intranet VPN; Remote Access VPN; Extranet VPN; Internet VPN; L2TP; Client/Server VPN.

3.2 Протокол PPTP

PPTP (англ. *Point-to-Point Tunneling Protocol*) — это протокол, изобретенный Microsoft для организации VPN через сети коммутируемого доступа. PPTP является стандартным протоколом для построения VPN уже на протяжении многих лет. Это только VPN-протокол и он опирается на различные методы аутентификации для обеспечения безопасности (наиболее часто используется MS-CHAP v.2). Доступен как стандартный протокол почти во всех операционных системах и устройствах, поддерживающих VPN, что позволяет использовать его без необходимости установки дополнительного программного обеспечения. PPTP остается популярным выбором как предприятий, так и VPN-провайдеров. Его преимущество также в том, что он использует меньше вычислительных ресурсов, следовательно обладает высокой скоростью работы.

Спецификация

Спецификация протокола была опубликована как «информационная» RFC 2637 в 1999 году. Она не была ратифицирована IETF. Протокол считается менее безопасным, чем IPSec. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий.

PPTP-трафик может быть зашифрован с помощью MPPE. Для аутентификации клиентов могут использоваться различные механизмы, наиболее безопасные из них — MS-CHAPv2 и EAP-TLS.

Реализация PPTP

Cisco первой реализовала PPTP и позже лицензировала эту технологию корпорации Microsoft.

PPTP удалось добиться популярности благодаря тому, что это первый протокол туннелирования, который был поддержан корпорацией Microsoft. Все версии Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав PPTP-клиент, однако существует ограничение на два одновременных исходящих соединения. А сервис удалённого доступа для Microsoft Windows включает в себя PPTP сервер.

Некоторое время в Linux-дистрибутивах отсутствовала полная поддержка PPTP из-за опасения патентных претензий по поводу протокола MPPE. Впервые полная поддержка MPPE появилась в Linux 2.6.13 (2005 год). Официально поддержка PPTP

была начата с версии ядра Linux 2.6.14. Тем не менее, сам факт применения MPPE в PPTP фактически не обеспечивает безопасность протокола PPTP.

Операционная система FreeBSD поддерживает PPTP протокол, используя в качестве сервера PPTP порт mpd (/usr/ports/net/mpd5), используя подсистему netgraph; можно также использовать программу PoPToP (/usr/ports/net/poptop). В качестве клиента PPTP в системе FreeBSD может выступать либо порт pptpclient (/usr/ports/net/pptpclient), либо порт mpd, работающий в режиме клиента.

Mac OS X поставляется со встроенным PPTP клиентом. Cisco и Efficient Networks продают реализации PPTP клиента для более старых версий Mac OS. С iOS10 поддержка PPTP прекращена! КПК Palm, имеющие поддержку Wi-Fi, поставляются с PPTP клиентом Mergic.

Microsoft Windows Mobile 2003 и более новые также поддерживают PPTP.

Безопасность протокола PPTP

Хотя PPTP обычно и используется со 128-битным шифрованием, в следующие несколько лет после включения этого протокола в состав Windows 95 OSR2 в 1999 году были найдены ряд уязвимостей. Наиболее серьезной из которых явилась уязвимость протокола аутентификации MS-CHAP v.2. Используя эту уязвимость, PPTP был взломан в течение 2 дней. И хотя компанией Microsoft была исправлена эта ошибка (за счет использования протокола аутентификации PEAP, а не MS-CHAP v.2), она сама рекомендовала к использованию в качестве VPN проколов L2TP или SSTP.

PPTP был объектом множества анализов безопасности, в нём были обнаружены различные серьёзные уязвимости. Известные относятся к используемым протоколам аутентификации PPP, устройству протокола MPPE и интеграции между аутентификациями MPPE и PPP для установки сессионного ключа. Краткий обзор данных уязвимостей:

- MSCHAP-v1 совершенно ненадёжен. Существуют утилиты для лёгкого извлечения хешей паролей из перехваченного обмена MSCHAP-v1.
- MSCHAP-v2 уязвим к словарной атаке на перехваченные challenge response пакеты. Существуют программы, выполняющие данный процесс.
- В 2012 году было показано, что сложность подбора ключа MSCHAP-v2 эквивалентна подбору ключа к шифрованию DES, и был представлен онлайн-сервис, который способен восстановить ключ за 23 часа.
- При использовании MSCHAP-v1, MPPE использует одинаковый RC4 сессионный ключ для шифрования информационного потока в обоих направлениях. Поэтому стандартным методом является выполнение XOR'а потоков из разных направлений вместе, благодаря чему криптоаналитик может узнать ключ.

•MPPE использует RC4 поток для шифрования. Не существует метода для аутентификации цифробуквенного потока и поэтому данный поток уязвим к атаке, делающей подмену битов. Злоумышленник легко может изменить поток при передаче и заменить некоторые биты, чтобы изменить исходящий поток без опасности своего обнаружения. Данная подмена битов может быть обнаружена с помощью протоколов, считающих контрольные суммы.

Плюсы:

- клиент PPTP встроен почти во все операционные системы
- очень прост в настройке
- работает быстро

Минусы:

- небезопасен (уязвимый протокол аутентификации MS-CHAP v.2 все еще много где используется)

3.3 Реализация PPTP-сервера в ОС Windows

Откройте список подключений Windows. Самый быстрый способ сделать это — нажать клавиши Win + R в любой версии Windows и ввести *ncpa.cpl*, затем нажать Enter.

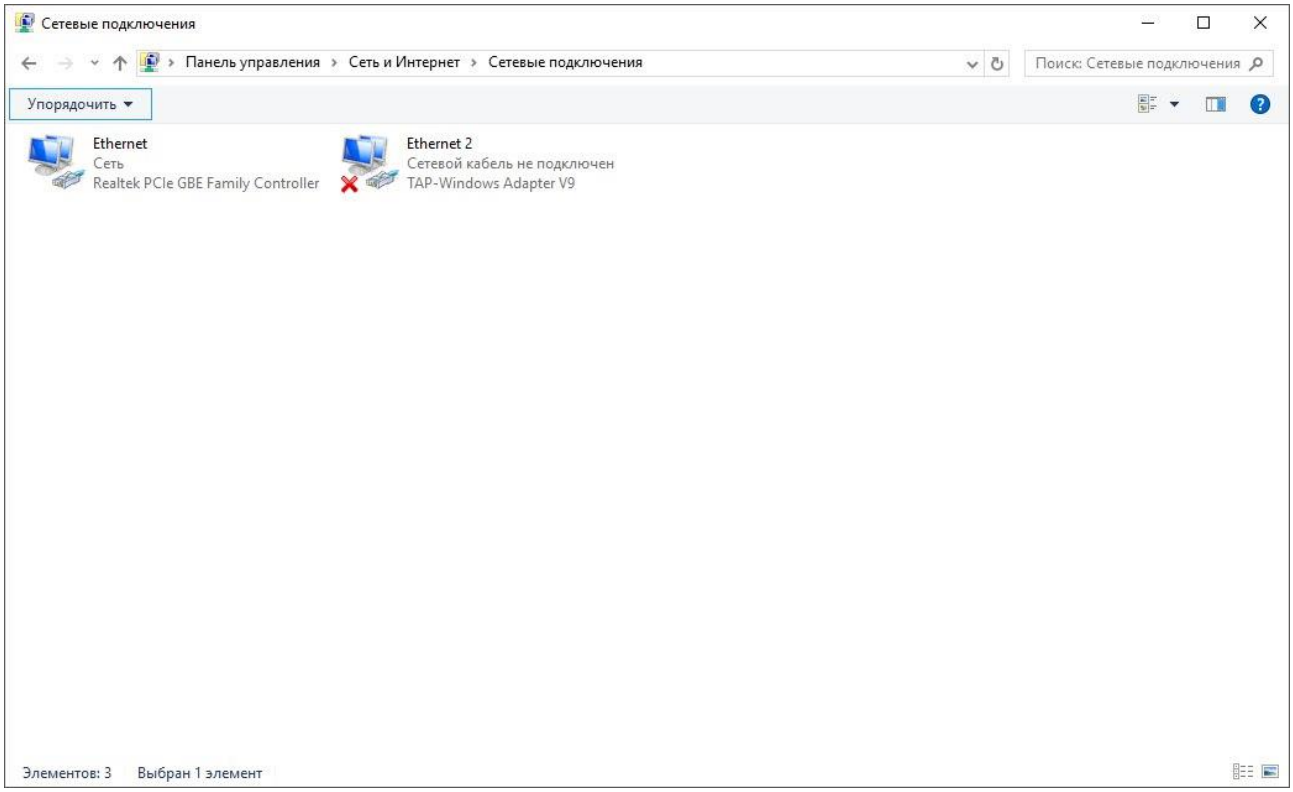

Рисунок 3.2.1 — Список подключений Windows

В списке подключений нажмите клавишу Alt и в появившемся меню выберите пункт «Новое входящее подключение».

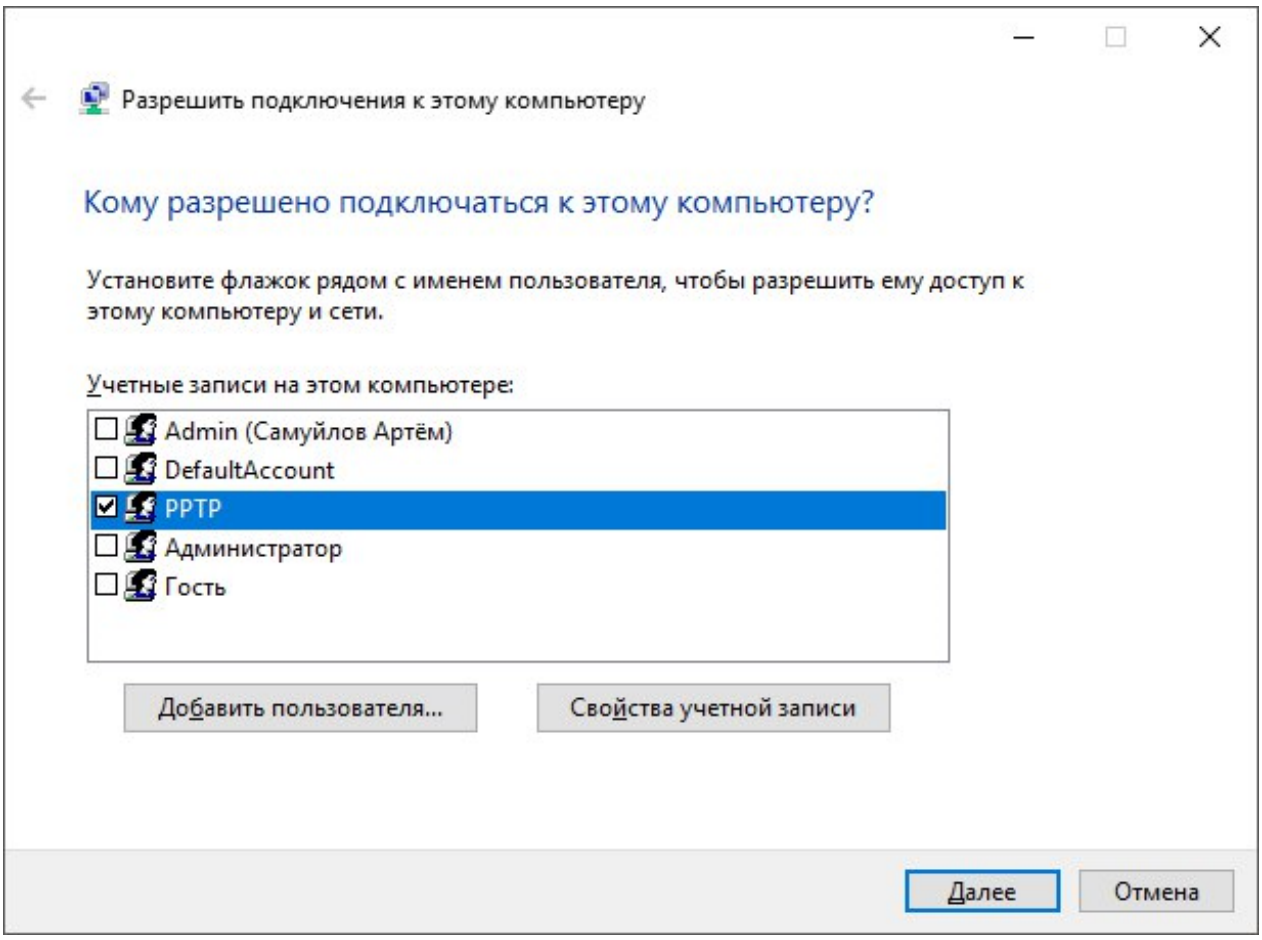

Рисунок 3.2.2 — Список учетных записей

На следующем этапе нужно выбрать пользователя, которому будет разрешено удаленное подключение. Для большей безопасности лучше создать нового пользователя с ограниченными правами и предоставить доступ к VPN только ему. Кроме этого, не забудьте установить хороший, пароль для этого пользователя.

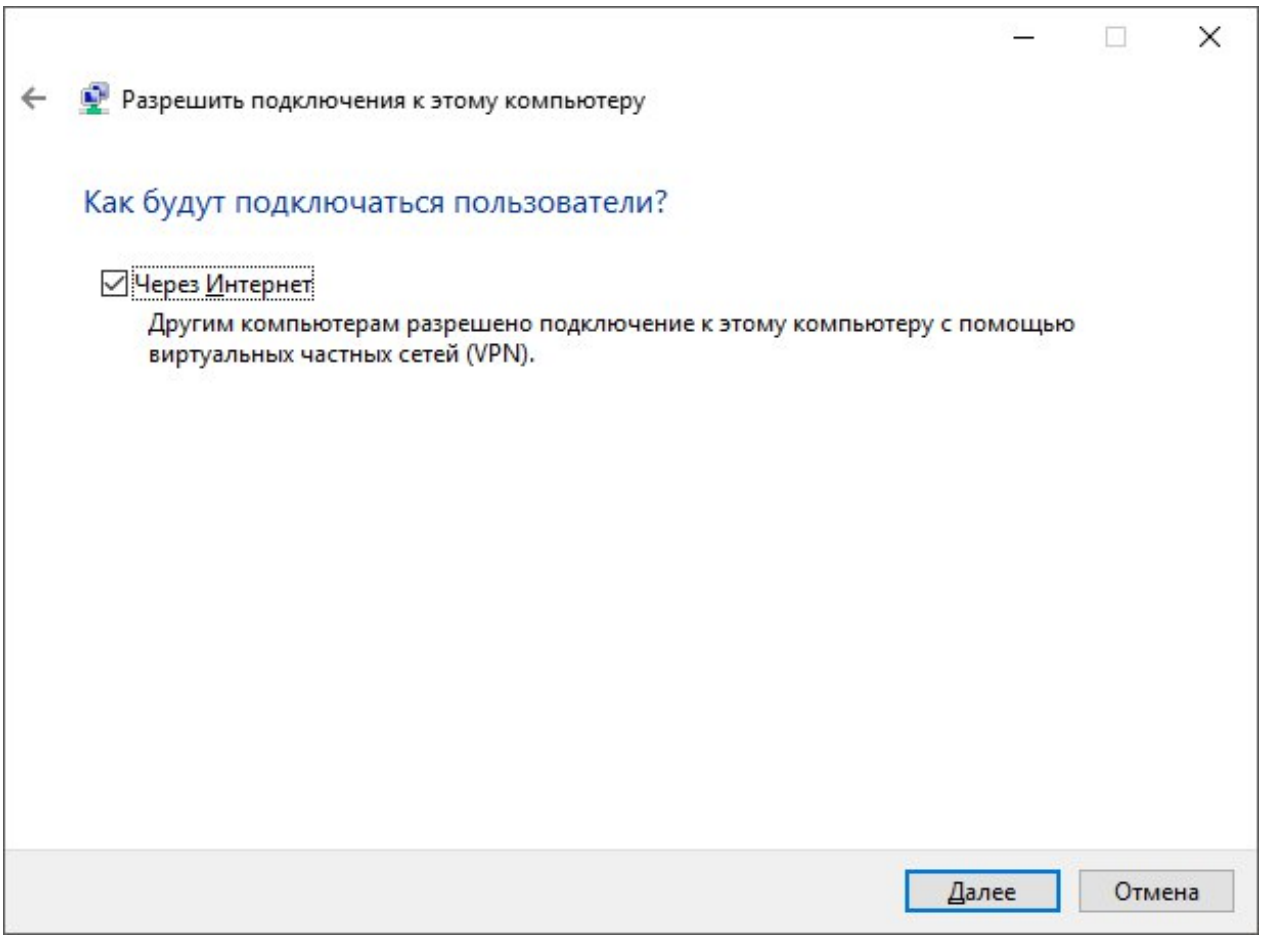

Рисунок 3.2.3 — Выбор типа подключения

Нажмите «Далее» и отметьте пункт «Через Интернет».

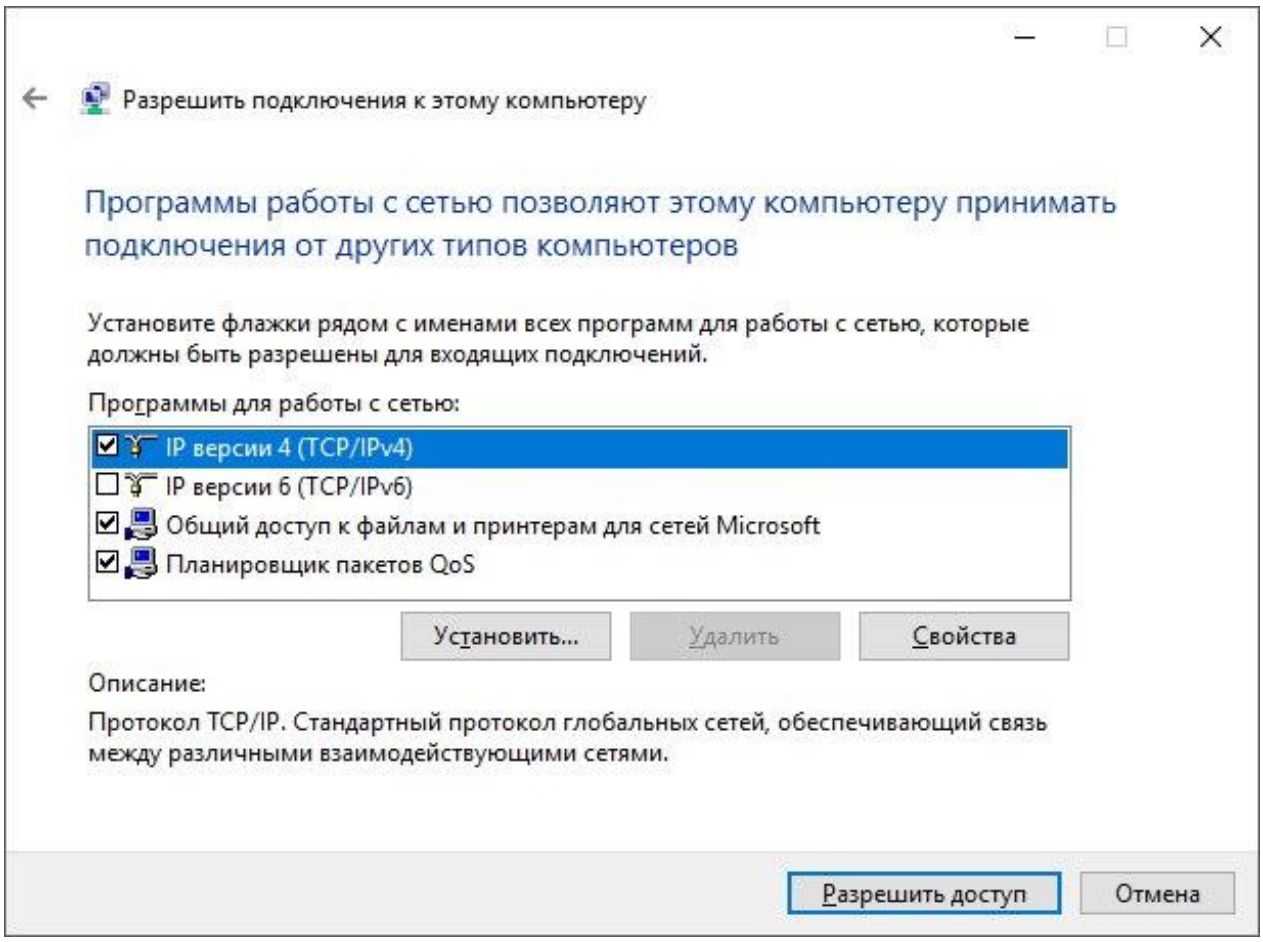

Рисунок 3.2.4 — Настройка выбранного типа подключения

В следующем диалоговом окне нужно отметить, по каким протоколам будет возможно подключение: если вам не требуется доступ к общим файлам и папкам, а также принтерам при VPN подключении, можно снять отметку с этих пунктов. Нажмите кнопку «Разрешить доступ» и дождитесь завершения создания VPN сервера Windows.

Если потребуется отключить возможность VPN подключения к компьютеру, кликните правой кнопкой мыши по «Входящие подключения» в списке подключений и выберите пункт «Удалить».

3.4 Установка и настройка OpenVPN сервера в ОС Linux

Виртуальная частная сеть (Virtual Private Network, VPN) позволяет использовать незащищённые сети таким образом, как если бы вы работали в частной сети. Весь ваш трафик в этом случае проходит через VPN-сервер.

В комбинации с использованием HTTPS-соединения описываемые далее настройки позволят вам обезопасить свою приватную информацию, например, логины и пароли, а также ваши покупки. Более того, вы сможете обходить региональные ограничения и цензуру, а также скрывать своё местонахождение и незашифрованный HTTP-трафик от незащищённой сети. представляет собой мощное и гибко настраиваемое программное обеспечение с открытым исходным кодом для работы с Secure Socket Layer (SSL) VPN. В этой главе мы установим и настроим OpenVPN сервер, а также научимся осуществлять к нему доступ из Windows, Mac OS, iOS и Android.

3.5 Подключение к серверу с помощью SSH

Информация о сервере и учетные данные для входа

Чтобы подключиться к удаленному серверу Linux через SSH, нужно обладать следующими данными:
- Имя пользователя
- Пароль и/или SSH ключ
- IP адрес сервера

Программное обеспечение клиента SSH

Существует множество SSH-клиентов, которые вы можете использовать для подключения к серверу Linux. Мы рассмотрим следующие два:
- OpenSSH (Linux и Mac OS X): коллекция программного обеспечения, которое поставляется с большинством Unix-подобных операционных систем, которое включает в себя команду ssh
- PuTTY (Windows): бесплатный SSH-клиент, который может работать в Windows и доступен для загрузки на странице загрузки PuTTY. Putty.exe - это SSH-клиент, а puttygen.exe также должен быть загружен, если вы хотите использовать SSH-ключи.

SSH авторизация с правами администратора

Вариант 1: OpenSSH (Linux и Mac OS X)

Клиент ssh OpenSSH - это инструмент командной строки, поэтому откройте окно «Терминал», чтобы начать работу.

Шаг 1 - Инициируйте соединение
В командной строке введите следующую команду, чтобы попытаться подключиться к серверу в качестве пользователя root (подставьте выделенное слово с IP-адресом вашего сервера):

```
ssh root@SERVER_IP_ADDRESS
```

Шаг 2 - Аутентификация

Шаг аутентификации включает в себя предоставление пароля и/или частного SSH-ключа, чтобы доказать, что вам разрешено входить в систему с правами администратора.

Если вы добавили SSH-ключ на свой сервер, и у вас есть закрытый ключ, установленный на вашем компьютере, OpenSSH попытается использовать ключ для аутентификации в корневой учетной записи. Если вы использовали ключ с парольной фразой, вам необходимо предоставить кодовую фразу для завершения процесса входа в систему. На этом этапе, если вы не можете войти в систему, вам может потребоваться запустить ваш ssh-agent и добавить к нему свои SSH-ключи с помощью следующей команды, а затем вернитесь к шагу 1:

```
eval `ssh-agent -s`
ssh-add ~/.ssh/id_rsa
```

Если вы не добавляли SSH ключ на свой сервер, вам будет предложено ввести временный пароль, и вам также потребуется его изменить. Для завершения процесса входа в систему выполните следующие действия:
- введите временный пароль в строке ввода пароля.
- в строке (current) UNIX password введите временный пароль
- в строке Enter new UNIX password введите новый пароль
- в строке Retype new UNIX password введите тот же новый пароль

Вариант 2: PuTTY (Windows)

Запустите putty.exe, дважды щелкнув по нему, чтобы запустить программу и перейти на экран конфигурации.

Примечание. Если вам нужно использовать ключи SSH с PuTTY, используйте PuTTYgen для генерации и загрузки ключей. Учебное пособие по этой теме можно найти здесь: Как использовать ключи SSH с PuTTY.

Шаг 1 - Настройка подключения
Чтобы правильно настроить соединение SSH, должны быть установлены следующие настройки:
- имя хоста (или IP-адрес): введите SERVER_IP_ADDRESS
- порт: 22 (по умолчанию)
- тип подключения: SSH (по умолчанию)

Теперь можно назвать и сохранить это соединение для использования в будущем, введя имя в поле «Сохраненные сеансы» и нажав «сохранить».

Шаг 2. Начало соединения.
Чтобы инициировать соединение, дважды щелкните по имени соединения и примите предупреждение безопасности (отображается только при первом подключении к серверу).

Шаг 3 - Аутентификация
Шаг аутентификации включает в себя предоставление учетных данных для входа, имени пользователя и временного пароля для подключения к серверу. После первоначального подключения вам потребуется изменить пароль.

Для завершения процесса входа в систему выполните следующие действия:
- в строке login as введите root
- в строке Password prompt введите пароль
- в строке (current) UNIX password введите временный пароль
- в строке Enter new UNIX password введите новый пароль
- в строке Retype new UNIX password введите тот же новый пароль

3.6 Начальная настройка сервера с помощью Ubuntu 16.04

При создании нового сервера Ubuntu 16.04, есть несколько этапов настройки, которые нужно выполнить на ранней стадии в рамках базовой установки. Это повысит безопасность и удобство использования сервера.

Шаг первый - вход в качестве пользователя root
Чтобы войти в свой сервер, нужно знать внешний IP-адрес сервера. Также понадобится пароль или, если установлен SSH-ключ для проверки подлинности, секретный ключ для учетной записи пользователя «root».

В командной строке введите следующую команду, чтобы попытаться подключиться к серверу в качестве пользователя root (замените выделенное слово общедоступным IP-адресом вашего сервера):

ssh root@SERVER_IP_ADDRESS

Завершите процесс входа в систему, приняв предупреждение о подлинности хоста, если оно появится, а затем предоставит вашу корневую аутентификацию (пароль или закрытый ключ). Если вы впервые заходите на сервер с паролем, вам также будет предложено изменить пароль root.

О пользователе root

Пользователь root является административным пользователем в среде Linux, который имеет очень широкие привилегии. Из-за повышенных привилегий учетной записи root фактически не рекомендуется использовать ее на регулярной основе. Это связано с тем, что часть власти, присущая учетной записи root - это возможность случайно совершать очень разрушительные.

Следующим шагом будет создание альтернативной учетной записи пользователя с уменьшенной степенью влияния на повседневную работу.

Шаг второй - создать нового пользователя
После входа в систему под учетной записью root, возможно добавить новую учетную запись пользователя, с которой мы будем работать с этого момента.

adduser username

Шаг третий — привилегии пользователя root
Теперь у нас есть новая учетная запись пользователя с обычными привилегиями учетной записи. Однако иногда нам могут понадобиться административные задачи.

Чтобы избежать необходимости выхода из нашего обычного пользователя и регистрации в качестве учетной записи root, мы можем настроить так называемые привилегии суперпользователя или root для нашей обычной учетной записи. Это позволит нашим обычным пользователям запускать команды с правами администратора, помещая слово sudo перед каждой командой.

Чтобы добавить эти привилегии новому пользователю, нам нужно добавить нового пользователя в группу «sudo». По умолчанию на Ubuntu 16.04 пользователям, принадлежащим к группе «sudo», разрешено использовать команду sudo.

В качестве пользователя root запустите эту команду, чтобы добавить нового пользователя в группу sudo:

usermod -aG sudo username

Шаг четвертый - добавление аутентификации с открытым ключом

Следующим шагом в обеспечении безопасности сервера является настройка аутентификации открытого ключа для нового пользователя. Настройка этого параметра повысит безопасность сервера, если для входа в систему потребуется приватный SSH-ключ.

Создание ключевой пары

Если у еще нет пары ключей SSH, которая состоит из открытого и закрытого ключей, необходимо сгенерировать ее. Если у уже есть ключ, который вы хотите использовать, перейдите к шагу «Копировать открытый ключ».

Чтобы создать новую пару ключей, введите следующую команду в терминал вашего локального компьютера (например, ваш компьютер):

ssh-keygen

Вы увидите вывод, который выглядит следующим образом:

Generating public/private rsa key pair.
Enter file in which to save the key (/Users/localuser/.ssh/id_rsa):

Это генерирует закрытый ключ, id_rsa и открытый ключ id_rsa.pub в каталоге .ssh домашнего каталога localuser. Помните, что закрытый ключ не должен быть доступен всем, у кого не должно быть доступа к вашим серверам.

Скопируйте открытый ключ

После создания пары ключей SSH вы захотите скопировать свой открытый ключ на новый сервер. Мы рассмотрим два простых способа сделать это.

Вариант 1: использование ssh-copy-id
Если на вашем локальном компьютере установлен скрипт ssh-copy-id, вы можете использовать его для установки вашего открытого ключа любому пользователю, у которого есть учетные данные для входа.

Запустите сценарий ssh-copy-id, указав пользователя и IP-адрес сервера, на который вы хотите установить ключ, например:

ssh-copy-id username@SERVER_IP_ADDRESS

После ввода пароля пароля в открытый ключ будет добавлен в файл .ssh / authorized_keys удаленного пользователя. Соответствующий закрытый ключ теперь можно использовать для входа в сервер.

Вариант 2: вручную установите ключ
Предполагая, что создана пару ключей SSH с использованием предыдущего шага, используйте следующую команду на терминале вашего локального компьютера для печати открытого ключа (id_rsa.pub):

cat ~/.ssh/id_rsa.pub

Эта команда должна вывести на экран открытый SSH ключ. Выберите открытый ключ и скопируйте его в буфер обмена.

Чтобы включить использование ключа SSH для аутентификации в качестве нового удаленного пользователя, нужно добавить открытый ключ к специальному файлу в домашнем каталоге пользователя.

На сервере, как пользователь root, введите следующую команду, чтобы временно переключиться на нового пользователя:

su — username

Так вы попадете в домашний каталог нового пользователя.

Создайте новый каталог с именем .ssh и ограничьте его разрешения следующими командами:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

Откройте файл в папке .ssh с именем authorized_keys с текстовым редактором. Используем nano для редактирования файла:

```
nano ~/.ssh/authorized_keys
```

Теперь скопируйте свой открытый ключ (который должен находиться в буфере обмена), вставив его в редактор.

Нажмите CTRL-x, чтобы выйти из файла, затем «y», чтобы сохранить сделанные вами изменения, затем нажмите ENTER, чтобы подтвердить имя файла.

Теперь ограничьте разрешения файла authorized_keys этой командой:

```
chmod 600 ~/.ssh/authorized_keys
```

Введите эту команду один раз, чтобы вернуться к пользователю root:

exit

Шаг пятый - отключить аутентификацию паролей

Теперь, когда ваш новый пользователь может использовать SSH-ключи для входа в систему, можно повысить безопасность сервера, отключив аутентификацию только для пароля. Это позволит ограничить доступ SSH к вашему серверу только для проверки подлинности с открытым ключом. То есть, единственный способ войти на сервер (кроме консоли) - это иметь закрытый ключ, который соединяется с открытым ключом, который был установлен.

Примечание. Отключать аутентификацию с помощью пароля стоит только, если установлен открытый ключ для пользователя, как показано в предыдущем разделе, шаг 4. В противном случае вы заблокируете себя от своего сервера.

Чтобы отключить проверку подлинности на вашем сервере, выполните следующие действия.

Как root или ваш новый пользователь sudo, откройте конфигурацию демона SSH:

sudo nano /etc/ssh/sshd_config

Найдите строку, которая определяет PasswordAuthentication, раскомментируйте ее, удалив предыдущее «#», а затем измените ее значение на «no». Так строка должна выглядеть так после того, как внесены изменения:

PasswordAuthentication no

Два других параметра, которые важны для проверки подлинности только для ключей и устанавливаются по умолчанию. Если ранее этот файл не был модифицирован, то не нужно изменять эти параметры:

PubkeyAuthentication yes
ChallengeResponseAuthentication no

Когда вы закончите внесение изменений, сохраните и закройте файл, используя метод, который использовали ранее (CTRL-X, затем Y, затем ENTER).

Введите эту команду, чтобы перезагрузить демон SSH:

sudo systemctl reload sshd

Аутентификация паролем теперь отключена. Теперь сервер доступен только с аутентификацией ключа SSH.

Шаг шестой - тестовый вход

Теперь, прежде чем выйти из сервера, вы должны проверить свою новую конфигурацию. Не выходите, пока вы не убедитесь, что можете успешно войти в систему через SSH.

В новом терминале на локальном компьютере войдите на свой сервер с помощью новой учетной записи, которая была создана ранее. Для этого используйте эту команду:

ssh username@SERVER_IP_ADDRESS

Если вы добавили аутентификацию открытого ключа вашему пользователю, как описано в шагах 4 и 5, ваш личный ключ будет использоваться в качестве аутентификации. В противном случае вам будет предложено ввести пароль пользователя.

Обратите внимание на проверку подлинности ключа. Если вы создали пару ключей с парольной фразой, вам будет предложено ввести кодовую фразу для вашего ключа. В противном случае, если ваша пара ключей не имеет кодовой фразы, вы должны войти на свой сервер без пароля.

Как только аутентификация будет предоставлена серверу, вы войдете в систему как новый пользователь.

Помните, что если вам нужно запустить команду с привилегиями root, введите префиес «sudo», она будет выглядеть так:

sudo command_to_run

Шаг седьмой - установка базового брандмауэра

Серверы Ubuntu 16.04 могут использовать брандмауэр UFW, чтобы убедиться, что разрешены только подключения к определенным службам. Мы можем легко настроить базовый брандмауэр с помощью этого приложения.

Различные приложения могут регистрировать свои профили с помощью UFW после установки. Эти профили позволяют UFW управлять этими приложениями по имени. OpenSSH, служба, позволяющая нам подключиться к нашему серверу, теперь имеет профиль, зарегистрированный в UFW.

Это можно увидеть, выполнив команду:

sudo ufw app list

Output:
Available applications:
OpenSSH

Нужно убедиться, что брандмауэр разрешает соединения SSH, чтобы можно могли подключиться в следующий раз. Можно разрешить эти соединения, набрав:

sudo ufw allow OpenSSH

Впоследствии нужно включить брандмауэр, набрав:

sudo ufw enable

Введите «y» и нажмите ENTER для продолжения. Можно видеть, что соединения SSH разрешены, набрав:

sudo ufw status

Output:
Status: active

```
To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
```

3.7 Настройка сервера OpenVPN в Ubuntu 16.04

Шаг 1. Установка OpenVPN

Сначала установим OpenVPN на наш сервер. OpenVPN доступен в стандартных репозиториях Ubuntu, мы можем использовать apt для его установки. Также мы установим пакет easy-rsa, который позволит нам настроить наш собственный внутренний центр сертификации (certificate authority, CA) для использования с нашей VPN.

Обновим список пакетов сервера и установим необходимые пакеты следующими командами:

```
sudo apt-get update
sudo apt-get install openvpn easy-rsa
```

Шаг 2. Создание директории центра сертификации

OpenVPN это виртуальная частная сеть, использующая TLS/SSL. Это означает, что OpenVPN использует сертификаты для шифрования трафика между сервером и клиентами. Для выпуска доверенных сертификатов (trusted certificates) нам потребуется создать наш собственный центр сертификации.
Для начала скопируем шаблонную директорию easy-rsa в нашу домашнюю директорию с помощью команды make-cadir:

```
make-cadir ~/openvpn-ca
```

Далее зайдём в эту директорию для начала настройки центра сертификации:

```
cd ~/openvpn-ca
```

Шаг 3. Настройка переменных центра сертификации

Для настройки переменных нашего центра сертификации нам необходимо отредактировать файл vars. Откройте этот файл в вашем текстовом редакторе:

```
nano vars
```

Внутри файла находятся переменные, которые можно отредактировать, и которые задают параметры сертификатов при их создании. Нужно изменить некоторые из этих переменных.
Ближе к концу файла и находятся настройки полей, используемые по умолчанию при создании сертификатов. Они должны выглядеть примерно так:

Output:
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"

Замените эти значения на свои, не оставляйте их не заполненными:

Output:
export KEY_COUNTRY="Country"
export KEY_PROVINCE="Province"
export KEY_CITY="City"
export KEY_ORG="Organization"
export KEY_EMAIL="example@example.com"
export KEY_OU="OrganizationalUnit"

В этом же файле, отредактируем значение KEY_NAME, которое заполняет поле субъекта сертификатов:

export KEY_NAME="server"

Сохраняем и закрываем файл (CTRL-X, затем Y, затем ENTER).

Шаг 4. Создание центра сертификации

Теперь мы можно использовать заданные переменные и утилиты easy-rsa для создания центра сертификации.

Убедитесь, что вы находитесь в директории центра сертификации и используйте команду source к файлу vars:

```
cd ~/openvpn-ca
source vars
```

Output:

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/sammy/openvpn-ca/keys
```

Убедимся, что работа происходит в "чистой среде", выполнив следующую команду:

```
./clean-all
```

Теперь мы можем создать наш корневой центр сертификации командой:

```
./build-ca
```

Эта команда запустит процесс создания ключа и сертификата корневого центра сертификации. Поскольку уже задны все переменные в файле vars, все необходимые значения будут введены автоматически. Нажимайте **ENTER** для подтверждения выбора:

Output:

```
Generating a 2048 bit RSA private key
.....................................................................................+++
.....................+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Country]:
State or Province Name (full name) [Province]:
Locality Name (eg, city) [City]:
Organization Name (eg, company) [Organization]:
Organizational Unit Name (eg, section) [OrganizationUnit]:
Common Name (eg, your name or your server's hostname) [Organization CA]:
Name [server]:
Email Address [example@example.com]:
```

Теперь есть центр сертификации, который можно использовать для создания всех остальных необходимых файлов.

Шаг 5. Создание сертификата, ключа и файлов шифрования для сервера

Далее создадим сертификат, пару ключей и некоторые дополнительные файлы, используемые для осуществления шифрования, для нашего сервера.

Начнём с создания сертификата OpenVPN и ключей для сервера. Это можно сделать следующей командой:

./build-key-server server

Вывод опять будет содержать значения по умолчанию, переданные этой команде (server), а также значения из файла vars.

Согласитесь со всеми значениями по умолчанию, нажимая **ENTER.** *Не задавайте* challenge password. В конце процесса два раза введите **y** для подписи и подтверждения создания сертификата:

Output:

. . .

Certificate is to be certified until May 1 17:51:16 2026 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

Далее создадим оставшиеся файлы. Можно сгенерировать сильные ключи протокола Диффи-Хеллмана, используемые при обмене ключами, командой:

./build-dh

Для завершения этой команды может потребоваться несколько минут.

Далее мы можем сгенерировать подпись HMAC для усиления способности сервера проверять целостность TSL:

openvpn --genkey --secret keys/ta.key

Шаг 6. Создание сертификата и пары ключей для клиента

Далее можно сгенерировать сертификат и пару ключей для клиента. Вообще это можно сделать и на клиентской машине и затем подписать полученный ключ центром сертификации сервера, но для простоты мы сгенерируем подписанный ключ на сервере.

Мы создадим ключ и сертификат только для одного клиента. Если у вас несколько клиентов, вы можете повторять этот процесс сколько угодно раз. Просто каждый раз передавайте уникальное значение скрипту.

Поскольку можно вернуться к этому шагу позже, повторим команду source для файла vars. Будем использовать параметр client1 для создания первого сертификата и ключа.

Для создания файлов без пароля для облегчения автоматических соединений используйте команду build-key:

```
cd ~/openvpn-ca
source vars
./build-key client1
```

Для создания файлов, защищённых паролем, используйте команду build-key-pass:

```
cd ~/openvpn-ca
source vars
./build-key-pass client1
```

В ходе процесса создания файлов все значения по умолчанию будут введены, вы можете нажимать **ENTER**. Не задавайте challenge password и введите **y** на запросы о подписи и подтверждении создания сертификата.

Шаг 7. Настройка сервиса OpenVPN

Далее настроим сервис OpenVPN с использованием созданных ранее файлов.

Копирование файлов в директорию OpenVPN

Необходимо скопировать нужные нам файлы в директорию /etc/openvpn.

Сначала скопируем созданные файлы. Они находятся в директории ~/openvpn-ca/keys, в которой они и были созданы. Необходимо скопировать сертификат и ключ центра сертификации, сертификат и ключ сервера, подпись HMAC и файл Diffie-Hellman:

```
cd ~/openvpn-ca/keys
sudo cp ca.crt ca.key server.crt server.key ta.key dh2048.pem /etc/openvpn
```

Далее необходимо скопировать и распаковать файл-пример конфигурации OpenVPN в конфигурационную директорию, этот файл будет использоваться в качестве базы для настроек:

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz | sudo tee /etc/openvpn/server.conf
```

Настройка конфигурации OpenVPN

Теперь, когда файлы находятся в нужных директориях, займёмся настройкой конфигурационного файла сервера:

```
sudo nano /etc/openvpn/server.conf
```

Базовая настройка

Сначала найдём секцию HMAC поиском директивы tls-auth. Удалите ";" для того, чтобы раскомментировать строку с tls-auth. Далее добавьте параметр key-direction и установите его значение в "0":

Output:

```
tls-auth ta.key 0 # This file is secret
key-direction 0
```

Далее найдём секцию шифрования, нас интересуют закомментированные строки cipher. Шифр AES-128-CBC обеспечивает хороший уровень шифрования и широко поддерживается другими программными продуктами. Удалите ";" для раскомментирования строки AES-128-CBC:

Output:
cipher AES-128-CBC

Под этой строкой добавьте строку auth и выберите алгоритм HMAC. Хорошим выбором будет SHA256:

Output:
auth SHA256

Наконец, найдите настройки user и group и удалите ";" для раскомментирования этих строк:

Output:
user nobody
group nogroup

(Опционально) Проталкивание изменений DNS для перенаправления всего трафика через VPN

Сделанные настройки создают VPN соединение между двумя машинами, но они не заставляют эти машины использовать VPN соединение. Если нужно использовать VPN соединение для всего трафика, необходимо протолкнуть (push) настройки DNS на клиентские машины.
Для этого необходимо раскомментировать несколько директив. Найдите секцию redirect-gateway и удалите ";" из начала строки для расскоментирования redirect-gateway:

Output:
push "redirect-gateway def1 bypass-dhcp"

Чуть ниже находится секция dhcp-option. Удалите ";" для обеих строк:

push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"

Это позволит клиентам сконфигурировать свои настройки DNS для использования VPN соединения в качестве основного.

(Опционально) Настройка порта и протокола

По умолчанию OpenVPN использует порт 1194 и протокол UDP для соединения с клиентами. Если вам необходимо изменить порт из-за каких-либо ограничений для ваших клиентов, вы можете сделать это изменив настройку port. Если вы не хотите

веб-контент на вашем OpenVPN сервере, вы можете использовать порт 443, поскольку этот порт обычно разрешён для использования в большинстве файрволов.

Output:
Optional!
port 443

Используемый протокол может иметь ограничения по номеру порта. В этом случае измените proto с UDP на TCP:

Output:
Optional!
proto tcp

Если у нет явной необходимости использовать другой порт, лучше оставить обе эти настройки со значениями по умолчанию.

(Опционально) Использование кастомного имени сертификата и ключа

Если во время использования команды ./build-key-server был указан параметр, отличный от server, измените настройки cert и key, чтобы они указывали на правильные файлы .crt и .key. Если был использовае server, эти настройки должны выглядеть таким образом:

cert server.crt
key server.key

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Шаг 8. Настройка сетевой конфигурации сервера

Далее необходимо настроить сетевую конфигурацию сервера, чтобы OpenVPN мог корректно перенаправлять трафик.

Настройка перенаправления IP

Сначала разрешим серверу перенаправлять трафик. Это ключевая функциональность VPN сервера.

Настроим это в файле /etc/sysctl.conf:

sudo nano /etc/sysctl.conf

Найдите строку настройки net.ipv4.ip_forward. Удалите "#" из начала строки, чтобы раскомментировать её:

Output:
net.ipv4.ip_forward=1

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Для применения настроек к текущей сессии наберите команду:

sudo sysctl -p

Настройка правил UFW для сокрытия соединений клиентов

Вне зависимости от того, используется ли файрвол для блокировки нежелательного трафика (что стоит делать практически всегда), в этом пункте файрвол потребуется для манипулирования с входящим на сервер трафиком. Нужно изменить файл настроек для сокрытия соединений (masquerading).
Перед тем, как изменить этот файл, нужно найти публичный интерфейс сети (public network interface). Для этого наберите команду:

ip route | grep default

Публичный интерфейс должен следовать за словом "dev". Например, в нашем случае этот интерфейс называется wlp11s0:

Output:
default via 203.0.113.1 dev wlp11s0 proto static metric 600

Зная название интерфейса откроем файл /etc/ufw/before.rules и добавим туда соответствующие настройки:

sudo nano /etc/ufw/before.rules

Это файл содержит настройки UFW, которое применяются перед применением правил UFW. Добавьте в начало файла выделенные красным строки. Это настроит правила, применяемые по умолчанию, к цепочке POSTROUTING в таблице nat и будет скрывать весь трафик от VPN:

Output:

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to eth0
-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE
COMMIT
# END OPENVPN RULES

# Don't delete these required lines, otherwise there will be errors
*filter
. . .
```

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Теперь нужно должны сообщить UFW, что ему по умолчанию необходимо разрешать перенаправленные пакеты. Для этого откройте файл /etc/default/ufw:

sudo nano /etc/default/ufw

Найдите в файле директиву DEFAULT_FORWARD_POLICY. Изменим значение с DROP на ACCEPT:

DEFAULT_FORWARD_POLICY="ACCEPT"

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Открытие порта OpenVPN и применение изменений

Далее настроим сам файрвол для разрешения трафика в OpenVPN.

Если вы не меняли порт и протокол в файле /etc/openvpn/server.conf, вам необходимо разрешить трафик UDP для порта 1194. Если вы изменили эти настройки, введите указанные вами значения.

Также добавим порт SSH на случай, если это не было сделано ранее.

sudo ufw allow 1194/udp
sudo ufw allow OpenSSH

Теперь деактивируем и активируем UFW для применения внесённых изменений:

sudo ufw disable
sudo ufw enable

Теперь сервер сконфигурирован для обработки трафика OpenVPN.

Шаг 9. Включение сервиса OpenVPN

Мы готовы включить сервис OpenVPN на нашем сервере. Мы можем сделать это с помощью команды systemd.

Необходимо запустить сервер OpenVPN указав имя нашего файла конфигурации в качестве переменной после имени файла systemd. Файл конфигурации для сервера называется /etc/openvpn/server.conf, поэтому добавим @server в конец имени файла при его вызове:

sudo systemctl start openvpn@server

Убедимся, что сервис успешно запущен командой:

sudo systemctl status openvpn@server

Если всё получилось, вывод должен выглядеть примерно следующим образом:

Output:
● openvpn@server.service - OpenVPN connection to server
Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
Active: active (running) since Tue 2017-05-03 15:30:05 EDT; 47s ago
Docs: man:openvpn(8)
https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
https://community.openvpn.net/openvpn/wiki/HOWTO
Process: 5852 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openvpn/%i.status 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/%i.conf --writepid /run/openvpn/%i.pid (code=exited, sta
Main PID: 5856 (openvpn)
Tasks: 1 (limit: 512)
CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
└─5856 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/server.conf --writepid /run/openvpn/server.pid

May 03 15:30:05 openvpn2 ovpn-server[5856]: /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
May 03 15:30:05 openvpn2 ovpn-server[5856]: /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
May 03 15:30:05 openvpn2 ovpn-server[5856]: GID set to nogroup
May 03 15:30:05 openvpn2 ovpn-server[5856]: UID set to nobody
May 03 15:30:05 openvpn2 ovpn-server[5856]: UDPv4 link local (bound): [undef]

May 03 15:30:05 openvpn2 ovpn-server[5856]: UDPv4 link remote: [undef]
May 03 15:30:05 openvpn2 ovpn-server[5856]: MULTI: multi_init called, r=256 v=256
May 03 15:30:05 openvpn2 ovpn-server[5856]: IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
May 03 15:30:05 openvpn2 ovpn-server[5856]: IFCONFIG POOL LIST
May 03 15:30:05 openvpn2 ovpn-server[5856]: Initialization Sequence Completed

Вы также можете проверить доступность интерфейса OpenVPN tun0 следующей командой:

ip addr show tun0

Output:
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever

Если всё в порядке, настроим сервис на автоматическое включение при загрузке сервера:

sudo systemctl enable openvpn@server

Шаг 10. Создание инфраструктуры настройки клиентов

Далее настроим систему для простого создания файлов конфигурации для клиентов.

Создание структуры директорий конфигураций клиентов

В домашней директории создайте структуру директорий для хранения файлов:

mkdir -p ~/client-configs/files

Поскольку файлы конфигурации будут содержать клиентские ключи, нужно должны настроить права доступа для созданных директорий:

chmod 700 ~/client-configs/files

Создание базовой конфигурации

Скопируем конфигурацию-пример в нашу директорию для использования в качестве нашей базовой конфигурации:

cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf

Откроем этот файл в текстовом редакторе nano:

nano ~/client-configs/base.conf

Сделаем несколько изменений в этом файле.

Сначала найдем директиву remote. Эта директива сообщает клиенту адрес сервера OpenVPN. Это должен быть публичный IP адрес сервера OpenVPN. Если был изменён порт, который слушает сервер OpenVPN, измените порт по умолчанию 1194 на ваше значение:

Output:
. . .
The hostname/IP and port of the server.
You can have multiple remote entries
to load balance between the servers.
remote SERVER_IP_ADDRESS 1194
. . .

Убедитесь, что протокол совпадает с настройками сервера:

Output:
proto udp

Раскомментируйте директивы user и group удаляя ";":

Output:
Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup

Найдите директивы ca, cert и key. Закомментируйте эти директивы, так как мы будем добавлять сертификаты и ключи в самом файле:

Output:
SSL/TLS parms.
See the server config file for more
description. It's best to use
a separate .crt/.key file pair
for each client. A single ca
file can be used for all clients.
#ca ca.crt
#cert client.crt
#key client.key

Добавьте настройки cipher и auth согласно заданным в файле /etc/openvpn/server.conf:

Output:
cipher AES-128-CBC
auth SHA256

Далее добавьте директиву key-direction в любое место в файле. Она **должна** иметь значение "1" для корректной работы сервера:

Output:
key-direction 1

Добавьте несколько **закомментированных** строк. Эти строки будут добавлены в каждый файл конфигурации, но включены они будут только для клиентов на Linux, которые используют файл /etc/openvpn/update-resolv-conf. Этот скрипт использует утилиту resolvconf для обновление информации DNS на клиентах Linux.

Output:
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf

Если ваш клиент работает на Linux и использует файл /etc/openvpn/update-resolv-conf, вы должны раскомментировать эти строки в сгенерированном клиентском файле конфигурации OpenVPN.

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Создание скрипта генерации файлов конфигурации

Теперь создадим простой скрипт для генерации файлов конфигурации с релевантными сертификатами, ключами и файлами шифрования. Он будет помещать сгенерированные файла конфигурации в директорию ~/client-configs/files.

Создайте и откройте файл make_config.sh внутри директории ~/client-configs:

nano ~/client-configs/make_config.sh

Вставьте следующие текст в этот файл:

Output:
#!/bin/bash

First argument: Client identifier

KEY_DIR=~/openvpn-ca/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \

```
<(echo -e '</cert>\n<key>') \
${KEY_DIR}/${1}.key \
<(echo -e '</key>\n<tls-auth>') \
${KEY_DIR}/ta.key \
<(echo -e '</tls-auth>') \
> ${OUTPUT_DIR}/${1}.ovpn
```

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Сделайте его исполняемым файлом командой:

```
chmod 700 ~/client-configs/make_config.sh
```

Шаг 11. Генерация конфигураций клиентов

Теперь мы можем сгенерировать файлы конфигурации клиентов.

Если созданы сертификат client1.crt и ключ клиента client1.key командой ./build-key client1 на шаге 6, можно сгенерировать конфигурацию для этих файлов перейдя в директорию ~/client-configs и используя только что созданный скрипт:

```
cd ~/client-configs
./make_config.sh client1
```

Если всё прошло успешно, мы должны получить файл client1.ovpn в директории ~/client-configs/files:

```
ls ~/client-configs/files
```

Output:
client1.ovpn

Доставка конфигураций клиентам

Теперь нужно переместить файл конфигурации на клиентское устройство. Например, на компьютер или смартфон.

Способ доставки файла зависит от операционной системы вашего устройства и программного обеспечения, которое вы захотите использовать для перемещения файла. Рекомендуется передавать файл по защищённому соединению, например, с использованием SFTP или SCP.

Далее приведен пример передачи файла client1.ovpn с использованием SFTP. Эту команду можно использовать на локальном компьютере под управлением Mac OS или Linux. Она перемещает файл .ovpn в домашнюю директорию:

sftp username@SERVER_IP_ADDRESS:client-configs/files/client1.ovpn ~/
Шаг 12. Установка файлов конфигураций клиентов

Установка в OS Windows
Загрузить клиент для работы с OpenVPN для Windows можно с официальной страницы загрузок OpenVPN. Нужно выбрать необходимую версию установщика.

Внимание: установка OpenVPN требует администраторской учётной записи.

После установки OpenVPN скопируйте ваш .ovpn файл в эту директорию:

C:\Program Files\OpenVPN\config

После запуска OpenVPN, клиент должен автоматически увидеть профиль.

Клиент OpenVPN требует запуска с правами администратора даже для аккаунтов администратора. Для запуска сделайте щелчок правой кнопкой мыши на клиенте и выберите **Run as administrator** каждый раз при запуске клиента. Это также означает, что обычные пользователи должны будут вводить пароль администратора для использования OpenVPN.

Для того, чтобы приложение OpenVPN всегда запускалось с правами администратора, сделайте щелчок правой кнопкой мыши на иконке клиента и перейдите в раздел **Properties**. В нижней части вкладки **Compatibility** нажмите на кнопку **Change settings for all users.** В открывшемся окне выберите **Run this program as an administrator**.

Соединение

Каждый раз при запуске клиента OpenVPN Windows будет спрашивать, хотите ли вы разрешить программе внести изменения в настройки вашего компьютера. Нажмите **Да**. Запуск клиента OpenVPN просто помещает приложение в системный трей, при этом само соединение не устанавливается автоматически.

Для установки соединения сделайте щелчок правой кнопкой мыши на иконке OpenVPN в системном трее. В открывшемся контекстном меню выберите **client1** (это наш профиль client1.ovpn) и нажмите **Connect**.

Откроется окно статуса, которое будет отображать лог соединения. При завершении соединения вы увидите соответствующее сообщение.
Закрыть VPN соединение можно точно так же: сделайте щелчок правой кнопкой мыши на иконке OpenVPN в системном трее, выберите профиль клиента и нажмите **Disconnect**.

Установка в Mac OS
Tunnelblick - это бесплатный OpenVPN клиент для Mac OS с открытым исходным кодом. Его можно загрузить со страницы загрузок Tunnelblickю Сделайте двойной щелчок на загруженном .dmg файле и следуйте инструкциям в процессе установки.

В конце процесса установки Tunnelblick спросит, есть ли у вас конфигурационные файлы. Проще всего ответить **No** и завершить установку Tunnelblick. Откройте Finder и сделайте двойной щелчок на client1.ovpn. Tunnelblick установит клиентский профиль. Для этого необходимы права администратора.

Соединение

Запустите Tunnelblick двойным щелчком из папки **Applications**. После запуска в панели меню в правой верхней части экрана появится иконка Tunnelblick. Для установки соединения нажмите на иконку, а затем **Connect.** Далее выберите соединение **client1**.

Установка в OS Linux

В зависимости от используемой версии Linux, возможно использовать самые разные программы для установки соединения. Возможно, это умеет делать даже используемый менеджер окон.

Наиболее универсальным способом установки соединения, тем не менее, является программное обеспечение OpenVPN.

В Ubuntu или Debian его можно установить точно так же, как и на сервере:

sudo apt-get update
sudo apt-get install openvpn

В CentOS иожно активировать EPEL репозитории и затем ввести следующие команды:

sudo yum install epel-release
sudo yum install openvpn

Настройка

Сначала проверьте, содержит ли дистрибутив скрипт /etc/openvpn/update-resolv-conf:

ls /etc/openvpn
Output:
update-resolve-conf

Далее отредактируйте полученный с сервера файл конфигурации клиента OpenVPN:

nano client1.ovpn

Если вам удалось найти файл update-resolv-conf, раскомментируйте следующие строки файла:

script-security 2
up /etc/openvpn/update-resolv-conf

down /etc/openvpn/update-resolv-conf

Если вы используете CentOS, измените group с nogroup на nobody:

group nobody

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Теперь можно соединиться с VPN используя команду openvpn следующим образом:

sudo openvpn --config client1.ovpn

В результате будет произведено подключение к серверу.

Шаг 13. Тестирование VPN соединения

После того, как всё установлено и настроено, убедимся, что всё работает правильно. Без установки соединения с VPN необходимо открыть браузер и зайти на сайт DNSLeakTest.

Этот сайт вернёт IP адрес, назначенный вашим Интернет-провайдером. Для того, чтобы проверить, какие DNS сервера используются, необходимо нажать на **Extended Test**.

Теперь, установив соединение, используя VPN клиент и необходимо обновить страницу в браузере. Выдаваемый IP адрес должен быть совершенно другим. Теперь в Интернете вы используете этот новый IP адрес. Нажмите **Extended Test** ещё раз, чтобы проверить настройки DNS и убедитесь, что теперь используются DNS сервера VPN.

Шаг 14. Отзыв клиентских сертификатов

Время от времени, может понадобиться отозвать клиентский сертификат для предотвращения доступа к серверу VPN.

Для этого необходимо зайти в директорию центра сертификации и ввести команды:

```
cd ~/openvpn-ca
source vars
```

Далее используйте команду revoke-full с именем клиента, сертификат которого вы хотите отозвать:

```
./revoke-full client1
```

Вывод результатов работы этой команды будет оканчиваться ошибкой 23. Это нормально. В результате работы будет создан файл crl.pem в директории keys с необходимой для отзыва сертификата информацией.

Необходимо переместить этот файл в директорию /etc/openvpn:

```
sudo cp ~/openvpn-ca/keys/crl.pem /etc/openvpn
```

Далее открыть файл конфигурации сервера OpenVPN:

```
sudo nano /etc/openvpn/server.conf
```

Добавить в конец файла строку crl-verify. Сервер OpenVPN будет проверять список отозванных сертификатов каждый раз, когда кто-то устанавливает соединение с сервером.

```
crl-verify crl.pem
```

Сохраните и закройте файл (CTRL-X, затем Y, затем ENTER).

Перезапустите OpenVPN для завершения процесса отзыва сертификата:

```
sudo systemctl restart openvpn@server
```

Теперь клиент не сможет устанавливать соединение с сервером OpenVPN используя старый сертификат.

Для отзыва дополнительных сертификатов выполните следующие шаги:

1.Сгенерируйте новый список отозванных сертификатов используя команду source vars в директории ~/openvpn-ca и выполните команду revoke-full с именем клиента.
2.Скопируйте новый список отозванных сертификатов в директорию /etc/openvpn перезаписав тем самым старый список.
3.Перезапустите сервис OpenVPN.

Эта процедура может быть использована для отзыва любых созданных ранее сертификатов.

Выводы по главе три

В данном разделе был рассмотрен способ настройки VPN посредством PPTP протокола стандартными средствами OS Windows. PPTP небезопасен (даже его создатели в Microsoft отказались от него), поэтому его использования следует избегать. В то время, как простота установки и кроссплатформенная совместимость являются привлекательными, L2TP/IPsec имеет те же преимущества и является более безопасным. А так же настройка полноценного VPN-сервера в OS Linux. OpenVPN является лучшим решением VPN несмотря на необходимость стороннего программного обеспечения во всех операционных системах. Это надежный, быстрый и безопасный протокол, хотя и требует немного больше усилий, чем другие протоколы. Первый вариант несмотря на предельную простоту настройки является крайне незащищенным, так что моей рекомендацией будет — не использовать его в повседневной деятельности, а тем более в профессиональной. Несмотря на слабую защищенность PPTP протокола — понимание принципов его работы является базой более полного понимания защиты информации при передачи её через полностью незащищенные и недостаточно защищенные беспроводные соединения. Второй вариант является гораздо более сложным для понимания и настройки и подойдет скорее опытным пользователям. Данный вариант установки VPN соединения отличается предельной гибкостью настройки в отличие от практически всех VPN сервисов, которые представлены на рынке в данный момент. Данная реализация защищенного соединения позволяет полностью удовлетворить потребность в анонимности или безопасной передаче информации как в профессиональной деятельности, так и при личном использовании.

ЗАКЛЮЧЕНИЕ

Было проведено изучение современных беспроводных сетей на канальном, сетевом, транспортном и прикладном уровнях. Возможности и способы их применения, а также их способность сохранять конфиденциальность, целостность и непротиворечивость, передаваемой ими информации. В результате анализа уязвимостей в практической части работы были представлены два способа повысить защищенность информации, при передаче её через беспроводные локальные сети, а также через сеть интернет.

Корпоративные или домашние беспроводные сети очень удобны, так как можно использовать компьютер практически в любом месте, а также подключаться к другим компьютерам этой сети и выходить в интернет. Однако если беспроводная сеть не защищена, то её использование может поставить под угрозу конфиденциальность передаваемой информации. Например, хакерское «облако» может:

- перехватить любые получаемые и отправляемые данные;
- получить доступ к вашим файлам;
- несанкционированно подключиться к интернету и полностью использовать пропускную способность канала связи или израсходовать лимит трафика.

Некоторые советы по интернет-безопасности помогут вам защитить вашу беспроводную сеть:

- **Не используйте пароль, установленный по умолчанию**
  Хакер может легко узнать стандартный пароль, заданный производителем для вашего беспроводного маршрутизатора, и использовать его для доступа к вашей беспроводной сети. Разумнее будет изменить пароль администратора для беспроводного маршрутизатора. При выборе нового пароля попробуйте подобрать сложный набор чисел и букв и не используйте пароль, который можно легко угадать.

- **Не разрешайте беспроводному устройству сообщать о своем присутствии**
  Отключите вещание сетевого имени (SSID), чтобы ваше беспроводное устройство не сообщало всем о своем присутствии.

•Измените SSID устройства

Хакер может легко узнать SSID, устанавливаемый по умолчанию производителем устройства, и затем использовать его, чтобы найти вашу беспроводную сеть. Измените SSID вашего устройства, установленный по умолчанию. Не используйте для него имя, которое можно легко угадать.

•Шифруйте данные

Убедитесь, что в настройках соединения включена функция шифрования. Если устройство поддерживает WPA-шифрование, используйте его. Если нет, используйте WEP-шифрование.

•Обеспечьте защиту от вредоносных программ и интернет-атак

Обязательно установите надежный антивирус на всех компьютерах и устройствах. Для своевременного обновления антивируса включите автоматическое обновление в настройках продукта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Александр Скуснов, «Тестирование точек доступа: беспроводной Интернет в каждую квартиру», компьютерный еженедельник «Upgrade», № 44 (186), 2004 г.

2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. No 1(1). С.2-9.

3. Варгаузин В.А. Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедиа. 2005. № 6. – С. 23-27.

4. Вишневский В. М. Теоретические основы проектирования компьютерных сетей М.: Техносфера. 2003. — 512 с.

5. Гольчевский Ю.В., Некрасов А.Н. К вопросу о кибербезопасности Интернет – пользователей // Известия Тульского государственного университета. Технические науки. 2013. No 3. С. 235-261.

6. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Информационное право. 2013. No 5. С. 10-13.

7. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. No 1(1). С. 10-16.

8. Кантор Л. Я. Спутниковая связь и вещание. Справочник / Л. Я. Кантор [и др.]. —2-еизд., перераб. и доп. — М. : Радио и связь, 1988. — 344 с.

9. Капто А.С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. No 7. С. 616.

10. Карцхия А.А. Развитие законодательства о промышленной собственности и реформа гражданского законодательства Российской Федерации // Мониторинг правоприменения. 2013. No 1. С.14-21.

11. Крекрафт, Д. Аналоговая электроника.Схемы,системы,обработка сигнала / Д.Крекрафт,С.Джерджли .— М. : Техносфера, 2005 .— 360с

12. Лихоносов А. Словарь-справочник по информационной безопасности. – М.: МФПА, 2010. — 390 с

13. Макаров С. Б. Передача дискретных сообщений по радиоканалам с ограниченной полосой пропускания / С. Б. Макаров, И. А. Цикин. — М. : Радио и связь, 1988. — 304 с.

14. Марков А.С., Цирлов В.Л. Управление рисками – нормативный вакуум информационной безопасности//Открытые системы. СУБД. 2007. No 8. С. 63-67.

15. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. No 1(1). С.61-64.

16. Олифер В. Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010 – 944 с.

17. Остроумов Б.А. Михаил Александрович Бонч-Бруевич // Радио. 1967. № 4. – С. 5.

18. Педжман Рошан, Джонатан Лиэри. Основы построения беспроводных локальных сетей стандарта 802.11. Руководство Cisco = 802.11 Wireless Local-Area Network Fundamentals. — : «Вильямс», 2004. — С. 304. — ISBN 5-8459-0701-2.

19. Пескова, С. А. Сети и телекоммуникации : учеб. пособие для вузов / С. А. Пескова, А. В. Кузин, А. Н. Волков .— 3-е изд., стер. — М. : Академия, 2008 .— 351с.

20. Попова Ю. Рупор революции // Энергия промышленного роста. 2009. № 8. – С. 34.

21. Пушкарев О.И. Кирпичики для построения сети ZigBee // Беспроводные технологии. 2006. № 1. – С. 34-38.

22. Росс Д. Wl-Pl. Беспроводные сети. Установка. Конфигурирование. Использование. - М.; ИТ Пресс, 2006. - 312 с.

23. Рошан П. Диэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. - М.: Бином, 2004. - 304 с.

24. Семенов Ю.А. Протоколы и ресурсы Интернет. – М.: Радио и связь, 1996. – 320 с.

25. Скляр Б. Цифровая связь М.: Вильямс. 2003 — 1104 с.

26. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2012 – 960 с.

27. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. No 1(1). С.17-27.

28. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. No 3. С. 4-14.