**Лекция №4.**

**Угрозы и риски безопасности беспроводных сетей**

Главное отличие беспроводных сетей от проводных связано с абсолютно неконтролируемой областью между конечными точками сети. В достаточно широком пространстве сетей беспроводная среда никак не контролируется. Современные беспроводные технологии предлагают ограниченный набор средств управления всей областью развертывания сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд нападений, которые были невозможны в проводной сети. Обсудим характерные только для беспроводного окружения угрозы безопасности, оборудование, которое используется при атаках, проблемы, возникающие при роуминге от одной точки доступа к другой, укрытия для беспроводных каналов и криптографическую защиту открытых коммуникаций.

**4.1. Подслушивание**

Наиболее распространенная проблема в таких открытых и неуправляемых средах, как беспроводные сети, - возможность анонимных атак. Анонимные вредители могут перехватывать радиосигнал и расшифровывать передаваемые данные.

Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое используется для обычного доступа к этой сети. Чтобы перехватить передачу, злоумышленник должен находиться вблизи от передатчика. Перехваты такого типа практически невозможно зарегистрировать, и еще труднее помешать им. Использование антенн и усилителей дает злоумышленнику возможность находиться на значительном растоянии от цели в процессе перехвата.

Подслушивание позволяет собрать информацию в сети, которую впоследствии предполагается атаковать. Первичная цель злоумышленника - понять, кто использует сеть, какие данные в ней доступны, каковы возможности сетевого оборудования, в какие моменты его эксплуатируют наиболее и наименее интенсивно и какова территория развертывания сети. Все это пригодится для того, чтобы организовать атаку на сеть. Многие общедоступные сетевые протоколы передают такую важную информацию, как имя пользователя и пароль, открытым текстом. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Даже если передаваемая информация зашифрована, в руках злоумышленника оказывается текст, который можно запомнить, а потом уже раскодировать.

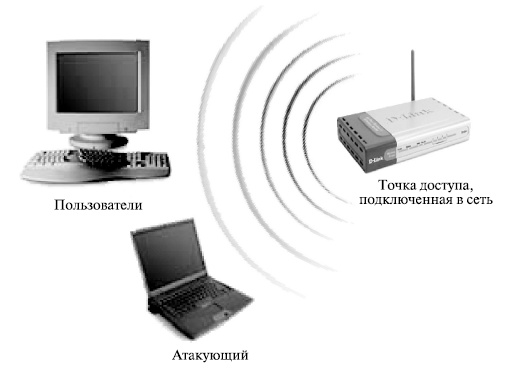


Рис. 1.  Атака "подслушивание"

Другой способ подслушивания - подключение к беспроводной сети. Активное подслушивание в локальной беспроводной сети обычно основано на неправильном использовании протокола *Address Resolution Protocol* (ARP). Изначально эта технология была создана для "прослушивания" сети. В действительности мы имеем дело с атакой типа MITM (Man In The Middle - "человек посередине") на уровне связи данных. Они могут принимать различные формы и используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Когда жертва атаки инициирует соединение, мошенник перехватывает его и затем завершает соединение с требуемым ресурсом, а потом пропускает все соединения с этим ресурсом через свою станцию. При этом атакующий может посылать и изменять информацию или подслушивать все переговоры и потом расшифровывать их.

Атакующий посылает ARP-ответы, на которые не было запроса, к целевой станции локальной сети, которая отправляет ему весь проходящий через нее трафик. Затем злоумышленник будет отсылать пакеты указанным адресатам.

Таким образом, беспроводная станция может перехватывать трафик другого беспроводного клиента (или проводного клиента в локальной сети).

**4.2. Отказ в обслуживании (Denial of Service - DOS)**

Полную парализацию сети может вызвать атака типа DOS. Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом. Эта атака выключает все коммуникации в определенном районе. Если она проводится в достаточно широкой области, то может потребовать значительных мощностей. Атаку DOS на беспроводные сети трудно предотвратить или остановить. Большинство беспроводных сетевых технологий использует нелицензированные частоты - следовательно, допустима интерференция от целого ряда электронных устройств.



Рис. 2.  Атака "отказ в обслуживании" в беспроводных коммуникациях

**4.3. Глушение клиентской станции**

Глушение в сетях происходит тогда, когда преднамеренная или непреднамеренная интерференция превышает возможности отправителя или получателя в канале связи, и канал выходит из строя. Атакующий может использовать различные способы глушения.

Глушение клиентской станции дает мошеннику возможность подставить себя на место заглушенного клиента. Также глушение может использоваться для отказа в обслуживании клиента, чтобы ему не удавалось реализовать соединение. Более изощренные атаки прерывают соединение с базовой станцией, чтобы затем она была присоединена к станции злоумышленника.

**4.4. Глушение базовой станции**

Глушение базовой станции предоставляет возможность подменить ее атакующей станцией. Такое глушение лишает пользователей доступа к услугам.



Рис. 3.  Атака глушения клиента для перехвата соединения



Рис. 4.  Атака глушения базовой станции для перехвата соединения

Как отмечалось выше, большинство беспроводных сетевых технологий использует нелицензированные частоты. Поэтому многие устройства, такие как радиотелефоны, системы слежения и микроволновые печи, могут влиять на работу беспроводных сетей и глушить беспроводное соединение. Чтобы предотвратить такие случаи непреднамеренного глушения, прежде чем покупать дорогостоящее беспроводное оборудование, надо тщательно проанализировать место его установки. Такой анализ поможет убедиться в том, что другие устройства не помешают коммуникациям.

**4.5. Угрозы криптозащиты**

В беспроводных сетях применяются криптографические средства для обеспечения целостности и конфиденциальности информации. Однако оплошности приводят к нарушению коммуникаций и использованию информации злоумышленниками.

WEP - это криптографический механизм, созданный для обеспечения безопасности сетей стандарта 802.11. Этот механизм разработан с единственным статическим ключом, который применяется всеми пользователями. Управляющий доступ к ключам, частое их изменение и обнаружение нарушений практически невозможны. Исследование WEP-шифрования выявило уязвимые места, из-за которых атакующий может полностью восстановить ключ после захвата минимального сетевого трафика. В Internet есть средства, которые позволяют злоумышленнику восстановить ключ в течение нескольких часов. Поэтому на WEP нельзя полагаться как на средство аутентификации и конфиденциальности в беспроводной сети. Использовать описанные криптографические механизмы лучше, чем не использовать никаких, но, с учетом известной уязвимости, необходимы другие методы защиты от атак. Все беспроводные коммуникационные сети подвержены атакам прослушивания в период контакта (установки соединения, сессии связи и прекращения соединения).

Сама природа беспроводного соединения не позволяет его контролировать, и потому оно требует защиты. Управление ключом, как правило, вызывает дополнительные проблемы, когда применяется при роуминге и в случае общего пользования открытой средой. Далее мы более внимательно рассмотрим проблемы криптографии и их решения.

**4.6. Анонимность атак**

Беспроводной доступ обеспечивает полную анонимность атаки. Без соответствующего оборудования в сети, позволяющего определять местоположение, атакующий может легко сохранять анонимность и прятаться где угодно на территории действия беспроводной сети. В таком случае злоумышленника трудно поймать и еще сложнее передать дело в суд.

В недалеком будущем прогнозируется ухудшение распознаваемости атак в Internet из-за широкого распространения анонимных входов через небезопасные точки доступа. Уже существует много сайтов, где публикуются списки таких точек, которые можно использовать с целью вторжения. Важно отметить, что многие мошенники изучают сети не для атак на их внутренние ресурсы, а для получения бесплатного анонимного доступа в Internet, прикрываясь которым, они атакуют другие сети. Если операторы связи не принимают мер предосторожности против таких нападений, они должны нести ответственность за вред, причиняемый другим сетям при использовании их доступа к Internet.

**4.7. Физическая защита**

Устройства беспроводного доступа к сети должны быть маленькими и переносимыми (КПК, ноутбуки), как и точки доступа. Кража таких устройств во многом приводит к тому, что злоумышленник может попасть в сеть, не предпринимая сложных атак, т. к. основные механизмы аутентификации в стандарте 802.11 рассчитаны на регистрацию именно физического аппаратного устройства, а не учетной записи пользователя. Так что потеря одного сетевого интерфейса и несвоевременное извещение администратора может привести к тому, что злоумышленник получит доступ к сети без особых хлопот.

### 4.8. Определение антенны

Антенну можно определить как проводник, используемый для излучения или улавливания электромагнитной энергии из пространства. Для передачи сигнала радиочастотные электрические импульсы передатчика с помощью антенны преобразуются в электромагнитную энергию, которая излучается в окружающее пространство. При получении сигнала энергия электромагнитных волн, поступающих на антенну, преобразуется в радиочастотные электрические импульсы, после чего подается на приемник.

Как правило, при двусторонней связи одна и та же антенна используется как для приема, так и для передачи сигнала. Такой подход возможен, потому что любая антенна с равной эффективностью поставляет энергию из окружающей среды к принимающим терминалам и от передающих терминалов в окружающую среду.

Для правильной настройки антенн разберем некоторые ее характеристики.

#### 4.9. Диаграмма направленности

Антенны излучают энергию во всех направлениях. Однако в большинстве случаев эффективность передачи сигнала для различных направлений неодинакова. Наиболее распространенным способом определения эффективности антенны является диаграмма направленности, которая представляет собой зависимость излучающих свойств антенны от пространственных координат. Диаграммы направленности антенн представляются как двухмерное поперечное сечение трехмерной диаграммы.

Один из наиболее простых типов диаграммы направленности соответствует идеальному случаю так называемой изотропной антенны. Под изотропной антенной понимают точку в пространстве, которая излучает энергию одинаково во всех направлениях. Диаграмма направленности для изотропной антенны представляет собой сферу, центр которой совпадает с положением антенны. Расстояние от антенны до любой точки диаграммы направленности прямо пропорционально энергии, которая была излучена антенной в данном направлении. Рядом представлен еще один идеализированный случай - направленная антенна с одним выделенным направлением излучения (вдоль горизонтальной оси).

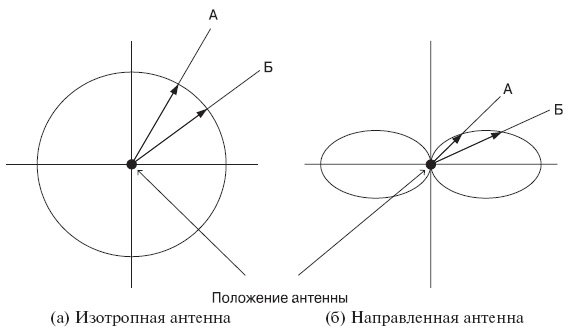


Рис. 5.  Диаграммы направленности

Размер диаграммы направленности может быть произвольным. Важно лишь, чтобы в каждом направлении были соблюдены пропорции. Чтобы на основе относительного расстояния определить приведенную мощность в заданном направлении, от точки размещения антенны до пересечения с диаграммой направленности проводят прямую линию под соответствующим углом наклона.

#### 4.10. Поляризация антенн

Важной характеристикой антенны является ее поляризация. В системах радиодоступа используют антенны с вертикальной, горизонтальной и круговой (с правым и левым вращением) поляризациями.

Учет поляризации позволяет получить дополнительные энергетические преимущества при решении задач электромагнитной совместимости, планировании зон обслуживания и т. д. При заполнении определенного пространства точками доступа до предельного уровня, после которого взаимные радиопомехи начинают мешать нормальной работе сетей, достаточно изменить поляризацию антенн, после чего можно продолжать наращивать радиосеть.

В плоской электромагнитной волне векторы вертикального электрического Eи магнитного Hполей в каждый момент времени ориентированы в пространстве определенным образом. Поляризация электромагнитной волны является ее пространственно-временной характеристикой и определяется видом траектории, описываемой концом вектора электрического поля в фиксированной точке пространства. На антеннах с поляризацией на задней стороне есть указатель в виде стрелки, который и определяет необходимую поляризацию.

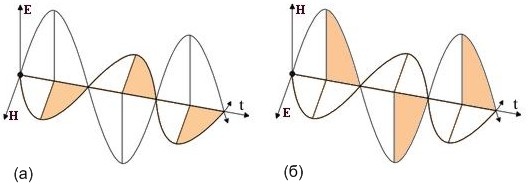


Рис. 6.  Вертикальная (а) и горизонтальная (б) поляризации

При круговой или циклической поляризации электромагнитное поле вращается вокруг оси Xс определенным циклом, или шагом, так, что в разных точках пространства принимает или вертикальную, или горизонтальную поляризацию. Такой вид поляризации применяется сравнительно редко.

#### 4.11. Коэффициенты усиления антенн

Коэффициент усиления является мерой направленности антенны. Данный параметр определяется как отношение мощности сигнала, излученного в определенном направлении, к мощности сигнала, излучаемого идеальной ненаправленной антенной в любом направлении.

Впервые использованная для измерений интенсивности сигнала единица измерения децибел была названа так в честь Александра Грэма Бэлла. Значения в децибелах вычисляются по логарифмической шкале, что позволяет обеспечить спецификацию характеристик в широком диапазоне напряжений или мощностей.

Увеличение мощности сигнала в одном направлении возможно лишь за счет остальных направлений распространения. Другими словами, увеличение мощности сигнала в одном направлении влечет за собой уменьшение мощности в других направлениях. Необходимо отметить, что коэффициент усиления характеризует направленность сигнала, а не увеличение выходной мощности по отношению к входной (как может показаться из названия), поэтому данный параметр часто еще называют коэффициентом направленного действия.

### 4.12. Распространение сигнала

При распространении сигнал, излученный антенной, может огибать поверхность Земли, отражаться от верхних слоев атмосферы либо распространяться вдоль линии прямой видимости.

#### 4.13. Дифракция электромагнитных волн

При огибании поверхности Земли путь распространения сигнала в той или иной степени повторяет контур планеты. Передача может производиться на значительные расстояния, намного превышающие пределы прямой видимости. Данный эффект имеет место для частот до 2 МГц. На способность сигналов, принадлежащих данной полосе частот, повторять кривизну земной поверхности влияет фактор дифракции электромагнитных волн. Данное явление связано с поведением электромагнитных волн при наличии препятствий.

Рассеяние электромагнитных волн указанного диапазона в атмосфере происходит таким образом, что в верхние атмосферные слои эти волны не попадают.

#### 4.14. Распространение волн вдоль линии прямой видимости

Если частота радиосигнала превышает 30 МГц, то огибание им земной поверхности и отражение от верхних слоев атмосферы становятся невозможными. В этом случае связь должна осуществляться в пределах прямой видимости.



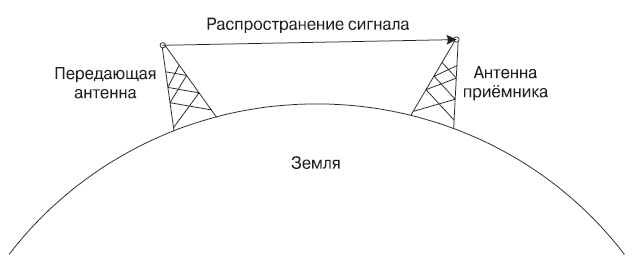


Рис. 8.  Распространение сигнала вдоль линии видимости (частота свыше 30 МГц)

При связи через спутник сигнал с частотой свыше 30 МГц не будет отражаться ионосферой. Такой сигнал может передаваться от наземной станции к спутнику и обратно при условии, что спутник не находится за пределами горизонта. При наземной связи передающая и принимающая антенны должны находиться в пределах эффективной линии прямой видимости. Использование термина "эффективный" связано с тем, что волны сверхвысокой частоты искривляются и преломляются атмосферой. Степень и направление искривления зависят от различных факторов. Однако, как правило, искривления сверхвысокочастотных волн повторяют кривизну поверхности Земли. Поэтому такие волны распространяются на расстояние, превышающее оптическую линию прямой видимости. Так как связь между точками доступа, работающими в стандартах 802.11a, 802.11b и 802.11g обычно рассчитывается на линию прямой видимости, то в следующей главе рассмотрим, как влияет окружающая среда на полезный сигнал.

### 4.15. Передача сигнала в пределах линии прямой видимости

Для любой системы связи справедливо утверждение, что принимаемый сигнал отличается от переданного. Данный эффект является следствием различных искажений в процессе передачи. При передаче аналогового сигнала искажения приводят к его случайному изменению, что проявляется в ухудшении качества связи. Если же передаются цифровые данные, искажения приводят к появлению двоичных ошибок - двоичная единица может преобразоваться в нуль и наоборот. Рассмотрим различные типы искажений, а также их влияние на пропускную способность каналов связи в пределах прямой видимости. Наиболее важными являются следующие типы искажений:

* затухание или амплитудное искажение сигнала;
* потери в свободном пространстве;
* шум;
* атмосферное поглощение;

#### 

#### 4.16. Затухание

При передаче сигнала в любой среде его интенсивность уменьшается с расстоянием. Такое ослабление, или затухание, в общем случае логарифмически зависит от расстояния. Как правило, затухание можно выразить как постоянную потерю интенсивности (в децибелах) на единицу длины. При рассмотрении затухания важны три фактора.

1. Полученный сигнал должен обладать мощностью, достаточной для его обнаружения и интерпретации приемником.
2. Чтобы при получении отсутствовали ошибки, мощность сигнала должна поддерживаться на уровне, в достаточной мере превышающем шум.
3. При повышении частоты сигнала затухание возрастает, что приводит к искажению.

Первые два фактора связаны с затуханием интенсивности сигнала и использованием усилителей или ретрансляторов. Для двухточечного канала связи мощность сигнала передатчика должна быть достаточной для четкого приема. В то же время интенсивность сигнала не должна быть слишком большой, так как в этом случае контуры передатчика или приемника могут оказаться перегруженными, что также приведет к искажению сигнала. Если расстояние между приемником и передатчиком превышает определенную постоянную, свыше которой затухание становится неприемлемо высоким, для усиления сигнала в заданных точках пространства располагаются ретрансляторы или усилители. Задача усиления сигнала значительно усложняется, если существует множество приемников, особенно если расстояние между ними и передающей станцией непостоянно.

Третий фактор списка известен как амплитудное искажение. Вследствие того, что затухание является функцией частоты, полученный сигнал искажается по сравнению с переданным, что снижает четкость приема. Для устранения этой проблемы используются методы выравнивания искажения в определенной полосе частот. Одним из возможных подходов может быть использование устройств, усиливающих высокие частоты в большей мере, чем низкие.

#### 4.17. Потери в свободном пространстве

Для любого типа беспроводной связи передаваемый сигнал рассеивается по мере его распространения в пространстве. Следовательно, мощность сигнала, принимаемого антенной, будет уменьшаться по мере удаления от передающей антенны. Для спутниковой связи упомянутый эффект является основной причиной снижения интенсивности сигнала. Даже если предположить, что все прочие причины затухания и ослабления отсутствуют, переданный сигнал будет затухать по мере распространения в пространстве.

Причина этого - распространение сигнала по все большей площади. Данный тип затухания называют потерями в свободном пространстве и вычисляют через отношение мощности излученного сигнала к мощности полученного сигнала. Для вычисления того же значения в децибелах следует взять десятичный логарифм от указанного отношения, после чего умножить полученный результат на 10.

Следовательно, если длина волны несущей и их разнесение в пространстве остаются неизменными, увеличение коэффициентов усиления передающей и приемной антенн приводит к уменьшению потерь в свободном пространстве.

#### 4.18. Шум

Для любой передачи данных справедливо утверждение, что полученный сигнал состоит из переданного сигнала, модифицированного различными искажениями, которые вносятся самой системой передачи, а также из дополнительных нежелательных сигналов, взаимодействующих с исходной волной во время ее распространения от точки передачи к точке приема. Эти нежелательные сигналы принято называть шумом. Шум является основным фактором, ограничивающим производительность систем связи.

Шумы можно разделить на четыре категории:

* тепловой шум;
* интермодуляционные шумы;
* перекрестные помехи;
* импульсные помехи.

Тепловой шум является результатом теплового движения электронов. Данный тип помех оказывает влияние на все электрические приборы, а также на среду передачи электромагнитных сигналов.

Если сигналы разной частоты передаются в одной среде, может иметь место интермодуляционный шум. Интермодуляционным шумом являются помехи, возникающие на частотах, которые представляют собой сумму, разность или произведение частот двух исходных сигналов. Например, смешивание двух сигналов, передаваемых на частотах f1 и f2 соответственно, может привести к передаче энергии на частоте f1 + f2. При этом данный паразитный сигнал может интерферировать с сигналом связи, передаваемым на частоте f1 + f2.

С перекрестными помехами сталкивался каждый, кто во время использования телефона переменно слышал разговор посторонних людей. Данный тип помех возникает вследствие нежелательного объединения трактов передачи сигналов. Такое объединение может быть вызвано сцеплением близко расположенных витых пар, по которым передаются множественные сигналы.

Перекрестные помехи могут возникать во время приема посторонних сигналов антеннами. Несмотря на то, что для указанного типа связи используют высокоточные направленные антенны, потерь мощности сигнала во время распространения избежать все же невозможно. Как правило, мощность перекрестных помех равна по порядку (или ниже) мощности теплового шума. Все указанные выше типы помех являются предсказуемыми и характеризуются относительно постоянным уровнем мощности. Таким образом, вполне возможно спроектировать систему передачи сигнала, которая была бы устойчивой к указанным помехам.

Однако кроме вышеперечисленных типов помех существуют так называемые импульсные помехи, которые по своей природе являются прерывистыми и состоят из нерегулярных импульсов или кратковременных шумовых пакетов с относительно высокой амплитудой. Причин возникновения импульсных помех может быть множество, в том числе внешние электромагнитные воздействия (например, молнии) или дефекты (поломки) самой системы связи.

#### 4.19. Атмосферное поглощение

Причиной дополнительных потерь мощности сигнала между передающей и принимающей антеннами является атмосферное поглощение, при этом основной вклад в ослабление сигнала вносят водные пары и кислород. Дождь и туман (капли воды, находящиеся во взвешенном состоянии в воздухе) приводят к рассеиванию радиоволн и в конечном счете к ослаблению сигнала. Указанные факторы могут быть основной причиной потерь мощности сигнала. Следовательно, в областях, для которых характерно значительное выпадение осадков, необходимо либо сокращать расстояние между приемником и передатчиком, либо использовать для связи более низкие частоты.