Беспроводные технологии, работают без физических и логических ограничений своих проводных аналогов. Это значительно повышает гибкость рабочего процесса и эффективность труда пользователей, а также снижает затраты на развертывание сетей. При этом беспроводные сети подвергают сетевую инфраструктуру и пользователей значительным рискам.

## ****Угрозы безопасности беспроводной сети****

**В отличие от традиционных проводных сетей, использующих для передачи информации кабель, то есть среду, которую можно контролировать и защитить физически, беспроводные сети используют общую, неограниченную среду – среду, сигнал в которой распространяется далеко за пределы помещения, где расположено оборудование для передачи.** Обеспечить эквивалент физической безопасности проводных сетей здесь просто невозможно [11]. Единственной физической границей беспроводной сети является уровень этого самого сигнала.Благодаря усилиям поставщиков потребительского Wi-Fi оборудования, развернуть беспроводную сеть сейчас может даже самый неподготовленный пользователь. Большинство устройств поставляется уже настроенными по умолчанию, что позволяет сразу начинать с ними работу, не заглядывая в конфигурацию. Еще большей проблемой является то, что беспроводные пользователи по определению мобильны. Пользователи могут появляться и исчезать, менять свое местоположение, и не привязаны к фиксированным точкам входа, как в случае с проводными сетями – они могут находиться где угодно в зоне покрытия. Всё это значительно осложняет задачу отслеживания источников беспроводных атак.

Кроме того, такая важная составляющая мобильности, как роуминг, является еще одной проблемой обеспечения беспроводной безопасности. На этот разпользователей. В отличие от проводных сетей, где пользователь «привязан» кабелем к определенной розетке и порту коммутатора доступа – в беспроводных сетях пользователь не привязан ни к чему. С помощью специального программного обеспечения достаточно несложно переадресовать его подключение с авторизованной точки доступа на неавторизованную или даже на ноутбук злоумышленника, работающий в режиме программно реализованной точки доступа, открывая возможность для целого ряда атак на ничего не подозревающего пользователя.

Поскольку радиосигналы имеют широковещательную природу, не ограничены стенами зданий и доступны всем приемникам, местоположение которых сложно или вообще невозможно зафиксировать – злоумышленникам особенно легко и удобно атаковать беспроводные сети. Беспроводные технологии, работающие без физических и логических ограничений своих проводных аналогов, значительно повышающие гибкость рабочего процесса и эффективность труда пользователей, снижающие затраты на развертывание сетей, также подвергают сетевую инфраструктуру и пользователей значительным рискам.

**Закладки (RogueDevices, Rogues)**

Закладками называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, зачастую в обход механизмов защиты, определенных корпоративной политикой безопасности. Чаще всего это самовольно установленные точки доступа. Даже если организация не использует беспроводную связь и считает себя в результате такого запрета защищенной от беспроводных атак – внедренная (умышленно или нет) закладка с легкостью исправит это положение. Помимо точек доступа в роли закладки могут выступить домашний роутер, поддерживающийWi-Fi, программная точка доступа, ноутбук с одновременно включенными проводным и беспроводным интерфейсом, сканер, проектор и т.д.

**Нефиксированная природа связи**

Беспроводные устройства не «привязаны» кабелем к розетке и могут менять точки подключение к сети прямо в процессе работы. К примеру, могут происходить случайные ассоциации, когда беспроводной клиент, достаточно доверительно относящейся ко всем беспроводным сетям, или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Такой механизм позволяет злоумышленникам переадресовывать ничего не ведающего пользователя для последующего сканирования уязвимостей, фишинга или атак Man-in-The-Middle[11].

**Неправильно сконфигурированные устройства.**

Некоторые сетевые устройства, могут быть более уязвимы, чем другие – то есть могут быть неправильно сконфигурированы, использовать слабые ключи шифрования или методы аутентификации с известными уязвимостями. Неудивительно, что в первую очередь злоумышленники атакуют именно их. Одна-единственная некорректно сконфигурированная точка доступаможет послужить причиной взлома корпоративной сети. Настройки по умолчанию большинства точек доступа не включают аутентификацию или шифрование, либо используют статические ключи, записанные в руководстве и потому общеизвестные.

**Утечки информации из проводной сети**

Практически все беспроводные сети в какой-то момент соединяются с проводными. Соответственно, любая беспроводная точка доступа может быть использована как плацдарм для атаки. Но это еще не все: некоторые ошибки в конфигурации точек доступа в сочетании с ошибками конфигурации проводной сети могут открывать пути для утечек информации. Наиболее распространенный пример – точки доступа, работающие в режиме моста (Layer 2 Bridge), подключенные в сеть с нарушениями сегментации VLAN (VirtualLocalAreaNetwork–виртуальная локальная частная сеть) и передающие в эфир широковещательные пакеты из проводного сегмента. Некоторые из этих данных могут быть полезными для организаций атак Man-in-The-Middle, различных Poisoning и DoS атак (DenialofService), и просто разведки [11].

Другой распространенный сценарий основывается на особенностях реализации протоколов 802.11. В случае, когда на одной точке доступа настроены сразу несколько ESSID (ExtendedServiceSetIdentifier), широковещательный трафик будет распространятся сразу во все ESSID.

**Активность в нерабочее время**

Поскольку беспроводные сети не ограничиваются пределами помещений, как проводные, подключиться к ним можно в любом месте и в любое время. Из-за этого, многие организации ограничивают доступность беспроводных сетей в своих офисах исключительно рабочими часами (вплоть до физического отключения точек доступа). Таким образом всякая беспроводная активность в сети в нерабочее время должна считаться подозрительной и подлежать расследованию.

**Интерференция**

Поскольку беспроводные сети используют радиоволны, качество работы сети зависит от многих факторов. Наиболее ярким примером является интерференция радиосигналов, способная значительно ухудшить показатели пропускной способности и количества поддерживаемых пользователей, вплоть до полной невозможности использования сети. Источником интерференции может быть любое устройство, излучающее сигнал достаточной мощности в том же частотном диапазоне, что и точка доступа: от соседних точек доступа в условиях густонаселенного офисного центра, до электромоторов на производствеи гарнитур Bluetooth. С другой стороны, злоумышленники могут использовать интерференцию для организации DoS атаки на сеть [12].Закладки, работающие на том же канале, что и легитимные точки доступа, открывают не только доступ в сеть, но и нарушают работоспособность «правильной» беспроводной сети. Кроме того, для реализации атак на конечных пользователей и для проникновения в сеть с помощью атаки Man-In-TheMiddle злоумышленники часто заглушают точки доступа легитимной сети, оставляя только одну — свою точку доступа с тем же самым именем сети.

## Атаки на беспроводную сеть

**Разведка**

Большинство традиционных атак начинаются с разведки, в результате которой злоумышленником определяются дальнейшие пути развития атаки. Для беспроводной разведки используются как средства сканирования беспроводных сетей (NetStumbler, Wellenreiter), так и средства сбора и анализа пакетов, т.к. многие управляющие пакеты WLAN незашифрованы. При этом очень сложно отличить станцию, собирающую информацию, от обычной станции, пытающейся получить авторизованный доступ к сети или от попытки случайной ассоциации.Простые методы защиты, такие как сокрытия названия сети в сигнальных фреймах, рассылаемых точками доступа, и путем отключения ответа на широковещательный запрос ESSID (Broadcast ESSID) являются недостаточными, т.к. атакующий все равно видит беспроводную сеть на определенном радиоканале, и всё, что ему остается – это ждать первого авторизованного подключения к такой сети, т.к. в процессе такого подключения в эфире передается ESSID в незашифрованном виде. После чего такая мера безопасности просто теряет смысл.

**Взлом шифрования**

Злоумышленникам давно доступны специальные средства для взлома сетей, основывающихся на стандарте шифрования WEP. Эти инструменты широко освещены в Интернет и не требуют особых навыков для применения. Они используют уязвимости алгоритма WEP, пассивно собирая статистику трафика в беспроводной сети до тех пор, пока собранных данных не окажется достаточно для восстановления ключа шифрования [13]. С использованием последнего поколения средств взлома WEP, использующих специальные методы инъекции трафика, срок колеблется от 15 секунд до 15 минут. Аналогично, есть уязвимости разной степени опасности и сложности, позволяющие вламывать TKIP и даже WPA2. Единственным надежным методом пока что остается использование WPA2-Enterprise (802.1x) с хотя бы серверными сертификатами.

**Имперсонация и IdentityTheft**

Имперсонация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и то и другое несложно подделать, а подделав – как минимум «откусить» часть пропускной способности сети, вставлять неправильные фреймы с целью нарушения авторизованный коммуникаций, а расколов хоть чуть-чуть алгоритмы шифрования – устраивать атаки на структуру сети (например, ARP Poisoning, как в случае с обнаруженной уязвимостью TKIP) [13].

**Отказывобслуживании (DenialofService, DoS)**

Задачей атаки «Отказ в обслуживании» является либо нарушение показателей качества функционирования сетевых услуг, либо полная ликвидация возможности доступа к ним для авторизованных пользователей [13]. Для этого, к примеру, сеть может быть завалена «мусорными» пакетами (с неправильной контрольной суммой и т.д.), отправленными с легитимного адреса. В случае беспроводной сети отследить источник такой атаки без специального инструментария просто невозможно, т.к. он может находиться где угодно. Кроме того, есть возможность организовать DoS на физическом уровне, просто запустив достаточно мощный генератор помех в нужном частотном диапазоне

## **2.2 Алгоритмы шифрованияиспользуемые в стандарте IEEE 802.11**

### **Алгоритм шифрования RC4**

RC4 - это потоковый шифр с переменным размером ключа, разработанный в 1987 году РономРивестом для RSA DataSecurity, Inc [14]. Алгоритм работает в режиме OFB: поток ключей не зависит от открытого текста. Ядро алгоритма поточных шифров состоит из генератора[гаммы](http://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5" \o "Гаммирование), который выдаёт ключевой поток (гамму). Генератор псевдослучайных чиселформирует последовательность битов, которая затем объединяется с открытым текстом в процедуре шифрования и с шифротекстом в процедуре дешифрования посредством[суммирования по модулю два](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2). Так получается шифрограмма.Для шифрования используется массив чисел, называемый s-блок и два счетчика. Процесс шифрования можно разделить на два этапа:

### Инициализация S-блока

### Генерация псевдослучайного слова K

S-блок имеетразмер 8\*8: S0, S1, . . . ,S255 и инициализируется следующим образом.Сначала s-блок заполняется линейно: S0 = 0, S1 = 1, . . . ,S255 = 255. Затем другим ключом заполняется 256-байтовый массив, при необходимости для заполнения всего массива ключ повторяется: K0, K1, . . . ,K255. Устанавливается значение индекса j равным 0. Затем выполняется следующий алгоритм:

### fori = 0 to 255:

### j = (j + Si + Ki) mod 256

### поменять местами Si и Sj

Для генерации псевдослучайного словаприменяется следующий алгоритм:

### i = (i + 1) mod 256

### j = (j + Si) mod 256

### поменять местами Si и Sj

### t = (Si + Sj) mod 256

### K = St

### Шифрование выполняется примерно в 10 раз быстрее, чем DES.

**Алгоритм шифрования AES**

### AdvancedEncryptionStandard является общеизвестным названием алгоритма Rijndael , который был разработан двумя бельгийскими криптографамиЙоаномДайменом и Винсентом Рэйменом. Алгоритм является блочным и симметричным. Принят в качестве стандарта шифрования данных для гос учреждений в США.AES является упрощенной версией алгоритма Rijndael [14]. С момента появления в публичном доступе, стандарт шифрования AES стал одним из наиболее часто используемых и наиболее безопасных алгоритмов, доступных на сегодняшний деньОригинальный алгоритм Rijndael отличается тем, что поддерживает более широкий набор длин блоков.AES представляет собой алгоритм шифрования 128-битных блоков данных с помощью ключей размером 128, 192 и 256 бит. Ключ, наряду с блоком, является входным данным алгоритма. Состояние (state) ― двумерный массив байтов, состоящий из четырех строк. В алгоритме AES состояние используется для представления блока.Раунд ― итерация цикла преобразований над формой. В зависимости от длины ключа раундов может быть от 10 до 14. Ключ раунда (roundkey) ― ключ, применяемый в раунде. Вычисляется для каждого раунда.Таблица подстановок (S-box) ― таблица, задающая биективное отображение байта в байт. Алгоритм AES состоит из часто повторяющихся раундов шифрования. Сначала на основе 128-битового ключа получают одиннадцать так называемых ключей раундов, каждый из которых имеет размер 128 бит. Каждый раунд включает в себя преобразование с использованием соответствующего криптографического ключа, для того чтобы обеспечить секретность шифрования.

Для шифрования в алгоритме AES применяются следующие процедуры преобразования данных:

### ExpandKey — Вычисление раундных ключей для всех раундов.

### SubBytes — Подстановка байтов с помощью таблицы подстановок;

### ShiftRows — Циклический сдвиг строк в форме на различные величины;

### MixColumns — Смешивание данных внутри каждого столбца формы;

### AddRoundKey — Сложение ключа раунда с формой.

### Преобразование SubBytes заключается в замене каждого байта {xy} формы (где x иy обозначают шестнадцатиричные цифры) на другой, в соответствии с таблицей подстановки[15].Преобразование ShiftRowsзаключается в циклическом сдвиге влево строк формы. Преобразование схематично представлено на рисунке 4. Первая строка остается неизменной. Во второй производится сдвиг на 1 байт, то есть первый байт переносится в конец. В третьей ― сдвиг на 2 байта, в четветрой ― на 3.



Рис. 4. Преобразование ShiftRows

### Преобразование MixColumns заключается в умножении квадратной матрицы 4-гопорядка на каждый столбец формы:

### 

### Над каждым столбцом операция производится отдельно, как показано на рисунке5.



Рис. 5. Преобразование MixColumns

### В преобразовании AddRoundKey 32-битные слова раундного ключа прибавляютсяк столбцам формы с помощью побитовой операции XOR:

= ⊕

### Здесь wi― это столбцы ключа.Над каждым столбцом операция производится отдельно.В алгоритме AES генерируются раундовые ключи на основе ключа шифрования с помощью процедуры ExpandKey. Процедура ExpandKey создает Nb\* (Nr + 1) слов: алгоритму требуется начальный ключ размером Nb, плюс каждый из Nr раундов требует ключ из Nb слов.Шифрование производится по алгоритму, приведенному на рисунке 6.



Рис. 6. Алгоритм шифрования AES

### При дешифровании все преобразования производятся в обратном порядке. Используются следующие обратные преобразования вместо соответствующих шифрующих:

### InvSubBytes ― Подстановка байтов с помощью обратной таблицы подстановок;

### InvShiftRows ― Циклический сдвиг строк в форме на различные величины;

### InvMixColumns ― Смешивание данных внутри каждого столбца формы;

### Процедуры ExpandKey и AddRoundKey остаются неизменными. Ключи раунда используются в обратном порядке.Преобразование InvShiftRowsобратно преобразованию ShiftRows. Первая строка формы остается неизменной. Вторая строка циклически сдвигается вправо на 1 байт, третья ― на 2, четвертая ― на 3.Преобразование InvSubBytesобратно преобразованию SubBytes. Подстановка байтов происходит аналогично с помощью обратной таблицы подстановок. ПреобразованиеInvMixColums обратно преобразованию MixColumns. InvMixColumns преобразует в форме каждый столбец отдельно.

### **Режимы применения алгоритма AES**

### Режим шифрования — метод применения блочного шифра, позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных. При этом для шифрации одного блока могут использоваться данные другого блока. Обычно режимы шифрования используются для модификации процесса шифрования так, чтобы результат шифрования каждого блока был уникальным вне зависимости от шифруемых данных и не позволял сделать какие-либо выводы об их структуре. Это обусловлено, прежде всего, тем, что блочные шифры шифруют данные блоками фиксированного размера, и поэтому существует потенциальная возможность утечки информации о повторяющихся частях данных шифруемых на одном и том же ключе [16]. Существует несколько стандартных режимов шифрования.В стандарте 802.11 – 2012 протоколе инкапсуляции алгоритм AESприменяется в двух режимах:

### Режим счетчика(Counter mode)

### Режим сцепления блоков (CBC)

Режим счетчика (Рис. 7)предполагает возврат на вход соответствующего алгоритма блочного шифрования значения счетчика, накопленного с момента старта. Увеличивая значение счетчика, алгоритм блочного шифрования образует строку битов, которая используется в качестве бегущего ключа[шифра Вернама](http://dic.academic.ru/dic.nsf/ruwiki/290927), т.е. к бегущему ключу и блокам исходного сообщения применяются операции XOR. Чтобы обеспечивать случайность, величина приращения может зависеть от номера блока. Исходный текст и блок зашифрованного текста имеют один и тот же размер блока, как и основной шифр.



Рис. 7. ШифрованиеAES в режиме счетчика

### В режиме CBC (CipherBlockChaining) к каждому блоку открытого текста перед шифрованием прибавляется результат шифрования предыдущего блока с помощью побитовой операции XOR. К первому блоку открытого текста прибавляется InitializationVector, который генерируется случайным образом и обычно передается вместе с шифрованными данными, чтобы их можно было дешифровать [16]. Шифрование в режиме CBC показано на рисунке 8.

### 

### Рис. 8. Шифрование в режиме CBC

### В режиме CBC для шифрования каждого следующего блока нужно иметь результат шифрования предыдущего блока, поэтому шифровать несколько блоков одновременно нельзя. Но можно производить дешифрование нескольких блоков параллельно, поскольку для дешифрования каждого блока нужно иметь только этот блок и предыдущий.

## ****Механизмы защиты информации в локальных беспроводных сетях****

### **Стандарт 802.11 – 2012 определяет два класса алгоритмов защиты беспроводных локальных сетей:**

* Алгоритмы для создания и использования концепции RSNA(RobustSecurityNetworkAssociation), называемые RSNA-алгоритмами(Рис. 9).
* Алгоритмы, которые использовались до принятия концепции RSNA - pre-RSNA-алгоритмы (Рис. 10).

RSNA-алгоритмы включают в себя следующие механизмы защиты:

### TKIP (Temporary Key Integrity Protocol)

### CCMP (Counter Mode with CBC-MAC Protocol)

### BIP (Broadcast Integrity Protocol)

### Процедуры установки и прекращения соединения, включая аутентификацию 802.1x и аутентификацию SAE.

### Процедуры управления ключами



Рис. 9. КонцепцияRSNA

pre-RSNA-алгоритмысостоят из:

### WEP (Wired Equivalent Privacy)

### Аутентификация IEEE 802.11

### Открытая аутентификация

### Аутентификация с общим ключом (sharedkey)



Рис. 10. Механизмы защиты pre-RSNA