Министерство образования и науки Российской Федерации

Государственного образовательного учреждения

Высшего профессионального образования

Тюменский государственный университет

Институт математики и компьютерных наук

*Кафедра информационной безопасности*

**Курсовая работа**

по специальности

на тему

«*Защита беспроводных сетей*»

**Выполнили:**

*Студент группы №357*

*Колбин С.С.*

**Руководитель:**

*Бажин К.А.*

Тюмень, 2009

Содержание.

[Введение. 3](#_Toc232404364)

[1. История развития защиты Wi-Fi. 5](#_Toc232404365)

[2. Опасности которым подвержена незащищенная беспроводная сеть. 6](#_Toc232404366)

[2.1 Ваши сетевые ресурсы будут доступны незнакомцам. 6](#_Toc232404367)

[2.2 Весь сетевой трафик может быть перехвачен для дальнейшего исследования. 6](#_Toc232404368)

[2.3 Ваш интернет-канал может использоваться для любой деятельности, в том числе и незаконной. 6](#_Toc232404369)

[3. Способы защиты от хакеров разного уровня подготовки. 7](#_Toc232404370)

[3.1 Умения нулевого уровня: любой владелец компьютера с беспроводным адаптером. 7](#_Toc232404371)

[3.2 Умения первого уровня: пользователь с общедоступным набором утилит для взлома WLAN 11](#_Toc232404372)

[3.3 Умения BToporo уровня: пользователь с расширенным набором утилит для взлома WEP/WPA-PSK 14](#_Toc232404373)

[3.4 Умения третьего уровня: профессиональный хакер 15](#_Toc232404374)

[Заключение. 18](#_Toc232404375)

[Список используемой литературы. 19](#_Toc232404376)

# Введение.

У беспроводных сетей очень много общего с проводными, но есть и различия. Для того, чтобы проникнуть в проводную сеть, хакеру необходимо физически к ней подключиться. В варианте Wi-Fi ему достаточно установить антенну в ближайшей подворотне в зоне действия сети.

Хотя сегодня в защите Wi-Fi-сетей и применяются сложные алгоритмические математические модели аутентификации, шифрования данных, контроля целостности их передачи, тем не менее, на начальных этапах распространения Wi-Fi нередко появлялись сообщения о том, что даже не используя сложного оборудования и специальных программ можно было подключиться к некоторым корпоративным сетям просто проезжая мимо с ноутбуком. Появились даже легенды о разъезжающих по крупным городам хакерах (war driver) с антеннами, сооруженными из консервной банки или упаковки из­ под чипсов. Якобы у них даже была своя условная система знаков, которые рисовались на тротуаре и указывали незащищенные должным образом точки доступа. Возможно, так и было, лишь вместо банок из-под чипсов использовались мощные антенны, а условные знаки обозначались на карте, связанной с системой глобального позиционирования (GPS). Данная курсовая работа посвящена защите беспроводных сетей. В ней я хочу рассказать, как можно защитить беспроводную сеть . Специалисты по сетевой безопасности знают, что невозможно полностью защитить сеть и такого понятия как «совершенная защита» просто нет. Для того чтобы правильно спланировать безопасность беспроводной сети (или проводной) нужно учитывать стоимость защищаемых ценностей, стоимость внедрения системы безопасности, а также способности потенциальных атакующих. Другими словами, прежде чем внедрять все меры защиты, известные человечеству, разумнее (и дешевле) внедрить меры защиты от наиболее частых угроз.

Например, беспроводные сети, расположенные в городах, обычно подвергаются атакам чаще, чем сети, расположенные в малонаселённой местности. За день в городе через вашу сеть могут пройти десятки и даже сотни посетителей. Кроме того, злоумышленники могут оставаться незамеченными, находясь в машине, припаркованной неподалёку. С другой стороны, точка доступа, расположенная в доме посередине деревни, вряд ли когда-нибудь увидит чужого посетителя, да и знакомый транспорт будет сразу же заметен.

Для некоторых пользователей настройка безопасности беспроводных сетей кажется сложной, они надеются на "авось пронесёт" и оставляют свою сеть абсолютно открытой, то есть незащищённой. Также люди иногда задаются вопросом, что если они используют сеть только для просмотра интернет страниц и на компьютерах нет секретной информации, то зачем им защищать свою сеть? На этот вопрос есть хороший ответ.

**Цель работы:** провести анализ безопасности беспроводных сетей, выделить методы их защиты и определить особенности каждого проанализированного метода.

# История развития защиты Wi-Fi.

В 1997 году вышел первый стандарт IEEE 802.11, безопасность которого, как оказалось, далека от идеала. Простой пароль SSID (Server Set ID) для доступа в локальную сеть по современным меркам нельзя считать защитой, особенно, учитывая факт, что к Wi-Fi не нужно физически подключаться.

Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII, что соответствует 40 или 104-разрядному шифрованию на статическом уровне. Как показало время, WEP оказалась не самой надёжной технологией защиты. И, кстати, все основные атаки хакеров пришлись как раз-таки на эпоху внедрения WEP.

После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.1Х, который использует вариант динамических 128 разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows ХР поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам.

В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1Х с кодированием протокола интеграции временного ключа Temporal Кеу Integrity Protocol (TКlP), протоколом расширенной аутентификации Extensible Authentication Protocol (ЕАР) и технологией проверки целостности сообщений Message Integrity Check (MIC).

Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPА2, или 802.11i, - максимально защищённый стандарт

2. Опасности которым подвержена незащищенная беспроводная сеть.

Незащищённая беспроводная сеть подвержена трём основным опасностям.

## 2.1 Ваши сетевые ресурсы будут доступны незнакомцам.

Когда кто-то подключается к вашей беспроводной сети, он ничем не отличается от пользователя, подсоединившегося к проводному коммутатору вашей сети. Если вы никак не ограничиваете доступ к общим ресурсам, то незваные гости могут делать всё то же самое, что и известные пользователи. Они могут копировать изменять или даже полностью удалять файлы, каталоги и даже целые диски. Или даже хуже - запускать перехватчики нажатий клавиатуры, "трояны" или другие вредоносные программы, которые будут работать на неизвестных хозяев.

## 2.2 Весь сетевой трафик может быть перехвачен для дальнейшего исследования.

Имея при себе нужные инструменты, можно в режиме реального времени про сматривать посещаемые вами web-страницы, адреса сайтов и, что хуже, перехватывать ваши пароли для дальнейшего использования, чаще всего в корыстных целях.

## 2.3 Ваш интернет-канал может использоваться для любой деятельности, в том числе и незаконной.

Если открытая беспроводная сеть будет использоваться для нелегального распространения фильмов или музыки, то во многих странах за это можно поплатиться иском со стороны правоохранительных органов. Если же канал использовался для передачи на внешний ресурс чего-то более противозаконного, например детской порнографии, или же такой сервер появился внутри сети, проблемы могут быть гораздо более серьёзными. Кроме того, каналом могут воспользоваться спамеры, любители атак DOS и распространители вредоносного ПО, вирусов, да и многие другие.

Вполне разумно раздавать доступ в Интернет всем вашим гостям. Но до тех пор, пока вы не обеспечите серьёзную защиту беспроводной сети, вы рискуете.

Далее в данной курсовой я рассмотрю меры по защите беспроводной сети в соответствии с предполагаемым уровнем умений незваных гостей. Мы приведём способы для защиты от хакеров разного уровня подготовки.

# 3. Способы защиты от хакеров разного уровня подготовки.

## 3.1 Умения нулевого уровня: любой владелец компьютера с беспроводным адаптером.

Для того чтобы взломать незащищённую сеть можно и не обладать какими­либо особыми навыками - каждый владелец компьютера с беспроводным адаптером потенциально способен это сделать. Простота использования чаще упоминается в контексте беспроводных сетевых решений как огромный плюс, однако это палка о двух концах. Во многих случаях, включив компьютер с поддержкой беспроводной сети, пользователь автоматически подключается к точке доступа или видит её в списке доступных.

Ниже приведены меры, которые позволят защитить сеть от случайных посетителей, но ничуть не затруднят доступ к ней более умелым взломщикам. Все меры упорядочены в списке по важности. Большинство из них настолько просты, что их рекомендуется реализовать их все, если позволяет оборудование.

**Смените настройки по умолчанию**

Измените пароль администратора (и имя пользователя, если можно) и идентификатор SSID (имя сети) на точке доступа. Как правило, учётные данные администратора, установленные по умолчанию, **открыты и доступны** для большинства беспроводного оборудования. Поэтому, не заменив их, вы рискуете однажды получить отказ при входе в систему и лишиться возможности управления беспроводной сетью (до тех пор, пока не сбросите все настройки)! Изменить SSID особенно необходимо в том случае, если вы работаете по соседству с другими точками доступа. Если соседние точки доступа окажутся того же производителя, то они имеют тот же SSID по умолчанию, и клиенты, что вполне вероятно, смогут неосознанно подключиться к вашей ТД, а не к своей. Для нового SSID не следует использовать личную информацию! Во время вардрайвинга удавалось заметить следующие SSID:

• имя и фамилия;

• улица, дом, квартира;

• номер паспорта;

• номер телефона.

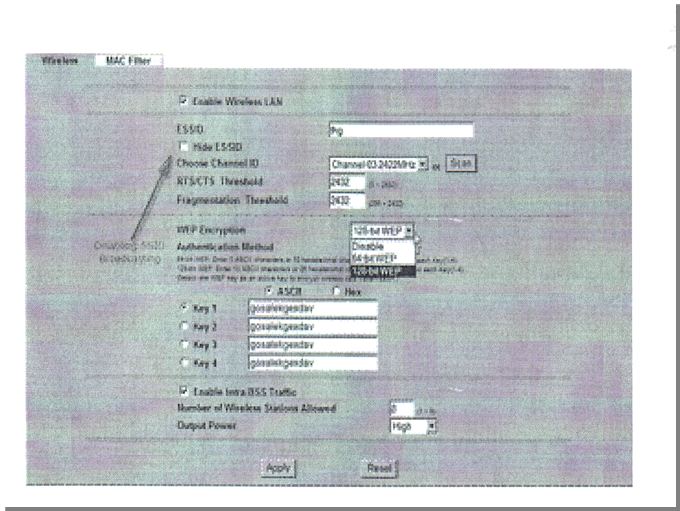
В принципе, если рядом есть несколько точек доступа, то имеет смысл изменить и канал, чтобы избежать взаимных помех. Однако эта мера не особо повлияет на защищённость, поскольку клиенты чаще всего просматривают все доступные каналы.

**Обновите прошивку и, если нужно, оборудование.**

Использование на точке доступа последней версии программного обеспечения также повышает безопасность. В новой прошивке обычно исправлены обнаруженные ошибки, а иногда и добавлены новые возможности защиты. У некоторых новых моделей точек доступа для обновления достаточно пару раз щёлкнуть кнопкой мыши. Точки доступа, выпущенные несколько лет назад, часто уже не поддерживаются производителями, то есть новых прошивок ожидать не стоит. Если же прошивка вашей точки доступа не поддерживает даже **WPA** (Wi-Fi Protected Access), не говоря о **WPA2**, то следует всерьёз задуматься о её замене. То же самое касается адаптеров! В принципе, всё продаваемое сегодня оборудование 802.11g поддерживает, как минимум, WPA и технически способно быть модернизировано до уровня WPА2. Однако производители не всегда торопятся с обновлением старых продуктов.

**Отключите широковещание SSID.**

Большинство точек доступа позволяют отключить широковещание SSID, что может обвести вокруг пальца некоторые утилиты вроде NetstumbIer. Кроме того, скрытие SSID блокирует обнаружение вашей сети средствами встроенной утилиты настройки беспроводной сети Windows ХР (Wireless Zero Configuration) и других клиентских приложений. На Рис. 1 показан пункт отключения широковещания SSID "Hide ESSID" на точке доступа ParkerVision. ("SSID" и "ESSID" в данном случае означают одно и то же).



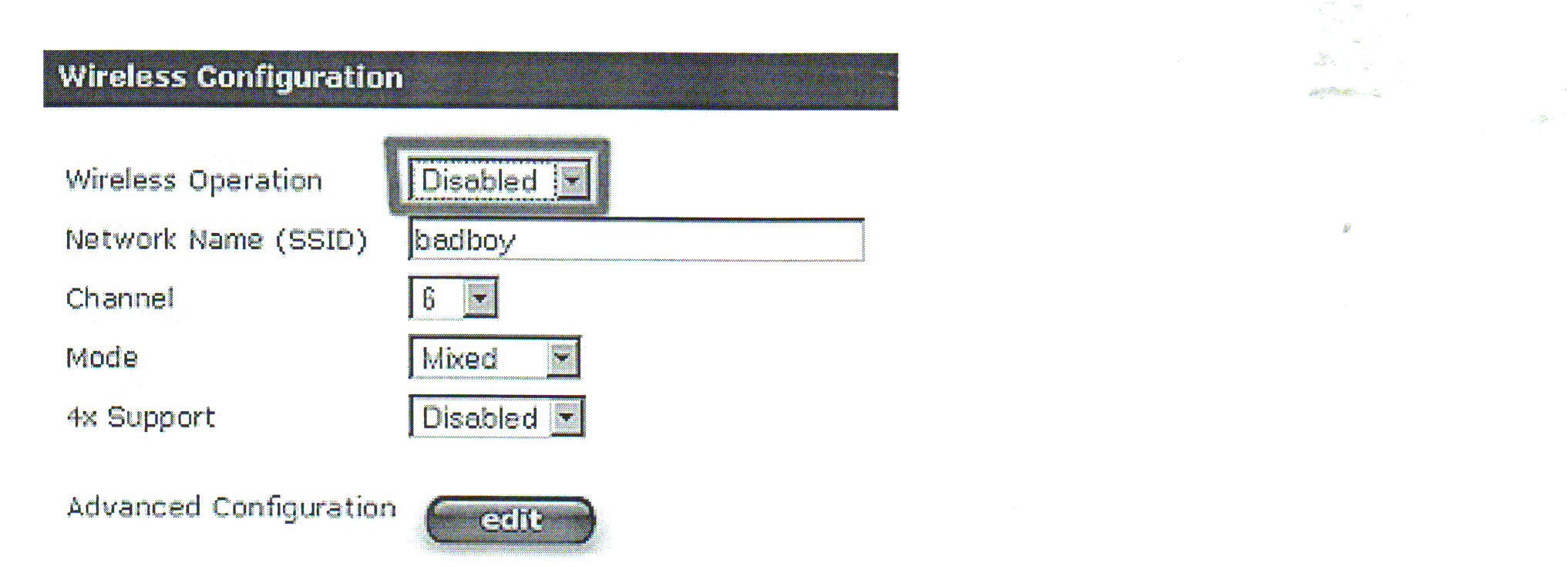
**Рис. 1. Отключение широковещания SSID на точке доступа Раrkеrvisiоn.**

**Примечание.** Отключение широковещания SSID не обезопасит вас от взломщиков, использующих такие средства, как **Kismet** или **АirМаgпеt**. Они определяют наличие беспроводной сети независимо от SSID.

**Выключайте сеть, когда не работаете!**

Часто пользователи пропускают мимо внимания самый простой способ защиты - выключение точки доступа. Раз нет беспроводной сети, то нет и проблем. Простейший таймер может отключать точку доступа, например, на ночь, пока вы ей не пользуетесь. Если для беспроводной сети и для доступа в Интернет вы используете один и тот же беспроводной маршрутизатор, то при этом соединение с Интернетом тоже не будет работать - вполне неплохо.

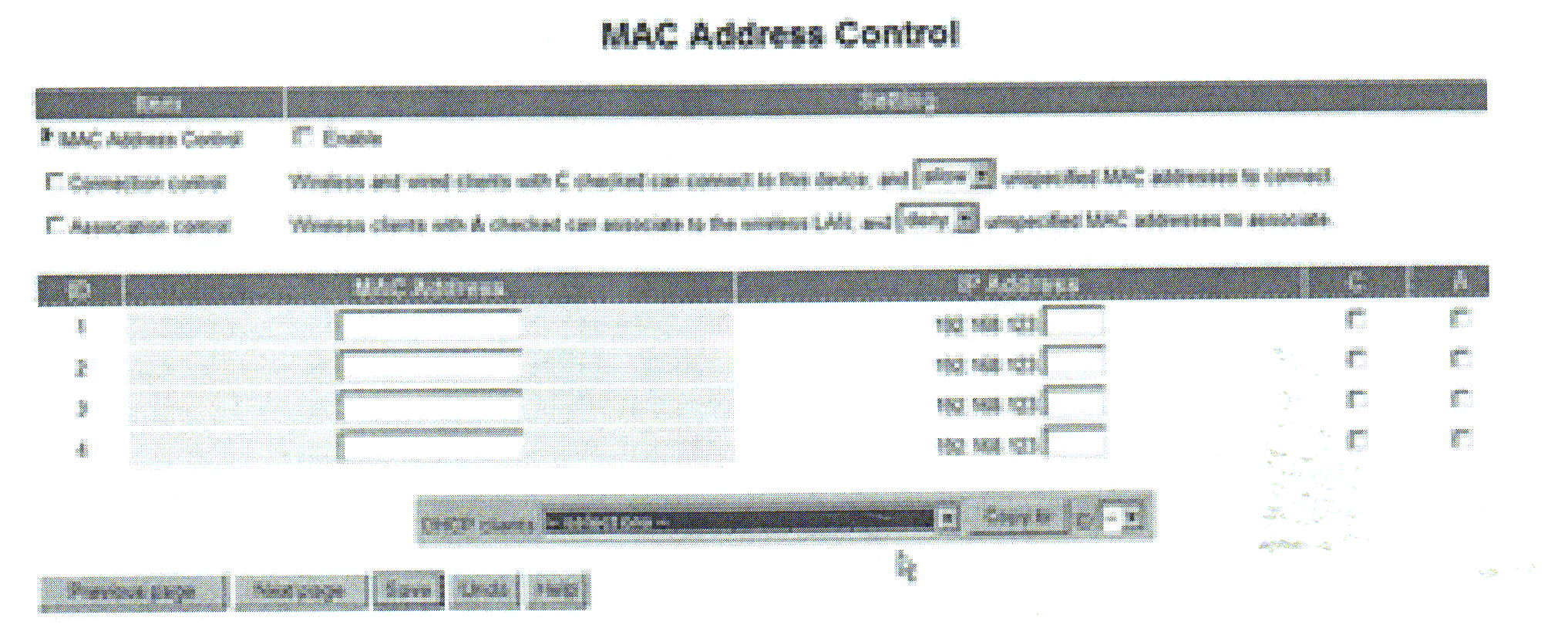
Если же вы не хотите отключать соединение с Интернетом, тогда можно отключать радиомодуль маршрутизатора вручную, если он это позволяет. На **Рис. 2** показан пункт отключения радиомодуля. Такой способ недостаточно надёжен, поскольку он зависит от "человеческого фактора" - можно просто забыть об отключении. Возможно, производители когда-нибудь добавят функцию отключения радиомодуля по расписанию.



**Рис. 2. Отключение радиомодуля.**

**Фильтрация по MAC-адресам**

Фильтрация по MAC-адресам используется для того, чтобы доступ к сети могли получить (или, наоборот, не получить) только те компьютеры, чьи адреса указаны в списке. Фильтрация защитит вашу сеть от новичков, но более опытные хакеры могут легко перехватить MAC-адреса и подменить свой адрес на один из разрешённых.



**Рис. 3. Фильтрация MAC-адресов на точке доступа USR 8011.**

**Снижение мощности передачи**

Лишь некоторые потребительские точки доступа имеют эту функцию, однако снижение мощности передачи позволит ограничить количество как преднамеренных, так и случайных неавторизованных подключений. Впрочем, чувствительность доступных массовому пользователю беспроводных адаптеров постоянно растёт, так что вряд ли стоит *озадачиваться этим способом, особенно если вы это делаете исключительно* из-за безопасности в многоквартирном доме. Опытные хакеры обычно используют мощные направленные антенны, что позволяет им обнаруживать даже очень слабый сигнал и сводит существенность этого пункта к нулю.

## 3.2 Умения первого уровня: пользователь с общедоступным набором утилит для взлома WLAN

Перейдём к более опытным пользователям, которые специально бродят по окрестностям в поисках беспроводных сетей. Некоторые занимаются этим просто из интереса, пытаясь обнаружить, сколько сетей находится рядом. Они никогда не пытаются использовать уязвимые сети. Но есть и менее доброжелательные хакеры, которые подключаются и используют сети, а иногда даже доставляют владельцам неудобства. Все принятые меры нулевого уровня не спасут от взломщиков первого уровня, и незваный гость может проникнуть в сеть. От него можно защититься, используя **шифрование** и **аутентификацию.** С аутентификацией будем разбираться немного позже, пока же остановимся на шифровании. Одно из возможных решений - пропускать весь беспроводной трафик через туннель VPN (Virtual Private Network) - виртуальная частная сеть.

**Шифрование**

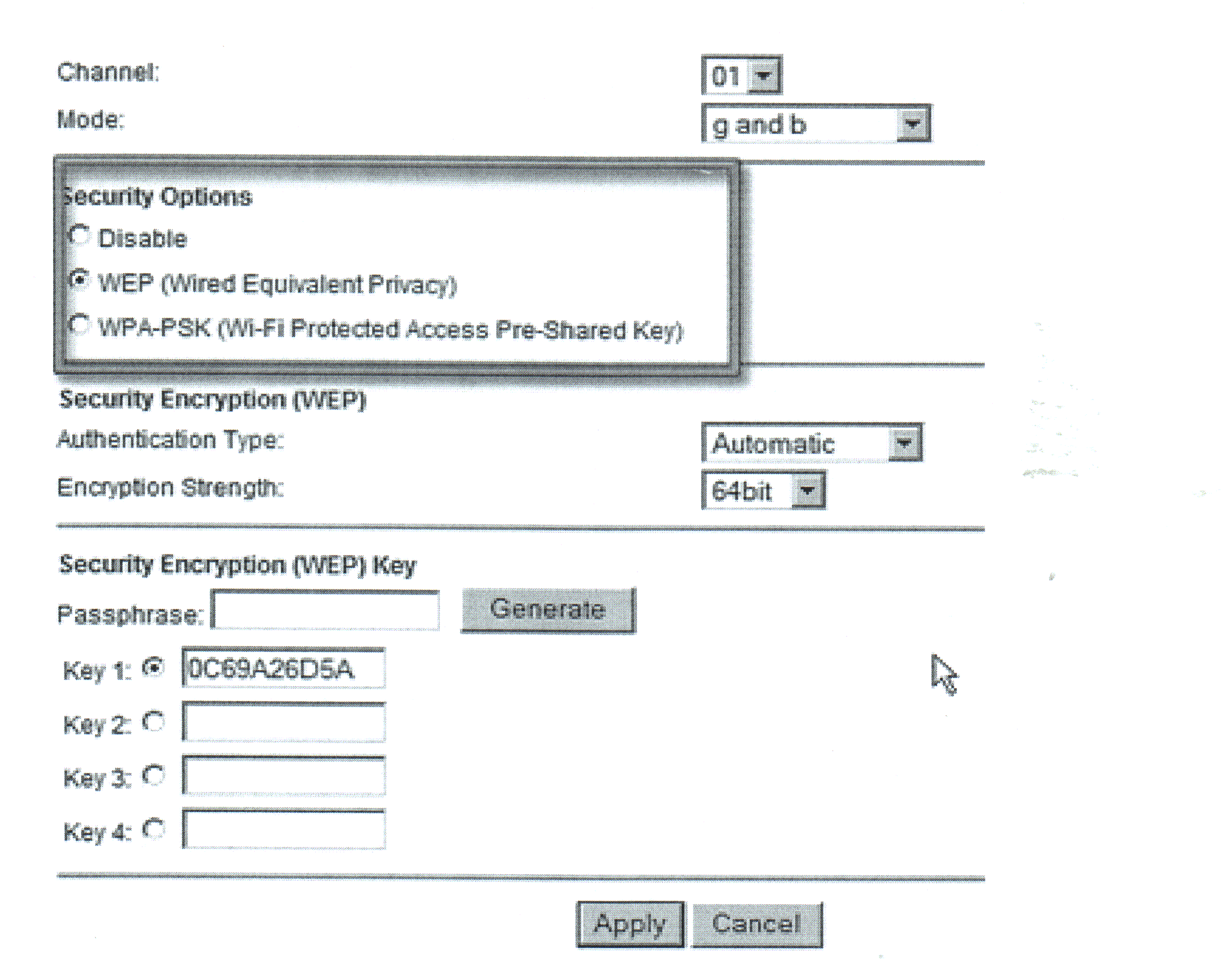
Владельцам беспроводных сетей следует использовать самый надёжный из доступных методов шифрования. Конечно, здесь всё зависит от оборудования, но, так или иначе, обычно можно выбрать WБР, WPA или WPА2. WEP (Wired Equivalent Privacy) - безопасность, эквивалентная проводной сети является наиболее слабым протоколом, но на текущее время он наиболее широко распространён и поддерживается практически всем оборудованием 802.11. Возможно, придётся остановиться на использовании этой технологии и потому, что не все производители беспроводного оборудования выпустили обновления прошивки с поддержкой WPA для оборудования 802.11 Ь. Некоторые до сих пор выпускают оборудование, которое поддерживает только WEP, например - беспроводные VoIP-­телефоны. Таким образом, приходится искусственно снижать безопасность сети из-за того, что не всё оборудование поддерживает более новые технологии.

Как WPA (Wi-Fi Protected Access), так и WPA2 обеспечивают хорошую защиту беспроводной сети, что достигается благодаря более стойкому алгоритму шифрования и улучшенному алгоритму управления ключами. Основное отличие между ними состоит в том, что WPА2 поддерживает более стойкое шифрование AES (Advanced Encryption Standard). Однако, ряд продуктов, поддерживающих WPA , тоже позволяют использовать алгоритм шифрования AES вместо стандартного TKIP.

Большинство продуктов 802.11 g поддерживают WPA, но есть и исключения. Что касается обновления старых продуктов до WPА2, то многие прошивки до сих пор находятся в состоянии разработки, несмотря на то, что стандарт 802.11i, на котором основан WPА2, был утверждён ещё в июне 2004.

Мы рекомендуем, по меньшей мере, использовать WPA. Его эффективность сопоставима с WPА2, и, как мы уже писали, стандарт поддерживается большим количеством оборудования. Конечно, внедрение WPA может потребовать покупки нового оборудования, особенно, если вы используете 802.11b. Однако оборудование 11g стоит сегодня относительно недорого и сможет оправдать себя.

Большинство потребительских точек доступа WPA и WPА2 поддерживают только режим с общим паролем WPA-PSK (Pre-Shared Кеу) **(Рис. 4)**. WPA2 или WPA "Enterprise" (он же WPA "RADIUS") также поддерживается в некотором оборудовании, однако его использование требует наличия сервера RADIUS



**Рис. 4. Шифрование трафика на точке доступа Netgear.**

Для большинства частных беспроводных сетей использование WPA-PSK обеспечит вполне достаточную защиту, но только при выборе относительно длинного и сложного пароля. Не следует использовать только цифры или слова из словаря, поскольку такие программы, как **cowpatty**, позволяют проводить словарные атаки против WPA-РSK.

Роберт Москович (Robert Moskowitz), старший технический директор ICSA Labs, в своей **статье** рекомендовал использовать 128-битное шифрование PSK. К счастью, все реализации WPA позволяют использовать цифробуквенные пароли, то есть для выполнения рекомендация Московича достаточно 16 символов.

В Интернете можно найти множество генераторов паролей, стоит лишь воспользоваться поисковой системой. И, наконец, некоторые производители

оборудования стали продавать точки доступа и беспроводные адаптеры с автоматической настройкой защиты беспроводных соединений. Buffalo Technology. выпустила серию продуктов с технологией **AOSS** (AirStation One­Touch Secure Station). Linksys недавно начала производство и продажу оборудования с поддержкой подобной технологии **SecureEasySetup** от Broadcom.

## 3.3 Умения BToporo уровня: пользователь с расширенным набором утилит для взлома WEP/WPA-PSK

WPA и WPА2 закрывают большинство проблем, которые есть у WEP, но они всё же остаются уязвимыми, особенно в варианте PSK. Взлом WPA и WPА2 с паролем более сложен и требует больших затрат, особенно при использовании шифрования AES, но всё же возможен.

**Аутентификация**

Для защиты от этой угрозы следует внедрять аутентификацию. Аутентификация добавляет ещё один уровень безопасности, требуя, чтобы компьютер клиента зарегистрировался в сети. Традиционно это выполняется при помощи сертификатов, маркеров или паролей (также известных как Pre­Shared-Key), которые проверяются на сервере аутентификации.

Стандарт **802.1Х** позволяет работать с WEP, WPA и WPA2 и поддерживает несколько типов аутентификации **ЕАР** (Extensible Authentication Protocol). Настройка аутентификации может оказаться затруднительной и дорогой задачей даже для профессионалов, не говоря об обычных пользователях. На нынешней конференции RSA в Сан-Франциско, например, многие посетители решили не настраивать безопасность беспроводных подключений только из-за того, что руководство занимало целую страницу!

К счастью, ситуация постоянно улучшается, уже не нужно покупать полноценный сервер **RADIUS**, поскольку появилось множество простых в установке альтернативных решений.

Подобный продукт от Wireless Security Corporation (недавно приобретённой McAfee) носит название WSC Guard. Цена подписки на него начинается от $4,95 в месяц за каждого пользователя, при оплате нескольких мест действуют скидки. Следующее решение больше подходит для опытных "сетевиков" - **TinyPEAP** является прошивкой с сервером RАDПJS, который поддерживает аутентификацию РЕАР на беспроводных маршрутизаторах **Linksys WRT54G** и **GS**. Отмечу, что прошивка официально не поддерживается Linksys, так что установка выполняется на свой страх и риск.

## 3.4 Умения третьего уровня: профессиональный хакер

До этого момента защита сводил ась к тому, чтобы не дать злоумышленнику подключиться к вашей сети. Но что делать, если, несмотря на все усилия. хакер пробрался в сеть?

Существуют системы обнаружения и предотвращения атак для проводных и беспроводных сетей, однако они нацелены на корпоративный уровень и имеют соответствующую стоимость. Также можно найти и решения, основанные на открытом исходном коде, но они, к сожалению, не совсем понятны для новичков. За многие годы существования проводных сетей были выработаны основные принципы безопасности, которые можно при менять и к беспроводным сетям. Они позволят защититься от вторжения злоумышленника.

**Общая безопасность сети**

Для усиления защиты сетей следует внедрить следующие меры

**• Аутентификация при обращении к любому сетевому ресурсу.**

Любой сервер, любой общий ресурс, панель управления маршрутизатором и т.д. должны требовать аутентификации. Хотя внедрить на уровне пользователей настоящую аутентификацию без соответствующего сервера невозможно. Как минимум, следует установить пароли на все общие ресурсы и отключить гостевую учётную запись, если вы используете Windows ХР. И никогда не предоставляйте в общее пользование целые разделы!

**• Сегментирование сети.**

Компьютер, не подключённый к сети, защищён от сетевых атак. Однако есть и другие способы ограничения доступа. Несколько правильно настроенных недорогих маршрутизаторов NAT могут послужить прекрасной основой для создания защищённых сегментов LAN, с возможностью доступа из них в Интернет. Подробнее об этом читайте здесь. Коммутаторы или маршрутизаторы с поддержкой VLAN помогут также с разделением сети. Впрочем, функции VLAN есть на большинстве управляемых коммутаторов, однако они практически не встречаются в недорогих маршрутизаторах и неуправляемых коммутаторах.

**• Программные средства защиты.**

Как минимум, нужно использовать обновлённые антивирусные решения и регулярно обновлять базы. Персональные брандмауэры, такие как **ZoneAlarm, BlackICE** и другие оповестят о подозрительной сетевой активности. К сожалению, последние версии вредоносных и "шпионских" программ требуют установки ещё и специального "анти­шпионского" программного обеспечения. Здесь можно отметить **Webroot Softwares Spy Sweeper**, а также **Sunbelt Software's CounterSpy.**

Отметим, что для организации надёжной защиты сети необходимо защитить все машины без исключения!

**• Шифрованиефайлов.**

Шифрование файлов с использованием криптостойких алгоритмов обеспечит надёжную защиту на случай неавторизованного доступа. Пользователи Windows ХР могут воспользоваться Windows Encrypted FiIe System (EFS). Пользователи Мас OS Х Tiger - FileVault. Из минусов шифрования можно отметить, что оно требует ресурсов процессора, а это может существенно замедлить работу с файлами.

# 

# Заключение.

Безусловно, беспроводные сети добавляют немало удобства, но нужно с умом подходить к их защите. Если вы не сделаете защиту самостоятельно, то никто не сделает это за вас. Конечно, от профессионального хакера вы вряд ли защититесь, но значительно осложните его работу. Да и вряд ли ваша сеть будет интересна профессионалам. А вот от многочисленных любителей «нашкодить» вы будете защищены. Так что взвесьте все "за" и "против" и защитите свою сеть!

# Список используемой литературы.

1. Сети и интернет: Wi-FI: боевые приемы взлома и защиты беспроводных сетей.
2. http://www.thg.ru/network/20050903/ - защита беспроводной сети
3. Журнал «Компьютер пресс» - Защита беспроводных сетей от взлома
4. Симонов С. Анализ рисков. Управление рисками//Jet Info, 1999. № 1. 3. Аудит безопасности информационных систем //Jet Info, 2000, № 1.
5. Высокие статистические технологии. Экспертные оценки. Учебник. Орлов А.И. – М.: Экзамен, 2007.