Защита сети Wi-Fi
категория: Интернет
добавлено: 12-10-2013
адрес материала: Защита сети Wi-Fi

Как защитить сеть Wi-Fi и для чего?

Много современных компьютеров имеют в своем арсенале поддержку беспроводного доступа к сети Интернет. Иначе говоря, у этих компьютеров есть возможность подключаться к интернету (и к другим устройствам, поддерживающим беспроводную связь) без сетевого кабеля. Главное преимущество беспроводных соединений — возможность работать с интернетом в любом месте в доме или офисе при условии, что компьютер и устройство беспроводного доступа находятся на допустимом расстоянии.

Однако если не позаботиться о безопасности своей беспроводной сети, то у злоумышленников появляется прекрасная возможность перехвата передаваемых или получаемых вами данных на расстоянии 100−150 м. от вашей точки доступа. Следовательно, если ваша беспроводная сеть не имеет хорошей защиты, взломщик может перехватить данные, получить доступ к вашей сети и файлам на персональном компьютере, а также без проблем сможет выходить в интернет, пользуясь вашим подключением.

Такая ситуация весьма неприятна, ибо злоумышленник может использовать ваш интернет канал без

вашего ведома, расходовать трафик, делать что-либо от вашего имени, и может доставить массу неприятностей своими незаконными действиями. Защитить Wi-Fi можно протоколом шифрования WEP или WPA. Протокол шифрования WEP сейчас многие уже не используют, так как у него очень низкая степень защиты шифрования (для теперешнего времени). Протокол WPA хоть и сложнее в настройке, однако, считается более защищенным. Если вы до сих пор используете устаревший Wi-Fi адаптер, который не поддерживает шифрование WPA, пора задуматься о приобретении более современной модели.

Абсолютной защиты Wi-Fi не может гарантировать никто, но придерживаясь некоторых правил можно обезопасить себя и свои данные на 90%. Оставшиеся 10% это те, кому домашняя сеть просто не интересна. Если вы не хотите оправдываться за атаки на правительственные сайты, банки и другие учреждения, которые вы не совершали или чтобы ваши фотографии просматривал, кто угодно — приступайте к защите своей домашней Wi-Fi сети.

Вот краткая инструкция шагов которые нужно выполнить для защиты точки доступа.

1. Обязательно включите 128 — битное (или больше) шифрование на точке доступа. Это сделает вашу домашнюю сеть намного более защищенной.
2. Установите свой пароль на маршрутизатор. Любой человек, получивший доступ к настройкам маршрутизатора может отключить все настройки безопасности, которые вы ввели. Используйте пароль максимально возможной длины и не переживайте если его забудете — пользоваться им вам придется очень редко, и у всех маршрутизаторов есть функция аппаратного сброса пароля.
3. Для доступа к сети используйте надежный пароль: не 123456 или qwerty, а случайную последовательность букв и цифр в разных регистрах. Создать хороший пароль несложно: берем легко запоминающуюся фразу, например, слово снегурочка. Записываем в английской раскладке и получаем: cytuehjxrf. Запомнить легко, а пароль не простой. Чем длиннее фраза тем сложнее пароль. Сложный пароль со сменой регистра взломать практически невозможно.
4. Обязательно смените сетевое имя. Если для доступа к сети используется логин «user» или «admin», присвоенный по умолчанию, то взломщикам останется подобрать только пароль. Если же имя пользователя будет придумано другое, то взломать сеть станет сложнее вдвойне.
5. Включите фильтрацию MAC — адресов на точке доступа. MAC — адрес — это уникальный номер каждого сетевого адаптера, и, если фильтрация будет включена, то точка доступа будет игнорировать запросы, посланные с «чужих» Wi-Fi адаптеров. Но не стоит расслабляться: злоумышленники могут клонировать ваш MAC — адрес на свой адаптер.
6. Отключите «удаленный вход в систему» — ведь это распахнутые настежь перед злоумышленниками ворота. Также отключите «беспроводное администрирование» — изменение настроек маршрутизатора без физического доступа к нему. Немного неудобно каждый раз подключаться к маршрутизатору с помощью кабеля для его настройки, зато, поверьте, намного надежнее.
7. Старайтесь не пользоваться «общим доступом» к папкам, а если и открываете его — закрывайте сразу же, как только в нем не будет необходимости, пользуйтесь файрволом и регулярно обновляйте программное обеспечение и антивирусные базы.
8. Отключите трансляцию ID сети и автоматическое подключение к другим сетям Wi-Fi.
9. Желательно уменьшить мощность сигнала. Если точка доступа Wi-Fi будет работать на 50, или даже на 30% мощности — этого хватит для уверенного приема в квартире и сильно уменьшит зону, из которой можно получить доступ к вашей сети. Этим советом не стоит пренебрегать, ведь злоумышленники часто используют специальные направленные антенны и усилители для получения устойчивого сигнала.
10. Ну и наконец, самый простой способ защиты Wi-Fi о котором многие пользователи часто

забывают. Он заключается в отключении точки доступа в том случае, если вы не работаете с ней. Нет сети — нет и проблем.

Вот такие простые методы помогут защитить wifi сеть и ваши нервы от злоумышленников.Защита домашней сети дело сугубо личное. Если вы стремитесь к публичности и считаете, что вам нечего скрывать — можете использовать wifi сеть без защиты и надеяться на господа бога и честных добропорядочных людей. Но поверьте, незащищенная точка доступа это большая глупость с вашей стороны, которая когда-нибудь о себе напомнит.
Много современных компьютеров имеют в своем арсенале поддержку беспроводного доступа к сети Интернет. Иначе говоря, у этих компьютеров есть возможность подключаться к интернету (и к другим устройствам, поддерживающим беспроводную связь) без сетевого кабеля. Главное преимущество беспроводных соединений — возможность работать с интернетом в любом месте в доме или офисе при условии, что компьютер и устройство беспроводного доступа находятся на допустимом расстоянии.
Однако если не позаботиться о безопасности своей беспроводной сети, то у злоумышленников появляется прекрасная возможность перехвата передаваемых или получаемых вами данных на расстоянии 100−150 м. от вашей точки доступа. Следовательно, если ваша беспроводная сеть не имеет хорошей защиты, взломщик может перехватить данные, получить доступ к вашей сети и файлам на персональном компьютере, а также без проблем сможет выходить в интернет, пользуясь вашим подключением.
Такая ситуация весьма неприятна, ибо злоумышленник может использовать ваш интернет канал без вашего ведома, расходовать трафик, делать что-либо от вашего имени, и может доставить массу неприятностей своими незаконными действиями. Защитить Wi-Fi можно протоколом шифрования WEP или WPA. Протокол шифрования WEP сейчас многие уже не используют, так как у него очень низкая степень защиты шифрования (для теперешнего времени). Протокол WPA хоть и сложнее в настройке, однако, считается более защищенным. Если вы до сих пор используете устаревший Wi-Fi адаптер, который не поддерживает шифрование WPA, пора задуматься о приобретении более современной модели.
Абсолютной защиты Wi-Fi не может гарантировать никто, но придерживаясь некоторых правил можно обезопасить себя и свои данные на 90%. Оставшиеся 10% это те, кому домашняя сеть просто не интересна. Если вы не хотите оправдываться за атаки на правительственные сайты, банки и другие учреждения, которые вы не совершали или чтобы ваши фотографии просматривал, кто угодно — приступайте к защите своей домашней Wi-Fi сети.
Вот краткая инструкция шагов которые нужно выполнить для защиты точки доступа.
1. Обязательно включите 128 — битное (или больше) шифрование на точке доступа. Это сделает вашу домашнюю сеть намного более защищенной.
2. Установите свой пароль на маршрутизатор. Любой человек, получивший доступ к настройкам маршрутизатора может отключить все настройки безопасности, которые вы ввели. Используйте пароль максимально возможной длины и не переживайте если его забудете — пользоваться им вам придется очень редко, и у всех маршрутизаторов есть функция аппаратного сброса пароля.
3. Для доступа к сети используйте надежный пароль: не 123456 или qwerty, а случайную последовательность букв и цифр в разных регистрах. Создать хороший пароль несложно: берем легко запоминающуюся фразу, например, слово снегурочка. Записываем в английской раскладке и получаем: cytuehjxrf. Запомнить легко, а пароль не простой. Чем длиннее фраза тем сложнее пароль. Сложный пароль со сменой регистра взломать практически невозможно.
4. Обязательно смените сетевое имя. Если для доступа к сети используется логин «user» или «admin», присвоенный по умолчанию, то взломщикам останется подобрать только пароль. Если же имя пользователя будет придумано другое, то взломать сеть станет сложнее вдвойне.
5. Включите фильтрацию MAC — адресов на точке доступа. MAC — адрес — это уникальный номер

каждого сетевого адаптера, и, если фильтрация будет включена, то точка доступа будет игнорировать запросы, посланные с «чужих» Wi-Fi адаптеров. Но не стоит расслабляться: злоумышленники могут клонировать ваш MAC — адрес на свой адаптер.
6. Отключите «удаленный вход в систему» — ведь это распахнутые настежь перед злоумышленниками ворота. Также отключите «беспроводное администрирование» — изменение настроек маршрутизатора без физического доступа к нему. Немного неудобно каждый раз подключаться к маршрутизатору с помощью кабеля для его настройки, зато, поверьте, намного надежнее.
7. Старайтесь не пользоваться «общим доступом» к папкам, а если и открываете его — закрывайте сразу же, как только в нем не будет необходимости, пользуйтесь файрволом и регулярно обновляйте программное обеспечение и антивирусные базы.
8. Отключите трансляцию ID сети и автоматическое подключение к другим сетям Wi-Fi.
9. Желательно уменьшить мощность сигнала. Если точка доступа Wi-Fi будет работать на 50, или даже на 30% мощности — этого хватит для уверенного приема в квартире и сильно уменьшит зону, из которой можно получить доступ к вашей сети. Этим советом не стоит пренебрегать, ведь злоумышленники часто используют специальные направленные антенны и усилители для получения устойчивого сигнала.
10. Ну и наконец, самый простой способ защиты Wi-Fi о котором многие пользователи часто забывают. Он заключается в отключении точки доступа в том случае, если вы не работаете с ней. Нет сети — нет и проблем.
Вот такие простые методы помогут защитить wifi сеть и ваши нервы от злоумышленников.

Дата редактирования: ***НКЛ служба поддержки*** *- 12-10-2013*