

Безопасность передачи данных по Wi-Fi

Введение

Последнее время современному человеку становится все тяжелее представить свое комфортное существование без интернета. Wi-Fi сети буквально окружили нас со всех сторон - сегодня во многих городах можно найти и бесплатно подключиться к беспроводному интернету. Однако, есть и коммерческие закрытые сети, подключение к которым не предназначено широкому кругу и важно обеспечить защиту доступа и передачу данных. Поэтому вопрос защиты и безопасности таких сетей будет актуален на протяжении всего периода их существования. Чтобы защитить Wi-Fi сети (стандарта 802.11), существует целый ряд технологий. Для того, чтобы понять, каким образом обеспечивается безопасность передачи данных посредством беспроводного подключения к сети интернет, нужно заранее ознакомиться, собственно, с мерами безопасности их передачи.^[1]

Функционирование беспроводной сети

При подключении используются три основных алгоритма: WEP, WPA, WPA2. После принятия первого в 2001 году он быстро был взломан, и сейчас довольно легко можно найти определённую утилиту для его расшифровки. Поэтому данный алгоритм считается ненадёжным. На смену ему последовательно пришёл WPA, а затем и WPA2.

WEP (WIRED EQUIVALENT PRIVACY). Использует генератор псевдослучайных чисел (алгоритм RC4) для получения ключа, а также векторы инициализации. Так как последний компонент не зашифрован, возможно вмешательство третьих лиц и воссоздание WEP-ключа.

WPA (WI-FI PROTECTED ACCESS) Основывается на механизме WEP, но для расширенной защиты предлагает динамический ключ. Ключи, сгенерированные с помощью алгоритма TKIP, могут быть взломаны посредством атаки Бека-Тевса или Охигаши-Мории. Для этого отдельные пакеты расшифровываются, подвергаются манипуляциям и снова отсылаются в сеть.

WPA2 (WI-FI PROTECTED ACCESS 2) Задействует для шифрования надежный алгоритм AES (Advanced Encryption Standard). Наряду с TKIP добавился протокол CCMP (Counter-Mode/CBC-MAC Protocol), который также базируется на алгоритме AES. Защищенную по этой технологии сеть до настоящего момента взломать не удавалось. Единственной возможностью для хакеров является атака по словарю или «метод грубой силы», когда ключ угадывается путем подбора, но при сложном пароле подобрать его невозможно.^[2]

От взлома информации и внешнего проникновения также защищает система проверки целостности сообщений (Message Integrity Check). Довольно сложный математический алгоритм помогает сверять данные, которые отправлены в одной точке, а получены в другой. Если результат сравнения и отмеченные изменения не подходят, то такие данные являются ошибочными.

Поэтому, сегодня у администраторов сетей и у обычных пользователей есть все средства надежной защиты Wi-Fi и, если нет никаких грубых ошибок, можно постоянно обеспечивать уровень безопасности, который соответствует ценности информации, что находится в такой сети. Сегодня беспроводная сеть является защищенной в том случае, если в ней работают три основных подразделения систем безопасности: целостность передачи данных и ее конфиденциальность, аутентификация пользователя. Для обеспечения высокого уровня безопасности информации нужно воспользоваться некоторыми правилами при организации и настройке правильной Wi-Fi сети:

- Шифрование данных посредством использования разных систем.
- Надежный уровень защиты обеспечить Virtual Private Network (VPN)
- Использование протокола 802.1X;
- Запретить доступ к настройкам точки доступа с помощью беспроводного соединения.
- Запретить трансляцию в эфир идентификаторов сессий SSID.
- Ограничить мощность радиосигнала.
- Использовать максимально длинные ключи.
- Изменить статические ключи и пароли.
- Не использовать в беспроводной сети DHCP. Вручную распределить все статические IP адреса между клиентами безопасней.
- Не использовать гостевой доступ к ресурсам общего пользования.
- По возможности не использовать в беспроводных сетях протокола TCP/IP для организации папок, файлов и принтеров общего доступа.
- Организация ресурсов, что разделяется средствами NETBEUI в данном случае безопасней.
- Использовать шифрование ключей WPA2. ^[3]

Вывод

Из данной статьи понятно что для обеспечения высокого уровня безопасности информации лучше использовать шифрование WPA2 т.к. для шифрования используется алгоритм AES, также известный как Rijndael — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Защищенную по этой технологии сеть до настоящего момента взломать не удавалось.

Описание электронного ресурса удаленного доступа(*Internet*)

1. Локальные сети Украины [Электронный ресурс]:Электронный журнал.-Украина,г.Киев. Режим к доступу журнала: <https://local.com.ua/>,свободный,-Загл. с экрана

2. Dom Wi-Fi [Электронный ресурс]:Электронный журнал.-Москва. Режим к доступу журнала: <http://dom-wifi.ru/>,свободный,-Загл. с экрана

3. LiveBusiness [Электронный ресурс]:Электронный журнал. Режим к доступу журнала: <http://www.liventerprise.com/> свободный,-Загл. с экрана