

ЗАЩИТА ДОМАШНЕЙ WI-FI СЕТИ ОТ ВЗЛОМА

Манко Е.М., Масальская Е.А.

Государственный ВУЗ «Национальный горный университет», nmu.org.ua,

Беспроводные сети не являются защищенными. Абсолютно надежными их сделать невозможно, но улучшить безопасность вполне возможно.

Ключевые слова: *безопасность сетей Wi-Fi, домашние сети.*

На сегодняшний день почти у всех есть Internet и у 50%, если не более, он является беспроводным (Wi-Fi). Основным недостатком беспроводной сети является ее защита. Можно выделить такую основную уязвимость сети как перехват данных, передаваемых по радиоканалу. Это не требует дорогостоящего оборудования и реализуемо при помощи ноутбука, пары утилит (таких как airodump и aircrack) и хорошей инструкции по взлому Wi-Fi.

Поэтому беспроводная сеть должна быть максимально защищена от различного рода атак: несанкционированных подключений, перехвата и прослушивания трафика, хищения важной информации, «ложных» точек доступа и т.п.

Рекомендации по защите домашних Wi-Fi сетей.

На сегодняшний день наиболее надежным для беспроводных сетей признан стандарт безопасности WPA2 (Wi-Fi Protected Access2). 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 [1]. 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.

Запретить вашему роутеру передавать «идентификатор сети» (SSID) – сеть станет «невидимой» для посторонних. Это даст защиту от случайных гостей, но не от серьезных взломщиков сетей[2].

Настроить роутер так, чтобы он подключал к сети только перечисленные вручную устройства. Тогда, другие компьютеры в принципе не смогут подключиться к данной сети.

Фильтрация по MAC адресу. MAC адрес – это уникальный идентификатор устройства (сетевое адаптера), «зашитый» в него производителем. На некотором оборудовании возможно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – MAC адрес можно подменить [2].

Именно Wi-Fi в настоящее время является не только самой распространённой технологией беспроводного доступа, но и самой удобной с точки зрения получения и передачи информации. Однако она несёт в себе множество серьезных угроз информационной безопасности объекта.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Защита Wi-Fi сетей /способ доступа: <http://mediapure.ru/stati/bezopasnost-wi-fi-pravilnaya-zashhita-wi-fi>
2. Взлом Wi-Fi / способ доступа: <http://www.thermidor.biz/about/70-wifi.html>