УДК 004.056

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ WI-FI

Панова Валерия Игоревна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, lerochka-panova@yandex.ru

В данной статье рассмотрена проблема безопасности беспроводных сетей WI-FI. Проанализированы основные меры защиты сети от несанкционированного доступа.

Ключевые слова – беспроводные сети, защита от несанкционированного доступа.

ВВЕДЕНИЕ

За последние десять лет беспроводные сети получили широкое распространение во всём мире. И, если ранее речь шла преимущественно об использовании беспроводных сетей в офисах, то теперь они широко используются в домашних условиях. С одной стороны технология WI-FI (Wireless Fidelity) обладает большими преимуществами, например, нет необходимости прокладки кабеля, лучшая масштабируемость и цена, но с другой стороны есть и недостатки – один из которых безопасность. Если безопасности не уделять должного внимания, такую сеть вполне можно считать публичной, что неизбежно отразится на ее функционировании не лучшим образом.

ОСНОВНАЯ ЧАСТЬ

Стандартом 802.11 предусмотрен ряд мер, позволяющих надежно защитить беспроводные сети, а также оборудование для WI-FI имеет пароли доступа для безопасности.

Основные меры предосторожности при организации и настройке WI-FI сети:

1. Центральной частью любого WI-FI оборудования является так называемая точка доступа или маршрутизатор (Router). Производители WI-FI-оборудования предоставляют специализированные веб-страницы, благодаря которым пользователи WI-FI могут входить в сеть, используя свой собственный аккаунт и специализированный особый сетевой адрес. Вся эта веб-конструкция защищена экраном-логином (имя пользователя и пароль), которое должно давать доступ в сеть только зарегистрированным пользователям. Однако, по умолчанию, логины предоставляются самими производителями WI-FI-оборудования. Необходимо изменить эти настройки.

2. Следует включить защиту шифрования WPA/WEP (WI-FI Protected Access/Wired Equivalent Privacy). Все виды WI-FI-оборудования поддерживают некоторые формы шифрования. Сама технология шифрования меняет должным образом все сообщения, которые рассылаются посредством WI-FI; наличие данного стандарта шифрования подразумевает, что не каждый сможет прочитать ваши сообщения.

3. Если точка доступа позволяет управлять доступом клиентов по MAC-адресам нужно использовать эту возможность. Маршрутизатор WI-FI-оборудования хранит в себе MAC-адреса (Media Access Control) всех тех девайсов, которые подключены к нему. Многие такие продукты предлагают пользователю эту опцию в виде ключа в MAC-адресах вашего оборудования, которое позволяет подключаться к сети только проверенным девайсам.

4. Необходимо поменять дефолтные SSID.

Маршрутизаторы для своей работы используют SSID (Service Set Identifier). Производители поставляют свое оборудование с одними и теми же настройками SSID. Когда пользователь будет конфигурировать свою WI-FI-сеть, то рекомендуется поменять дефолтные SSID, чтоб его никто не знал.

5. Отключить передачу SSID. В WI-FI-сети маршрутизатор, в типичном своем состоянии, передает имя сети(SSID) в эфир через регулярные интервалы. Эта особенность была спроектирована для тех случаев, когда WI-FI клиенты могут входить и выходить из зоны действия их собственной сети. Но, находясь у себя дома, данная функция роуминга полностью бесполезна. В большинстве WI-FI-маршрутизаторов есть особенность отключения данного роуминга через панель администратора.

6. Не стоит подключаться через открытые WI-FI-сети.

7. Поставить статические IP на все девайсы. Большинство домашних WI-FI-линий тяготеют к использовании динамических IP адресов. DHCP (Dynamic Host Configuration Protocol) технология в наше время является наилучшим решением по этой части. Однако не все так просто: именно это удобство позволяет хакерам перехватывать сигналы, которые могут с легкостью получить статический IP из канала вашего DHCP. Следует отключить DHCP на вашем маршутизаторе, и поставить вместо него фиксированный IP.

8. Активировать Firewall (межсетевой экран) на каждом компьютере и на самом маршрутизаторе. Современные маршрутизаторы уже содержат в себе встроенный Firewall.

9. Местонахождение самого маршрутизатора и безопасность всей сети.

В нормальном состоянии WI-FI-сигналы не должны распространяется на большие расстояния, всегда есть вероятность перехвата и его дальнейшего использования. Когда пользователь будет инсталлировать свою домашнюю WI-FI-систему, то следует помнить, что местонахождение самого маршрутизатора играет не самую последнюю роль. Его следует расположить посередине комнаты, а не возле окна, что также позволит минимизировать утечку сигнала.

10. Еще одним из неплохих решением является выключения оборудования, когда пользователь вообще не пользуетесь им. Это резко снижает взлом. Естественно, довольно непрактично выключать его

очень часто, но во время продолжительного отсутствия отключение оборудования является наилучшим выходом. Диски компьютера не любят постоянный цикл: включение/выключение, но для широкополосных модемов и маршрутизаторов все это не так уж и страшно.

ЗАКЛЮЧЕНИЕ

Безопасности беспроводных сетей стоит уделять особое внимание, ведь беспроводная сеть имеет большой радиус действия. Соответственно, злоумышленник может перехватывать информацию или же атаковать сеть, находясь на безопасном расстоянии от устройства. Придерживаясь выше перечисленных мер, пользователь может быть уверен в обеспечении необходимого уровня безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андрей Владимиров «Атакуем клиентские устройства на WI-FI сетях», «Взлом и защита», 2006.
2. Гордейчик С.В., Дубровин В.В. «Безопасность беспроводных сетей », 2008.