УДК 00.004

Алексеев П.А., студент 1 курса,
факультет информационных технологий,
Брянский государственный технический университет,
г. Брянск, Россия

ЧЕМ ОПАСЕН ОТКРЫТЫЙ WI-FI

Аннотация. *В статье рассказывается об видах защиты WI-FI роутеров, а также потенциальной опасности подключения к открытому роутеру.*

Ключевые слова: *Wi-Fi, перехват трафика, защита сети.*

Annotation: *The article describes the types of protection for WI-FI routers, as well as the potential danger of connecting to an open router.*

Keywords: *Wi-Fi, traffic interception, network protection.*

Виды защиты роутеров

Роутер, он же маршрутизатор, используется повсеместно в самых разных сферах общественной жизни. Это небольшое устройство служит для беспроводного подключения пользователя к сети интернет. Принцип работы того или иного маршрутизатора сводится к тому, что блок данных (пакет) пересылается между сегментами сети, для более эффективного сетевого трафика. Важную роль во всем этом процессе играют таблицы маршрутизации, содержащие идентификатор сети получателя.

Защита роутера (маршрутизатора), к ней стараются прибегать практически все пользователи, у кого имеется доступ к WI-FI. Без надёжной и эффективной защиты можно лишиться доступа к своему же маршрутизатору. Роутером могут воспользоваться, не только сторонние люди/мошенники, куда опаснее взлом самого маршрутизатора, с занесением в него вируса.

Существуют различные виды защиты роутеров, в частности, самый простой и, в то же время более чем верный способ, - никому не сообщать свой пароль (шифрование WPA2). Помимо этого можно установить для своего роутера специальную утилиту/программу - защита от взломов и вирусов. Защитить маршрутизатор можно и при помощи включения фильтров для MAC-адресов. Отключение функции SSID, а также изменение данного идентификатора, напрямую помогает защитить роутер от рук злоумышленников. Используйте сеть VPN (шифровальщик IP-адреса) или отключите удаленный доступ, все эти меры также помогают защитить роутер.

Как видим, существует огромное количество самых разных видов защиты роутера. Иногда нужно быть просто внимательным: не стоит открывать ссылки электронных писем, ежедневно проводите сканирование системы, блокируйте скрипты и т.д.

Почему роутер может быть без пароля

Если говорить о том, почему роутер может быть без пароля, то лучше всех на этот вопрос ответят именно IT-специалисты. Любой маршрутизатор задаётся настройками, среди которых - подключение к сети WI-FI через пароль. Пароль можно и вовсе не использовать, тогда подключение к сети интернет будет общедоступным. Любой человек может подключиться к определенному роутеру, даже если пароль остаётся неизвестным (автогенератор подбора паролей).

Все мы прекрасно знаем о том, что во многих общественных местах (кафе, общепиты, аэропорты, автостанции) WI-FI работает по общедоступной сети, подключиться к нему может любой желающий. Роутеры без пароля позволяют быстро найти точку доступа WI-FI и подключиться к ней. Если человек забыл свой собственный пароль от своего же роутера, то эту проблему вполне легко решить, например, сбросить старый пароль и создать при этом новый. Функция WPS - с помощью WI-FI Protected Setup даже не нужно вводить пароль, подключение к роутеру занимает считанные секунды.

Роутер без пароля работает по тому же стандарту, что и с паролем. Если нет возможности создать password (отсутствует подобного рода функция), то скорее всего причина кроется в самом устройстве. Перепрошивка маршрутизатора, сбой в настройках, - все то позволяет говорить о том, что роутер не имеет возможности генерировать собственный пароль, и с этим уже ничего не поделаешь.

В случае когда невозможно создать надёжный пароль для роутера (отсутствует такого рода функция), следует воспользоваться другим маршрутизатором. Если вы не обращаете никакого внимания на password, то проблема отпадает сама собой. Если же вы не часто пользуетесь маршрутизатором без пароля, то можно не беспокоиться о его безопасности, впрочем, существует огромное количество всевозможных способов по защите роутера.

Перехват трафика: возможное воровство паролей

Перехват трафика по открытой сети WI-FI (отсутствует пароль) представляется вполне очевидной вещью. Персональные данные передаются по радиоволнам, поэтому злоумышленникам не составляет труда воспользоваться ими по своему усмотрению. Перехваченный трафик другим человеком строго наказывается законом во многих странах земного шара, но для России это большая редкость.

Дабы не допустить подобной ситуации, обязательно нужно использовать пароль при работе того или иного маршрутизатора. Если перехват трафика - это ещё пол беды, то воровство пароля представляется куда более серьезной вещью. Украденный password может сыграть на руку мошенникам, и даже если роутер находится у вас дома, по факту, он уже вам не принадлежит. При воровстве пароля следует приостановить работу роутера и, сгенерировать новый пароль. Если ничего не выходит, тогда следует обратиться к специалистам, они помогут разрешить данную проблему.

В обычной ситуации, перехват трафика и воровство паролей, происходит из-за банальной невнимательности самого юзера, который пользуется беспроводной сетью WI-FI по открытой линии. При отличном сигнале к маршрутизатору могут подключиться десятки людей, что порой приводит к потере скорости интернета. Перехватить трафик могут и при работе залогиненного роутера, но это случается не так чтобы часто. Если ваш трафик достается не вам, а вы ещё и платите ежемесячный взнос за услуги по интернету, то следует задуматься над тем, как вычислить злоумышленника. Будьте осторожны с паролями, просматривайте статистику подключенных пользователей к вашей беспроводной сети, анализируете каждое проводимое вами действие, только в этом случае можно быть уверенным в надёжной и эффективной работе вашего же маршрутизатора. С каждым годом надёжность роутеров становится более совершенной, но расслабляться на этом не стоит.

Почему не стоит пользоваться/подключаться к чужим роутерам

Чем опасен чужой роутер, тем более, если он без пароля? Казалось бы, просто подключился к свободному WI-FI и наслаждайся высокоскоростным интернетом, но, не все так просто как кажется. Если вы подключились к чужому роутеру, то нужно понимать: ваши действия могут привести к плачевным последствиям. Фактически, говоря обывательским языком, человек ворует интернет у другого человека, и за этим могут последовать неприятности.

Подключившись к чужому маршрутизатору, человек может попасть в ситуацию, когда его же персональные данные окажутся в руках у мошенников. Помимо всего прочего, велика вероятность подцепить вирус на свое устройство, будь то компьютер или же смартфон. Если вы решили попользоваться чужим трафиком в своих личных целях, то будьте готовы к тому, что в скором времени доступ к роутеру вам будет ограничен.

Когда идёт речь об общественных местах, где доступен free WI-FI, следует помнить одну простую вещь: чужой бесплатный интернет может

сыграть с вами злую шутку. Через различные шпионские программы все ваши сведения могут оказаться в поле зрения чужих лиц, может дойти до того, что вашим гаджетом начнут управлять извне. Старайтесь пользоваться исключительно своим роутером со своим же паролем, так вы будете знать, что никто иной не подключился к вашему устройству.

Если вам вовсе не нужны проблемы, но при этом есть возможность подключиться к чужому маршрутизатору, то согласуйте все условия с владельцем активного сетевого оборудования. В УК РФ предусмотрена статья 272 "Неправомерный доступ к компьютерной информации", согласно которой, человека могут привлечь к тюремному заключению, в том числе, если тот использует доступ к чужому роутеру. Ко всему прочему, вам может быть предъявлен иск в суд, если владелец роутера обнаружит, что именно вы пользовались его сетью WI-FI. Из всего этого следует, что подключаться и пользоваться чужими роутера вовсе не стоит.

Список используемых источников:

1. Росс Джон. Wi-Fi. Беспроводная сеть.2007 – СТР 60-79

2. Пролетарский А.В., Баскаков И.В., Федотов Р.А. Беспроводные сети Wi-Fi - 2016- СТР 134-139.