УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ РАБОТЕ С WI-FI

А.К. Курманбай
(г. Юрга, Юргинский технологический институт Томского политехнического университета)
E-mail: aigera_0796@mail.ru

INFORMATION SECURITY THREATS TO WORK WITH WI-FI

A.K. Kurmanbay
(Jurga, Yurginskiy Technological Institute of the National Research Tomsk Polytechnic University)

Abstract. The article deals with the use of wi-fi and safety when working with them, as with the development of information technology, a huge role in a person's life began to play online. He uses us every day: check the mail sit in social networks, communicate in social networks, watch movies and videos. Often, the use of wired internet is impractical because it limits our movement, and the wires are confused and interfere.

Keywords: wi-fi, information security, threatening.

В статье рассмотрено использование wi-fi и безопасность при работе с ним, так как с развитием информационных технологий, огромную роль в жизни человека стал играть Интернет. Он пользуется нами повседневно: проверяем почту, сидим в социальных сетях, общаемся в социальных сетях, просматриваем фильмы и видео. Зачастую использование проводного интернета является нецелесообразным, так как он ограничивает наше перемещение, а провода путаются и мешаются.

На замену проводам пришли Wi-Fi технологии, которые позволили, подключаться к высокоскоростному Интернету не используя проводные соединения. Wi-Fi получил широкое распространение при организации беспроводного интернета во многих современных предприятиях, школах, домах, университетах и в публичных местах, как альтернатива проводному интернету. Большинство современных портативных устройств (ноутбуки, КПК, смартфоны) имеют встроенные средства для работы в беспроводных сетях. Количество точек беспроводного доступа в мире растет с каждым днем, и при этом мы можем выйти в интернет, откуда угодно и без особых проблем. Самое главное, чтобы под рукой оказался ноутбук, смартфон или планшетный компьютер [1]. Находясь в кафе, торговом комплексе, дома или на работе мы используем Wi-Fi сети, так как это удобно, практично и мобильно. Но немногие задавались вопросом, безопасно ли это?

Wi-Fi или Wireless Fidelity переводится как «высокая точность беспроводной передачи данных». Это стандарт оборудования для построения локальных вычислительных сетей. В сети, созданной по технологии Wi-Fi, передача данных осуществляется без физического соединения устройств, посредством радиосигнала. Еще одним неоспоримым преимуществом (кроме отсутствующих проводов) является простота развертывания и настройки Wi-Fi и при этом одна точка доступа может обеспечить охват в радиусе до 200 метров, в зависимости от роутера. Широкое распространение, помимо домашних и офисных сетей, Wi-Fi нашел в сфере организации публичного доступа в Интернет (хот-спотов). Например, в городе Уфа насчитывается около 160 хот-спотов, которые обеспечивают бесплатный выход в Интернет. С использованием этой технологии любой посетитель гостиницы, кафе, ресторана, бизнес-центра или аэровокзала получает возможность мобильного подключения к сети посредством своего ноутбука, КПК или телефона, поддерживающего стандарт беспроводного доступа. Для функционирования Wi-Fi сетей разработано множество стандартов, одним из часто использующихся является IEEE 802.11n.

Стандарт IEEE802.11n – один из передовых стандартов Wi-Fi, на данный момент. Используются частотные каналы в спектрах 2.4GHz и 5GHz. Совместим с 11b/11a/11g. Стандарт 802.11n использует совершенно новые технологии, повышающие скорость передачи данных и увеличивающие радиус покрытия. Так, например, заявленная скорость передачи данных для этого стандарта – около 430Мбит\с. Используется модуляция – MIMO (Multiple Input Multiple Output). Данная модуляция построена на основе применения множества антенн, соответственно, создается множество информационных потоков, что в разы увеличивает скорость передачи данных [2].

Для удобства передачи данных частота поделена на так называемые каналы.

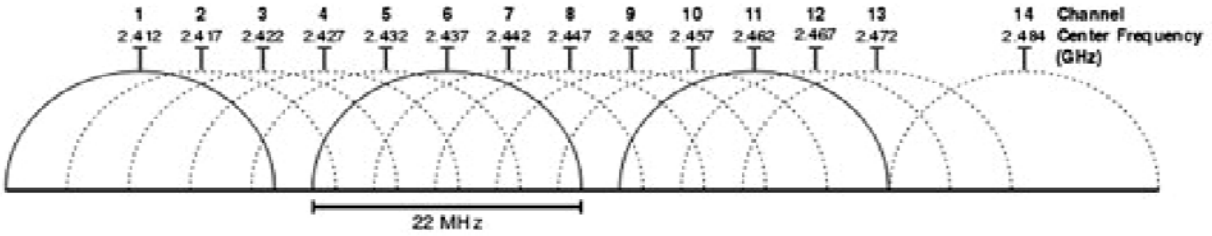

Рис. 1. Распределение частот по каналам

Из изображения видно, что каналов всего 14, но в зависимости от страны, в которой мы находимся, разрешенными для использования могут быть только некоторые из них. Так, например, в России разрешено использовать с 1 по 13 канал в США с 1 по 11, а в Японии все 14.

При передаче данных по сети немаловажным аспектом является шифрование трафика, так как для перехвата передаваемой информации не нужно физическое воздействие, а достаточно просто подключиться к сети и, «подслушивая» канал, перехватывать информацию. На данный момент существуют несколько видов шифрования, таких как:

1. WEP. Самый простой алгоритм шифрования. Поддерживается всеми точками доступа и клиентами.

2. WPA. В основе используется все тот же RC4, но дополнительно применяются алгоритмы TKIP и MIC.

Суть алгоритма – проверка целостности данных, чтобы исключить возможность подделки пакетов. Протокол WPA так же поддерживается всеми устройствами без проблем в его двух вариантах:

WPA-PSK – здесь используется заранее предопределенная ключевая фраза в качестве пароля. Этот вариант часть применяется в домашних условиях.

WPA-802.1x – доступ к сети осуществляется после проверки дополнительным сервером аутентификации. Этот способ наиболее подходит для крупных организаций. Из этих двух вариантов легче всего взломать WPA-PSK, однако это будет все равно тяжелее, чем WEP.

С целью обеспечения большей надежности защиты информации был разработан стандарт WPA2.

WPA2 Основное отличие от WPA заключается в использовании более стойкого алгоритма шифрования AES [1].

Технология Wi-Fi безусловно удобна и универсальна для организации беспроводного доступа к информации. Однако она несёт в себе множество серьёзных угроз информационной безопасности. Wi-Fi-соединение может быть взломано, а данные перехвачены посредством сниффинга («прослушивания» сетевого трафика) либо атак по типу man-in-the-middle attack (MITM). Этот способ является наиболее простым, так как не нужно физическое воздействие.

Вопрос безопасности wi-fi сетей актуален, так как сниффинг программы находятся в открытом доступе и на основе данных программ можно показать наглядно, как небезопасны беспроводные сети в независимости от сложности пароля и шифрования трафика.

Алгоритм перехвата выглядеть следующим образом:

Пользователь, идентифицировавшийся в сети, как правило, отправляет данные на беспроводной маршрутизатор. Эту информацию в дальнейшем можно перехватить и прочитать, но не ту, что зашифрована, например пароль от почты или логин. Для того чтобы после каждого клика пользователь не вводил пароль, сайт посылает ему «идентификатор сессии» после входа в систему, который нужен для работы с сайтом, которые хранятся в «куки». Как правило, только пользователь знает этот идентификатор, так как он получает его в зашифрованном виде. Но когда он использует Wi-Fi, он распространяет свой идентификатор сессии по Wi-Fi для всех. Злоумышленник принимает этот идентификатор сессии, и использует его. IP-адрес и идентификатор сессии.

Для защищенных WPA/WPA2 Wi-Fi-сетей программа использует DNS-Spoofing атаки. ARP-Spoofing означает, что она заставляет все устройства в сети думать, что программа –

виртуальный роутер, и пропускает все данные через себя. Благодаря чему зашифрованная информация перехватывается, и злоумышленник получает доступ к вашей информации: почте, социальным сетям, запросам в поисковиках и других посещённых сайты.

Таким образом, сниффинг является одной из актуальных проблем в Wi-Fi сетях. И для того, чтобы обезопасить себя в беспроводных сетях, необходимо:

- При подключении к сети устанавливать зашифрованное соединение HTTPS-протокол и SSL.
- После каждого подключения к открытым сетям менять пароль или использовать анти-сниффинг программы заблаговременно проанализировав перед отправкой своих данных по сети.

Нужно отметить, что Wi-Fi технология в настоящее время является одной из самой популярной и удобной беспроводной сетью с точки зрения мобильности и удобства, но, в то же время она несёт в себе угрозы информационной безопасности, так как данные циркулирующие в данной сети могут быть перехвачены и расшифрованы. Поэтому, нужно быть осторожными при подключении к открытым сетям используя защищенное соединение https, ssl. И быть тщательными при организации точек в доме, офисе и на предприятии, так как кроме сниффинга существуют и другие программно-аппаратные решения для взлома, и перехвата данных

Список литературы

1. Щербяков, А. К. Wi-fi: всё, что вы хотели знать, но боялись спросить/ А.К. Щербяков. – М.: Бук-пресс, 2005–11 с.

2. Постановление Правительства Российской Федерации от 12 октября 2004 г. № 539 г.

SMART WORLD КАК ДОМИНИРУЮЩАЯ КОНЦЕПЦИЯ РАЗВИТИЯ УСТОЙЧИВОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Б.Х. Курмангалиева[1], А.А. Тихомиров[2], А.И. Труфанов[3], О.Г. Берестнева[4]
[1](г. Астана, Национальный инфокоммуникационный холдинг «Зерде» Министерства транспорта и коммуникаций Республики Казахстан),
[2](г. Инчеон, университет Инха),
[3](г. Иркутск, Иркутский национальный исследовательский технический университет),
[4](г. Томск, Томский политехнический университет)
E-mail: kbikesh@me.com, troufan@gmail.com, alexeitikhomirovprof@gmail.com, ogb6@yandex.ru

SMART WORLD AS A DOMINANT CONCEPT OF SUSTAINABLE INFORMATION SOCIETY

B. Kh. Kurmangaliyeva[1], A.A. Tikhomirov[2], A.I. Trufanov[3], O.G. Berestneva[4]
[1](Astana, National information and communication Holding «Zerde», Ministry of transport and communications , Rrepublic of Kazakhstan),
[2](Incheon, Inha University),
[3](Irkutsk, Irkutsk National Research Technical University)
[4](Tomsk, Tomsk Polytechnic University)

Abstract. In the frame of e-government concept a network interpretation for complex interaction of national infrastructure elements has been proposed and its sustainable development perspective has been built.

Keywords: E-government, smart world, network platform, sustainable development

Введение. Современные подходы, нацеленные на развитие устойчивого информационного общества – глобального, национального, регионального или городского предполагают использование таких перспективных средств как электронное управление и электронное правительство. Термин «электронное правительство» не имеет единого строгого определения. ООН и Американская Организация по вопросам государственного управления указы-