

4. *Тедеев, А.А.* Электронное государство [Текст] : монография / А.А. Тедеев, В.Е. Усанов. – М. : ООО «Издательство «Элит», 2008. – 312 с.
5. Рабочая программа по дисциплине цикла Б2 «Математика». – Москва : ФГНУ ИНИПИ РАО, ОФЭРНиО, 2012. – № 18529.
6. *Лаго, Г.Н.* Ускоренный способ обучения практической английской грамматике с использованием лагограм, символов и таблиц [Текст] / Г.Н. Лаго. – М : ФГНУ Госкоорцентр, ОФАП, 2008. – №1052.
7. *Куклев, В.А.* Электронный схемокурс “Безопасность жизнедеятельности в схемах и таблицах” – М : ФГНУ Госкоорцентр, ОФАП. – № 3506.
8. *Тимофеева, Ю.Ф.* Электронный образовательный ресурс "Техническая физика и ТРИЗ" (ТФ и ТРИЗ) – М: ФГНУ ИНИПИ РАО, ОФЭРНиО, 2011. – № 17024.
9. *Галкина, А.И.* Теория и практика электронной регистрации результатов интеллектуальной деятельности работников науки и образования [Текст] / А.И. Галкина // Информатизация науки и образования. – М : ФГНУ ИТТ «Информика», 2012. – № 1 (13). – С. 132-145.

УДК 378.1

Е.Н. Глушков, Г.Д. Бухарова
КАК ЗАЩИТИТЬ ЧАСТНУЮ СЕТЬ WI-FI ОТ ВЗЛОМА?

Глушков Евгений

zhecker@mail.ru

Бухарова Галина Дмитриевна

gd-buharova@yandex.ru

ФГАОУ ВПО «Российский государственный профессионально-педагогический университет», Россия, г. Екатеринбург

HOW TO PROTECT PRIVATE WI-FI NETWORK FROM HACKING?

Glushkov Evgeny

Bukharova Galina Dmitrievna

Rushydro Vpo «Russian University Of Educational Information Technology»,

Russia, Yekaterinburg

Аннотация. Wi-fi в последние годы получил широкое распространение не только в промышленных и производственных компьютерных сетях. Эту технологию используют для реализации беспроводного доступа в Интернет дома, в учебные заведения, библиотеки, кафе, рестораны, вокзалы и аэропорты. Технология Wi-fi практически повсеместно позволяет получить доступ в Интернет без использования проводов.

Abstract. Wi-fi in recent years, is widespread not only in industrial and manufacturing of computer networks. This technology is used for the implementation of wireless Internet access at home, in schools, libraries, cafes, restaurants, railway stations and airports. Wi-fi technology almost everywhere allows you to access the Internet without wires.

Ключевые слова: *Wi-fi технология, Интернет, беспроводная технология*

Keywords: *Wi-fi technology, the Internet and wireless technology*

С развитием технологий широкое распространение получила технология беспроводных сетей на основе стандарта IEEE 802.11 – Wi-fi (1).

Wi-fi в последние годы получил широкое распространение не только в промышленных и производственных компьютерных сетях. Эту технологию используют для реализации беспроводного доступа в Интернет дома, учебные заведения, библиотеки, кафе, рестораны, вокзалы и аэропорты.

Технология Wi-fi практически повсеместно позволяет получить доступ в Интернет без использования проводов. Некоторые Интернет-провайдеры разворачивают комплексы точек доступа Wi-fi, которые покрывают сетью целые кварталы мегаполисов.

Операционные системы Android и iOS, используемые в подавляющем большинстве современных мобильных устройства, нацелены на тесную интеграцию смартфона с онлайн-сервисами и социальными сетями. Все современные смартфоны оборудованы модулем Wi-fi. Кроме этого сети Wi-fi поддерживаются широким спектром современных мультимедийных устройств, игровыми консолями и офисной периферией.

Все это, наряду с низкими ценами на оборудование Wi-fi для домашнего использования, предопределило лавинообразное распространение домашних Wi-fi сетей.

Любая частная сеть может стать объектом атаки. Злоумышленник, получив доступ к чужой сети, может систематически красть трафик, информацию об аккаунтах пользователей в сетях, платежных системах, а также совершать от чужого имени противоправные действия в сети.

Всё сказанное свидетельствует о необходимости предпринятия комплекса мер по защите домашней сети Wi-fi.

Одной из защит частных сетей Wi-fi могут быть пароли со стандартами WEP, WPA или WPA2.

Стандарт WEP считается устаревшим (2). Использовать его не рекомендуется, так как уже довольно давно в открытом доступе в сети выложены алгоритмы подбора паролей WEP без словаря. Поэтому безопаснее использовать стандарт WPA-2. Правила установки пароля для беспроводной сети мало отличаются от правил задания паролей. Для этого следует использовать буквы разного регистра, специальные знаки, знаки препинания и цифры.

Крайне важно изменить логин и пароль для входа в панель управления роутером. Если на роутере стоит последнее обновление прошивки и задан сложный пароль, взломать его будет непросто.

При первоначальной настройке сети лучше сменить SSID сети. Можно также сделать его скрытым.

В SSID по умолчанию зачастую указана модель роутера, что может помочь злоумышленнику быстрее взломать сеть.

Скрытие SSID – дополнительная мера, и на безопасность влияет мало, поскольку все взломы производятся с использованием адаптеров в режиме мониторинга, которые перехватывают широковещательные пакеты, передающиеся даже по скрытым сетям. Несмотря на это, скрытие сети поможет не привлекать повышенного внимания – она не будет видна для устройств со стандартным ПО.

Бытует мнение, что панацеей может стать фильтр по MAC-адресам, настраиваемый в панели управления роутером. Однако, как показывает практика, это далеко не так.

Связано это с тем, что при взломе беспроводной сети адаптер переводится в режим мониторинга, разрешенный MAC-адрес будет виден при передаче широковещательных пакетов. Это делает фильтр по MAC-адресам абсолютно неэффективным. Злоумышленнику достаточно сменить собственный MAC-адрес, и тогда он легко проходит фильтр.

Последнее немаловажное правило построения защищенной сети Wi-fi – обязательное отключение технологии WPS, которая позволяет получать ключ от сети, отправив на роутер восьмизначный код, состоящий из цифр. Этот код формируется по определенным правилам. Количество возможных пин-кодов ограничено, что облегчает их подбор.

На данный момент это одна из серьезнейших уязвимостей сетей Wi-fi. Через подбор пин-кода WPS сеть с паролем любой сложности взламывается (в зависимости от ПО роутера) за несколько часов. В некоторых прошивках роутеров реализована защита от частых попыток подключения, однако она лишь замедляет неминуемый взлом.

Получение пароля сети с включенной технологией WPS займет около 60-80 часов. Важно отметить, что взлом системы с WPS – довольно простая операция и при достаточном уровне сигнала осуществима почти в 100% случаев.

Отключение WPS, задание сложных паролей сети и панели управления роутером, скрытие измененного SSID сделают сеть Wi-fi намного более устойчивой к взлому.

В содержании статьи нами сделана попытка о возможной вероятности защиты частных сетей Wi-fi от взлома.

Список литературы

1. Безопасность wi-fi. Правильная защита wi-fi. [Электронный ресурс]. – URL: <http://mediapure.ru/stati/bezopasnost-wi-fi-pravilnaya-zashhita-wi-fi/> (дата обращения 31.11.2013).
2. Как защитить Wi-Fi от взлома [Электронный ресурс]. – URL: <http://wefavor.ru/article/35-s-wi-fi-security> (дата обращения 31.11.2013).

УДК 004.94

А.В. Горохов, А.С. Зубов ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИННОВАЦИОННЫХ ПРОЦЕССОВ НА БАЗЕ НАУЧНО-ОБРАЗОВАТЕЛЬНОГО КОМПЛЕКСА

Горохов Андрей Витальевич

GorokhovAV@volgatech.net

Зубов Александр Сергеевич

Zubov-a-s@yandex.ru

*ФГБОУ ВПО «Поволжский государственный технологический университет»,
Россия, г. Йошкар-Ола,*

IMITATION MODELING OF INNOVATION PROCESSES BASED ON SCIENTIFIC AND EDUCATIONAL COMPLEX

Gorokhov Andrey Vitalevitch

Zubov Alexander Sergeevich

Volga State University of Technology, Russia, Yoshkar-Ola