УЯЗВИМОСТИ ПРОТОКОЛОВ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ

Кучко А.С.
студент 4 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь

Сегодня доступ в Интернет можно получить практически в любом месте в парке, в кафе, в школе, в университете и на остановках общественного транспорта. Это стало возможным благодаря беспроводным сетям. Однако, не все беспроводные сети являются безопасными. Для обеспечения безопасности пользователей были разработаны беспроводные протоколы безопасности: WEP, WPA / WPA2, WPS, OPEN.

Цель этой работы – найти уязвимости в протоколах беспроводной сети, изучить их и предоставить рекомендации по безопасности.

Материал и методы. Для сравнения протоколов безопасности, мы использовали данные об уязвимостях этих протоколов. Нами были проанализированы сообщения разных пользователей на форумах в Интернете и изучена документация для протоколов безопасности беспроводной сети.

Результаты и их обсуждение. Проанализировав данные собранные от пользователей на разных форумах были выбраны следующие протоколы для сравнения их уровня безопасности.

OPEN – это сеть, в которой не использует протоколы безопасности. Информация между пользователем и точкой доступом никак не шифруется. Любой пользователь может подключится к данной сети так как зона покрытия беспроводной сети составляет от 10 метров и больше, с учетом длины антенны хакера. Поэтому конфиденциальность данных при открытой передаче по беспроводной сети находится под угрозой.

WEP (*Wired Equivalent Privacy*) – первый стандарт защиты Wi-Fi, был придуман в конце 90-х годов. Стандарт защиты WEP является самым не защищенным протоколом на сегодняшний день. Основным механизмом шифрования, используемым WEP, является RC4, который широко используется в различных интернет-протоколах, включая защищенные веб-страницы (HTTPS). Первая проблема протокола заключается в самой реализации RC4. В WEP возможно повторение ключей безопасности, что нарушает главное правило RC4: никогда не использовать повторно ключ.

Второй проблемой WEP является то, что пароли в WEP имеют длину 40 бит или 104 бита, то есть очень маленькие комбинации. Подобрать её можно за несколько минут.

И последняя проблема, при шифровании пакетов используется временный ключ. В WEP, с каждым пакетом данных, передаётся несколько байт используемого ключа. Таким образом, вне зависимости от количества символов, используемых при создании защитного ключа можно взломать беспроводную сеть на основе WEP имея достаточное количество перехваченных пакетов.

WPA (*Wi-Fi Protected Access*) – новое поколение протоколов, кардинально отличающийся от протокола WEP. Пароль задается произвольным количеством символов, от 8 до 63 байт, что делает его подбор намного сложнее нежели в WEP. Стандарт поддерживает два алгоритма шифрования данных: TKIP и CCMP. Одна из особенностей TKIP – возможность Michael-атаки. Michael-атака – простая передача «испорченных» пакетов для полного отключения всей сети. Достаточно всего двух пакетов, для полного выведения сети из строя на 60 секунд.

Как и любой широкий программный комплекс, система несовершенна. Недоработки или критические дыры в системе безопасности не исключены. Для быстрых исправлений некоторых критичных дыр в WEP с TKIP было введено правило, по которому точка доступа должна блокировать все соединения через себя. То есть «впадать в спячку» на одну минуту, если выявляется атака на подбор ключа.

WPA2 определяется стандартом связи IEEE 802.11i, принятым в июне 2004 года, и призван заменить WPA. конце 2017 года специалисты обнаружили большую уязвимость WPA2. Они создали компьютерную программу EXPLOIT, благодаря которой злоумышленник мог перехватывать логины и пароли. Несмотря на то, что в WPA2 используется AES-шифрование, это не помогло. Однако данная программа не была презентована.

WPS (*Wi-Fi Protected Setup*) – новая технология, с помощью которой пользователь может не вводить пароль для подключения к беспроводной сети. Но при разработке данной технологии была допущена критическая ошибка. Пользователь, подключается к точке доступа с поддержкой WPS по PIN-коду, состоящему из восьми символов. Однако из-за уязвимости в WPS нужно подобрать только четыре символа из восьми. Взломщику хватит десяти тысяч переборов, чтобы подключиться к сети. Злоумышленник может получить доступ к точке доступа через несколько часов: от трёх до пятнадцати, ведь в секунду можно отправлять от десяти до пятидесяти запросов.

Узнав о уязвимости, производители начали внедрение технологии, которая ограничивает число попыток входа за минуту. Если лимит попыток подключений превышен, точка доступа на время отключается. Тем не менее, устройств с такой технологией на рынке пока мало. Более того, даже если точка доступа отключится на время – это ничего не меняет, это просто увеличит время взлома данной точки доступа с поддержкой WPS.

Заключение. Исследование выявило уязвимости в часто используемых протоколах безопасности. Это показывает, что использование Wi-Fi-сетей небезопасно. Wi-Fi не подходит для передачи секретной и личной информации. Чтобы максимально повысить безопасность, следуйте этим простым рекомендациям: не подключайтесь к открытым сетям, перед подключение проверьте тип протокола, это можно сделать в настройках вашего устройства, используйте последнюю версию программного обеспечения, если ваша точка доступа поддерживает технологию WPS, убедитесь, что WPS выключен.

Литература

1. Росс, Дж. Wi-Fi, уязвимости беспроводных сетей, 2005. – 98 с.
2. Олифер, Ф. Компьютерные сети. Принципы, технологии, протоколы, 2016. – 72 с.
3. Сергеев, А.Основы построения локальных сетей, 2013. – 205 с.
4. Одом, Ю. Протоколы в беспроводных сетях, 2016. – 103 с.
5. Чайка, Ю. Современные беспроводные сети, 2011. – 202 с.
6. Электронный ресурс: habrahabr.ru/post/224955/

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА УРОКАХ В НАЧАЛЬНОЙ ШКОЛЕ

Лабовкина О.В.

выпускница ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь

Научный руководитель – Лабовкин В.Н., канд. техн. наук, доцент

Информатизация общества предъявляет к учителям начальной школы повышенные требования владения инструментарием информационных технологий (ИТ). Успех внедрения ИТ в образовательный процесс во многом зависит от квалификации педагога, правильного выбора компьютерных образовательных ресурсов, методов и форм организации учебной деятельности. Владение ИТ во многом определяет образованность современного человека, поэтому развивать информационную культуру необходимо с начальной школы, когда закладывается основы фундамента образования, от которого зависит дальнейшая деятельность человека в информационном обществе [1].

Цель работы – исследовать влияние применения информационных технологий на успеваемость учащихся начальной школы

Материал и методы. Исследования проводились на базе Государственного учреждения образования «Средняя школа № 21 г. Витебска». В нем приняли участие учащиеся начальной школы в количестве 25 человек. На первом этапе, когда ученики обучались во 2 классе, занятия проводились традиционными методами. На втором этапе, когда эти же ученики были в 3 классе, преподавание велось с использованием информационных технологий. В качестве методов исследования использовались педагогическое наблюдение, сравнительный анализ, обобщение и статистическая обработка данных.

Результаты и их обсуждение. Информатизация современного общества ставит перед учителем начальной школы задачу научить детей работать с большими объемами информации. Ее решение видится в комбинировании традиционных методов обучения с компьютерными информационными технологиями.

Ограничение времени нахождения младших школьников за компьютером 10–15 минутами позволяет использовать для представления информации мультимедийного проектора, подключенного к ПК [2]. Это позволяет учителю применять красочный иллюстративный материал с элементами анимации, развивая тем самым наглядно – образное мышление учащихся, что активизирует процесс усвоения нового учебного материала, дает возможность использования большого количества дидактического материала, обеспечивает индивидуальный подход к обучению.

Удобной формой представления материала в виде мультимедийной презентации предоставляет приложение PowerPoint, входящее в пакет Microsoft Office. Наполнение слайдов формируется в зависимости от целей урока и его информационной базы. Большое значение имеет логическое сочетание набора упражнений и их последовательность.

При подготовке к урокам автором разрабатывались презентации, состоящие из 5–10 слайдов. На них не только представлялся новый материал по теме урока, но и предлагались упражнения для закрепления материала. Мультимедийная презентация использовалась на разных этапах урока: повторение пройденного материала, объяснение, закрепление и проверка нового материала. Кроме фронтальной работы презентации использовались в режиме индивидуальной работы учащихся для выполнения тренировочных и проверочных заданий. Особенно эффективным оказалось использование презентаций на уроках русского и белорусского языка и литературы, математики. Для наполнения слайдов использовались собственные разработки автора и электронные копии белорусских и российских учебных пособий, размещенных в интернете в открытом доступе.

Эксперимент по применению ИТ в начальной школе показал, что компьютерные наглядные пособия позволяют повысить темп урока на 10–20%, это дает возможность учителю более рационально орга-