УДК 004.056

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ WPS С ПОМОЩЬЮ ПРИЛОЖЕНИЯ ДЛЯ ANDROID «WPS CONNECT»

Конищева Е.С., магистрант; Петров Д.А., магистрант; Фунтиков М.Н., ст. преп.
(ГОУ ВПО «Донецкий национальный технический университет», г. Донецк, ДНР)

На сегодняшний день беспроводные сети стандарта IEEE 802.11n широко распространены среди пользователей. Увеличение числа пользовательских устройств дает возможность проводить проверку сети на уязвимости с помощью смартфона. Для того чтобы осуществить проверку сети достаточно установить приложение.

Для исследования был использован смартфон LG G2, с версией Android 5.0.2. В работе было исследовано приложение для Android «WPS Connect», которое позволяет сканировать радиоэфир на обнаружение беспроводных сетей. После чего возможно получить ключ доступа к обнаруженным беспроводным сетям. Приложение создано для проверки уязвимостей собственной сети, однако ни что не ограничивает пользователя, использовать приложение не по назначению.

На рисунке 1 показан результат сканирования радиоэфира: зеленым выделены сети, проверку уязвимости протокола WPS которых можно осуществить; красный цвет означает, что протокол WPS(QSS) отключен, также приложение показывает уровень сигнала и протокол шифрования.

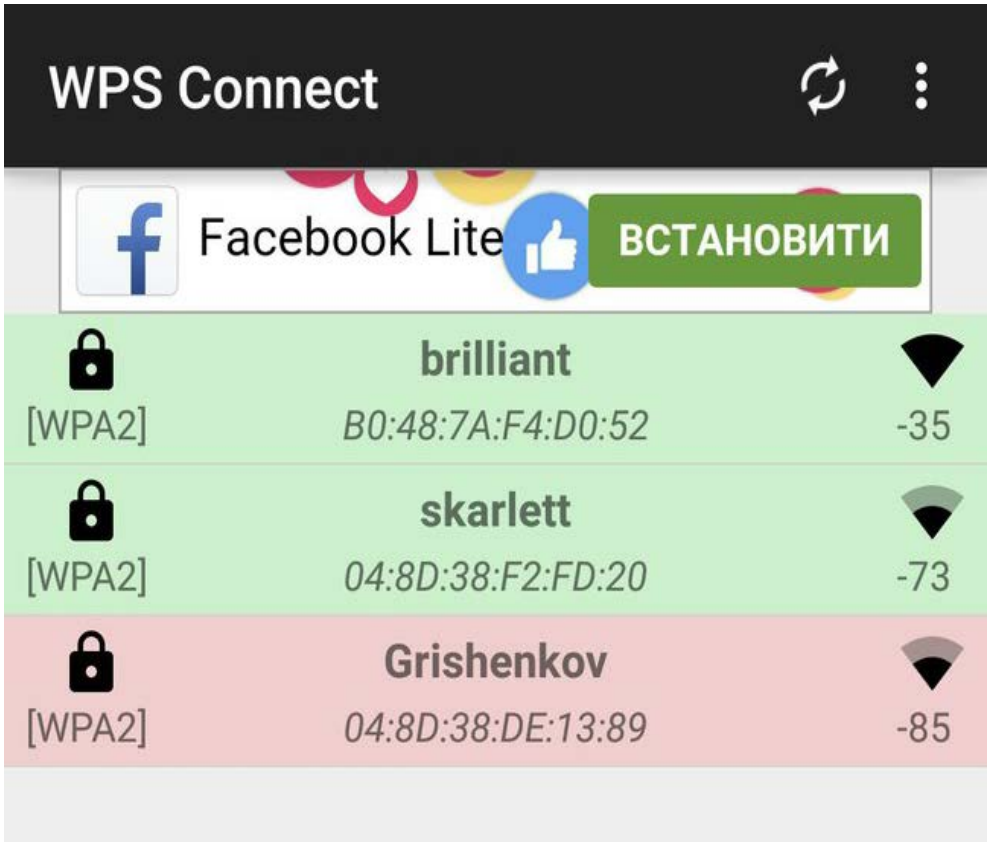

Рисунок 1 – Результат сканирования радиоэфира

В процессе сканирования радиоэфира была обнаружена исследуемая пользовательская сеть «brilliant». Далее для проверки безопасности сети была произведена попытка получения доступа к ней, рисунок 2.

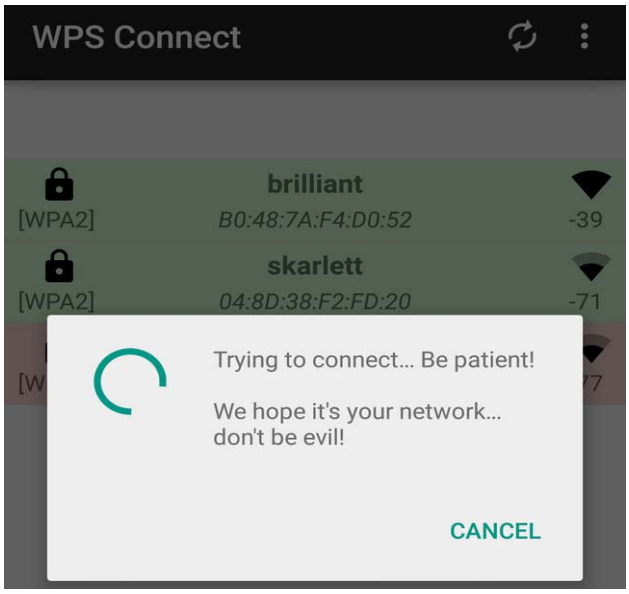

Рисунок 2 – Попытка получения доступа к сети

Приложение предоставило полную информацию, включая секретный ключ доступа, об исследуемой беспроводной сети «brilliant». Данная информация предоставлена на рисунке.

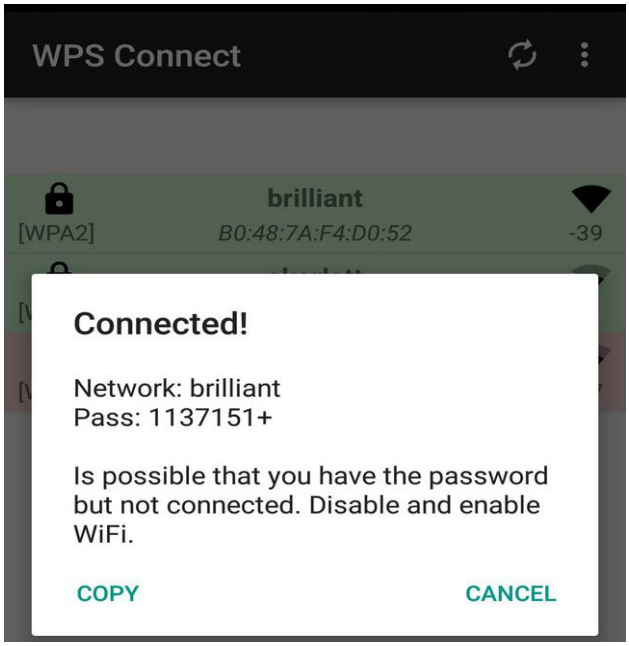

Рисунок 3 – Результат, полученный от программы при попытке получения доступа к пользовательской беспроводной сети «brilliant»

Таким образом, при наличии включённого WPS возможно получение ключа доступа к беспроводной сети. Исследование показало, что подключение к сети доступно любому пользователю при наличии определенных условий. Исследования по данной тематики проводится на кафедре радиотехники и защиты информации.

Перечень ссылок

1. Губенков, А. А. Исследование проблем безопасности протокола WPS [Электронный ресурс] / А. А. Губенков // Информационная безопасность регионов. - 2014. - №2 (15). - Режим доступа : https://cyberleninka.ru/article/n/issledovanie-problem-bezopasnosti-protokola-wps. – Загл.с экрана.