Лабораторная работа № 3.

Анализ устойчивости алгоритмов шифрования WEP и WPA-TKIP

Оформление отчета

**Напишите ответы на вопросы в соответствии с Вашим вариантом**

10. Может ли WPA-PSK обеспечить надежную защиту информации?

Да, WPA2-PSK с паролем от 12 символов a-z обеспечит защиту на 2000+ лет.

**Заполните таблицу**

|  |  |  |
| --- | --- | --- |
|  | WEP | WPA-PSK |
| Пароль | 12345678 | 12345678 |
| Время определения пароля, с | 360 | 440 |
| Количество пакетов, необходимых для опре-деления па-роля | 2407 | 1634 |

**Напишите вывод по лабораторной работе. Сравните в выводе эффективность атак на протоколы WEP и WPA-PSK. Укажите, какие меры необходимо принять для обеспечения необходимого уровня защиты беспроводной сети от взлома**

WEP и WPA используют алгоритм RC4 для шифрования сетевых данных. RC4 по своей сути небезопасен, особенно в случае WEP, который использует небольшие ключи и управление ключами. Поскольку WEP отправляет пароли в текстовом виде по сети, довольно просто взломать сеть, используя сетевые снифферы.

WEP, WPA используют PSK (предварительный общий ключ) для аутентификации. Хотя WEP использует простой ключ PSK, WPA объединяет его с другими методами шифрования, такими как WPA-PSK и EAP-PSK, чтобы сделать процесс аутентификации более безопасным. Стандарт WPA для аутентификации — 802.1x / EAP.  
WPA использует 256-битное шифрование для аутентификации, которое достаточно безопасно. Но поскольку у пользователей, как правило, возникают трудности с установкой таких длинных паролей, кодовая фраза может составлять от 8 до 65 символов, которая сочетается с EAP для шифрования и аутентификации.

Если у вас старое устройство, которое не поддерживает WPA2, тогда вы должны выбрать WPA с высоким уровнем шифрования и аутентификации. Вариант похуже — перейти с WPA и относительно низким качеством шифрования и аутентификации. Я бы предложил WEP как выбор последнего средства, поскольку он по-прежнему лучше, чем просто поддерживать беспроводную сеть без безопасности.

При использовании алгоритма WEP получить доступ к сети возможно за несколько минут, при наличии активного клиента, подключенного к данной точке доступа.

Подбор ключа WPA-PSK будет успешным только в том случае, если он будет присутствовать в словаре по которому ведется перебор. Если пароль достаточно большой, то подбор будет либо очень долгим, либо никогда не завершится.