

---

# Практическое задание № 11.

## Безопасность беспроводных сетей

Опубликовано 29.11.2022

Дедлайн 20.12.2022

---

## 1 Введение

Лабораторная работа посвящена анализу безопасности беспроводных сетей. Для выполнения работы необходим компьютер установленной системой Linux или с запущенной через Live-CD или USB-flash системой Kali Linux. Виртуальные машины для выполнения работы не подходят. Кроме того драйвер сетевой карты должен поддерживать перевод карты в неразборчивый режим.

## 2 Задания

### 2.1 Открытые сети

1. Переведите сетевую карту в неразборчивый режим:

```
airmon-ng start wlan0
```

2. Запустите Wireshark (предпочтительно также использовать `airodump-ng`, чтобы слушать все каналы) и проверьте наличие данных из открытых Wi-Fi сетей.

В случае, если карта/драйвер не поддерживает неразборчивый режим, то будут видны только широковещательные (broadcast) и групповые (multicast) пакеты.

3. Выяснить насколько защищена информация в таких сетях? Возможен ли перехват личной информации пользователей? Какую информацию вы можете перехватить от своего отдельного устройства? Приведите примеры.

### 2.2 Закрытые сети

Для выполнения аудита закрытой сети необходимо использовать утилиту `airodump-ng`, которая служит для записи передаваемых данных в файл. Для выполнения атаки необходимо перехватить момент подключения клиента к сети, после чего ключ к сети может быть подобран с помощью утилиты `aircrack-ng`

1. Перевести сетевую карту в неразборчивый режим, если она еще не переведена.

2. Запустите `airodump` и дождитесь подключения клиента (также возможна активная атака с использованием `aireplay-ng`):

```
airodump-ng -w file mon0
```

3. Подбор ключа:

```
aircrack-ng -w /path/to/dictionary file-01.cap
```

4. Если ключ найден, то для просмотра трафика добавьте его в настройках Wireshark.

## Материалы

1. <https://www.aircrack-ng.org/documentation.html>
2. <https://wiki.wireshark.org/CaptureSetup/WLAN>

