

# Руководство пользователя

## 1. Установка необходимых компонентов

Для запуска веб-приложения на локальном компьютере необходимо выполнить следующие действия:

1. Установить Python версии 3.8 или выше. Рекомендуется использовать официальный дистрибутив с сайта [python.org](https://python.org).
2. Установить системную утилиту `tcpdump`, если она ещё не установлена:
  - Для Linux/macOS: воспользоваться пакетным менеджером (например, `apt`, `brew`).
  - Для Windows: установить через WSL или использовать альтернативный способ захвата трафика.
3. Скачать проект с GitHub.
4. Перейти в каталог проекта и установить зависимости командой:

```
pip install -r requirements.txt
```

## 2. Запуск приложения

1. Откройте терминал и перейдите в директорию с проектом.
2. Выполните команду:

```
sudo python3 app.py
```

и введите пароль от устройства

3. Откройте браузер и перейдите по адресу `http://127.0.0.1:5000`.

### 3. Работа с интерфейсом

Интерфейс приложения состоит из нескольких вкладок:

- **Главная:** краткое описание проекта и его возможностей.
- **Мониторинг трафика:** запуск/остановка захвата пакетов, просмотр таблицы с сетевыми данными, обновляемой в реальном времени.
- **Визуализация:** графики распределения протоколов, сервисов, количества соединений и аномалий.
- **Классификация:** отображение результата анализа — нормальный трафик или кибератака.
- **Инструкция:** справочная информация о работе системы.

### 4. Действия пользователя

1. Перейдите на вкладку **Мониторинг трафика**.
2. Нажмите кнопку «Старт» для запуска захвата сетевых пакетов.
3. Наблюдайте за обновлением таблицы и визуализацией трафика в реальном времени.
4. При необходимости нажмите «Стоп» для приостановки захвата.
5. Перейдите на вкладку **Классификация**.
6. Нажмите кнопку «Запустить анализ» для выполнения классификации собранных пакетов.
7. Ознакомьтесь с результатами: если обнаружены подозрительные соединения, будет выведено соответствующее уведомление.

### 5. Возможные ошибки и их решение

- **Ошибка доступа к интерфейсу:** убедитесь, что tcpdump запускается с правами администратора.
- **Приложение не запускается:** проверьте, что все зависимости установлены (`pip install -r requirements.txt`).
- **Пустая таблица:** проверьте подключение к интернету или правильность работы сетевого интерфейса.

### 6. Выход из системы

Для завершения работы достаточно закрыть окно браузера и остановить выполнение скрипта в терминале с помощью сочетания клавиш **Ctrl + C**.