

# **Описание функциональных характеристик «Программное обеспечение модуля искусственного интеллекта SNNAPS для определения аномалий сетевого трафика в формате pcapng в автоматизированных системах управления технологическими процессами»**

## **Анализ сетевого трафика:**

SNNAPS способен анализировать сетевой трафик, получая данные из файлов в формате pcapng. Это позволяет ему мониторить и анализировать сетевую активность.

## **Обнаружение аномалий:**

Основной функцией SNNAPS является обнаружение аномалий в сетевом трафике. При помощи методов машинного обучения и алгоритмов анализа, SNNAPS идентифицирует аномальные паттерны и потенциальные угрозы безопасности.

## **Обучение моделей:**

SNNAPS позволяет обучать свои модели для анализа сетевого трафика. Это включает в себя процесс обучения с использованием размеченных данных, чтобы модель могла более точно определять аномалии в будущем.

## **Настройка параметров:**

Пользователь может настраивать параметры анализа сетевого трафика, включая пороговые значения, чувствительность обнаружения и другие настройки для более точного анализа.

## **Отчетность:**

SNNAPS может предоставлять отчеты о результатах анализа, включая список обнаруженных аномалий, статистику и визуализацию данных.

## **Оповещения (по желанию):**

Пользователи могут настраивать оповещения, чтобы получать уведомления в случае обнаружения аномалий. Это позволяет оперативно реагировать на потенциальные угрозы.

## **Интеграция:**

SNNAPS имеет возможность интеграции с другими системами управления технологическими процессами или системами безопасности для автоматического реагирования на обнаруженные аномалии.

## **Логирование и аудит:**

SNNAPS может вести журнал действий и аудита, чтобы сохранить историю событий и обнаруженных аномалий для последующего анализа.