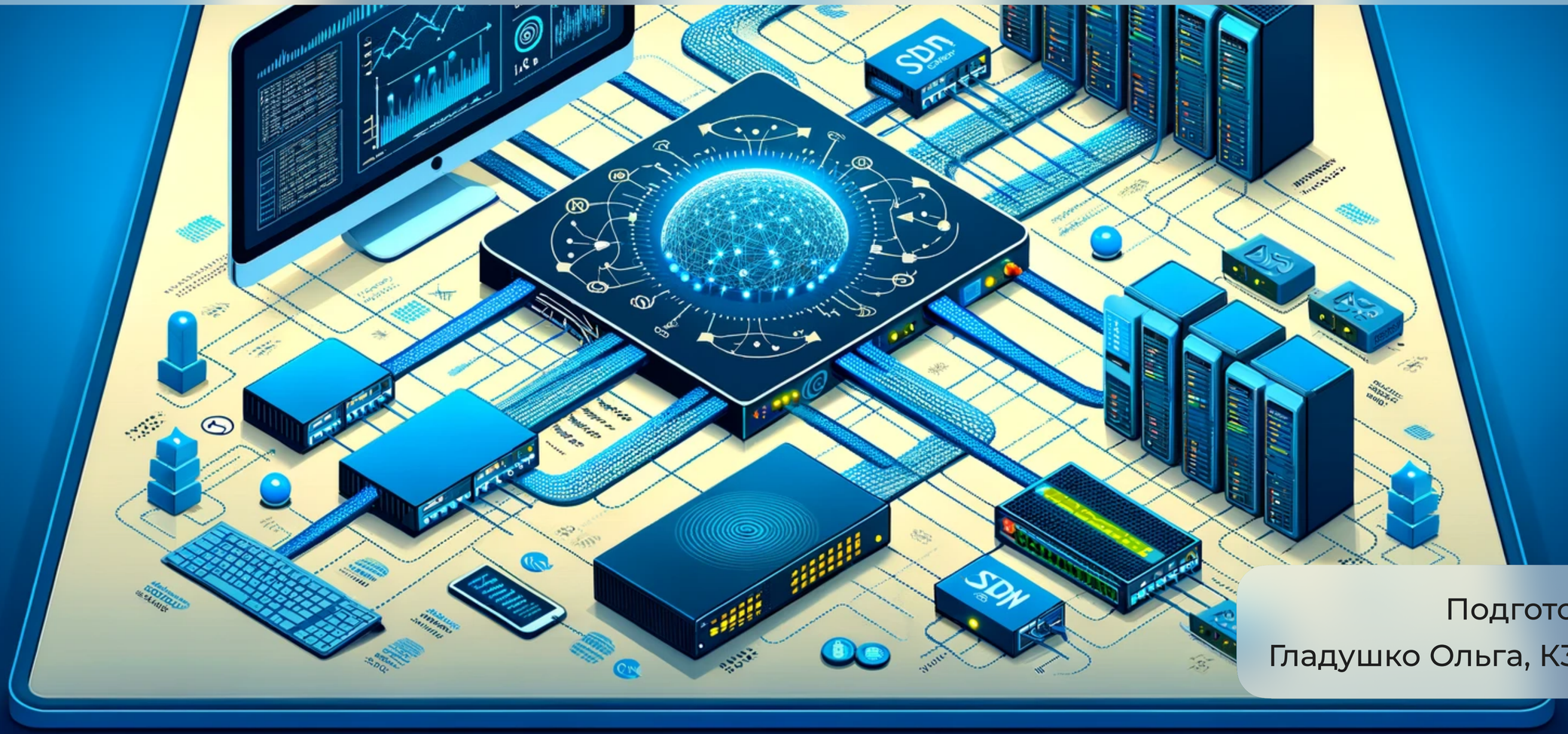
ML для классификации трафика в SDN-сетях



Подготовила
Гладушко Ольга, К34202

Этапы классификации потоков трафика

- Формирование базы данных для классификации
- Формирование матрицы признаков
- Определение классов с применением методов ML

Способы создания базы данных для классификации

- Моделирование потоков трафика в лабораторных условиях
  - Генерация потоков трафика
  - Открытые БД смоделированного трафика
- Мониторинг реального трафика на реальной сети
  - Социальный способ
  - Использование пользовательских терминалов
  - Открытые БД реального трафика
- Мониторинг реального трафика в условиях смоделированной сети
  - Имитация работы пользователя
  - Проигрывание ранее сохраненных трасс

Разметка базы данных

- Разметка перед отправкой пакета
  - Автоматическая разметка, DPI
  - Разметка генератором трафика
- Разметка уже готовой базы данных
  - Специальные инструментов
  - Ручная разметка
  - Анализ лог-файлов
- Изоляция
  - Временная изоляция
  - Физическая изоляция
- Кластеризация

Матрица признаков

- Базовые стат. данные одностороннего потока
- Расширенные стат. данные одностороннего потока
- Данные заголовков протокола TCP
- Расширенные стат. характеристики двухстороннего потока
- Глубокий анализ пакета

Наиболее распространенные алгоритмы классификации сетевого трафика методами ML

- Классическое обучение с учителем
- Классическое обучение без учителя
- Обучение с подкреплением
- Нейросети
- Ансамблевые методы

Инструменты для классификации

- Платформы WEKA и RapidMiner
- Языки программирования
- Statgraphics, Statistica, MATLAB и др.

Анализ работоспособности алгоритма

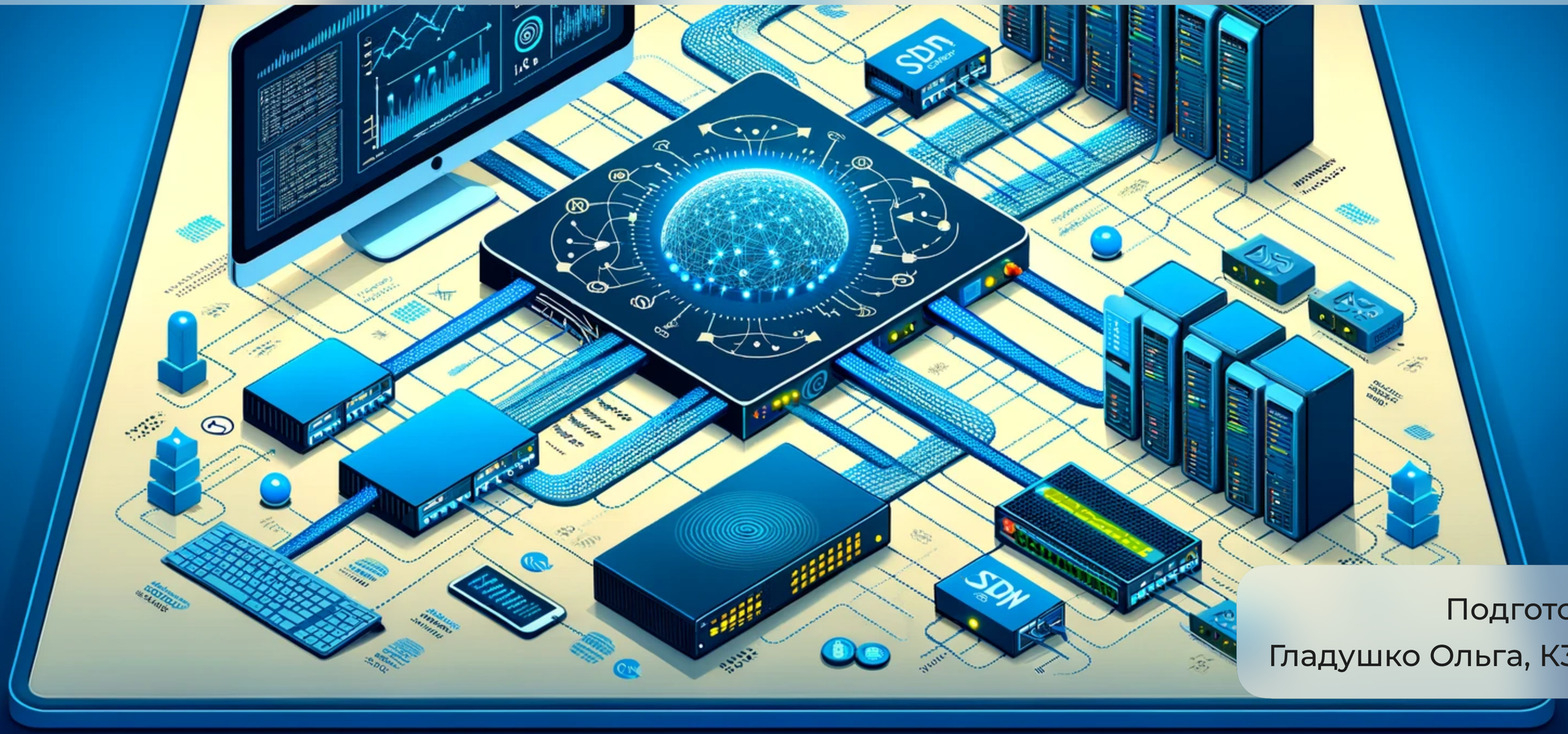
Параметры алгоритма, влияющие на скорость работы всей системы

- Количество пакетов потока, необходимое для классификации
- Время существования потока, необходимое для классификации
- Скорость построения модели
- Минимальное количество потоков одного класса, необходимое для построения модели
- Возможность дообучения
- Сложность внедрения алгоритма в сеть

Оценка результатов работы алгоритма

- Матрица несоответствий
- Доля правильных ответов
- Полнота
- Точность
- F1-мера

Спасибо за внимание!



Подготовила
Гладушко Ольга, К34202