Метод обнаружения сетевых атак с использованием многослойной нейронной сети

Студент: Криков Антон Владимирович

Группа: ИУ7-83Б

Научный руководитель: Клорикьян Петрос Вазгенович

Цель и задачи

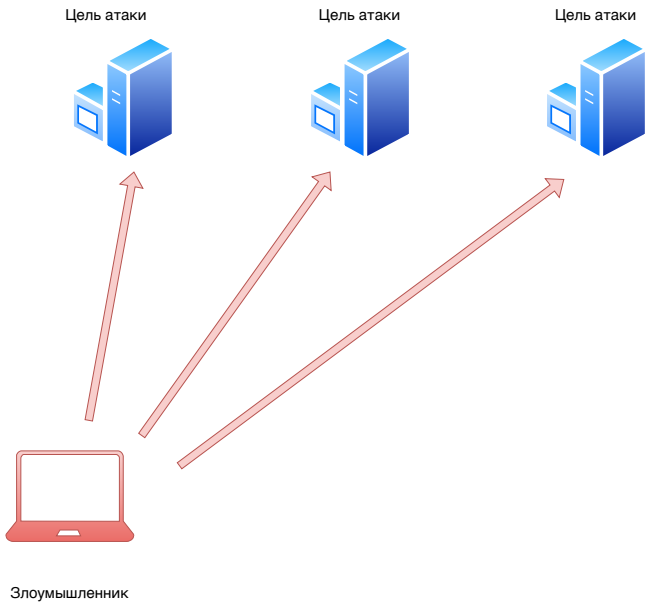
Цель — разработать метод обнаружения сетевых атак с использованием многослойной нейронной сети.

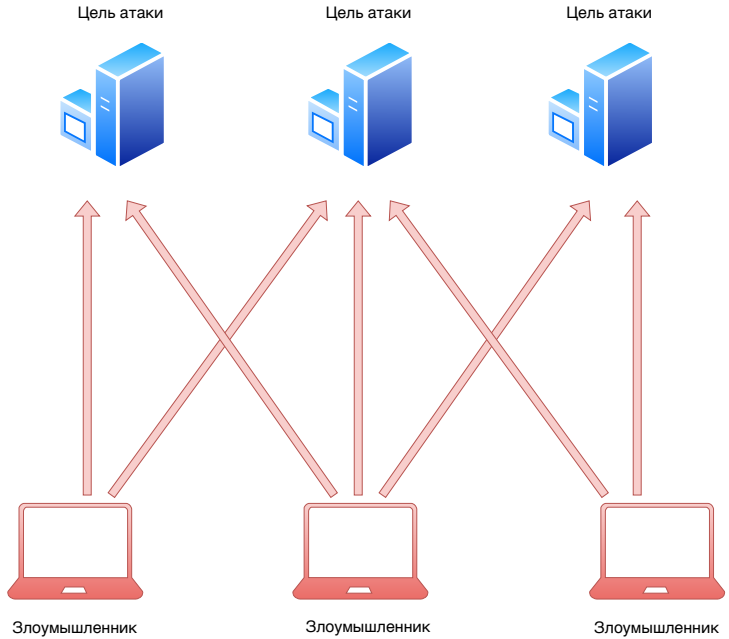
Задачи:

- Описать термины предметной области и обозначить проблему
- Описать технологии, с помощью которых можно реализовать метод
- Разработать метод обнаружения сетевых атак
- Разработать программный комплекс, реализующий интерфейс для взаимодействия с разработанным методом
- Исследовать разработанный метод на применимость

Модели атак

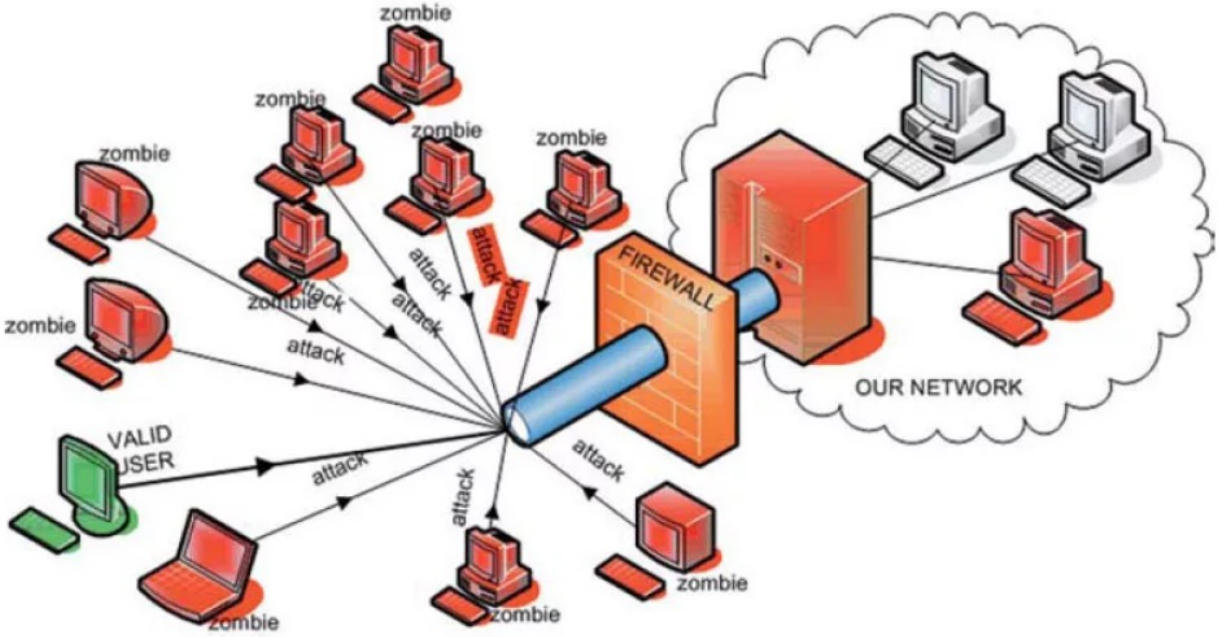
- Классическая
- Распределенная





Классификация сетевых атак

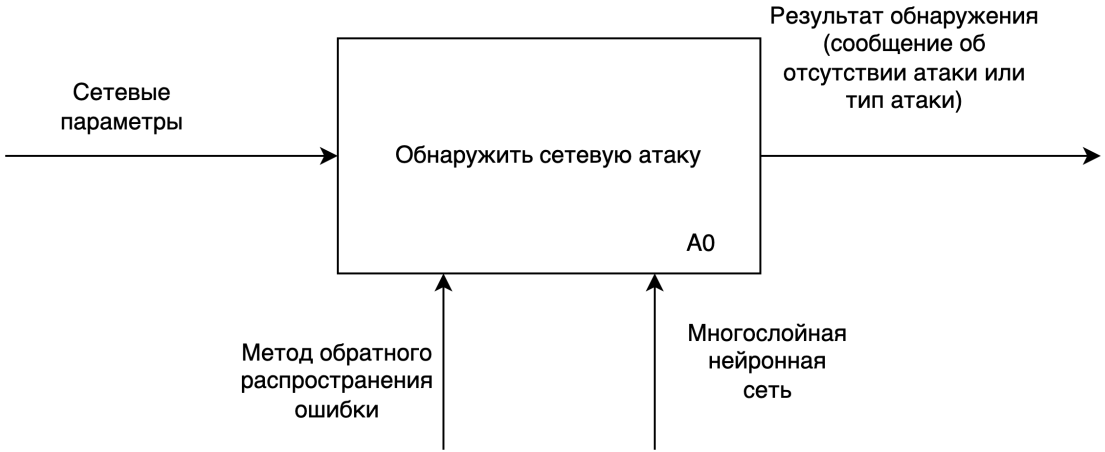
- PortScan
- DoS
- DDoS
- DDoS Hulk
- DDoS Heartbleed
- DDoS Slowloris
- Brute Force
- XSS
- SQLi



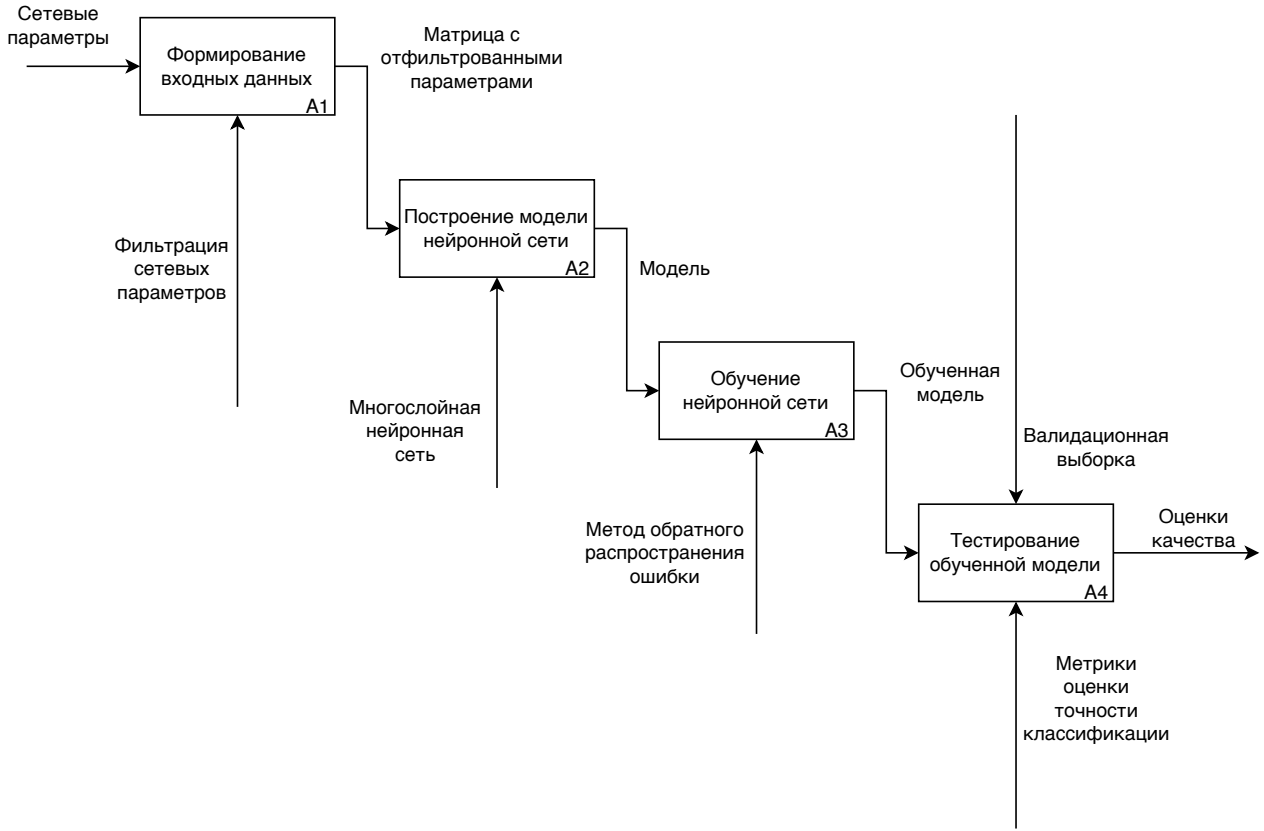
Постановка задачи

Ограничения:

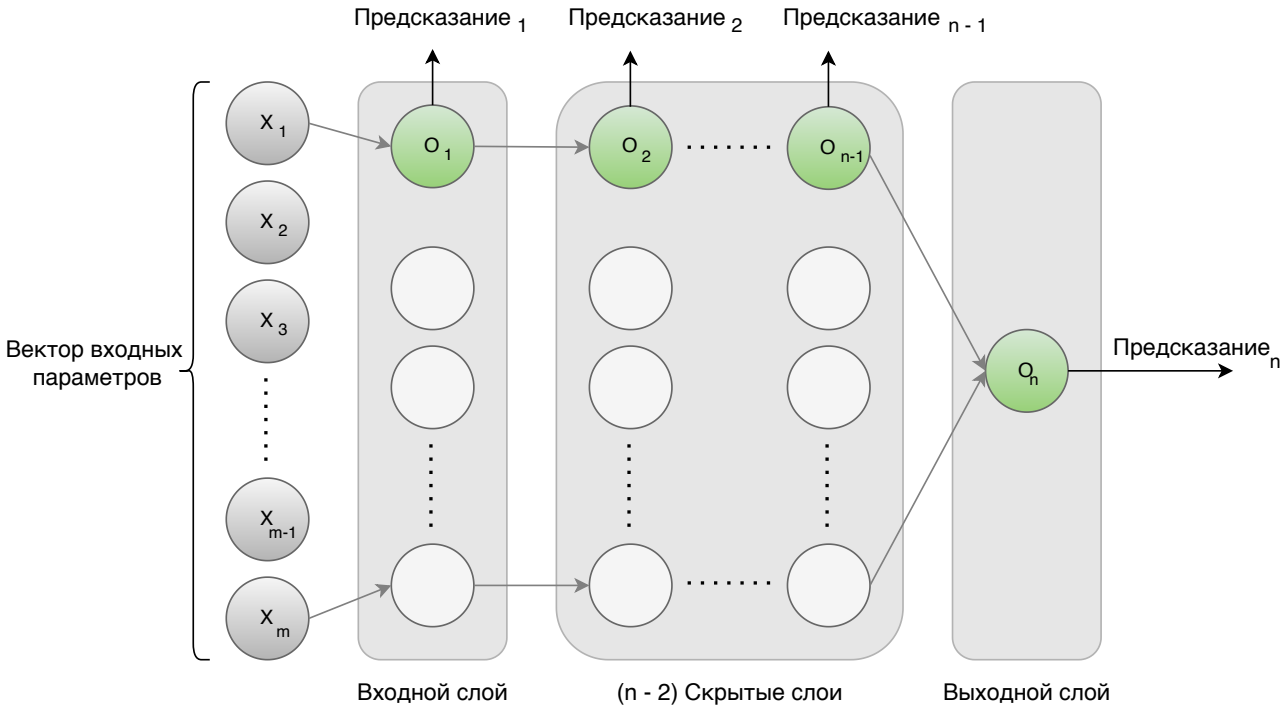
- На вход подается массив с информацией о сетевом трафике.
- Количество входных сетевых параметров = 30
- Количество классов = 15



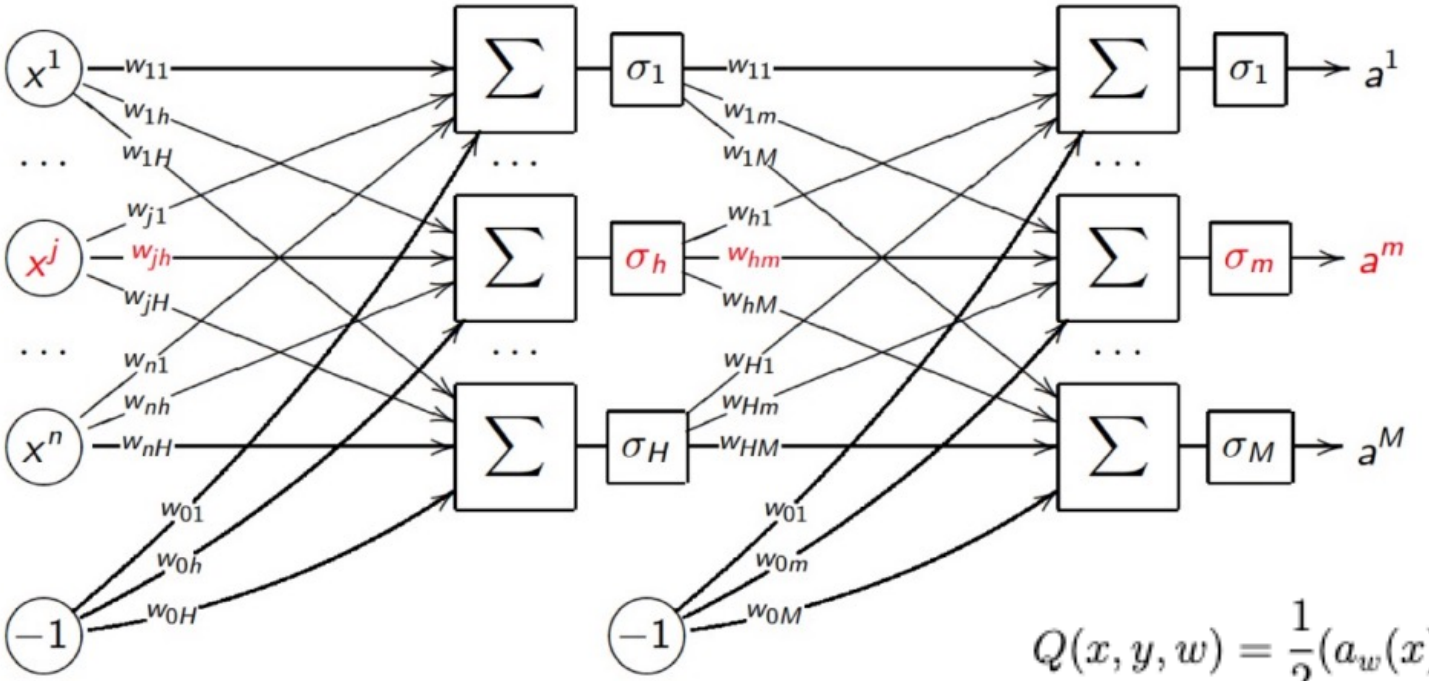
Метод обнаружения сетевых атак



Архитектура нейронной сети



Метод обратного распространения ошибки



$$Q(x, y, w) = \frac{1}{2}(a_w(x) - y)^2.$$

Оценка точности классификации

f-мера — это гармоническое среднее между точностью и полнотой

$$f1 = \frac{2 \times precision \times recall}{precision + recall}$$

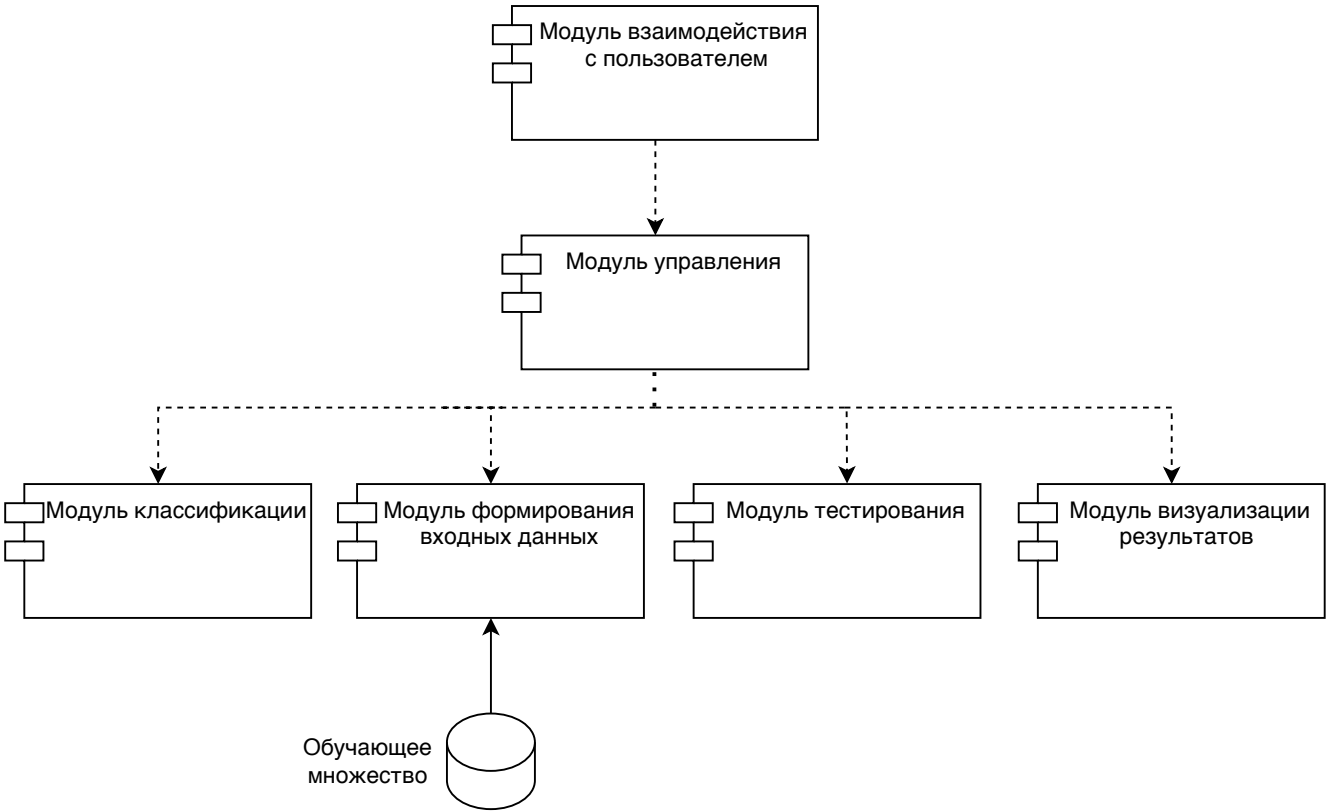
$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

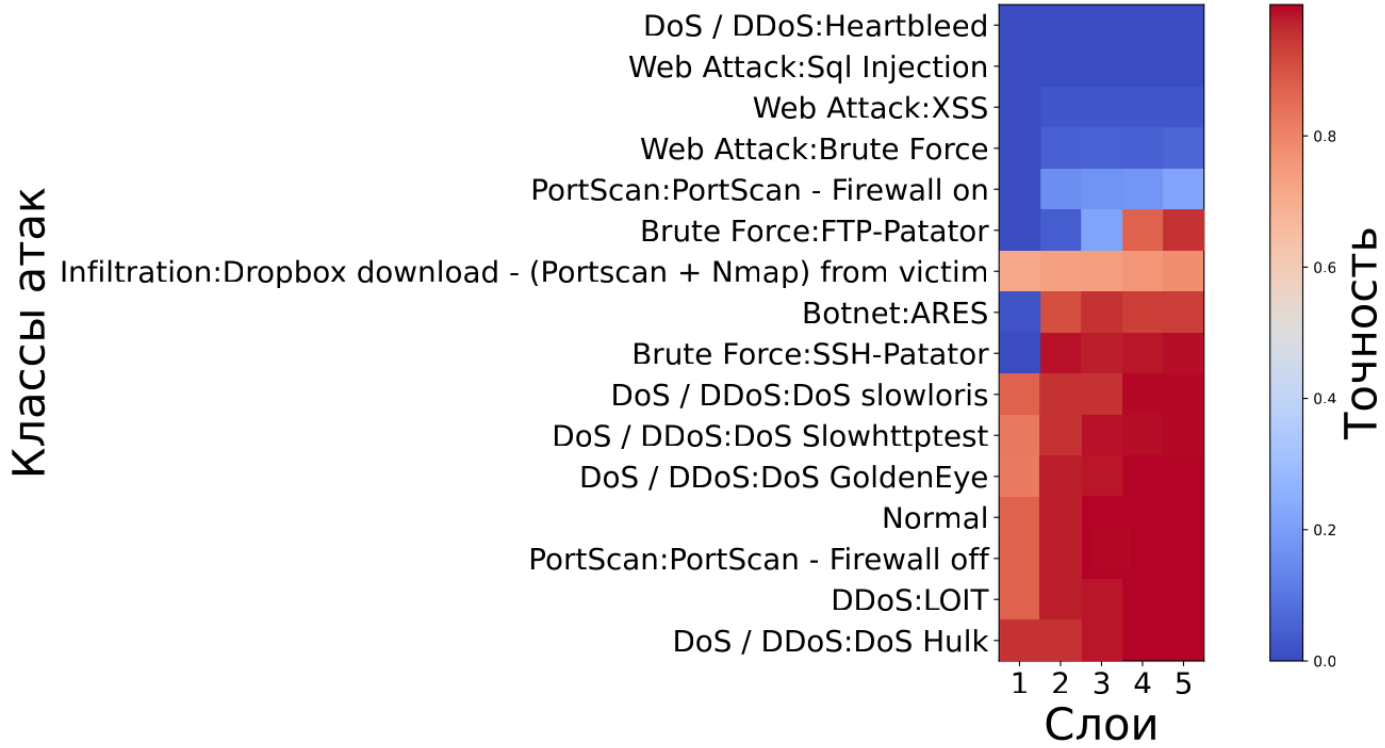
$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

		Экспертная оценка	
		Положительная	Отрицательная
Оценка системы	Положительная	True Positive (TP)	False Positive (FP)
	Отрицательная	False Negative (FN)	True Negative (TN)

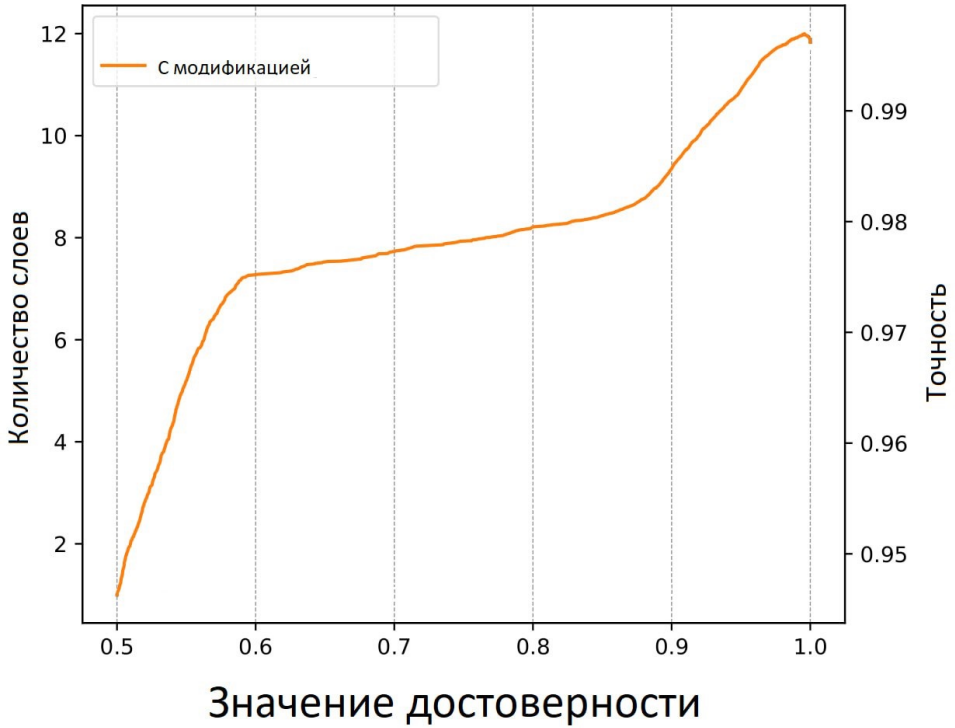
Структура ПО



Зависимость точности модели от класса сетевой атаки и количества слоев



Требуемое количество слоев для модели нейронной сети



Заключение

Достигнута цель: разработан метод обнаружения сетевых атак с использованием многослойной нейронной сети

Решены поставленные задачи:

- Описаны термины предметной области и обозначена проблема
- Описаны технологии, с помощью которых можно реализовать метод
- Разработан метод обнаружения сетевых атак
- Разработан программный комплекс, реализующий интерфейс для взаимодействия с разработанным методом
- Разработанный метод исследован на применимость

Дальнейшее развитие

- Обучение модели на других датасетах
- Распознавание незатронутых сетевых атак