Метод обнаружения сфальсифицированных видео на основе нейронных сетей

Студент: Куликов Дмитрий Алексеевич

Группа: ИУ7-82Б

Руководитель: Тассов Кирилл Леонидович

Москва, 2022

Актуальность

Ежедневно увеличивается рост дезинформации в интернете. В сети появилось огромное количество поддельных видеороликов. Большая часть из них созданы для того, чтобы навредить репутации и дискредитировать личность.

Мошенники создали сфальсифицированное видео с Олегом Тиньковым для рекламы поддельной страницы «Тинькофф Инвестиций».

Обзор существующих решений

Сервис	Стоимость	Общедоступность	Точность обнаружения
KaiCatch	1.7$ за один прогноз	+	Высокая, 90%
Deepware	Бесплатно	+	Низкая, работает нестабильно
Microsoft Video Authenticator	-	-	Неизвестно

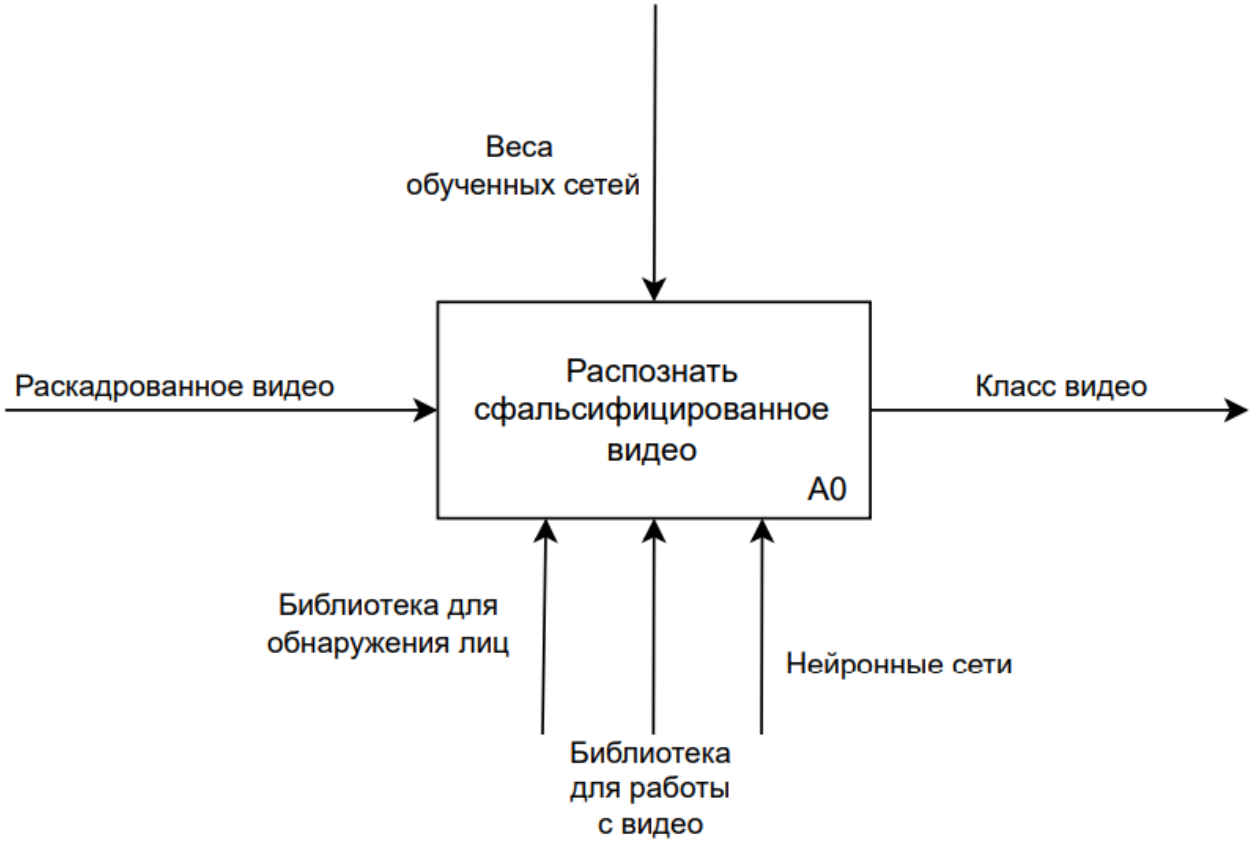
Цель и задачи работы

Цель работы — разработать и реализовать метод обнаружения сфальсифицированных видео на основе нейронных сетей.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать предметную область;
- выполнить обзор существующих подходов обнаружения поддельных видео с помощью нейронных сетей;
- в результате полученных во время анализа данных разработать метод обнаружения сфальсифицированных видео на основе нейронных сетей;
- реализовать разработанный метод в программном продукте;
- провести исследование работоспособности реализованного метода обнаружения.

Постановка задачи



Ограничение на вход:

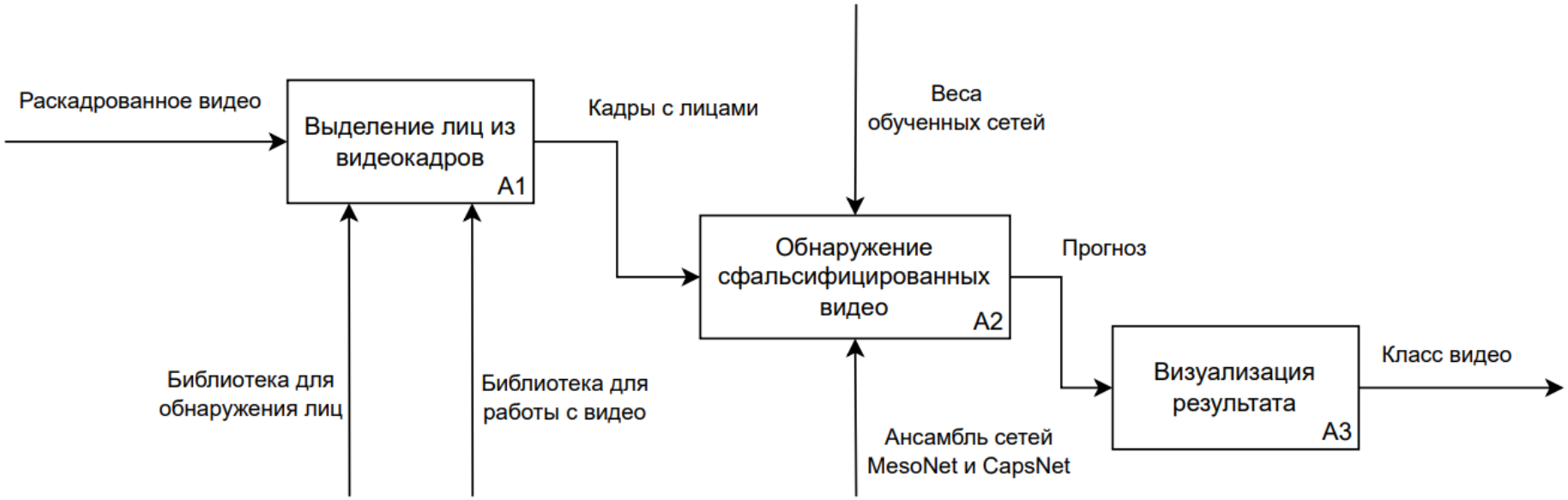
- допустимые видеоформаты — .MP4 и .AVI.

Методы обнаружения сфальсифицированных видео

Метод обнаружения	Зависимость видео от разного качества	Зависимость видео от визуальных дефектов
Реккурентная сеть, выявляющая моргание	+	+
Сверточная сеть, выявляющая частоту сердечных сокращений	+	+
SVM для оценки лицевых ориентиров	+	+
Сверточная сеть MesoNet	-	-
Капсульная сеть	-	-

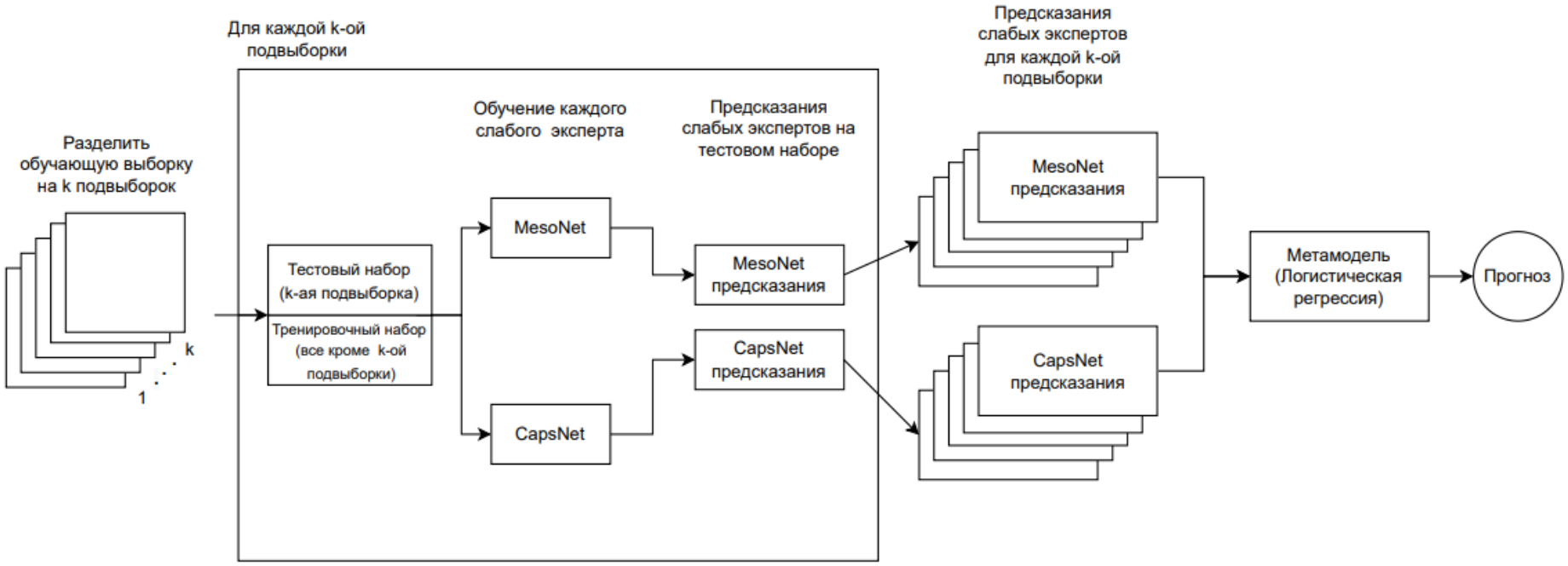
Таким образом, предлагается разработать и реализовать ансамбль сетей MesoNet и CapsNet на основе слабых экспертов. Так как данные модели являются гетерогенными, то при проектировании ансамбля необходимо следовать подходу стекинга.

Функциональная схема метода

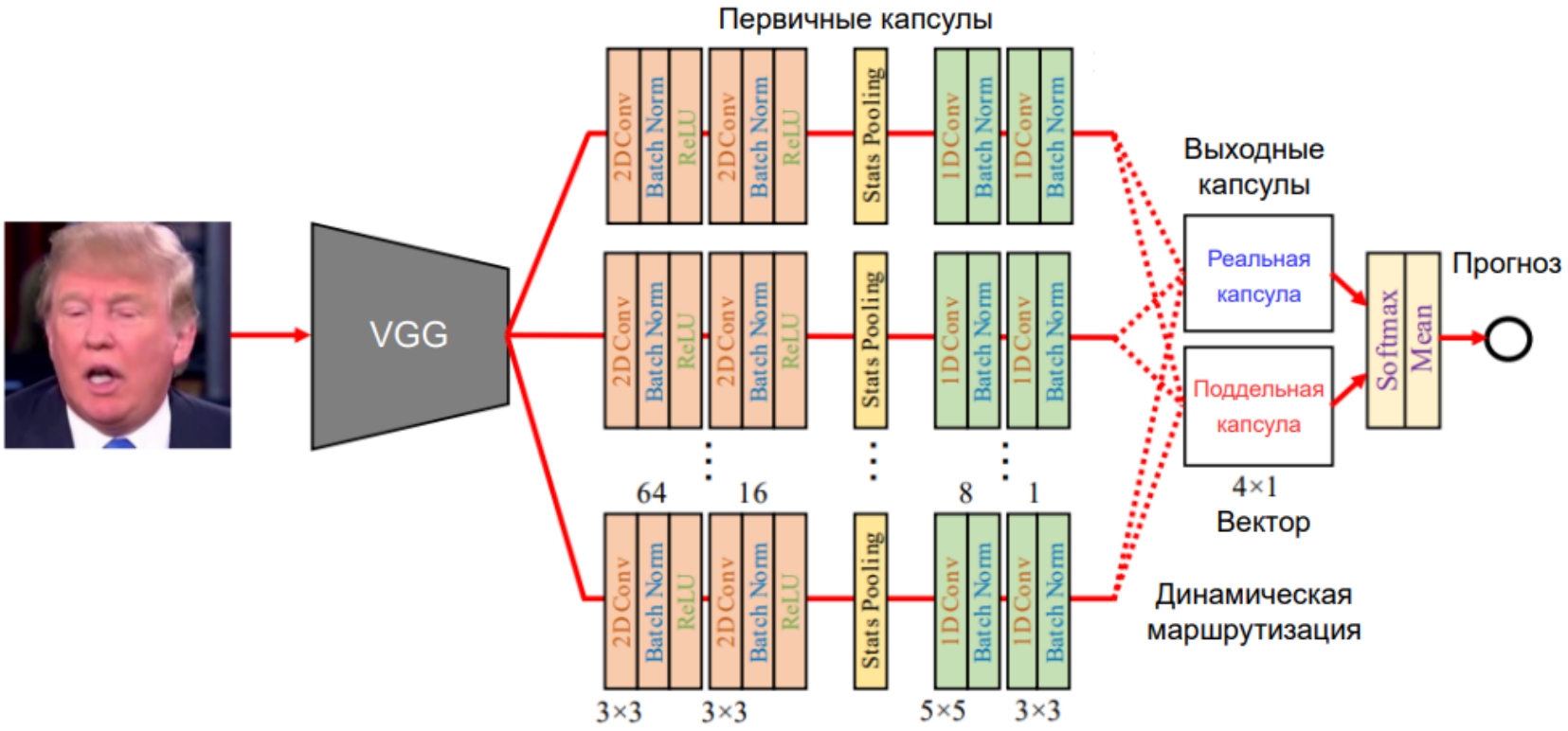


Структура ансамбля нейросетей

Построение ансамбля CapsNet и MesoNet осуществляется по методу стекинга.



Структура капсульной сети



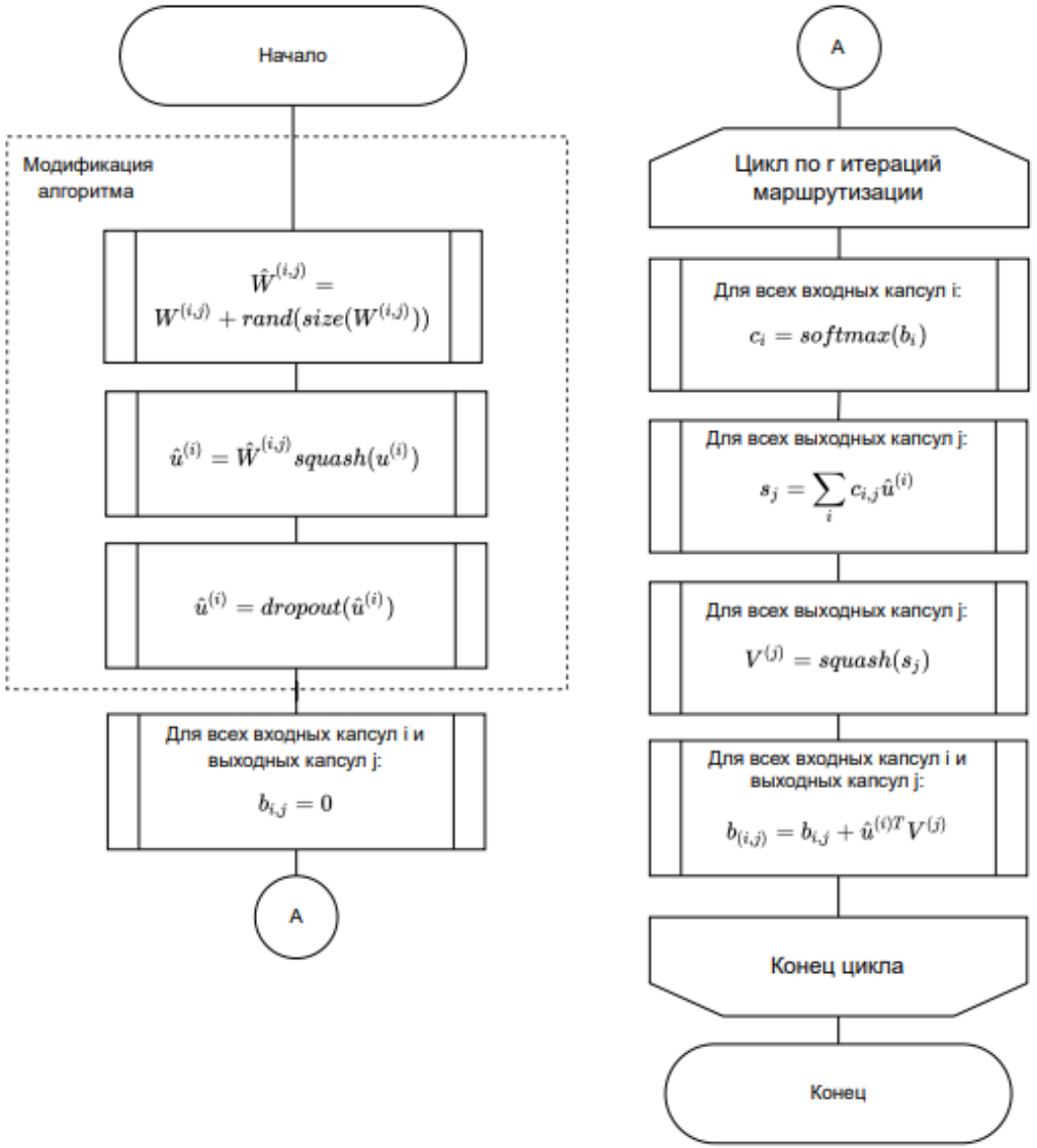
CapsNet включает в себя десять первичных капсул, две выходные капсулы (настоящая и поддельная).

Модифицированный алгоритм динамической маршрутизации

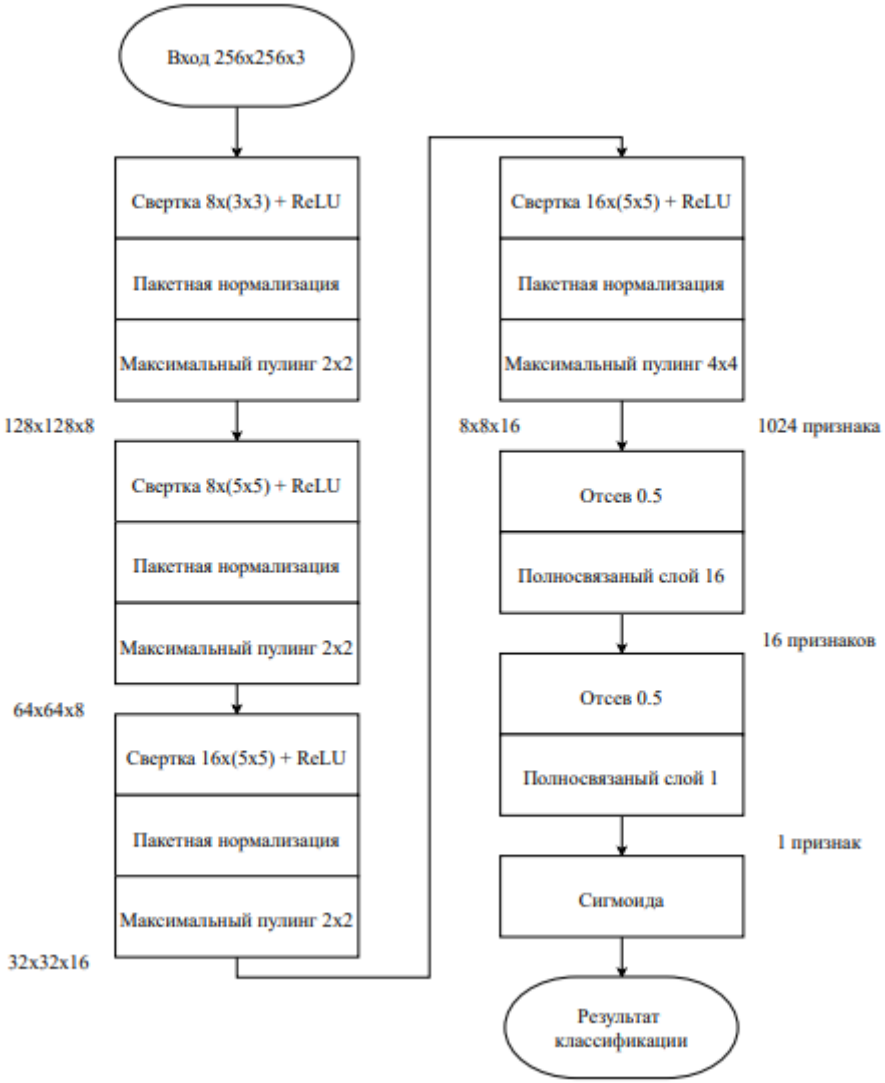
На вход алгоритма подается:

- $u^{(i)}$ — первичная капсула;
- $W^{(i,j)}$ — матрица, используемая для маршрутизации $u^{(i)}$ в $V^{(j)}$;
- r — количество итераций маршрутизации.

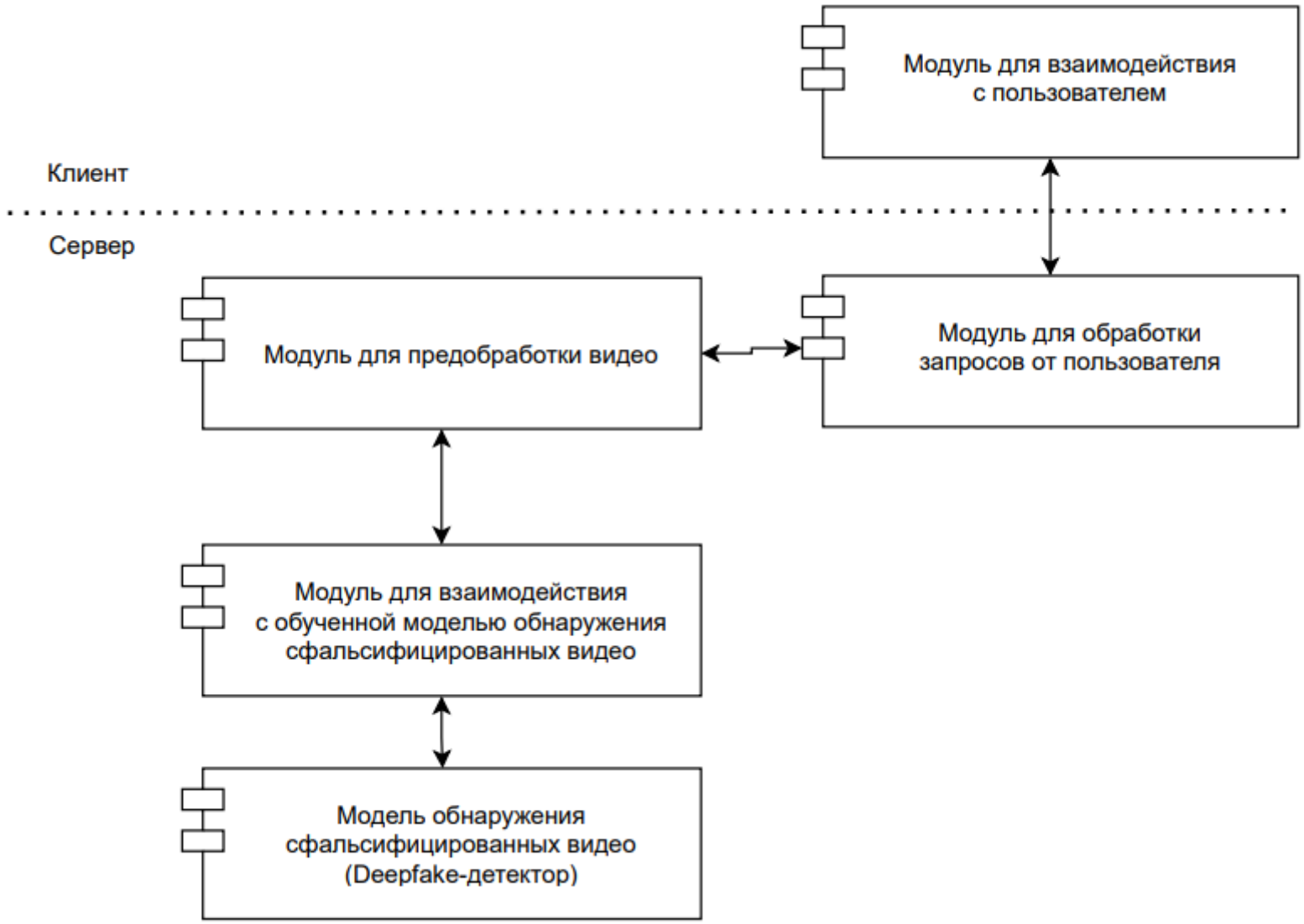
На выходе получается выходная капсула более высокого уровня $V^{(j)}$.



Структура сети MesoNet



Структура ПО



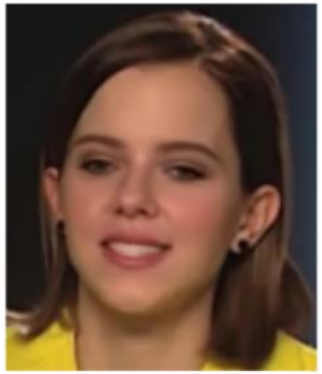
Подготовка данных для обучения

На данный момент существует несколько общедоступных датасетов с сфальсифицированными видео для обучения нейронных сетей:

- The FaceForensics++ (1000 оригинальных и несколько тысяч поддельных видео, размер — 2ТБ);
- DFDC (более 5000 поддельных видео, размер — 471.84 ГБ);
- Celeb-DF (590 оригинальных и 5639 поддельных видео, размер — 9,26 ГБ).

FaceForensics++

DFDC

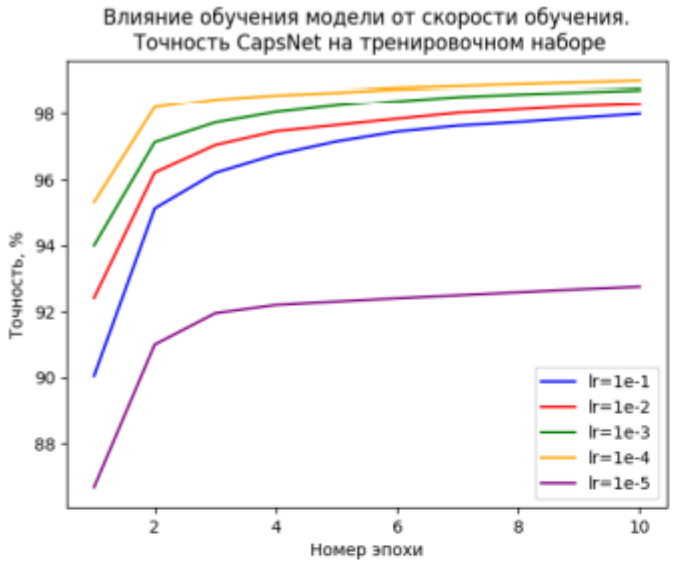


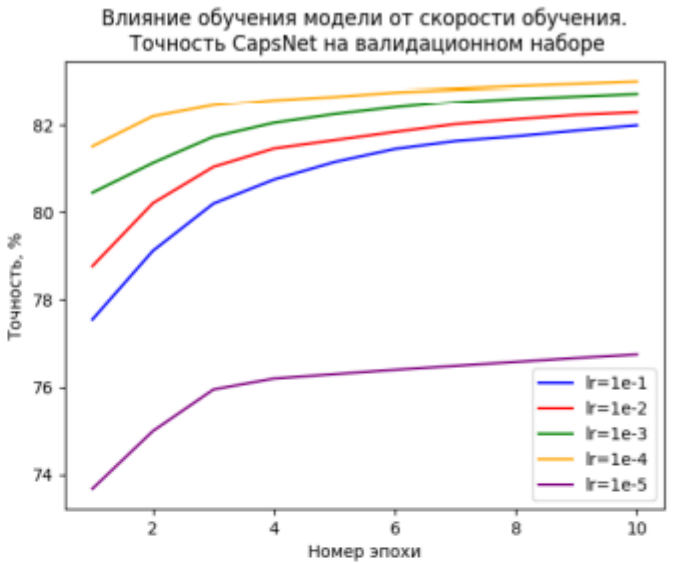
Celeb-DF

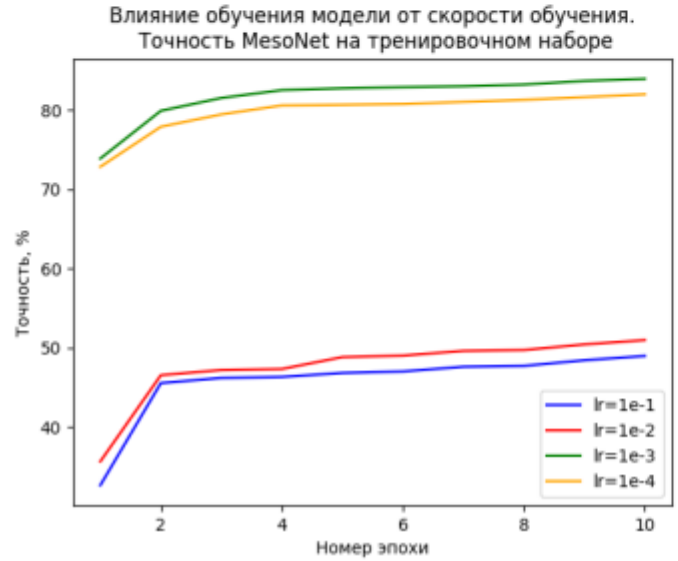
Был составлен собственный сбалансированный датасет из доступных, обладающий следующими характеристиками:

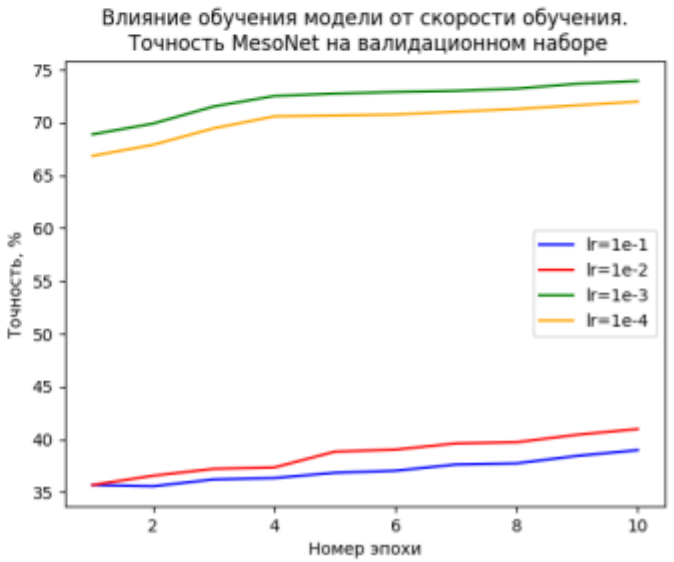
- состоит из 3075 реальных и 3075 поддельных видео;
- общее число кадров — 2 316 492;
- размер датасета — 20 ГБ.

Исследование скорости обучения

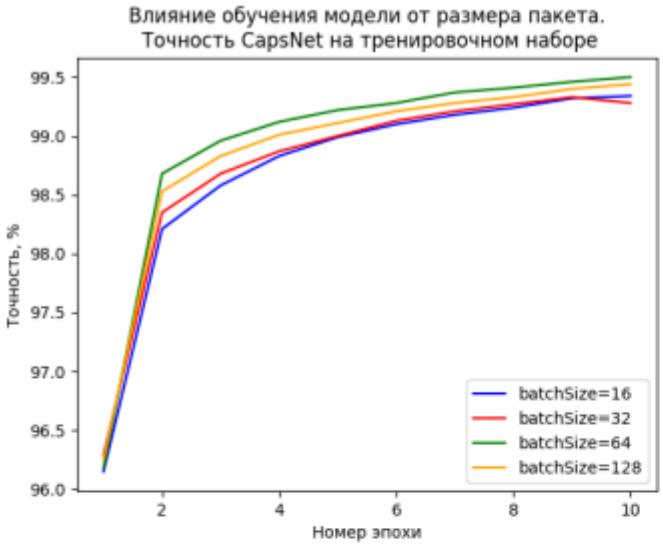


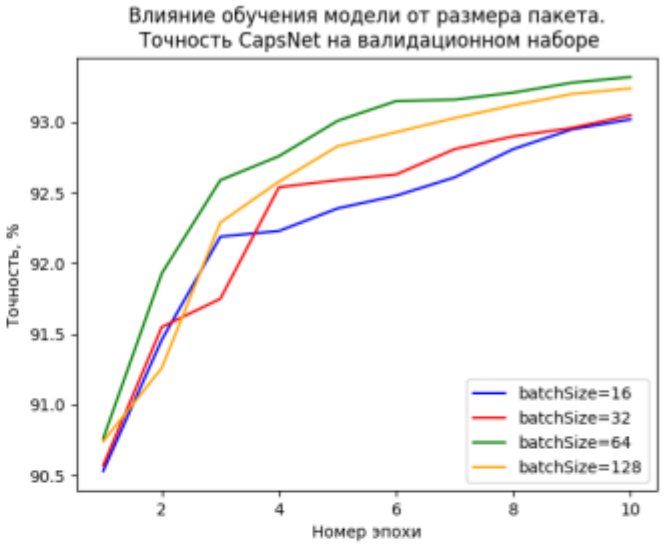


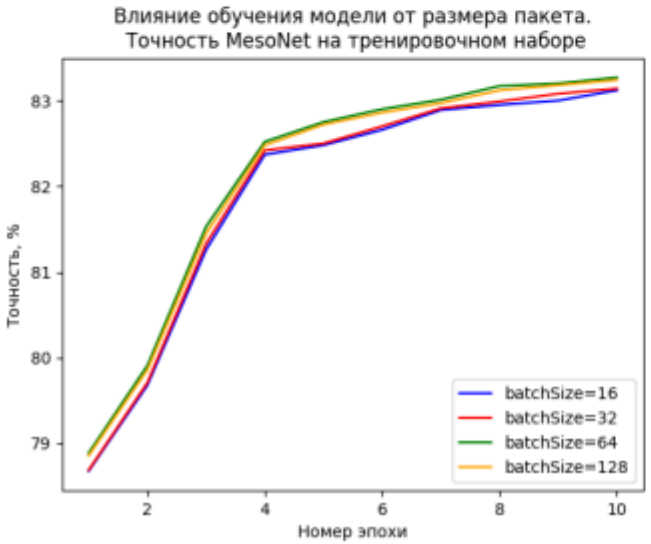


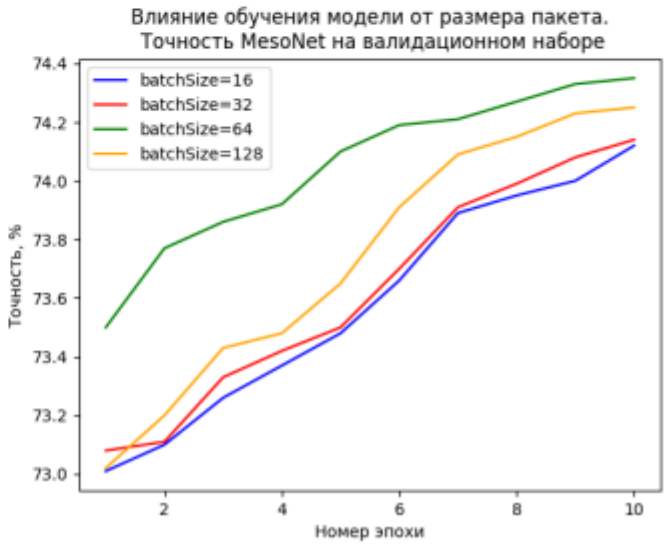


Исследование размера пакета

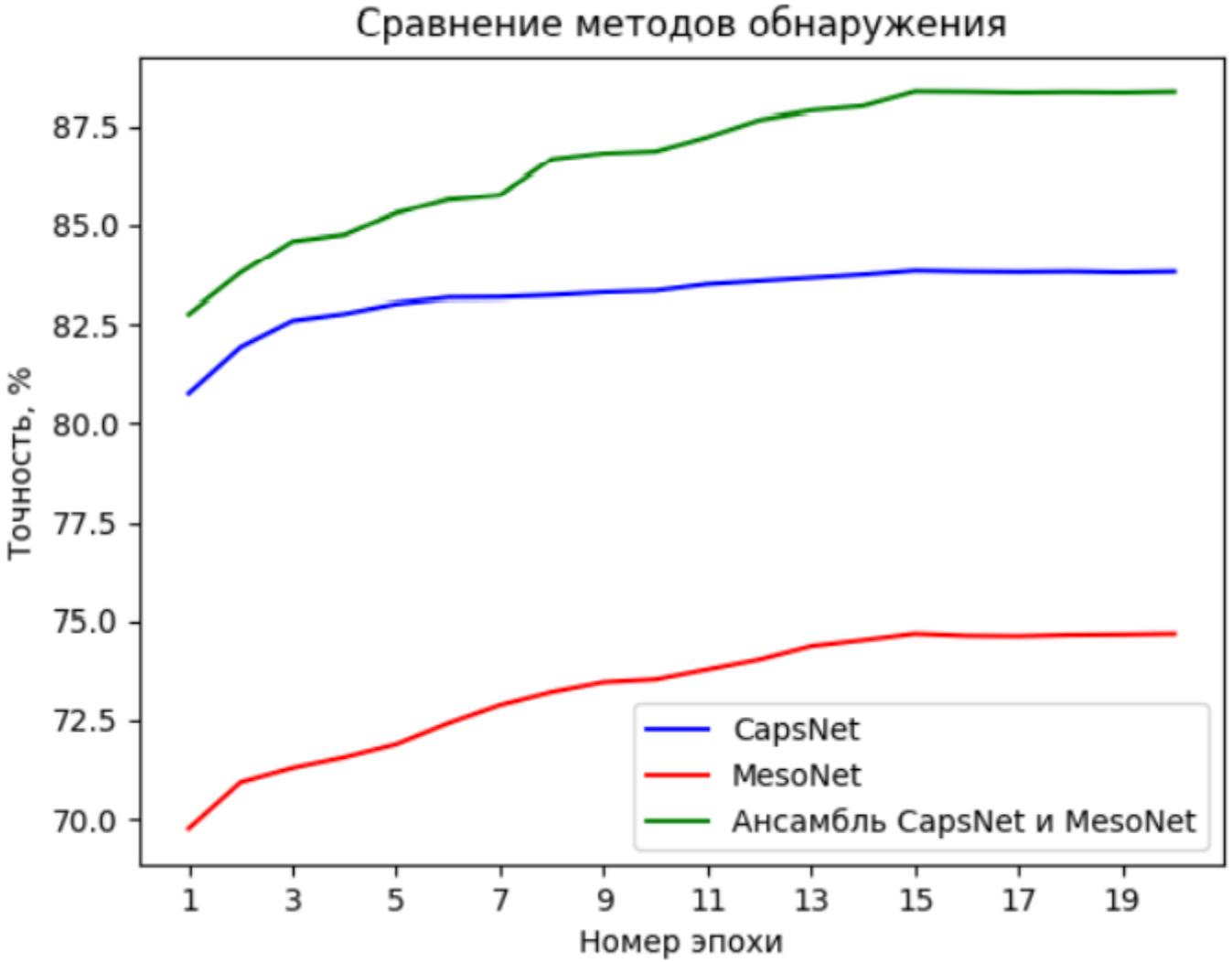








Сравнение реализованных методов обнаружения



Заключение

В рамках выпускной квалификационной работы был разработан метод обнаружения сфальсифицированных видео на основе ансамблевой модели обучения сетей CapsNet и MesoNet, использующей подход стекинга.

Были решены все поставленные задачи:

- проанализирована предметная область и проведено сравнение существующих решений;
- проведен обзор существующих подходов обнаружения поддельных видео с помощью нейронных сетей;
- в результате полученных во время анализа данных разработан метод обнаружения сфальсифицированных видео на основе нейронных сетей;
- реализован разработанный метод в программном продукте;
- проведено исследование работоспособности реализованного метода обнаружения.

Дальнейшее развитие

Разработанная система имеет перспективу дальнейшего развития и улучшения:

- увеличение количества данных обучающей выборки для повышения показателей точности;
- систему можно сделать универсальной путем расширения метода обнаружения сфальсифицированных видео без лиц;
- возможны улучшения с точки зрения добавления дополнительной функциональности и оформления программного интерфейса.