

|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное  учреждение высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

Институт комплексной безопасности и специального приборостроения

**Отчет** по лабораторной работе №2

**по дисциплине:** «Анализ защищенности систем искусственного интеллекта»

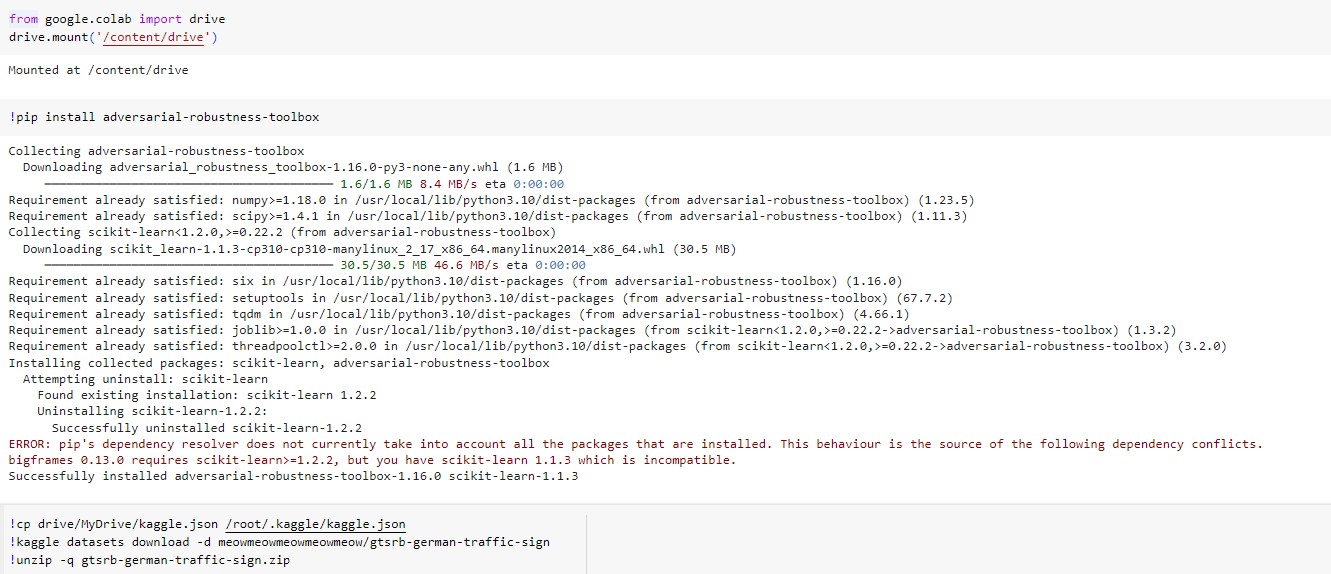
**Выполнил:**

Студент группы ББМО-01-22 ФИО: Карпова Н.Ю.

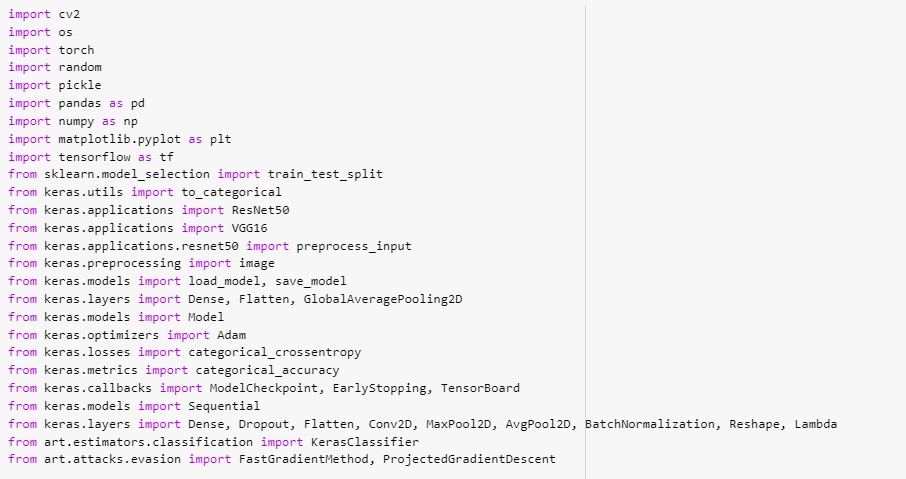
**Москва 2023**

Задание 1.

1. Устанавливаем требуемые инструменты.



1. Производим импорт библиотек.



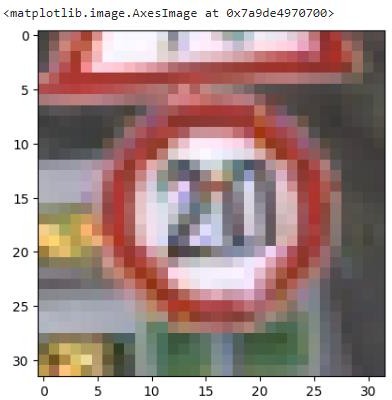
1. Извлечем картинки для создания тренировочной выборки.



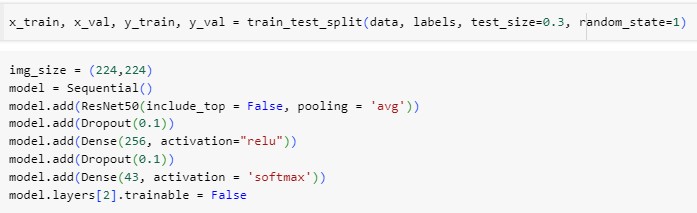
1. Загружаем dataset «CIFAR-10» и отредактируем его.



1. Результат на выходе.

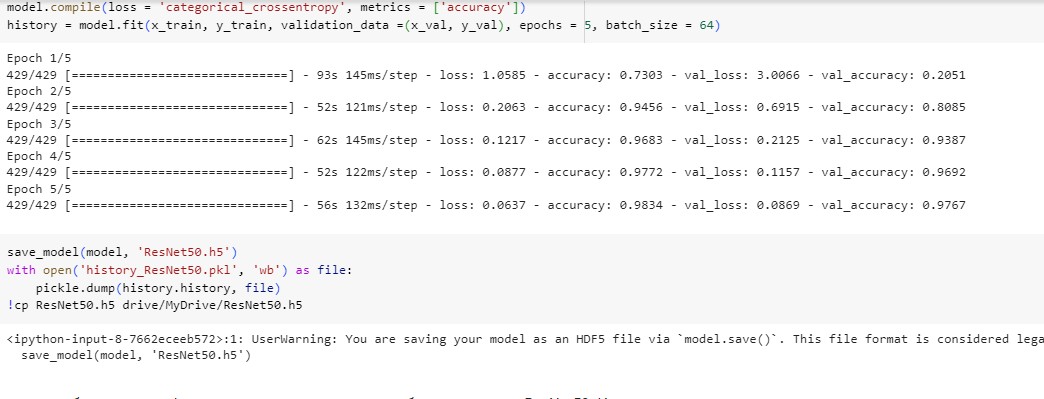


1. Производим выходные слои модели, для осуществления классификации изображений.

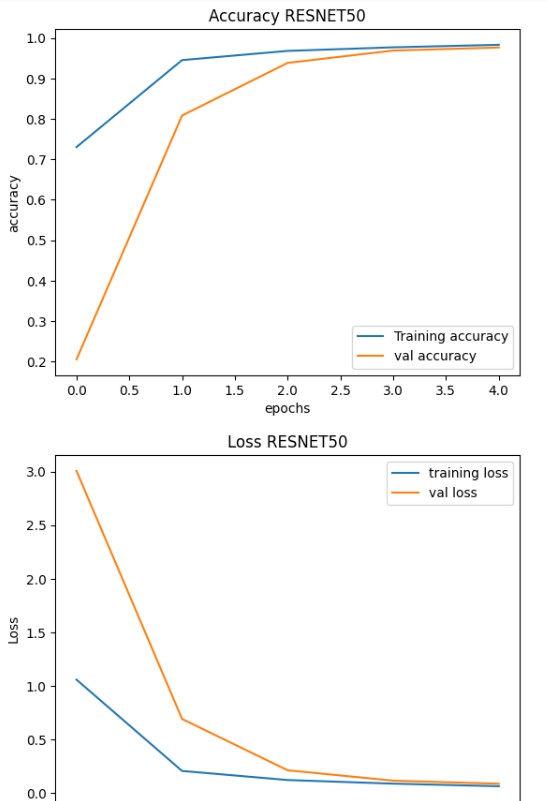


1. Для валидации возьмем 30% процентов тренировочного

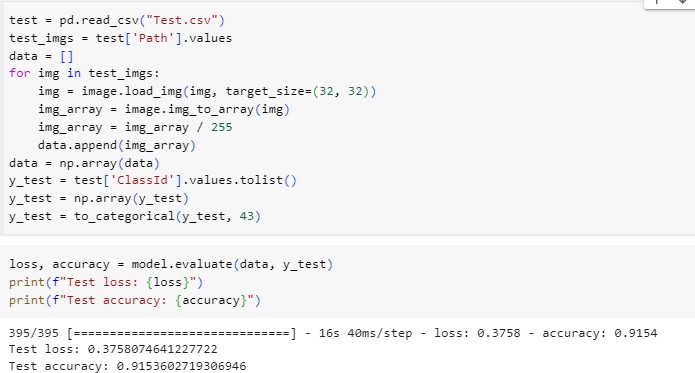
набора.



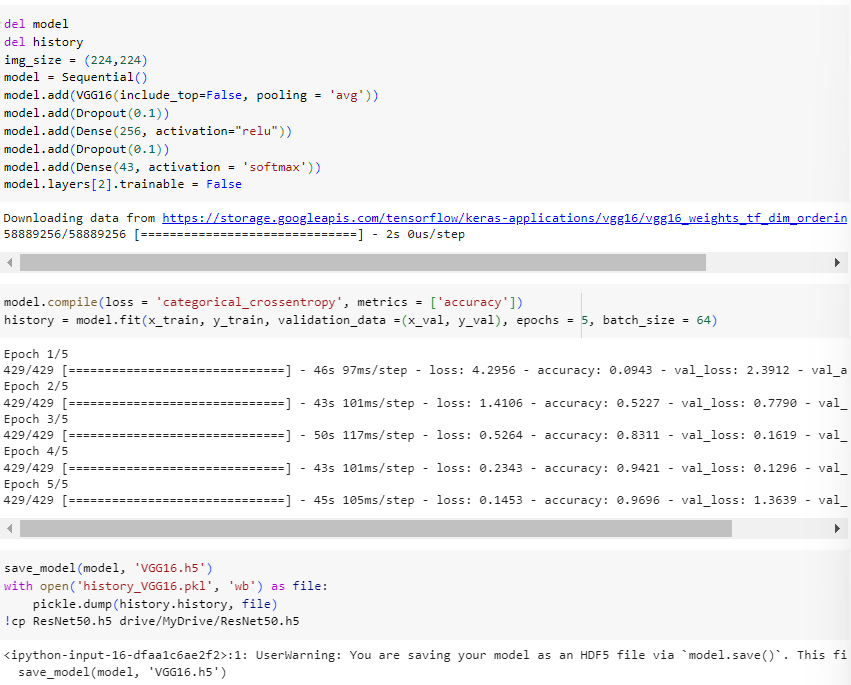
1. Построим графики и посмотрим, что будет на выходе.

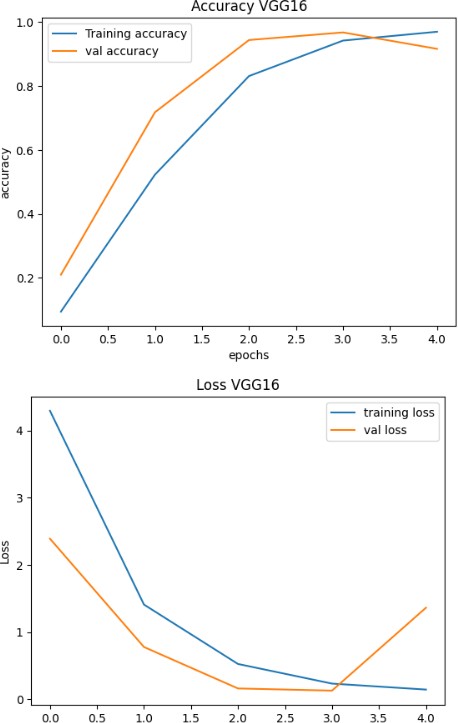


1. Сформируем тестовую выборку и оценим

точность модели.

1. Используем готовый набор для тренировки.



1. Сделаем отображение графиков точности и потерь для модели VGG16.

Задание 2.

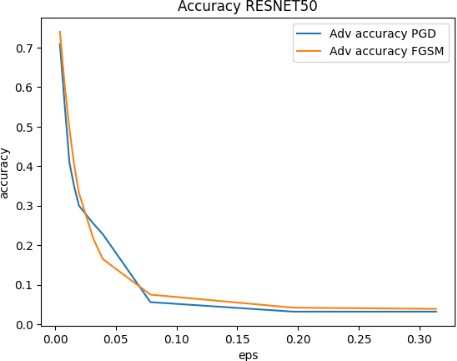
* 1. В ходе данной работы мы должны

взаимодействовать с моделью ResNet50 FGGM. Определим eps и выведем

изображения.

|  |  |
| --- | --- |
|  |  |

* 1. Теперь попробуем использовать атаку PGD для различных вариантов eps и изобразим изображения до и после атаки.



* 1. Приступим к созданию модели для использования атаки VGG16 FGSM и

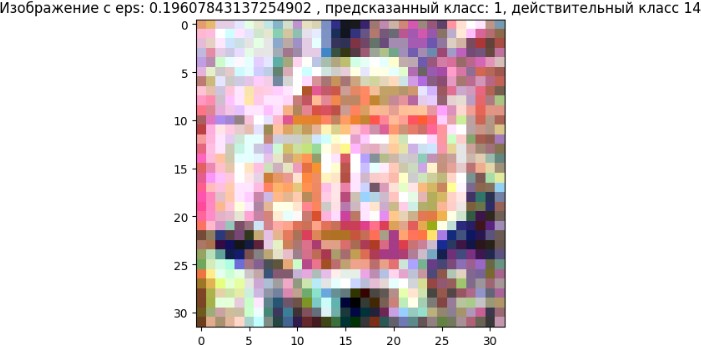
посмотрим изображения до и после атаки.

|  |  |
| --- | --- |
|  |  |

Задание 3.

1. Создадим модель для атаки Targeted FGSM Attack и отобразим модель атаки.





**Вывод**

В ходе выполнения данной лабораторной работы получен опыт работы с инструментами атак на модели машинного обучения. Были проведены некие эксперименты с атакой на модели машинного обучения.