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

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по лабораторной работе №2

по дисциплине: «Анализ защищенности систем искусственного интеллекта»

**Выполнил**:

Студент группы ББМО-02-22

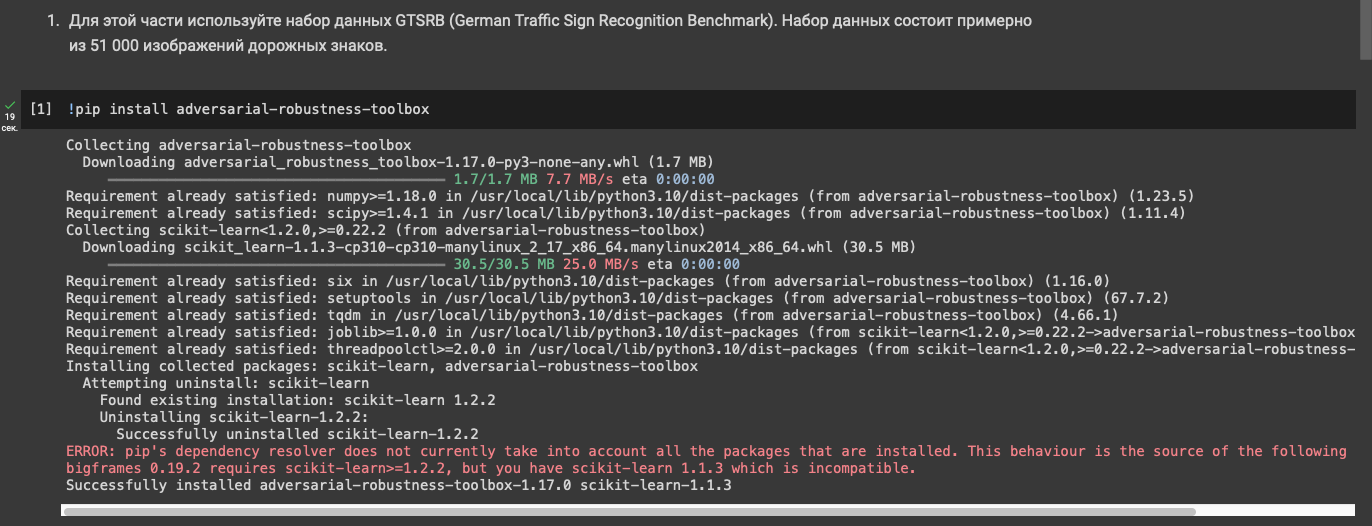
Филиппов Леонид Алексеевич

**Проверил**:

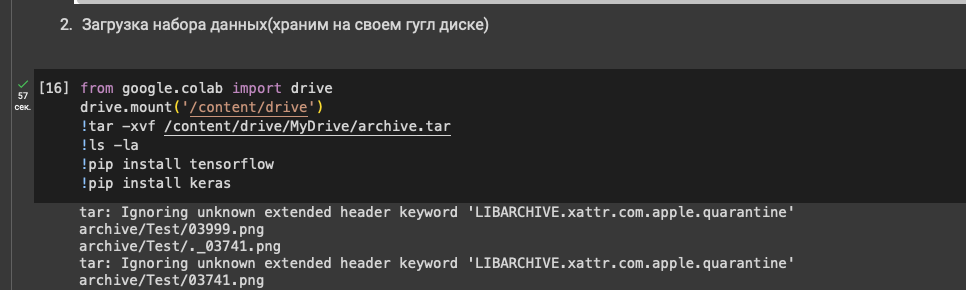
Спирин Андрей Андреевич

Москва 2024

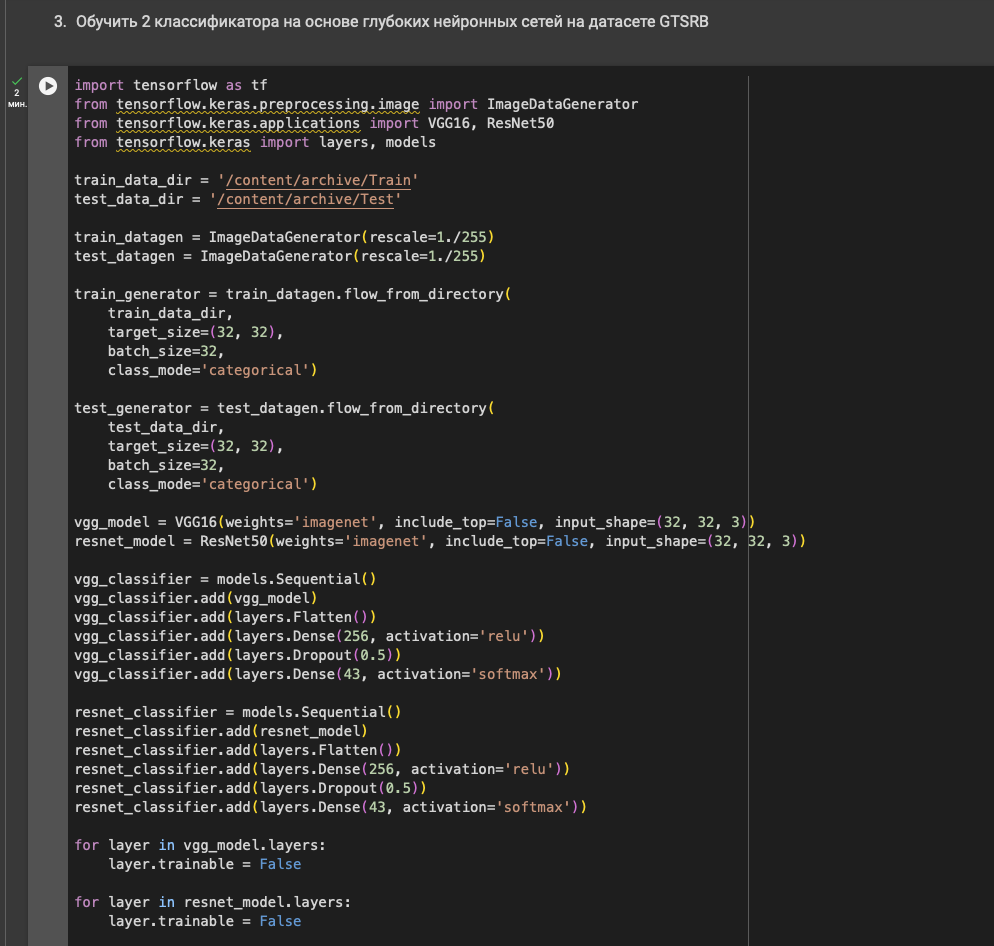
1. Загрузка основной библиотеки ART

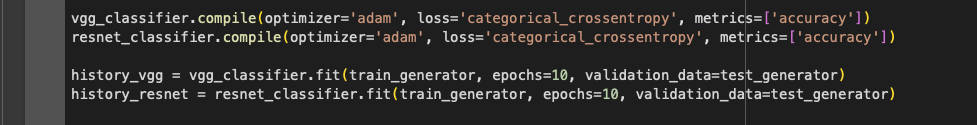
****

1. Загрузка набора данных с диска

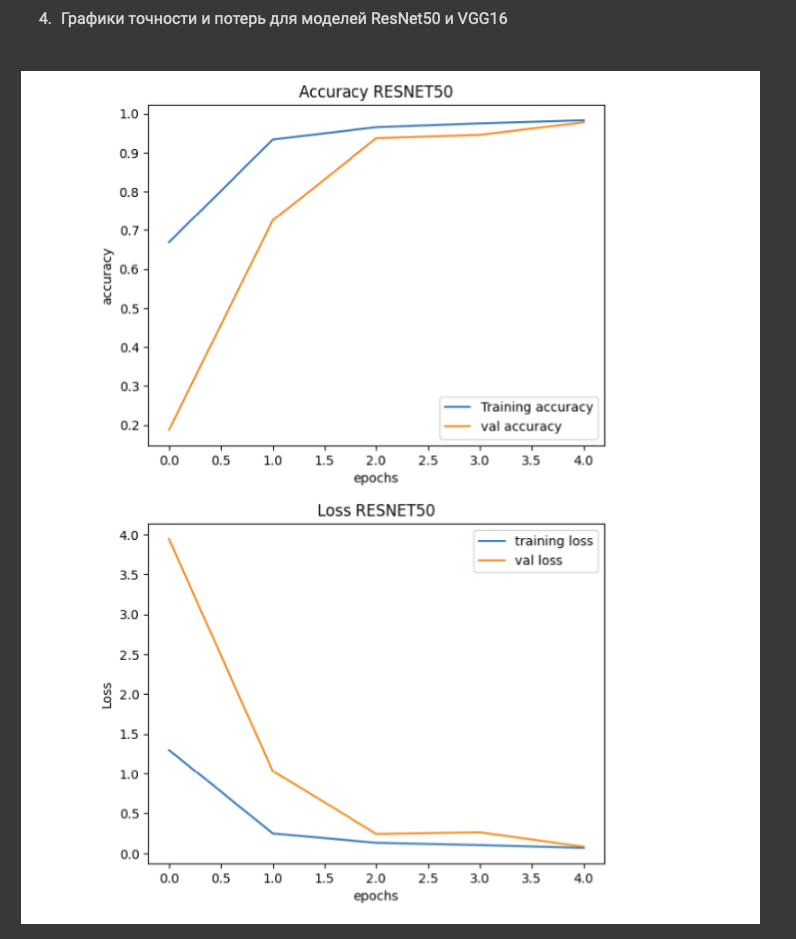
****

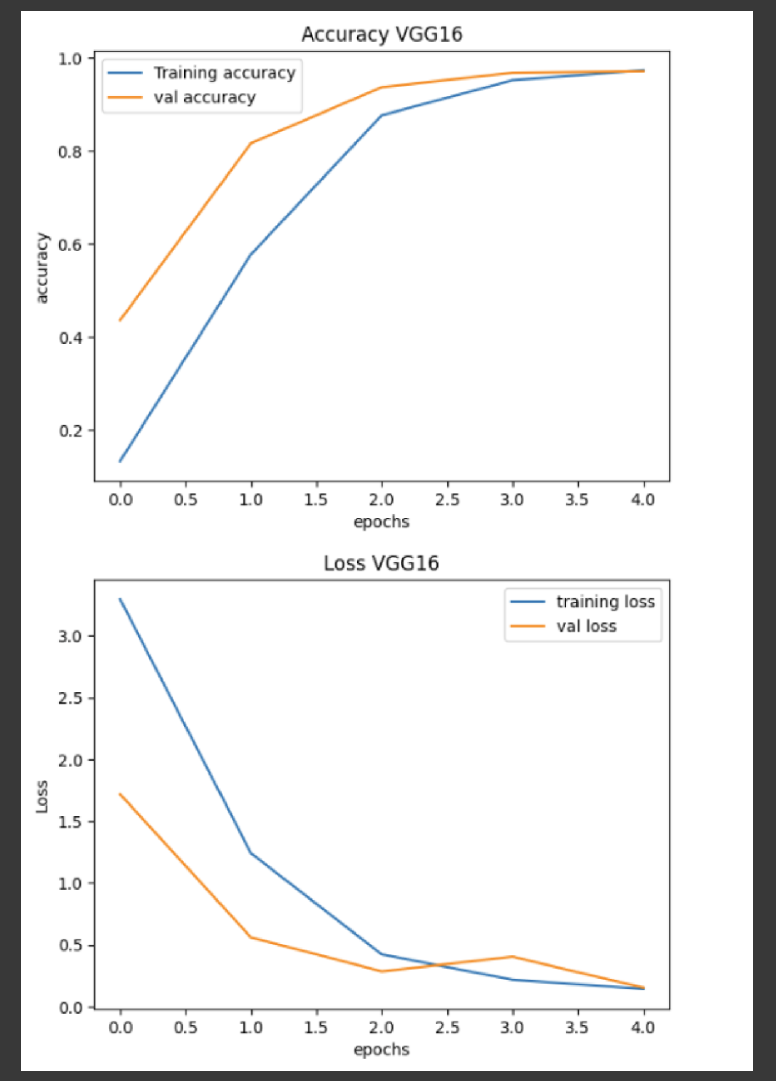
1. Обучение двух классификаторов на основе глубоких нейронных сетей на датасете GTSRB



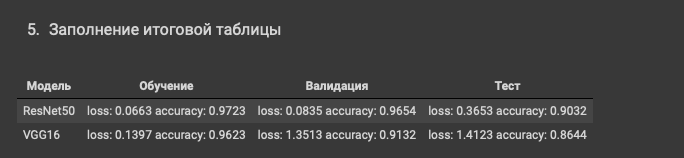


1. Графики точности и потерь для моделей ResNet 50 и VGG16

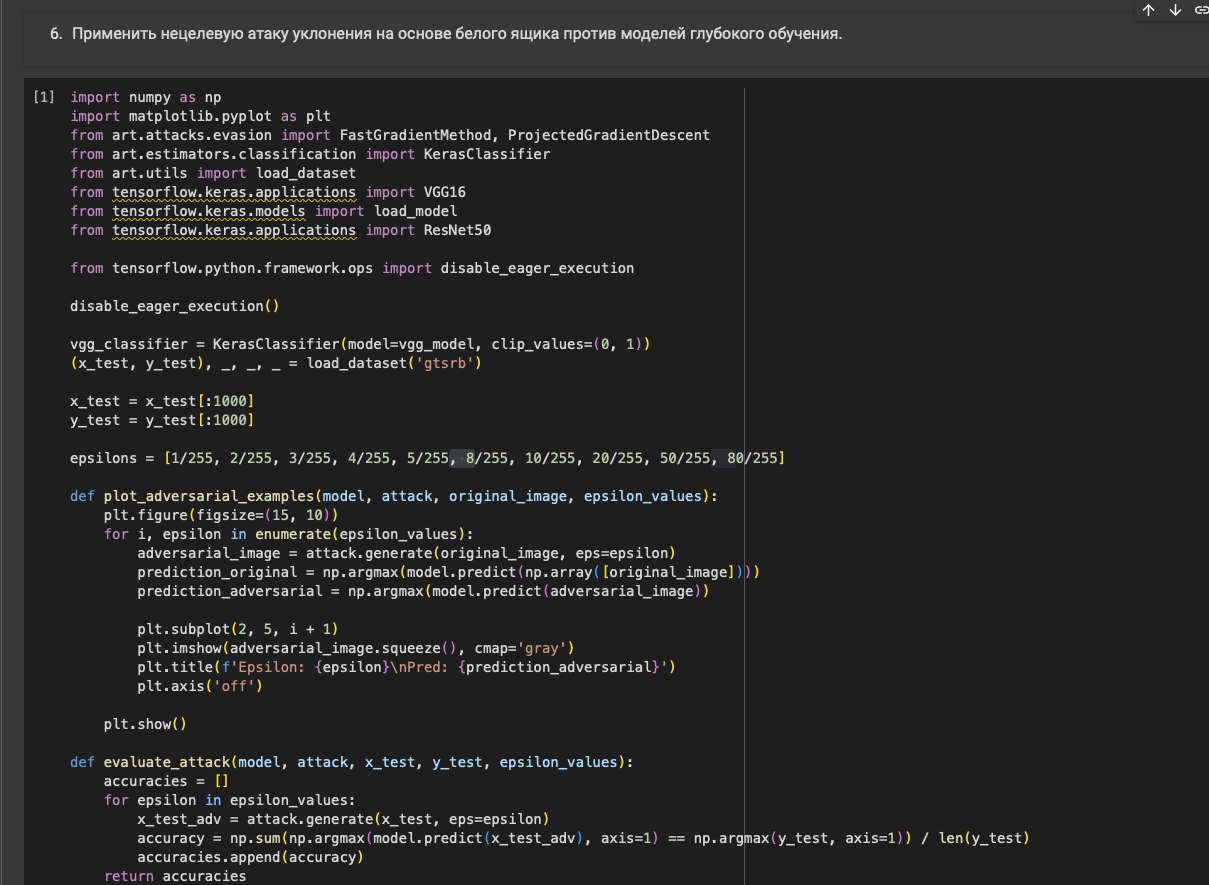


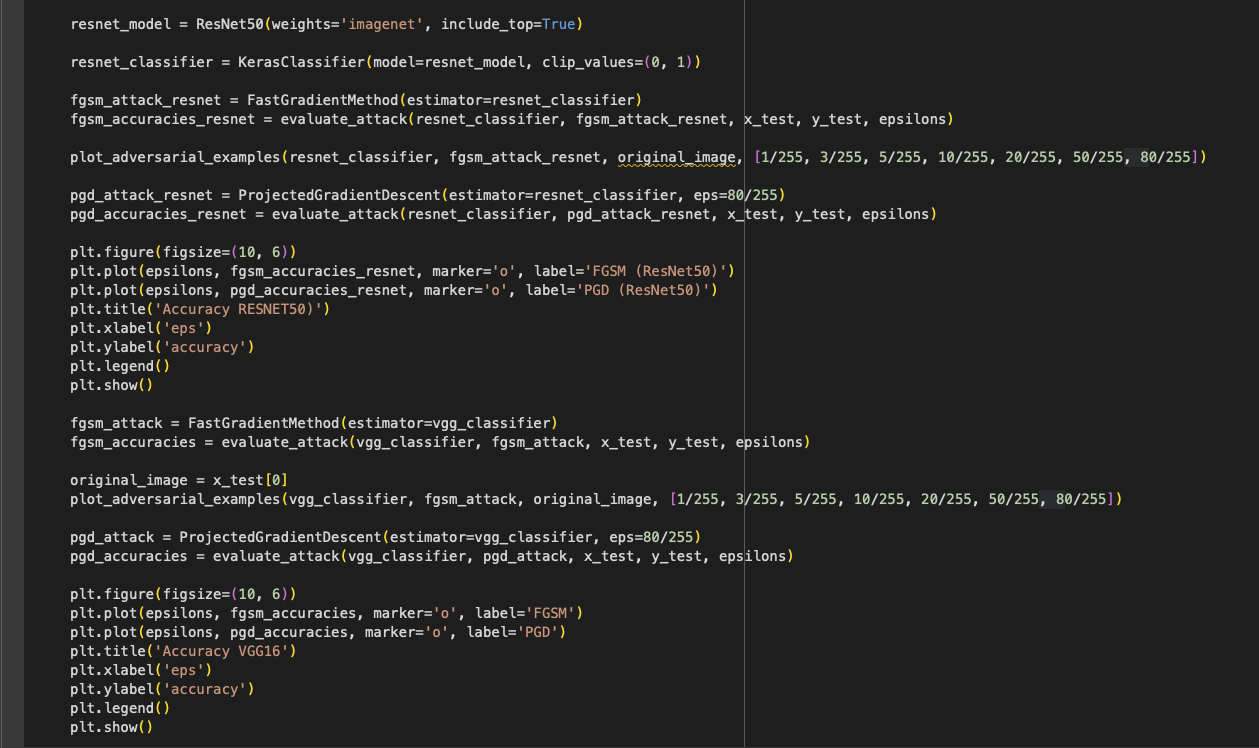


1. Заполнение итоговой таблицы

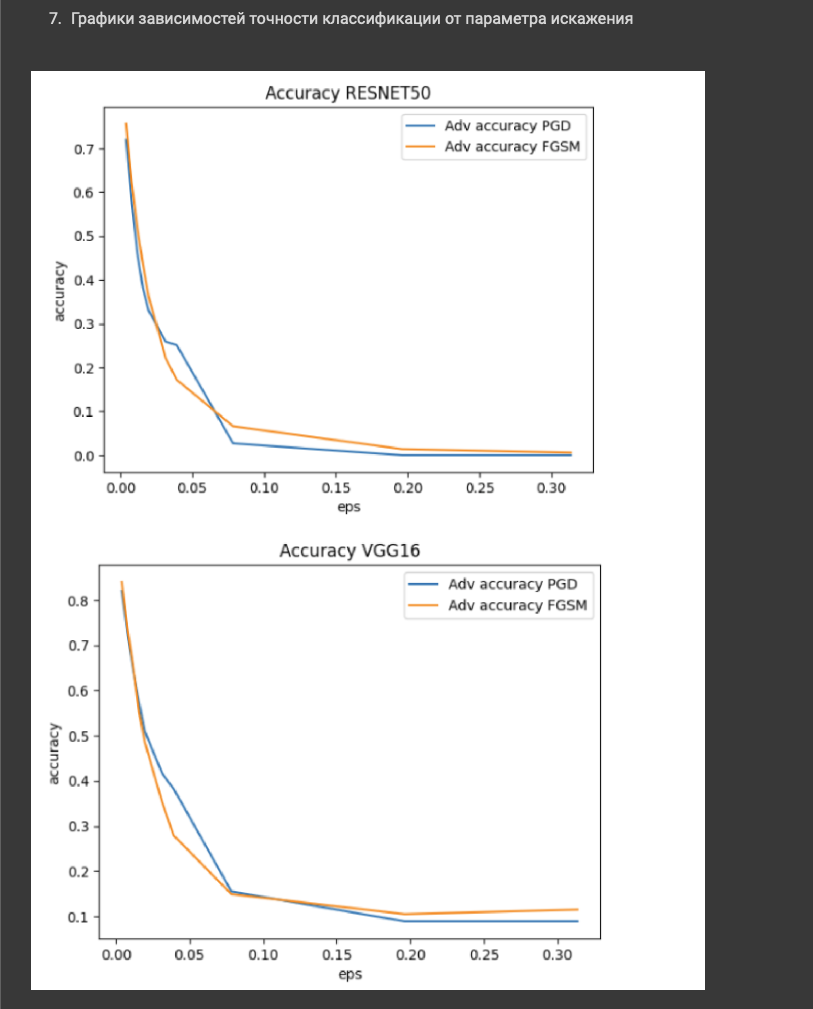


1. Применить нецелевую атаку уклонения на основе белого ящика против моделей глубокого обучения

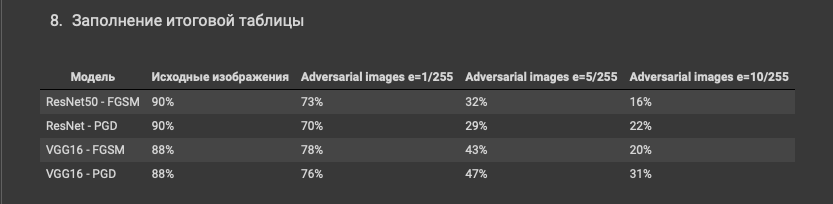




1. Графики зависимостей классификации от параметра искажения

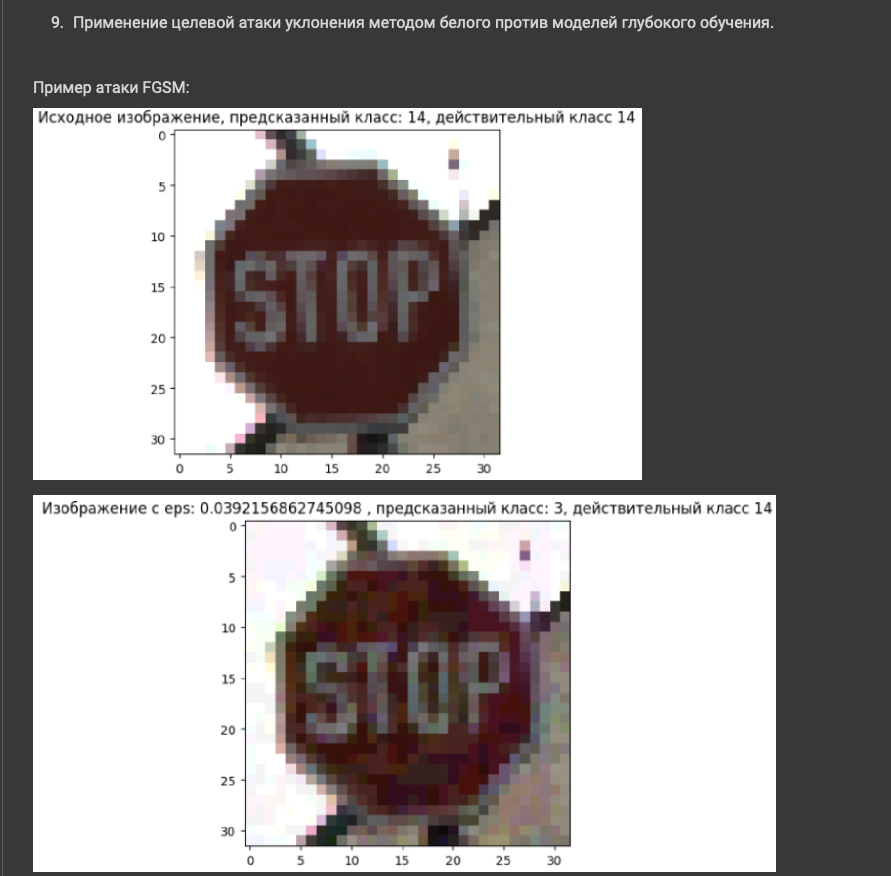


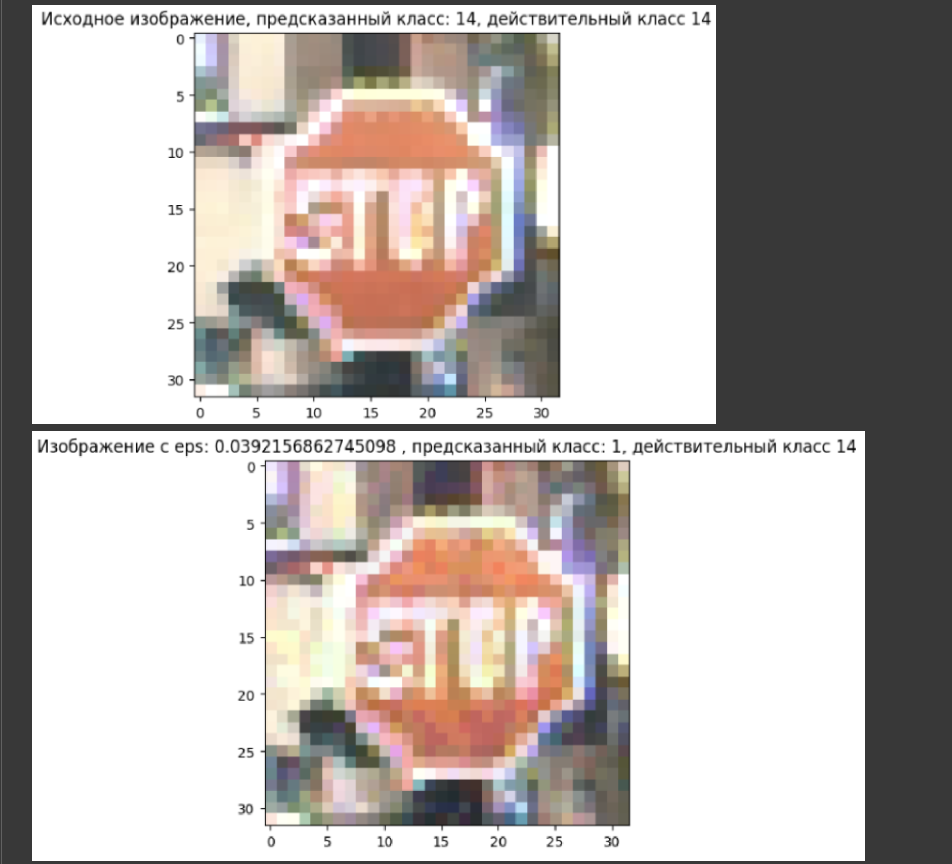
1. Заполнение итоговой таблицы

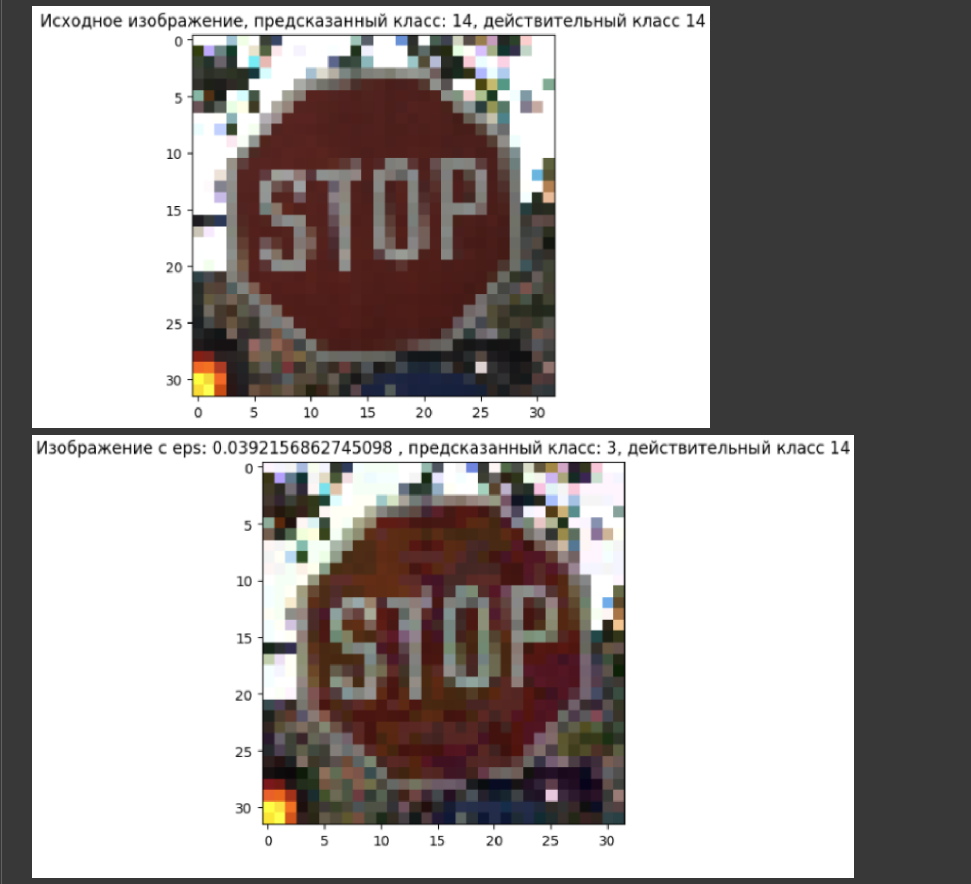


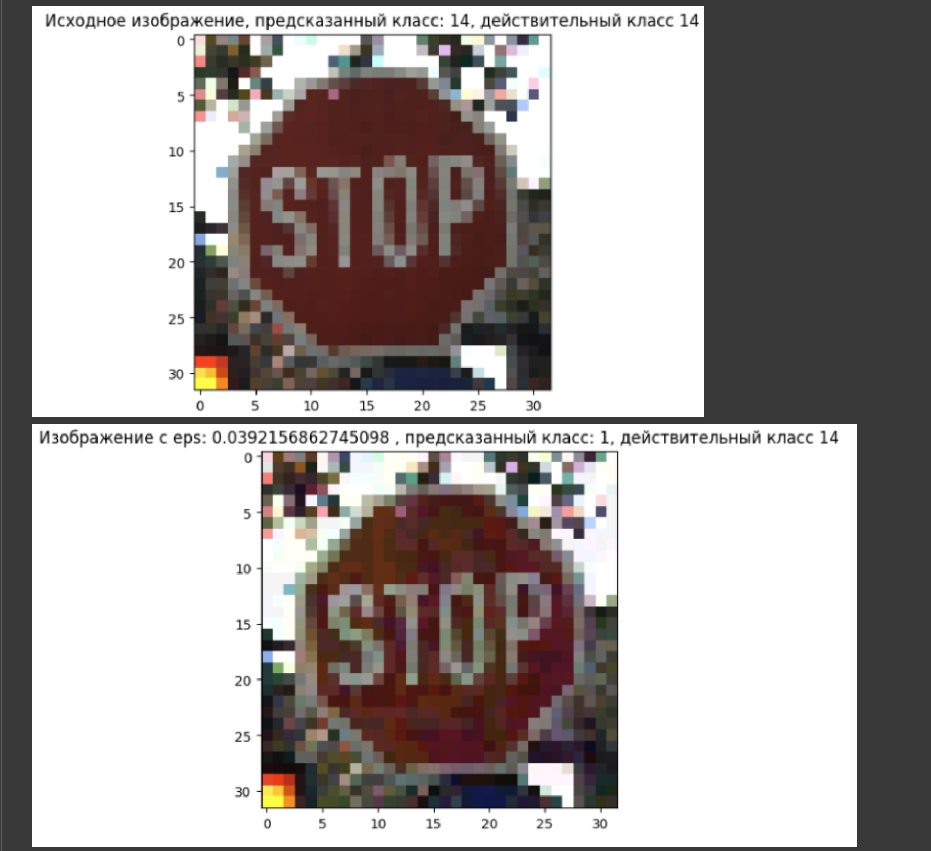
1. Применение целевой атаки уклонения методом белого против моделей глубокого обучения

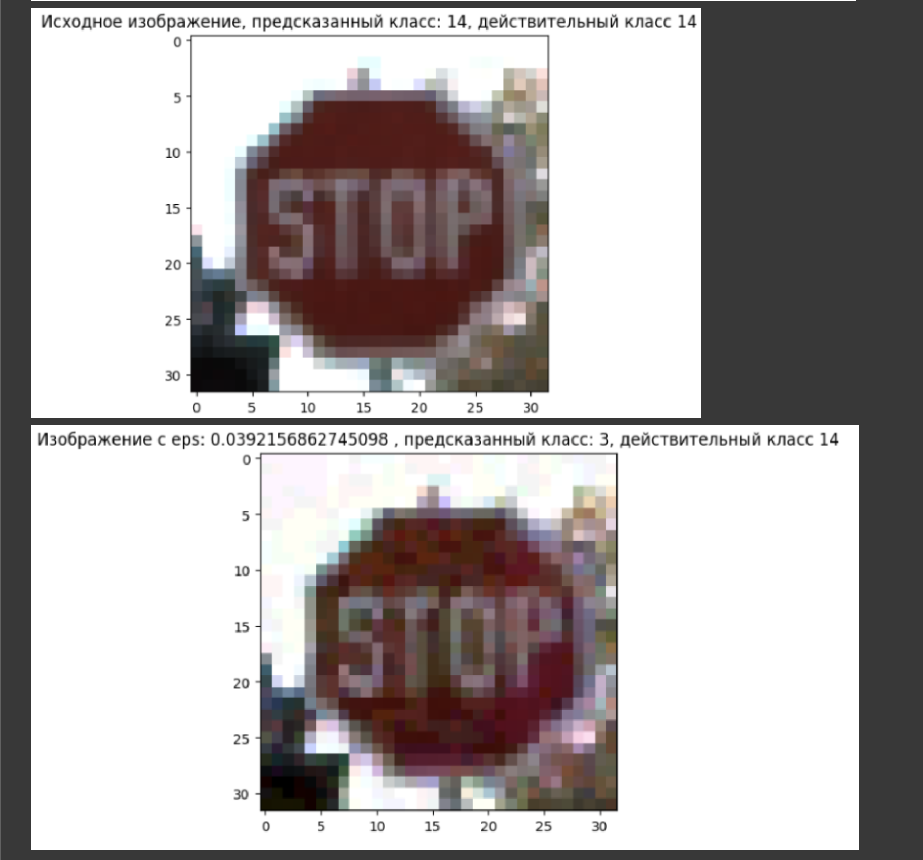
Пример атаки FGSM:



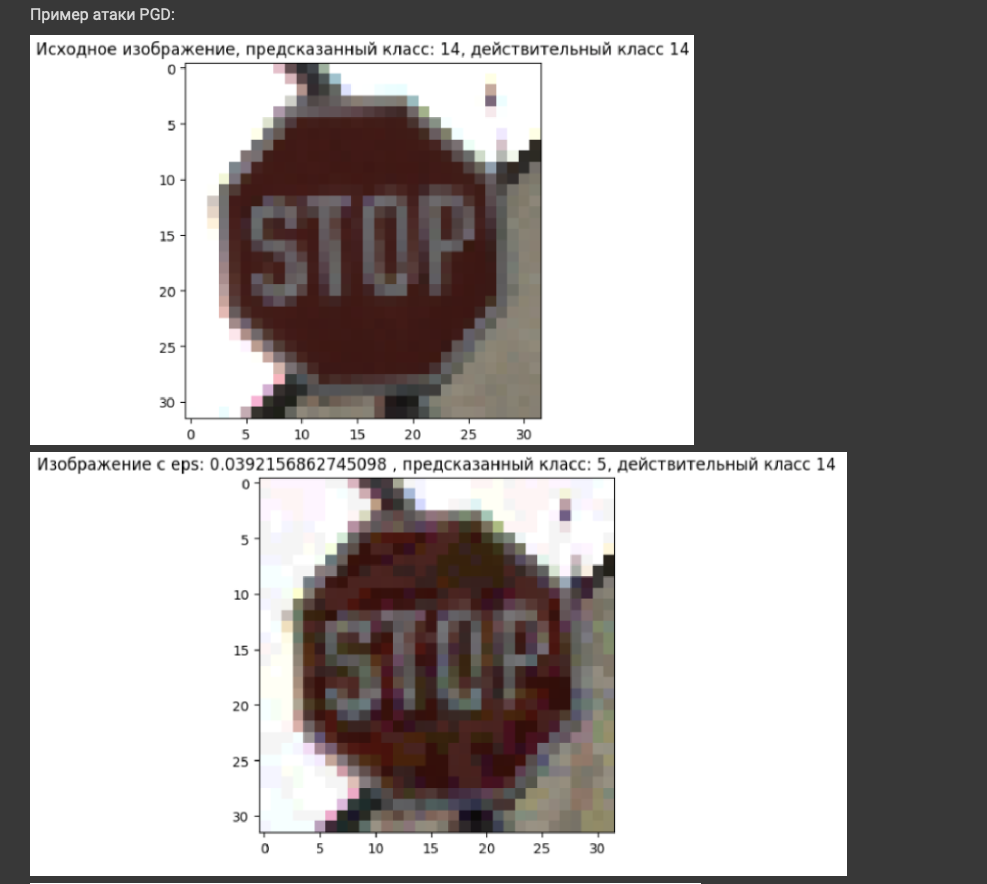


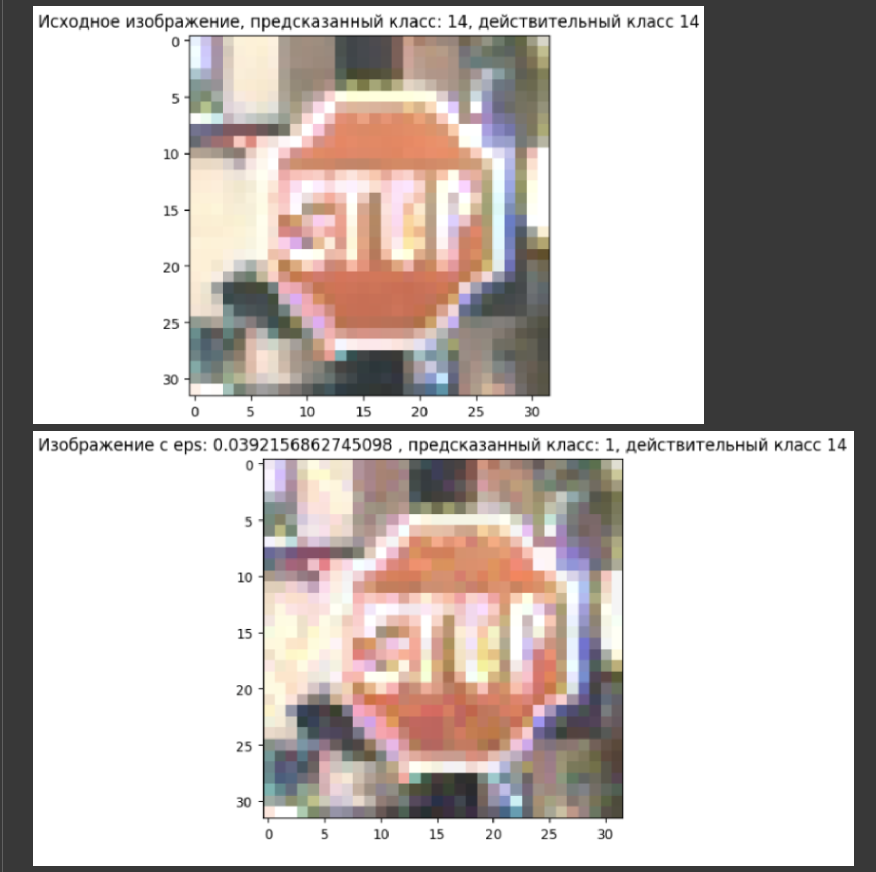


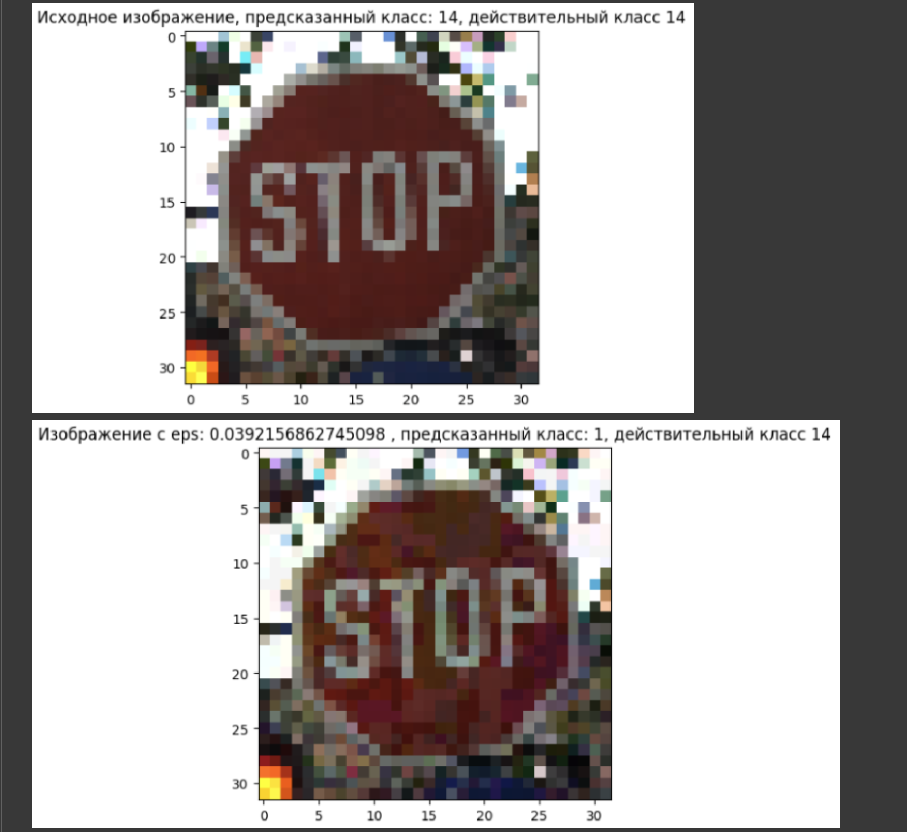


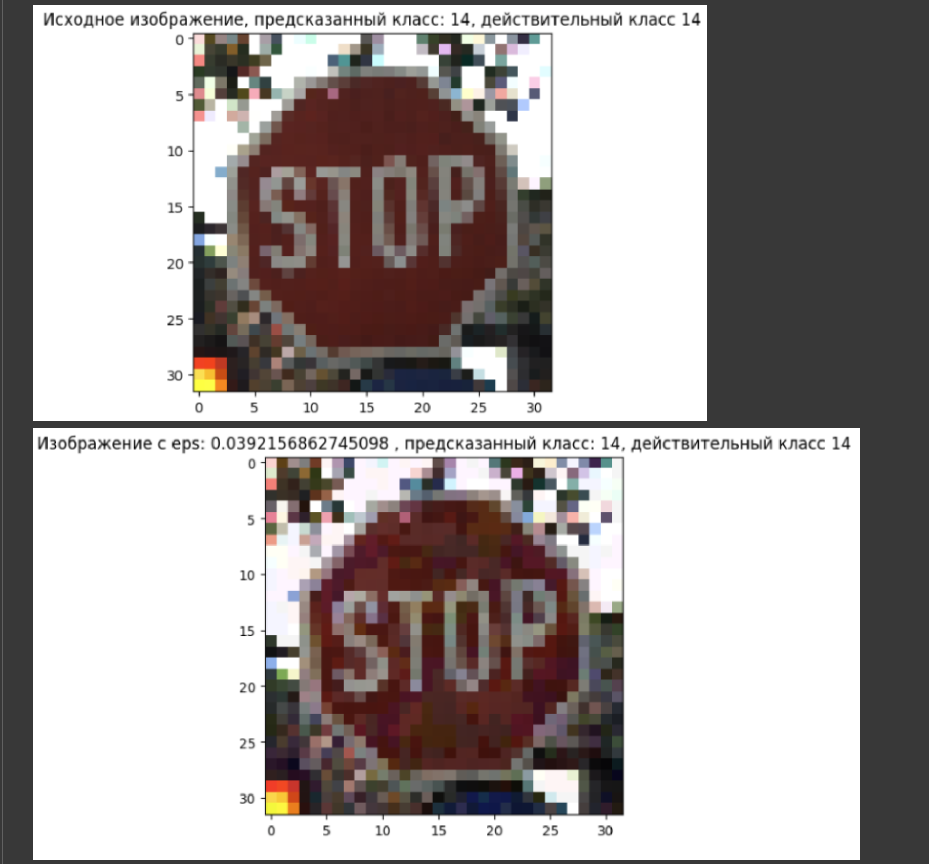


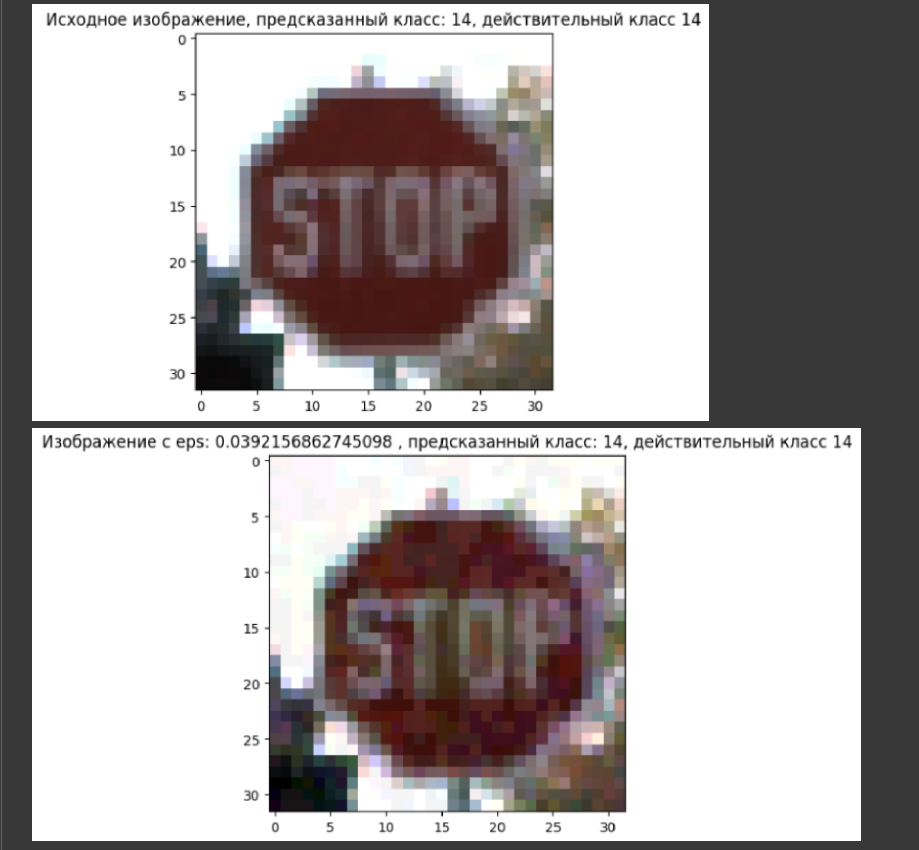
Пример атаки PGD:











1. Заполнение итоговой таблицы

