|  |
| --- |
|  |
| 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 №1

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

**Выполнил:**

Студент группы ББМО-01-22

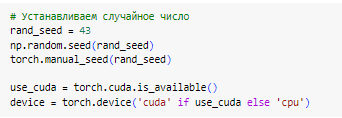
ФИО: Карев Д.П.

**Москва 2023**

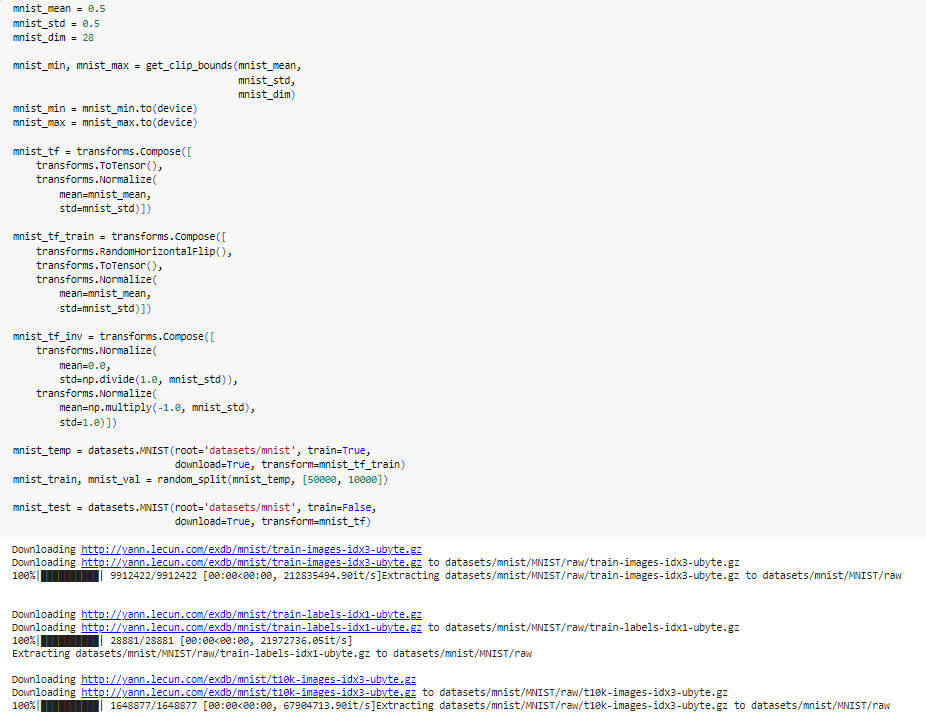
1. Клонируем репозиторий и загружаем нужные библиотеки.



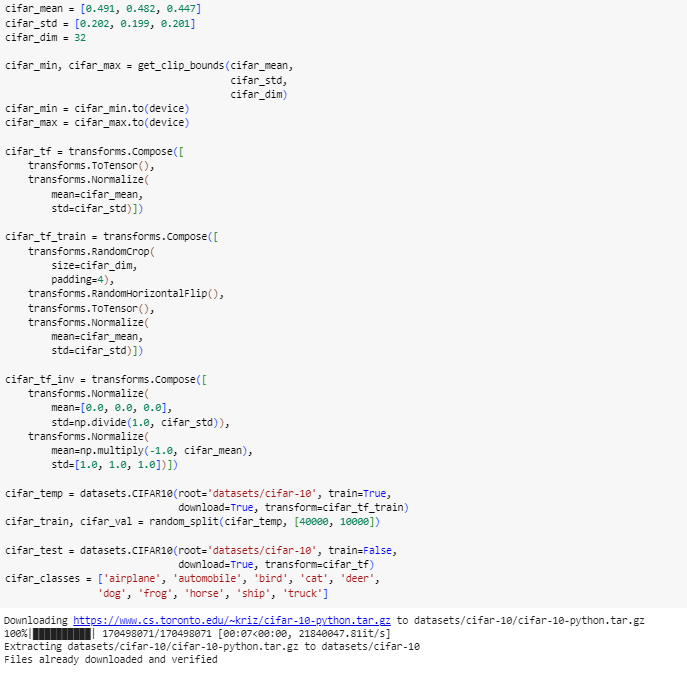
1. Устанавливаем случайное число и выбираем устройство выполнения.



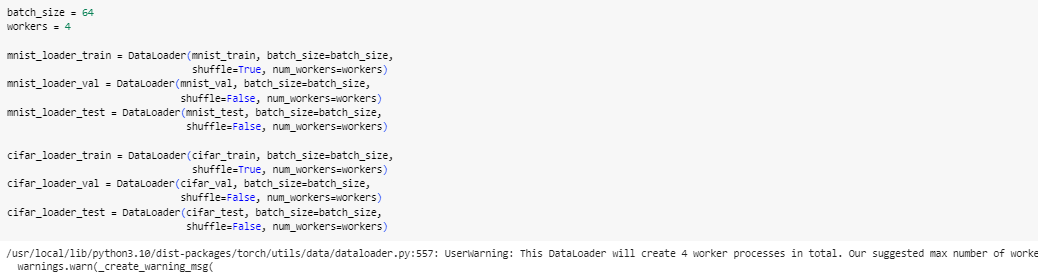
1. Загружаем dataset «MNIST» и отредактируем его.



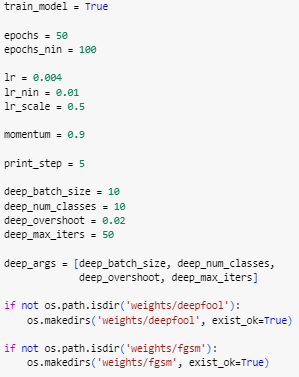
1. Загружаем dataset «CIFAR-10» и отредактируем его.



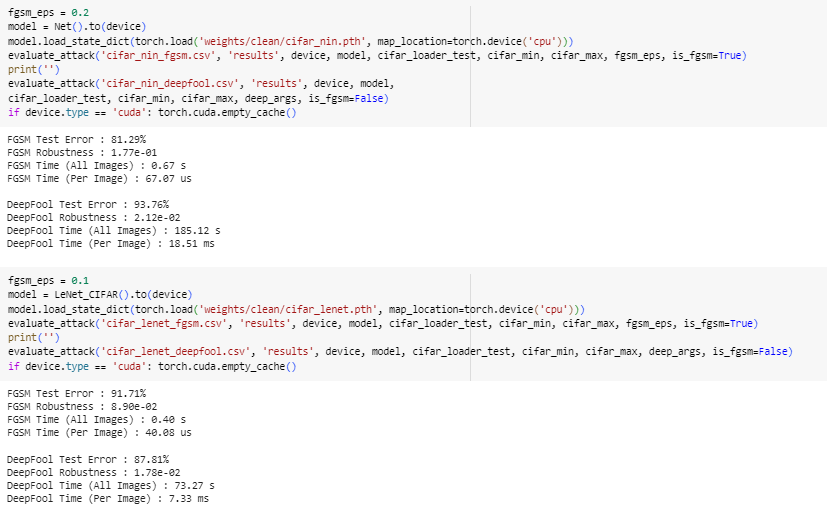
1. Отредактируем гиперпараметры.



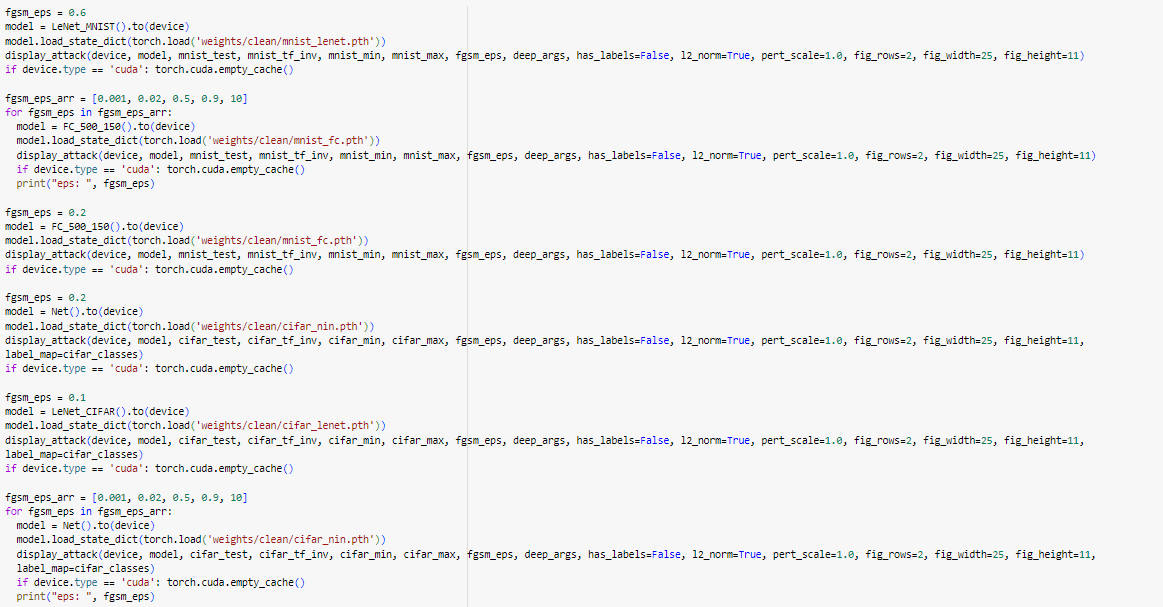
1. Зададим параметры на модель.



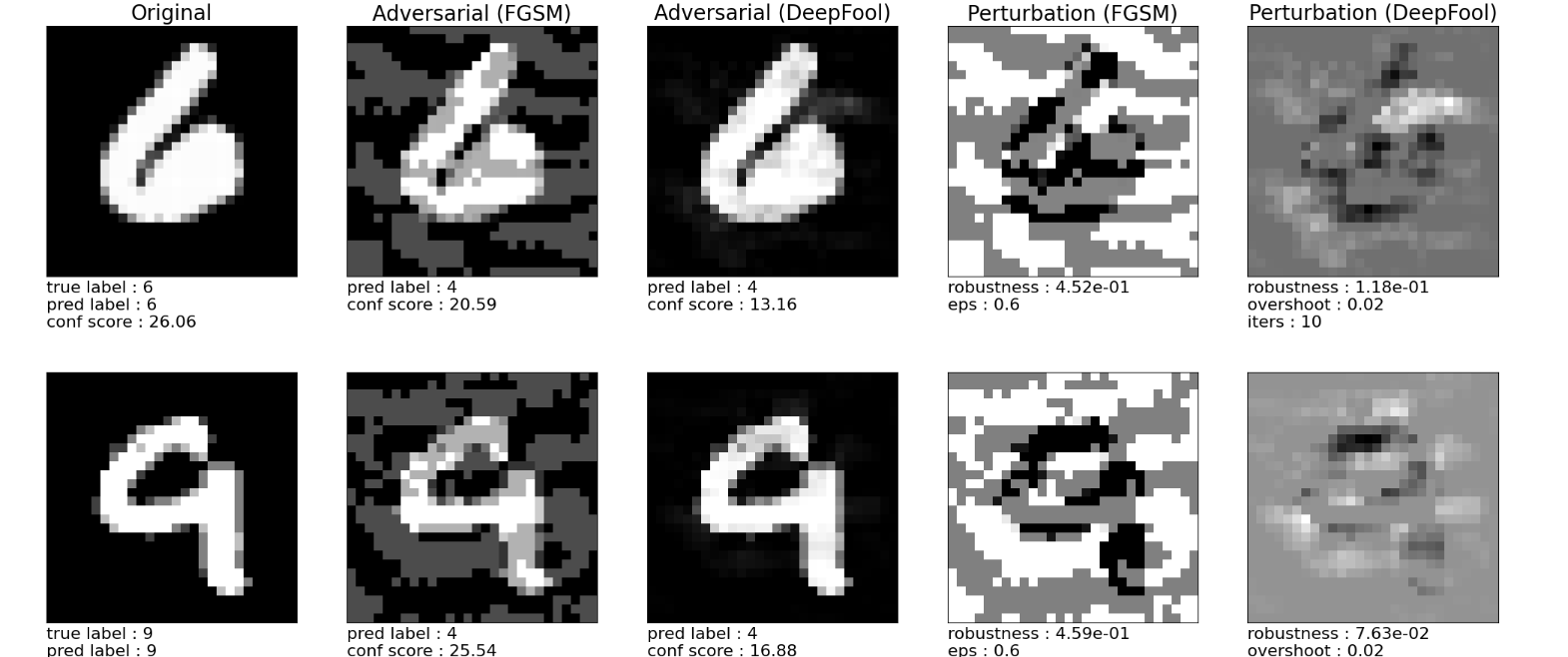
1. Загрузим и оценим стойкость модели.

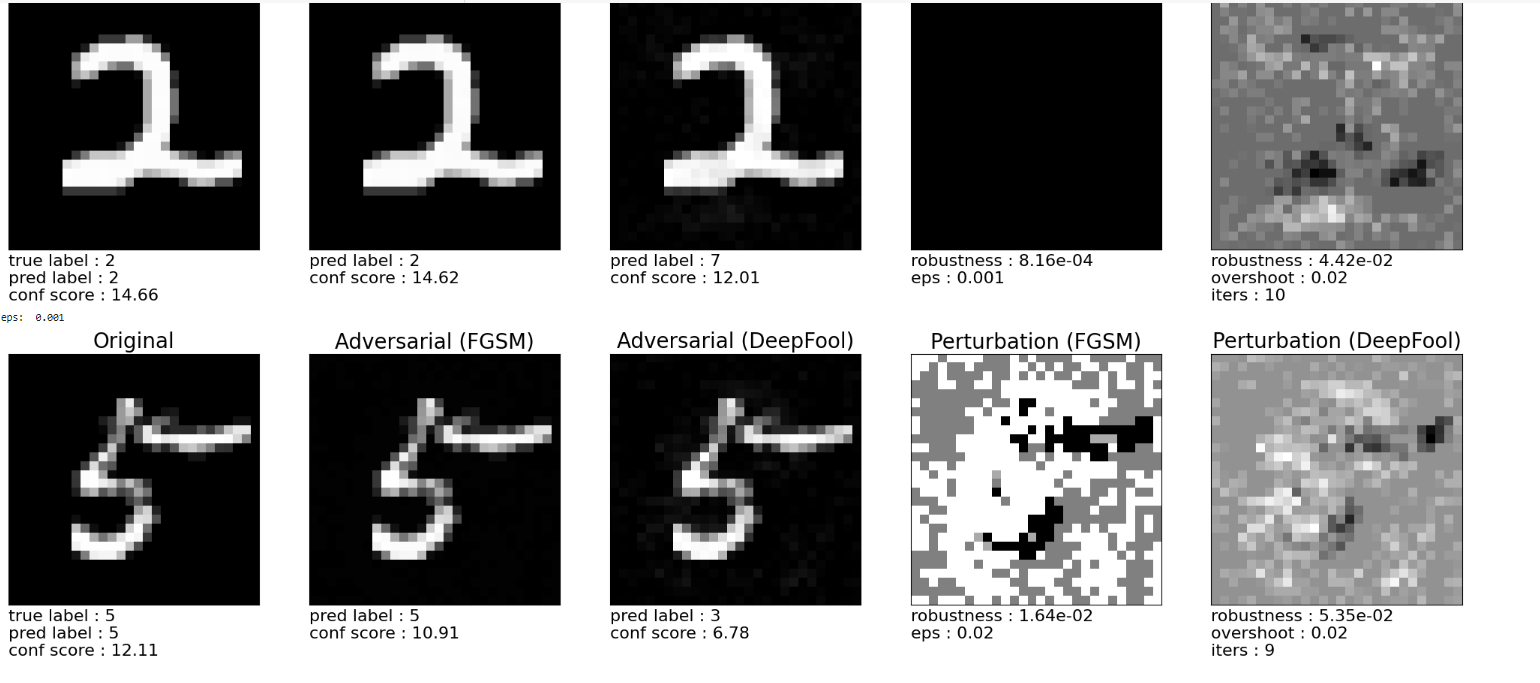


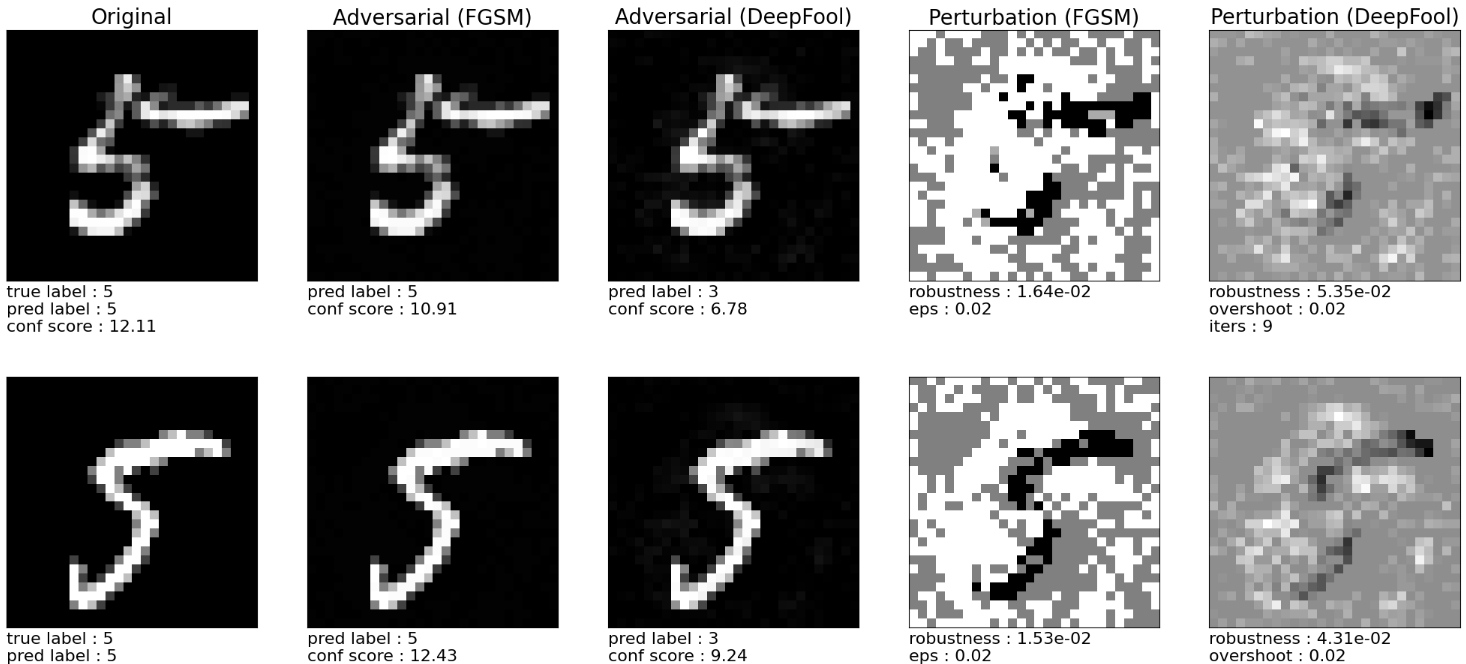
1. Выполним оценку атакующих примеров для сетей.

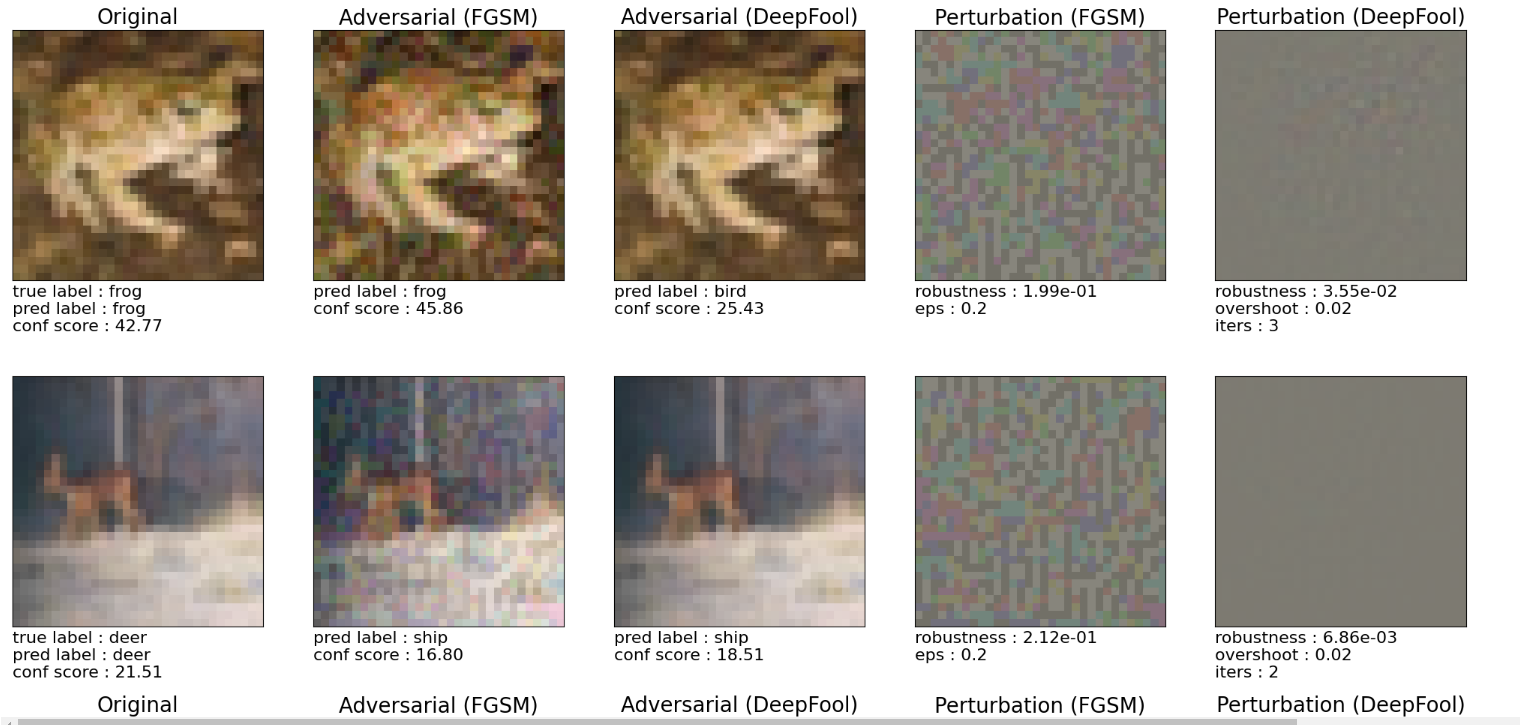


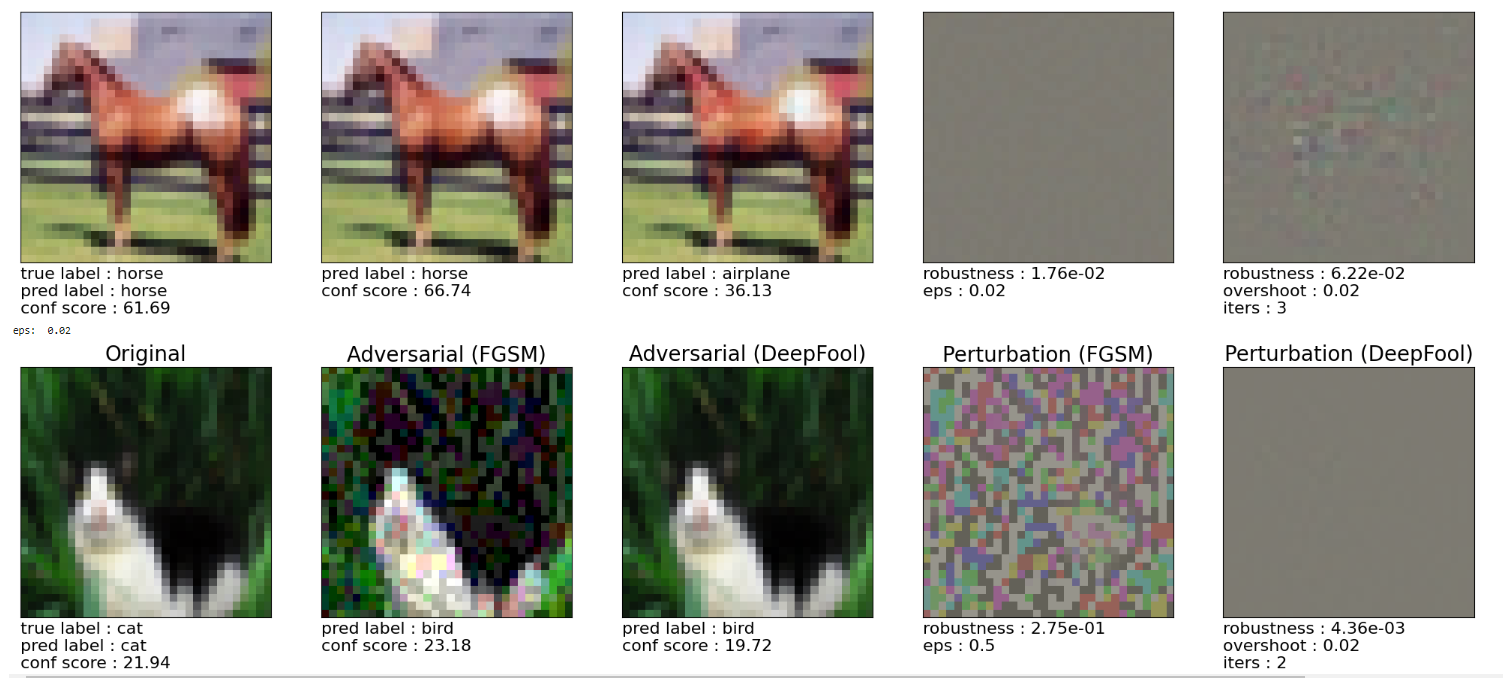
1. Оценим результат атаки.

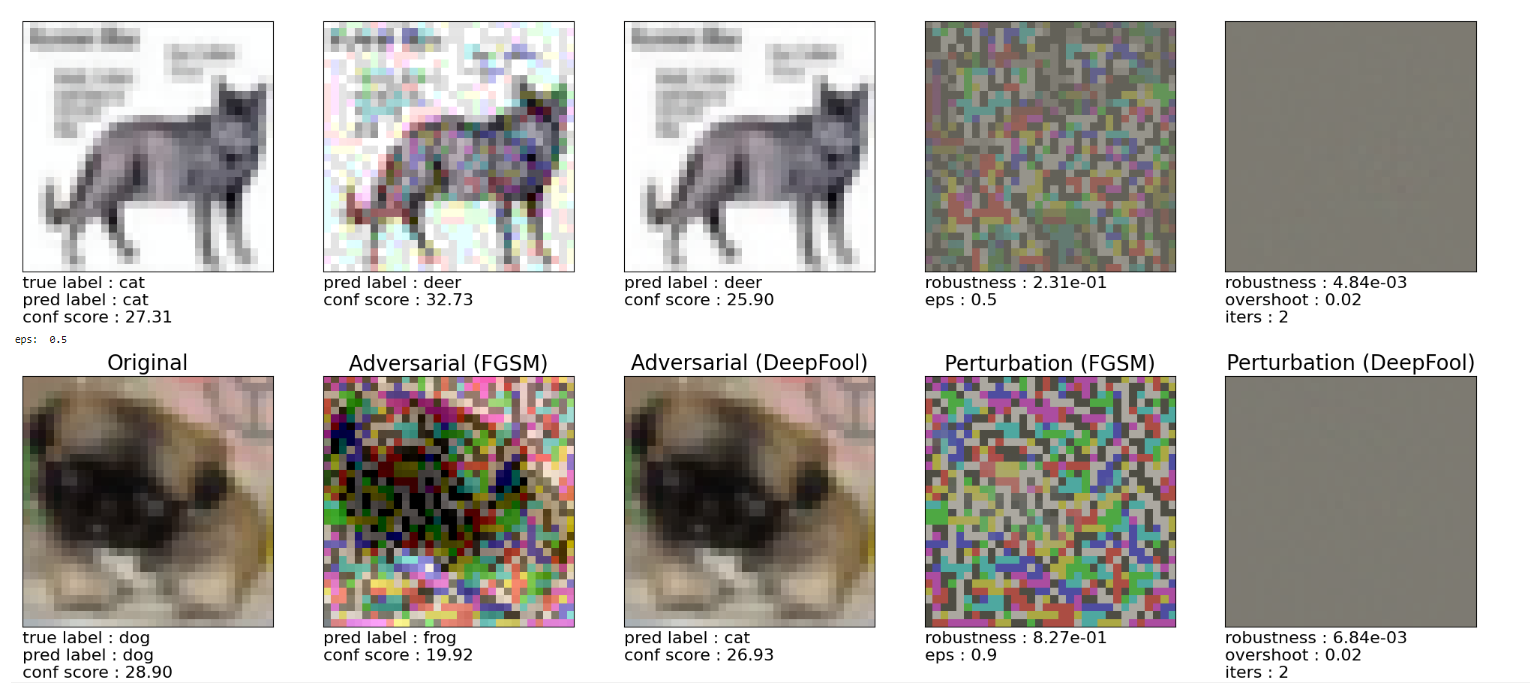


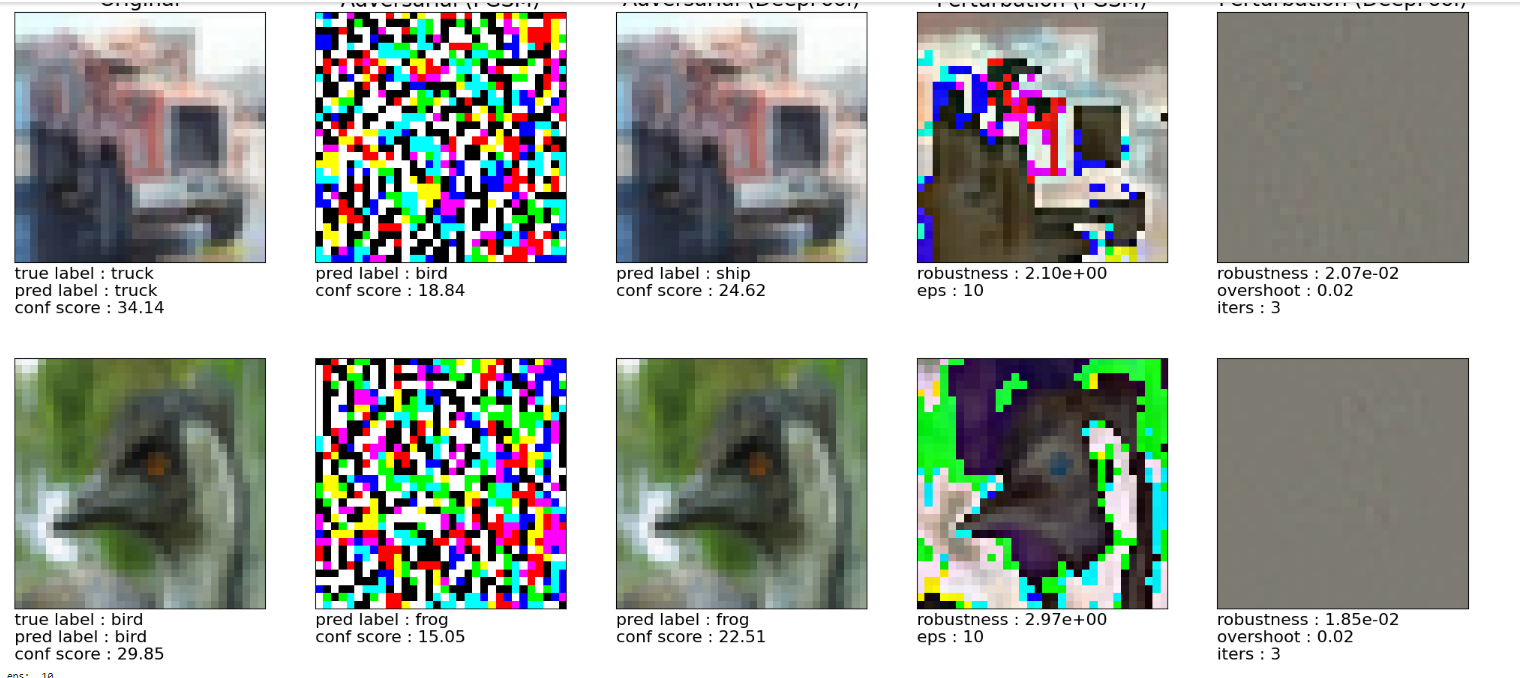












**Выводы**

В ходе выполенния лабораторной работы 1 было обнаружено, что маленькие значения fgsm eps сохраняют устойчивость сетей к атакам, и ошибки классификации остаются низкими. Однако при увеличении fgsm\_eps сети становятся более уязвимыми к атакам и допускают больше ошибок классификации. Для сети FC LeNet на датасете MNIST и для сети NiN LeNEt на датасете CIFAR не наблюдается отсутствие влияния параметра fgsm eps. Наоборот, параметр fgsm\_eps существенно влияет на стойкость сетей к атакам.