

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

# РТУ МИРЭА

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

# Лабораторная работа №1

по дисциплине

«Анализ защищенности систем искусственного интеллекта»

Группа:

ББМО-01-22

Выполнил:

Орлянский В.Е.

Проверил: Спирин А.А.

Москва 2023

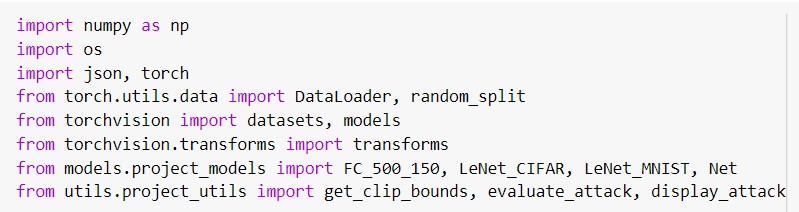
1. Клонируем репозиторий.



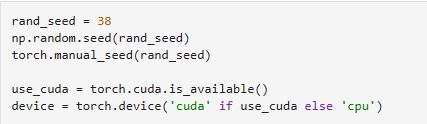
1. Сменим директорию исполнения на вновь созданную папку "EEL6812\_DeepFool\_Project" проекта.



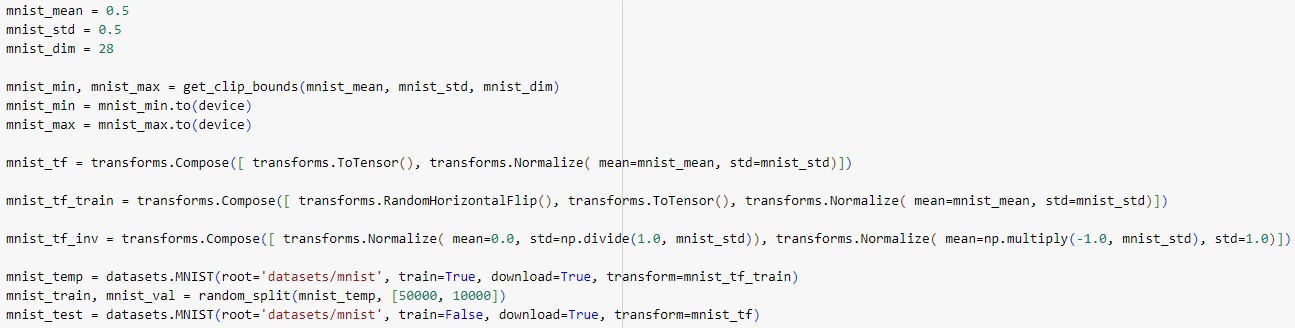
1. Выполним импорт стандартных и вспомогательных библиотек.



1. Установим случайное рандомное значение на номер в списке (38).



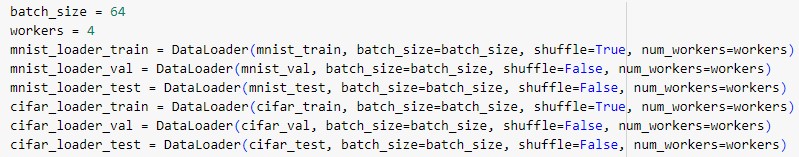
1. Загрузим датасет MNIST.



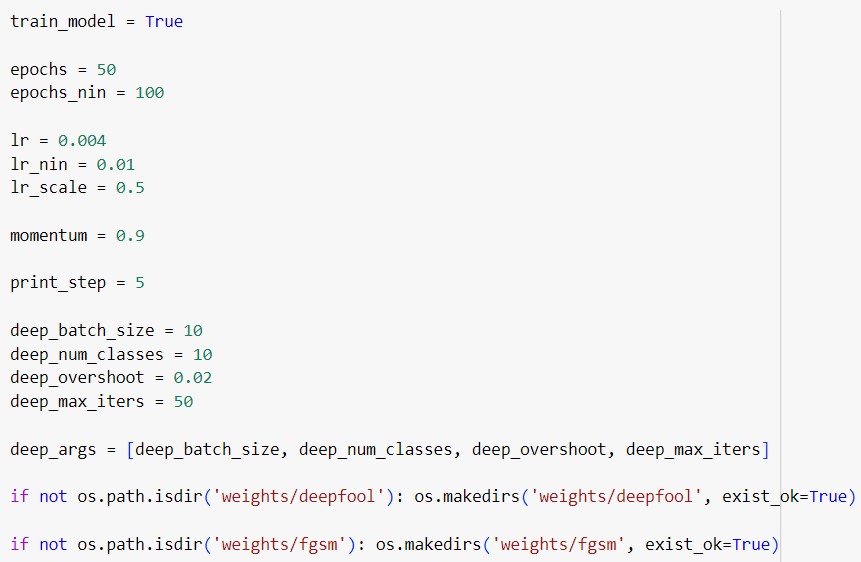
1. Загрузим датасет CIFAR-10.



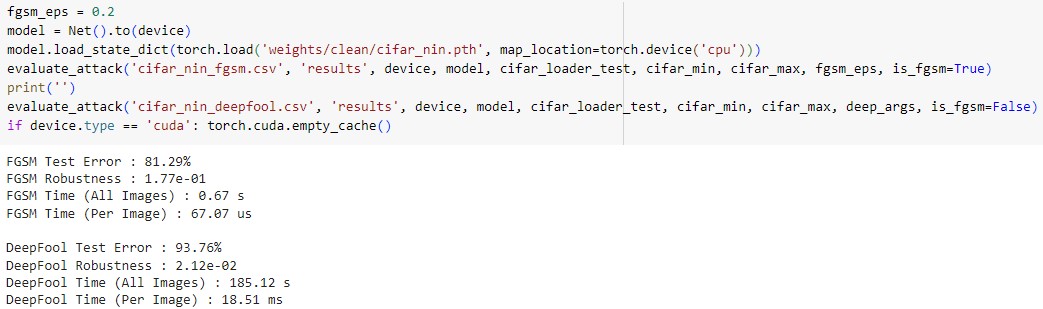
1. Выполним настройку и загрузку DataLoader.



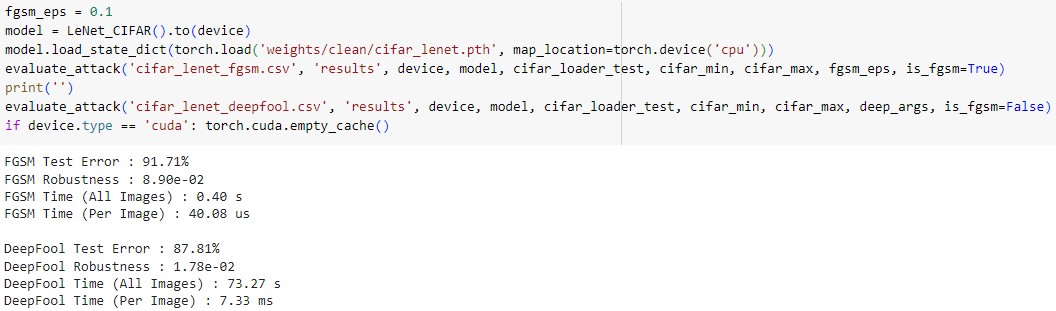
1. Настроим обучающую модель.



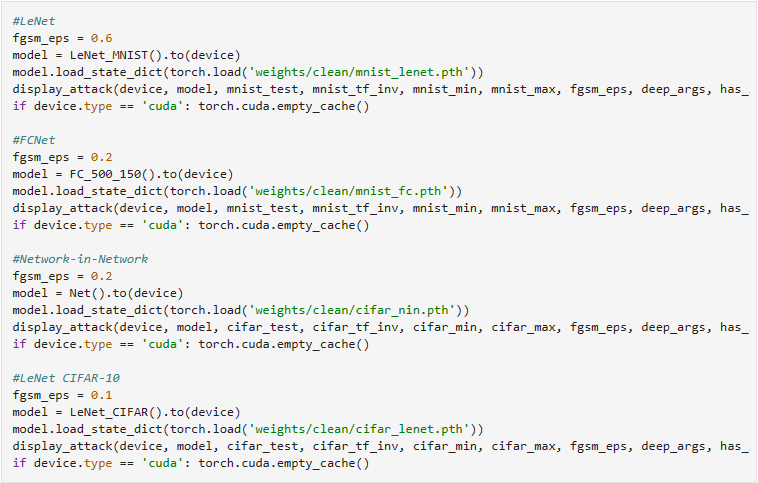
1. Загрузим и оценим стойкость модели Network-In-Network Model к FGSM и DeepFool атакам на основе датасета CIFAR-10.

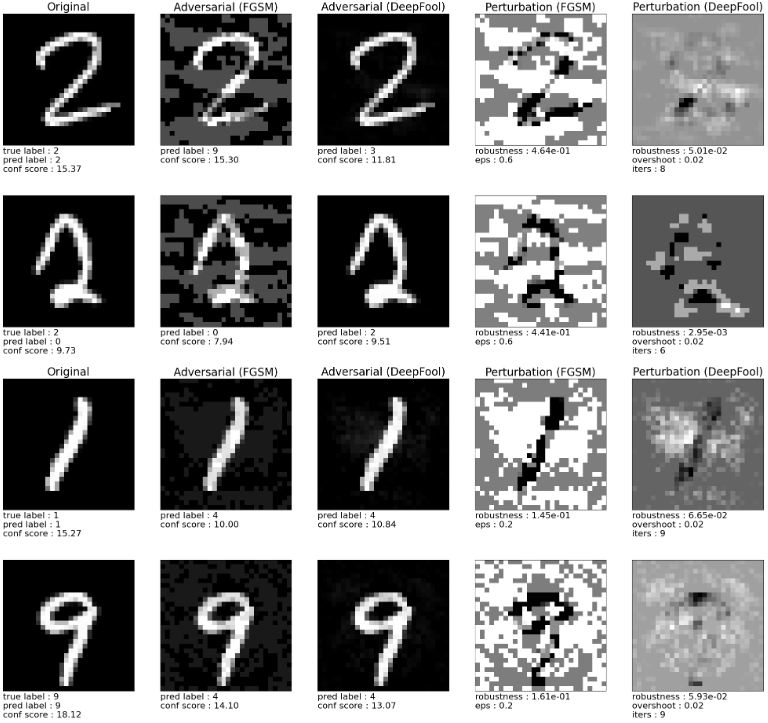


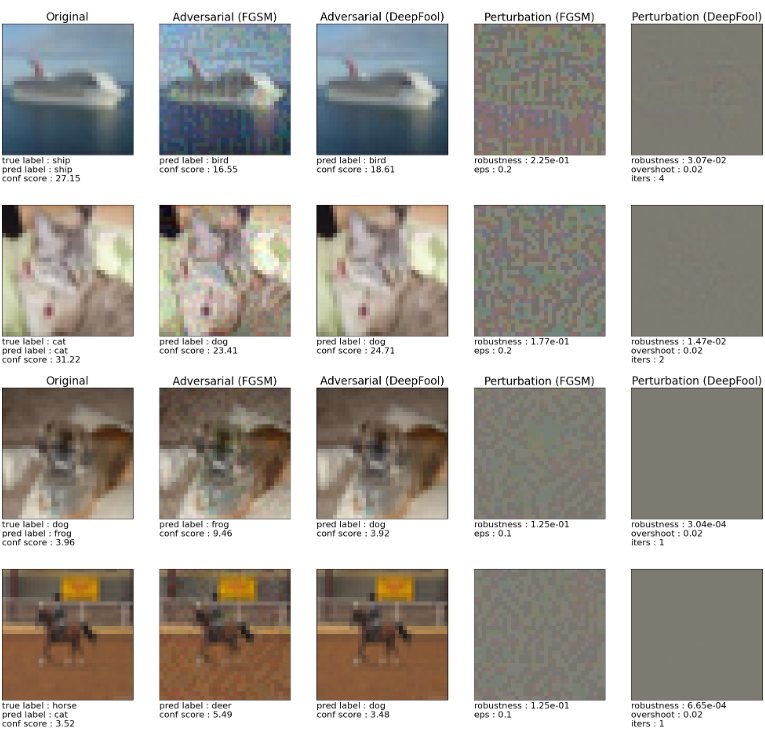
1. Загрузим и оценим стойкость модели LeNet к FGSM и DeepFool атакам на основе датасета CIFAR-10.



1. Выполним оценку атакующих примеров для сетей.

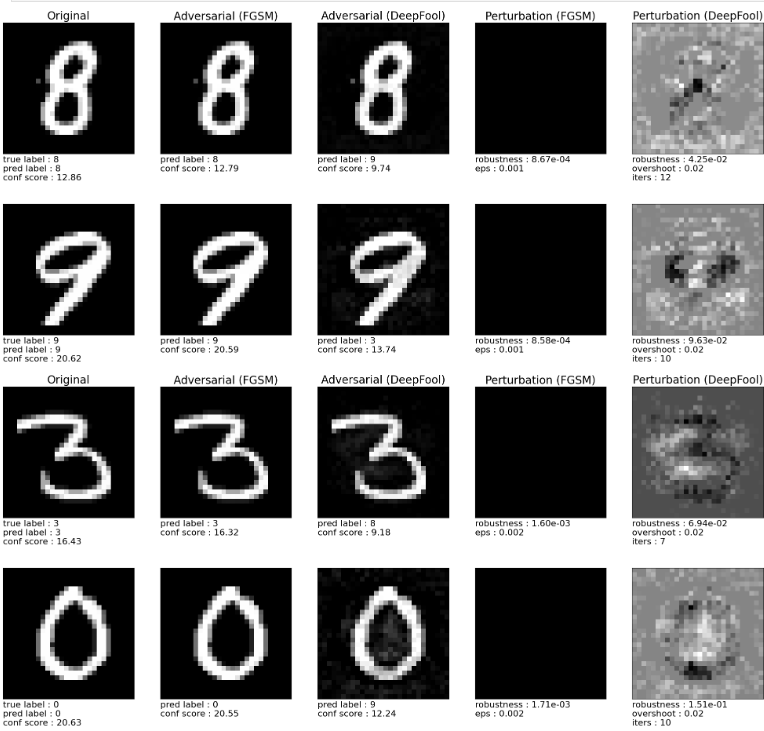


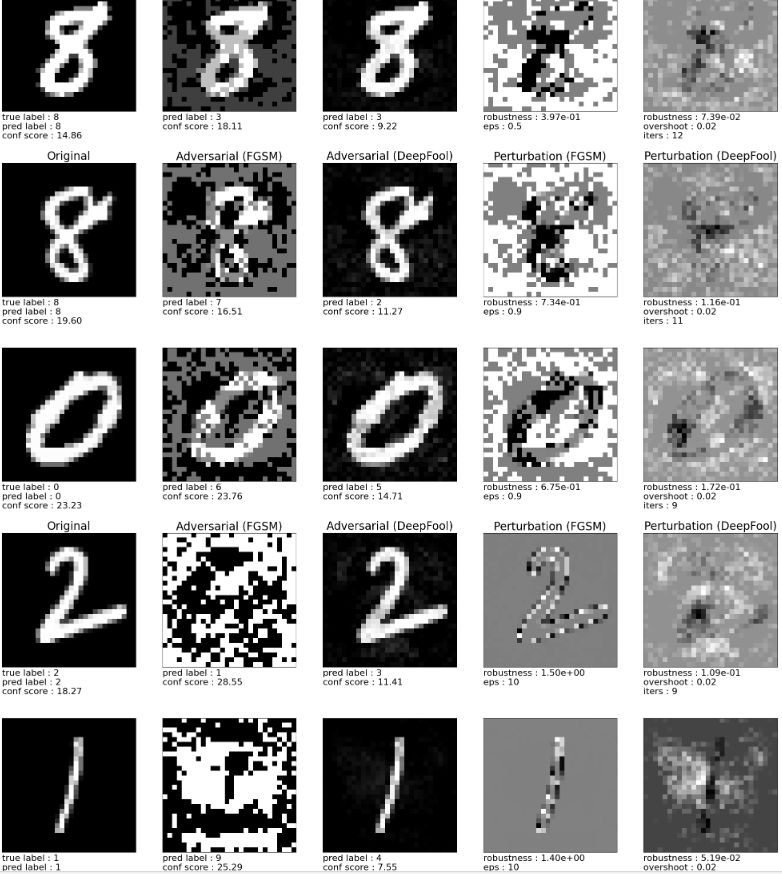


\

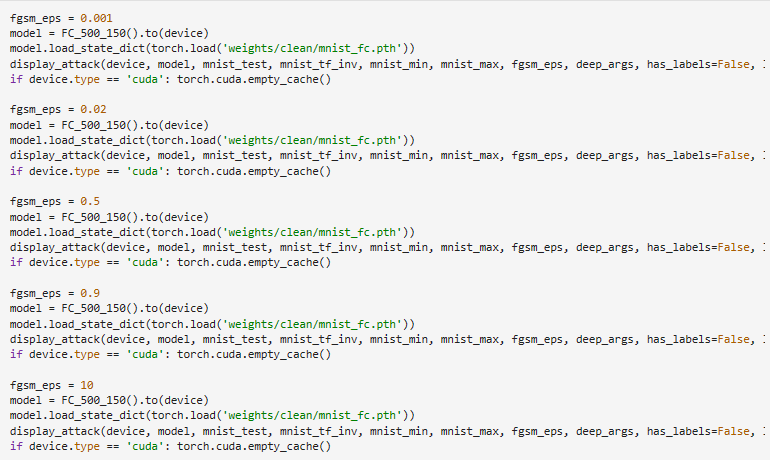
1. Отражаем отличия для fgsm\_eps=(0.001, 0.02, 0.5, 0.9, 10).

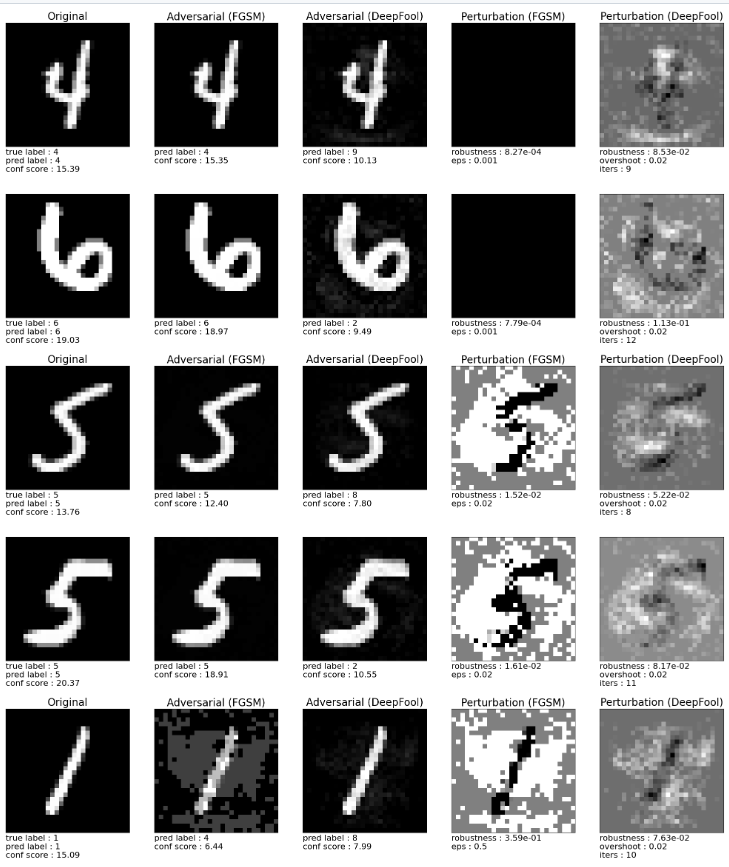


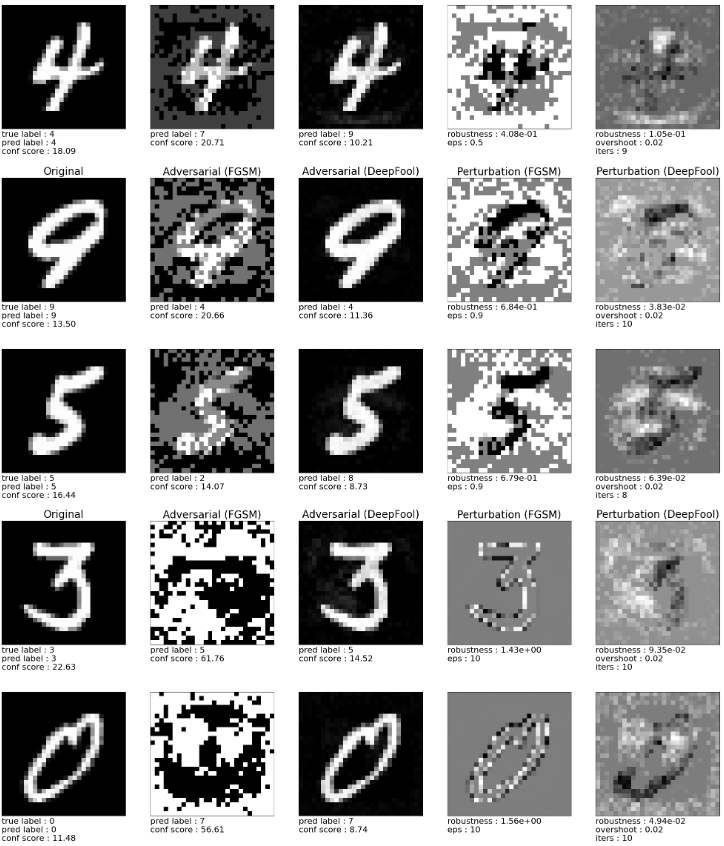


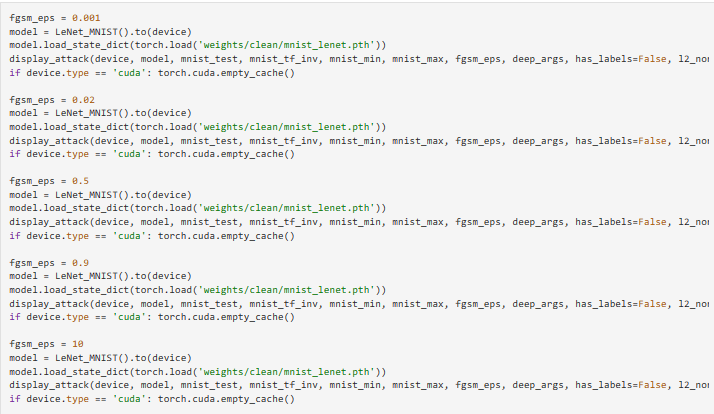


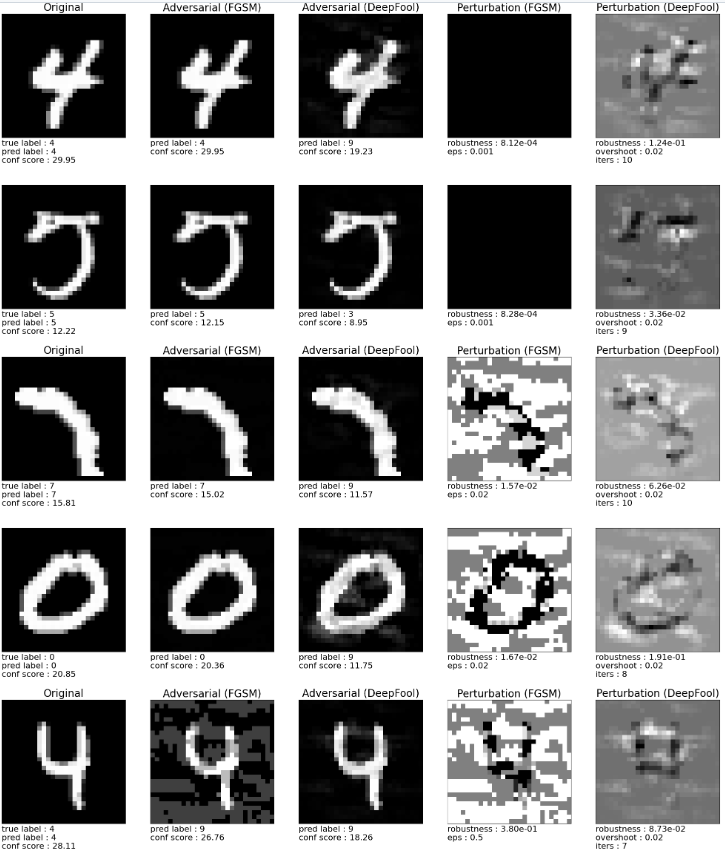
1. Проверим влияние параметра fgsm\_eps для FC на датасете MNIST.

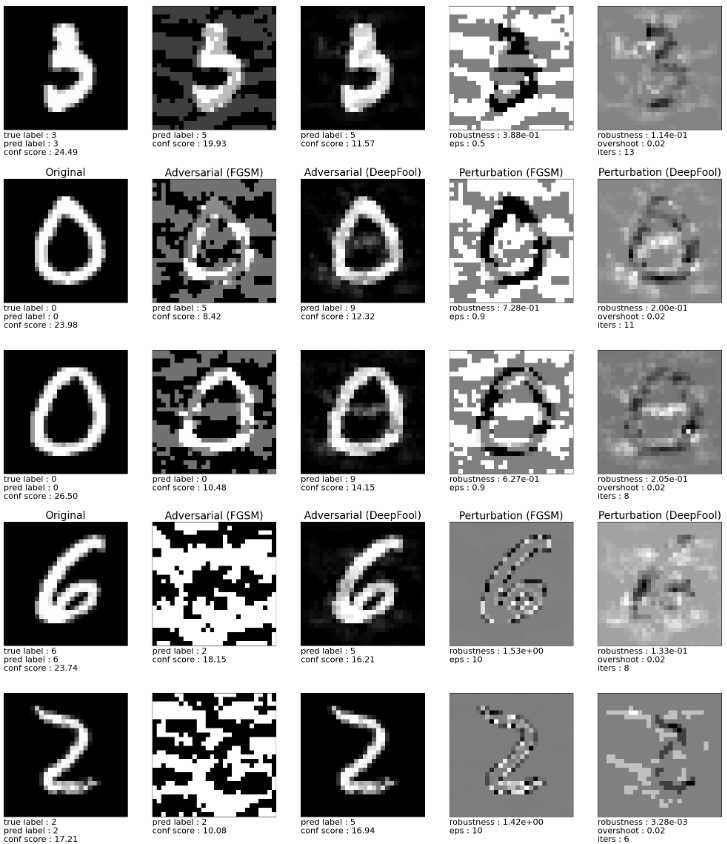




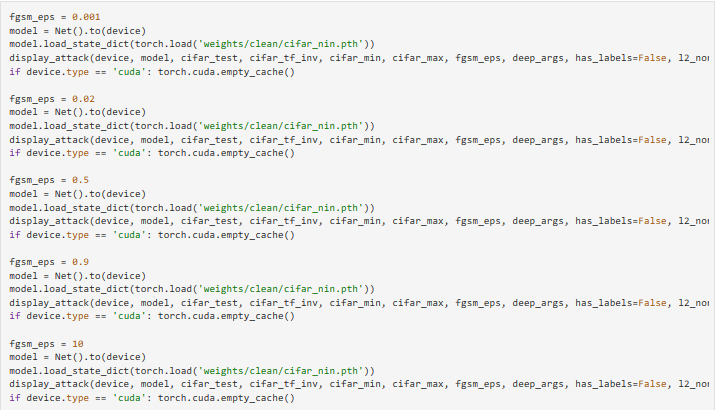


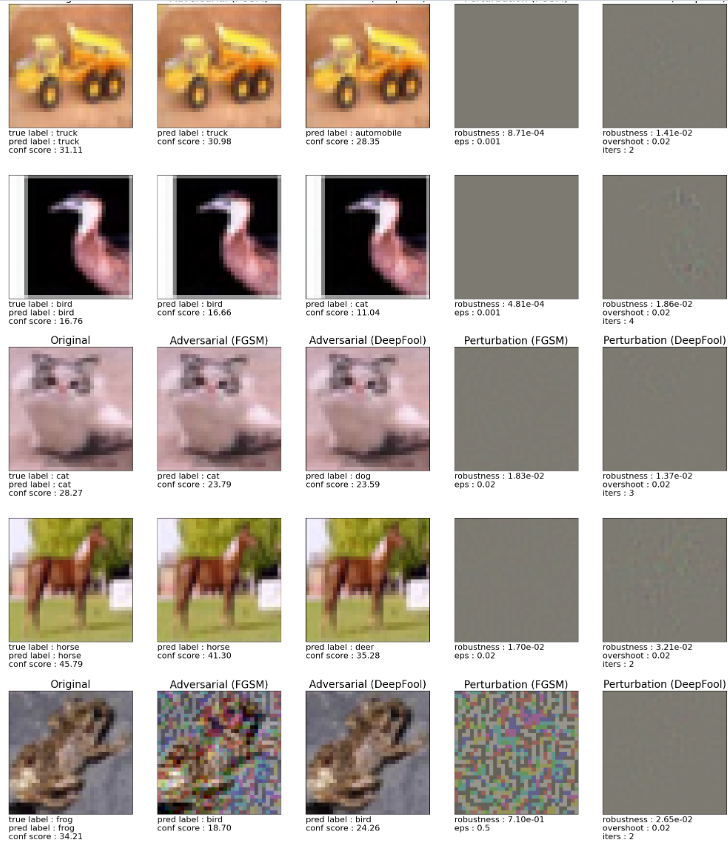
1. Проверим влияние параметра fgsm\_esp для LeNet на датасете MNIST. 

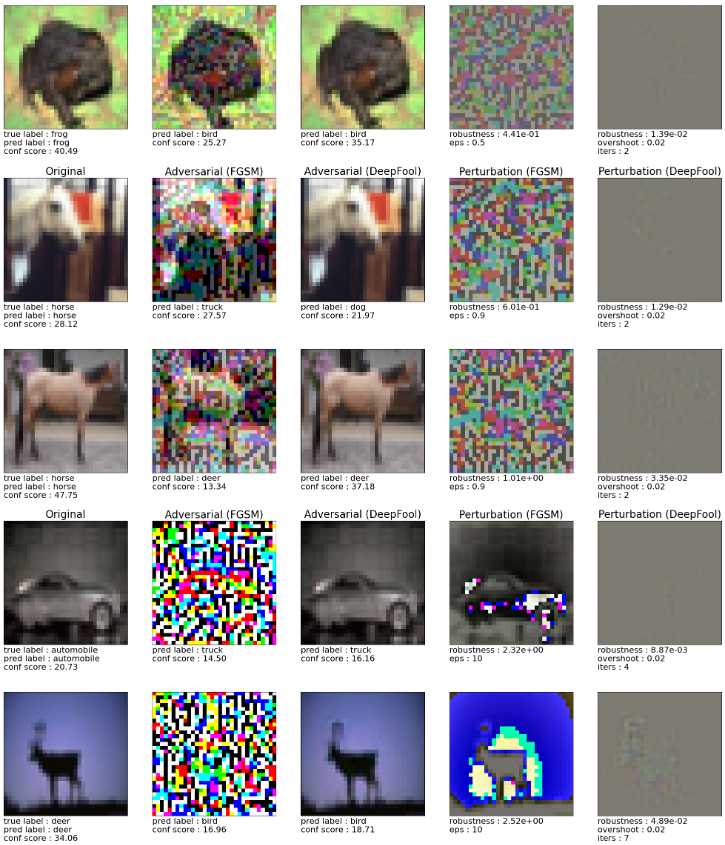




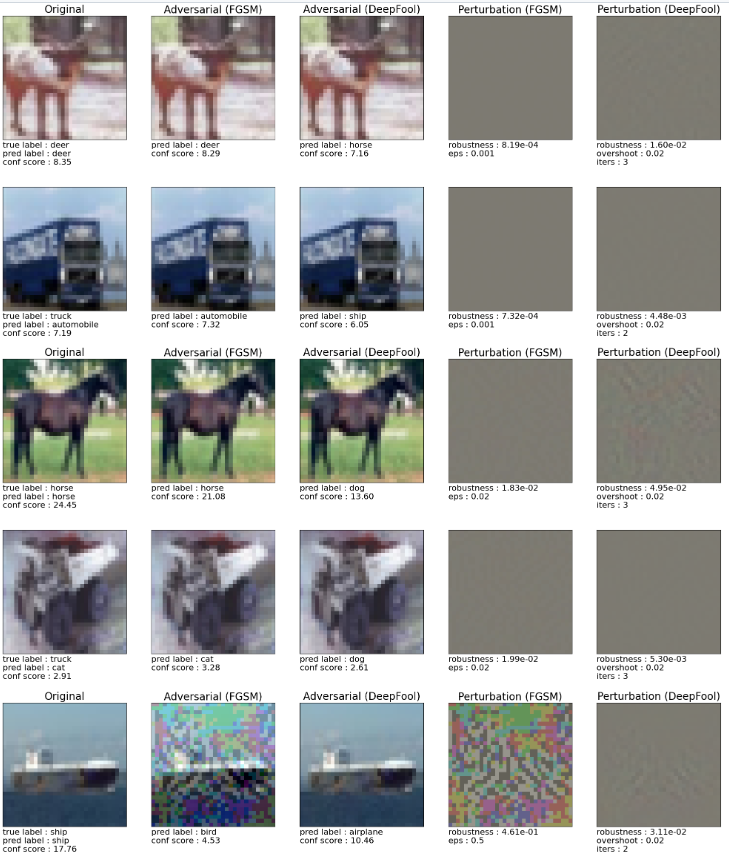
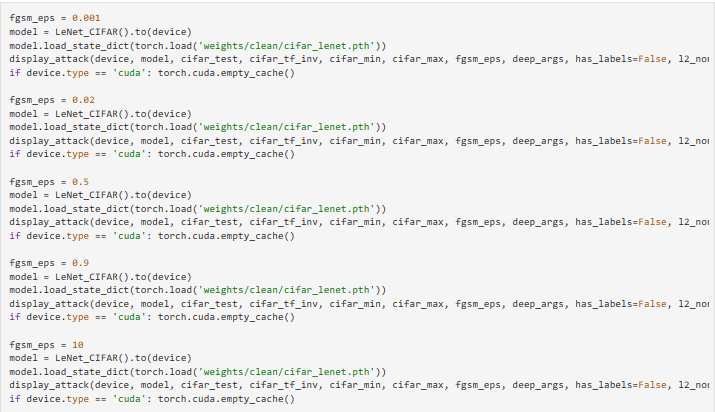
1. Проверим влияние параметра fgsm\_esp для NiN на датасете Cifar-10.

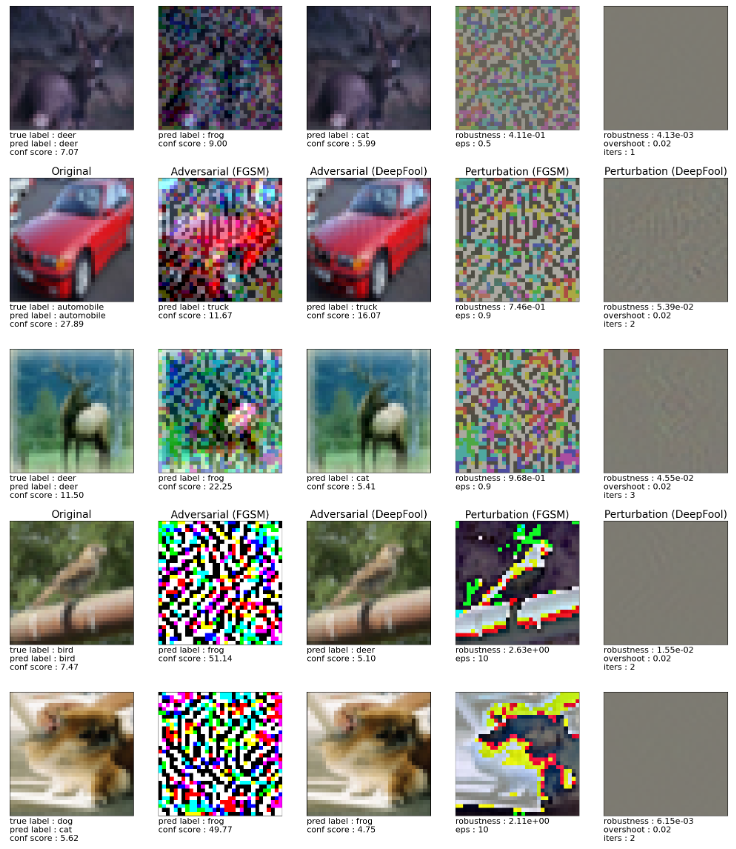






1. Проверим влияние параметра fgsm\_esp для LeNet на датасете Cifar-10.





Вывод: параметр fgsm\_esp влияет на устойчивость сети. При увеличении значения fgsm\_esp сети становятся уязвимыми к атакам.