|  |
| --- |
|  |
| 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 №1

по дисциплине: «Анализ защищенности систем искусственного интеллекта»

**Выполнил**:

Студент группы ББМО-02-22

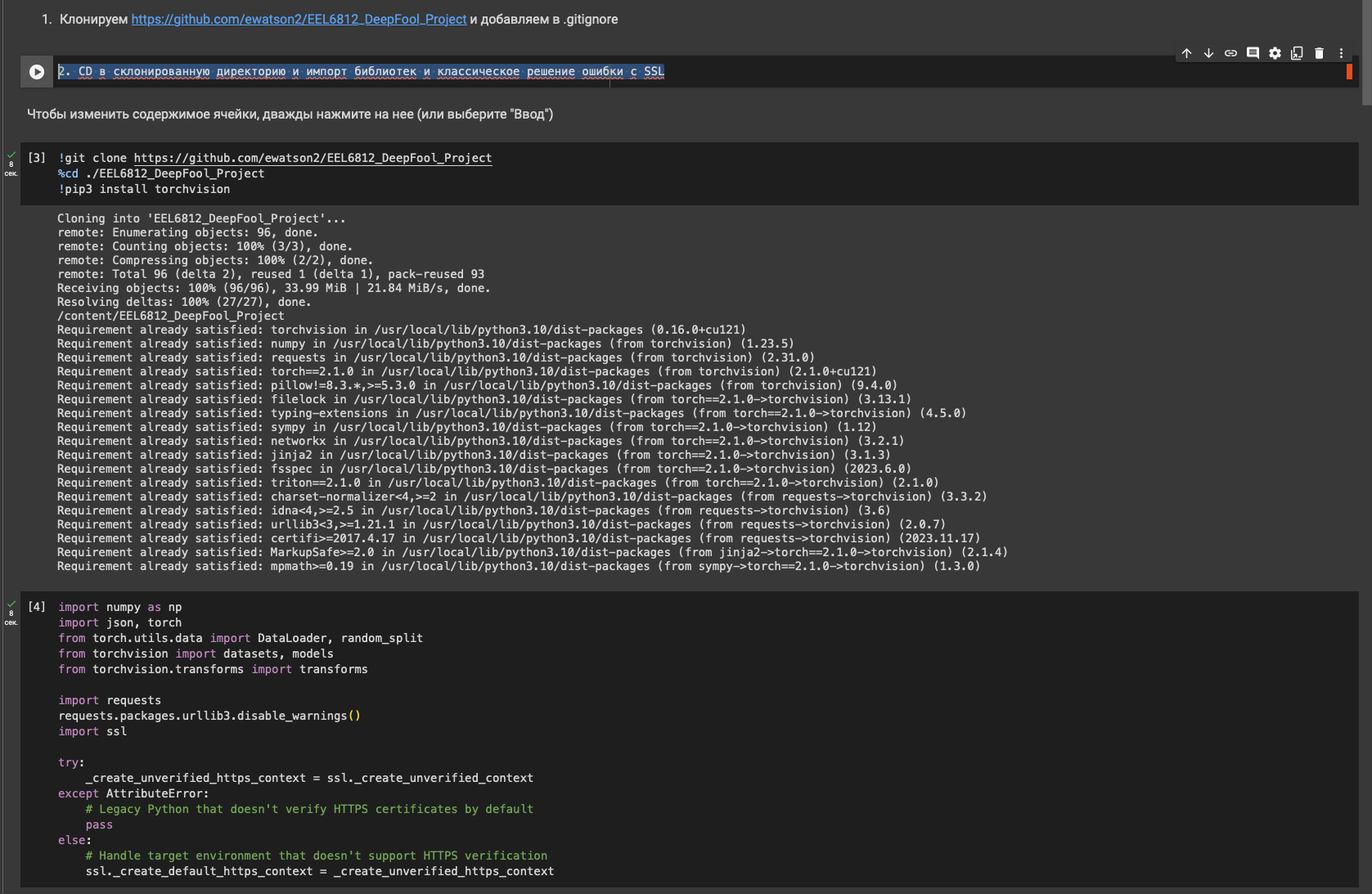
Филиппов Леонид Алексеевич

**Проверил**:

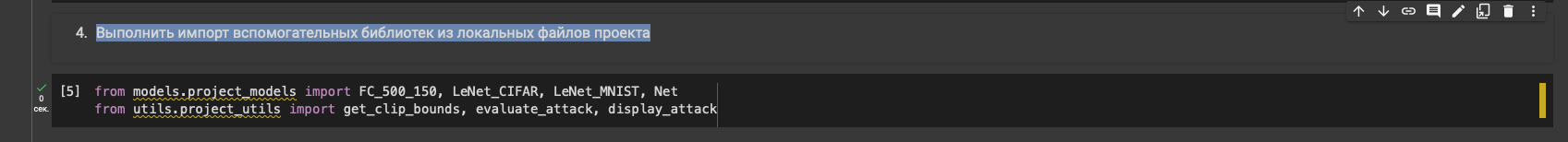
Спирин Андрей Андреевич

Москва 2024

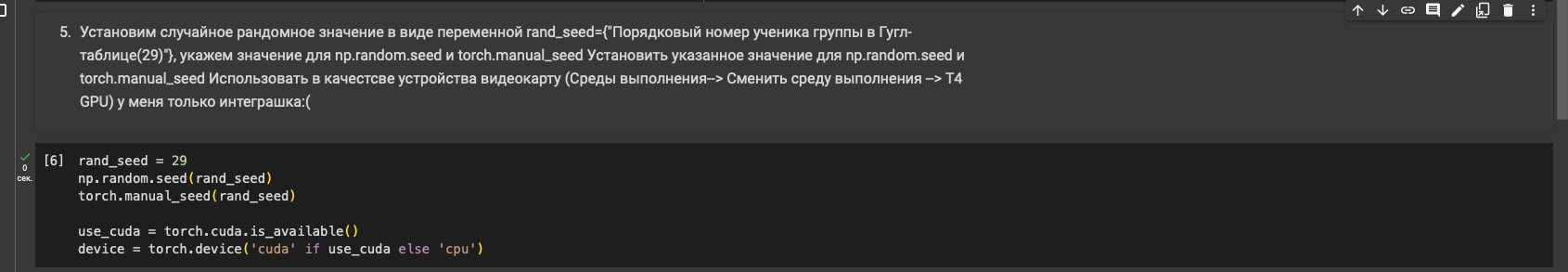
1. Клонируем <https://github.com/ewatson2/EEL6812_DeepFool_Project> и добавляем в .gitignore
2. CD в склонированную директорию и импорт библиотек и классическое решение ошибки с SSL



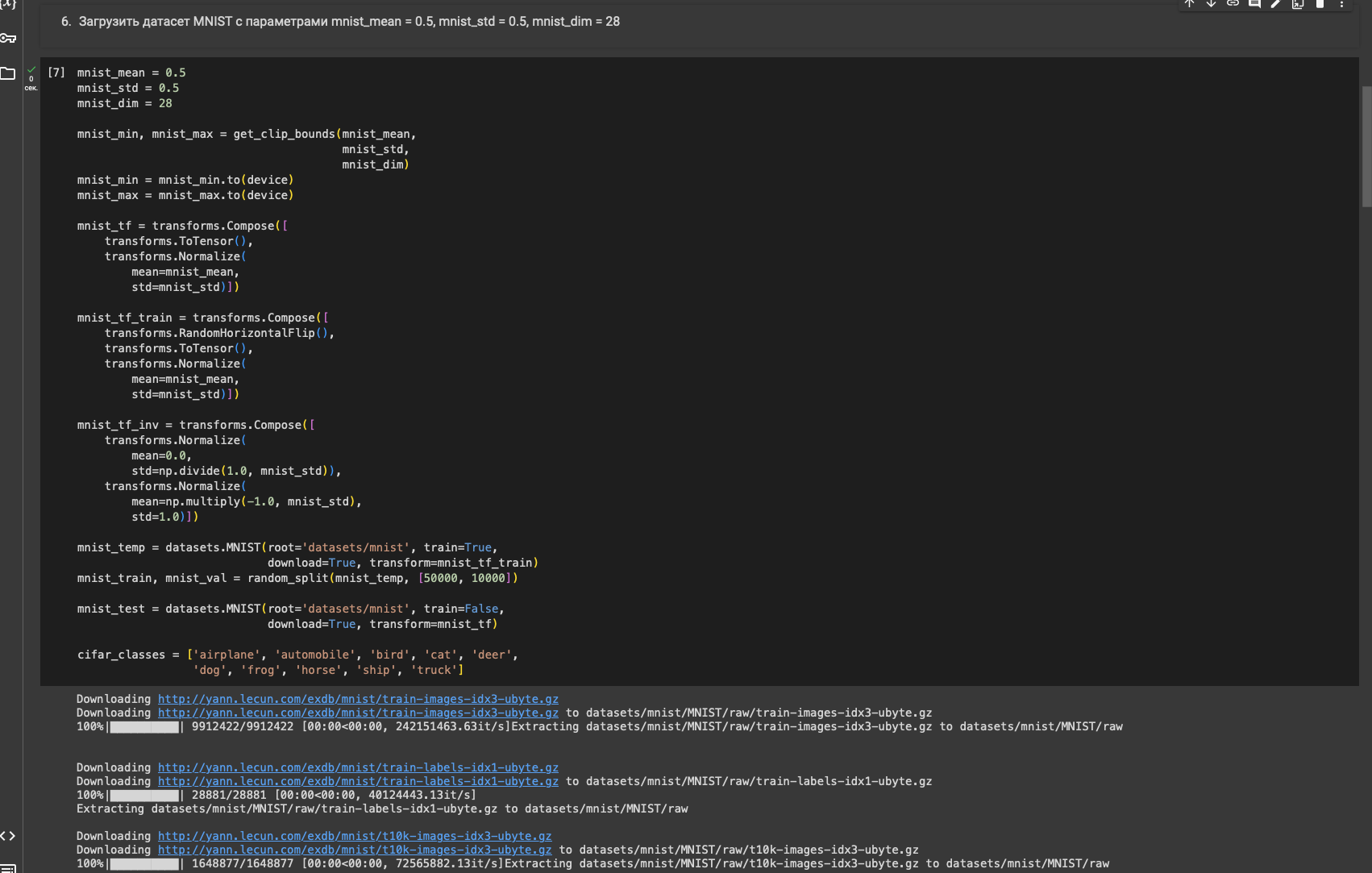
1. Выполнить импорт вспомогательных библиотек из локальных файлов проекта



1. Установим случайное рандомное значение в виде переменной rand\_seed={"Порядковый номер ученика группы в Гугл-таблице(29)"}, укажем значение для np.random.seed и torch.manual\_seed Установить указанное значение для np.random.seed и torch.manual\_seed Использовать в качестсве устройства видеокарту (Среды выполнения--> Сменить среду выполнения --> T4 GPU) у меня только интеграшка:(



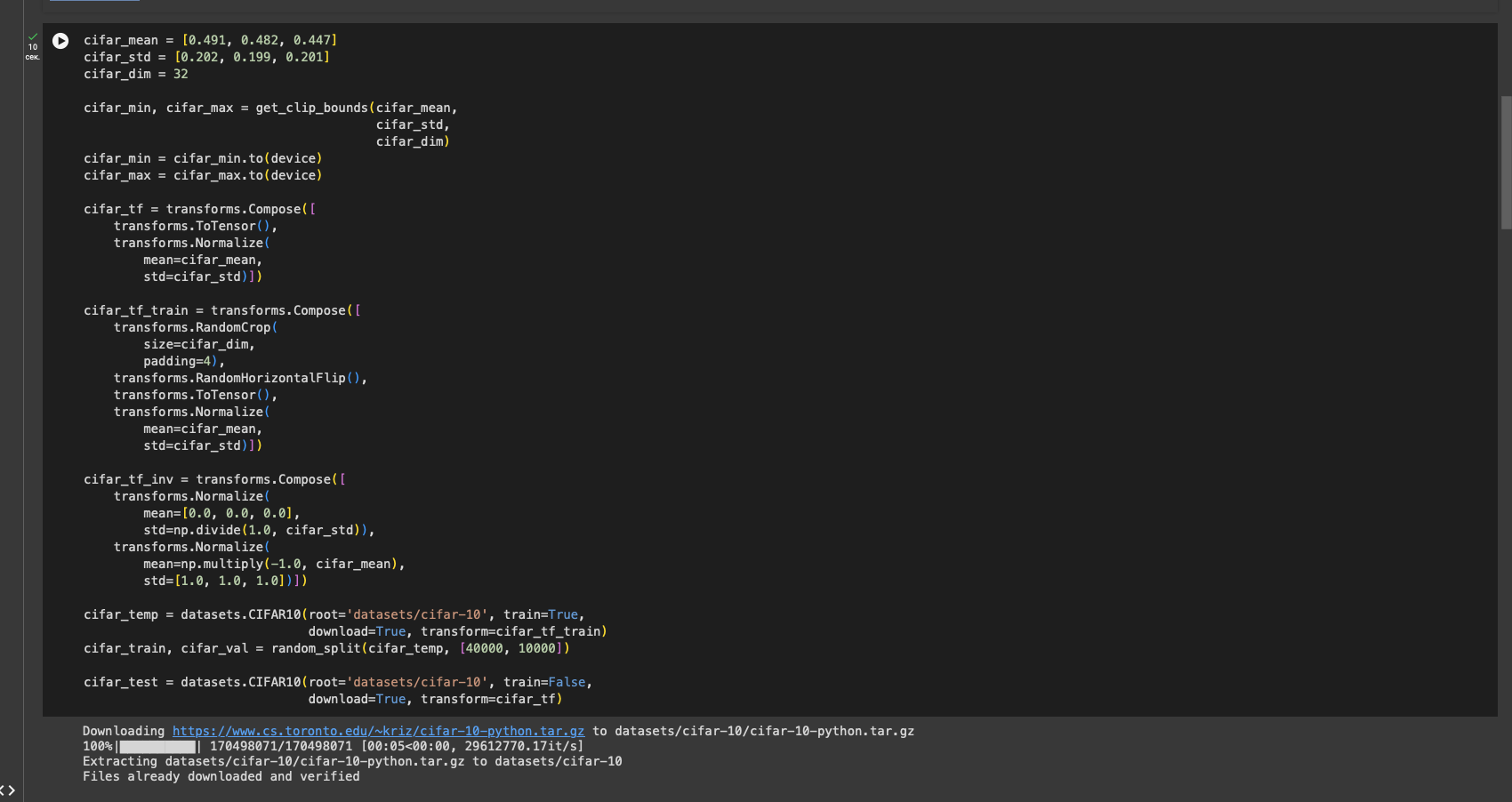
1. Загрузить датасет MNIST c параметрами mnist\_mean = 0.5, mnist\_std = 0.5, mnist\_dim = 28



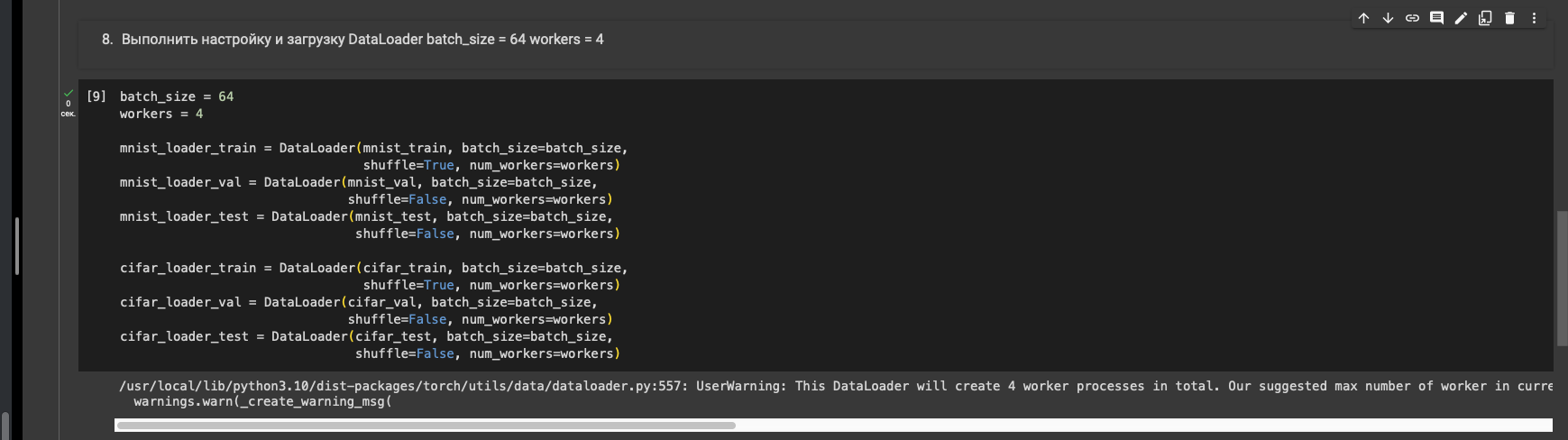
1. Загрузить датасет CIFAR-10 c параметрами cifar\_mean = [0.491, 0.482, 0.447]

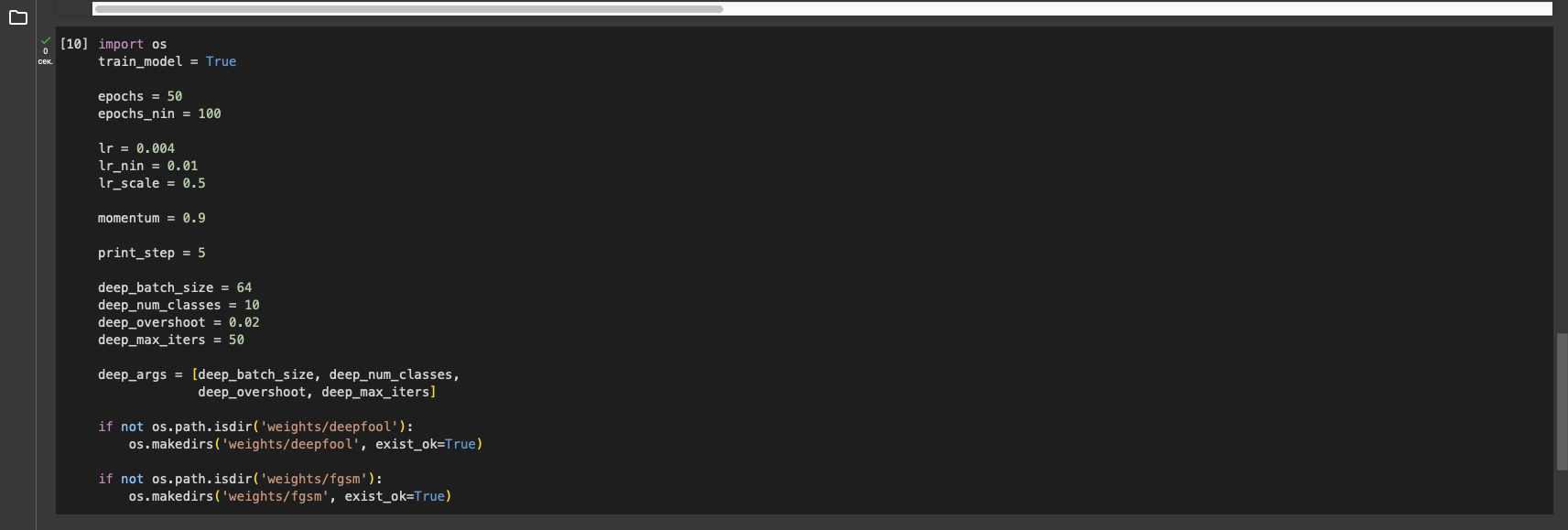
cifar\_std = [0.202,0.199, 0.201]

cifar\_dim = 32

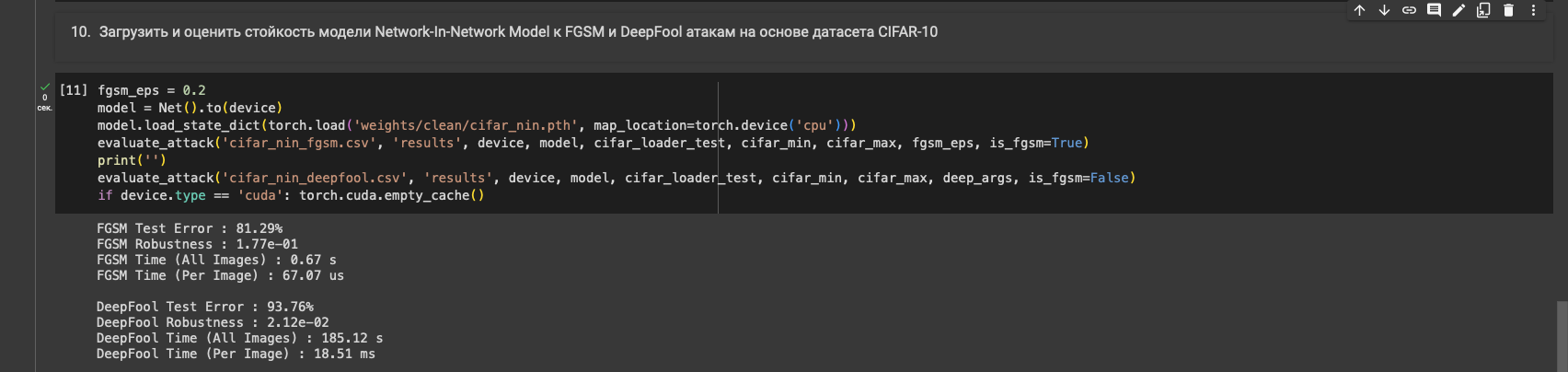


1. Выполнить настройку и загрузку DataLoader batch\_size = 64 workers = 4

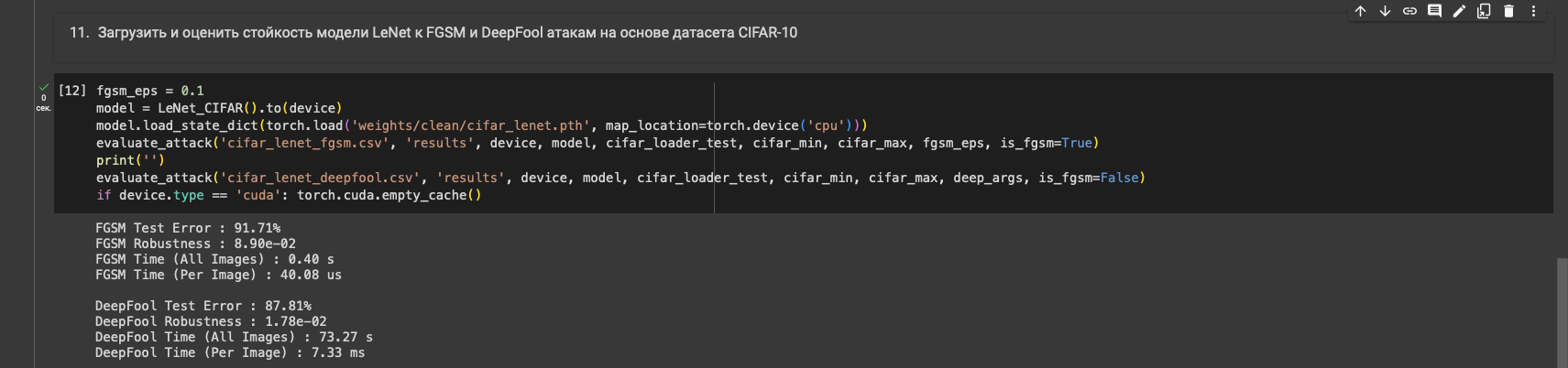




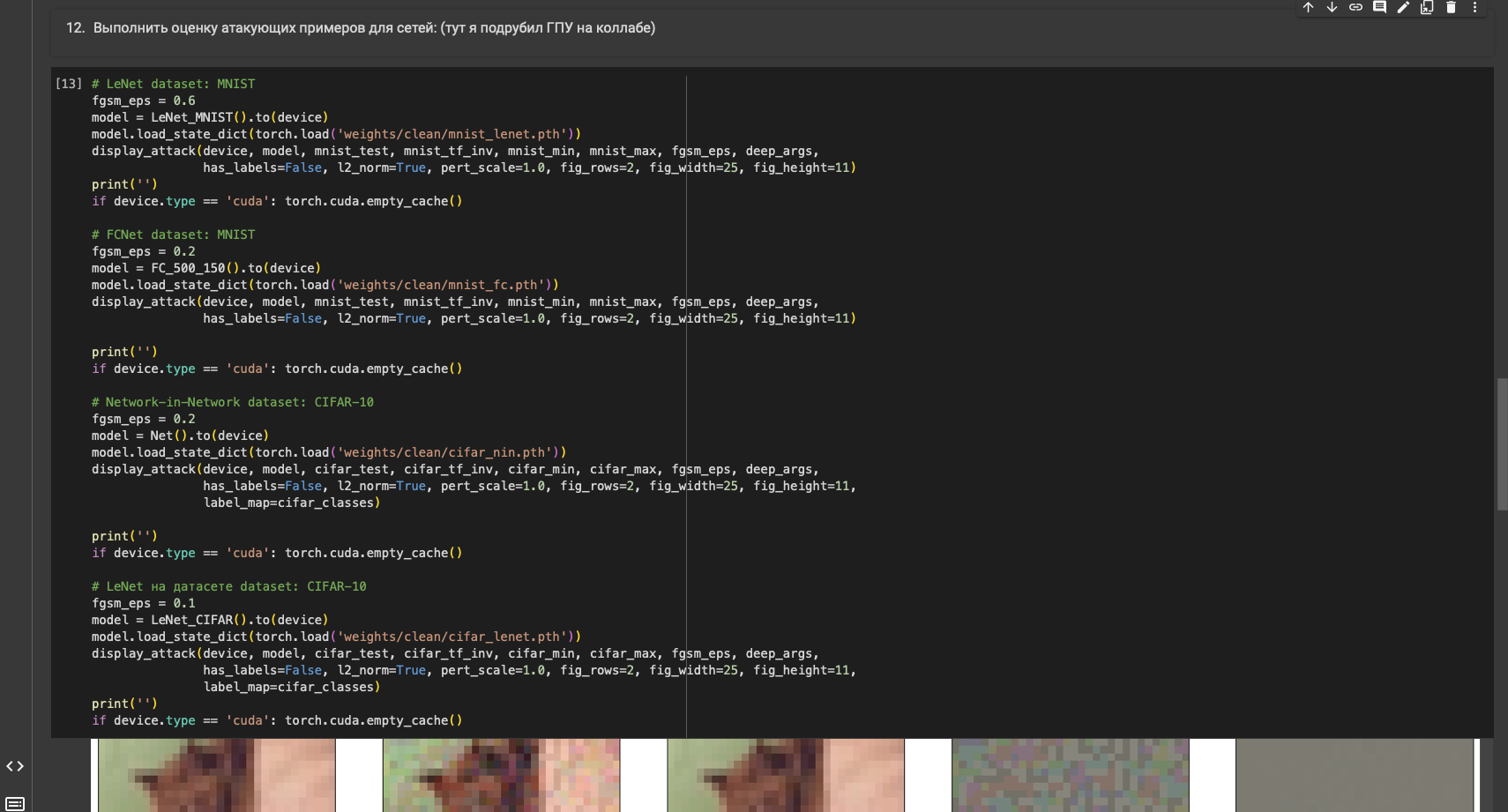
1. Загрузить и оценить стойкость модели Network-In-Network Model к FGSM и DeepFool атакам на основе датасета CIFAR-10



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



1. Выполнить оценку атакующих примеров для сетей: (тут я подрубил ГПУ на коллабе)



1. Подготовить отчет в формате pdf (отразить отличия для fgsm\_eps=(0.001, 0.02, 0.5, 0.9, 10) и выявить закономерность/обнаружить отсутсвие влияние параметра eps для сетей FC LeNet на датасете MNIST, NiN LeNEt на датасете CIFAR )

