

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»

# Практическая работа №4

по дисциплине

«Анализ защищенности систем искусственного интеллекта»

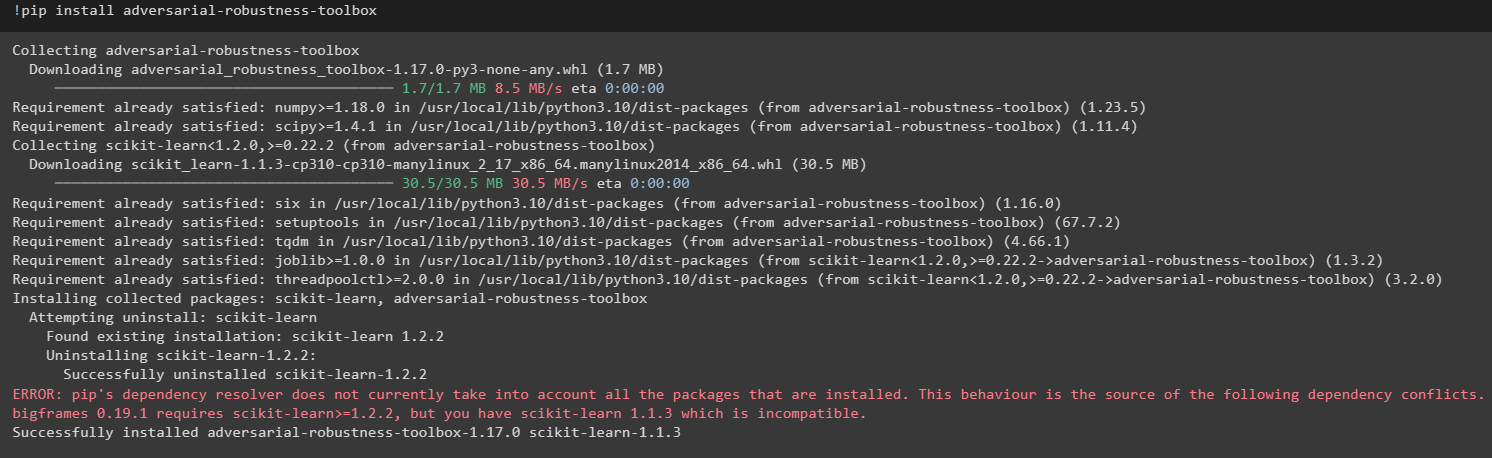
Группа: ББМО-01-22

Выполнил: Некрасов Е.А.

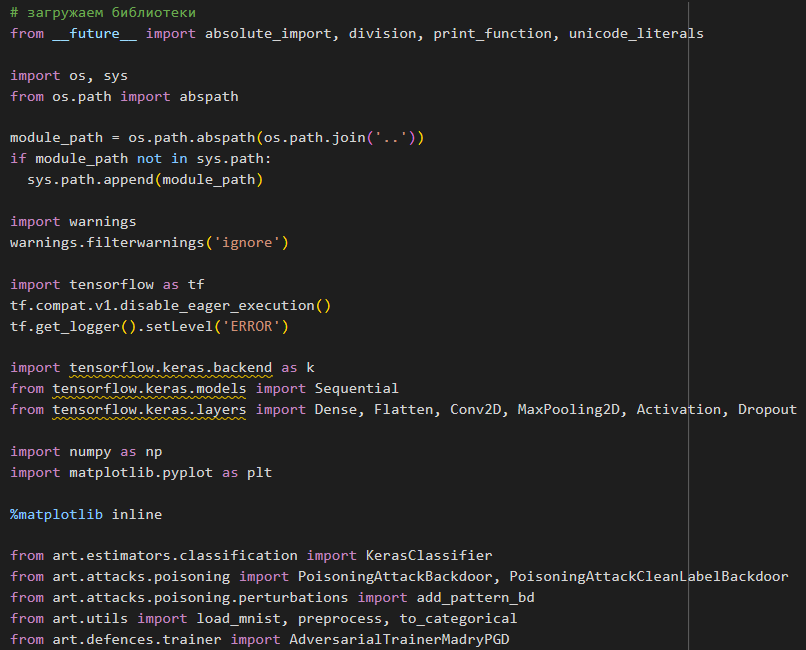
Проверил: Спирин А.А.

Москва 2024

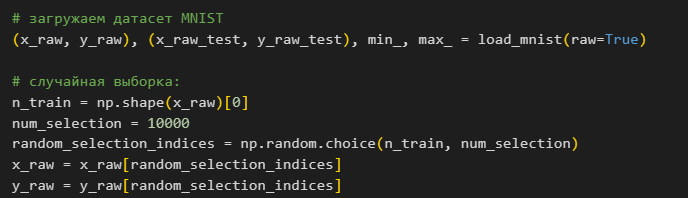
1. Установим пакет art



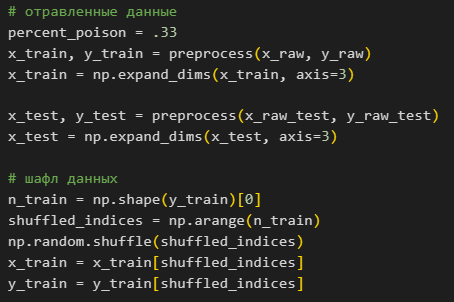
1. Загружаем необходимые библиотеки



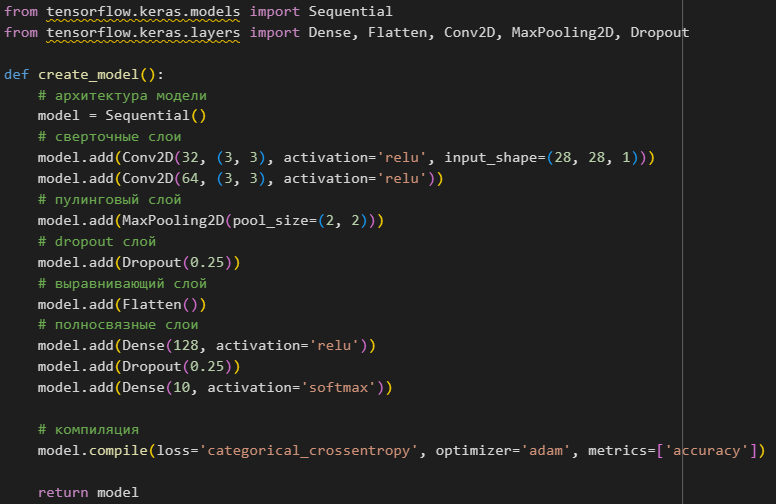
1. Загружаем датасет MNIST и разделяем его на обучающую и тестовую выборки



1. Выполняем отравление данных



1. Пишем функцию create\_model() для создания последовательной модели из 9 слоев



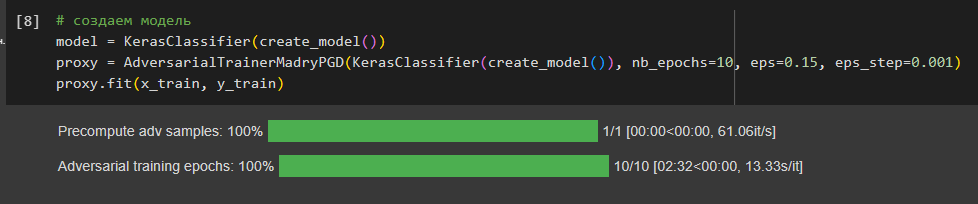
1. Создаем атаку



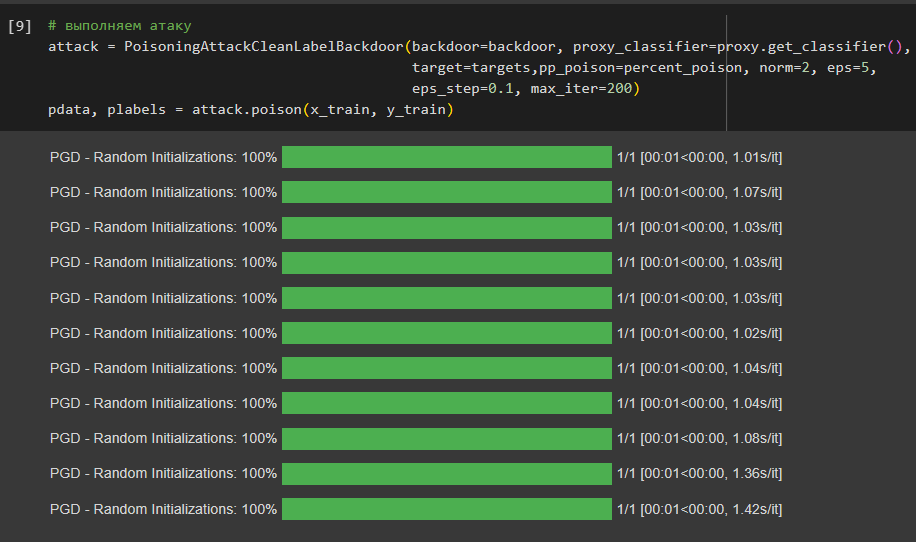
1. Определяем целевой класс атаки



1. Создадим модели и обучим



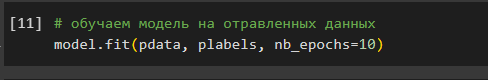
1. Выполним атаку



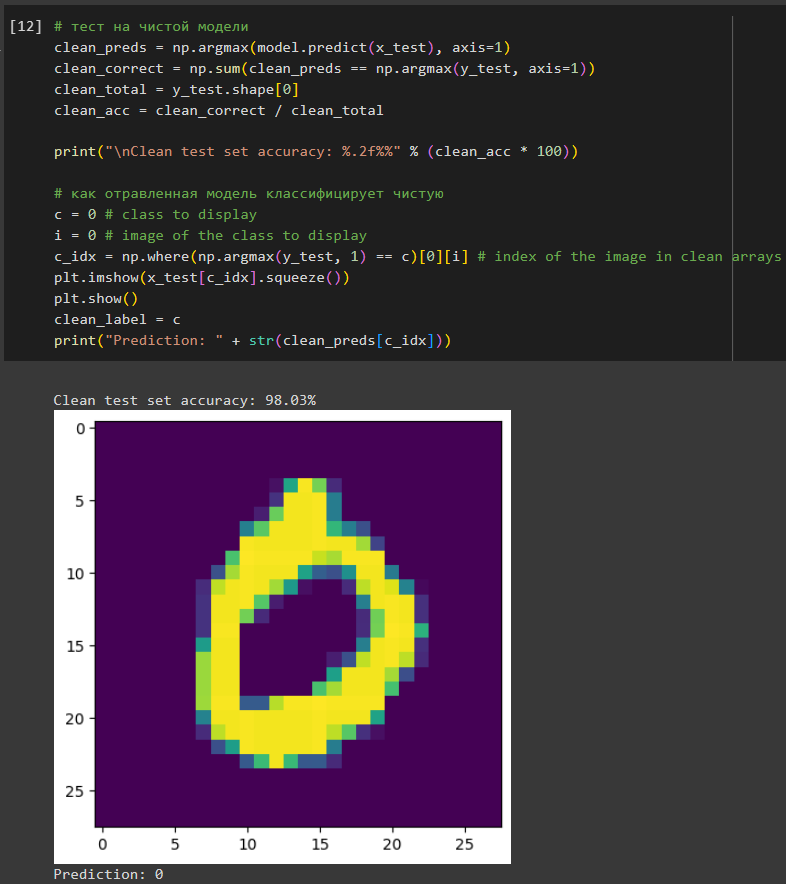
1. Создадим отравленные примеры данных и отобразим одно из отравленных



1. Обучим модель на отравленных данных



1. Выполним проверку работы модели в обычных условиях на чистых данных



1. Проверим работу модели на отравленных данных

