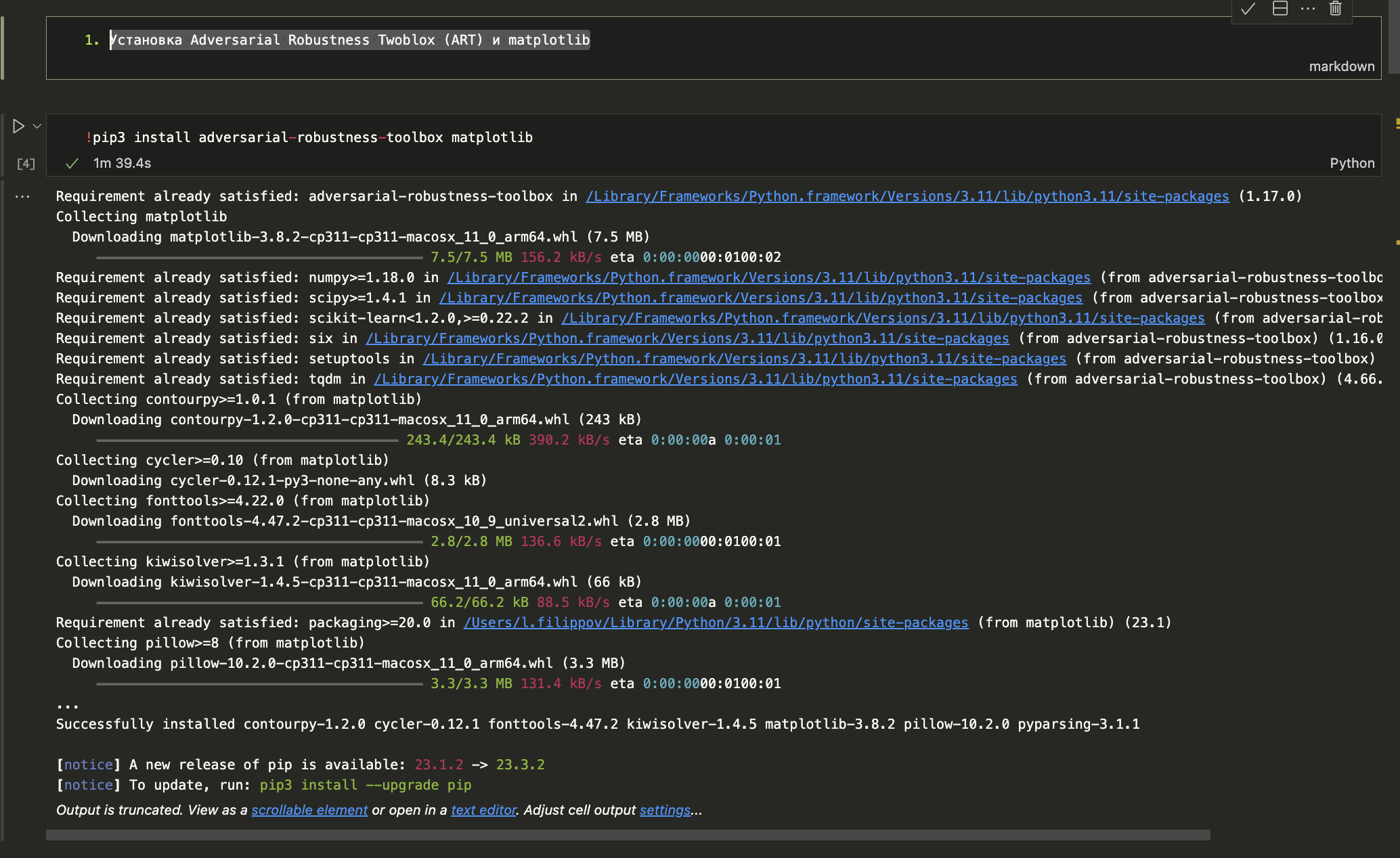
**ББМО-02-22 Филиппов Л.А**

**«Анализ защищенности систем искусственного интеллекта»**

**Практическая работа 4**

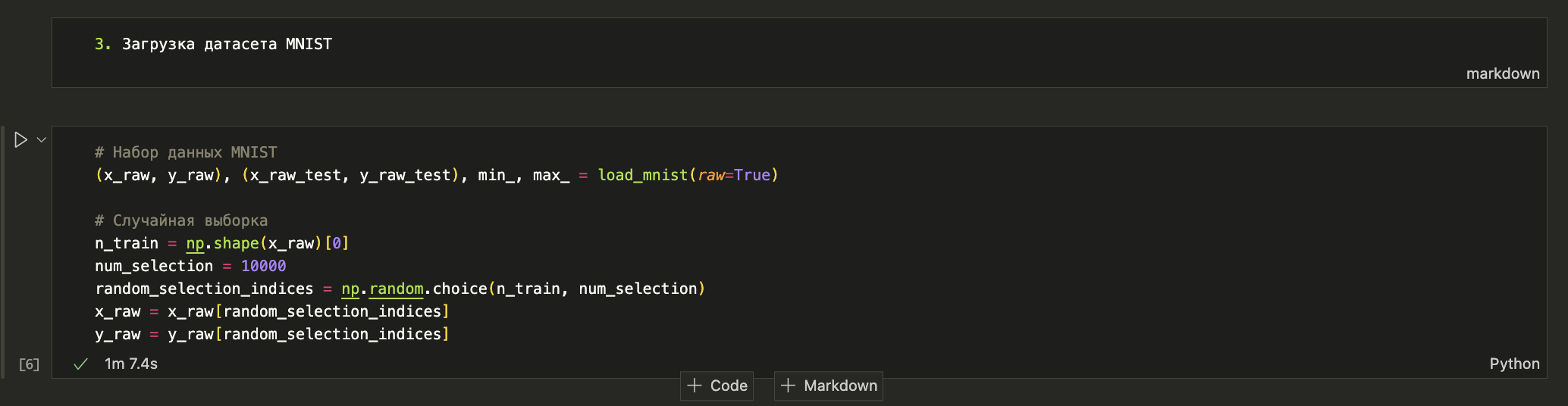
1. Установка Adversarial Robustness Twoblox(ART) и matplotlib



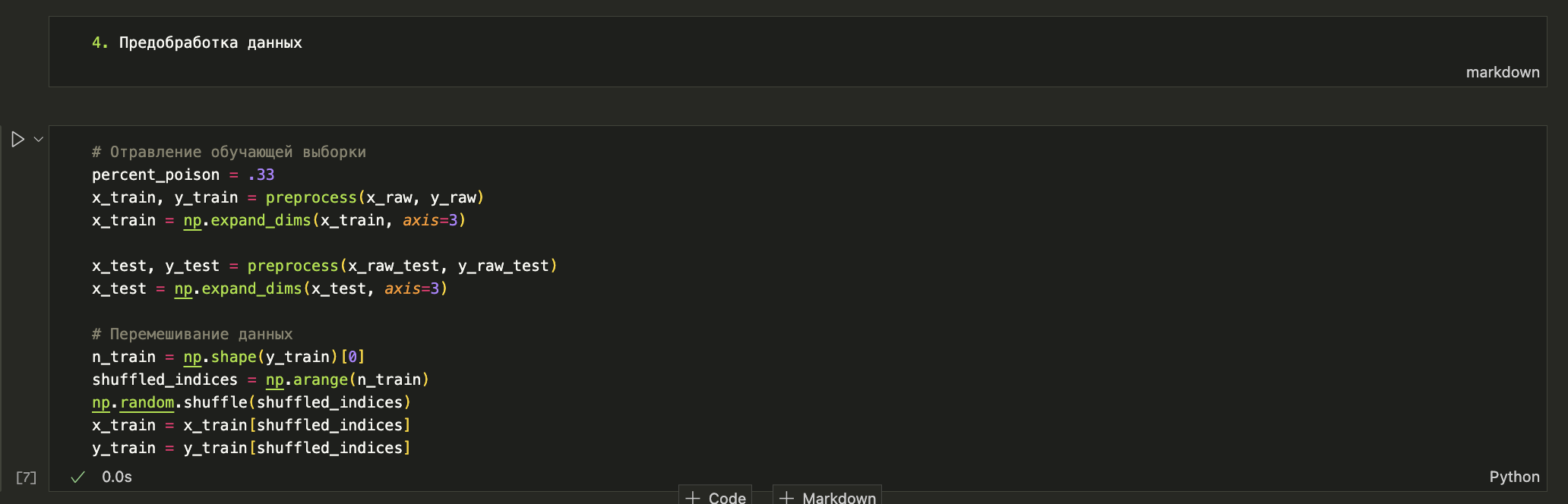
1. Импорт необходимых библиотек



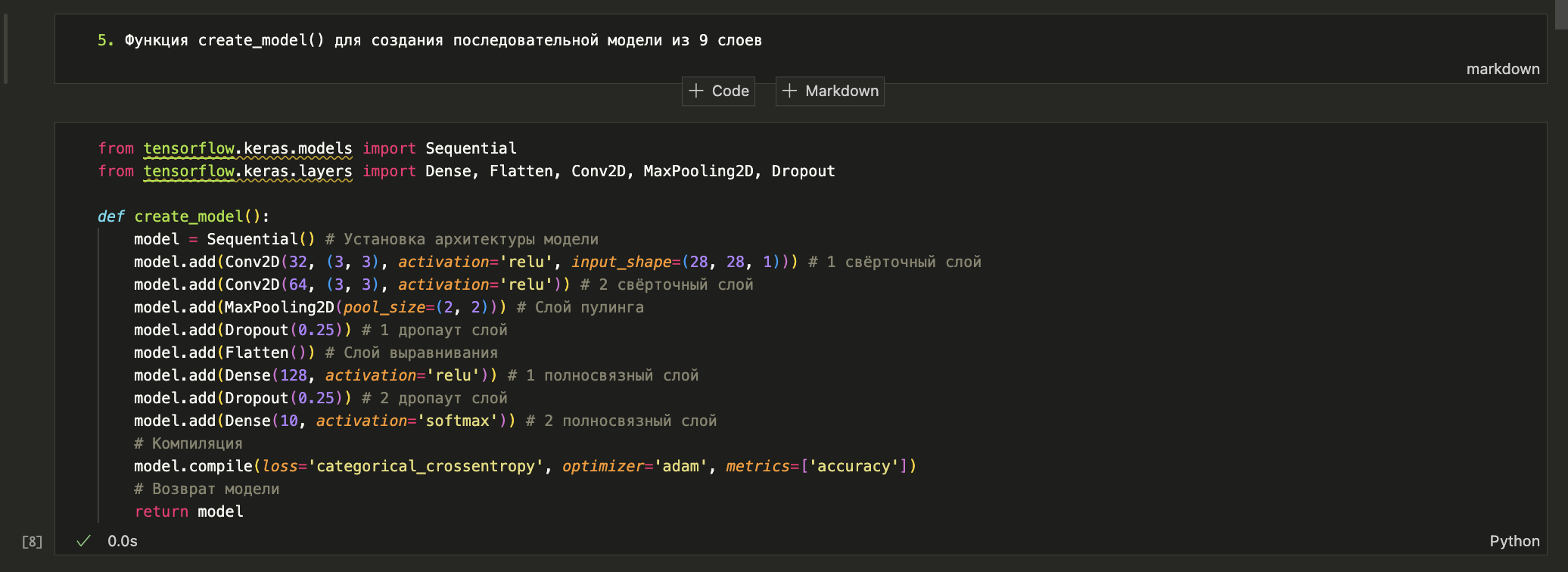
1. Загрузка датасета MNIST



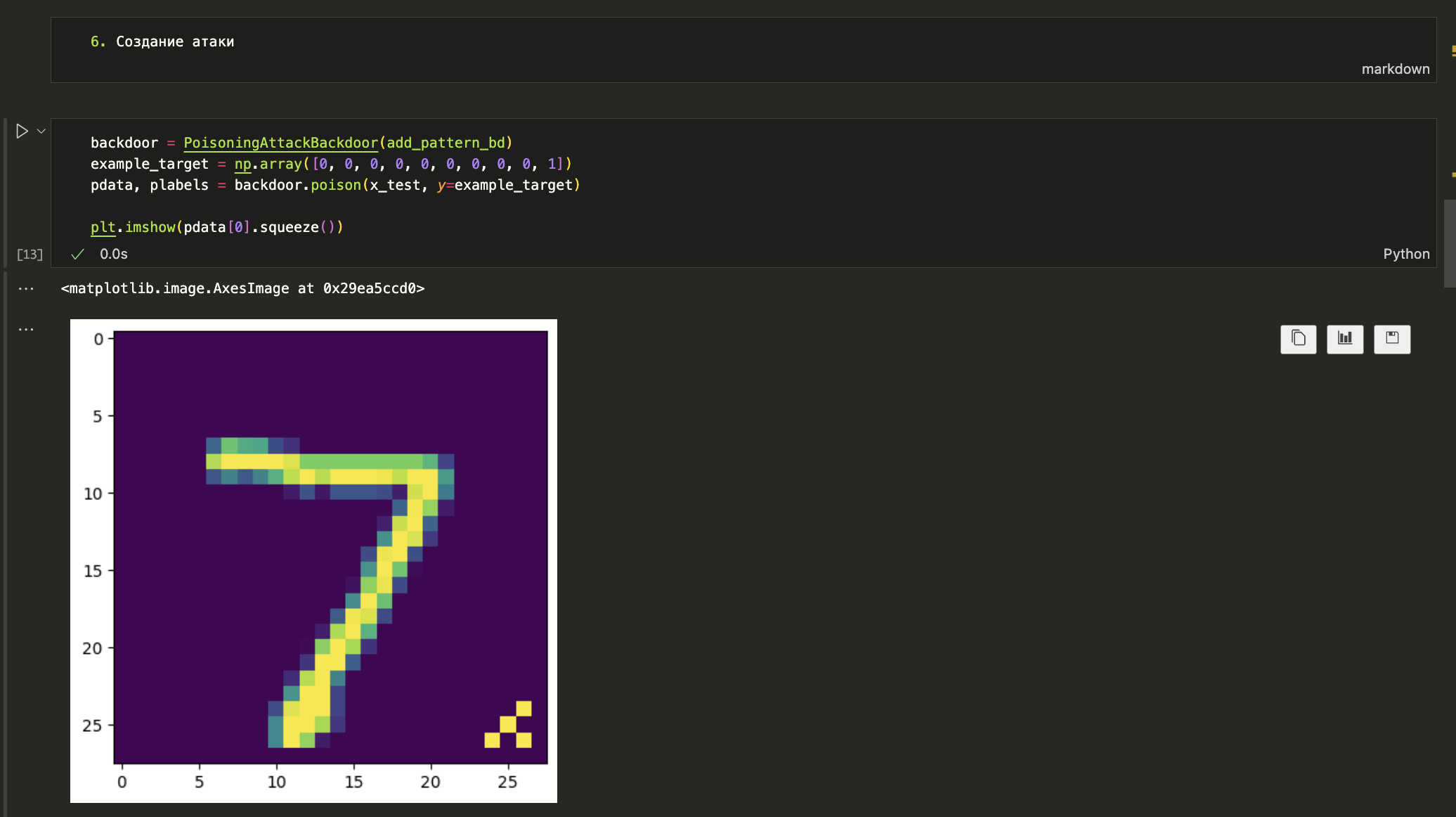
1. Предобработка данных



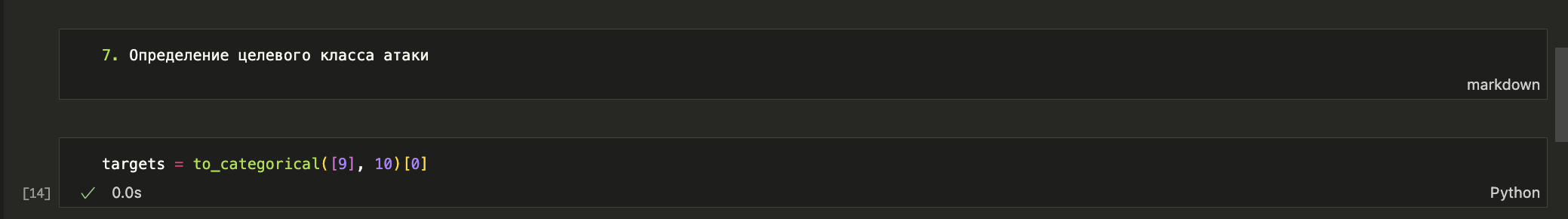
1. Функция create\_model() для создания последовательности из 9 слоев



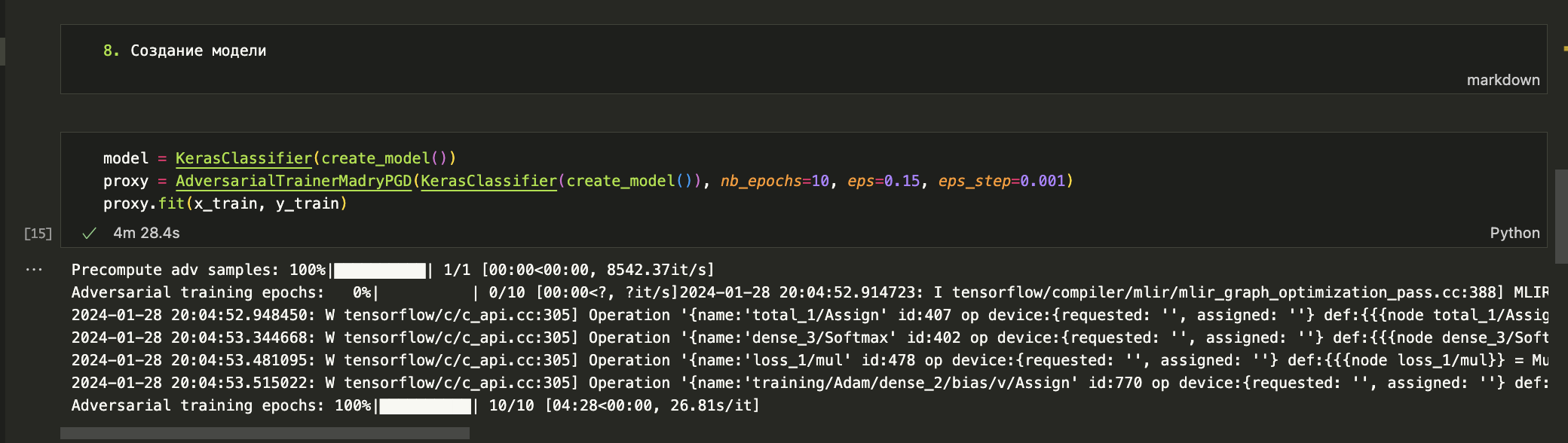
1. Создание атаки



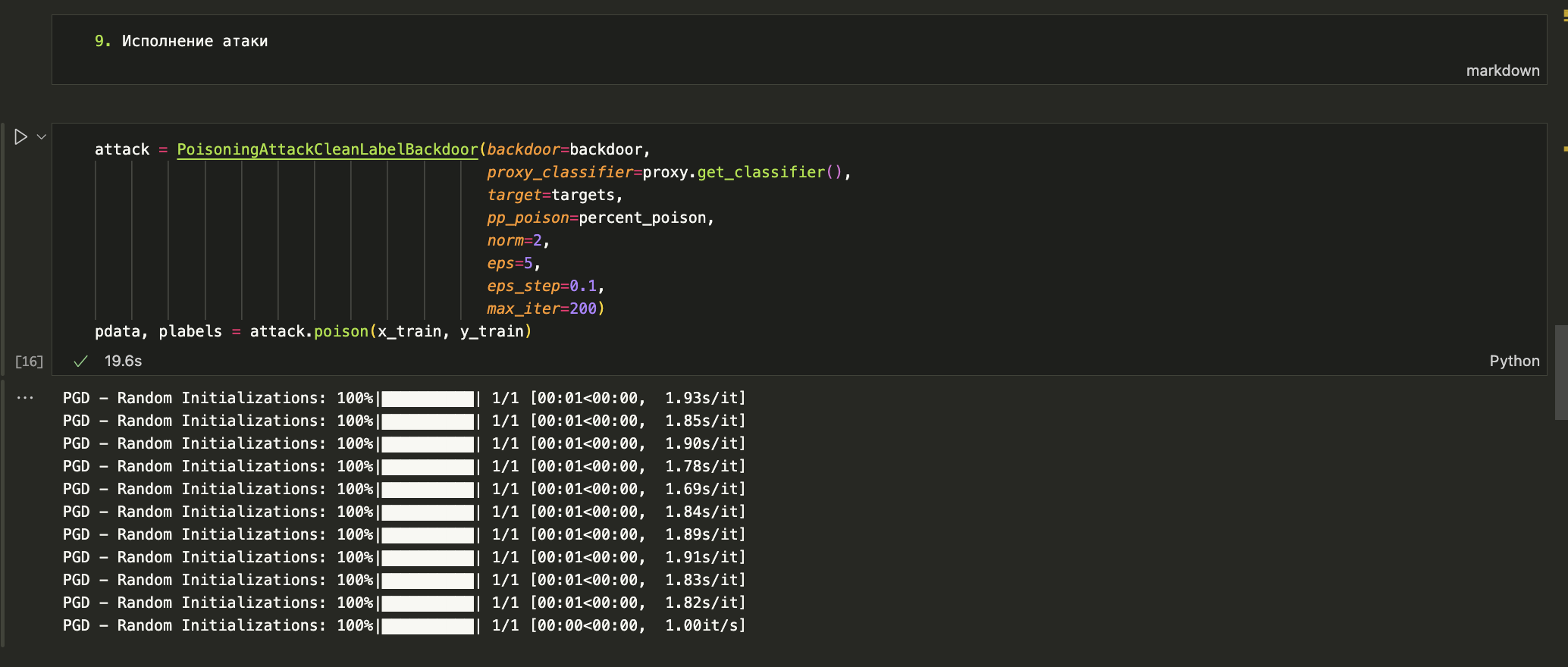
1. Определение целевого класса атаки



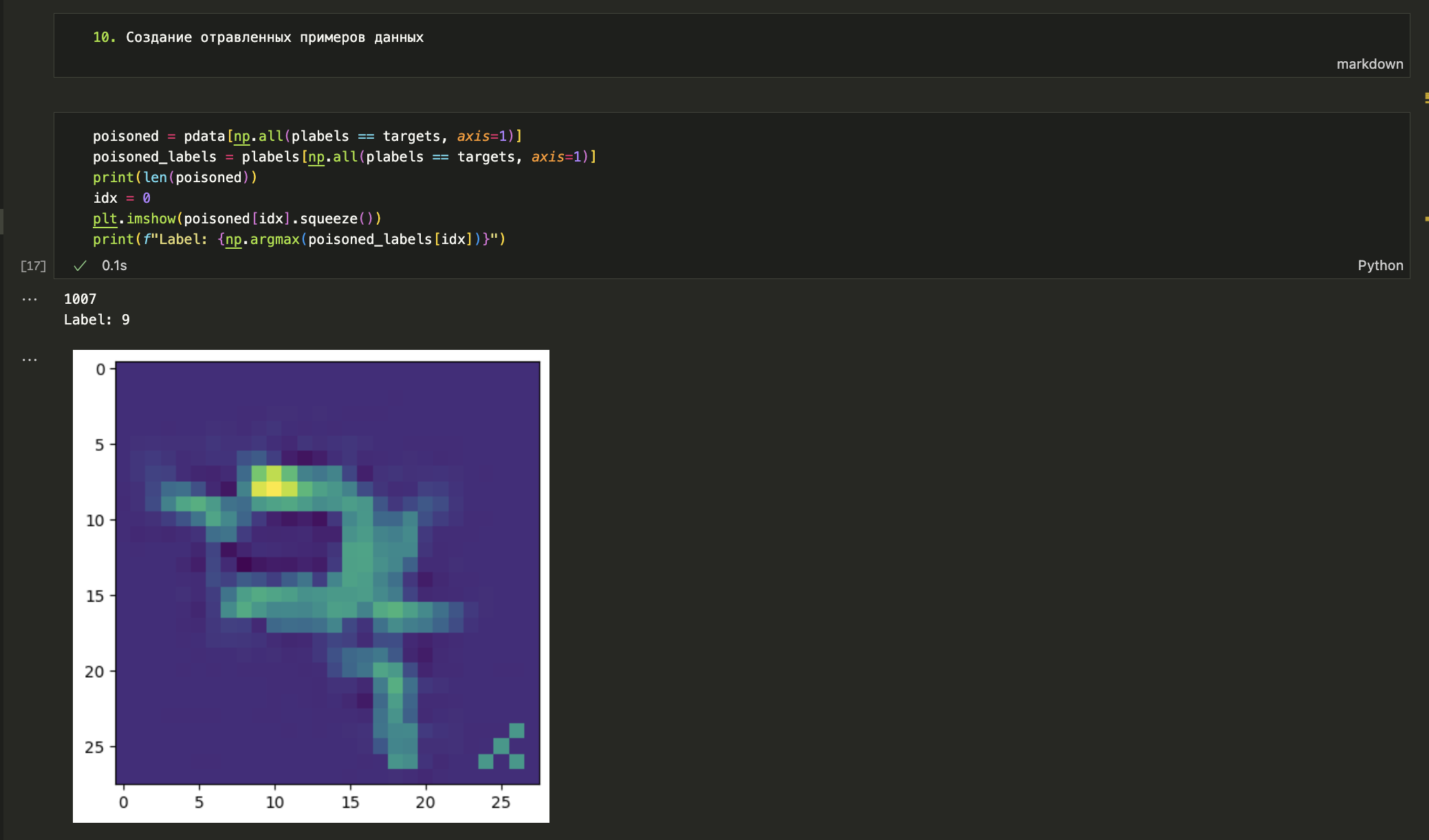
1. Создание модели



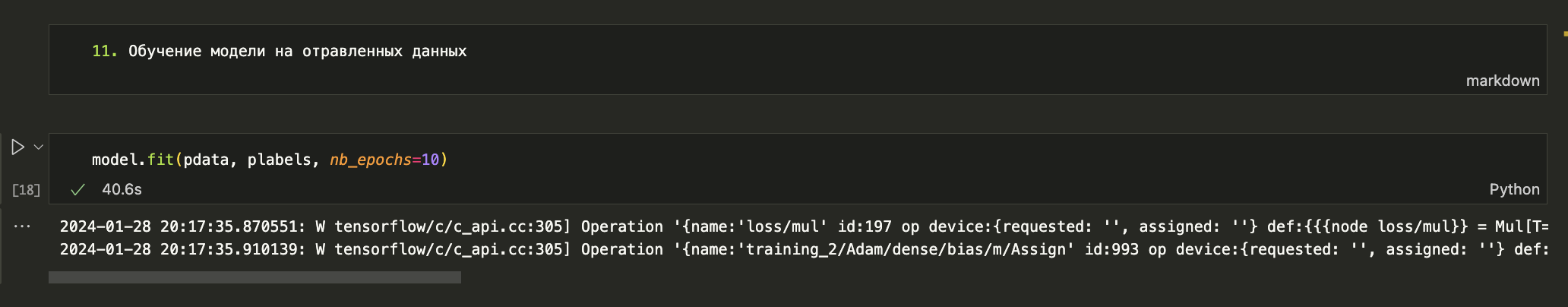
1. Исполнение атаки



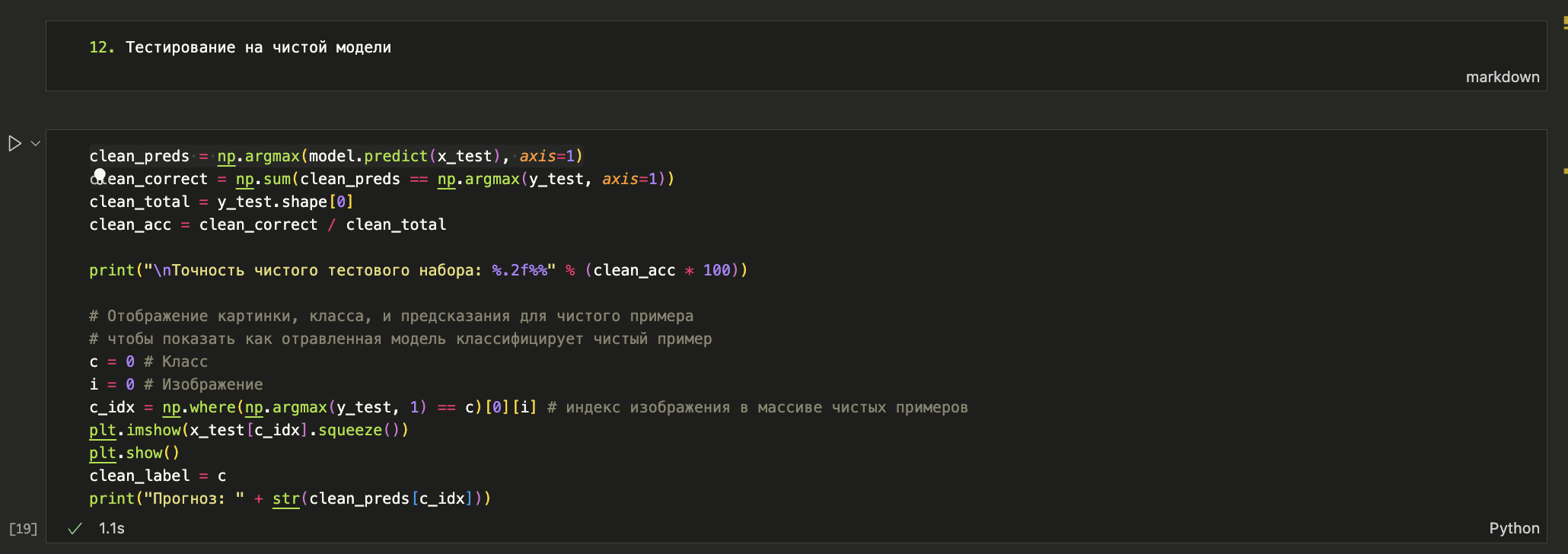
1. Создание отравленных примеров данных

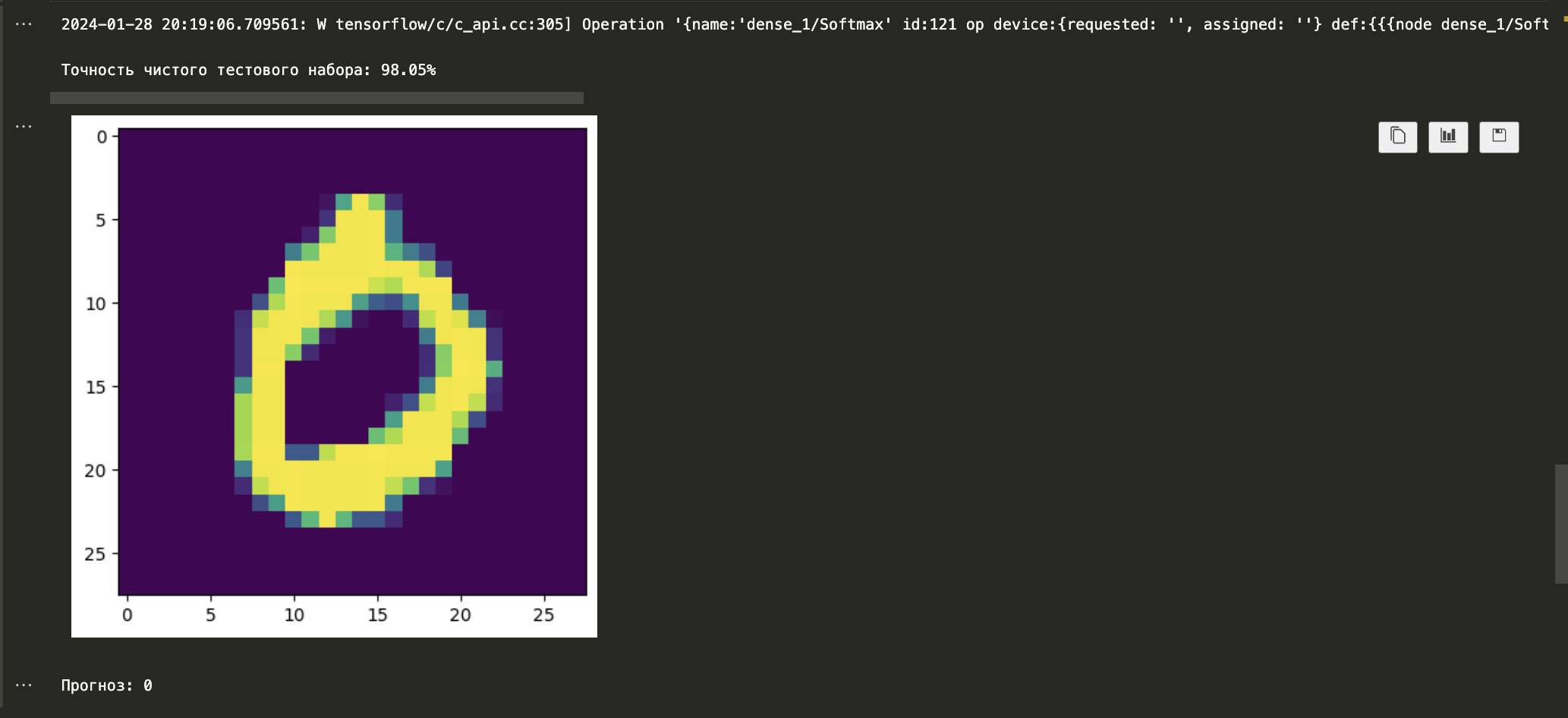


1. Обучение модели на отравленных данных



1. Тестирование на чистой модели





1. Получение результатов атаки на модель

