Изображение выглядит как текст, коллекция картинок

Автоматически созданное описание

МИНОБРНАУКИРОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА**— **Российский технологический университет»**

**РТУМИРЭА**

Институт кибербезопасности и цифровых технологий направление 10.04.01 «Информационная безопасность»

Кафедра КБ-4«Интеллектуальные системы информационной безопасности»

**Лабораторная работа №1**

По дисциплине

«Анализ защищенности систем искусственного интеллекта»

Выполнил:

Суслов Антон Константинович

Группа: ББМО-02-22

Москва 2023

Ход работы:

1. Клонирование репозитория

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Загрузка библиотек и установка значения переменной rand\_seed(номер по списку)

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Загрузка датасетов MNIST и Cifar-10

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Настройка и загрузка DataLoader

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Настройка модели

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

1. Загрузка и оценка стойкости модели LeNet к FGSM и DeepFool атакам, также загрузка и оценка стойкости модели LeNet к FGSM и DeepFool атакам

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

1. Оценка атакующих параметров

Изображение выглядит как текст, снимок экрана, черно-белый

Автоматически созданное описание

Изображение выглядит как текст, черно-белый, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

1. Влияние параметров fgsm\_esp для LeNet на датасетах MNIST и Cifar-10

Изображение выглядит как текст, снимок экрана, Шрифт, меню

Автоматически созданное описание

Вывод: параметр fgsm\_esp влияет на искажение изображения, чем выше параметр, тем искажение больше.