

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

----------------------------------------------------------------------------------------------------

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

----------------------------------------------------------------------------------------------------

**Отчет по практике**

По дисциплине

«Анализ защищенности систем искусственного интелекта»

Тема: «Практика 6: Атака по переносу (Transfer Attack) на модели ИИ »

Студент Макаров Павел Андреевич

Группа ББМО-02-23

Работу проверил

Спирин А.А.

Москва, 2024











