Отзыв научного руководителя

на бакалаврскую работу студента 4 курса факультета ПМ-ПУ СПбГУ Киндулова Михаила Львовича на тему «Модели машинного обучения, устойчивые к состязательным атакам».

Бакалаврская работа Киндулова М. Л. посвящена такому актуальному направлению в области информационной безопасности, как защита методов и технологий машинного обучения от состязательных атак.

Целью выпускной квалификационной работы было построение алгоритма, позволяющего обнаруживать атакованные объекты. Киндулов М.Л. приводит краткий обзор известных типов состязательных атак и защит от них. Автор также предлагает собственный подход, для демонстрации работы которого используются нейронная сеть ResNet-18, атаки DeepFool, FSGM и набор данных CIFAR-10. Для тестирования предложенного подхода выбраны наборы данных CIFAR-10 и MNIST.

В ходе выполнения выпускной квалификационной работы ее автор показал достаточный уровень теоретических знаний, полученных в процессе обучения, для полноценного применения их на практике, умение самостоятельно ставить и решать прикладные задачи, хорошую подготовку в области современных подходов машинного обучения. Предложенный подход показал высокую точность и универсальность. При анализе метода были выявлены его сильные и слабые стороны.

На основании вышеизложенного считаю, что выпускная квалификационная работа Киндулова М. Л. выполнена в соответствии с предъявленными требованиями и заслуживает оценки «отлично».

Научный руководитель,
доктор физ.-мат. наук,
профессор  Крылатов А. Ю.