



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

УТВЕРЖДАЮ

Проректор РТУ МИРЭА

О. Е. Винокуров

2024 г.



ОТЗЫВ

на автореферат диссертации Зиядинова Вадима Валерьевича на тему
«Оптимизация помехоустойчивости и точности нейросетевого распознавания
изображений», представленной на соискание
учёной степени кандидата технических наук по специальности 2.2.13
«Радиотехника, в том числе системы и устройства телевидения»

Исследования, направленные на повышение устойчивости свёрточных нейронных сетей к различного рода искажениям в изображениях, в том числе состязательным, несомненно являются актуальными. Аппараты распознавания изображений на основе нейронных сетей становятся неотъемлемой частью множества процессов и технологий, применяются в различных областях, таких как медицина, финансы, технологии автоматизированного производства и многих других. При этом свёрточные нейронные сети обладают некоторыми недостатками, в том числе наличием уязвимостей, которые могут ограничить

Вход. № 63/ау
«30» 05 2024.
подпись

применимость нейронных сетей, если не будут устранены. Повышение устойчивости нейронных сетей к искажениям способствует развитию безопасности в различных сферах применения, обеспечивая защиту от сбоев и злонамеренных вторжений. Это позволит улучшить качество работы систем и повысить доверие к аппаратам на основе искусственного интеллекта. Таким образом, актуальность работы по повышению устойчивости нейронных сетей, проведенной автором, неоспорима и имеет большое значение для обеспечения безопасности и надежности применения нейронных сетей в будущем.

Автором опубликовано 19 работ по теме диссертации, из них 9 публикаций в изданиях, входящих в перечень ВАК при Минобрнауки РФ или индексируемых в международных базах данных WoS и Scopus (в т. ч. 3 в журналах Q1) и 9 свидетельств об официальной регистрации программы для ЭВМ. Материалы диссертации обсуждались на четырех научно-технических конференциях.

Основные результаты работы автора следующие:

1. автором разработаны математические модели, позволяющие оценить характеристики устойчивости СНС к искажениям;
2. автором получена зависимость точности распознавания изображений от интенсивности искажений в обучающем наборе данных. Предположено и доказано существование оптимальной интенсивности искажений в обучающем наборе данных и показано, что определение этого оптимума может быть выполнено с помощью статистического моделирования;
3. автором доказано, что существует оптимальный способ аугментации обучающего набора данных для повышения устойчивости нейронных сетей;
4. автором предложен метод повышения устойчивости глубоких свёрточных нейронных сетей к высокочастотным атакам.

Можно выделить следующие недостатки:

1. в разделе 5 автором рассмотрены только методы противостояния высокочастотным искажениям (состязательная атака FGSM), при этом не

принято во внимание влияние низкочастотных искажений, таких как искажения цветового пространства, яркости и контраста изображения;

2. подписи к рисункам 1, 2 и 3 автореферата оформлены неверно — после рисунка следует оставлять одну строку отступа;

3. из автореферата не ясно, рассматривает ли автор типы нейронных сетей, отличные от свёрточных.

Общая оценка диссертации положительная. Работа «Оптимизация помехоустойчивости и точности нейросетевого распознавания изображений» соответствует требованиям к диссертации на соискание ученой степени кандидата технических наук, указанным в «Положении о порядке присуждения ученых степеней» (постановление Правительства №842 от 24.09.2013 в актуальной редакции). Автор работы «Оптимизация помехоустойчивости и точности нейросетевого распознавания изображений» Зиядинов Вадим Валерьевич заслуживает присуждения ученой степени кандидата технических наук по специальности 2.2.13 «Радиотехника, в том числе системы и устройства телевидения».

Ведущий научный сотрудник
Научно-инжинирингового центра
специальной радиосвязи
и радиомониторинга РТУ МИРЭА, д.т.н.



А. В. Николаев

Специальность, по которой защищался автор отзыва Николаев Алексей Витальевич, 05.12.13 – Системы, сети и устройства телекоммуникаций.


Почтовый адрес: 119454, г. Москва, проспект Вернадского, д. 78

Тел.: +7 (499) 600-80-80, доб. 24056

e-mail: nauka@mirea.ru

Подпись А.В. Николаева
Заверено

Проректор РТУ МИРЭА



О. Е. Винокуров