

Отзыв

на автореферат диссертационной работы

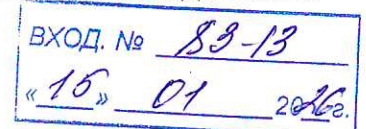
Лушникова Никиты Дмитриевича

на тему «Модели и алгоритмы мультимодальной биометрической аутентификации на основе сверточной нейронной сети»,
представленную на соискание ученой степени кандидата технических наук
по специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность

1. Актуальность темы научно-квалификационной работы (диссертации)

Стремительное развитие технологий генеративного искусственного интеллекта в последние несколько лет привело к возникновению нового класса угроз информационной безопасности, связанных с возможностью правдоподобной имитации (спуфинг, дипфейки) злоумышленником основных биометрических признаков человека. Так, по данным отчета компании Resemble AI, только за первый квартал 2025 года прямые финансовые потери от атак с применением дипфейков превысили 200 млн долларов. При этом резко сократилась потребность в сборе исходных данных для проведения атаки. Так, например, для генерации правдоподобного изображения лица достаточно одного изображения, а для копирования голоса всего 3-5 секунд аудиозаписей, что обеспечивает совпадение тембра на 85%.

В то же время, применяемые одномодальные технологии противодействия биометрическому спуфингу при переходе от лабораторных к реальным условиям окружения демонстрируют снижение эффективности до 45–50% (способность человека распознать подделку не превышает 55–60%). Однако подходы, основанные на объединении признаков лица, голоса и поведенческих характеристик обеспечивают существенное повышение качества классификации биометрических образцов в условиях реального времени и являются наиболее перспективным направлением исследования.



Таким образом, разработка мультимодальных систем аутентификации приобретает не только прикладное, но и фундаментальное значение.

2. Обоснованность научных положений, выводов, сформулированных в НКР (диссертации)

Автореферате представлены следующие новые научные результаты:

1. Модель биометрической аутентификации пользователей информационной системы по изображению лица в составе мультимодальной биометрической системы с применением предварительной обработки изображения лица.

2. Модель биометрической аутентификации пользователей информационной системы по голосу в составе мультимодальной биометрической системы с применением предварительной шумоочистки данных.

3. Алгоритмы обучения сверточной нейронной сети в составе мультимодальной системы биометрической аутентификации.

4. Мультимодальная система биометрической аутентификации пользователей информационной системы, реализующая разработанные модели и алгоритмы.

3. Достоверность основных выводов и результатов, выносимых на защиту

Достоверность результатов диссертационного исследования, представленных в автореферате, обеспечивается:

— использованием основных принципов системного подхода при постановке научной задачи;

— корректным применением методов системного анализа (абстрагирование, декомпозиция, формализация, анализ и синтез) для решения задач биометрической аутентификации;

- применением апробированных математических методов и архитектур машинного обучения при решении научной задачи;

Достоверность полученных результатов подтверждается:

- соответствием экспериментальных результатов теоретическим выводам; непротиворечивостью полученных результатов с известными научными работами в данной предметной области;

- использованием как общедоступных датасетов, так и авторского набора данных.

- апробацией полученных результатов в научно-рецензируемых изданиях и их публичным представлением на научно-практических конференциях.

4. Теоретическая значимость, научная и практическая ценность результатов исследования

Теоретическая значимость диссертационной работы заключается в развитии моделей и алгоритмов мультимодальной биометрической аутентификации пользователей информационных систем на основе совместного использования признаков изображения лица и голоса с применением методов предварительной обработки и сверточных нейронных сетей. В работе обоснована целесообразность конкатенации биометрических признаков разной природы и показана роль предварительной шумоочистки и фильтрации (в частности, с использованием фильтра Калмана) в повышении помехоустойчивости и снижении ошибок первого и второго рода.

Научную ценность представляют предложенные алгоритмы обучения нейронных сетей, ориентированные на извлечение дополнительных визуальных и акустических дескрипторов, а также учет динамических характеристик лица, что расширяет теоретические представления о способах повышения устойчивости биометрических систем к подделкам, реализуемым с применением дипфейк-технологий.

Практическая значимость работы состоит в разработке и программной реализации мультимодальной системы биометрической аутентификации пользователей, обеспечивающей высокую точность распознавания и апробированной в реальных условиях эксплуатации. Полученные модели и алгоритмы могут быть использованы при проектировании и внедрении систем аутентификации и разграничения доступа в корпоративных и ведомственных информационных системах для повышения надежности идентификации пользователей и устойчивости к современным атакам на биометрические системы.

5. Характеристика опубликованных работ по теме диссертации

Основные научные результаты диссертации Лушникова Никиты Дмитриевича получены лично автором, что подтверждается их отражением в тексте автореферата, программными реализациями предложенных алгоритмов, а также апробацией результатов на российских и международных научно-технических конференциях.

Всего о материалах диссертационного исследования опубликовано 30 научных работ, в том числе 7 статей в рецензируемых журналах, рекомендованных ВАК РФ (из них: 6 статей категории К2 и 1 статьи категории К3), 1 статья в изданиях RSCI, 3 публикации в журналах, индексируемых Web of Science и Scopus; получено 3 свидетельства о государственной регистрации программ для ЭВМ, опубликовано 16 работ в трудах международных и всероссийских конференций.

6. Общая характеристика НКР (диссертации), замечания и недостатки

Автореферат написан четким, лаконичным языком, достаточно подробно иллюстрирован и обладает внутренним единством. Представленные результаты экспериментальных исследований позволяют сделать вывод о достижении цели, поставленной в диссертационном исследовании.

Тем не менее, следует отметить отдельные недостатки:

1. В автореферате не приведены оценки результативности предложенных методов по сравнению с наиболее современными подходами к анализу биометрии и распознаванию дипфейков на основе архитектуры визуальных трансформеров, методов распознавания живости с применением самообучения на основе видео, сквозного антиспуфинга и т. д., что несколько снижает универсальность выводов.

2. Заявленная высокая точность мультимодальной системы не сопровождается подробным анализом обобщающей способности моделей на перекрестных датасетах и сценариях сдвига домена, при которых распределение данных, на которых модель обучалась, отличается от распределения данных, на которых она применяется, что критично для биометрических систем промышленного уровня. Возникает вопрос: насколько верифицируемы заявленные показатели ($FRR = 0,11\%$, $FAR = 0,01\%$)?

3. Предложенный в работе способ конкатенации биометрических признаков с равнозначным вкладом модальностей не предусматривает механизмов адаптивного взвешивания в зависимости от качества входных данных (условия освещенности, уровень акустического шума, особенности канала записи). Это может приводить к снижению устойчивости мультимодальной системы в условиях реальной эксплуатации при деградации одной из модальностей.

Отмеченные недостатки в целом не влияют на высокую оценку научного уровня проведенных исследований и позволяют сделать положительный вывод о качестве результатов выполненной диссертационной работы Лушников Никиты Дмитриевича.

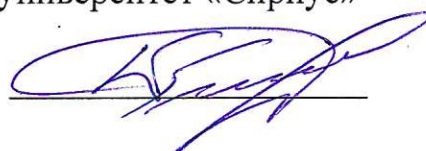
7. Заключение

Представленные в автореферате сведения позволяют сделать вывод о том, что диссертационная работа Лушников Никиты Дмитриевича выполнена на актуальную тему, обладает научной новизной, теоретической и

практической значимостью, прикладной ценностью полученных результатов, выполнена лично соискателем и имеет заверченный характер. Автореферат полностью удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, соответствует п. 9-11, п. 13, 14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (с изменениями и дополнениями), а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Гнидко Константин Олегович

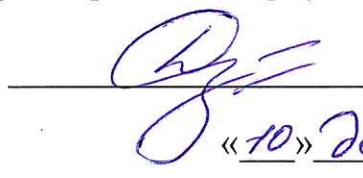
доктор технических наук, доцент, заместитель руководителя научной группы
Научного центра информационных технологий и искусственного интеллекта,
АНОО ВО Научно-технологический университет «Сириус»



Гнидко К.О.

Петренко Сергей Анатольевич

доктор технических наук, профессор, руководитель научной группы Научного
центра информационных технологий и искусственного интеллекта,
АНОО ВО Научно-технологический университет «Сириус»


«10» декабря 2025 г.

Петренко С.А.

Адрес места основной работы:

354340, РФ, Краснодарский край, ФТ «Сириус», Олимпийский проспект, д. 1,
АНОО ВО «Научно-технологический университет «Сириус»

Рабочий телефон: 8 (862) 241 98 44

Адрес эл. почты: gnidko.ko@talantiuspeh.ru, petrenko.sa@talantiuspeh.ru

Даю согласие на включение моих персональных данных в документы, связанные с защитой Лушникова Никиты Дмитриевича и их дальнейшую обработку.

 Гнидко К.О.

Даю согласие на включение моих персональных данных в документы, связанные с защитой Лушникова Никиты Дмитриевича и их дальнейшую обработку.

 Петренко С.А.

Подписи Гнидко К.О. и Петренко С.А. заверены



22.12.2025

 Косуля И.С.