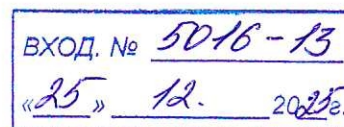


ОТЗЫВ

официального оппонента

доктора технических наук, доцента Шакурского Максима Викторовича
на диссертационную работу Лушников 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

Актуальность темы диссертации обусловлена стремительным ростом числа киберугроз и постоянно повышающимися требованиями к защите персональных данных в цифровой среде. Повсеместное внедрение биометрии, как инструмента аутентификации приводит к повышенному интересу злоумышленников к алгоритмам взлома данных систем. В этих условиях развитие систем противодействия возможным угрозам фальсификации биометрических образов, в том числе и с применением искусственного интеллекта, является безусловно актуальной задачей. Особенно перспективными считаются мультимодальные системы, сочетающие несколько биометрических признаков (например, лицо и голос), что значительно повышает устойчивость к спуфинг-атакам, включая современные дипфейки. При этом остаются актуальными задачи повышения помехоустойчивости, снижения ошибок распознавания и защиты от подделки биометрических данных. Современное законодательство стимулирует развитие сертифицированных и защищенных биометрических решений. Таким образом, разработка надежной, адаптивной и юридически соответствующей мультимодальной системы аутентификации на основе нейронных сетей представляет собой научно и практически значимую задачу.



Оценка структуры и содержания работы

Работа состоит из введения, четырех глав, заключения, списка литературы и приложений. Общее количество страниц – 188, включая 62 рисунка, 10 таблиц и 3 приложения. Список использованных источников состоит из 128 наименований.

Во введении обоснована актуальность исследования, определены его цель и задачи, а также обозначены элементы научной новизны и практическая ценность полученных результатов.

Первая глава посвящена анализу современного состояния исследований в области биометрической аутентификации пользователей на основе нейронных сетей. Рассмотрены нормативно-правовые основы, включая российские и международные стандарты, а также ГОСТ Р 54411–2018 по мультимодальным технологиям. Описаны ключевые методы биометрической идентификации – как по изображению лица (методы Виолы–Джонса, LBP, HOG, ORB), так и по голосу (MFCC, LPC, PLP и др.). Особое внимание уделено мультимодальным и мультибиометрическим системам, которые повышают надежность распознавания за счет объединения нескольких биометрических признаков. Проанализированы уровни объединения данных (от признаков до принятия решений) и способы снижения корреляции между модальностями. Также подчеркивается роль нейронных сетей и методов машинного обучения в повышении точности аутентификации. Обоснована необходимость разработки эффективной мультимодальной системы на основе нейросетевых технологий.

Вторая глава посвящена разработке и исследованию модели распознавания пользователей информационной системы по изображению лица. Рассмотрены методы предварительной обработки изображений, включая морфологические преобразования и фильтрацию, а также извлечение признаков с использованием гистограмм ориентированных градиентов (HOG) и локальных бинарных шаблонов (LBP). Предложена архитектура сверточной нейронной сети, обученной на собственном датасете, и проведено сравнение ее эффективности с известными архитектурами (ResNet, AlexNet, FeatherNet,

YOLO). Особое внимание уделено применению адаптивного фильтра Калмана для подавления цифрового шума, что позволило достичь высоких показателей качества (в работе указано $MSE = 0,0019$, $PSNR = 27,39$ дБ). Разработан программный модуль, способный противодействовать атакам с использованием дипфейков и распечатанных изображений. Модель протестирована в режиме реального времени на видеопотоке и показала высокую точность распознавания (до 98,14%) при низких ошибках первого и второго рода. В целом, глава демонстрирует комплексный подход к повышению надежности и точности биометрической аутентификации на основе лиц.

Третья глава посвящена разработке и исследованию модели распознавания пользователей информационной системы по голосу. Рассмотрены ключевые акустические признаки – мел-частотные кепстральные коэффициенты (MFCC), коэффициенты линейного предсказания (LPC), перцепционные коэффициенты (PLP), а также дополнительные признаки: Q-константные кепстральные коэффициенты (CQCC) и частота спектрального центроида (SCF). Описана процедура предварительной обработки речевого сигнала, включая шумоочистку методом RASTA и нормализацию спектральных характеристик. На основе собственного датасета из 450 аудиозаписей двух пользователей разработаны две архитектуры нейронных сетей – с разным набором входных признаков – и проведено их обучение. Особое внимание уделено защите от синтезированных голосов (дипфейков) за счет извлечения дополнительных речевых дескрипторов. Модель показала высокую точность: ошибка ложного отказа (FRR) составила 0,11%, ошибка ложного принятия (FAR) – 0,01%. В целом, глава демонстрирует комплексный подход к построению надежной голосовой биометрической системы в составе мультимодальной аутентификации.

Четвертая глава посвящена апробации разработанных моделей распознавания по лицу и голосу, а также созданию и оценке эффективности мультимодальной системы биометрической аутентификации на основе конкатенации векторов признаков и сверточной нейронной сети. Описаны этапы

интеграции признаков – DLBP и HOG для изображений лица, MFCC, LPC, PLP, CQCC и SCF для голоса – и их объединение в единый вектор размерностью 512. Приведены результаты тестирования: точность распознавания по лицу достигла 98,14%, по голосу – $FRR = 0,11\%$ и $FAR = 0,01\%$. На основе конкатенации модальностей достигнута общая точность 99,31% при функции потерь 0,032. Особое внимание уделено защите от дипфейков – как визуальных, так и синтезированных голосов. Разработан программный комплекс с использованием Python и библиотек OpenCV, Librosa, Dlib и др., реализующий полный цикл аутентификации. Глава завершается выводом о высокой надежности и помехоустойчивости предложенной мультимодальной системы.

В заключении приведены основные результаты диссертационного исследования.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Научные положения, выводы и рекомендации, сформулированные в диссертации, обоснованы как теоретически, так и экспериментально. Соискатель опирается на действующие нормативно-правовые акты, а также на международные стандарты (NIST), что обеспечивает соответствие разработок современным требованиям в области биометрической аутентификации. Полученные результаты соответствуют заявленным автором пунктам (12 и 15) паспорта научной специальности 2.3.6 Методы и системы защиты информации; информационная безопасность.

Достоверность полученных результатов подтверждается корректностью примененных методов математического и компьютерного моделирования, включая использование проверенных признаков пространств, адаптивной фильтрации на основе фильтра Калмана и современных архитектур сверточных нейронных сетей. Экспериментальные данные согласуются с теоретическими оценками и демонстрируют высокую воспроизводимость на собственных датасетах. Все выносимые на защиту положения строго обоснованы с точки зрения теории машинного обучения, биометрической аутентификации,

нормативно-правовых требований и принципов построения устойчивых к дипфейк-атакам мультимодальных систем.

Научная новизна полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертационной работе, заключаются в разработке моделей и алгоритмов биометрической аутентификации пользователей информационной системы на основе изображения лица и голоса, а также в создании мультимодальной системы, объединяющей эти модальности через конкатенацию векторов признаков и обучение сверточной нейронной сети. К новым научным результатам, полученным в исследовании, следует отнести следующие:

1. Предложена модель биометрической аутентификации по изображению лица, в которой для повышения помехоустойчивости в условиях мультимодальной системы применяется предварительная обработка изображений с использованием адаптивного фильтра Калмана.

2. Создана модель биометрической аутентификации по голосу, основанная на комбинированном подходе: применении метода шумоподавления и расширенном наборе акустических признаков, что обеспечивает снижение вероятностей ложного отказа и ложного принятия в мультимодальной системе.

3. Разработан алгоритм обучения сверточной нейронной сети для распознавания пользователей по лицу в составе мультимодальной системы, особенностью которого является извлечение дополнительных изобразительных дескрипторов, повышающих устойчивость к атакам с использованием поддельных изображений (дипфейков).

4. Предложен алгоритм обучения сверточной нейронной сети для распознавания пользователей по голосу в мультимодальной системе, отличающийся использованием расширенного набора речевых признаков, что способствует эффективному противодействию синтезированным (поддельным) голосам.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость диссертационной работы заключается в развитии научных основ защищенной мультимодальной биометрической аутентификации на основе нейронных сетей с учетом требований современного нормативно-правового регулирования (ФЗ № 572-ФЗ, ГОСТ Р 54411–2018). В работе предложены оригинальные модели извлечения и объединения биометрических признаков – DLBP и HOG для лица, MFCC, LPC, PLP, CQCC и SCF для голоса – в том числе с применением адаптивного фильтра Калмана и метода RASTA-шумоочистки, что способствует повышению устойчивости к шумам и дрейфу характеристик. Разработан новый подход к построению мультимодальной системы на основе конкатенации векторов признаков и сверточной нейронной сети, впервые интегрирующий расширенный набор дескрипторов для противодействия синтезированным атакам (дипфейкам). Это расширяет теорию построения помехоустойчивых и защищенных биометрических систем и вносит вклад в развитие методов надежного машинного обучения, соответствующих требованиям национальных стандартов и практикам информационной безопасности.

Практическая значимость работы обусловлена реализацией комплексного решения для надежной и помехоустойчивой мультимодальной биометрической аутентификации на основе изображения лица и голоса в реальных условиях эксплуатации. Разработанный программный комплекс, обеспечивает высокую точность распознавания, эффективную защиту от атак с использованием дипфейков и распечатанных изображений, а также снижает ошибки первого и второго рода. Применение адаптивного фильтра Калмана и метода RASTA-шумоочистки повышает устойчивость системы к цифровым искажениям и меняющимся условиям захвата данных. Предложенные модели и алгоритмы могут быть интегрированы в системы информационной безопасности, в том числе в банковские приложения, корпоративные платформы

и системы контроля доступа, где требуется не только достоверная верификация личности, но и защита от современных методов биометрического спуфинга.

Замечания по работе

1. В работе не приводится анализ возможных угроз безопасности для разработанного мультимодального метода биометрической аутентификации. Результат рассматривается только в сравнении с известными решениями.

2. Соискатель сформировал собственные датасеты (600 изображений, 450 аудиозаписей), но не обосновал, почему именно такие признаки, как DLBP, HOG, CQCC, SCF и др., были выбраны в совокупности, и не проводится анализ их взаимной корреляции.

3. Терминологические замечания. В главах 2 и 3 термин «ошибка первого/второго рода» используется некорректно: в биометрии корректно говорить о FRR (False Rejection Rate – ложный отказ) и FAR (False Acceptance Rate – ложное принятие), а не о статистических ошибках I/II рода, которые относятся к проверке гипотез.

4. Замечания по оформлению. Рисунки 2.4, 2.14 и 3.7 практически не читаемы. Также в тексте диссертации встречаются повторяющиеся конструкции. Например, «модель распознавания пользователей информационной системы...», что несколько снижает стилистическое разнообразие изложения.

Вышеуказанные замечания не влияют на общую положительную оценку научных результатов выполненного соискателем диссертационного исследования и не снижают ценности полученных результатов.

Заключение

Диссертационная работа Лушникова Никиты Дмитриевича по своей научной новизне, теоретической проработке и практической значимости является законченной научно-квалификационной работой, решающей актуальную задачу биометрической аутентификации в условиях роста киберугроз и распространения технологий синтеза биометрических данных.

Диссертационная работа соответствует требованиям 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, Лушников Никита Дмитриевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Заведующий кафедрой
информационной безопасности,
ФГБОУ ВО «Поволжский
государственный университет
телекоммуникаций и информатики»,
д.т.н., доцент



Шакурский
Максим Викторович
«22» декабря 2025 г.

Докторская диссертация защищена по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Адрес места основной работы: 443090, г. Самара, ул. Московское шоссе, д. 77, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Рабочий телефон: +7(846) 339-11-43

Адрес эл. почты: m.shakurskiy@psuti.ru

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

 Шакурский М.В.

