

УТВЕРЖДАЮ

И.о. проректора по научной
деятельности и цифровизации ФГБОУ
ВО «Казанский национальный
исследовательский технический
университет им. А.Н. Туполева-КАИ»,
кандидат технических наук, доцент
Матвеев С.А.



«15» 12

2025 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ» 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. Актуальность диссертационной работы Лушников Никиты Дмитриевича обусловлена ростом числа киберпреступлений, связанных с подделкой биометрических данных с использованием дипфейк-технологий. Традиционные методы аутентификации (пароли, токены) уязвимы к утере, краже и компрометации, в то время как биометрические системы опираются на уникальные физиологические и поведенческие характеристики человека, что делает их более надежными. Однако даже они подвержены ошибкам первого и второго рода, а также могут быть обмануты с помощью синтезированных

изображений или голоса. Одним из перспективных решений является мультимодальная биометрическая аутентификация, сочетающая несколько признаков – например, лицо и голос, – что значительно повышает устойчивость к атакам. Тем не менее, остаются нерешенными задачи эффективного объединения модальностей, предобработки сигналов от шумов и противодействия современным методам синтеза биометрических данных. Особенно остро стоит проблема обеспечения защиты мультимодальных систем от несанкционированного доступа на основе нейросетевых атак. В этой связи разработка моделей и алгоритмов, способных повысить надежность распознавания пользователей и снизить вероятность подделки, является крайне востребованной. Применение сверточных нейронных сетей, конкатенации признаков и специализированных методов предварительной обработки позволяет существенно улучшить качество аутентификации. Таким образом, диссертационная работа направлена на решение практически значимой задачи повышения уровня информационной безопасности за счет создания устойчивой, точной и защищенной мультимодальной биометрической системы.

Оценка структуры и содержания работы

Диссертационная 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 диссертационной работы, определены цель, задачи, научная новизна и практическая значимость исследования.

Первая глава диссертации посвящена анализу современного состояния исследований в области биометрической аутентификации пользователей на основе нейронных сетей. В ней рассмотрены ключевые нормативно-правовые акты и стандарты, регулирующие использование биометрических данных, включая ГОСТ Р 54411–2018 и Федеральный закон

№ 572-ФЗ. Проведен обзор существующих методов биометрической аутентификации – как по лицу (методы PCA, LBP, HOG, Виолы – Джонса), так и по голосу (MFCC, LPC, PLP, CQCC, спектральный центроид), оценивая их преимущества и недостатки. Особое внимание уделено уязвимостям биометрических систем перед дипфейк-атаками, а также проблемам ошибок первого и второго рода.

Вторая глава диссертации посвящена разработке и исследованию модели распознавания пользователей информационной системы по изображению лица. В ней описаны методы предварительной обработки изображений, включая морфологические преобразования и применение фильтра Калмана для снижения влияния шумов и повышения помехоустойчивости. Рассмотрены современные методы извлечения признаков – локальные бинарные шаблоны (LBP) и гистограммы ориентированных градиентов (HOG), а также обоснован выбор сверточной нейронной сети в качестве основного инструмента распознавания. Приведена архитектура нейросети, формирование обучающей выборки, а также особенности обучения модели на видео в реальном времени. Отдельное внимание уделено модулю противодействия дипфейк-атакам, в том числе распознаванию изображений с экранов и бумажных носителей. Экспериментальные результаты показали, что использование фильтра Калмана позволяет достичь значения $MSE = 0,0019$, что свидетельствует о высокой эффективности предобработки. В целом, глава демонстрирует комплексный подход к повышению надежности и точности биометрической аутентификации по лицу в условиях современных угроз.

Третья глава диссертации посвящена разработке и исследованию модели распознавания пользователей информационной системы по голосу. В ней подробно описаны методы выделения акустических признаков, включая мел-частотные кепстральные коэффициенты (MFCC), коэффициенты линейного предсказания (LPC), перцепционные коэффициенты линейного предсказания (PLP), признаки частоты спектрального центроида (SCF) и Q-

константные кепстральные коэффициенты (CQCC). Особое внимание уделено этапу предварительной обработки аудиоданных, в частности применению метода RASTA-фильтрации для подавления шумов и повышения устойчивости к искажениям. Экспериментальные результаты показали, что использование расширенного набора признаков позволяет достичь ошибки первого рода (FRR) 0,11 % и ошибки второго рода (FAR) 0,01 %. Также во второй главе описан модуль противодействия синтезу речи (дипфейк-атакам) и продемонстрирована эффективность предложенной модели.

Четвертая глава диссертации посвящена апробации разработанных моделей распознавания по лицу и голосу, а также формированию и оценке эффективности мультимодальной системы биометрической аутентификации на основе конкатенации векторов признаков и сверточной нейронной сети. В ней представлены архитектура и программная реализация объединенной системы, включающей извлеченные признаки HOG, LBP, MFCC, LPC, PLP, CQCC и SCF. Описан процесс конкатенации признаков и приведены результаты экспериментов по распознаванию пользователей как по отдельным модальностям, так и в их комбинации. Особое внимание уделено противодействию дипфейк-атакам – как визуальным (через экран или бумажный носитель), так и аудио-подделкам. Экспериментальные данные показали, что предложенная мультимодальная система достигает точности аутентификации 99,31 % при значении функции потерь 0,032. Проведен сравнительный анализ различных архитектур нейросетей и подходов к обработке данных, а также продемонстрирована практическая применимость разработанного программного комплекса. Результаты подтверждают, что использование конкатенации признаков лица и голоса значительно повышает надежность и устойчивость системы к современным угрозам информационной безопасности.

В заключении подведены итоги диссертационного исследования: сформулированы основные результаты, отмечена практическая применимость разработанного программного комплекса.

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

Научные положения, выводы и рекомендации, сформулированные в диссертации, обоснованы как теоретически, так и экспериментально. Все разработанные модели и алгоритмы прошли комплексную экспериментальную проверку на собственных и общедоступных датасетах, что позволило достичь высоких показателей точности и низких значений ошибок первого и второго рода.

Диссертационная работа содержит достаточное количество иллюстраций, схем и таблиц, полно и наглядно интерпретирующих результаты проведенных исследований.

Содержание автореферата в полной мере отражает основные научные положения, выводы и практические результаты, представленные в диссертации. Все полученные результаты соответствуют заявленным автором пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность полученных результатов подтверждается их теоретической обоснованностью, строгим соответствием на действующие нормативно-правовые акты Российской Федерации, а также на международные стандарты, что обеспечивает соответствие предложенных решений современным требованиям в области биометрической аутентификации.

Обоснованность и достоверность полученных результатов подтверждается обширной публикационной активностью автора: диссертация сопровождается 30 научными публикациями, включая 7 статей в рецензируемых журналах, рекомендованных ВАК РФ, 1 статью в издании, индексируемом в RSCI, 3 статьи в журналах, входящих в базы данных Web of

Science и Scopus, 3 свидетельства о государственной регистрации программ для ЭВМ. Результаты диссертационной работы представлены на международных и всероссийских конференциях.

Научная новизна полученных результатов заключается в следующем:

1. Разработана модель биометрической аутентификации по изображению лица, в которой применена предварительная обработка данных с использованием адаптивного фильтра Калмана. Это позволило значительно повысить помехоустойчивость распознавания и снизить влияние шумов и искажений на точность идентификации в условиях реального времени.

2. Предложена модель аутентификации по голосу, основанная на расширенном наборе акустических признаков (MFCC, LPC, PLP, CQCC, SCF) и методе RASTA-фильтрации. Такой подход обеспечил снижение показателей ошибок первого (FRR = 0,11 %) и второго рода (FAR = 0,01 %) и повысил устойчивость системы к синтетическим атакам.

3. Разработан оригинальный алгоритм обучения сверточной нейронной сети для распознавания по лицу, включающий извлечение дополнительных текстурных дескрипторов (LBP, HOG) и специализированный модуль противодействия дипфейк-атакам, в том числе при подаче изображения с экрана или бумажного носителя.

4. Создан алгоритм обучения сверточной нейронной сети для аутентификации по голосу, который впервые в сочетании использует Q-константные кепстральные коэффициенты (CQCC) и спектральный центроид (SCF) в составе мультимодальной системы, что позволило эффективно противодействовать современным методам синтеза речи и повысить надежность верификации.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость проведенного исследования заключается в развитии научных основ мультимодальной биометрической аутентификации

на базе нейросетевых технологий. Предложены оригинальные подходы к предварительной обработке биометрических данных – с использованием фильтра Калмана для изображений лица и метода RASTA-фильтрации для речевых сигналов. Это позволило повысить помехоустойчивость и снизить влияние шумов на точность распознавания. Разработанные алгоритмы извлечения и конкатенации признаков (включая HOG, LBP, MFCC, LPC, PLP, SCF и CQCC) вносят вклад в теорию построения устойчивых к дипфейк-атакам мультимодальных систем. Кроме того, предложенные архитектуры сверточных нейронных сетей, адаптированные под задачи верификации по лицу и голосу, расширяют существующие модели машинного обучения в контексте информационной безопасности.

Практическая значимость работы подтверждена созданием программного комплекса мультимодальной биометрической аутентификации, достигающего высокой точности распознавания. Разработанные решения успешно внедрены в реальные информационные системы ООО «Информзащита» (Уфа) и ООО «ИТЭнигма Уфа», а также используются в процессах Координационного центра ФГБОУ ВО «Уфимский университет науки и технологий».

Таким образом, работа обладает как научной новизной, так и высокой прикладной ценностью для обеспечения защищенного доступа к информационным системам.

Замечания по работе:

1. На рисунке 2.3 приведена обобщенная схема архитектуры CNN, но отсутствуют ключевые параметры: размеры ядер свертки, шаг (stride), тип и параметры пулинга, количество фильтров на каждом слое, функции активации в каждом слое. Это затрудняет воспроизводимость результатов.

2. Описание адаптивного фильтра Калмана дается преимущественно в терминах временных рядов и пространства состояний, но не поясняется, как именно он адаптирован под двумерную структуру изображений (например, по строкам, блокам или пиксельным траекториям).

3. В диссертации рассмотрена обучающая выборка, содержащая 450 аудиозаписей с длительностями 8, 15 и 25 секунд. Однако не указано сколько записей каждого типа (длительности) приходится на каждого пользователя, а также при каких условиях (фон, оборудование, расстояние до микрофона) производилась запись.

4. В диссертационном исследовании указывается применение метода RASTA для шумоподавления, но не приведено сравнение его эффективности с альтернативными методами (спектральное вычитание, Wiener-фильтрация, современные deep learning-подходы типа DNN-based denoising).

5. Каким образом мультимодальная система обеспечивает устойчивость и сохраняет приемлемый уровень точности в реальных условиях, в случае потери одной из биометрических модальностей (например, из-за сильного шума в аудиосигнале или отсутствия изображения лица)?

6. Каковы временные характеристики работы разработанной мультимодальной системы (включая время обработки аудио и видео, а также время инференса нейронной сети), и как ее производительность варьируется на аппаратных платформах разного уровня (ПК, мобильные устройства и др.)?

Вышеуказанные замечания не снижают ценности полученных результатов исследования и не влияют на общую положительную оценку диссертации.

Диссертационная работа Лушникова Никиты Дмитриевича представляет собой завершенную научно-квалификационную работу, направленную на решение актуальной задачи повышения надежности биометрической аутентификации пользователей информационных систем на основе нейронных сетей. Работа отличается научной новизной, глубокой теоретической проработкой и значимым практическим результатом.

Диссертация полностью соответствует требованиям п.п. 9-11, 13, 14 Постановления Правительства Российской Федерации от 24 сентября 2013 г.

№ 842 «О порядке присуждения ученых степеней», а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертация, автореферат и отзыв обсуждены на заседании кафедры автоматизированных систем обработки информации и управления ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (Протокол № 13 от 15 декабря 2025 г.).

Заведующий кафедрой
автоматизированных систем
обработки информации и
управления ФГБОУ ВО «Казанский
национальный исследовательский
технический университет
им. А.Н. Туполева-КАИ»,
кандидат технических наук, доцент

Шлеймович
Михаил Петрович

«15» 12 2025 г.

Кандидатская диссертация защищена по специальности 05.13.05 – Элементы и устройства вычислительной техники и системы управления

Даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета 24.2.479.07 и их дальнейшую обработку.

Подпись _____
завещаю. Начальник управления
делопроизводства и контроля

Шлеймовича М.П.



Шлеймович М.П.

Доцент кафедры
автоматизированных систем
обработки информации и
управления ФГБОУ ВО «Казанский
национальный исследовательский
технический университет
им. А.Н. Туполева-КАИ»,
кандидат технических наук, доцент

Мокшин

Владимир Васильевич

«15» 12 2025 г.

Кандидатская диссертация защищена по специальности 05.13.18 –
Математическое моделирование, численные методы и комплексы программ

Даю согласие на включение моих персональных данных в документы,
связанные с работой диссертационного совета 24.2.479.07 и их дальнейшую
обработку.

Мокшин В.В.

420111, Россия, Республика Татарстан, г. Казань, ул. К. Маркса, д. 10.
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Казанский национальный исследовательский
технический университет им. А.Н. Туполева-КАИ»

Телефон: +7 (843) 231-97-34

Адрес электронной почты: kai@kai.ru

Подпись Мокшина В.В.
заверяю. Начальник управления
делопроизводства и контроля

