

УТВЕРЖДАЮ

Проректор по научной работе и
инновационной деятельности

ФГБОУ ВО «ПГУ»

Д.Э.Н. профессор

С.М. Васин

2025 г.



ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию Иниватова Даниила Павловича на
тему

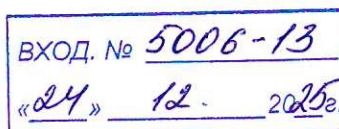
«Нейросетевая аутентификация по голосовым паролям с защитой биометрических
эталонов и учётом функционального состояния пользователя», представленную на
соискание учёной степени кандидата технических наук по специальности 2.3.6.

Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

В условиях интенсивного развития технологий искусственного интеллекта (ИИ) и их интеграции в системы информационной безопасности особое значение приобретает обеспечение надежной защиты биометрических данных. Биометрическая аутентификация по голосу представляет собой перспективное направление, сочетающее удобство использования с возможностью оценки функционального состояния (ФС) пользователя, однако она сталкивается с вызовами, такими как уязвимость к атакам воспроизведения, синтеза речи и компрометации шаблонов. Современные подходы к решению этих проблем опираются на концепцию доверенного ИИ, ориентированного на повышение устойчивости систем к деструктивным воздействиям, включая дрейф биометрических данных под влиянием факторов, изменяющих состояние человека.

Серия стандартов ГОСТ Р 52633 предлагает использование нейросетевого преобразователя «биометрия-код» (НПБК), позволяющего связывать биометрический образ с криптографическим ключом или паролем, что минимизирует риски утечки конфиденциальной информации. Актуальность исследований усиливается необходимостью учета изменчивости голосовых характеристик, вызванной функциональным состоянием, и обеспечения защиты эталонов от несанкционированного доступа. В этом контексте разработки, направленные на создание устойчивых к дрейфу и атакам систем голосовой аутентификации, имеют



стратегическое значение для применения в сферах, требующих высокой безопасности, таких как финансовые сервисы и корпоративные системы доступа.

Таким образом, диссертационная работа Иниватова Д.П., посвященная решению научной задачи повышения точности и устойчивости нейросетевой аутентификации по голосовым паролям с защитой биометрических эталонов и учетом функционального состояния пользователя, является актуальной.

Оценка структуры и содержания работы

Диссертационная работа состоит из введения, 4 глав, заключения, списка литературы (119 наименований) и 2 приложений. Общий объем диссертации составляет 144 страницы, включающих в себя 16 таблиц и 37 рисунков.

Во введении сформулированы цель и задачи диссертационного исследования, обозначена его актуальность, отмечена степень проработанности темы, а также перечислены элементы научной новизны работы, теоретической и практической значимости результатов.

Первая глава содержит аналитический обзор методов биометрической аутентификации, технологий защищенного исполнения процедур в цифровой среде, состязательных атак на биометрические системы и способов противодействия им, включая защиту шаблонов. Рассматривается дрейф голосовых данных под влиянием ФС пользователя, анализируются существующие базы голосовых образов и достигнутые результаты по аутентификации пользователя по голосу. Выявлены основные проблемы, такие как низкая устойчивость к дрейфу и компрометации, что позволило сформулировать цель и задачи исследования.

Во второй главе разработана статистическая модель изменения характеристик голосового сигнала в зависимости от ФС, основанная на влиянии таких факторов как алкогольная интоксикация и сонное состояние. Описано формирование базы голосовых паролей, анализ влияния ФС на параметры голоса и результаты аутентификации, что демонстрирует снижение точности в измененных состояниях и обосновывает необходимость учета этих факторов в системах распознавания.

Третья глава посвящена разработке метода извлечения признаков из голосового образа и алгоритма настройки НПБК. Описана предобработка голосовых образов, архитектура сверточной нейронной сети для извлечения признаков, ансамблирование предобученных автокодировщиков с одинаковой архитектурой, но обученных на разных репрезентациях голосовых образов, модель НПБК на базе гибридного слоя тригонометрических корреляционных нейронов и алгоритм его настройки. Преимущество использования двух типов нейронов заключается в обработке пар

признаков с высокой и низкой взаимной корреляцией, что позволяет лучше сепарировать образы "свой"/"чужой" и повышает общую точность. Приведены результаты экспериментов по распознаванию пользователя по голосовым паролем, демонстрирующие повышение точности аутентификации.

В четвертой главе предложена методика аутентификации по голосу с учетом ФС, включая архитектуру нейросетевой модели для выявления изменённого функционального состояния, что позволяет не только верифицировать личность, но и классифицировать состояние пользователя для динамической корректировки прав доступа в системе. Проведённый анализ устойчивости полученного НПБК к изменениям ФС подтвердил уменьшение влияния дрейфа данных на точность аутентификации пользователя по голосу, а разработанный программный модуль для реализации предложенных подходов был успешно внедрён в образовательный процесс.

В заключении приведены основные выводы и результаты по работе.

Область исследования диссертации соответствует следующим пунктам паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность:

п. 12 «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа»;

п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Оформление диссертации в целом соответствует ГОСТ Р 7.0.11-2011. Автореферат диссертации соответствует установленным требованиям, предоставляя полное представление о содержании работы, полученных теоретических и практических результатах, а также выводах.

Новизна полученных результатов

1. Разработана статистическая модель голосовых образов пользователя, основанная на экспериментальных данных об изменении голосовых параметров у испытуемых обоих полов от 18 до 50 лет в различных ФС, которая, в отличие от существующих ранее моделей, учитывает изменения голосовых биометрических признаков в различных ФС пользователя и позволяет предсказывать характер дрейфа биометрических данных.

2. Разработан метод извлечения признаков из голосовых образов, основанный на ансамбле автокодировщиков, который, в отличие от традиционных методов, осуществляет расширение набора биометрических данных на этапе распознавания

пользователя, что позволяет повысить точность аутентификации при дрейфе данных за счёт учёта спектральных особенностей, извлечённых из различных репрезентаций голосового сигнала.

3. Разработан алгоритм настройки НПБК с обеспечением защиты биометрических шаблонов от компрометации, основанный на использовании двух типов нейронов, каждый из которых осуществляет обработку голосовых данных с различным уровнем взаимной корреляции, что, в отличие от ранее известных алгоритмов обучения НПБК, обеспечивает более высокую точность аутентификации пользователя в условиях дрейфа биометрических данных.

4. Разработана методика аутентификации по голосу с распознаванием ФС пользователя, основанная на ансамблевых методах машинного обучения, что, в отличие от существующих ранее методик, позволяет проводить не только верификацию личности, но и выполнять классификацию ФС пользователя, регистрируя отклонения его состояния от нормы, что служит решающим фактором для ограничения прав доступа в процессе авторизации.

Защищаемые научные положения, связанные с ними результаты работы и вытекающие из них рекомендации вполне **оригинальны**. Проектирование предложенных автором моделей и алгоритмов осуществляется на современном уровне. При этом использован анализ экспериментальных данных о голосовых параметрах с применением методов машинного обучения и спектрального анализа. Все результаты теоретических исследований подтверждены данными экспериментов. Многие результаты работы сопоставляются с результатами, которые получены и опубликованы другими авторами. На программные модули и электронные ресурсы получены свидетельства о государственной регистрации программ для ЭВМ, а также акты о внедрении в учебный и производственный процессы.

Достоверность полученных результатов подтверждается корректной постановкой задач и обоснованным выбором методов исследования, их обсуждением на научных конференциях, а также апробацией в ходе экспериментов с применением разработанных программных средств и практическим применением полученных моделей и алгоритмов в образовательной и производственной сферах.

Публикации по теме диссертации

По материалам диссертации опубликовано 17 работ, 4 из которых изданы в журналах, рекомендованных перечнем ВАК; 5 научных публикаций индексируются в международной информационно-аналитической системе научного цитирования Scopus; 8 научных работ опубликованы в других изданиях. Получено 4 свидетельства о регистрации

программ для ЭВМ.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость диссертационной работы состоит в создании статистической модели изменений голосовых характеристик под влиянием ФС пользователя, опирающейся на амплитудно-частотные свойства речи и учитывающей вариабельность реакций в разных состояниях. Модель помогает прогнозировать зоны спектра, уязвимые к дрейфу признаков. Кроме того, предложены алгоритм настройки НПБК с учетом ФС, метод извлечения признаков и методика аутентификации с распознаванием состояния. Метод извлечения признаков на основе ансамбля автокодировщиков, осуществляющего расширение набора биометрических данных на этапе распознавания образа увеличивает точность и надёжность аутентификации. Особый вклад вносит анализ корреляционных связей голосовых параметров, на основе которого происходит выбор типа нейронов, используемых в НПБК, что повышает точность аутентификации и сопротивление дрейфу, вызванному изменению ФС пользователя.

Практическая значимость заключается в повышении надежности голосовой биометрической аутентификации и защите компьютерных ресурсов от несанкционированного доступа с помощью созданного программного модуля. Достигнутый коэффициент равной вероятности ошибок в 2,1% подтверждает высокую точность для задачи аутентификации пользователя.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертации рекомендуются для внедрения в организациях, разрабатывающих биометрические системы защиты информации, включая банки, корпоративные сети, в предприятия, оказывающие транспортные услуги, а также в государственные учреждения, где голосовая аутентификация может быть применена для адаптации прав доступа в зависимости от ФС пользователя.

Замечания по работе

1. В третьей главе не проведено сравнение предложенного метода извлечения признаков на базе ансамбля автокодировщиков с альтернативными подходами на одной и той же выборке, что затрудняет оценку относительных преимуществ в условиях дрейфа биометрических характеристик.

2. Работа не содержит обоснования размера используемой базы данных в итоговом эксперименте (130 пользователей). Рекомендуется дополнить раздел статистическим

анализом (например, расчетом размера выборки на основе ожидаемой ошибки).

3. В работе приведено сравнение устойчивости НПБК к голосовым образам пользователей в изменённых функциональных состояниях, при этом все такие состояния объединены в один класс «изменённое ФС». Отсутствует отдельный анализ устойчивости модели к каждому конкретному состоянию, что существенно снизило информативность эксперимента и не позволяет оценить, насколько по-разному каждое из состояний влияет на точность аутентификации.

4. В тексте имеются опечатки и стилистические неточности, например на с. 97 указано «использованы НПБК, обученные в рамках параграфа 3.6», но в указанном параграфе был обучен только один НПБК.

5. В рамках эксперимента по выявлению ИФС из 4 главы была использована только предложенная автором база голосовых образов, но не был использован корпус ALC, фигурирующий в обзоре.

Выявленные недостатки не снижают общей положительной оценки научных результатов, достигнутых соискателем в ходе выполнения диссертационного исследования, и не умаляют значимости работы, вносящей существенный вклад в развитие научной области.

Заключение

Диссертация Иниватова Даниила Павловича на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании проведенных автором исследований решена задача повышения точности и устойчивости нейросетевой аутентификации по голосовым паролям с защитой биометрических эталонов и учетом функционального состояния пользователя, результаты которой обладают научной новизной, теоретической и практической значимостью.

Диссертационная работа Иниватова Д.П. соответствует требованиям п.п. 9-11, 13, 14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года №842 (с изменениями и дополнениями), а её автор, Иниватов Даниил Павлович, заслуживает присуждения учёной степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертационная работа Иниватова Д.П. и настоящий отзыв заслушаны и одобрены на заседании кафедры «Информационная безопасность систем и технологий» факультета информационных технологий и электроники Федерального государственного бюджетного образовательного учреждения высшего образования

«Пензенский государственный университет» (протокол № 6 от 16 декабря 2025 г.).

Отзыв составили:

Зав. кафедрой «Информационная
безопасность систем и технологий»
ФГБОУ ВО «ПГУ»,
к.т.н., доцент



Зефирова Сергей Львович

«16» 12 2025 г.

Кандидатская диссертация защищена по специальности 05.12.14 – Сети, узлы связи и распределение информации.

Даю согласие на обработку персональных данных.

Доцент кафедры «Информационная
безопасность систем и технологий» ФГБОУ
ВО «ПГУ»,
д.т.н.



Егорова Наталья Алексеевна

«16» 12 2025 г.

Докторская диссертация защищена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Даю согласие на обработку персональных данных.

Доцент кафедры «Информационная
безопасность систем и технологий» ФГБОУ
ВО «ПГУ»,
к.т.н., доцент



Иванов Алексей Петрович

«16» 12 2025 г.

Кандидатская диссертация защищена по специальности 05.12.13 - Системы, сети и устройства телекоммуникаций.

Даю согласие на обработку персональных данных.

Адрес места основной работы: 440026 г. Пенза, ул. Красная,
д. 40, рабочий телефон: +7 (8412) 20-84-35
Адрес эл. почты: ibst@pnzgu.ru

Подписи Зефирова С.Л., Егоровой Н.А., Иванова А.П. заверяю.

Ученый Секретарь ученого совета
к.т.н., доцент



Дорофеева Ольга Станиславна

12 2025 г.