

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

профессора кафедры систем информационной безопасности
ФГБОУ ВО «Казанский национальный исследовательский технический
университет им. А.Н. Туполева-КАИ», доктора технических наук, профессора

Катасёва Алексея Сергеевича

на диссертационную работу Иниватова Даниила Павловича на тему
**«Нейросетевая аутентификация по голосовым паролям с защитой
биометрических эталонов и учетом функционального состояния
пользователя»,**

представленную на соискание ученой степени кандидата технических наук
по специальности 2.3.6 Методы и системы защиты информации,
информационная безопасность.

Актуальность темы диссертации

Голосовая аутентификация набирает популярность благодаря интеграции в различные сценарии от банковских транзакций до корпоративного доступа, предлагая бесконтактный и интуитивный подход. Тем не менее, она сталкивается с фундаментальными проблемами: повышенной уязвимостью к атакам воспроизведения, позволяющим обходить системы с помощью поддельных записей, дрейфом голосовых параметров из-за изменений функционального состояния (ФС) пользователя (усталость, опьянение или эмоциональные сдвиги), что приводит к росту ложных отказов, а также рискам компрометации шаблонов. При этом украденные голосовые данные могут быть использованы злоумышленниками. Эти недостатки ограничивают применение голосовой биометрии в высокозащищенных средах, где статические методы показывают лучшую стабильность, но не учитывают динамику ФС. В результате существующие системы не полностью соответствуют требованиям конфиденциальности и устойчивости, особенно в условиях растущих киберугроз.

Решением могут стать нейросетевые преобразователи «биометрия-код» (НПБК), связывающие речевой образ с криптографическим паролем для защиты от компрометации, но их эффективность снижается под воздействием дрейфа голосовых параметров. Согласно ФЗ № 572, биометрические системы должны быть построены на доверенном искусственном интеллекте, устойчивом к деструктивным факторам, что делает актуальными исследования по робастному извлечению признаков и адаптивной аутентификации.

Следовательно, тема диссертации Иниватова Д.П., посвященной решению научной задачи разработки системы нейросетевой аутентификации по голосовым паролям с защитой биометрических эталонов и учетом функционального состояния пользователя, является актуальной.

ВХОД. № 4943-13
«19» 12. 2025.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений, списка литературы и двух приложений. Диссертация изложена на 144 страницах машинописного текста, содержит 37 рисунков и 16 таблиц. Библиографический список включает в себя 119 наименований. Структура и содержание диссертации соответствует цели и задачам исследования.

Во введении обоснована актуальность темы диссертации, определены ее цель и задачи, сформулированы положения, выносимые на защиту, научная новизна, а также практическая и теоретическая значимость полученных результатов.

Первая глава диссертационного исследования посвящена аналитическому обзору задачи аутентификации по голосу с учетом функционального состояния и защиты биометрических шаблонов. Выделены ключевые методы биометрической аутентификации, включая статические и динамические классы признаков, с акцентом на голосовую модальность. Рассмотрены технологии защищенного исполнения процедур в цифровой среде, состязательные атаки (воспроизведения, синтеза) и способы противодействия, включая биокриптографические системы и ГОСТ Р 52633. Анализ дрейфа голосовых данных под влиянием функционального состояния, обзор существующих баз образов и достигнутых результатов по голосовому распознаванию позволил выявить недостатки текущих подходов, такие как низкая устойчивость к компрометации и дрейфу, подчеркивая необходимость улучшений в контексте голосовой биометрии, что позволило сформулировать цель и задачи работы.

Во второй главе диссертации разработана статистическая модель влияния функционального состояния человека на параметры его голоса и результаты аутентификации. Модель основана на анализе воздействия алкоголя на организм и обзоре результатов распознавания интоксикации с формированием собственной базы голосовых паролей. Модель описывает изменения характеристик сигнала (амплитудно-частотные свойства) в различных состояниях, включая нормальное, сонное и градации опьянения, и оценивает их влияние на точность аутентификации, показывая рост ошибок в измененных условиях.

В третьей главе предложен метод извлечения признаков из голосового образа и алгоритм настройки НПБК. Метод включает предобработку образов, архитектуру сверточной сети для извлечения признаков и ансамблирование предобученных автокодировщиков. Предложен алгоритм настройки НПБК на базе тригонометрических корреляционных нейронов, который обеспечивает обработку пар признаков с разным уровнем корреляции, что повышает точность классификации и длину криптографического ключа. Экспериментальная оценка продемонстрировала снижение EER по сравнению с другими реализациями, подтверждая эффективность в задачах голосового распознавания.

В четвертой главе представлена методика биометрической аутентификации по голосу с учетом ФС человека. В ее основе лежит анализ устойчивости НПБК к изменениям ФС, архитектура модели для распознавания состояния и методика аутентификации, интегрирующая оценку ФС для динамической корректировки доступа. Методика реализована в программном модуле, протестирована и внедрена в образовательный процесс, что подтверждено соответствующим актом.

В заключении выделены основные результаты, полученные в диссертации.

Приложения содержат акты о внедрении результатов работы, а также свидетельства о государственной регистрации программ для ЭВМ.

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

Обоснованность научных положений и выводов, представленных в диссертации, подтверждается широтой их апробации. Основные результаты диссертационного исследования опубликованы в 4-х статьях в журналах из Перечня ВАК, в 5-ти статьях в журналах и материалах конференций из базы Scopus, а также в 8-ми статьях, опубликованных в других изданиях. Кроме того, получено 4 свидетельства о регистрации разработанных программ для ЭВМ.

Диссертация включает в себя достаточное количество иллюстраций и таблиц, необходимых для полного понимания результатов проведенных исследований. Автореферат адекватно отражает содержание диссертации, а также ключевые выводы и результаты, представленные в работе.

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 результатами проведенных компьютерных экспериментов, государственной регистрацией программ для ЭВМ, а также успешным внедрением разработанной системы в образовательные и бизнес-процессы. Основные результаты диссертационного исследования прошли апробацию на научных конференциях различного уровня.

Научная новизна полученных результатов

К новым научным результатам, полученным в диссертации, относятся:

1. 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. 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 счет учета спектральных особенностей, извлеченных из различных репрезентаций голосового сигнала.

3. 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. 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 человека, но и выполнять классификацию ФС пользователя, регистрируя отклонения его состояния от нормы, что служит решающим фактором для ограничения прав доступа в процессе авторизации.

Основные научные положения диссертационного исследования, выносимые на защиту, связанные с ними результаты работы и вытекающие из них практические рекомендации являются оригинальными и свидетельствуют о значимом вкладе автора диссертации в науку.

Теоретическая и практическая значимость результатов, полученных автором диссертации

Теоретическая значимость результатов диссертационной работы заключается в предложенных моделях и алгоритмах для нейросетевого преобразователя «биометрия-код», устойчивого к дрейфу голосовых признаков под влиянием ФС пользователя. Новый подход к извлечению признаков на базе ансамбля автокодировщиков и гибридного слоя нейронов позволяет генерировать надежный криптографический код, защищая биометрические эталоны от компрометации.

Практическая значимость полученных результатов состоит в разработке системы голосовой биометрической аутентификации с учетом ФС пользователя, основанной на предложенных моделях и алгоритмах. Полученные результаты работы системы, реализованной и протестированной с помощью специального программного модуля, также прошли апробацию, подтвержденную актами о внедрении в учебный и производственные процессы.

Замечания

1. Цель диссертационной работы сформулирована как «повысить точность и устойчивость к дрейфу биометрических данных процедуры аутентификации пользователя...». В этой формулировке присутствует неоднозначность: автор стремится повысить точность процедуры аутентификации или точность результата аутентификации? Повышение точности процедуры аутентификации означает улучшение процесса проверки подлинности, а повышение точности аутентификации – улучшение надежности метода. Судя по полученным результатам и формулировкам в тексте диссертации, автор исследования стремится повысить точность аутентификации, как точность распознавания пользователя. Следовательно, формулировка цели диссертации требует пояснения и уточнения.

2. Решаемые в диссертации задачи связаны исключительно с разработкой (разработка модели, разработка метода, разработка алгоритма, разработка методики, разработка программного модуля). При этом нет формулировок задач, связанных с анализом, реализацией, тестированием, апробацией, хотя такие задачи в диссертации фактически решаются.

3. В блок-схеме алгоритма настройки параметров НПБК (см. рис. 3.11, стр. 85 диссертации) блок «Подсчет всех возможных пар признаков» ошибочно оформлен в виде блока ввода данных, хотя по смыслу – это блок выполнения операции, который требуется оформлять в виде прямоугольника. Кроме того, в представленной схеме отсутствует блок вывода, что не в полной мере отражает суть представленного алгоритма.

4. Четвертая глава диссертации, в частности, посвящена вопросам апробации. В конце главы достаточно подробно представлены результаты внедрения в учебный процесс Омского государственного технического университета (с описанием ряда лабораторных работ и результатами их выполнения студентами). Однако в диссертации отсутствует подобное описание использования полученных результатов в проектной деятельности компании ООО «ОСМИ-ИТ» (кроме имеющего акта об использовании), что представляет наибольший интерес с точки зрения апробации результатов диссертационного исследования.

5. В акте о внедрении результатов диссертационного исследования в учебный процесс в разделе «Утверждаю» в наименовании ВУЗа пропущено слово «технический»: вместо «Омский государственный технический университет» написано «Омский государственный университет».

Указанные замечания носят рекомендательный и уточняющий характер, не снижают значимости результатов диссертационного исследования и не влияют на общую положительную оценку работы.

Заключение

Диссертация Иниватова Д.П., представленная на соискание ученой степени кандидата технических наук, является завершенной научно-квалификационной работой, посвященной решению актуальной задачи для повышения точности, устойчивости и защищенности голосовой биометрической аутентификации с учетом функционального состояния пользователя.

Результаты диссертационного исследования обладают научной новизной, теоретической и практической значимостью.

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

Профессор кафедры систем информационной безопасности ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», д.т.н., профессор



Катасёв Алексей Сергеевич

«15» декабря 2025 г.

Докторская диссертация защищена по специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ»

Я, Катасёв Алексей Сергеевич, даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

Почтовый адрес: 420111, г. Казань, ул. К. Маркса, д. 10

Телефон: +7 (927) 408-94-68

E-mail: ASKatasev@kai.ru

Подпись 
заверяю. Начальник управления
делопроизводства и контроля

