

ОТЗЫВ

официального оппонента

доктора физико-математических наук, доцента Исмагиловой Альбины Сабирьяновны 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

Актуальность диссертационной работы обусловлена стремительным развитием биометрических систем и растущими требованиями к их надежности, безопасности и адаптивности в реальных условиях эксплуатации. Голосовая аутентификация, несмотря на удобство и бесконтактность, остается уязвимой к дрейфу голосовых характеристик, вызванному изменением функционального состояния (ФС) пользователя: усталостью, сонливостью, стрессом или интоксикацией. Такие изменения приводят к значительному росту ошибок (FRR/FAR), что снижает доверие к системе и ограничивает ее применение в критически важных сценариях. Одновременно сохраняется острая проблема защиты биометрических шаблонов: в случае компрометации их невозможно заменить, в отличие от паролей. Существующие подходы либо недостаточно устойчивы к вариациям ФС, либо обеспечивают защиту за счет снижения точности.

В связи с вышеуказанным, исследование Иниватова Д.П. становится особенно актуальным. В данной диссертационной работе предложено комплексное решение, сочетающее устойчивое к дрейфу извлечение признаков на основе ансамбля предобученных автокодировщиков, нейросетевой преобразователь «биометрия-код» (НПБК) с тригонометрическими нейронами, адаптированными к уровню корреляции

признаков, и классификатор ФС на базе CatBoost. Это позволяет не только генерировать криптографически стойкие ключи длиной 1024 бита без раскрытия биометрических данных, но и динамически регулировать права доступа в зависимости от текущего состояния пользователя. Разработанные методы повышают устойчивость системы к дрейфу, обеспечивают высокую точность распознавания ФС и реализуют принцип «безопасной аутентификации», что особенно важно для банковских, транспортных и корпоративных систем.

Оценка структуры и содержания работы

Работа состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы и приложений. Общее количество страниц – 144, включая 37 рисунков, 16 таблиц и 2 приложения. Список использованных источников состоит из 119 наименований.

Во введении сформулированы цель и задачи диссертационного исследования, обоснована его актуальность, а также выделены компоненты научной новизны работы и практическая значимость полученных результатов.

В первой главе рассматриваются методы и технологии голосовой биометрической аутентификации с учетом функционального состояния пользователя и защиты биометрических шаблонов. Анализируются достоинства и недостатки динамических (голос) и статических (отпечатки, лицо, радужка) биометрических методов, подчеркиваются уязвимости голосовой аутентификации к атакам воспроизведения и синтеза речи, а также влияние дрейфа голосовых характеристик, вызванного усталостью, стрессом, интоксикацией и другими факторами. Рассматриваются такие подходы к защите биометрических данных как классическое и гомоморфное шифрование, нечеткие экстракторы, а также НПБК, обеспечивающий криптографическую защиту и устойчивость к подделкам. Отмечается необходимость адаптации систем к дрейфу данных и концепций с помощью

ансамблевых методов, онлайн-обучения и нормализации сигналов. Приводится обзор популярных голосовых корпусов (VoxCeleb2, TIMIT, RedDots, Common Voice и др.), включая специализированные наборы с записями в измененных функциональных состояниях (алкогольное опьянение, сонливость). Подводятся итоги современных достижений в области голосовой идентификации: использование х-векторов, ResNet, ЕСАРА-TDNN и гибридных архитектур позволило существенно снизить EER. В заключение формулируется цель исследования – повышение точности и устойчивости аутентификации по голосу с применением НПБК и адаптацией к функциональному состоянию пользователя.

Во второй главе диссертации исследуется влияние ФС пользователя, в частности, алкогольной интоксикации и сонливости, на параметры голосового сигнала и эффективность систем аутентификации. Приводятся физиологические основы воздействия этанола на речевой аппарат и центральную нервную систему, что приводит к замедлению речи, изменению тембра, высоты тона и спектральных характеристик. На основе собственного корпуса голосовых данных (130 русскоязычных испытуемых в 5 различных ФС) построена статистическая модель трансформации акустических признаков, выявлены частотные диапазоны, наиболее чувствительные к изменениям ФС. Показано, что признаки выше 600 Гц повышают информативность при ИФС 1–2, но сильно варьируются между состояниями, что снижает надежность аутентификации. Эксперименты с «широкими» нейросетями и различными мерами близости (Пирсона, хи-модуль, байесовские функционалы и др.) продемонстрировали рост ошибок FRR и FAR более чем в 5 раз при смене ФС. Наилучшую устойчивость показали меры Пирсона и хи-модуль. Также подтверждено, что обучение модели на смешанных данных (нормальное и измененное ФС) улучшает распознавание в состоянии опьянения, но ухудшает его в норме, что указывает на необходимость адаптивных или многоэталонных подходов. Результаты

подчеркивают важность учета ФС при проектировании защищенных и надежных биометрических систем.

В третьей главе диссертации представлена разработка гибридного НПБК, обеспечивающего высокую точность аутентификации по голосу и криптографическую защиту биометрических шаблонов. Предложен метод извлечения признаков на основе ансамбля предобученных сверточных автокодировщиков, каждый из которых обрабатывает усредненный амплитудный спектр голосового пароля, полученный с использованием различных оконных функций (прямоугольное, Хемминга, Гаусса и др.). Это позволяет сформировать комплементарные признаковые описания, повышающие устойчивость к вариациям голоса. Для преобразования признаков в 1024-битный ключ разработаны два типа тригонометрических нейронов: косинусные применяются для слабо коррелированных признаков, и котангенсные – для сильно коррелированных (с отдельной обработкой положительной и отрицательной корреляции). Алгоритм настройки НПБК включает калибровку по репрезентативной выборке, сегментацию пространства признаков на три сектора и автоматическую сборку нейронов с уникальными парами входов, исключающую повторное использование признаков и устойчивую к атакам Маршалко. Эксперименты на собственном корпусе AIC-spkr-130 (включающем записи в нормальном и измененном функциональном состоянии) и на RedDots показали EER = 2,1% и 3,2% соответственно – результат, сопоставимый с мировым уровнем, но при значительно большей длине ключа и повышенной защищенности. Модель устойчива к офисному шуму (рост EER не превышает 17%) и поддерживает конфиденциальность биометрических данных без применения внешнего шифрования.

В четвертой главе диссертации представлена методика защищенной голосовой аутентификации с учетом ФС пользователя. Показано, что предложенный НПБК на основе тригонометрических корреляционных нейронов устойчив к дрейфу голосовых характеристик: при переходе

пользователя из нормального состояния в измененное (сон, алкогольное опьянение) рост EER составляет всего 29% против 52% у традиционных систем (например, GMM-UBM). Это объясняется тем, что коррелированные признаки при дрейфе смещаются согласованно, и котангенсные нейроны адекватно оценивают их взаимосвязи. Для классификации ФС разработана модель на основе ансамблевого алгоритма CatBoost, использующая комбинированные признаки (MFCC + Wav2Vec2 + HuBERT + ECAPA-TDNN). На собственном корпусе AIC-spkr-130 (130 русскоязычных участников, 5 состояний) она достигла макро-F1 = 0,954, что превосходит аналоги даже при более сложной постановке задачи (многоклассовая, а не бинарная). Предложена двухэтапная схема аутентификации: сначала НПБК подтверждает личность, затем модель ФС определяет текущее состояние и динамически регулирует права доступа – например, в состоянии ИФС 3 блокируется подпись документов или финансовые операции. Реализация методики выполнена в рамках модернизированного программного комплекса AIC Desktop, поддерживающего построение, обучение и тестирование НПБК и нейросетей, визуализацию ошибок и работу в защищенном криптографическом режиме. Результаты открывают путь к созданию адаптивных биометрических систем, учитывающих не только «кто», но и «в каком состоянии» пользователь.

В заключении приведены основные результаты диссертационного исследования.

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

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

Основные положения и выводы, представленные в данной работе, обладают полной обоснованностью, что подтверждается корректным применением методов исследования, четкой формулировкой целей и задач, а также соответствующими публикациями, основанными на материалах

диссертации. Диссертация отличается логичной и последовательной структурой и сопровождается достаточным количеством иллюстраций и таблиц, которые наглядно демонстрируют ключевые результаты исследования. Содержание автореферата полностью отражает основные идеи и выводы, изложенные в диссертационной 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 корректностью примененных методов математического и компьютерного моделирования, согласованностью экспериментальных данных с теоретическими оценками, а также воспроизводимостью результатов на двух независимых голосовых корпусах. Все выносимые на защиту положения строго обоснованы с точки зрения теории машинного обучения, биометрической аутентификации и информационной безопасности.

Научная новизна полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертационной работе, состоят в разработке научно-обоснованного концептуального подхода, моделей и алгоритмов решения поставленных в диссертации задач. К новым научным результатам, полученным в диссертационном исследовании следует отнести следующие:

1. Разработана статистическая модель голосовых образов, построенная на основе экспериментальных данных, полученных от мужчин и женщин в возрасте 18–50 лет, находившихся в различных ФС. В отличие от ранее известных подходов, данная модель учитывает особенности трансформации голосовых биометрических признаков в зависимости от ФС и позволяет прогнозировать характер дрейфа биометрических данных.

2. Предложен оригинальный метод извлечения признаков из голосовых сигналов, основанный на ансамбле предобученных автокодировщиков, каждый из которых обрабатывает спектральную репрезентацию, полученную

с использованием различных оконных функций. В отличие от традиционных подходов, этот метод расширяет информативную базу на этапе распознавания за счет комплементарных спектральных характеристик, что повышает точность аутентификации при наличии дрейфа голосовых данных.

3. Создан алгоритм настройки НПБК, обеспечивающий защиту биометрических шаблонов от компрометации и использующий два типа тригонометрических нейронов: один – для слабо коррелированных признаков, другой – для сильно коррелированных (с разделением на положительную и отрицательную корреляцию). В отличие от существующих алгоритмов обучения НПБК, предложенный подход повышает устойчивость и точность аутентификации в условиях дрейфа биометрических характеристик.

4. Разработана комплексная методика голосовой аутентификации, интегрирующая распознавание ФС пользователя на основе ансамблевых методов машинного обучения. В отличие от традиционных схем, данная методика позволяет не только верифицировать личность, но и классифицировать текущее ФС, выявляя отклонения от нормы и динамически ограничивать права доступа в зависимости от выявленного состояния, что повышает безопасность критически важных операций.

Защищаемые научные положения, связанные с ними результаты работы и вытекающие из них рекомендации оригинальны.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость диссертационной работы заключается в развитии научных основ защищенной голосовой биометрии с учетом ФС пользователя. В работе предложена оригинальная статистическая модель трансформации голосовых признаков под влиянием различных ФС, что углубляет понимание механизмов дрейфа биометрических данных. Разработан гибридный подход к построению НПБК, впервые интегрирующий тригонометрические корреляционные нейроны с адаптацией

к уровню взаимной корреляции признаков. Это расширяет теорию построения устойчивых к дрейфу биометрических систем и вносит вклад в развитие методов защищенного машинного обучения, соответствующих требованиям ГОСТ Р 52633.

Практическая значимость работы обусловлена реализацией комплексного решения для надежной и безопасной аутентификации по голосу в реальных условиях. Разработанный программный модуль, интегрированный в платформу AIC Desktop, позволяет генерировать криптографически стойкие 1024-битные ключи на основе голосового пароля, обеспечивая защиту биометрических шаблонов без применения внешнего шифрования. Методика динамической адаптации прав доступа в зависимости от выявленного ФС открывает новые возможности применения голосовой аутентификации в банковских системах, корпоративной информационной безопасности, системах дистанционного управления транспортом и других сценариях, где критически важна не только идентификация личности, но и оценка ее текущего состояния.

Замечания по работе

1. В экспериментах, описанных во второй главе (п. 2.5), показано, что при переходе пользователя в измененное состояние ошибки FRR/FAR растут. Однако в главе 4 утверждается, что предложенный НПБК снижает этот рост до 29%. Не противоречит ли это оценке – ведь 29% роста ошибки все еще критичен для многих прикладных сценариев? Как вы объясните эту разницу и насколько она приемлема для реальных систем?

2. В п. 3.4 предложен гибридный НПБК с тригонометрическими нейронами (косинус/котангенс), и показано, что он устойчив к дрейфу коррелированных признаков. Однако не представлены результаты анализа корреляционной структуры признаков в разных ФС. Какие именно пары признаков демонстрируют высокую устойчивость корреляции при переходе в ИФС, и сколько их в общем наборе?

3. В главе 3 предложено использовать усредненный амплитудный спектр вместо полной спектрограммы при формировании входных данных, ссылаясь на снижение размерности и устойчивость к шуму. Были ли проведены сравнительные эксперименты с моделями, использующими полную спектрограмму или другие временно-частотные представления, чтобы подтвердить, что потеря временной информации не снижает способность модели адаптироваться к ИФС?

4. В главе 3 при отборе пар признаков для каждого нейрона вводится требование уникальности пар. Возможно ли масштабировать предложенный алгоритм настройки НПБК в условиях ограниченного признакового пространства, не ослабляя при этом криптографическую стойкость за счет вынужденного повторного использования пар?

5. Модель CatBoost показывает высокую точность распознавания ФС, но при этом обучалась на признаках, извлеченных из предобученных моделей (ЕСАРА-TDNN, Wav2Vec2 и др.). Не создает ли это риска утечки биометрической информации на этапе передачи признаков между модулями? Как обеспечивается защита этих высокоуровневых представлений в «защищенном режиме»?

Необходимо отметить, что вышеуказанные замечания не влияют на общую положительную оценку научных результатов выполненного соискателем диссертационного исследования и не снижают ценности полученных результатов.

Заключение

Диссертационная работа Иниватова Даниила Павловича по своей научной новизне, теоретической проработке и практической значимости является законченной научно-квалификационной работой, решающей актуальную задачу повышения точности, устойчивости и защищенности голосовой биометрической аутентификации с учетом функционального состояния пользователя.

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, Иниватов Даниил Павлович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Заведующий кафедрой управления
информационной безопасностью,
ФГБОУ ВО «Уфимский университет
науки и технологий», доктор физико-
математических наук, доцент

А.С.

Исмагилова

Альбина Сабирьяновна

«19» декабря 2025 г.

Докторская диссертация защищена по специальности 02.00.04
Физическая химия (физико-математические науки)

Адрес места основной работы:

450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, 32/1

Рабочий телефон: +7 (347) 273-66-92

Адрес эл. почты: ismagilova.as@ugatu.su

Даю согласие на включение моих персональных данных в документы,
связанные с защитой Иниватова Д.П. и их дальнейшую обработку.

А.С.

Исмагилова А.С.



Письмо Иниватовой А.С.
подтверждаю «19» 12 2025г.
Зам.начальника общего отдела УУНИТ Т. Ини
Иниватова Т. Р.