

ОТЗЫВ

на автореферат диссертационной работы

Иниватова Даниила Павловича на тему:

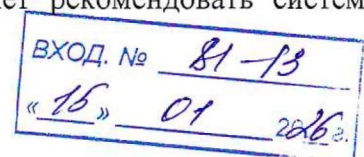
«Нейросетевая аутентификация по голосовым паролям с защитой биометрических эталонов и учётом функционального состояния пользователя», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность

В цифровом мире биометрические методы аутентификации приобретают все большую роль, поскольку они позволяют точно подтверждать личность без дополнительных устройств. Голосовые системы здесь выделяются удобством: их применяют в банковских приложениях, кол-центрах и умных устройствах, где пользователь просто произносит фразу. Однако голос подвержен изменениям от функционального состояния, такого как усталость или сонливость, что приводит к ошибкам в распознавании и создает дополнительные риски. Например, доступ в критические системы, полученный в состоянии сильной усталости, может вызвать непреднамеренные действия или облегчить атаки извне. Кроме того, биометрические шаблоны уязвимы к краже и подделке, особенно если злоумышленник получит записи голоса легального пользователя. В условиях цифровизации, когда удаленный доступ становится нормой в работе и образовании, такие проблемы требуют новых подходов, чтобы связать голос с защищенным кодом и учесть вариации состояния.

В связи с этим тематика исследования Иниватова Д.П., направленная на обеспечение защиты биометрических шаблонов и устойчивость к изменениям функционального состояния пользователя, становится особенно актуальной. Предложенные модели и алгоритмы отвечают современным потребностям, учитывают влияние дрейфа голосовых данных и предотвращают утечку биометрических образов.

Научная новизна исследования заключается в следующих положениях: во-первых, создана статистическая модель изменений голосовых параметров под влиянием функционального состояния, основанная на данных о людях разного пола и возраста, позволяющая предсказывать дрейф биометрии. Во-вторых, предложен метод извлечения признаков на базе ансамбля автокодировщиков, расширяющий набор данных за счет спектральных особенностей из разных репрезентаций голосового сигнала. В-третьих, разработан алгоритм настройки нейросетевого преобразователя "биометрия-код" с гибридным слоем нейронов для обработки коррелированных признаков, устойчивый к компрометации шаблонов. В-четвертых, создана методика аутентификации, сочетающая верификацию личности с классификацией состояния для динамического управления доступом.

Практическая значимость работы обусловлена разработкой системы нейросетевой аутентификации по голосовым паролям, которая объединяет предложенные модели, алгоритмы и методику, обеспечивая защиту эталонов от кражи и устойчивость к дрейфу данных при смене функционального состояния. Предложенная система ориентирована на защиту биометрических шаблонов зарегистрированных пользователей, устойчивость к атакам, а также к угрозам компрометации знаний. Корректность теоретических положений, выдвинутых в диссертации, подтверждена результатами экспериментов на собственной и общедоступных базах голосовых образов, что позволяет рекомендовать систему для



применения в сферах с повышенными требованиями к безопасности. Основные результаты опубликованы в 17 работах, включая 4 статьи в журналах из перечня ВАК и 5 в Scopus.

В качестве замечаний по автореферату можно отметить:

1. В работе отсутствует анализ устойчивости разработанного НПБК к спуфинг-атакам и атакам с использованием воспроизведенных голосовых записей
2. Автореферат содержит ограниченное число ссылок на работы, позволяющие сравнить устойчивость НПБК к вариациям функционального состояния пользователя с существующими методами.

Вместе с тем, указанные замечания не снижают теоретической и практической значимости полученных результатов, а также общей положительной оценки. Считаю, что диссертационная работа Даниила Павловича Иниватова, является завершенным самостоятельным научным исследованием, полностью удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, соответствует 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, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Директор института прикладной математики и компьютерных наук,
заведующий кафедрой информационной безопасности
ФГБОУ ВО «Тульский государственный университет»,
доктор технических наук, доцент

Алексей Алексеевич Сычугов
22 декабря 2025 г.

Докторская диссертация защищена по специальности 05.13.01 – Системный анализ, управление и обработка информации (по отраслям)

Даю согласие на обработку персональных данных.

Место работы:
ФГБОУ ВО «Тульский государственный университет»
300012, г. Тула, пр. Ленина, д.92
e-mail: xru2003@list.ru
Телефон: 9-960-594-88-53

