

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07 НА БАЗЕ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ
НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____
решение диссертационного совета от 19.01.2026 № 1

О присуждении Иниватову Даниилу Павловичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Нейросетевая аутентификация по голосовым паролям с защитой биометрических эталонов и учётом функционального состояния пользователя» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 14.11.2025 г., протокол № 12 диссертационным советом 24.2.479.07 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданного приказом Министерства образования и науки Российской Федерации от 24.03.2023 г. № 542/нк (с изменениями приказами от 18.12.2023 г. № 2368/нк и от 11.06.2024 г. № 581/нк).

Соискатель **Иниватов Даниил Павлович**, 11 февраля 1997 года рождения, работает ассистентом кафедры «Комплексная защита информации» радиотехнического факультета федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет» Министерства науки и высшего образования Российской Федерации.

В 2020 г. с отличием окончил ФГАОУ ВО «Омский государственный технический университет» по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере. В 2024 г. окончил очную аспирантуру ФГАОУ ВО «Омский государственный технический университет» по направлению подготовки 09.06.01 Информатика и вычислительная техника.

Диссертация выполнена на кафедре «Комплексная защита информации» ФГАОУ ВО «Омский государственный технический университет» Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, Сулавко Алексей Евгеньевич, профессор кафедры «Комплексная защита информации» ФГАОУ ВО «Омский государственный технический университет».

Официальные оппоненты:

1. Катасёв Алексей Сергеевич, доктор технических наук, профессор, профессор кафедры систем информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»;

2. Исмагилова Альбина Сабирьяновна, доктор физико-математических наук, доцент, заведующий кафедрой управления информационной безопасностью федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий», **дали положительные отзывы о диссертации.**

Ведущая организация – федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет», г. Пенза, в своем положительном отзыве, подписанном заведующим кафедрой «Информационная безопасность систем и технологий», кандидатом технических наук, доцентом Зефировым Сергеем Львовичем, доцентом кафедры «Информационная безопасность систем и технологий», доктором технических наук, Егоровой Натальей Алексеевной, доцентом кафедры «Информационная

безопасность систем и технологий», кандидатом технических наук, доцентом Ивановым Алексеем Петровичем, и утвержденном проректором по научной работе и инновационной деятельности, доктором экономических наук, профессором Васиным Сергеем Михайловичем, указала, что диссертация Иниватова Даниила Павловича на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании проведенных автором исследований решена научная задача, заключающаяся в разработке модели, метода, алгоритма, методики и программного модуля для создания биометрической системы аутентификации по голосовым паролям, устойчивой к изменению функционального состояния (ФС) пользователя, на основе нейросетевых алгоритмов доверенного искусственного интеллекта, результаты которой обладают научной новизной, теоретической и практической значимостью.

Диссертация соответствует требованиям пункта 9, 10, 11, 13, 14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (в редакции от 25.04.2024 г.), а её автор, Иниватов Даниил Павлович, заслуживает присуждения ему ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 17 опубликованных работ, в том числе: 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 5 статей в ведущих зарубежных рецензируемых журналах, индексируемых в базах данных Web of Science и Scopus, из них 1 статья, входящая в первый квартиль (Q1), 8 статей в других изданиях, 4 свидетельства о регистрации программы ЭВМ. 5 публикаций выполнены соискателем единолично, остальные в соавторстве, при непосредственном участии соискателя.

Общий объем публикаций – 9,94 п. л., авторский вклад – 4,78 п. л. Наиболее значимые работы по теме диссертации:

1. Иниватов, Д. П. Аналитическое исследование проблемы биометрической идентификации и аутентификации субъектов по голосу / Д. П. Иниватов // Вопросы

защиты информации. – 2023. – № 3(142). – С. 28-38. – DOI 10.52190/2073-2600_2023_3_28.

2. Аутентификация по голосовым паролям с обеспечением конфиденциальности биометрических данных на основе корреляционных нейронов / А. Е. Сулавко, Д. П. Иниватов, В. И. Васильев [и др.] // Информационно-управляющие системы. – 2024. – № 2(129). – С. 21-38. – DOI 10.31799/1684-8853-2024-2-21-38.

3. Иниватов Д.П. Аутентификация по голосовому паролю с учётом функционального состояния пользователя / Вестник УрФО № 3(57), 2025. С. 61–72.

4. Inivatov D. P., Sulavko A. E., Samotuga A. E. The Study of an Impact of Alcohol Intoxication on Voice Parameters in Biometric Authentication Systems //2023 Dynamics of Systems, Mechanisms and Machines (Dynamics). – IEEE, 2023. – С. 1-6.

5. Sulavko A. et al. Biometric-based key generation and user authentication using voice password images and neural fuzzy extractor //Applied System Innovation. 2025.T. 8. №. 1. С. 13.

6. Преобразователь образов голосовых паролей дикторов в криптографический ключ на основе комитета предварительно обученных сверточных нейронных сетей / Сулавко А.Е., Иниватов Д.П., Стадников Д.Г. [и др.] // Вопросы защиты информации. – 2021. - №4. – С. 23-33.

7. Влияние психофизиологического состояния диктора на параметры его голоса и результаты биометрической аутентификации по речевому паролю / А.Е. Сулавко, А.В. Еременко, Р.В. Борисов, Д.П. Иниватов // Компьютерные инструменты в образовании, 2017 г., с. 29-47.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации; соискатель ссылается на авторов и источники заимствования.

На диссертацию и автореферат поступили **положительные** отзывы, в которых содержатся ряд замечаний:

– **ведущей организации** федерального государственного бюджетного образовательного учреждения высшего образования «Пензенский государственный университет», г. Пенза. *Замечания:* 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.

– **официального оппонента**, доктора технических наук, профессора, Катасёва Алексея Сергеевича, профессора кафедры систем информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ». *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».

– **официального оппонента**, доктора физико-математических наук, доцента, Исмагиловой Альбины Сабирьяновны, заведующего кафедрой управления информационной безопасностью, Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий». *Замечания:* 1. В экспериментах, описанных во второй главе (п. 2.5), показано, что при переходе пользователя в изменённое 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 всё ещё 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 усреднённый 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 счёт вынужденного повторного использования пар? 5. Модель CatBoost показывает высокую точность распознавания ФС, но при этом обучалась на признаках, извлечённых из предобученных моделей (ESCAP-TDNN, Wav2Vec2 и др.). Не создаёт ли это риска утечки биометрической информации на этапе передачи признаков между модулями? Как обеспечивается защита этих высокоуровневых представлений в «защищённом режиме»?

Получено **шесть положительных** отзывов на автореферат:

1. Федеральное государственное автономное образовательное учреждение высшего образования «Сибирский федеральный университет» (г. Красноярск), кандидат технических наук, доцент, руководитель центра искусственного интеллекта, доцент кафедры систем искусственного интеллекта, **Пятаева Анна Владимировна** *Замечания:* 1. В автореферате недостаточно подробно обсуждается влияние внешних акустических факторов (фоновый шум, микрофонов различных классов, reverberation) на работу ансамбля автокодировщиков и НПК. Для практического применения системы желательно оценить её устойчивость к указанным типам возмущений. 2. Представленный подход демонстрирует высокую точность классификации ФС пользователя, однако распределение выборок по пяти состояниям может быть неравномерным. Было бы полезно включить анализ влияния дисбаланса классов и методов его компенсации.

2. Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (г. Челябинск), заведующий кафедрой компьютерной безопасности и прикладной алгебры, доктор технических наук, доцент, **Ручай Алексей Николаевич**. *Замечания:* 1. В работе отсутствует анализ влияния акцента или диалекта на эффективность предложенных методов. Вероятнее всего, полученные результаты точности аутентификации и выявления изменённого функционального состояния будут иными. 2. Также отсутствует оценка ресурсов и зависимости времени выполнения от размеров выборки, что важно для анализа масштабируемости системы в промышленных приложениях.

3. Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет» (г. Воронеж), заведующий лабораторией медицинской кибернетики, доктор технических наук, доцент, профессор кафедры цифровых технологий факультета компьютерных наук **Туровский Ярослав Александрович**. *Замечания:* 1. В описании экспериментов отсутствует информация о влиянии шумов на точность аутентификации. 2. Не обоснован выбор функциональных

состояний, отсутствует контроль ФС объективными методами. 3. Частота регистрации звуковых феноменов ограничена 8 кГц, однако диапазон голоса существенно шире. В автореферате отсутствует обоснование данного ограничения.

4. Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» (г. Москва), заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности», доктор технических наук, доцент, **Максимова Елена Александровна.** *Замечания:* 1. В работе отсутствует детальный анализ вычислительной сложности алгоритма настройки НПБК (третья глава), которая бы включала оценку времени для обучения. 2. Не проводилась оценка дрейфа данных вследствие возрастных изменений. 3. Недостаточно детализировано описание выбора параметров сверточной нейронной сети для извлечения признаков (число слоёв, размер шага, ядра и т.д.).

5. Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет» (г. Тула), директор института прикладной математики и компьютерных наук, заведующий кафедрой информационной безопасности, доктор технических наук, доцент, **Сычугов Алексей Алексеевич.** *Замечания:* 1. В работе отсутствует анализ устойчивости разработанного НПБК к спуфинг-атакам и атакам с использованием воспроизведенных голосовых записей. 2. Автореферат содержит мало ссылок на исследования, которые позволили бы полноценно сравнить достигнутые показатели устойчивости НПБК к вариациям функционального состояния пользователя с аналогичными существующими подходами.

6. Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)» (г. Омск), и.о. зав. кафедрой «Информационная безопасность», кандидат технических наук, **Толкачева Елена Викторовна.** *Замечания:* 1. В тексте работы приводятся конкретные параметры обучения НПБК (длина ключа 1024 бита и 4 входа на нейрон), однако отсутствует объяснение, почему выбраны именно они и как они влияют на точность

аутентификации. 2. На с. 13 приводится сравнение устойчивости предлагаемого НПБК и модели GMM-UBM к изменениям функционального состояния, однако не приводятся параметры этой модели и детали её обучения, что затрудняет оценку сравнения.

Выбор официальных оппонентов и ведущей организации обосновывается их достижениями в данной отрасли наук, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации. Ведущая организация и оппоненты не имеют совместных проектов и публикаций с соискателем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **предложены:** 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;

- **разработаны:** статистическая модель голосовых образов пользователя, основанная на экспериментальных данных об изменении голосовых параметров у испытуемых обоих полов от 18 до 50 лет в различных функциональных состояниях (ФС), которая, в отличие от существующих ранее моделей, учитывает изменения голосовых биометрических признаков в различных ФС пользователя и позволяет предсказывать характер дрейфа биометрических данных; алгоритм настройки нейросетевого преобразователя «биометрия-код» (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; методика аутентификации по голосу с распознаванием ФС пользователя,

основанная на ансамблевых методах машинного обучения (МО), 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;

– **экспериментально доказана** эффективность и целесообразность применения разработанных метода, моделей, алгоритмов и методики, а также программного модуля для решения задачи нейросетевой аутентификации по голосовым паролям с защитой биометрических эталонов и учетом ФС пользователя, позволяющих учитывать дрейф биометрических данных в измененных ФС, а также противодействовать компрометации биометрических шаблонов.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (то есть с получением обладающих новизной результатов) **использованы** методы теории информационной безопасности, классификации и идентификации образов, биометрической аутентификации, теории вероятностей и математической статистики, спектрального и корреляционного анализа, аппарат искусственных нейронных сетей (ИНС);

– **изложены** аргументы и факты, подтверждающие актуальность разработки методов и алгоритмов защищенной биометрической аутентификации по голосу с учетом ФС и защиты шаблонов, отличительной особенностью которых является использование ансамбля автокодировщиков и двух типов нейронов в НПБК, что обеспечивает устойчивость к дрейфу данных и повышает защищенность процедуры биометрической аутентификации по голосу от атак на биометрическое предъявление;

– **раскрыты** противоречия, связанные с применением существующих систем голосовой биометрии, а также установлено отсутствие комплексного решения на основе НПБК, способного учитывать дрейф биометрических данных, вызванный сменой ФС пользователя, и оказывать противодействие атакам, направленным на

компрометацию биометрических эталонов НПБК, обеспечивающего реализацию процедуры аутентификации;

– **изучены** современные подходы к защищенной биометрической аутентификации по голосу на основе НПБК, уделено внимание уязвимостям, характерным для систем на их основе, а также существующим методам защиты биометрических данных, на основании чего сделан вывод о необходимости повышения защищённости процедуры биометрической аутентификации пользователя по голосу и учёта его ФС;

– **проведена модернизация** известных методов защиты информации на основе защищенной нейросетевой биометрической аутентификации с помощью НПБК и с использованием моделей и алгоритмов его обучения на базе двух типов нейронов, каждый из которых осуществляет обработку голосовых данных с различным уровнем взаимной корреляции, что обеспечивает более высокую точность аутентификации пользователя в условиях дрейфа биометрических данных.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– **разработаны и внедрены** в бизнес-процессы компаний ООО «ОСМИ-ИТ» г. Москва, а также в учебный процесс ФГАОУ ВО «Омский государственный технический университет»: статистическая модель, учитывающая особенности изменения голосовых образов; метод извлечения признаков при помощи ансамблирования автокодировщиков на базе свёрточных слоёв, обрабатывающих различные представления голосового образа и повышающий точность аутентификации; методика биометрической аутентификации по голосу с распознаванием функционального состояния пользователя; программный модуль, реализующий алгоритм настройки модели НПБК, в рамках существующей системы;

– **определены** рекомендации по практическому применению результатов диссертационной работы для реализации защищенной биометрической аутентификации по голосу в организациях и приложениях, в которых требуется

устойчивость к дрейфу при изменении ФС и обеспечение требуемого уровня безопасности при работе с биометрическими данными;

– **разработаны** алгоритм настройки модели НПБК, методика биометрической аутентификации по голосу с распознаванием ФС пользователя и программный модуль, реализующий алгоритм настройки модели НПБК;

– **представлены** результаты экспериментальной оценки и показатели эффективности применения разработанных методов и алгоритмов, подтверждающие практическую значимость предложенных решений. Эксперименты показали, что в изменённых состояниях EER для предложенной модели растёт всего на 29 % (с 2,1 % до 2,71 %), в то время как для существующих моделей, рост составляет 52 % (с 8,1 % до 12,3 %). Применение НПБК и алгоритма классификации ФС позволяет достичь метрики макро-F1 = 0,954.

Оценка достоверности результатов исследования выявила:

– **для экспериментальных работ** использованы разработанные диссертантом программные средства, модифицированный программный комплекс AIC Desktop, персональные компьютеры, а также подготовленные диссертантом и открытые наборы обучающих данных;

– **теоретическая часть работы** базируется на использовании известных положений, подходов, принципов и технологий биометрической аутентификации, методов машинного обучения и защиты биометрических данных. Она опирается на результаты вычислительных экспериментов, а также на проверяемые и апробированные данные и факты. Положения согласуются с опубликованными ранее работами и экспериментальными результатами других авторов, что обеспечивает научную обоснованность и преемственность представленных выводов;

– **идея базируется** на результатах анализа современных подходов к голосовой аутентификации с учётом функционального состояния пользователя, а также анализе современных реализаций нейросетевых методов обработки данных, биометрических криптосистем и их уязвимостей;

– **использованы** экспериментальные данные голосовых сигналов в различных функциональных состояниях (нормальное, сонливость, три градации алкогольного опьянения), что позволило провести комплексный анализ эффективности предложенных решений. Результаты экспериментальной оценки показали, что предложенные методы по точности аутентификации не уступают существующим аналогам, при этом демонстрируют более высокую защищенность от атак компрометации биометрических образов, способны учитывать ФС пользователя при голосовой аутентификации, а также выявлять изменённое ФС пользователя; Ансамблирование нейросетевых моделей увеличивает информативность признаков, снижая чувствительность к шуму и вариациям ФС, что приводит к снижению EER на 5,07%;

– **установлено** совпадение авторских результатов с результатами решений задач защиты биометрических шаблонов и учета функционального состояния, представленных в независимых исследованиях, при этом улучшены показатели эффективности и защищенности процедуры аутентификации, такие как точность распознавания, устойчивость к дрейфу голосовых признаков и противодействие атакам на извлечение знаний из классификатора.

Личный вклад соискателя состоит: в постановке целей и задач исследования, анализе современного состояния научных разработок в области биометрической аутентификации на основе искусственных нейронных сетей и защиты биометрических данных с учетом функционального состояния, разработке модели, метода, алгоритма, методики и программного модуля, представленных в диссертационной работе; организации и проведении экспериментов для оценки эффективности предложенных решений; получении и интерпретации результатов на каждом этапе исследования, их апробации и подготовке основных публикаций по теме диссертации.

В целом, диссертация Иниватова Даниила Павловича «Нейросетевая аутентификация по голосовым паролям с защитой биометрических эталонов и учётом функционального состояния пользователя» представляет собой завершённую научно-квалификационную работу, в которой содержится решение

научной задачи, заключающейся в разработке модели, метода, алгоритма, методики и программного модуля для создания биометрической системы аутентификации по голосовым паролям, устойчивой к изменению функционального состояния пользователя, на основе нейросетевых алгоритмов доверенного искусственного интеллекта, имеющей важное значение для современной теории и практики обеспечения защиты биометрических данных в условиях возможного воздействия деструктивных факторов.

Диссертационный совет пришел к выводу о том, что в диссертации:

- соблюдены установленные Положением о порядке присуждения ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени кандидата технических наук;
- отсутствуют недостоверные сведения об опубликованных соискателем ученых степеней работах, в которых изложены основные научные результаты диссертации;
- соискатель ссылается на авторов и источники заимствования;
- оригинальность диссертационной работы составляет 95,72 %.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. В диссертационной работе явным образом не обозначены сферы применения разработанного программного модуля и методики.

Соискатель Иниватов Д.П. согласился с замечанием и привёл собственную аргументацию:

Предполагается, что основная область применения разработанной методики – это биометрические системы, в которых требуется дискреционный доступ, где необходимо регулировать уровень доступа в зависимости от выявленного ФС:

1. Проверка ФС при выполнении наиболее ответственных операций в банковских приложениях (оформление кредита или перевод крупных сумм);
2. Оценка ФС водителей в приложениях по вызову такси перед началом рабочей смены.

Разработанный программный модуль уже используется в образовательном процессе для формирования практических навыков студентов в области биометрии, цифровой обработки сигналов, извлечения признаков, построению различных архитектур нейросетевых преобразователей «биометрия-код», их обучения и анализа эффективности.

Диссертационная работа Иниватова Даниила Павловича на тему «Нейросетевая аутентификация по голосовым паролям с защитой биометрических эталонов и учётом функционального состояния пользователя» соответствует п. 9 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (в редакции от 25.01.2024 г.), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность по пунктам: 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».

Диссертация Иниватова Д.П. на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения научной задачи, заключающейся в разработке модели, метода, алгоритма, методики и программного модуля для создания биометрической системы аутентификации по голосовым паролям, устойчивой к изменению функционального состояния пользователя, на основе нейросетевых алгоритмов доверенного искусственного интеллекта, имеющей важное значение для современной теории и практики обеспечения защиты биометрических данных в условиях возможного воздействия деструктивных факторов.

На заседании 19.01.2026 г. диссертационный совет принял решение:

– за решение актуальной научной задачи, заключающейся в разработке модели, метода, алгоритма, методики и программного модуля для создания биометрической системы аутентификации по голосовым паролям, устойчивой к изменению функционального состояния пользователя, на основе нейросетевых алгоритмов доверенного искусственного интеллекта, имеющей важное значение для современной теории и практики обеспечения защиты биометрических данных в условиях возможного воздействия деструктивных факторов, присудить Иниватову Даниилу Павловичу ученую степень кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 14 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 18 человек, входящих в состав совета, проголосовали: за – 14, против – 0.

Председатель
диссертационного совета
д-р техн. наук, профессор



Султанов Альберт Ханович

Ученый секретарь
диссертационного совета
д-р техн. наук

Вульфин Алексей Михайлович

19 января 2026 года