На правах рукописи

Уймин Антон Григорьевич

СИСТЕМА НЕПРЕРЫВНО-ДИСКРЕТНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ АНАЛИЗА ПОТОКА ДАННЫХ КОМПЬЮТЕРНОЙ МЫШИ

Специальность 2.3.8 – «Информатика и информационные процессы»,
специальность 2.3.6 – «Методы и системы защиты информации, информационная безопасность»
(технические науки)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2026

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»

Научный руководитель:	**Белоусов Александр Валерьевич,** кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий федерального государственного автономного образовательного учреждения высшего образования "Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина"
Официальные оппоненты:	**Будзко Владимир Игоревич,** доктор технических наук, главный научный сотрудник Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) **Лаута Олег Сергеевич,** доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Института водного транспорта Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова»
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет»

Защита диссертации состоится «17» сентября 2026 г. в 11-00 на заседании диссертационного совета 24.1.107.03 при Федеральном государственном бюджетном учреждении науки Институте проблем управления им. В.А. Трапезникова Российской академии наук по адресу: 117997, Москва, Профсоюзная ул., 65, ИПУ РАН.

С диссертацией можно ознакомиться в библиотеке ИПУ РАН и на сайте университета https://www.ipu.ru

Автореферат разослан «__» _____ 202 г.

Учёный секретарь
диссертационного совета 24.1.107.03,
кандидат технических наук М. А. Романова

Общая характеристика работы.

Актуальность темы исследования.

В классической теории информационных процессов предполагается, что идентификация источника информации либо предшествует взаимодействию, либо осуществляется однократно в момент установления соединения (Шеннон, 1948; Альсведе и др., 2006). В децентрализованных системах существует априорно заданное множество идентификаторов субъектов доступа (база учетных записей), хранящееся на центральном сервере аутентификации. Это решает задачу начального разграничения доступа, но не обеспечивает динамическую устойчивость системы в условиях удаленного взаимодействия. Поскольку факт принадлежности субъекта к доверенному множеству устанавливается сервером однократно в момент входа, основная информационная нагрузка по обеспечению устойчивости системы переносится на постаутентификационную фазу. Основным вектором нарушения устойчивости при этом в настоящее время является не столько отказ аппаратных узлов, сколько компрометация субъекта доступа.

Механизм контроля подлинности в данном контексте перестает быть исключительно прикладной сервисной функцией и трансформируется в базовый информационный процесс обеспечения безопасности. При этом само наличие сервера аутентификации определяет уже практически традиционные векторы атак, критически значимые для децентрализованных и удаленных узлов (Walter M., 2024; Viega J., 2002): атака подмены контекста (CAPEC-593, злоумышленник перехватывает управление устройством легитимного пользователя уже после прохождения процедуры входа на сервере); атака отложенной компрометации (CAPEC-29, 60, 61, 226 и др., между моментом проверки подлинности сервером и моментом исполнения критической команды в децентрализованной среде субъект может быть заменен без повторного обращения к центральному серверу); деградация атрибутов субъекта (CAPEC-121, пользовательские ключи могут быть скомпрометированы, о чем сервер аутентификации остается неосведомленным до следующего планового запроса).

С точки зрения информационной безопасности, классическая парадигма, основанная на однократной проверке учетных данных сервером аутентификации, создает временную уязвимость: после успешного прохождения процедуры входа субъект получает мандат на выполнение операций в течение длительного времени. В условиях неопределенного числа удаленных пользователей риск компрометации сеанса на клиентской стороне или в канале связи между узлами децентрализованной сети многократно возрастает.

В отличие от дискретного «шлюзового» контроля, непрерывная аутентификация представляет собой особый класс информационных процессов, реализующих функцию мониторинга и верификации подлинности субъекта на всем протяжении активной фазы взаимодействия с системой.

Информационный процесс непрерывного контроля подлинности субъектов доступа характеризуется асинхронностью, высокой энтропией исходных данных, потоковой природой. Результат процесса — не бинарное решение, а непрерывная функция доверия, значения которой должны быть доступны подсистемам управления доступом в режиме реального времени.

Актуальность исследования в контексте информационных процессов обусловлена необходимостью формализации, моделирования и алгоритмизации непрерывных информационных потоков контроля подлинности, которые протекают параллельно с основными (целевыми) потоками данных. В отличие от классических задач сжатия или помехоустойчивого кодирования, здесь требуется анализ процесса сбора косвенных (поведенческих) признаков подлинности для минимизации задержки принятия решения при обнаружении аномалии, но при сохранении допустимой нагрузки на вычислительные узлы и каналы связи.

Актуальность исследования в контексте обеспечения информационной безопасности продиктована необходимостью ликвидации разрыва между доверием, установленным сервером, и реальной подлинностью оператора в каждый момент времени. Непрерывный контроль подлинности выступает здесь как механизм обеспечения свойства динамической устойчивости системы к атакам, направленным на легитимные сессии.

Таким образом, исследование выполнено на стыке двух научных направлений. С позиции информатики оно направлено на изучение класса непрерывных, слабоструктурированных информационных процессов, протекающих в фоновом режиме и обеспечивающих жизнеспособность сложных технических систем, а с позиции информационной безопасности - на решение критически важной прикладной задачи — защиты сессионного уровня в условиях стохастического множества удаленных акторов и наличия централизованного сервера аутентификации, но при отсутствии гарантий неизменности состояния клиентской среды в течение сеанса связи.

Одним из наиболее эффективных решений, способных обеспечить непрерывный фоновый мониторинг без прерывания целевой деятельности пользователя (наряду с основными потоками данных), является поведенческая биометрия. В отличие от статических биометрических признаков (геометрия лица, отпечаток пальца), требующих дискретного сканирования и несущих высокие риски компрометации чувствительных персональных данных в случае утечки, анализ поведенческих паттернов позволяет формировать оценку доверия непрерывно.

В качестве одного из наиболее перспективных направлений поведенческой биометрии в рамках данной работы рассматривается анализ динамики взаимодействия пользователя с компьютерной мышью. Данный подход обладает рядом фундаментальных преимуществ для построения систем непрерывной аутентификации: он позволяет извлекать уникальные цифровые признаки из стандартных потоков информационного обмена (движения курсора, клики, скроллинг) без необходимости оснащения рабочих

мест специализированными аппаратно-программными средствами сбора биометрии. Кроме того, математическая модель движения мыши представляет собой высокоэнтропийный поток данных, достаточный для поддержания непрерывной функции доверия, но при этом не позволяющий однозначно деанонимизировать личность пользователя за пределами конкретной информационной системы, что нивелирует риски нарушения конфиденциальности.

В основу исследования положена гипотеза о том, что интеграция методов потоковой обработки сигналов динамики компьютерной мыши в архитектуру сессионного уровня позволяет создать эффективный механизм непрерывной биометрической аутентификации, устойчивый к атакам подмены контекста.

Степень разработанности темы исследования.

Проблематика биометрической идентификации и аутентификации получила развитие в работах отечественных и зарубежных исследователей, рассматривающих как теоретические основы построения биометрических систем, так и вопросы их практической реализации в информационных средах различного назначения.

Существенное значение имеют работы Ю.П. Гаврильченко, М.Ю. Ларионова, И.Н. Карцана, А.А. Шелупанова и других авторов, в которых рассмотрены методы биометрической идентификации и аутентификации, включая анализ поведенческих признаков, распознавание лиц, обработку дактилоскопических данных и иные подходы к верификации личности.

Отдельное значение имеют исследования Е.К. Брагина, Т.И. Лапина, А.М. Трошкова, И.Е. Шакера и других авторов, посвященные цифровой обработке сигналов, математическому описанию биометрических признаков и их применению в задачах распознавания и классификации. Методологически близкими к теме исследования являются труды А.А. Дорофеюка, Ю.А. Дорофеюка, В.В. Кульбы, Р.В. Мещерякова, развивающие методы интеллектуального анализа данных, распознавания образов, поддержки принятия решений и обеспечения информационной безопасности. Эти исследования значимы для построения систем непрерывной биометрической аутентификации, поскольку анализ потока данных компьютерной мыши предполагает выделение поведенческих признаков, обработку динамических траекторий, классификацию состояний субъекта доступа и принятие решений о его подлинности в условиях вариативности и зашумленности данных.

Зарубежные исследования также оказали значимое влияние на развитие биометрических технологий, включая модели поведенческой аутентификации, оценку устойчивости биометрических признаков и повышение надежности распознавания пользователей. В их числе J. Wayman, D. Bhattacharyya, A.C. Weaver, A.K. Jain, Z. Rui и др.

Целью диссертационной работы является разработка методов повышения эффективности информационных процессов аутентификации пользователей информационных систем с применением нейросетевых технологий на основе создания программной системы, обеспечивающей непрерывно-дискретную биометрическую аутентификацию.

Для достижения указанной цели в рамках исследования были поставлены и решены следующие **задачи**:

- Проведен анализ существующих подходов к идентификации и аутентификации пользователей для выявления ограничений, влияющих на стоимость и качество решения.
- Исследованы возможности использования в информационных процессах аутентификации стандартных средств ввода-вывода персональных компьютеров.
- Разработан новый метод аутентификации пользователя на основе индивидуальных признаков, выделяемых в потоке данных, получаемых от компьютерной мыши.
- Сформулированы требования к программной системе, обеспечивающей постоянную (непрерывно-дискретную) биометрическую аутентификацию пользователей по результатам анализа.
- Создана программная реализация системы непрерывно-дискретной биометрической аутентификации пользователей.
- Предложены рекомендации по применению разработанной системы в различных контекстах.

Объектом исследования являются информационные процессы в децентрализованных автоматизированных информационных системах с разграничением доступа, применяемые для аутентификации пользователей.

Предметом исследования выступают методы, модели, алгоритмические и программные средства обработки информации для аутентификации пользователей, реализуемые на основе анализа поведенческих (биометрических) паттернов.

Научная новизна работы заключается в следующем:

1. Предложен новый метод аутентификации пользователей на основе динамики движения компьютерной мыши, отличающийся устойчивостью к поведенческой изменчивости пользователей и наличием механизмов адаптации к разнородным условиям взаимодействия, что позволяет усовершенствовать информационные процессы аутентификации в части повышения точности цифровой интерпретации поведения в условиях удалённого доступа (пункт 3 паспорта специальности 2.3.8, пункт 2 паспорта специальности 2.3.6).
2. Разработана многоуровневая модель информационного процесса удалённого управления, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, что обеспечивает возможность формализации и автоматической интерпретации действий пользователя как информационного субъекта, находящегося вне

контролируемой зоны, для проведения его аутентификации (пункт 1 паспорта специальности 2.3.8, пункт 12 паспорта специальности 2.3.6).

3. Разработана архитектура системы биометрической аутентификации на основе сверточных нейронных сетей, учитывающая особенности непрерывно-дискретного поведенческого потока при удаленной работе и предусматривающая режим адаптивного обучения, что обеспечивает устойчивую классификацию цифрового поведения в реальном времени с высокой точностью при низкой вычислительной нагрузке (пункт 9 паспорта специальности 2.3.8, пункт 15 паспорта специальности 2.3.6).

Теоретическая значимость работы состоит в развитии подходов к моделированию информационных процессов удалённого взаимодействия пользователей с информационными ресурсами, формализации цифрового поведения субъекта, находящегося вне контролируемой зоны, и применению методов поведенческой биометрии в задачах аутентификации. Предложенные модели и методы могут использоваться для анализа непрерывно-дискретных информационных потоков, формирования паттернов цифрового поведения и их распознавания в условиях нестабильных коммуникационных сред.

Практическая значимость работы заключается в повышении эффективности цифрового контроля административных действий путем внедрения программной системы, реализующей предложенные методы анализа поведенческих признаков без использования дополнительного оборудования. Полученные результаты применены при построении систем доверенного удалённого доступа, в том числе в инфраструктурах образовательных, корпоративных и телекоммуникационных систем, а также при разработке решений в области информационной безопасности с акцентом на подтверждение подлинности субъектов управления.

Результаты диссертационного исследования докладывались и получили положительную оценку на следующих международных, всероссийских и региональных научных конференциях:

− при подготовке и участии в 2021 Asia-Pacific Best Practice Marathon (Марафон лучших практик Азиатско-Тихоокеанского региона), проводившемся на базе Хабаровского края с участием стран АТР и СНГ по компетенции «Сетевое и системное администрирование»; результаты разработанной системы использовались для организации безопасного доступа к удаленной инфраструктуре, отслеживания соответствия заявленного пользователя фактическому участнику и анализа поведенческой активности пользователей (акт внедрения от 25.03.2022);

− в ходе проведения отраслевого чемпионата REASkills-2022 ГК «Росатом», где компоненты методики биометрического мониторинга применялись в рамках имитационного модуля цифровой безопасности (акт внедрения от 14.04.2022);

− при разработке учебных и контрольно-оценочных материалов в Ростовском государственном экономическом университете (РИНХ), на факультете компьютерных технологий и информационной безопасности, где

результаты диссертационной работы использовались в учебном процессе кафедры информационных систем и прикладной информатики при проведении текущей аттестации студентов бакалавриата по дисциплине «Инфокоммуникационные системы, сети и технологии» (акт внедрения от 26.09.2024);

− при разработке учебных и методических материалов в Санкт-Петербургском горном университете императрицы Екатерины II, где разработанная система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши использовалась в учебном процессе института базового инженерного образования на кафедре информационных систем и вычислительной техники при выполнении практических работ по дисциплинам «Надежность информационных систем» и «Вычислительные системы», а также при выполнении курсовой работы по дисциплине «Инструментальные средства информационных систем» (акт внедрения от 25.09.2024);

− при разработке учебных и научно-методических материалов в Федеральном государственном бюджетном образовательном учреждении высшего образования «Северо-Кавказский горно-металлургический институт (государственный технологический университет)» (2024 г.), где технологии биометрической аутентификации использовались в лабораторном практикуме по дисциплине «Информационная безопасность» (акт внедрения от 20.09.2024);

− в Учреждении образования «Гомельский государственный университет имени Франциска Скорины» (2024 г., Республика Беларусь) — при реализации межфакультетской программы по кибербезопасности с интеграцией результатов диссертационного исследования в модуль поведенческой аутентификации пользователей в обучающих информационных системах (акт внедрения от 23.09.2024).

Разработанные модули программного обеспечения прошли государственную регистрацию программ для электронных вычислительных машин (получены свидетельства о регистрации программ для ЭВМ № 2021619990, № 2021615378, № 2021614803, № 2021614735, № 2021614613, № 2021661218, № 2023683139).

Методы исследования. В диссертационной работе применяются методы системного анализа, теории информационных процессов, теории вероятностей и математической статистики. Для обработки поведенческих биометрических признаков использован аппарат машинного обучения, в частности, алгоритмы на основе свёрточных нейронных сетей (CNN). Используются методы цифровой обработки сигналов, регрессионный и корреляционный анализ, методы многокритериальной оценки эффективности, а также критерии статистической достоверности (ROC-анализ, FAR/FRR/EER).

Для построения и верификации модели цифрового информационного взаимодействия администратора с системой применялись методы

имитационного моделирования и экспериментальной оценки устойчивости цифрового поведения в условиях удалённого доступа. В рамках аналитического этапа использовались структурный и сравнительный анализ научной, патентной и технической литературы, а также опросы специалистов в области информационной безопасности.

Положения, выносимые на защиту:

1. Метод непрерывно-дискретной биометрической аутентификации, основанный на применении глубокого обучения (CNN) для автоматического извлечения пространственно-временных признаков динамики мыши. Метод обеспечивает устойчивую верификацию цифрового профиля в режиме реального времени с точностью (Accuracy) до 98,50 % в сценарии одиночных движений и минимальным уровнем половинной частоты ошибок (HTER = = 0,0120) при обработке комплексных поведенческих паттернов (координатно-временных траекторий перемещения, наведения и кликов). При этом вычислительный алгоритм характеризуется низким уровнем ресурсоемкости, обеспечивая суммарную нагрузку на компоненты пользовательской системы в пределах 7,1 %, что не снижает общую производительность среды функционирования.
2. Многоуровневая модель информационного процесса удалённого доступа, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, что позволяет снизить число ложноположительных событий в 1,5 раза по сравнению с аналогами.
3. Архитектура системы биометрической аутентификации на основе сверточных нейронных сетей, учитывающая динамику и структуру поведенческих сигналов непрерывно-дискретного поведенческого потока при удаленной работе и предусматривающая режим адаптивного обучения, повышает устойчивость биометрических систем к колебаниям пользовательского поведения до 15 % в эксперименте с контрольными группами.

Достоверность результатов обеспечивается за счет корректного применения математического аппарата, методов имитационного моделирования, программного обеспечения и подтверждается экспериментами на эмпирических наборах данных, включая вышеперечисленные апробационные мероприятия, но не ограничиваясь ими. Все реализованные методы подробно описаны.

Апробация работы. Основные положения и результаты работы докладывались и обсуждались на ряде конференций:

ГОД	Название конференции и место проведения конференции
2022	Skills Camp в рамках подготовки к BRICS Future Skills Challenge 2022 по кибербезопасности (Информационная безопасность), Москва
2022	Третья всероссийская научно-практическая конференция: «Цифровая трансформация промышленности: новые горизонты», Москва
2022	Первая Российская конференция «Образовательная инициатива: Школа будущего», МГИМО, Москва

ГОД	Название конференции и место проведения конференции
2023	International Scientific Siberian Transport Forum - TransSiberia 2023, Новосибирск
2023	Всероссийская научно-практическая конференция «Обеспечение информационной безопасности: вопросы теории и практики», Институт права, социального управления и безопасности, ФГБОУ ВО «Удмуртский государственный университет», Ижевск
2023	II Всероссийская научно-практическая конференция «Современные цифровые технологии», Алтайский государственный технический университет им. И.И. Ползунова, Барнаул
2023	Конференция «Киберугрозы транспортной отрасли», организатор - Positive Technologies, Москва
2023	V Научно-практическая конференция «Формирование и развитие культуры информационной безопасности субъектов образовательного пространства», РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва
2024	Национальный исследовательский университет МЭИ «Тридцатая международная научно-техническая конференция студентов и аспирантов радиоэлектроника, электротехника и энергетика», Москва
2024	II Научно-практической конференции «Актуальные проблемы защиты информации: современность и перспективы», МГТУ им. Баумана, Москва
2024	397-е заседание Томского IEEE-семинара, ТУСУР, Томск
2024	VI Международная научная конференция, посвященная академику Б. В. Бокутю «Проблемы взаимодействия излучения с веществом», Гомель, Беларусь
2025	VI Евразийский творческий форум «EURASIA 2025: SAFETY, SUSTAINABILITY AND INNOVATION» «ЕВРАЗИЯ 2025: БЕЗОПАСНОСТЬ, УСТОЙЧИВОСТЬ И ИННОВАЦИИ», Алматы
2025	2025 9th International Conference on Information, Control, and Communication Technologies (ICCT), Gomel, Belarus

Соответствие паспорту специальности

Работа выполнена в соответствии со следующими пунктами паспорта научной специальности *2.3.8 «Информатика и информационные процессы»*:

П.1. Разработка компьютерных методов и моделей описания, оценки и оптимизации информационных процессов и ресурсов, а также средств анализа и выявления закономерностей на основе обмена информацией пользователями и возможностей используемого программно-аппаратного обеспечения.

П.3. Разработка методов и алгоритмов кодирования, сжатия и размещения информации для повышения эффективности и надежности функционирования инфокоммуникационных систем при её хранении и передаче.

П.9. Разработка архитектур программно-аппаратных комплексов поддержки цифровых технологий сбора, хранения и передачи информации в инфокоммуникационных системах, в том числе, с использованием «облачных» интернет-технологий и оценка их эффективности.

Работа выполнена в соответствии со следующими пунктами паспорта научной специальности *2.3.6 «Методы и системы защиты информации, информационная безопасность»*:

П.2. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

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.

Публикации.

По материалам диссертационного исследования опубликовано 36 печатных работ. Из них 11 статей размещены в рецензируемых изданиях, входящих в перечень ВАК по соответствующим научным специальностям: 3 работы — по научной специальности 2.3.8, 6 работ — по научной специальности 2.3.6, 2 работы — по научным специальностям 2.3.8 и 2.3.6. Кроме того, опубликованы 3 работы в изданиях, индексируемых в базе Scopus, 1 работа — в издании, индексируемом в базе Web of Science, получено 7 свидетельств о государственной регистрации программ для ЭВМ. Также опубликованы 6 работ в прочих изданиях из перечня ВАК и 8 работ в иных рецензируемых изданиях, индексируемых в РИНЦ.

Личный вклад соискателя. Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно в ходе выполнения научных исследований. В публикациях, подготовленных в соавторстве, соискателю принадлежит ключевая роль в разработке методологических основ, построении моделей и алгоритмов, а также в проведении и интерпретации экспериментальных исследований.

Структура и объем работы.

Диссертационная работа включает в себя введение, 4 главы, заключение и список используемой литературы (189 ссылок). Материал диссертации изложен на 219 страницах машинописного текста, содержит 22 таблицы, 20 рисунков.

Содержание работы

Во **введении** обоснована актуальность темы диссертационной работы, сформулированы цель и основные задачи исследований, представлены научная новизна, теоретическая и практическая значимость полученных результатов.

Первая глава посвящена анализу специфики функционирования систем удаленного доступа, проблематике обеспечения их информационной

безопасности, а также исследованию существующих подходов к непрерывной идентификации и аутентификации пользователей.

В главе раскрываются определения и сущность аутентификации, в том числе биометрической, которая рассматривается как автоматизированное или полуавтоматизированное распознавание людей по физическим, поведенческим или психофизиологическим признакам. Выделяется три основные группы средств аутентификации: на основе биометрических данных, идентификатором и знания секретной информации. Наиболее перспективной считается биометрическая аутентификация, так как она обеспечивает высокую надежность и удобство использования.

Процедура биометрической аутентификации включает последовательное выполнение этапов регистрации биометрического признака, его предварительной обработки и анализа, формирования биометрического шаблона, сопоставления с эталонными данными и принятия решения о предоставлении либо отказе в доступе.

При разработке и эксплуатации биометрических систем необходимо учитывать ряд ограничений. К ним относятся вариативность биометрических характеристик у одного и того же пользователя, невозможность получения отдельных признаков в ряде эксплуатационных условий, риск имитации или подделки биометрических данных, необходимость их защищенного хранения и обработки, а также вопросы совместимости различных технических и программных решений.

Дополнительным фактором является необходимость соблюдения требований к защите персональных данных и обеспечению приватности пользователей, поскольку биометрическая информация относится к категории данных, компрометация которых может иметь долговременные последствия.

В заключительной части главы рассматриваются подходы к повышению эффективности биометрической аутентификации. К таким подходам относятся совершенствование алгоритмов обработки признаков, применение методов нормализации и фильтрации данных, повышение устойчивости биометрических шаблонов к атакам и использование организационно-технических мер, направленных на снижение вероятности несанкционированного доступа. Также рассматриваются стандарты и нормативная документация, направленные на улучшение безопасности и совместимости биометрических систем.

Основные теоретические положения и результаты первой главы диссертационного исследования изложены в работе [4]. В публикации проведен критический анализ уязвимостей традиционных средств аутентификации, основанных на факторе «обладания информацией», что послужило фундаментальным обоснованием необходимости перехода к биометрическим методам защиты.

Вторая глава посвящена исследованию возможностей использования в информационных процессах аутентификации стандартных средств ввода-вывода персональных компьютеров, включая разработку многоуровневой

модели информационного процесса, а также разработке нового метода биометрической аутентификации на основе индивидуальных признаков, выделяемых в потоке данных, получаемых от компьютерной мыши.

Подавляющее большинство традиционных высокоточных решений сопряжено с критическим барьером внедрения — необходимостью глубокой аппаратной модернизации клиентских автоматизированных рабочих мест (АРМ). Интеграция специализированных дактилоскопических сенсоров, считывателей рисунка вен или 3D-камер влечет за собой не только существенные капитальные затраты на закупку оборудования, но и экспоненциальный рост нагрузки на IT-инфраструктуру. Использование специализированных аппаратных средств биометрической защиты связано с дополнительными затратами на приобретение, внедрение и сопровождение оборудования, а также усложняет администрирование гетерогенного парка рабочих станций. В связи с этим представляет интерес подход, основанный на использовании штатных устройств ввода — компьютерной мыши и клавиатуры, которые являются типовыми компонентами пользовательского рабочего места.

Применение стандартной периферии позволяет перенести основную часть задач биометрической аутентификации в программный контур. Такой подход снижает зависимость системы от аппаратной совместимости конечных устройств, упрощает масштабирование решения и обеспечивает возможность внедрения механизмов непрерывной биометрической защиты без существенного изменения существующей инфраструктуры.

В рамках настоящего исследования основное внимание уделяется динамике работы пользователя с компьютерной мышью как поведенческому биометрическому признаку, отражающему индивидуальные особенности моторики, скорости, траекторий и характера пользовательских действий. Анализ этой динамики позволяет выявить уникальные способы взаимодействия пользователя с компьютерной системой, что делает методы на основе анализа движения мыши менее навязчивыми и более естественными для пользователей по сравнению с традиционными методами биометрической аутентификации.

Ключевыми компонентами многоуровневой модели биометрической аутентификации, описанной в главе (рисунок 1), являются сбор и анализ данных о поведении пользователей (рисунок 2), использование методов цифровой обработки сигналов для выявления уникальных поведенческих паттернов (рисунок 3), также применение алгоритма Дугласа-Пеккера.

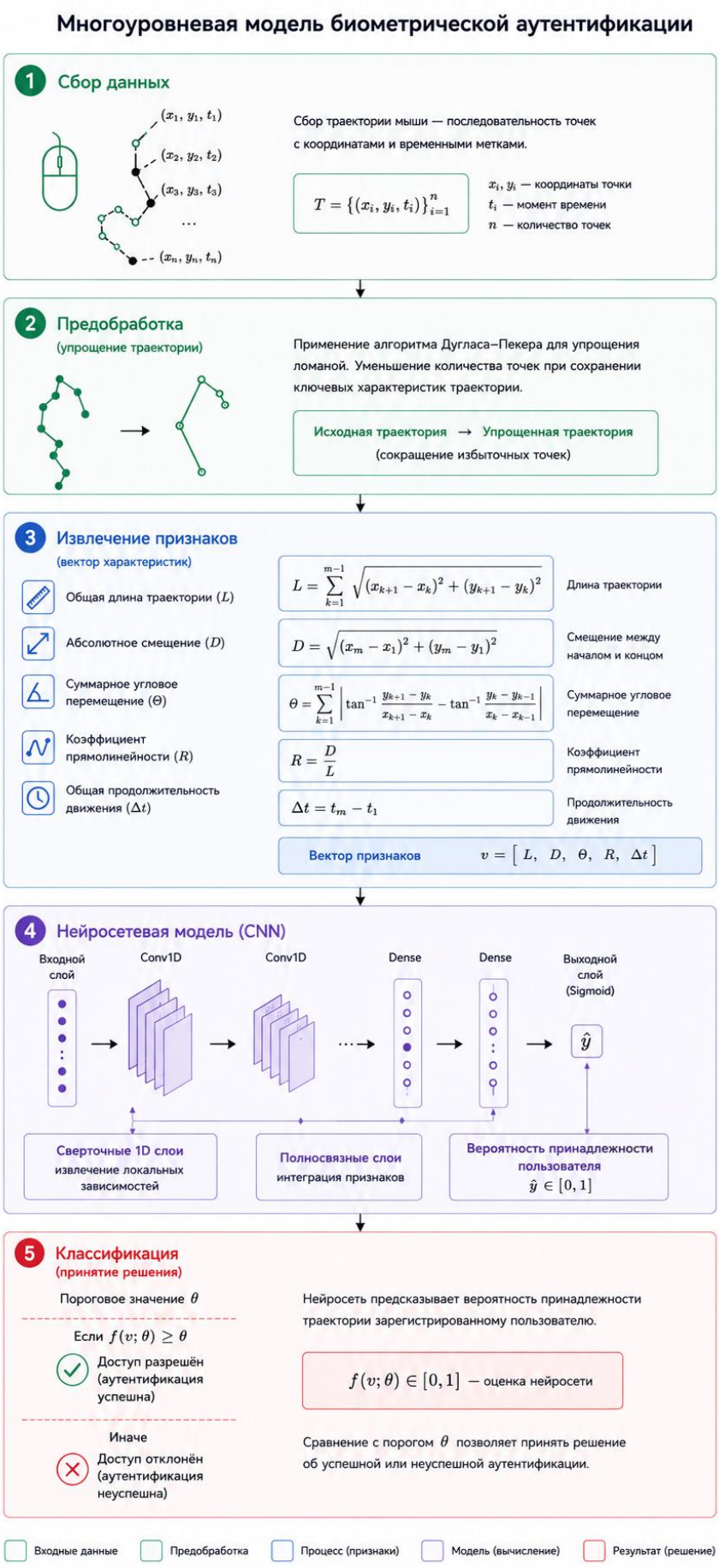

Рисунок 1. Многоуровневая модель биометрической аутентификации

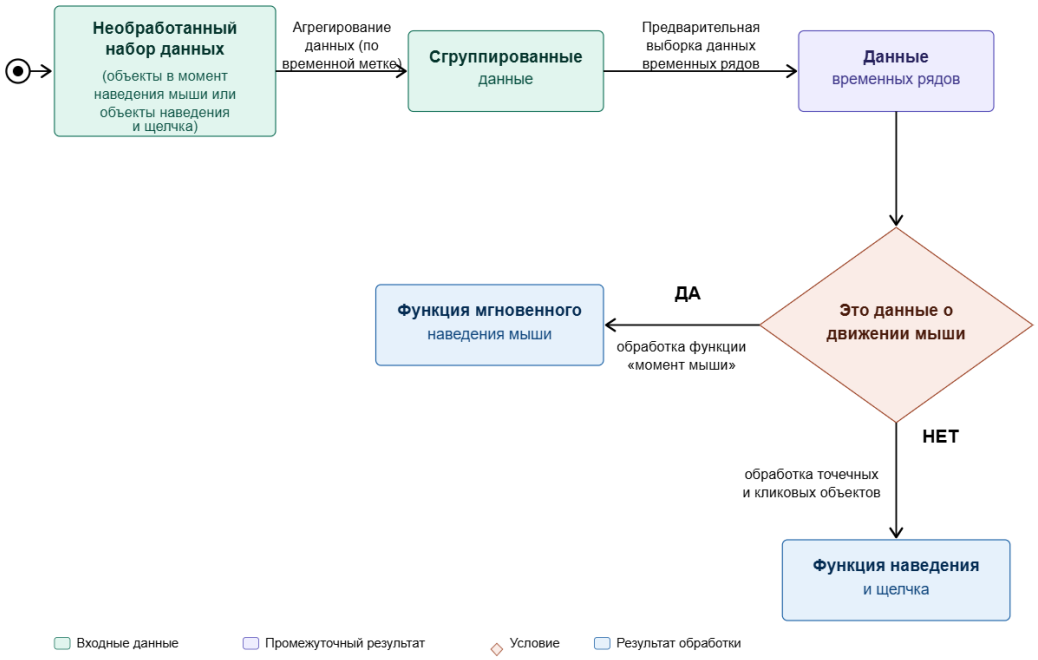

Рисунок 2. Схема действий по предварительной обработке данных

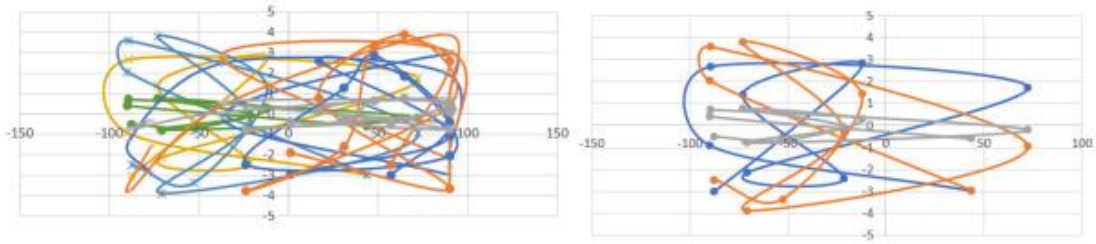

Рисунок 3. (а) Поведение пользователя при движении манипулятора, наведении курсора и щелчке. (б) Движение мыши, наведение курсора и щелчки манипулятора у трех пользователей.

В классическом виде практическая реализация описанной модели на базе полных массивов телеметрии неизбежно сталкивается с проблемой информационной избыточности. Высокая частота опроса манипулятора генерирует плотный поток координат, содержащий множество промежуточных точек на линейных и монотонных участках траектории. Обработка таких «сырых» пространственно-временных рядов напрямую нейронной сетью кратно увеличивает размерность входного вектора, что не только зашумляет процесс выделения биометрических признаков, но и неоправданно завышает вычислительную сложность инференса. Для обеспечения заявленной ранее минимальной ресурсоемкости на клиентском АРМ потребовался переход от ресурсозатратного пошагового анализа всех координат к экстракции чистого геометрического каркаса моторного действия.

Важным аспектом является обеспечение защищенности самих биометрических шаблонов. Исходя из предлагаемой модели угроз и модели

нарушителя, для защиты биометрических данных на всех этапах их обработки и хранения применяются криптографические методы преобразования.

Таким образом, разработка модели биометрической аутентификации на основе методов цифровой обработки сигналов компьютерной мыши направлена на создание эффективной и надежной системы, обеспечивающей высокий уровень безопасности и удобство для пользователя.

Результаты, полученные во второй главе, изложены в работах [1, 3, 5, 6, 8, 12]. Математическая формализация вычислительных процессов и разработка моделей безопасности подробно представлены в публикациях [6, 12]. Вопросы предобработки сигналов координатного устройства ввода как ключевого этапа поведенческой биометрии, а также их последующий интеллектуальный анализ, раскрыты в статьях [1, 8]. Методологические основы создания среды для функционирования и проверки алгоритмов, включая подходы к моделированию телекоммуникационных сетей и разработке их цифровых двойников, отражены в [3, 5].

<u>В третьей главе</u> описаны требования к информационной системе, ее реализация и экспериментальная оценка. Архитектура информационной системы, раскрытая в тексте главы, представлена на рисунке 4.

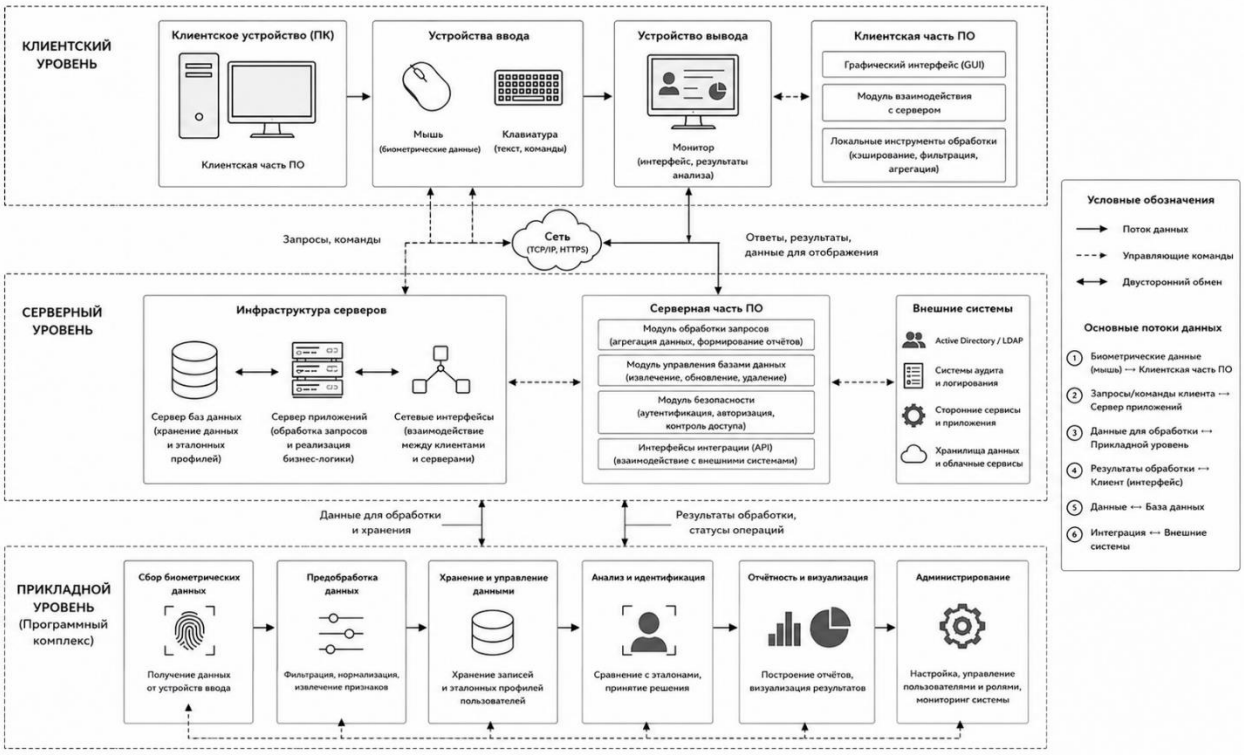

Рисунок 4. (а) Архитектура информационной системы.

Проведённые экспериментальные исследования подтвердили применимость методов машинного обучения и глубокого обучения для решения задачи поведенческой биометрической аутентификации пользователя по динамике работы с манипулятором «мышь». В рамках исследования были рассмотрены три сценария пользовательской активности: одиночное перемещение мыши, действие наведения с последующим щелчком,

а также комбинированный набор действий, включающий перемещение, наведение и щелчок. Сравнительный анализ классификаторов KNN, DT, RF и CNN показал, что используемые поведенческие признаки обладают достаточной информативностью для различения легитимного пользователя и потенциального нарушителя.

Наиболее устойчивые и результативные показатели были получены при использовании сверточной нейронной сети. По результатам экспериментальной оценки классификатор на основе сверточной нейронной сети показал наилучшие значения по совокупности метрик Accuracy, Recall, Precision и F1-score. Полученные результаты свидетельствуют о способности CNN-модели выделять информативные пространственно-временные закономерности из траекторий движения мыши и связанных с ними пользовательских действий.

В отдельных экспериментальных сценариях точность классификации достигала 98,50 %, а значение F1-score — 97,87 %. Это указывает на согласованность между полнотой выявления целевого класса и точностью принимаемых моделью решений.

Дополнительная оценка качества классификации по показателям FAR, FRR и HTER подтвердила преимущество CNN-модели не только по общей точности, но и по критериям, значимым для задач биометрической аутентификации. Снижение FAR характеризует уменьшение вероятности ошибочного допуска нарушителя, а снижение FRR — уменьшение вероятности ошибочного отклонения легитимного пользователя. Минимальные значения HTER для CNN указывают на сбалансированность модели при решении задачи непрерывной аутентификации и выявления аномального поведения.

Полученные результаты позволяют обосновать целесообразность применения сверточной нейронной сети в качестве основного классификатора в разрабатываемой системе биометрической идентификации и непрерывной аутентификации. Предложенный подход обеспечивает высокий уровень достоверности распознавания пользователя и может использоваться как дополнительный механизм защиты информационной системы от несанкционированного доступа.

Вместе с тем следует отметить ограничение проведенного исследования, связанное с отсутствием механизма адаптации модели к изменению разрешения экрана и параметров пользовательской среды. Данное обстоятельство определяет направление дальнейших исследований, связанных с повышением инвариантности модели к условиям эксплуатации, расширением экспериментальной выборки и совершенствованием процедур нормализации биометрических признаков.

Несмотря на указанное ограничение, результаты исследования подтверждают перспективность использования поведенческих данных, получаемых при работе с компьютерной мышью, для решения задач

биометрической аутентификации, анализа пользовательского поведения и повышения защищенности программных систем.

Эффективность и практическая значимость разрабатываемой системы биометрической аутентификации оцениваются с позиции ее функциональной пригодности, устойчивости к ошибкам классификации и применимости в условиях реальной эксплуатации. Данный комплексный критерий базируется на ключевых атрибутах функциональной пригодности и качества системы: точности классификации, латентности (времени принятия решения) и аппаратной ресурсоемкости (нагрузке на систему пользователя). В совокупности эти метрики детерминируют применимость решения в реальных условиях: высокая точность гарантирует надежность защиты от несанкционированного доступа, минимальное время отклика обеспечивает оперативность реагирования системы, а низкая вычислительная нагрузка позволяет интегрировать механизм фонового мониторинга без деградации производительности клиентского оборудования и снижения эргономики рабочего процесса.

Рассмотрим количественные критерии эффективности выбранной модели (в частности, время принятия решения и интегральную вычислительную нагрузку на клиентский АРМ) для сопоставления их с результатами оценки, проведенной в главе 2.

Для оценки временных характеристик конвейера аутентификации была проведена серия из 100 экспериментальных измерений.

Суммарное время принятия решения определялось как сумма временных затрат на сбор данных, передачу, обработку, сетевое взаимодействие и сопоставление с эталонным профилем:

$$T_d = T_{collect} + T_{transmit} + T_{process} + T_{network} + T_{compare} = 1000 \pm 10.73 \text{ мс}$$

Полученное значение среднего времени принятия решения составляет около одной секунды, что соответствует требованиям к системам непрерывной биометрической аутентификации. Такой уровень задержки обеспечивает возможность своевременного выявления отклонений в поведении пользователя и принятия решения о дополнительной проверке либо блокировке сессии.

Для оценки интегральной нагрузки на систему использовалась взвешенная модель потребления вычислительных ресурсов. Весовые коэффициенты для аппаратных подсистем были определены с учетом характера выполняемых операций и значимости соответствующих ресурсов для функционирования конвейера аутентификации.

Наибольший вес был присвоен процессорной подсистеме ($w_{\text{CPU}} = 0.5$). Это обусловлено тем, что инференс CNN-модели требует выполнения регулярных матричных операций, а обработка координат манипулятора в скользящем временном окне формирует преимущественно вычислительную нагрузку.

Для оперативной памяти был задан следующий весовой коэффициент:

($w_{\mathrm{Memory}} = 0.3$). Значимость данного ресурса связана с необходимостью хранения параметров обученной модели, буферизации потоковых данных и обеспечения обработки признаков в режиме, близком к реальному времени. Использование оперативной памяти для размещения промежуточных данных позволяет снизить задержки, связанные с обращением к внешним накопителям или файлу подкачки.

Дисковая подсистема ($w_{\mathrm{Disk}} = 0.2$): минимальный вес присвоен I/O операциям. В режиме фонового мониторинга обращения к диску сведены к минимуму: они ограничены лишь первичной загрузкой весов модели в память и асинхронным логированием событий безопасности (запись аудита), что не создает узких мест (bottlenecks).

В ходе эксперимента были зафиксированы следующие доли утилизации ресурсов процессом аутентификации:

CPU: 10% (0.10 в долях), память: 5% (0.05 в долях), дисковые операции: 3% (0.03 в долях)

Интегральная нагрузка рассчитывается по формуле взвешенной суммы:

$$L = 0.5 \cdot 0.10 + 0.3 \cdot 0.05 + 0.2 \cdot 0.03 = 0.05 + 0.015 + 0.006 = 0.071$$

Таким образом, итоговая нагрузка на систему L составляет 0.071 или 7.1 %. При сопоставлении этого значения с паттернами штатного использования клиентских АРМ, где чувствительная деградация пользовательского опыта начинается при фоновой загрузке свыше 50 %, можно констатировать, что решение работает с большим запасом производительности. Полученные значения доказывают, что система эффективно справляется с задачами аутентификации в реальном времени, оставаясь абсолютно незаметной для пользователя и не мешая выполнению его основных рабочих задач. Дальнейшие исследования могут быть направлены на снижение метрики L за счет квантования модели CNN или переноса части рутинных задач по сбору телеметрии на уровень модулей ядра операционной системы.

Основные результаты третьей главы, посвященные практической реализации и экспериментальной оценке предложенной модели биометрической аутентификации, нашли отражение в публикациях [9, 11, 13, 14, 16–22]. Эмпирическая оценка разработанных подходов, а также сравнение производительности различных алгоритмов машинного обучения в задачах классификации трафика и онлайн-аутентификации пользователей, представлены в статьях [9, 11, 13, 14]. Практическая реализация инструментария для отслеживания действий пользователя и обработки данных закреплена комплексом свидетельств о государственной регистрации программ для ЭВМ [16–22].

В четвертой главе проведен комплексный анализ потенциала и перспектив внедрения разработанной модели биометрической аутентификации в структуру современных информационных систем. Рассмотрены возможные модификации подсистемы анализа данных, ориентированные на повышение эффективности обработки пространственно-

временных признаков и расширение базиса регистрируемых параметров моторной активности пользователя. Сформулированы концептуальные направления синергии предложенного метода с иными биометрическими технологиями в рамках построения многоуровневых гибридных систем защиты. Особое внимание уделено оценке масштабируемости технологии, её адаптивности к гетерогенным средам функционирования, а также механизмам стандартизации и обеспечения конфиденциальности обрабатываемых данных.

Результаты исследований, составившие основу четвертой главы и отражающие перспективы практического применения разработанной модели, опубликованы в работах [2, 7, 10, 15]. Использование методов поведенческой биометрии для защиты систем с комплексной передачей данных и повышения безопасности сеансов удаленного администрирования обосновано в [7, 10]. Вопросы внедрения предложенных подходов в образовательный процесс при подготовке ИТ-специалистов, включая адаптацию педагогических методологий и применение отечественного телекоммуникационного оборудования, подробно рассмотрены в работах [2, 15].

В заключении приводятся основные результаты и выводы, полученные автором в ходе работы.

Основные результаты и выводы.

На основании выполненных исследований:

1. Разработан и экспериментально обоснован новый метод непрерывно-дискретной биометрической аутентификации на основе потоковых данных компьютерной мыши. За счет применения усовершенствованных алгоритмов обработки сигналов и глубокого обучения (CNN) обеспечено автоматическое извлечение пространственно-временных признаков пользователя. Метод позволяет осуществлять устойчивую классификацию цифрового профиля в режиме реального времени с точностью 97 % без использования специализированного аппаратного обеспечения, обеспечивая снижение вычислительной нагрузки на клиентский узел до 7,1 %.
2. Создана многоуровневая модель информационного процесса удалённого управления, формализующая и интерпретирующая действия пользователя как информационного субъекта, находящегося вне контролируемой зоны. Предложенная модель, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, позволила усовершенствовать процедуру аутентификации и сократить количество ложноположительных событий в 1,5 раза по сравнению с существующими решениями.
3. Спроектирована архитектура и реализована программная система (прототип) биометрической аутентификации, учитывающая специфику непрерывно-дискретного поведенческого потока. Интеграция в архитектуру механизмов адаптивного обучения позволила повысить устойчивость системы к естественной поведенческой изменчивости пользователей на 15 %. Практическая реализация предложенной архитектуры показала соответствие

разработанного программно-аппаратного комплекса требованиям, предъявляемым к системам фонового мониторинга и непрерывной биометрической аутентификации. Полученные результаты подтверждают возможность применения разработанного подхода в распределенных и децентрализованных информационных средах. Результаты исследования могут быть использованы при разработке и внедрении систем информационной безопасности в образовательных, государственных и корпоративных информационных системах, где требуется дополнительный механизм контроля легитимности пользовательской сессии.

Предложенный подход также может применяться для повышения уровня защиты персональных данных за счет использования поведенческих биометрических признаков, формируемых на основе работы пользователя со стандартными устройствами ввода. Это позволяет расширить функциональность существующих средств защиты без обязательного внедрения специализированного биометрического оборудования.

Кроме того, результаты работы могут быть использованы при модернизации действующих биометрических систем, в том числе за счет применения методов цифровой обработки сигналов, машинного обучения и анализа траекторных данных, получаемых при взаимодействии пользователя с компьютерной мышью.

Публикации автора по теме диссертации

В журналах из перечня ВАК по специальности 2.3.8:

1. **Уймин, А. Г.** Интеллектуальный анализ динамики трехпозиционного графического манипулятора типа "мышь" как элемента поведенческой биометрии / А. Г. Уймин // Системы управления и информационные технологии. – 2022. – № 2(88). – С. 92-96. – DOI 10.36622/VSTU.2022.88.2.018. – EDN XGHBWO.
2. **Уймин, А. Г.** , Греков В. С. Применение алгоритма Дугласа-Пеккера в вопросах онлайн-аутентификации инструментов удалённой работы при подготовке специалистов укрупнённой группы специальностей 10.00.00 "Информационная безопасность" / А. Г. Уймин, В. С. Греков // Электронные библиотеки. – 2024. – Т. 27, № 4. – С. 679-694. – DOI 10.26907/1562-5419-2024-27-4-679-694. – EDN QYROFU.
3. **Уймин, А. Г.** Цифровые двойники сетевых инфраструктур: точность, методы и практические решения / А. Г. Уймин // Радиотехнические и телекоммуникационные системы. – 2023. – № 3(51). – С. 44-52. – DOI 10.24412/2221-2574-2023-3-44-52. – EDN QUSITK.

В журналах из перечня ВАК по специальности 2.3.6:

4. Никитин, О. Р., **Уймин, А. Г.** Инфраструктура JSON Web Token. Реализация основных типов атак / О. Р. Никитин, А. Г. Уймин // Перспективы науки. – 2023. – № 2(161). – С. 28-34. – EDN VOHMOG.

5. **Уймин, А. Г.** , Никитин, О. Р. Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников / А. Г. Уймин, О. Р. Никитин // I-methods. – 2023. – Т. 15, № 2. – EDN NFJDVH.
6. **Уймин, А. Г.** , Морозов И. М. Оценка безопасности wine с использованием методологии stride: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164-170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP.
7. **Уймин, А. Г.** , Белоусов А. В. Поведенческая биометрическая аутентификация и ее применимость в системах с комплексной дискретно-непрерывной передачей данных / А. Г. Уймин, А. В. Белоусов // Системы управления, связи и безопасности. – 2025. – № 4. – С. 1-26. – DOI 10.24412/2410-9916-2025-4-001-026. – EDN WAOURY.
8. **Уймин, А. Г.** Предобработка данных манипулятора "мышь" для использования в анализе поведенческой биометрии / А. Г. Уймин // Научно-технический вестник Поволжья. – 2022. – № 7. – С. 94-97. – EDN NJNUTH.
9. **Уймин, А. Г.** , Никитин О. Р**.** Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры / А. Г. Уймин, О. Р. Никитин // Наукоемкие технологии в космических исследованиях Земли. – 2023. – Т. 15, № 2. – С. 33-40. – DOI 10.36724/2409-5419-2023-15-2-33-40. – EDN ELOYEH.

В журналах из перечня ВАК по специальностям 2.3.6 и 2.3.8:

10. **Уймин, А. Г.** , Белоусов А. В. Оценка возможностей применения поведенческой биометрии: анализ движений компьютерной мыши для защиты сеансов удаленного администрирования / А. Г. Уймин, А. В. Белоусов // Computational Nanotechnology. – 2025. – Т. 12, № 3. – С. 170-177. – DOI 10.33693/2313-223X-2025-12-3-170-177. – EDN BULODR.
11. **Уймин, А. Г.** Эмпирическая оценка методов машинного обучения в задачах онлайн-аутентификации / А. Г. Уймин // Вестник компьютерных и информационных технологий. – 2022. – Т. 19, № 8(218). – С. 49-57. – DOI 10.14489/vkit.2022.08.pp.049-057. – EDN EUAYKG.

В изданиях из перечня Scopus:

12. Demidenko O., **Uymin A.,** et al. Formalization of Computational Process Using Informative Coloring of User Resource Requests in a Local Area Network Node //2025 9th International Conference on Information, Control, and Communication Technologies (ICCT). – IEEE, 2025. – С. 1-4.
13. **Uymin A.** Application of machine learning in the classification of traffic in telecommunication networks: working with network modeling systems / A. Uymin // E3S Web of Conferences : International Scientific Siberian Transport Forum - TransSiberia 2023, Novosibirsk, Russia, 16–19 мая 2023

года. Vol. 402. – Novosibirsk, Russia: EDP Sciences, 2023. – P. 03001. – DOI 10.1051/e3sconf/202340203001. – EDN ZMBVYO.

14. **Uymin A.** User identification and authentication in browser environments via machine learning / A. Uymin // E3S Web of Conferences. – 2024. – Vol. 549. – P. 08019. – DOI 10.1051/e3sconf/202454908019. – EDN NPJUNS.

В журналах из перечня Web of Science:

15. **Uymin A.**, Grekov V. Applying the Douglas–Peucker Algorithm in Online Authentication of Remote Work Tools for Specialist Training in 10.00.00 “Information Security” Integrated Group of Specialties / A. G. Uymin, V. S. Grekov // Automatic Documentation and Mathematical Linguistics. – 2024. – Vol. 58, No. S4. – P. S265-S268. – DOI 10.3103/S0005105525700323. – EDN CJXWPX.

Свидетельства о регистрации программ для ЭВМ

16. Свидетельство о государственной регистрации программы для ЭВМ № 2021619990 Российская Федерация. RemoteTopology-модуль авторизации : № 2021613424 : заявл. 09.03.2021 : опубл. 21.06.2021 / **А. Г. Уймин**, С. В. Любкин. – EDN KEDGKG,
17. Свидетельство о государственной регистрации программы для ЭВМ № 2021615378 Российская Федерация. RemoteTopology-Администрирование : № 2021614090 : заявл. 16.03.2021 : опубл. 07.04.2021 / **А. Г. Уймин**. – EDN FTNONQ,
18. Свидетельство о государственной регистрации программы для ЭВМ № 2021614803 Российская Федерация. Программный модуль-тренажер подготовки к демонстрационному экзамену профессионального мастерства для обучения студентов СПО по специальности "Системное и сетевое администрирование" : № 2021613749 : заявл. 24.03.2021 : опубл. 30.03.2021 / **А. Г. Уймин**, В. О. Антонов, Д. А. Шерунтаев, М. М. Агафонова ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN CNHXZQ,
19. Свидетельство о государственной регистрации программы для ЭВМ № 2021614735 Российская Федерация. Программный интерфейс взаимодействия участников соревнований WorldSkills по компетенции 39 "Системное и сетевое администрирование" с удаленной сетевой инфраструктурой : № 2021613729 : заявл. 24.03.2021 : опубл. 29.03.2021 / **А. Г. Уймин**, М. М. Агафонова, Д. А. Шерунтаев, М. И. Костарев ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN RNAFOG,
20. Свидетельство о государственной регистрации программы для ЭВМ № 2021614613 Российская Федерация. Программная модель-симулятор сетевой инфраструктуры для обучения студентов ВПО и СПО по

компетенции 39 "Системное и сетевое администрирование" WorldSkills : № 2021613770 : заявл. 24.03.2021 : опубл. 26.03.2021 / **А. Г. Уймин** ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN FCAHFK,

21. Свидетельство о государственной регистрации программы для ЭВМ № 2021661218 Российская Федерация. RemoteTopology-Интерфейс пользователя : № 2021613953 : заявл. 16.03.2021 : опубл. 07.07.2021 / **А. Г. Уймин**, Л. М. Черкашин. – EDN NQQVEK,
22. Свидетельство о государственной регистрации программы для ЭВМ № 2023683139 Российская Федерация. Remote Topology extensions: Клиент-серверное браузерное расширение, обеспечивающие отслеживание действий пользователя с целью проведения биометрической аутентификации : № 2023682110 : заявл. 25.10.2023 : опубл. 02.11.2023 / **А. Г. Уймин**. – EDN MSIISH.