УТВЕРЖДАЮ

Первый проректор ФГБОУ ВО «МИРЭА – Российский технологический университет»

доктор химических наук,

профессор

_____ Н.И. Прокопов

«26» августа 2026 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет» на диссертационную работу Уймина Антона Григорьевича «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши», представленную на соискание учёной степени кандидата технических наук по научным специальностям 2.3.8 – «Информатика и информационные процессы» и 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования

Задача аутентификации пользователей информационных систем исторически рассматривалась как разовая процедура, выполняемая в момент установления логического соединения. Массовый переход к удалённой работе, распределённые автоматизированные системы, отсутствие жёсткого физического контроля над клиентскими рабочими местами и появление устойчивых векторов атак сессионного уровня (CAPEC-593 – подмена контекста, CAPEC-60, 61 – захват сеанса, CAPEC-29, 226 – отложенная компрометация,

CAPEC-121 – деградация атрибутов субъекта) привели к тому, что классическая «шлюзовая» модель более не обеспечивает требуемого уровня защищённости на постаутентификационной фазе. Между моментом успешного входа и завершением сеанса открывается устойчивое окно уязвимости, в котором злоумышленник действует от имени легитимного пользователя.

Решение этой проблемы за счёт статических биометрических методов (дактилоскопия, распознавание лица, радужной оболочки, рисунка вен) сопряжено с необходимостью массовой аппаратной модернизации клиентских автоматизированных рабочих мест, что критично для гетерогенных инфраструктур образовательных, корпоративных и государственных информационных систем. В связи с этим исследования, направленные на построение программно-определяемых систем непрерывной поведенческой аутентификации, использующих штатные средства ввода-вывода, представляют собой актуальное и практически значимое научное направление.

Диссертационная работа А.Г. Уймина посвящена решению данной задачи на базе анализа потока данных компьютерной мыши с применением аппарата глубокого обучения. Тема исследования лежит на пересечении двух научных специальностей: 2.3.8 (в части моделирования и оптимизации непрерывно-дискретных информационных процессов сбора, векторизации и потоковой обработки телеметрии, а также разработки архитектур программно-аппаратных комплексов) и 2.3.6 (в части разработки технологий идентификации и аутентификации пользователей и совершенствования средств защиты информации), что определяет её самостоятельную научную и прикладную ценность.

Структура и содержание диссертации

Диссертационная работа изложена на 219 страницах машинописного текста и состоит из введения, четырёх глав, заключения и списка литературы (189 наименований). Работа содержит 22 таблицы и 20 рисунков.

Во введении обоснована актуальность темы, сформулированы цель и задачи исследования, определены объект и предмет, обозначены научная новизна, теоретическая и практическая значимость, а также перечислены положения, выносимые на защиту.

Первая глава посвящена анализу информационных процессов аутентификации в распределённых системах. Показана принципиальная ограниченность парадигмы однократного шлюзового контроля, проведена классификация векторов атак сессионного уровня в терминах MITRE CAPEC, обоснован переход к парадигме непрерывного мониторинга подлинности. Систематизирован российский и международный нормативно-правовой контекст (ФЗ-152, ФЗ-149, ФЗ-572, ГОСТ Р 58624.2-2019, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 58833-2020, ISO/IEC 19794). Проведён сравнительный анализ статических и поведенческих биометрических методов с точки зрения требований к аппаратной модернизации, конфиденциальности и устойчивости к спуфингу.

Во второй главе разработана многоуровневая модель информационного процесса удалённого доступа, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков. Предложен признаковый базис (скорости, ускорения, рывки, угловые перемещения, кривизна), обоснован выбор модифицированного алгоритма Дугласа–Пекера для редукции размерности входного вектора нейросетевого классификатора, приведены соответствующие вычислительные соотношения и рассмотрены функции активации.

В третьей главе сформулированы требования к системе, описана её архитектура с разграничением серверной (обучение, эталонное профилирование) и клиентской (сбор телеметрии, локальный инференс) сторон. Проведены эксперименты с классификаторами KNN, Decision Tree, Random Forest и свёрточной нейронной сетью в трёх сценариях пользовательской активности

(перемещение, наведение с щелчком, комбинированный сценарий). Показано преимущество CNN-модели по совокупности метрик (Accuracy до 98,50 %, F1-score 97,87 %, HTER 0,0120), обоснована взвешенная модель интегральной ресурсоёмкости и получена оценка среднего времени принятия решения по 100 измерениям ($Td = 1000 \pm 10{,}73$ мс) при интегральной нагрузке на клиентский узел 7,1 %.

В четвёртой главе рассмотрены перспективы внедрения разработанной системы, возможные модификации подсистемы анализа, направления интеграции с другими биометрическими технологиями в многоуровневые гибридные схемы, вопросы масштабируемости, стандартизации и обеспечения конфиденциальности обрабатываемых данных.

В заключении приведены основные результаты и выводы, определены перспективные направления дальнейших исследований.

Работа хорошо структурирована, материал изложен последовательно, логика построения глав от аналитической части к моделированию, программной реализации и оценке перспектив прослеживается чётко.

Соответствие паспортам научных специальностей

Содержание и основные результаты диссертационной работы соответствуют паспортам двух научных специальностей.

По специальности 2.3.8 – «Информатика и информационные процессы» результаты работы охватывают следующие направления исследований:

– пункт 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) – реализован в многоуровневой модели информационного процесса удалённого управления;

– пункт 3 (разработка методов и алгоритмов кодирования, сжатия и размещения информации для повышения эффективности и надёжности функционирования инфокоммуникационных систем при её хранении и передаче) – реализован в методе векторизации потоковых траекторий манипулятора на основе модифицированного алгоритма Дугласа–Пекера и нормализованных направляющих косинусов;

– пункт 9 (разработка архитектур программно-аппаратных комплексов поддержки цифровых технологий сбора, хранения и передачи информации в инфокоммуникационных системах и оценка их эффективности) – реализован в архитектуре программной системы непрерывно-дискретной биометрической аутентификации с количественной оценкой её эффективности.

По специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» результаты работы охватывают следующие направления исследований:

– пункт 2 (методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида) – реализован в программно-определяемом методе аутентификации на штатных средствах ввода;

– пункт 12 (технологии идентификации и аутентификации пользователей и субъектов информационных процессов; системы разграничения доступа) – реализован в модели и архитектуре подсистемы непрерывной аутентификации, формирующей непрерывную функцию доверия для подсистемы разграничения доступа;

– пункт 15 (принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности) – реализован в программной системе, повышающей защищённость сеансов удалённого администрирования без развёртывания специализированного аппаратного обеспечения.

Научная новизна полученных результатов

Автором получены следующие результаты, обладающие научной новизной:

1) Предложен новый метод аутентификации пользователей по динамике движения компьютерной мыши, отличающийся устойчивостью к поведенческой изменчивости и наличием механизмов адаптации к разнородным условиям взаимодействия, что позволяет усовершенствовать информационные процессы аутентификации в части повышения точности цифровой интерпретации поведения субъекта в условиях удалённого доступа.

2) Разработана многоуровневая модель информационного процесса удалённого управления, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, что обеспечивает формализацию и автоматическую интерпретацию действий пользователя как информационного субъекта, находящегося вне контролируемой зоны. Модель позволяет снизить число ложноположительных событий в 1,5 раза по сравнению с аналогами.

3) Разработана архитектура системы биометрической аутентификации на основе свёрточных нейронных сетей, учитывающая особенности непрерывно-дискретного поведенческого потока при удалённой работе и включающая режим адаптивного обучения. Архитектура обеспечивает устойчивую классификацию цифрового поведения в реальном времени с высокой точностью при интегральной нагрузке на клиентский узел не более 7,1 % и повышает устойчивость модели к колебаниям пользовательского поведения до 15 %.

Достоверность и обоснованность полученных результатов

Достоверность и обоснованность полученных результатов подтверждаются: корректным применением методов системного анализа, теории информационных процессов, теории вероятностей и математической статистики, аппарата цифровой обработки сигналов и глубокого обучения;

экспериментальной проверкой на репрезентативных наборах данных с использованием метрик Accuracy, Recall, Precision, F1-score, FAR, FRR, HTER и построением ROC-кривых; серией из 100 измерений временных характеристик конвейера принятия решения; сравнительным анализом с классификаторами KNN, DT, RF, показавшим последовательное преимущество CNN-модели по совокупности значимых метрик. Полученные результаты не противоречат данным, приводимым другими авторами для смежных задач поведенческой биометрии.

Апробация работы

Основные положения и результаты диссертационной работы докладывались и обсуждались на более чем десяти международных, всероссийских и отраслевых научно-практических конференциях, в том числе на TransSiberia-2023 (Новосибирск), REASkills-2022 (ГК «Росатом»), Всероссийской НПК «Обеспечение информационной безопасности: вопросы теории и практики» (УдГУ, Ижевск, 2023), II НПК «Актуальные проблемы защиты информации: современность и перспективы» (МГТУ им. Н.Э. Баумана, 2024), 397-м заседании Томского IEEE-семинара (ТУСУР, 2024), Международной конференции ICCT-2025 (Gomel, Belarus), Евразийском творческом форуме «EURASIA 2025» (Алма-Аты) и других.

По теме диссертации опубликовано 36 печатных работ, в том числе 11 статей в изданиях, включённых в перечень ВАК (из них 3 – по специальности 2.3.8, 6 – по специальности 2.3.6, 2 – по обеим специальностям), 3 публикации в изданиях, индексируемых в Scopus, 1 публикация в издании Web of Science; получено 7 свидетельств о государственной регистрации программ для ЭВМ.

Теоретическая и практическая значимость работы

Теоретическая значимость работы состоит в расширении предметной области информационных процессов за счёт формализации класса непрерывно-

дискретных фоновых процессов верификации подлинности, характеризующихся асинхронностью, высокой энтропией исходных данных и потоковой природой; в развитии подходов к обеспечению динамической устойчивости сеансового уровня распределённых информационных систем; а также в развитии математического аппарата признакового описания поведенческих паттернов работы с устройствами ввода.

Практическая значимость работы заключается в повышении эффективности цифрового контроля административных действий за счёт внедрения программной системы, реализующей предложенные методы без применения специализированного биометрического оборудования. Результаты диссертационного исследования применены и внедрены в АНО «Агентство развития профессионального мастерства», в отраслевом чемпионате REASkills-2022 ГК «Росатом», в учебном процессе Ростовского государственного экономического университета, Санкт-Петербургского горного университета императрицы Екатерины II, Северо-Кавказского горно-металлургического института и Гомельского государственного университета имени Ф. Скорины (Республика Беларусь), что подтверждается соответствующими актами внедрения.

Рекомендации по использованию результатов диссертационной работы

Разработанные А.Г. Уйминым методы, модели и программную систему непрерывно-дискретной биометрической аутентификации по данным компьютерной мыши рекомендуется использовать:

– при построении подсистем защиты сеансов удалённого администрирования в информационных системах образовательного, корпоративного и государственного секторов, в первую очередь в контурах доверенного удалённого доступа;

– при разработке средств прокторинга и цифрового контроля легитимности пользовательской сессии в системах дистанционного обучения и проведения оценочных процедур;

– при проектировании модульных систем поведенческой биометрии, интегрируемых со средствами многофакторной аутентификации и подсистемами разграничения доступа;

– в учебном процессе высших учебных заведений при подготовке кадров по направлениям 10.00.00 «Информационная безопасность», 09.00.00 «Информатика и вычислительная техника».

Замечания по диссертационной работе

1. В работе многократно подчёркивается непрерывный характер аутентификации, при этом используется понятие непрерывно-дискретной аутентификации, которое не является устоявшимся, но в работе не поясняется; также не указан и не определен уровень дискретизации, при котором процесс перестаёт считаться непрерывным. Автору стоило бы ввести количественный критерий, разграничивающий эти режимы.

2. В разработанной системе к массиву исходных данных применяется аппроксимация (алгоритм Дугласа-Пекера), при этом не представлено исследование влияния степени аппроксимации на точность работы системы.

3. В работе не рассмотрено влияние точностных, функциональных и эргономических характеристик мыши, рабочей поверхности и прочих факторов. Данные характеристики могут влиять на точность работы системы, так как изменение характеристик периферийных устройств и условий их функционирования вносит изменения в поведенческие характеристики курсора.

4. В качестве нейросетевых моделей рассмотрены только сверточные, но предоставленная задача представляет собой анализ пространственно-временных закономерностей, для данной задачи также актуально применение моделей трансформеров (Vision Transformer) и темпоральных сверточных

нейронных сетей, а также капсульных нейронных сетей (позволяющих отслеживать расположение деталей изображения друг относительно друга). Автор ограничился рассмотрением одной классической архитектуры, возможно, стоило рассмотреть и другие в нейросетевые архитектуры.

5. Отдельные фрагменты диссертации содержат повторы и неточности (например, дублирование несколько раз формулы сигмоидной функции в описании нейросетевой модели, опечатка в формуле 59 и пр.), что не влияет на содержание, но требует технической вычитки перед печатью.

Приведённые замечания имеют дискуссионный и уточняющий характер, не затрагивают существа полученных научных результатов и не снижают общей положительной оценки работы.

Заключение

Диссертационная работа Уймина Антона Григорьевича «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши» является законченным самостоятельным научным исследованием, выполненным на высоком научном уровне. В работе получены новые научно обоснованные технические решения, имеющие существенное значение как для развития теории информационных процессов (специальность 2.3.8), так и для развития методов и систем защиты информации в распределённых информационных системах (специальность 2.3.6). Указанные в замечаниях недостатки не снижают общей положительной оценки работы, её научной и практической ценности.

Автореферат диссертации в целом соответствует содержанию работы и полностью отражает её основные положения и выводы.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, предъявляемым к диссертациям на соискание учёной степени кандидата

технических наук, а её автор – Уймин Антон Григорьевич – заслуживает присуждения учёной степени кандидата технических наук по научным специальностям 2.3.8 – «Информатика и информационные процессы» и 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Отзыв на диссертационную работу Уймина А.Г. обсуждён и одобрен на расширенном заседании кафедры компьютерной и информационной безопасности Института искусственного интеллекта РТУ МИРЭА, протокол № 01-26/27 от 25 августа 2026 г.

Директор Института искусственного интеллекта
д.т.н., доцент Ш.Г. Магомедов

Заведующий кафедрой компьютерной и
информационной безопасности
к.т.н., доцент А.Н. Чесалин

Сведения о ведущей организации

Полное наименование: федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет».

Сокращённое наименование: РТУ МИРЭА.

Адрес: 119454, г. Москва, проспект Вернадского, д. 78.

Телефон: +7 (495) 434-93-83.

Электронная почта: rector@mirea.ru

Web-сайт: https://www.mirea.ru