

ОТЗЫВ

на автореферат диссертации Уймина Антона Григорьевича «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши», представленной на соискание учёной степени кандидата технических наук по специальностям 2.3.8 – «Информатика и информационные процессы» и 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Уймина А.Г. посвящена непрерывному подтверждению подлинности пользователей в сеансах удалённого доступа. Для оператора связи, обслуживающего массовые сервисы удалённых рабочих мест, виртуальных рабочих столов и корпоративных подключений, актуальность темы очевидна: периметр современной инфраструктуры проходит не по границе сети, а по каждому клиентскому устройству, и компрометация легитимной сессии после успешной аутентификации остаётся одним из наиболее трудно обнаруживаемых видов инцидентов. Существующие каналные и сетевые механизмы защиты не верифицируют физическую подлинность оператора, и предлагаемое автором решение восполняет именно этот пробел.

Существенным достоинством работы считаю её эксплуатационную ориентированность. Для систем фоновое мониторинга, развёртываемых в масштабе тысяч рабочих мест, определяющими являются не только показатели точности, но и частота ложных срабатываний, порождающих обращения в службы поддержки и реагирования. Автор уделяет этому аспекту центральное внимание: по данным автореферата, применение многоуровневой модели информационного процесса сократило число ложноположительных событий в 1,5 раза (исходные значения и методика сравнения с аналогами в автореферате не детализированы), что напрямую транслируется в снижение эксплуатационных издержек.

Научная новизна работы заключается в следующем:

1. Метод непрерывно-дискретной биометрической аутентификации по динамике компьютерной мыши на основе свёрточных нейронных сетей, обеспечивающий точность до 98,50% в сценарии одиночных движений и $HTER = 0,0120$ на комплексных паттернах без специализированного оборудования.

2. Многоуровневая модель информационного процесса удалённого управления, включающая уровни взаимодействия, поведенческого контекста и потоковой оценки признаков и формализующая действия пользователя вне контролируемой зоны.

3. Архитектура системы с адаптивным дообучением профилей, повышающая устойчивость классификации к поведенческой изменчивости на 15% при интегральной нагрузке на клиентский узел 7,1%, что создаёт предпосылки для массового развёртывания на штатных рабочих местах.

Концептуально важным считаю переход от бинарной модели «аутентифицирован / не аутентифицирован» к непрерывной функции доверия, пересчитываемой по мере поступления поведенческих данных. Такая постановка сближает контроль подлинности с эксплуатационным мониторингом качества сервиса: появляется измеримая величина, допускающая пороговую обработку, трендовый анализ и корреляцию с иными событиями инфраструктуры. Теоретическая значимость работы определяется формализацией этого класса непрерывно-дискретных информационных процессов и обоснованием методов их потоковой обработки.

Достоверность результатов сомнений не вызывает: применён общепринятый статистический аппарат оценивания биометрических систем (ROC-анализ, FAR/FRR/EER), выполнено имитационное моделирование, эксперименты проведены на эмпирических наборах данных при различных сценариях пользовательской активности. Количественные результаты согласуются с выводами.

Автореферат составлен качественно: постановка задачи, модельный аппарат, архитектура и экспериментальные результаты изложены последовательно и позволяют судить о содержании диссертации в целом; основные результаты опубликованы в изданиях перечня ВАК и представлены научному сообществу на профильных конференциях.

Практическая значимость подтверждена апробацией в инфраструктуре всероссийских и международных соревнований профессионального мастерства, внедрением в учебный процесс университетов и государственной регистрацией программных модулей (семь свидетельств). Предложенная система применима в корпоративных сервисах удалённых рабочих мест как дополнительный, прозрачный для пользователя рубеж контроля подлинности, а непрерывная функция доверия – в перспективе, при проработке интеграционных интерфейсов, – как источник событий для систем мониторинга инцидентов.

К содержанию работы могут быть сделаны следующие замечания:

В автореферате не исследовано влияние характеристик канала связи (задержка, джиттер, потери) на временную структуру потока событий манипулятора при терминальном доступе и, как следствие, на точность классификации.

Отмеченные недостатки не носят принципиального характера и не снижают общей высокой оценки выполненного исследования.

Анализ автореферата позволяет сделать вывод о том, что диссертация является законченным научно-квалификационным исследованием на актуальную тему, обладающим научной новизной и практической значимостью. Диссертация соответствует требованиям пункта 9 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а её автор, Уймин Антон Григорьевич, заслуживает присуждения учёной степени кандидата технических наук по специальностям 2.3.8 – «Информатика и информационные процессы» и 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Согласен на включение в аттестационное дело и дальнейшую обработку моих персональных данных, необходимых для процедуры защиты диссертации.

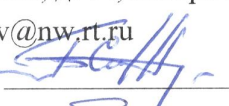
Бушеленков Сергей Николаевич

кандидат наук (2.2.15 – «Системы, сети и устройства телекоммуникаций»),

Главный эксперт Отдела стандартизации решений технической инфраструктуры
Департамента по техническому развитию ПАО «Ростелеком»

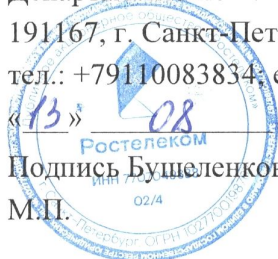
191167, г. Санкт-Петербург, Синопская наб., д. 14, литера А

тел.: +79110083834, e-mail: S.Bushelenkov@nw.rt.ru

«13» 08 2026 г. подпись 

Подпись Бушеленкова С.Н. удостоверяю

М.П.



Сильченко Т. Ю. 13.08.2026
Начальник отдела документационного сопровождения