

ОТЗЫВ

на автореферат диссертации **Уймина Антона Григорьевича** на тему **«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 оператора в течение сеанса работы с информационной системой. Актуальность темы определяется структурой современных инцидентов информационной безопасности: значительная их часть реализуется внутри легитимных, корректно аутентифицированных сессий – при компрометации учётных данных, оставленных без присмотра рабочих мест, умышленной передаче доступа третьим лицам. Традиционные механизмы разграничения доступа фиксируют полномочия субъекта, но не верифицируют его физическую подлинность на протяжении сеанса, и разработка средств непрерывного поведенческого контроля, закрывающих постаутентификационную фазу, является востребованным направлением защиты информации.

Автором предложен и доведён до программной реализации механизм непрерывно-дискретной биометрической аутентификации по динамике компьютерной мыши. Методологически важно, что защитный механизм привязан к предметной модели угроз постаутентификационной фазы (подмена контекста, отложенная компрометация, деградация атрибутов субъекта) и описан в терминах непрерывной функции доверия – измеримой величины, допускающей пороговую обработку и сопряжение с политиками управления доступом. Признаки извлекаются из штатного потока событий устройства ввода, что не требует специализированного оборудования.

Научная новизна работы заключается в следующем:

1. Разработан метод непрерывно-дискретной биометрической аутентификации, в котором пространственно-временные признаки поведенческого потока извлекаются свёрточной нейронной сетью автоматически; достигнута точность классификации до 98,50% в сценарии одиночных движений при $HTER = 0,0120$ на комплексных поведенческих паттернах.

2. Предложена многоуровневая модель информационного процесса удалённого управления, формализующая действия пользователя как информационного субъекта вне контролируемой зоны; применение модели сократило число ложноположительных срабатываний в 1,5 раза.

3. Построена архитектура системы с режимом адаптивного дообучения поведенческих профилей, повысившая устойчивость классификации к естественной изменчивости поведения на 15% при интегральной фоновой нагрузке на клиентский узел 7,1%.

Достоверность результатов обеспечена корректным применением статистического аппарата оценивания биометрических систем (ROC-анализ, показатели FAR/FRR/EER), методов имитационного моделирования и экспериментальной проверкой на эмпирических наборах данных с контрольными группами; выводы согласуются с приведёнными количественными данными.

Существенным достоинством работы является её эксплуатационная реалистичность: решение является чисто программным, а сокращение числа ложноположительных срабатываний в 1,5 раза прямо снижает нагрузку на службы реагирования – фактор, во многом определяющий применимость средств мониторинга в реальных инфраструктурах. Приоритет программной реализации закреплён семью свидетельствами о государственной регистрации программ для ЭВМ.

Практическая значимость подтверждена апробацией в инфраструктуре всероссийских и международных соревнований профессионального мастерства и внедрением в учебный процесс ряда университетов, а именно - приложены семь свидетельств о государственной регистрации программ для ЭВМ и шесть актов о внедрении. Предложенный механизм может использоваться как дополнительный рубеж контроля подлинности в составе комплексных систем защиты информации корпоративных и ведомственных информационных систем. Автореферат выполнен технически грамотно и отражает содержание исследования. Основные результаты опубликованы в рецензируемых изданиях перечня ВАК и апробированы на профильных конференциях.

При общем высоком уровне проведенной работы по тексту автореферата можно высказать следующие замечания:

1. Недостаточно полно раскрыт порядок реагирования при устойчивом снижении функции доверия (блокировка сессии, повторная аутентификация, эскалация в службу безопасности) и критерии выбора соответствующих пороговых значений для систем различного класса.
2. Из автореферата неясно как влияет на уникальные цифровые признаки из стандартных потоков информационного обмена выбор типа, модели и производителя компьютерной мыши.
3. Погрешности (опечатка) в базовых формулах: формула FPR записана как $FP/(FP+FN)$ вместо $FP/(FP+TN)$; формула угла использует atan вместо atan2 ; формула обновления весов не содержит оператора градиента.
4. Численная неточность при переносе рыночной статистики (указано «млн долларов» вместо «млрд долларов» согласно заголовку первоисточника: Total biometrics market to reach \$127B by 2030. Biometric Update. 2022. (<https://www.biometricupdate.com/>)).

Данные замечания не умаляют научной и практической ценности выполненного диссертационного исследования.

На основании анализа автореферата можно заключить, что диссертационная работа «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши» представляет собой завершённое научно-квалификационное исследование, выполненное на актуальную тему и содержащее решение задачи, имеющей значение для развития информатики и информационной безопасности. 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.

Рецензент: Кессаринский Леонид Николаевич

Учёная степень, учёное звание: к.т.н. (05.13.05 «Элементы и устройства вычислительной техники и систем управления»), без звания

Должность: ученый секретарь диссовета МИФИ.2.05, заместитель директора АИЦ ИБСЗИ, доцент кафедры №43 «Стратегии и технологии кибербезопасности»,

Организация: НИЯУ МИФИ

Почтовый адрес организации: 115409, г. Москва, Каширское ш., 31

Телефон: (495) 788-56-99, доб. 6937

Адрес электронной почты: LNKessarinskiy@mephi.ru

Подпись: _____

« 26 » 08 2026 г.

/ Кессаринский Л.Н. /

Подпись _____ заверяю.
М.П.

ЗАМЕСТИТЕЛЬ
ДИРЕКТОРА ДКПСР
НОСОВА О.В.

Согласие на обработку персональных данных, содержащихся в отзыве, для целей формирования аттестационного дела и размещения отзыва в предусмотренных нормативными актами информационных системах:

_____ / Кессаринский Л.Н. /