

ОТЗЫВ

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

Диссертация Уймина А.Г. посвящена применению нейросетевых методов анализа данных к задаче непрерывной биометрической аутентификации пользователей по динамике компьютерной мыши. Тема находится на пересечении двух активно развивающихся направлений – интеллектуального анализа поведенческих данных и защиты информации – и актуальность ее несомненна: контроль подлинности субъекта после успешного входа в систему остается слабо закрытым участком большинства эксплуатируемых архитектур безопасности, а зрелость аппарата глубокого обучения впервые делает поведенческий контроль практически реализуемым.

С позиций нейросетевого анализа данных работа выполнена на современном уровне. Автор обоснованно применяет сверточные архитектуры к пространственно-временному представлению потока событий манипулятора, отказываясь от ручного конструирования признаков; вводит режим адаптивного дообучения, компенсирующий дрейф поведенческих характеристик; корректно строит процедуру оценивания на эмпирических наборах данных с контрольными группами. Достигнутые показатели – точность до 98,50% в сценарии одиночных движений, NTER = 0,0120 на комплексных паттернах – высоки для данного класса задач, а прирост устойчивости к изменчивости поведения на 15%, связываемый автором с адаптивным обучением, свидетельствует в пользу выбранной стратегии сопровождения моделей.

Научная новизна работы заключается в следующем:

1. Метод непрерывно-дискретной биометрической аутентификации на основе сверточных нейронных сетей с автоматическим извлечением пространственно-временных признаков поведенческого потока.

2. Многоуровневая модель информационного процесса удаленного управления, применение которой сократило число ложноположительных срабатываний в 1,5 раза – показатель, определяющий эксплуатационную пригодность систем фоновой мониторинга.

3. Архитектура системы с режимом адаптивного дообучения профилей при интегральной фоновой нагрузке на клиентский узел 7,1%, допускающая массовое развертывание на штатных рабочих местах.

Экспериментальный протокол построен добротно: наборы данных охватывают различные сценарии пользовательской активности, оценки получены с контрольными группами, а сопоставление режимов работы системы (с адаптивным дообучением и без него) выполнено на сопоставимых выборках; вместе с тем детали дизайна контрольных групп в автореферате раскрыты кратко.

Достоверность результатов обеспечена корректной методикой оценивания (ROC-анализ, FAR/FRR/EER), имитационным моделированием информационного процесса и согласованностью результатов, полученных различными методами. Программная реализация закреплена семью свидетельствами о государственной регистрации программ для ЭВМ, что закрепляет приоритет автора.

Теоретическая значимость работы состоит в обосновании применимости сверточных архитектур к потоковой классификации высокоэнтропийных поведенческих сигналов и в формализации процедуры адаптивного сопровождения моделей в условиях

дрейфа данных – задачи, значимой далеко за пределами исходной прикладной постановки.

Практическая значимость подтверждена апробацией в инфраструктуре соревнований профессионального мастерства и внедрением в учебный процесс ряда университетов; предложенная система применима как дополнительный рубеж контроля подлинности в корпоративных и ведомственных информационных системах, а экспортируемая непрерывная функция доверия – как источник признаков для систем поведенческой аналитики более высокого уровня.

Автореферат составлен грамотно и полно отражает содержание работы; основные результаты опубликованы в рецензируемых изданиях перечня ВАК, включая издания, индексируемые в международных базах, и апробированы на профильных конференциях.

Наряду с общей положительной оценкой считаю необходимым высказать следующее замечание:

В автореферате не исследована устойчивость нейросетевого классификатора к состязательным воздействиям – целенаправленным возмущениям поведенческого потока, формируемым нарушителем для обхода решающего правила, включая предъявление траекторий, синтезированных генеративными моделями.

Приведенное замечание имеет характер пожеланий по дальнейшему развитию работы и не влияют на ее положительную оценку.

По содержанию автореферата диссертационная работа оценивается как завершенное научное исследование актуальной задачи, значимой для развития методов информатики и защиты информации. Диссертация соответствует требованиям пункта 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а ее автор, Уймин Антон Григорьевич, заслуживает присуждения ученой 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.

Вульфин Алексей Михайлович

доктор технических наук (2.3.6 – «Методы и системы защиты информации, информационная безопасность»),

профессор кафедры вычислительной техники и защиты информации

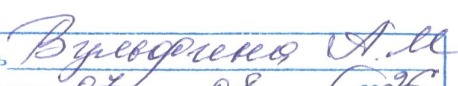
ФГБОУ ВО «Уфимский университет науки и технологий»

450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32

тел.: 8-917-400-21-89; e-mail: vulfinam@uust.ru

« 07 » 08 2026 г. подпись 



Подпись 
достоверяю « 07 » 08 2026 г.
Начальник общего отдела УНИТ 