

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 разработке системы непрерывно-дискретной биометрической аутентификации пользователей по потоку данных компьютерной мыши и включает в себя разработку метода, модели, архитектуры системы, а также выполнение ее программной реализации. Актуальность темы определяется структурой современных инцидентов информационной безопасности: значительная их часть реализуется через легитимные, корректно аутентифицированные сессии – при компрометации учётных данных, оставленных без присмотра рабочих мест, умышленной передаче доступа. Традиционные механизмы разграничения доступа принципиально не наблюдают этот класс угроз. По существу речь идёт об организации нового непрерывного информационного процесса – потоковой верификации подлинности субъекта, протекающего параллельно с целевыми информационными процессами системы, – что особенно актуально при рассмотрении современных угроз информационной безопасности.

Разработанная автором многоуровневая модель биометрической аутентификации опирается на сбор данных о поведении пользователей, использовании методов цифровой обработки сигналов для выявления поведенческих паттернов и применении алгоритма Дугласа-Пеккера.

Научная новизна работы заключается в следующем:

1. Метод непрерывно-дискретной биометрической аутентификации на основе свёрточных нейронных сетей с автоматическим извлечением пространственно-временных признаков; достигнута точность классификации до 98,50% в сценарии одиночных движений при $HTER = 0,0120$ на комплексных поведенческих паттернах.

2. Многоуровневая модель информационного процесса удалённого управления, формализующая уровни взаимодействия, поведенческого контекста и потоковой оценки признаков; применение модели снизило число ложноположительных срабатываний в 1,5 раза.

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

Работа охватывает полный цикл создания средства защиты: сформулированы требования к системе постоянной аутентификации, обоснованы модельные и архитектурные решения, выполнена программная реализация и предложены рекомендации по применению в различных эксплуатационных контекстах; результат доведён до уровня прототипа, пригодного для опытной эксплуатации.

Теоретическая значимость исследования состоит в формализации непрерывно-дискретного поведенческого потока как объекта классификации и в развитии методического аппарата привязки поведенческих средств защиты к предметной модели угроз, что задаёт воспроизводимую схему обоснования подобных систем.

Практическая значимость подтверждена апробацией в инфраструктуре всероссийских и международных соревнований профессионального мастерства,

внедрением в учебный процесс ряда университетов и семью свидетельствами о государственной регистрации программ для ЭВМ. Материалы работы представляют интерес и для образовательного процесса по направлениям информационной безопасности – как современный пример доведения поведенческого метода защиты от модели угроз до действующего прототипа.

Автореферат структурирован канонично, изложение последовательно и терминологически аккуратно; основные результаты опубликованы в рецензируемых изданиях перечня ВАК и апробированы на профильных конференциях.

В качестве замечаний по автореферату отмечу следующее:

1. В автореферате не рассмотрена стойкость системы к атакам воспроизведения: предъявлению записанной ранее телеметрии легитимного пользователя, в том числе с внесением малых искажений для обхода детектирования повторов.

2. В целом методика экспериментального исследования корректна: применены ROC-анализ и стандартные показатели ошибок биометрических систем (FAR/FRR/EER). В то же время в автореферате отсутствуют данные об используемых наборах данных при различных сценариях пользовательской активности. Количественные результаты экспериментов в автореферате отражены скупо, они характеризуют проделанную работу, но не дают полной картины.

3. Не раскрыты конкретные механизмы защиты целостности и подлинности потока телеметрии на пути от точки регистрации до подсистемы классификации: применение криптографических преобразований при обработке и хранении в автореферате заявлено, однако протоколы и способ защиты канала не специфицированы.

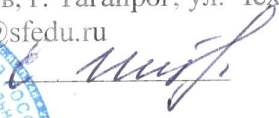
Указанные замечания носят рекомендательный характер, не снижают научной и практической значимости полученных результатов и не влияют на общую положительную оценку диссертационного исследования Уймина А.Г.

Автореферат позволяет заключить, что диссертация является завершённой научно-квалификационной работой, в которой решена актуальная задача обеспечения непрерывной подлинности пользователей информационных систем, имеющая значение для 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».

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

Ищукова Евгения Александровна

кандидат технических наук (05.13.19 – «Методы и системы защиты информации, информационная безопасность»), доцент, доцент кафедры безопасности информационных технологий имени О.Б. Макаревича ИКТИБ Южного федерального университета, 347922, Ростовская область, г. Таганрог, ул. Чехова, д. 2
тел.: 8-928-143-58-98; e-mail: uaishukova@sfedu.ru

«03» 09 2026 г. Подпись: 

Подпись Ищуковой Е.А. удостоверяю
Директор ИКТИБ

Г.Е. Веселов

