

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».

Диссертация Уймина А.Г. посвящена обеспечению непрерывной подлинности оператора в сеансах удалённого доступа. Автором предложен и доведён до программной реализации механизм непрерывно-дискретной биометрической аутентификации по потоку данных компьютерной мыши. Источником признаков служит штатная телеметрия устройства ввода.

Актуальность работы подтверждена предметной проработкой Модели угроз:

- привязкой результатов к конкретным векторам атак;
- проанализирована угроза подмены оператора за легитимным клиентским рабочим местом, дополнение защитой сессионного уровня, опирающейся на поведенческие признаки конкретного человека, закрывает этот слепой участок.

Автор оперирует классами атак на постаутентификационную фазу сессии (подмена контекста, отложенная компрометация, деградация атрибутов субъекта) и демонстрирует сокращение окна существования каждой из угроз за счёт непрерывного пересчёта функции доверия. Формируемую непрерывную функцию доверия целесообразно в дальнейшем сделать доступной внешним системам мониторинга и управления доступом.

Научная новизна работы включает в себя разработанные и описанные:

1. Метод непрерывно-дискретной аутентификации на основе свёрточных нейронных сетей, автоматически извлекающих пространственно-временные признаки поведенческого потока; точность классификации достигает 98,50% при NTER = 0,0120.
2. Многоуровневая модель информационного процесса удалённого управления, формализующая поведение пользователя вне контролируемой зоны; её применение сократило ложноположительные срабатывания в 1,5 раза, что снижает эксплуатационную нагрузку на службы реагирования.
3. Архитектура системы с режимом адаптивного обучения, устойчивая к естественной изменчивости поведения (прирост устойчивости 15%) при интегральной фоновой нагрузке на клиентский узел 7,1%.

Также интересны озвученные автором идеи более общего характера:

- Отслеживание поведенческих признаков при использовании оператором инструментария;
- Использование поведенческих признаков оператора инструментария для аутентификации;
- Отслеживание изменений в поведенческих признаках оператора посредством инструментария, используемого оператором;
- Использование изменений в поведенческих признаках оператора инструментария в качестве триггера событий.

Работа отличается полнотой инженерного цикла:

- автором сформулированы требования к системе постоянной аутентификации;
- выполнена программная реализация системы постоянной аутентификации, проведена экспериментальная оценка и предложены рекомендации по применению в различных эксплуатационных контекстах.

Существенно, что программный прототип прошёл апробацию в реальных мероприятиях, где ложные блокировки участников нежелательны, а подмена оператора должна выявляться оперативно.

Плюсом является, что предложенное решение реализуется посредством имеющегося инструментария (ПК оператора) и не требует модификации сетевой инфраструктуры и специализированного оборудования.

Достоверность результатов подтверждена:

- корректным применением статистического аппарата (ROC-анализ, FAR/FRR/EER), имитационным моделированием и экспериментами на эмпирических наборах данных;
- выводы согласуются с количественными результатами.

Основные результаты диссертации опубликованы в рецензируемых изданиях перечня ВАК, апробированы на всероссийских и международных конференциях; приоритет программных решений закреплён свидетельствами о государственной регистрации.

Практическая значимость определяется доведением решения до работоспособного прототипа:

- система апробирована в инфраструктуре соревнований профессионального мастерства;
- внедрена в учебный процесс ряда университетов;
- программные модули зарегистрированы установленным порядком (семь свидетельств).

При условии проработки интеграционных интерфейсов решение перспективно как элемент комплексных систем мониторинга безопасности.

По автореферату имеются следующие замечания:

В автореферате не рассмотрена интеграция системы с внешними средствами мониторинга событий безопасности (SIEM) и системами управления доступом: форматы передачи функции доверия, протоколы и модель событий.

Цифры оценки загрузки (CPU, RAM, дисковая подсистема) компонентов рабочего места оператора показаны как относительные значения, без указания данных, необходимых для определения абсолютных значений. Также было бы полезным сравнение по этим показателям с системами, выполняющими аутентификацию с использованием видеокамер.

Высказанные замечания не затрагивают существа полученных результатов и не ставят под сомнение общую положительную оценку диссертационной работы.

Судя по автореферату, диссертационная работа представляет собой самостоятельное завершённое исследование, содержащее новое решение актуальной

научно-технической задачи непрерывной аутентификации пользователей. 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.

Тряпицын Алексей Васильевич

к.т.н. (05.12.13 Системы, сети и устройства телекоммуникаций),

Сетевой Архитектор ООО «РДП Инновации»

121205, г. Москва, тер. Инновационного Центра Сколково, Большой б-р, д. 42, стр. 1

тел.: +7 (495) 204-94-00; e-mail: sales@ecorouter.ru

« 29 » июля 2026 г.

подпись



Подпись Тряпицына А.В. удостоверяю
Заместитель генерального директора
по развитию программных продуктов
ООО «РДП Инновации»



Куликов С.И.