

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 защите сессионного уровня при удалённом взаимодействии пользователей с информационными системами. Проблема, поставленная автором, хорошо известна практикам построения защищённых каналов связи: криптографические средства гарантируют конфиденциальность и целостность передаваемых данных, а также подлинность оконечных узлов, однако принципиально не отвечают на вопрос о том, кто фактически находится за клиентским рабочим местом после успешного установления защищённого соединения. Атаки подмены контекста и отложенной компрометации реализуются внутри легитимной, криптографически корректной сессии, поэтому развитие механизмов непрерывного подтверждения подлинности оператора образует самостоятельный и востребованный рубеж защиты, дополняющий каналные средства.

Автором обоснована гипотеза о достаточности потока данных компьютерной мыши для поддержания непрерывной функции доверия и предложен комплекс моделей, методов и программных средств, реализующих непрерывно-дискретную биометрическую аутентификацию без специализированного оборудования, исключительно на основе штатной телеметрии устройств ввода.

Научная новизна работы заключается в следующем:

1. Метод непрерывно-дискретной аутентификации на основе автоматического извлечения пространственно-временных признаков динамики мыши свёрточными нейронными сетями; достигнута точность до 98,50% в сценарии одиночных движений при NTER = 0,0120 на комплексных поведенческих паттернах.

2. Многоуровневая модель информационного процесса удалённого доступа, включающая уровни взаимодействия, поведенческого контекста и потоковой оценки признаков и обеспечившая снижение числа ложноположительных срабатываний в 1,5 раза, что критично для эксплуатации фонового мониторинга в производственных инфраструктурах.

3. Архитектура системы с адаптивным обучением, устойчивая к естественной изменчивости поведения (повышение устойчивости на 15%) и характеризующаяся интегральной нагрузкой на клиентский узел 7,1%, что допускает совместное функционирование с криптографическими средствами защиты канала без деградации производительности рабочего места.

Модель угроз, положенная в основу исследования, сформулирована предметно: автор оперирует известными классами атак на постаутентификационную фазу (подмена контекста, отложенная компрометация, деградация атрибутов субъекта по классификации CAPEC) и показывает, каким образом непрерывная функция доверия, вычисляемая по поведенческим признакам, сокращает окно существования каждой из перечисленных угроз. Такая привязка результатов к конкретным векторам атак выгодно отличает работу от исследований, ограничивающихся абстрактной постановкой.

Автореферат адекватно отражает содержание диссертации, изложение последовательно и терминологически строго; основные результаты опубликованы в рецензируемых изданиях перечня ВАК и апробированы на всероссийских и международных конференциях.

Достоверность полученных результатов обеспечивается корректным применением статистического аппарата оценивания биометрических систем (ROC-анализ, показатели FAR/FRR/EER), методов имитационного моделирования и экспериментами на эмпирических наборах данных, охватывающими различные сценарии пользовательской активности.

Практическая значимость подтверждена внедрениями в инфраструктуры соревнований профессионального мастерства и учебный процесс ряда университетов, а также государственной регистрацией программных модулей. Предложенная система может рассматриваться как естественное дополнение решений по организации защищённого удалённого доступа, замыкающее контур доверия от канала связи до конкретного оператора.

К содержанию работы могут быть сделаны следующие замечания:

Для вариантов развёртывания с централизованной обработкой поведенческих признаков в автореферате не приведена оценка объёма служебного трафика телеметрии, существенная для низкоскоростных и нестабильных каналов удалённого доступа.

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.

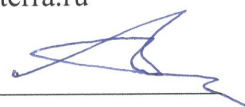
Васенков Алексей Андреевич

кандидат технических наук КТ№119237, 05.12.14 Радиолокация и радионавигация

Начальник отдела разработки NGFW, ООО «С-Терра СиЭсПи»

124460, г. Москва, г. Зеленоград, ул. Конструктора Лукина, д. 14, стр. 12

Тел: +79107900450; e-mail: a.vasenkov@s-terra.ru

«17» ОФ 2026 г. подпись 

Подпись Васенкова А.А. удостоверяю

