ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, академика Академии криптографии Российской Федерации, главного научного сотрудника Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук»
Будзко Владимира Игоревича

на диссертацию Уймина Антона Григорьевича на тему «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши», представленную на соискание учёной степени кандидата технических наук по научным специальностям 2.3.8 – «Информатика и информационные процессы» и 2.3.6 – «Методы и системы защиты информации, информационная безопасность» в диссертационный совет 24.1.107.03 при Федеральном государственном бюджетном учреждении науки Институте проблем управления им. В.А. Трапезникова Российской академии наук.

Актуальность темы диссертационного исследования

Диссертационное исследование А.Г. Уймина посвящено разработке методов повышения эффективности аутентификации пользователей с применением нейросетевых технологий и построению программного обеспечения процессов непрерывно-дискретной биометрической аутентификации по потоку данных компьютерной мыши. Актуальность темы определяется необходимостью усиления динамического контроля доверия на уровне пользовательского сеанса в распределённой среде в связи с постоянным изменением характера взаимодействия удалённых пользователей с информационными системами. Классическая шлюзовая модель контроля подлинности, восходящая к работам К. Шеннона и Р. Альсведе, обеспечивает идентификацию при установлении соединения, но не решает задачу непрерывного отслеживания доверия к установленному соединению.

В условиях массового перехода к удалённому доступу при гетерогенном парке автоматизированных рабочих мест и стохастическом множестве акторов за-

дача формализации, моделирования и алгоритмизации непрерывных информационных потоков контроля подлинности, протекающих параллельно с целевыми потоками данных, приобретает самостоятельное значение. Эта задача выходит за рамки классических постановок теории информационных процессов (сжатие, помехоустойчивое кодирование, маршрутизация) и требует разработки новых компьютерных методов и моделей описания, оценки и оптимизации информационных процессов на основе обмена информацией пользователей и возможностей штатного программно-аппаратного обеспечения. Работа полностью соответствует научной специальности 2.3.8.

Дополнительным фактором, повышающим актуальность работы, является программно-определяемый характер предложенного решения: перенос основной нагрузки биометрической аутентификации в программный контур на базе штатных устройств ввода снимает барьер аппаратной модернизации клиентских узлов и обеспечивает масштабируемость решения на инфокоммуникационные системы образовательного, корпоративного и телекоммуникационного назначения. Это соответствует магистральным направлениям развития архитектур программно-аппаратных комплексов поддержки цифровых технологий сбора, хранения и передачи информации.

Обоснованность и достоверность научных положений и выводов

Обоснованность научных положений, выносимых на защиту, подтверждается корректным использованием методов системного анализа, теории информационных процессов, теории вероятностей и математической статистики, а также аппарата цифровой обработки сигналов и глубокого обучения. Автором строго формализованы входные данные (координатно-временные последовательности событий манипулятора «мышь»), процедуры их предварительной обработки (агрегация по временным меткам, ресэмплирование, разложение на классы событий MM/PC/DD), а также этапы экстракции признаков (скорости, ускорения, рывки,

угловые перемещения, кривизна, статистические агрегаты по выборкам ON KEY/OFF KEY).

Важный методический результат диссертации – решение задачи компактного представления траекторий манипулятора «мышь». Модифицированный алгоритм Дугласа–Пекера визуального упрощения кривой используется для формирования признакового пространства. Расстояния от точек до сегментов, нормированные направляющие косинусы и полученные на их основе признаки образуют элементы для обучения нейросетевой модели. Тем самым автор связывает редукцию телеметрического потока с задачами кодирования и сжатия данных, сохраняя при этом информативность признакового описания.

Выводы автора опираются на несколько независимых процедур проверки:

1. Проведены эксперименты на репрезентативных выборках с применением ROC-анализа и показателей FAR, FRR, HTER, Accuracy и F1-score.

2. Отдельно получены временные характеристики конвейера принятия решения: серия из 100 замеров позволяет оценить не только качество классификации, но и эксплуатационную пригодность решения.

3. Результаты прошли внешнюю апробацию и внедрены в шести организациях. Полученные значения показателей Accuracy до 98,50 %, F1-score 97,87 % и HTER 0,0120 при сопоставлении с KNN, DT и RF внутренне согласованны и подтверждает корректность выбранной экспериментальной схемы.

Научная новизна результатов

Научная новизна диссертации состоит в разработке метода непрерывной поведенческой аутентификации, применение которого повышает степень защищенности информационной системы. Специальности 2.3.8 прежде всего соответствуют следующие результаты:

1. Разработана модель удалённого управления как многоуровневого информационного процесса. В ней пользовательское взаимодействие, контекст поведения и потоковая оценка цифровых признаков представлены как связанные, но

функционально различимые уровни. Такой подход позволяет трактовать действия удалённого субъекта не набором разрозненных событий, а как основание для динамически пересчитываемой функции доверия. По содержанию данный результат относится к п. 1 паспорта специальности 2.3.8.

2. Предложен способ потокового описания динамики манипулятора «мышь», в котором исходная траектория переводится в компактное признаковое представление. После векторизации модифицированным алгоритмом Дугласа–Пекера сегменты описываются нормализованными направляющими косинусами, что уменьшает объём входных данных без утраты различающих свойств. По своей технической сущности этот результат соотносится с п. 3 паспорта 2.3.8, поскольку направлен на более экономное представление и обработку информации в инфокоммуникационной системе.

3. Представлена архитектура разработанного программно-аппаратного комплекса поддержки непрерывно-дискретной аутентификации. В ней разграничены серверная часть (обучение, эталонное профилирование, управление политиками) и клиентская часть (сбор телеметрии, локальный инференс), а также обоснованы требования к вычислительным ресурсам и дана оценка эффективности функционирования. Результат соответствует п. 9 паспорта 2.3.8, посвящённому архитектурам комплексов поддержки цифровых технологий сбора, хранения и передачи информации.

Теоретическая и практическая значимость

Теоретическая значимость работы состоит в расширении предметной области информационных процессов за счёт формализации класса непрерывно-дискретных фоновых процессов верификации подлинности, характеризующихся асинхронностью, высокой энтропией исходных данных и потоковой природой. Введённая многоуровневая модель задаёт основу для постановки задач мониторинга цифрового поведения в распределённых средах, а полученные оценки времен-

ной сложности и ресурсной нагрузки могут использоваться в качестве ориентиров при проектировании систем того же класса.

Практический результат работы состоит в разработке программных продуктов (по теме диссертации зарегистрированы семь программ для ЭВМ – № 2021619990, 2021615378, 2021614803, 2021614735, 2021614613, 2021661218, 2023683139) и их экспериментальной проверке, успешное применение которых подтверждено актами внедрения в АНО «Агентство развития профессионального мастерства», в мероприятиях отраслевого чемпионата ГК «Росатом» (REASkills-2022), а также в учебном процессе Ростовского государственного экономического университета, Санкт-Петербургского горного университета, Северо-Кавказского горно-металлургического института и Гомельского государственного университета имени Ф. Скорины. Накладные расхода при их применении не велики: интегральный показатель нагрузки на клиентский узел составляет 7,1 %, а среднее время принятия решения равно 1000 ± 10,73 мс.

Краткое содержание работы

Диссертация в объёме 219 страниц включает: введение, четыре содержательные главы, заключение и библиографический список из 189 источников. Материал содержит 22 таблицы и 20 рисунков.

Во введении определяется общий формат исследования: обоснование актуальности, формулировка цели и задач, определение объекта и предмета исследования, а также положений, выносимых на защиту, определение научной новизны, теоретической и практической значимости работы.

В первой главе выполняются теоретико-аналитические обоснования исследования. Рассмотрена аутентификация в распределённых системах, показано, почему разовый шлюзовый контроль недостаточен при работе с неопределённым множеством удалённых субъектов, приведена классификация атак сессионного уровня по CAPEC (593, 29, 60, 61, 121, 226), а также обозначены нормативно-

правовые ограничения, влияющие на выбор модели непрерывного контроля подлинности.

Во второй главе выполняется формальное описание информационного процесса удалённого доступа. Задаётся схема потоковой обработки координатно-временных рядов, вводятся кинематические, динамические и статистические признаки, объясняется выбор алгоритма Дугласа–Пекера для сокращения траекторий, приводятся расчётные зависимости и рассматриваются функции активации нейросетевого классификатора.

Третья глава посвящена системной реализации предложенного подхода. Сформулированы требования к программному комплексу, описаны архитектурные решения и сравниваются несколько классификаторов: KNN, DT, RF и CNN. По совокупности показателей Accuracy до 98,50 %, F1-score 97,87 % и HTER 0,0120 преимущество демонстрирует CNN-модель; отдельно рассмотрены интегральная оценка ресурсоёмкости и время принятия решения.

В четвертой главе обсуждаются расширение признакового пространства, включение иных биометрических технологий в гибридные схемы, вопросы масштабирования, стандартизации и защиты конфиденциальной информации.

В заключении сформулированы основные результаты и выводы, определены перспективные направления дальнейших исследований.

Соответствие диссертации паспорту научной специальности 2.3.8

Содержание диссертации соответствует паспорту научной специальности 2.3.8 «Информатика и информационные процессы» (технические науки) и ее результаты соотносятся со следующими направлениями исследований паспорта:

– пункт 1 (разработка компьютерных методов и моделей описания, оценки и оптимизации информационных процессов и ресурсов) – реализован в многоуровневой модели информационного процесса удалённого управления;

– пункт 3 (разработка методов и алгоритмов кодирования, сжатия и размещения информации для повышения эффективности и надёжности функционирова-

ния инфокоммуникационных систем) – реализован в методе векторизации потоковых траекторий манипулятора на основе алгоритма Дугласа–Пекера и нормализованных направляющих косинусов;

– пункт 9 (разработка архитектур программно-аппаратных комплексов поддержки цифровых технологий сбора, хранения и передачи информации в инфокоммуникационных системах и оценка их эффективности) – реализован в архитектуре программной системы непрерывно-дискретной биометрической аутентификации с разграничением серверной и клиентской сторон и количественной оценкой её эффективности.

Оценка автореферата и публикаций

Автореферат в полном объёме отражает содержание диссертации, структурирован в соответствии с требованиями к работам данного уровня, содержит обоснование актуальности, цель, задачи, элементы научной новизны, положения, выносимые на защиту, а также перечень публикаций и испытаний. По материалам диссертации опубликовано 36 печатных работ, в том числе 11 статей в изданиях из перечня ВАК (из них 3 – по специальности 2.3.8, 6 – по специальности 2.3.6, 2 – по обеим специальностям), 3 публикации в изданиях, индексируемых в Scopus, 1 публикация в издании Web of Science, получено 7 свидетельств о государственной регистрации программ для ЭВМ. Объём и уровень публикаций полностью соответствуют требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук.

Замечания по диссертационной работе

1. В разделе, посвящённом многоуровневой модели информационного процесса, целесообразно подробнее представить формальное описание переходов между уровнями (взаимодействия, анализа поведенческого контекста и потоковой оценки), в частности сигнатуры интерфейсов и правила синхронизации; в текущем изложении часть связей восстанавливается читателем по контексту.

2. Порог tol в модифицированном алгоритме Дугласа–Пекера, соответствующий допустимой среднеквадратичной ошибке 5 %, выбран по результатам эмпирической оценки. Этот вывод стал бы убедительнее при добавлении серии сравнений для нескольких значений tol, что позволило бы явно показать компромисс между степенью сжатия траектории и качеством классификации.

3. В интегральном показателе нагрузки на клиентский узел используются экспертно заданные веса wCPU = 0,5; wMemory = 0,3; wDisk = 0,2. Пояснение по чувствительности итоговой оценки к изменению этих весов при разных профилях загрузки АРМ или описание процедуры их калибровки увеличили бы достоверность предлагаемых решений.

4. Архитектура программно-аппаратного комплекса описана достаточно полно, однако сценарии отказов серверной части раскрыты кратко. Не понятно поведение системы при временной недоступности узла обучения, а также порядок восстановления и синхронизации эталонных профилей после такого отказа.

5. Автор справедливо указывает на ограничение, связанное с переносом модели между пользовательскими средами с различным разрешением экрана и иными параметрами конфигурации. В диссертации нет качественной оценки влияния изменения клиентской конфигурации на стабильности метрик.

6. Есть редакционные замечания, прежде всего к первой главе, например, повторы фразового блока «Существенное значение имеют работы…». Они не влияют на полученный научный результат.

Указанные замечания не влияют на общую высокую оценку диссертационной работы.

Заключение

Диссертационная работа Уймина Антона Григорьевича «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши» представляет собой самостоятельную завершённую научно-квалификационную работу. В ней получены научно обоснованные технические

решения, значимые для развития процессов аутентификации пользователей в распределённых информационных системах. Работа выполнена на высоком научном и техническом уровне, отличается внутренней логической связностью, обоснованностью выводов и практической значимостью.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 «Положения о присуждении учёных степеней» (постановление Правительства Российской Федерации от 24 сентября 2013 г. № 842), предъявляемым к кандидатским диссертациям, а 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».

Официальный оппонент:

главный научный сотрудник Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», доктор технических наук, с.н.с, академик Академии криптографии Российской Федерации

_____ / В.И. Будзко /

«09» июля 2026 г.

Адрес места работы: 119333, г. Москва, ул. Вавилова, д. 44, корп. 2, ФИЦ «Информатика и управление» РАН. Тел.: +7 (499) 135-42-22. E-mail: vbudzko@frccsc.ru.

«Подпись В.И. Будзко заверяю»

Начальник отдела кадров _____ /Л.А. Петрова/

«09» 07 2026 г.