ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора, профессора кафедры «Комплексного обеспечения информационной безопасности» Института водного транспорта Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Лауты Олега Сергеевича

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 диссертационной работы

Тема диссертационной работы А.Г. Уймина, посвящённой созданию системы непрерывно-дискретной биометрической аутентификации по потоку данных компьютерной мыши, чрезвычайно актуальна для теории и практики защиты информации. Классические механизмы контроля доступа, опирающиеся на однократную процедуру аутентификации в момент установления сеанса, объективно исчерпали свой ресурс в условиях распределённых сред, удалённого доступа и отсутствия жёсткого физического контроля над клиентской инфраструктурой.

Действующая шлюзовая парадигма создаёт устойчивое временное окно уязвимости на постаутентификационной фазе, в рамках которой злоумышленник, овладевший сессионным маркером или получивший физический доступ к оставленному без присмотра автоматизированному рабочему месту, реализует широкий спектр атак сессионного уровня: подмену контекста (CAPEC-593), захват сеанса (CAPEC-60, 61), отложенную компрометацию (CAPEC-29, 226), деградацию атрибутов субъекта (CAPEC-121). Указанные векторы атак непосредственно угрожают конфиденциальности, целостности и доступности защищаемой информации в информационных системах, используемых в государственном, образовательном и корпоративном секторах.

В этих условиях направление исследований, реализующее переход от дискретной верификации к непрерывному поведенческому мониторингу подлинности субъекта доступа, приобретает статус приоритетного. Дополнительную актуальность работе придаёт учёт российского нормативно-правового контекста (ФЗ-152, ФЗ-149, ФЗ-572; ГОСТ Р 58624.2-2019, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 58833-2020) и международных стандартов

ISO/IEC 19794, что обеспечивает прикладную применимость предложенных решений в контурах защиты информации.

Степень обоснованности научных положений, выводов и рекомендаций

Научные положения диссертации получены с использованием непротиворечивого методологического аппарата, включающего теорию информационной безопасности, теорию вероятностей и математическую статистику, методы цифровой обработки сигналов, ROC-анализ, взвешенные интегральные показатели нагрузки, а также аппарат глубокого обучения на основе свёрточных нейронных сетей. Автором корректно построена модель угроз и модель нарушителя, определены критерии функциональной пригодности, надёжности и защищённости системы в соответствии с ГОСТ Р ИСО/МЭК 25010-2015.

Достоверность результатов подтверждается: экспериментальной проверкой предложенных методов на репрезентативной выборке данных с использованием метрик Accuracy, Recall, Precision, F1-score, FAR, FRR и HTER; сравнительным анализом с альтернативными классификаторами (KNN, Decision Tree, Random Forest) в трёх сценариях пользовательской активности (перемещение, наведение с щелчком, комбинированный сценарий); серией измерений временных характеристик конвейера принятия решения ($Td = 1000 \pm 10{,}73$ мс по 100 измерениям); а также независимой апробацией на международных, всероссийских и отраслевых мероприятиях и актами внедрения в шести организациях.

Полученные значения (Accuracy до 98,50 %, F1-score 97,87 %, HTER 0,0120, интегральная нагрузка на клиентский узел 7,1 %) согласованы между собой, согласуются со сведениями, приводимыми в отечественной и зарубежной литературе для поведенческой биометрии на устройствах ввода, и не содержат внутренних противоречий.

Степень обоснованности выводов и рекомендаций, сформулированных в диссертации, следует признать достаточной и в целом высокой, поскольку они базируются на последовательно выстроенной логике исследования, адекватно выбранной методологии и комплексе взаимодополняющих теоретических и экспериментальных методов. Из содержания автореферата следует, что автор опирается на анализ отечественных и зарубежных научных публикаций, а также использует современный инструментарий исследования в области интеллектуальной обработки данных и распознавания, что придает сделанным выводам необходимую научную убедительность.

Существенным основанием для положительной оценки степени обоснованности выводов является то, что основные результаты работы не ограничиваются постановочными или декларативными положениями, а подтверждаются экспериментально. В автореферате приведены результаты сопоставления применяемых моделей и алгоритмов, включая KNN, DT, RF и CNN, а оценка эффективности выполнена с использованием общепринятых и репрезентативных метрик – Accuracy, Recall, Precision, F1-score, FAR, FRR и

HTER. Такой подход свидетельствует о корректности выбора критериального аппарата и позволяет считать сделанные выводы доказательными, поскольку они опираются не на отдельные частные наблюдения, а на систему количественно измеряемых показателей.

Особо следует отметить, что автор приводит конкретные результаты, характеризующие качество предложенного решения, в частности для CNN-модели указаны значения Accuracy 98,50, F1-score 97,87 и HTER 0,0120. Наличие таких данных позволяет сделать вывод о том, что положения диссертации подтверждены результатами вычислительных экспериментов, а выдвигаемые рекомендации имеют под собой достаточную эмпирическую основу. Тем самым достигается необходимая связь между теоретическими положениями исследования, разработанным инструментарием и итоговыми научными выводами.

Научная новизна результатов

Научная новизна исследования применительно к предметной области специальности 2.3.6 определяется следующими результатами:

1) Разработан новый метод непрерывно-дискретной биометрической аутентификации, основанный на программно-определяемом сборе поведенческих признаков штатного координатного манипулятора и глубоком обучении свёрточной нейронной сети. Метод отличается устойчивостью к естественной поведенческой изменчивости пользователя и адаптивностью к разнородным условиям взаимодействия, что соотносится с направлением «Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида» (п. 2 паспорта 2.3.6).

2) Предложена технология идентификации и аутентификации субъекта информационного процесса, реализующая непрерывный фоновый контроль подлинности через анализ пространственно-временных паттернов управления интерфейсом. Обеспечен переход от бинарного «шлюзового» решения к непрерывной функции доверия, интегрируемой в подсистему разграничения доступа. Результат соответствует направлению «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа» (п. 12 паспорта 2.3.6).

3) Обоснованы принципы и техническое решение по совершенствованию существующих средств защиты информации, выражающиеся в архитектуре системы поведенческой биометрической аутентификации, оптимизированной по показателям ресурсоёмкости (интегральная нагрузка на клиентский узел не более 7,1 %) и латентности принятия решения (не более 1 с), что позволяет применять её как дополнительный контур защиты в существующих информационных системах без существенной модификации инфраструктуры. Данный результат отвечает направлению «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (п. 15 паспорта 2.3.6).

Теоретическая и практическая значимость

Теоретическая значимость работы состоит в развитии подходов к обеспечению динамической устойчивости сеансового уровня распределённых информационных систем к атакам подмены контекста и захвата сессии, в формализации непрерывной функции доверия как основы взаимодействия подсистемы аутентификации и подсистемы разграничения доступа, а также в развитии математического аппарата признакового описания поведенческих паттернов работы с устройствами ввода.

Практическая значимость подтверждается программной реализацией системы, зарегистрированными результатами интеллектуальной деятельности (семь свидетельств о государственной регистрации программ для ЭВМ, в частности № 2023683139 «Remote Topology extensions», обеспечивающее отслеживание действий пользователя с целью проведения биометрической аутентификации), а также актами внедрения результатов работы при подготовке специалистов по информационной безопасности и системному администрированию в АНО «Агентство развития профессионального мастерства», ГК «Росатом» (REASkills-2022), Ростовском государственном экономическом университете, Санкт-Петербургском горном университете, Северо-Кавказском горно-металлургическом институте и Гомельском государственном университете имени Ф. Скорины. Применение предложенного решения обеспечивает повышение защищённости сеансов удалённого администрирования и цифрового контроля административных действий без обязательного развёртывания специализированного биометрического оборудования.

Краткое содержание работы

Диссертация состоит из введения, четырёх глав, заключения и списка литературы (189 источников), изложена на 219 страницах и содержит 22 таблицы и 20 рисунков.

Первая глава посвящена анализу специфики функционирования систем удалённого доступа и проблематики обеспечения их информационной безопасности. Рассмотрены группы средств аутентификации (на основе биометрических данных, обладания информацией, знаний), классифицированы векторы атак сессионного уровня в терминах MITRE CAPEC, показана принципиальная ограниченность парадигмы шлюзового контроля. Приведён развёрнутый сравнительный анализ статических и поведенческих биометрических методов с точки зрения требований к аппаратной модернизации, конфиденциальности и устойчивости к спуфингу. Дан анализ действующей нормативно-правовой базы (ФЗ-152, ФЗ-149, ФЗ-572; ГОСТ Р 58624.2-2019, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 58833-2020; ISO/IEC 19794).

Во второй главе рассмотрены возможности использования штатных средств ввода-вывода АРМ для целей аутентификации, предложена многоуровневая модель информационного процесса удалённого доступа, разработан новый метод биометрической аутентификации по индивидуальным признакам динамики манипулятора «мышь». Приведены формализация

признакового базиса (кинематические, динамические и статистические характеристики движений и щелчков), обоснование применимости модифицированного алгоритма Дугласа-Пекера, выкладки по нормализации направляющих косинусов сегментов траекторий и обзор функций активации нейросетевых классификаторов.

В третьей главе описаны требования к программной системе, приведена её архитектура и результаты экспериментальных исследований. Проведён сравнительный анализ классификаторов KNN, DT, RF и CNN в трёх сценариях (перемещение, наведение с щелчком, комбинация действий), показано преимущество CNN-модели по совокупности метрик; дана количественная оценка временных характеристик и интегральной нагрузки на клиентский узел.

В четвёртой главе рассмотрены перспективы внедрения системы, возможные модификации подсистемы анализа, направления интеграции с иными биометрическими технологиями в многоуровневые гибридные схемы, вопросы масштабируемости, стандартизации и обеспечения конфиденциальности обрабатываемых данных.

Заключение содержит основные результаты и выводы, определены направления развития исследования.

Соответствие диссертации паспортам научных специальностей 2.3.6 и 2.3.8

Содержание диссертационной работы соответствует паспортам научных специальностей 2.3.6 «Методы и системы защиты информации, информационная безопасность» и 2.3.8 «Информатика и информационные процессы» по техническим наукам.

В части научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» результаты диссертационной работы соответствуют следующим направлениям паспорта специальности:

пункту 2, предусматривающему разработку методов, аппаратно-программных средств и организационных мер защиты систем формирования и предоставления пользователям информационных ресурсов различного вида, что отражено в предложенном программно-определяемом методе непрерывно-дискретной биометрической аутентификации на основе штатных средств ввода;

пункту 12, связанному с технологиями идентификации и аутентификации пользователей и субъектов информационных процессов, а также системами разграничения доступа, что реализовано в многоуровневой модели информационного процесса удалённого доступа и соответствующей архитектуре подсистемы аутентификации;

пункту 15, охватывающему принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности, что выражено в разработке программной системы, направленной на повышение защищённости сеансов удалённого администрирования без необходимости развёртывания специализированного аппаратного обеспечения.

В части научной специальности 2.3.8 «Информатика и информационные процессы» результаты диссертационной работы соответствуют следующим направлениям паспорта специальности:

пункту 1, предусматривающему разработку компьютерных методов и моделей описания, оценки и оптимизации информационных процессов и ресурсов, а также средств анализа и выявления закономерностей на основе обмена информацией пользователями и возможностей используемого программно-аппаратного обеспечения, что отражено в разработанной модели информационного процесса удалённого доступа и методах анализа поведенческих характеристик пользователя при работе со штатными средствами ввода;

пункту 3, связанному с разработкой методов и алгоритмов кодирования, сжатия и размещения информации для повышения эффективности и надёжности функционирования инфокоммуникационных систем при её хранении и передаче, что проявляется в предложенных подходах к представлению, обработке и использованию признаковых описаний пользовательской активности в рамках информационного процесса аутентификации;

пункту 9, охватывающему разработку архитектур программно-аппаратных комплексов поддержки цифровых технологий сбора, хранения и передачи информации в инфокоммуникационных системах, в том числе с использованием облачных интернет-технологий, и оценку их эффективности, что реализовано в архитектуре программной подсистемы сбора, обработки и анализа данных биометрической аутентификации в составе инфокоммуникационной системы удалённого доступа.

Оценка автореферата и публикаций

Автореферат в полном объёме отражает основные положения, научные результаты и выводы диссертационной работы. Его структура соответствует установленным требованиям, а содержание позволяет сделать вывод о соответствии представленного исследования заявленным научным специальностям 2.3.6 «Методы и системы защиты информации, информационная безопасность» и 2.3.8 «Информатика и информационные процессы».

По материалам диссертационной работы опубликовано 36 печатных работ. Из них 11 статей размещены в рецензируемых изданиях, входящих в перечень ВАК по соответствующим научным специальностям: 3 работы – по научной специальности 2.3.8, 6 работ – по научной специальности 2.3.6, 2 работы – по научным специальностям 2.3.8 и 2.3.6. Кроме того, опубликованы 3 работы в изданиях, индексируемых в базе Scopus, 1 работа – в издании, индексируемом в базе Web of Science, получено 7 свидетельств о государственной регистрации программ для ЭВМ. Также опубликованы 6 работ в прочих изданиях из перечня ВАК и 8 работ в иных рецензируемых изданиях, индексируемых в РИНЦ.

Количество, уровень и тематическая направленность публикаций соответствуют требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук, и подтверждают апробацию основных результатов исследования по заявленным научным специальностям.

Замечания по диссертационной работе

1. Модель угроз, положенная в основу построения системы, проработана с опорой на классификацию MITRE CAPEC, однако в явном виде не рассмотрены атаки, направленные непосредственно на классификатор (adversarial-примеры, атаки уклонения и отравления обучающей выборки). Учитывая, что ядро системы – свёрточная нейронная сеть, включение соответствующего раздела в модель угроз повысило бы полноту анализа защищённости.

2. В работе отмечено применение криптографических методов преобразования для защиты биометрических шаблонов на всех этапах их обработки и хранения. Соответствующие протоколы и режимы использования описаны обобщённо. Читатель, работающий в интересах реального внедрения, был бы признателен автору за более развёрнутое описание криптографической подсистемы, включая параметры ключевого материала и режим обновления эталонных шаблонов.

3. Пороговые значения FAR < 0,5 % и FRR < 0,5 %, принятые как критерий функциональной корректности, заданы автором в разделе требований. Обоснование выбора именно этих значений (в частности, соотнесение с уровнями риска для конкретных категорий защищаемых информационных систем) в тексте раскрыто фрагментарно.

4. В экспериментальной части работы сравнение проведено с тремя классификаторами (KNN, DT, RF). За рамками остались гибридные и рекуррентные архитектуры (LSTM, Transformer), которые в открытых источниках упоминаются как перспективные для обработки поведенческих временных рядов; их упоминание хотя бы в качестве направления сопоставления сделало бы оценку эффективности CNN более полной.

5. При обсуждении применимости системы в задачах прокторинга и цифрового контроля административных действий автору стоило бы подробнее рассмотреть организационные меры (порядок получения согласия субъекта персональных данных, регламенты хранения и уничтожения биометрических признаков), связывающие техническое решение с требованиями ФЗ-152 и ФЗ-572.

6. Разделение действий пользователя на укрупнённые категории «перемещение» и «наведение с щелчком» методически оправдано, однако интеграция с признаками клавиатурного почерка и скроллинга упоминается только как перспектива развития; их предварительная качественная оценка усилила бы обоснование гибридных сценариев применения.

Приведённые замечания имеют дискуссионный или уточняющий характер, не касаются основных научных результатов и не влияют на общую положительную оценку работы.

Заключение

Диссертационная работа Уймина Антона Григорьевича «Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши» представляет собой законченное самостоятельное научное исследование, содержащее новые научно

обоснованные технические решения, имеющие существенное значение для развития методов и систем защиты информации в распределённых информационных системах. Работа выполнена на актуальную тему, отличается методологической корректностью, обоснованностью выводов и практической полезностью полученных результатов.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук, а её автор – Уймин Антон Григорьевич – заслуживает присуждения учёной степени кандидата технических наук по научным специальностям 2.3.6 – «Методы и системы защиты информации, информационная безопасность» и 2.3.8 – «Информатика и информационные процессы».

Официальный оппонент, профессор кафедры комплексного обеспечения информационной безопасности Института водного транспорта
Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова»
доктор технических наук, профессор
Лаута Олег Сергеевич

«27» 08 2026 г.

Подпись Лаута О.С. удостоверяю
Начальник общего отдела
Н.А. Чепурная
27 08 2026

Адрес места работы: 198035, г. Санкт-Петербург, ул. Двинская, д. 5/7, ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова». Тел.: +7 (812) 748-96-96. E-mail: laoles@mail.ru.