ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

к.т.н., доцента Кашевника Алексея Михайловича

на диссертацию Альотума Юсефа Мохаммеда Абд Аллх

«Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web - приложениях»,

представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

1 Актуальность темы исследования

В рамках диссертационного исследования рассматривается вопрос повышения эффективности многофакторной поведенческо-биометрической аутентификации (статической и непрерывной) и обеспечения безопасности поведенческо-биометрических систем от кибератак с помощью технологии алгоритмов динамики нажатия клавиш и мыши. Исследование фокусируется на решении проблемы усиления надежности многофакторной поведенческо-биометрической аутентификации (статической и непрерывной) и повышения защищенности поведенческо-биометрических систем от хакерских атак через применение технологии алгоритмов динамики нажатия клавиш и мыши.

Хотя поведенческая биометрия является современным методом аутентификации, в веб-приложениях она не может быть основным инструментом из-за нестабильности оцениваемых характеристик и риска ошибочной идентификации, когда система может неверно классифицировать как авторизованных, так и неавторизованных пользователей. В контексте веб-приложений метод поведенческой биометрии не может выступать в роли основного средства аутентификации из-за его изменчивой природы и опасности неправильной интерпретации поведенческих шаблонов, что чревато ошибками как в сторону допуска неавторизованных пользователей, так и отказа легитимным.

Целью исследования является повышение точности многофакторной и непрерывной поведенческо-биометрической аутентификации на основе динамики нажатия клавиш клавиатуры и мыши. Для достижения цели исследования в работе решена фундаментальная научная задача: разработана система многофакторной аутентификации на основе биометрических измерений динамики нажатий клавиш и мыши.

Объектом исследования в диссертационной работе является система статической и непрерывной многофакторной аутентификации на основе поведенческо-биометрического подчерка.

Предметом исследования является поведенческо-биометрическая аутентификация.

Таким образом, диссертационное исследование Альотума Юсефа Мохаммеда Абд Аллх, направленное на совершенствование методик и алгоритмов

многофакторной и непрерывной поведенческо-биометрической аутентификации, является актуальным востребованным в современном мире.

2 Оценка содержания диссертации

Диссертация содержит введение, четыре главы, заключение, список использованных источников, содержащий 198 наименований. Основной текст работы изложен на 176 страницах, проиллюстрирован 47 рисунками и 8 таблицами.

Во введении обоснованы актуальность и степень разработанности темы исследования, на основе которых сформулированы цель работы и решаемые задачи для ее достижения.

В первой главе проведён анализ изъянов безопасности в системах аутентификации веб-приложений, выполнен обзор Российского законодательства в области систем биометрической идентификации, а также обзор стандартов и требований к поведенческой биометрической аутентификации. Анализ показал, что использование биометрических данных о динамике нажатий клавиш и мыши в рамках поведенческой биометрии является многообещающим научным направлением и активно применяется для защиты систем от несанкционированного доступа. В первой главе сформулирована цель диссертационного исследования. Определены задачи, которые необходимо решить для достижения поставленных целей. Реализация предложенных решений значительно повысит эффективность системы аутентификации веб-приложений, построенной на основе поведенческой биометрии нажатий клавиш и мыши, что обеспечит минимальный уровень ложных отклонений и ложных принятий, гарантируя высокий уровень безопасности.

Во второй главе Разработана биометрическая система аутентификации, анализирующая динамику нажатий клавиш и мыши. Она интегрирована в двухфакторную систему защиты (2FA), комбинирующую поведенческие и мягкие биометрические показатели. Первый уровень защиты основан на знании (пароль), второй – на биометрических характеристиках пользователя. Характеристики извлекаются через временные метки, при этом предложено анализировать все нажатия клавиш, независимо от их отношения к вводу пароля. Создана биометрическая модель аутентификации, анализирующая динамику нажатий клавиш и мыши.

В третьей главе представлена методика многофакторной аутентификации, основанная на сочетании поведенческой биометрии нажатий клавиш и технологии OTP. Система специально разработана для усиления защиты пользователей: получение OTP-кода злоумышленником не даст ему возможности доступа без соответствующих биометрических характеристик. Разработанная методика многофакторной аутентификации объединяет поведенческую биометрию с системой одноразовых паролей (OTP), создавая многоуровневую защиту. Такой подход гарантирует, что даже при перехвате OTP-кода злоумышленник не сможет имитировать поведенческие характеристики законного пользователя.

В четвертой главе разработана система непрерывной аутентификации пользователей на основе динамики мыши. Предложен подход разделения веб-страниц на сектора и расчет порогового значения непосредственно во время проверки, что отличается от традиционных подходов, где это делается на этапе обучения. Такой подход, использующий расстояние Левенштейна при каждой остановке движения, позволяет многократно проверять данные на странице без привязки к времени или количеству движений мыши.

В заключении выделены основные результаты, полученные в диссертации.

Изложение материала диссертационного исследования является структурированным и логичным, применяемая в работе терминология – корректна. Поставленная в работе цель достигнута.

Автореферат диссертации соответствует ее содержанию и достаточно полно отражает полученные научные и практические результаты.

3 Степень обоснованности и достоверность научных положений, выводов и рекомендаций

Обоснованность положений, выносимых диссертантом на защиту, подтверждается применением научного подхода при разработке алгоритмов, корректным их применением при решении поставленных задач.

Достоверность положений, выносимых диссертантом на защиту, подтверждается наличием имитационного моделирования с применением современного математического аппарата, а также обсуждением результатов диссертационной работы на конференциях; публикацией основных результатов диссертации в ведущих рецензируемых журналах.

4 Новизна научных положений, выводов и рекомендаций

Научная новизна полученных автором результатов состоит в следующем:

1. Разработана инновационная система двухфакторной аутентификации для веб-приложений, демонстрирующая значительно более высокую точность идентификации пользователей по сравнению с существующими решениями. В основе модели лежит комплексный анализ поведенческих и мягких биометрических параметров, включая особенности нажатий клавиш и движений мыши. Для определения индивидуального порогового значения каждого пользователя применяется уникальный математический подход. При обработке клавиатурного ввода используется комбинация трех метрик: Манхэттенского, Евклидова и Чебышевского расстояний. На их основе формируется прямоугольный треугольник, после чего с помощью теоремы Пифагора вычисляется угол при гипотенузе, выступающий в качестве персонального порогового значения. Такой метод позволяет существенно снизить вероятность как ложного отклонения, так и ложного принятия. При анализе действий мыши применяются метрика Минковского, рассчитываемая по кривой четверти круга, и Манхэттенское

расстояние, определяемое через площадь и длину дуги четверти круга. Сбор биометрических данных осуществляется путем фиксации временных меток каждого нажатия клавиши и движения мыши, производимых пользователем. В результате повышается количество использованных биометрических систем до 3; количество извлечённых поведенческо-биометрических характеристик до 21; скорость обработки данных ~ 0.37 С; снижается уязвимость от брутфорс атак до ~ 8%. Степень точности системы по разработанной методики составляет 97.9%. Эффективность динамики нажатия клавиш повышается на 4%, динамики мыши на 2%, определения рук на 10%.

2. Создана инновационная методика многофакторной аутентификации для веб-приложений, объединяющая генерацию случайного пароля с анализом биометрического клавиатурного почерка пользователя. Ключевое преимущество данной методики заключается в её экономичности и высокой скорости работы. В отличие от существующих решений, она использует комплексный подход к измерению расстояния Жаккара, при этом финальное тестирование может проводиться с применением как Манхэттенского, так и Евклидова расстояния. Методика демонстрирует превосходство над альтернативными методами аутентификации благодаря отсутствию необходимости в дополнительном внешнем оборудовании. Это позволяет достичь оптимального баланса между эффективностью защиты и минимальными затратами на реализацию, делая её особенно привлекательной для практического применения. В результате количество факторов аутентификации повышается до 3; снижается уязвимость от брутфорс атак до ~10%; снижается уязвимость связи с фишинговыми атаками до ~ 5%; скорость обработки данных ~ 0.12%; уменьшаются затраты на внедрение системы на ~ 85%. Степень точности системы по разработанной методики составляет 93%.

3. Впервые предложена система непрерывной аутентификации пользователей на основе разделения пространства web-страниц на сектора с четырьмя особыми типами динамики мыши. Разработанная система непрерывной динамической аутентификации отличается от существующих решений тем, что осуществляет постоянный контроль подлинности пользователя на протяжении всего времени работы с приложением. Уникальность подхода заключается в комплексном анализе различных метрик: помимо традиционного клавиатурного почерка, система отслеживает динамику движений мыши. Для оценки соответствия действий пользователя эталонным параметрам применяются различные математические метрики: расстояние Левенштейна (для расчета отклонений от обучающей выборки), а также Манхэттенское, Евклидово, векторное и Минковского расстояния. Такой многопараметрический подход обеспечивает более надежную и точную идентификацию пользователя по сравнению с традиционными методами аутентификации. За счет этого удалось снизить число ложно положительных решений на 3.4%, ложно отрицательных на 1.8%, и сократить время выявления аномалий в поведении пользователя на 4%. Благодаря этому удалось повысить

точность аутентификации до 97.2%, по сравнению с предыдущими результатами. Эффективность повышается на 2%.

Научные результаты получены автором самостоятельно, что подтверждается наличием публикаций без соавторов, перечисленные результаты диссертационного исследований являются новыми и достоверными.

5 Теоретическая и практическая значимость результатов работы

Теоретическая значимость исследования заключается в построении модели учитывающий большее число факторов биометрического подчерка пользователя по нажатию клавиш клавиатуры и мыши, использование которых позволяет создать более эффективные алгоритмы аутентификации. Также имеет место сочетание в методике различных методов изменения расстояния, осуществления процедуры аутентификации на всех этапах работы пользователя с веб-приложением, учете особенностей клавиатурного подчерка в процессе генерации одноразовых паролей, что позволяет создать более надежные системы аутентификации пользователей.

Практическая значимость представленных в работе результатов заключается в возможности создания систем аутентификации пользователей веб-приложений, усиленных одноразовыми паролями, дополнительно проверяемыми по уникальному клавиатурному подчерку пользователя, что особенно актуально для систем онлайн-платежей и подтверждения покупок в интернет-магазинах. За счет использования предложенных непрерывная аутентификации на основе динамического динамики движение мыши при работе с веб-приложениями, удаётся создать более точную систему аутентификации. Предлагаемая система непрерывной аутентификации может применяться в банковских системах, интернет-магазинах и других ресурсах, доступ к которым осуществляется с помощью веб-приложений.

6 Апробация работы и публикации по диссертации

Основные результаты диссертационных исследований обсуждены и одобрены на 7 конференциях и опубликованы в 12 научных печатных работах, в том числе: 4 – в научных журналах перечня ВАК; 7 – в материалах конференций и других изданиях. Получено свидетельство о Государственной регистрации программы для ЭВМ. Среди опубликованных работ в научных журналах перечня ВАК две написаны лично диссертантом.

7 Соответствие работы паспорту научной специальности

Диссертация соответствует одному пункту паспорта специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность (технические науки)»: п. 12. «Технологии идентификации и аутентификации

пользователей и субъектов информационных процессов. Системы разграничения доступа» (1-3 научные результаты);

8 Замечания по диссертации

1. Из работы не понятно, чем именно является «Динамическая непрерывная аутентификации пользователей» в плане представления как научного результата. Есть представление что данное наименование является «методом», однако автор классифицирует данное понятие как «систему».

2. Для повышения надежности системы необходимо учитывать общие недостатки и разрабатывать механизмы их компенсации, включая адаптивные алгоритмы, многоуровневую аутентификацию и постоянное обновление моделей на основе новых данных. В работе нет разбора индивидуальных вариаций, технических ограничений, внешних факторов, биометрических особенностей изменений характеристик со временем влияющих прямо или косвенно на полученные результаты.

3. Неясно, проходит ли пользователь аутентификацию нормально, если используются протоколы аутентификации с единым входом (SSO), данный анализ был бы полезен, учитывая тему диссертационного исследования. Возникает вопрос о том, насколько эффективно функционирует разработанная система аутентификации при использовании протоколов единого входа (SSO). Особенно актуальным представляется анализ взаимодействия предложенной методики с существующими SSO-решениями, учитывая специфику диссертационного исследования. Важно было бы определить, сохраняется ли заявленная точность идентификации и скорость работы системы при интеграции с протоколами единого входа, а также оценить возможные риски и ограничения такого взаимодействия.

4. В предыдущих исследованиях, связанных с областью поведенческой биометрической аутентификации, использовались системы машинного обучения и нейронные сети, однако, по мнению автора, они не отвечают требованиям, предъявляемым к аутентификации. Недостаточно раскрыта проблематика существующих систем.

5. При анализе эффективности предложенных методов и моделей автор говорит о характеристиках известных систем (степень защиты, быстрое обнаружение подозрительного поведения и вероятность перехвата сеанса), однако не понятно, что значит интегральная характеристика известной методики? Среднее, наилучшее, наихудшее? Была бы ценно отразить конкретные методики и сравнить с ними. Также не понятно, почему измерение быстрого обнаружения осуществляется в процентах?

6. Имеют место большое количество синтаксических, пунктуационных и стилистических ошибок в тексте, например: «расстояние, полученное от клавиатуры», «модели учитывающий», не согласованы выводы по второй главе, и др. Третье положение, выносимое на защиту, также содержит ошибки: «Динамическая непрерывная аутентификации пользователей и субъектов доступа

для веб-приложения в процессе работы Степень достоверности и апробация результатов».

7. Большое количество рисунков в работе представлено на английском языке, было бы целесообразнее представить их на русском.

Вместе с тем отмеченные недостатки не носят принципиального характера и не снижают ценности представленной диссертационной работы, которая, несомненно, имеет большую практическую ценность. Важным достоинством работы является то, что научные результаты, предложенные автором, доведены до готовой реализации в виде программного обеспечения.

9 Заключение о соответствии диссертации критериям, установленным Положением о присуждении учёных степеней

Диссертационная работа Альотума Юсефа Мохаммеда Абд Аллх «Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web - приложениях» по актуальности, научной новизне, теоретической и практической значимости соответствует требованиям п. 9-14 «Положения о присуждении ученых степеней» ВАК Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, так как является научно-квалификационной работой, в которой изложены научно обоснованные технические и программные решения в области биометрических поведенческих систем, имеющие существенное значение для развития систем обеспечения информационной безопасности в мире.

Тема и содержание диссертации «Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web - приложениях» полностью соответствует выбранной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)».

Альотум Юсеф Мохаммед Абд Аллх заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки).

Официальный оппонент:
кандидат технических наук по специальности: 05.13.01 – Системный анализ, управление и обработка информации (технические системы), доцент,
Старший научный сотрудник лаборатории интегрированных систем автоматизации, Санкт-Петербургский федеральный исследовательский центр Российской академии наук
Адрес: 14-я лин. Васильевского острова, 39, Санкт-Петербург, 199178
Тел.: +79112119880, e-mail: alexey.kashevnik@iias.spb.su

Дата.
09.06.2025

[redacted]

Кашевник Алексей Михайлович

Подпись руки Кашевника А.М. заверяю
Начальник отдела кадров СПб ФИЦ РАН
Николаева Т.Б.
«9» июня 2025 г.

[redacted]