МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «РГГМУ», РГГМУ)

ул. Воронежская, д.79, Санкт-Петербург, 192007

Тел./ факс: (812) 712-80-77; тел.: (812) 633-01-82

e-mail: rshu@rshu.ru

ОКПО 02068568; ОГРН 1027804199653

ИНН /КПП 7806012117 / 781601001

11.06.2025 № 618/016

На № _____ от _____

«УТВЕРЖДАЮ»

Проректор по развитию и научной работе
кандидат юридических наук

[redacted] Д.В. Леонтьев

«11» июня 2025 года

Отзыв ведущей организации

на диссертацию Альотума Юсефа Моха.ммеда Абд Аллх «Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web - приложениях», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

1. Актуальность темы диссертационной работы

Биометрические системы аутентификации на основе клавиатурного подчерка является одним из перспективных методов, которому посвящается все больше работ. Не смотря на присущие данному методу недостатки, он может быть серьезным дополнением, не только в качестве вторичного уровня аутентификации, но и обеспечить контроль несанкционированных действий внутреннего нарушителя по перехвату устройств ввода для управления информационных систем, например во время отвлечения внимания (отсутствия на рабочем месте) штатного оператора.

Необходимо подчеркнуть, что данная процедура аутентификации осуществляется без специального оборудования, в том числе скрытой от пользова-

теля форме. Каждый человек обладает уникальным, присущем только ему клавиатурным подчерком, однако эти характеристики сильно зависят как от конкретного типа оборудования, так и от состояния пользователя, окружающей среды, что требует постоянного обучения и адаптации системы.

Применение биометрических методов аутентификации позволяет существенно повысить работы пользователей с веб-приложениями, содержащих большое количество персональной и конфиденциальной информации.

Диссертация соответствует п. 12. «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа» паспорта специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность (технические науки)».

Таким образом тема диссертации Альотума Юсефа Мохаммеда Абд Аллх, направленное на совершенствование методик и алгоритмов многофакторной и непрерывной поведенческо-биометрической аутентификации, является актуальной.

2. Новизна исследования и полученных научных результатов сформулированных в диссертации

В диссертационной работе автором предлагается разработка механизма защиты пользовательских данных в веб-приложениях в основе которого лежит принцип многофакторной аутентификации на основе биометрических и поведенческих данных. Предлагаемый комбинированный метод основан на сочетании процессов двухфакторной аутентификации, динамике нажатия клавиш и мыши, и вычислении мягких метрик для отдельных пользователей (определение распознавание количества рук, использованных при наборе на клавиатуре) в дополнение к методу генерации случайного одноразового пароля сгенерированного с учетом особенностей уникального клавиатурного подчерка.

Объект и предмет исследования. Объектом исследования является система статической и непрерывной многофакторной аутентификации. Предметом исследования является методика и алгоритмы защиты аутентификационных данных пользователей.

Цель и задачи исследования. Целью работы является обеспечение защиты от угроз информационной безопасности в системах веб-приложений и защита их от несанкционированного доступа.

Для достижения цели исследования в работе решена научная задача:

Разработка системы многофакторной аутентификации на основе биометрических измерений динамики нажатий клавиш и перемещения мыши во время сеанса.

Научная новизна результатов исследования состоит в следующем:

1. Создана модель двухфакторной аутентификации веб-приложений, построенная на поведенческих биометрических характеристиках работы пользователя с устройствами ввода, которая способна идентифицировать пользователя с большей точностью по сравнению с известными системами аутентификации. Модель основывается на объединении трех различных методов: Манхэттенского расстояния, Евклидова расстояния и расстояния Чебышева. В процессе извлекаются большее число биометрические характеристик, осуществляется идентификация пишущей руки, с использованием законов движения кинематики. В результате повышается количество использованных биометрических систем до 3; количество извлечённых поведенческо-биометрических характеристик до 21; скорость обработки данных ~ 0.37 с., повышается точность системы аутентификации по разработанной методики составляет 97.9%.
2. Создана методика многофакторной аутентификации пользователей веб-приложения на основе генерации случайного пароля на основе использования нажатия сочетания символов с характерными биометрического клавиатурного подчерка. Предложенная методика многофакторной аутентификации основана на использовании множества способов измерения расстояния, таких как Жаккара, Манхэттенское и Евклидово расстояние. В результате, количество факторов аутентификации было повышено до 3; снижается уязвимость системы от атак до ~ 5%; повышается скорость обработки данных ~ 0.12%;
3. Созданная система непрерывной аутентификации пользователей на основе разделения пространства web-страниц на сектора с различными типами динамики мыши. Каждое из движений представляют соответствующие метрики, с использованием расстояния Левенштейна, которое рассчитывает отличия от обучающей выборки. В отличии от известных, предложенная непрерывная динамическая аутентификация позволяет проверять аутентификацию на всем времени работы с приложением, учитывает не только клавиатурный подчерк пользователя, но и динамику движений мыши с использованием расстояний Левен-

штейна, Манхэттенского, Евклидова, векторного и Минковского. 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.

Достоверность полученных результатов подтверждается:

1. анализом научных работ в данной области;
2. корректностью постановки научной задачи;
3. Результатами экспериментов с привлечением большого числа испытуемых.

3. Теоретическая и практическая значимость работы.

Теоретическая значимость работы заключается в следующем:

1. построении модели учитывающий большее число факторов биометрического подчерка пользователя по нажатию клавиш клавиатуры и мыши, использование которых позволяет создать более эффективные алгоритмы аутентификации
2. в сочетании в методике различных методов изменения расстояния, осуществления процедуры аутентификации на всех этапах работы пользователя, учете особенностей клавиатурного подчерка в процессе генерации одноразовых паролей, что позволяет создать более надежные системы аутентификации пользователей.
3. в создании непрерывной аутентификации на всем этапе работ пользователя.

Практическая значимость диссертации заключается в том, что:

1. Использование предложенной модели позволят более эффективно решать задачи построения программных систем идентификации пользователей web-приложений не только на этапе запуска, но и на всем протяжении его работы без использования дополнительного оборудования.
2. Заключается в возможности создания систем аутентификации пользователей web- приложений, усиленных одноразовыми паролями, дополнительно проверяемыми по уникальному клавиатурному подчерку пользователя, что особенно актуально для систем онлайн-платежей и подтверждения покупок в интернет-магазинах.

3. Апробация работы и публикации автора по теме диссертации

Результаты диссертационной работы использованы при проведении научно-исследовательских работ в АО «НИИ «Масштаб», а также в учебном процессе по кафедре Защищенных систем связи СПбГУТ.

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 по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (уровня К2). Две статьи в журналах перечня ВАК написаны лично соискателем.

Получено свидетельство о Государственной регистрации программы для ЭВМ.

Основные положения диссертации докладывались соискателем лично на международных и всероссийских конференциях, таких как: Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024), Региональная информатика (РИ-2024), 65-ая Научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС СПбГУТ), Международная научно-практическая конференция (Астрахань, 2021) и др.

4. Общая оценка диссертационной работы

Диссертации состоит из введения, четырех глав, заключения, списка литературы. Общий объем работы 176 страниц, из них основного текста 153 страница. Работа содержит 47 рисунок и 8 таблиц. Список литературы включает 198 источников.

Во введении определены актуальность темы диссертации, цель и задачи диссертационной работы, сформулированы положения, выносимые на защиту, научная новизна результатов их теоретическая и практическая значимость, приведены сведения об опубликованных работах, выступлениях на конференциях и семинарах.

В первой главе сформулирована цель диссертационного исследования. Определены задачи, которые необходимо решить для достижения поставленных целей. Решение задач позволит эффективность системы аутентификации web-прилежаний, основанной на поведенческой биометрии нажатия клавиш

и мыши, обеспечивая очень низкий уровень ложного отклонения и ложного принятия и, следовательно, высокую степень безопасности.

Во второй главе предложена биометрическая модель аутентификации пользователя на основе динамики нажатия клавиш и мыши. Создается система двухфакторной аутентификации (2FA), основанной на поведенческих и мягких биометрических измерениях.

В третьей главе предложена методика многофакторной аутентификации на основе поведенческой биометрии нажатий клавиш с использованием метода одноразовых паролей.

В четвертой главе представлена система непрерывной аутентификации пользователей.

В заключении приведены основные результаты, полученные в диссертации.

Автореферат корректно отражает содержание диссертации.

5. Замечания по диссертационной работе:

1. В работе не приводится анализ влияния конкретного типа оборудования, используемого пользователем, а также времени необходимого для переобучения системы в случае замены оборудования.
2. При использовании нескольких методов определения расстояния остается не ясным с какими весами учитываются результаты, полученные с помощью различных методов. Отсутствуют сравнение преимущество и недостатков каждого из используемых методов межу собой.
3. Нет обоснования выбора оценок эффективности системы непрерывной аутентификации пользователей на основе разделения пространства web-страниц.
4. В работе не обосновывается достаточность числа участников экспериментов по анализу эффективности предложенных методов.
5. В работе встречаются стилистические и орфографические ошибки, ряд терминов являются плохо перевеянными с иностранного языка терминами, например «железные ворота».

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

6. Заключение

Диссертационная работа Альотума Юсефа Мохаммеда Абд Аллх «Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web - приложениях» по актуальности, научной новизне, объему и обоснованности научных результатов отвечает всем требованиям ВАК при Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата наук. Работа соответствует требованиям пп. 9-14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства РФ № 842 от 24 сентября 2013 г. (с изменениями и дополнениями), так как является научно-квалификационной работой, в которой содержатся технические и программные решения задачи классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного и вредоносного контента, имеющей важное значение для развития методов интеллектуального анализа данных, применяемых в том числе в системах обеспечения информационной безопасности.

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).

Диссертация и автореферат рассмотрены и обсуждены на научном семинаре кафедры Информационных технологий и систем безопасности Российского Государственного Гидрометеорологического Университета 6 июня 2025 г, протокол № 6.

Директор института Информационных систем и геотехнологий доктор технических наук профессор [redacted] Е.П. Истомин

профессор кафедры Информационных технологий и систем безопасности доктор технических наук [redacted] В.Г. Бурлов

профессор кафедры Информационных технологий и систем безопасности доктор технических наук [redacted] О.М. Лепешкин

10 июня 2025