

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

д.т.н., проф. Александровой Елены Борисовны

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

Тема диссертационной работы Альотума Юсефа Мохаммеда Абд Аллх, посвящённая разработке методики и алгоритмов защиты аутентификационных данных пользователей в web-приложениях на основе поведенческой биометрии, является актуальной в условиях стремительного роста угроз информационной безопасности в цифровой среде.

В настоящее время наблюдается устойчивый тренд на цифровизацию сервисов — от онлайн-банкинга и электронной коммерции до телемедицины и государственных порталов. При этом значительная часть атак на информационные системы направлена на компрометацию идентификационных данных пользователей. Традиционные методы аутентификации (например, пароли и одноразовые коды) теряют эффективность ввиду уязвимости к фишингу и социальному инжинирингу.

В этих условиях особенно востребованы адаптивные, многофакторные и непрерывные методы аутентификации, которые обеспечивают защиту как на этапе входа, так и в процессе работы пользователя с системой. Одним из наиболее перспективных направлений является поведенческая биометрия, позволяющая идентифицировать пользователя по индивидуальному стилю взаимодействия с устройством (нажатие клавиш, движения мыши и др.) без дополнительных аппаратных средств и нарушения пользовательского опыта.

Актуальность выбранной темы подтверждается как динамикой развития мирового рынка биометрических технологий, так и отсутствием комплексных решений, объединяющих статическую, непрерывную и многофакторную аутентификацию в рамках веб-приложений.

В диссертационной работе решается **научно-техническая проблема**, которая заключается в повышении надежности многофакторной поведенческо-

биометрической аутентификации (статической и непрерывной) и защищенности поведенческо-биометрических систем от хакерских атак, основанных на отслеживании динамики нажатия клавиш и мыши.

Выявлен общий недостаток, который заключается в том, что из-за различий в формате или размере обучающих данных разные алгоритмы классификации могут давать разную частоту ошибок, и, кроме того, показатели точности для разных пользователей могут сильно отличаться, а также зависеть от общего числа пользователей в базе данных. Выбор способа анализа набора текста с клавиатуры и жестов мыши может увеличить время, необходимое для принятия правильного решения о проверке, а также повысить риск кражи, компрометации или несанкционированного доступа к конфиденциальной информации. Исходя из степени разработанности, диссертационное исследование Альотума Юсефа Мохаммеда Абд Аллх, направленное на разработку системы многофакторной аутентификации на основе биометрических измерений динамики нажатий клавиш и мыши и мониторинга поведения пользователя во время сеанса, является актуальным.

2 Степень обоснованности и достоверность научных положений, выводов и рекомендаций

Обоснованность положений, выносимых диссертантом на защиту, подтверждается следующим:

Обоснованность *первого* положения подтверждается анализом биометрических данных, классификацией характеристик, этапами обучения и тестирования, а также использованием статистических методов и метрик (евклидово расстояние, расстояние Минковского, Чебышева и др.).

Обоснованность *второго* положения подтверждается математическим аппаратом (расстояние Жаккара, евклидово и манхэттенское), используемым для анализа совпадений, а также анализом процессов формирования, обучения и тестирования моделей.

Обоснованность *третьего* положения подтверждается построением пространственной модели и метрик сравнения с эталоном, а также за счет применения расстояния Левенштейна.

Достоверность результатов и обоснованность выводов, сформулированных в диссертационной работе, определяется всесторонним анализом работ по тематике, обоснованным выбором основных допущений и ограничений, принятых в качестве исходных данных при постановке научной

задачи, экспериментальным подтверждением предлагаемых теоретических решений, публикацией результатов проведенного исследования в рецензируемых научных изданиях.

3 Новизна научных положений, выводов и рекомендаций

Научная новизна полученных автором результатов состоит в следующем:

1. Разработаны новые модели двух- и трехфакторной поведенческой биометрической аутентификации, использующие комбинирование поведенческих и мягких биометрических признаков. В результате повышается количество использованных биометрических систем до трех; количество извлеченных поведенческо-биометрических характеристик до 21; скорость обработки данных составляет приблизительно 0,37 с; снижается уязвимость от брутфорс-атак до ~8%. Степень точности разработанной методики составляет 97,9%. Эффективность динамики нажатия клавиш повышается на 4%, динамики мыши на 2%, определения рук на 10%.

2. Разработана оригинальная методика формирования одноразового пароля на основе поведенческих биометрических характеристик пользователя, использующая расстояние Жаккара, а также манхэттенское и евклидово расстояния для проверки достоверности одноразового пароля. В результате, число факторов аутентификации повышается до трех; снижается уязвимость от брутфорс-атак до ~10%; снижается уязвимость к фишинговым атакам до ~5%; скорость обработки данных ~0,12%; уменьшаются затраты на внедрение системы на ~85%. Степень точности системы составляет 93%.

3. Разработана система непрерывной аутентификации пользователей во время сеанса, использующая уникальную методику динамического мониторинга активности на web-страниц и сравнивающая поведение пользователей с эталоном с использованием различных метрик. В результате удалось снизить число ложноположительных решений на 3,4%, ложноотрицательных – на 1,8%, а также 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%.

Перечисленные результаты диссертационного исследований являются новыми и достоверными.

4 Теоретическая и практическая значимость результатов работы

Теоретическая значимость работы заключается в развитии и обосновании научных подходов к построению многофакторных систем аутентификации пользователей web-приложений на основе поведенческой биометрии. Автором предложены оригинальные модели, сочетающие динамику нажатий клавиш, характеристики движений мыши и элементы мягкой биометрии, такие как определение пишущей руки. Разработаны новые методы извлечения, нормализации и анализа биометрических признаков с применением комплекса метрик (евклидово и манхэттенское расстояния, расстояния Минковского, Левенштейна и др.), что позволяет адаптировать аутентификацию под индивидуальные особенности пользователей и повысить ее точность.

Также к числу теоретических результатов следует отнести:

- формализацию модели непрерывной аутентификации на основе анализа нажатия клавиш клавиатуры и компьютерной мыши;
- интеграцию нескольких поведенческих факторов в единую систему;
- математическое описание способов построения индивидуальных порогов принятия решений, учитывающее пространственные и временные характеристики поведения.

Таким образом, работа представляет собой ценный вклад в развитие теории поведенческой биометрии и информационной безопасности.

Практическая значимость диссертации состоит в разработке методики, подходящей для внедрения в реальные программные решения без использования специализированного оборудования. Предложенные подходы могут быть эффективно использованы для повышения защищенности web-приложений, особенно в таких критически важных сферах, как интернет-банкинг, электронная коммерция, государственные цифровые сервисы и системы дистанционного обучения.

К наиболее значимым прикладным результатам можно отнести следующие:

- возможность реализации трехфакторной аутентификации без использования токенов, смарт-карт или биометрических сканеров;
- реализация непрерывного контроля подлинности пользователя в фоновом режиме без ухудшения пользовательского опыта;
- высокая точность аутентификации (до 97,9%) при низком уровне ложных срабатываний;

– снижение риска атак (фишинга, подбора паролей и др.) за счет постоянного мониторинга поведенческого шаблона пользователя.

Результаты диссертационной работы могут быть использованы при проектировании защищённых web-систем, а также в образовательном процессе высших учебных заведений, реализующих подготовку по информационной безопасности и программной инженерии.

5 Апробация работы и публикации по диссертации

Основные результаты диссертационных исследований обсуждены и одобрены на 5 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 9 написаны автором диссертации единолично.

Апробация проведена на таких конференциях, как Научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов, Региональная информатика, Актуальные проблемы инфотелекоммуникаций в науке и образовании.

Исходя из апробации результатов исследований, можно сделать вывод об их качественном обсуждении и апробации.

6 Соответствие работы паспорту научной специальности

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).

7 Оценка содержания диссертации

Диссертация содержит введение, четыре главы, заключение, список литературы, содержащий 198 наименований, и одно приложение. Основной текст работы изложен на 153 страницах, проиллюстрирован 47 рисунками и 8 таблицами.

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

В первой главе представлен анализ методов биометрической аутентификации, рассмотрены требования к системам поведенческой биометрической аутентификации, выполнен обзор промышленных систем аутентификации на основе поведенческой биометрии, выделены их недостатки, а также проанализирован математический аппарат, используемый в методах аутентификации при анализе динамики нажатия клавиш и движения мыши.

Во второй главе приведены разработанные биометрические модели, позволяющие описать динамику нажатия клавиш и движения мыши, а также идентифицировать руку пользователя по использованию клавиатуры.

Третья глава посвящена построению методики трёхфакторной аутентификации с применением одноразового пароля, формируемого с учётом поведенческих характеристик. Методика отличается низкими затратами на реализацию и высокой скоростью работы.

В четвертой главе предложена оригинальная система непрерывной аутентификации пользователей в процессе работы с веб-приложением. Разработка основана на анализе траектории движения мыши и использовании метрик расстояния (в том числе расстояния Левенштейна) для выявления отклонений от эталонного поведения.

Работа насыщена наглядным иллюстративным материалом, имеет достаточное число ссылок на отечественные и зарубежные источники, а ее основные положения прошли апробацию на авторитетных конференциях и опубликованы в рецензируемых изданиях.

В целом, содержание диссертации отвечает требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата наук, а изложенные в ней положения и выводы обладают научной новизной и практической значимостью для информационной безопасности.

Автореферат диссертации полностью отражает содержание диссертации.

8 Замечания по диссертации

1. В диссертации неоднократно используется термин «мягкая биометрия» (soft biometrics), однако его научное содержание и отличие от других видов биометрии (например, поведенческой и физиологической) не получили четкого пояснения. В частности, при описании процесса идентификации пишущей руки автор относит его к категории мягкой биометрии, тогда как в современной научной литературе под мягкой биометрией чаще понимаются такие признаки, как пол, возраст, телосложение, длина пальцев и т.п. — то есть такие признаки,

которые не обладают высокой дискриминационной способностью, но могут быть учтены как дополнительный фактор.

2. Из приведенных результатов не вполне понятно, какое влияние оказывают такие аспекты, как смена клавиатуры и мыши, травма руки пользователя, уровень стресса, на точность результатов и требуется ли в этом случае проведение переобучения.

3. Неясно, как часто необходимо выполнять корректировку пороговых значений в системе непрерывной аутентификации, чтобы учитывать изменение поведения пользователя с течением времени.

4. Неясно, предъявляются ли какие-либо требования к оригинальному паролю, на основе которого формируется одноразовый пароль в модели одноразового пароля на основе динамики нажатия клавиш.

5. В работе наблюдается достаточно вольное обращение с такими терминами, как «модель», «метод», «методика», «технология», «подход». Например, один и тот же результат представляется как «трехфакторная технология аутентификации пользователей», «методика трехфакторной аутентификации пользователей», «модель многофакторной аутентификации» (глава 3).

6. Текст диссертации содержит стилистические неточности, перегруженные или некорректно построенные предложения, что затрудняет восприятие материала. Примеры включают:

- повтор слов («Создана Создана методика...»);
- языковые сбои («динамического динамики мыши»);
- некорректные обороты («угол, прилежащий к гипотенузе»), вызывающие сомнение в правильности математического описания.

7. В работе имеются ошибки в нумерации разделов и подпунктов, что затрудняет навигацию и вызывает путаницу при чтении. Например, в главе 2 встречается подпункт с номером 1.2.3, который по логике относится к главе 1. Подобные технические нарушения свидетельствуют о недостаточной вычитке окончательной версии документа. Также в работе присутствуют фактические ошибки (SVM отнесен к системам нейронной классификации, перепутано описание факторов аутентификации – владения и свойства – в п. 1.2).

Вместе с тем отмеченные недостатки носят частный характер и, в целом, не влияют на высокое качество представленной на отзыв диссертационной работы.

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, 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», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г. (с изменениями и дополнениями), так как является научно-квалификационной работой, в которой содержится решение задачи многофакторной аутентификации на основе биометрических измерений динамики нажатий клавиш и мыши и мониторинга поведения пользователя во время сеанса, имеющей важное значение для развития методов защиты аутентификационных данных.

Диссертационная работа «Разработка методики и алгоритмов защиты аутентификационных данных пользователей в web-приложениях» соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки), а ее автор, 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:

Александрова Елена Борисовна

доктор технических наук (специальность 2.3.6. Методы и системы защиты информации, информационная безопасность), профессор,
профессор Института компьютерных наук и кибербезопасности

федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»,

195251, г. Санкт-Петербург, вн. тер. г. муниципальный округ Академическое,
ул. Политехническая, д.29 литера Б

Тел. 8(812) 552-76-32

E-mail: helen@ibks.spbstu.ru



09 июня 2025 г.