На правах рукописи

Альотум Юсеф Мохаммед Абд Аллх

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

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург 2025

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» на кафедре защищенных систем связи

Научный руководитель:	кандидат технических наук, доцент **Красов Андрей Владимирович**
Официальные оппоненты:	**Александрова Елена Борисовна** доктор технических наук, профессор Санкт-Петербургский политехнический университет Петра Великого, Высшая школа кибербезопасности, профессор
	Кашевник Алексей Михайлович кандидат технических наук, доцент Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский федеральный исследовательский центр Российской академии наук», лаборатория интегрированных систем автоматизации, старший научный сотрудник
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет», г. Санкт-Петербург

Защита состоится 25 июня 2025 г. в 14:00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», «Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 25 апреля 2025 г.

Учёный секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Сегодня мировой рынок поведенческой биометрии находится в фазе активного роста (по данным Research and Markets вырос с 2,14 млрд долларов в 2023 году до 2,57 млрд долларов в 2024 году. Ожидается, что он продолжит расти со среднегодовым темпом роста 20,64% и достигнет 7,97 млрд долларов к 2030 году).

Поведенческие биометрические системы внедряются повсеместно, например, в онлайн-банкинге, электронной коммерции, платежах и на рынках аутентификации с высоким уровнем безопасности.

Рост рынка биометрических поведенческих систем обусловлен новыми тенденциями и вызовами, с которыми столкнулось общество и государство. К таким вызовам относятся: увеличение объемов данных о действиях пользователей в сети Интернет, которые могут быть использованы в злоумышленных целях (обострились проблемы приватности, анонимности пользователей и защищенности биометрических шаблонов от компрометации); использование методов искусственного интеллекта для проведения атак с использованием затенения и мошенничества, а также фальсификации биометрических изображений человека на основе физиологических биометрических измерений, таких как отпечатки глаз, отпечатки лиц и отпечатки пальцев.

В настоящее время поведенческий биометрический анализ используется в качестве метода аутентификации, потому что технология поведенческой биометрии предлагает надежную, соответствующую риску аутентификацию личности и меры по борьбе с мошенничеством, которые не требуют усилий со стороны пользователей и не требуют специального оборудования или дополнительных мер безопасности.

Данный метод обеспечивает: Гибкость – практически безграничный набор поведенческих биометрических характеристик доступен для анализа, а выбранные функции можно легко настроить в соответствии с конкретными потребностями использования; Удобство — поведенческая биометрия анализирует характерное поведение пользователя устройства, не нарушая пользовательский опыт; Эффективность — для аутентификации личности поведенческая биометрия применяется в режиме реального времени и работает одновременно с устаревшими механизмами аутентификации, такими как ввод пароля. Для обнаружения мошенничества биометрический поведенческий анализ значительно сокращает время, необходимое для выявления и дифференциации мошенничества от законного поведения пользователя; Безопасность — поведенческая биометрия — это внутренние характеристики, которые людям чрезвычайно трудно распознать и практически невозможно воспроизвести, особенно когда одновременно исследуются несколько поведенческих характеристик.

Поскольку пользователи могут быть зарегистрированы в фоновом режиме во время нескольких обычных взаимодействий, поведенческая биометрия абсолютно беспроблемна и не замедляет, не прерывает и иным образом не мешает сеансу пользователя.

Однако для веб-приложений метод поведенческой биометрии не рассматривается в качестве основной системы аутентификации из-за изменяющейся баллистической природы этого метода и опасений по поводу неверного чтения шаблонов поведенческой биометрии пользователя, путем принятия недействительного пользователя в качестве действительного и наоборот.

Также рассматривается метод статической аутентификации - тип управления доступом, обычно используется в качестве одноразовой проверки личности во время первого процесса входа в систему. Для всего сеанса предполагается, что пользователь является законным. При создании любого веб-приложения необходимо учитывать угрозы безопасности и уязвимости, которым может подвергнуться пользователь во время входа в систему. Необходимо создать интегрированную систему аутентификации, основанную на проверке личности пользователя с самого начала процесса входа в систему до момента завершения сеанса. До этого момента не существует системы биометрической поведенческой аутентификации, основанной на аутентификации пользователя на всех этапах использования веб-приложения и с наименьшими затратами.

В связи с этим современная высоконадежная поведенческая биометрическая система должна быть статической и непрерывной, и строиться на основе алгоритма динамики нажатия клавиш клавиатуры и мыши; с использованием алгоритма и метода непрерывной аутентификацией для классификации поведения пользователя и принятия решений на их основе для снижения риска принятия ложного пользователя за действительного.

Настоящее диссертационное исследование посвящено решению **научной задачи**, которая заключается в повышении надежности многофакторной поведенческо-биометрической аутентификации (статической и непрерывной) и защищенности поведенческо-биометрических систем от хакерских атак на основе технологии исполнения алгоритмов динамика нажатия клавиш и мыши.

Степень разработанности темы. Динамическая аутентификация пользователей, основанная на использовании рукописного ввода на клавиатуре и динамики движения мыши, является достаточно перспективным направлением исследований и широко применяется для обеспечения безопасности несанкционированного доступа злоумышленников и защиты данных пользователей.

Первые исследования в области анализа динамики нажатия клавиш были проведены в 1980-х годах Национальным научным фондом и Национальным бюро стандартов и биометрии, а анализ на основе динамики мыши был впервые предложен Ахмедом и соавторами в 2007 году. В качестве анализа привычек использования мыши человеком был сделан вывод о том, что шаблоны набора текста и стиль жестов мыши имеют уникальные характеристики, которые можно идентифицировать и использовать в качестве критериев идентификации и проверки. Значимые результаты в области анализа динамики нажатия клавиш и мыши на основе аутентификации пользователя были получены в работах российских и зарубежных ученых, таких как: Р.В. Киричек, В.И. Коржик, Q. Zhou, Y. Yang, F. Hong, Y. Feng, Z. Guo, R. Maxion, N. Zheng, A. Paloski, H. Wang, S. J. Quraishi, S. S Bedi, C. Shen, Z. Cai, X. Guan, P. Kasprowski, Z. Borowska, K. Harezlak, C. Shen, Z. Cai, X. Guan, Y. Deng, Y. Zhong, J. Gaikwad, B. Kulkarni, N. Phadol, S. Sarukte, / M. Seeger, B. Bours, E.L. Gaines, E. Rybnik, S.H. Pin, S. Deian, Y. Zhong, I.H. Shimaa, H.Z. Hala, M.S. Mazen, G. Jyotsna, Bryan, J.V. Harter, Monaco, N. Benkelman, P. Bours, S. Mondal, Y. Deng. А.Р. Абзалов, И.И. Кашапов, А.Ю. Орлов, И.Р. Мамлеев, Е.А. Кочегурова, Ю.А. Мартынова, А.А. Стрельников, М.В. Тумбинская, М.А. Казачук, N. Altwaijry, O.A. Salman, S.M. Hameed, J. Kim, P. Kang, H. Kim

Объект и предмет исследования. Объектом исследования является система статической и непрерывной многофакторной аутентификации на основе поведенческо-биометрического подчерка, а предметом является поведенческо-биометрическая аутентификация.

Цель и задачи исследования. *Целью* работы является повышение точности многофакторной и непрерывной поведенческо-биометрической аутентификации на основе динамики нажатия клавиш клавиатуры и мыши.

Для достижения цели исследования в работе решена задача по разработке системы многофакторной аутентификации на основе биометрических измерений динамики нажатий клавиш и мыши и мониторинга поведения пользователя во время сеанса.

Данная задача подразделяется на следующие частные *задачи*:

– Создать модель, извлекающую все биометрические характеристики нажатий клавиш и движений мыши и разработать модели идентификации руки на основе динамики нажатия клавиш;

– Создать модель для генерации случайного одноразового пароля на основе динамики нажатий клавиш и создать трехфакторную технологию аутентификации пользователей и субъектов доступа для веб-приложения;

– Создать непрерывную систему аутентификации на основе динамики мыши при использовании веб-приложений, с помощью кинематики и расстояния Левенштейна;

Научная новизна результатов исследования состоит в следующем:

- Создана модель двухфакторной аутентификации веб-приложений, которая способна идентифицировать пользователя с высокой точностью, в отличие от известных систем аутентификации. Предлагаемая модель аутентификации построена на основе поведенческих и мягких биометрических измерений нажатий клавиш и мыши. Чтобы найти отдельное пороговое значение для каждого пользователя, расстояние, полученное от клавиатуры, было найдено путем объединения трех расстояний: Манхэттенского расстояния, Евклидова расстояния и расстояния Чебышева, чтобы найти прямоугольный треугольник и вычислить теорему Пифагора для нахождения угла, прилежащего к гипотенузе, как отдельного порогового значения для каждого пользователя, чтобы уменьшить значение частоты ложного отклонения и ложного принятия. Для нахождения порогового значения через данные, полученные от мыши, используются расстояние Минковского, которое рассчитывается через кривую четверти круга, и Манхэттенское расстояние, которое находится через площадь четверти круга и длину дуги четверти круга. Извлекаются все биометрические характеристики нажатий клавиш и движений мыши через значение временной метки каждого нажатия кнопки на клавиатуре и каждого движения мыши, совершаемого пользователем. Разработана модель для идентификации пишущей руки, чтобы добавить степень безопасности, позволяющую идентифицировать пользователя на основе динамики нажатий клавиш 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; 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%.

- Создана методика многофакторной аутентификации пользователей веб-приложения на основе генерации случайного пароля с учетом модели биометрического клавиатурного подчерка пользователя, которая способна идентифицировать пользователя с низкими затратами и высокой скоростью, В отличии от известных предложенная методика многофакторной аутентификации основана на использовании множества способов измерения расстоянию Жаккара для принятия решения будут проходить измерения тестирования через

Манхэттенское или Евклидово расстояние. При наименьших затратах и скорости реализации он превосходит другие методы аутентификации из-за отсутствия зависимости от внешних устройств. 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%.

- Созданная система непрерывной аутентификации пользователей на основе разделения пространства web-страниц на сектора с четырьмя особыми 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 Левенштейна, 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. Эффективность повышается на 2%.

Теоретическая значимость работы заключается в следующем**:**

1. 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.
2. заключается в сочетании в методике различных методов изменения расстояния, осуществления процедуры аутентификации на всех этапах работы пользователя с web-приложением, учете особенностей клавиатурного подчерка в процессе генерации одноразовых паролей, что позволяет создать более надежные системы аутентификации пользователей.
3. Заключается в создании непрерывной аутентификации на всем этапе работы web приложений используя динамику движения мыши, т.е. без привлечения дополнительного оборудования. Применяются методы определения расстояния Евклидова, Манхэттенского, векторного расстояния и расстояния Минковского. Использование всех перечисленных методов позволит разрабатывать программное обеспечение, повышающее точность аутентификации web-приложений.

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. Модель рассматривается, как безопасная, экономичная и надежная система с классификацией степени точности результатов и возможностью сокращения времени аутентификации за счет отсутствия прямого контакта с пользователем.
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. Заключается в том, что за счет использования предложенных непрерывная

аутентификации на основе динамического динамики движение мыши при работе с web 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 web-приложений.

Реализация и внедрение результатов работы. Результаты диссертационного исследования внедрены в образовательный процесс Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Методология и методы исследования. Для решения задач, представленных в диссертации, были использованы поведенческие биометрические измерения, основанные на динамике нажатия клавиш, динамике мыши и мягких биометрических измерениях для определения рукописного текста на клавиатуре, реализации Евклидова, Манхэттенского, векторного расстояния, расстояния Минковского, Чебышева для определения порогового значения и аутентификации пользователя, разрабатывающий одноразовый пароль или метод OTP для генерации случайного пароля. обеспечения дифференциальной конфиденциальности данных и знаний, идентификации и аутентификации. Модель непрерывной аутентификации, основанная на биометрических измерениях динамики движения мыши, реализации законов движения кинематика, моделировании предлагаемого метода многофакторной и непрерывной аутентификации. Аутентификация реализована на основе веб-приложения, разработанного на языках программирования PHP, JavaScript, HTML, CSS, JQuery, и с использованием базы данных PHPMyAdmin.

Основные научные положения, выносимые на защиту:

1. Биометрическая модель аутентификации пользователя на основе динамики нажатия клавиш и мыши.
2. Методика трех факторной аутентификации пользователей для веб-приложения
3. Динамическая непрерывная аутентификации пользователей и субъектов доступа для веб-приложения в процессе работы Степень достоверности и апробация результатов.

Достоверность результатов, обоснованность положений и выводов, сформулированных в диссертации, обеспечивается учетом большого количества факторов, влияющих на решение поставленной научной задачи; обоснованным выбором основных допущений и ограничений, принятых в качестве исходных данных при ее постановке; использованием современного математического аппарата; обсуждением результатов диссертационной работы на конференциях; публикацией основных результатов диссертации в ведущих рецензируемых журналах.

Апробация результатов

Основные результаты диссертации докладывались и обсуждались на конференциях: Актуальные проблемы инфотелекоммуникаций в науке и образовании (Санкт- Петербург, 2023–2024); Региональная информатика (РИ-2024) (Санкт- Петербург, 2024); Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации, ПКМ-2024 (Санкт- Петербург, 2024); Научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов, НТК ППС 2025 (Санкт-Петербург, 2025); Международной научно-практической конференции (Астрахань, 2021).

Публикации по теме диссертации. Всего по теме диссертации опубликовано 12 работ, из них 4 статьи в рецензируемых научных журналах, входящих в перечень изданий, рекомендуемых ВАК Минобрнауки России, зарегистрирована программа для ЭВМ, 7 статей в журналах и сборниках конференций, включенных в РИНЦ.

Соответствие паспорту специальности. Содержание диссертации соответствует следующим пунктам паспорта специальности 2.3.6 Методы и системы защиты информации, информационная безопасность: п.12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.

Личный вклад автора. Все научные результаты получены автором лично, что подтверждается наличием личных публикаций. Личный вклад автора заключается в анализе систем и факторов аутентификации, а также принципов построения системы многофакторной аутентификации и непрерывной аутентификации на основе поведенческой и мягкой биометрии. Результаты теоретических и экспериментальных исследований получены автором самостоятельно.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы. Общий объем работы 177 страниц, из них основного текста 153 страниц. Работа содержит 47 рисунков и 8 таблиц. Список литературы включает 198 источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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 диссертации проанализированы рынок поведенческой биометрии и современных методов анализа динамики щелчков клавиш и мыши пользователя с целью проведения процесса аутентификации, обзора современных компаний в этой области и анализа уязвимостей безопасности в системе аутентификации веб-приложений. Выявлено, что убытки в Соединённых Штатах Америки увеличиваются с каждым годом, а потери слабых систем аутентификации в 2023 году достигли 12 с половиной миллиардов долларов.

Проведен анализ изъянов безопасности в системах аутентификации веб-приложений. Проведен обзор Российского законодательства в области систем биометрической идентификации. Обзор стандартов и требований к поведенческой биометрической аутентификации.

Выявлено, что использование поведенческой биометрии в области аутентификации пользователей на основе анализа биометрических данных динамики нажатий клавиш и мыши является перспективным направлением исследований и широко применяется для обеспечения безопасности систем, а также для повышения степени защищенности систем предотвращение несанкционированного доступа хакеров. Современные методы не в полном объёме способны решить проблему изменения баллистического характера пользователей путем изменения со временем стиля письма или движения мыши. В ходе исследований в области поведенческой биометрии стало ясно, что не существует стабильной и непрерывной интегрированной системы аутентификации, основанной на аутентификации пользователя в процессе входа в систему и мониторинге пользователя во время использования системы до завершения сеанса. Целью процесса аутентификации является повышение степени безопасности и предотвращение несанкционированного доступа. В ходе исследований в области и методах аутентификации было обнаружено, что многофакторная аутентификация имеет возможность повысить степень безопасности и проверить подлинность пользователя. Текущие работы не используют многофакторную аутентификацию в поведенческих биометрических измерениях.

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. Первый - фактор знания: что-то, что мы знаем — это пароль. Второй - фактор свойства: что-то, что является частью нас — это биометрические измерения. Проводится извлечение характеристик через временную метку. Разработанный подход позволяет извлечь характеристики нажатых клавиш от всех случаев использования клавиатуры, включая не валидные к вводу пароля (рисунок 1).

Предлагается подход к повышению точности динамического нажатия клавиш путем использования и комбинирования Манхэттенского расстояния, Евклидова расстояния, расстояния Чебышева и закона Пифагора для прямоугольных треугольников. Данный подход позволил решить проблему для определения точного порогового значения и тем самым повысить качество аутентификации пользователей в среднем на 4% по сравнению с используемой в существующих работах стандартизацией признаков.

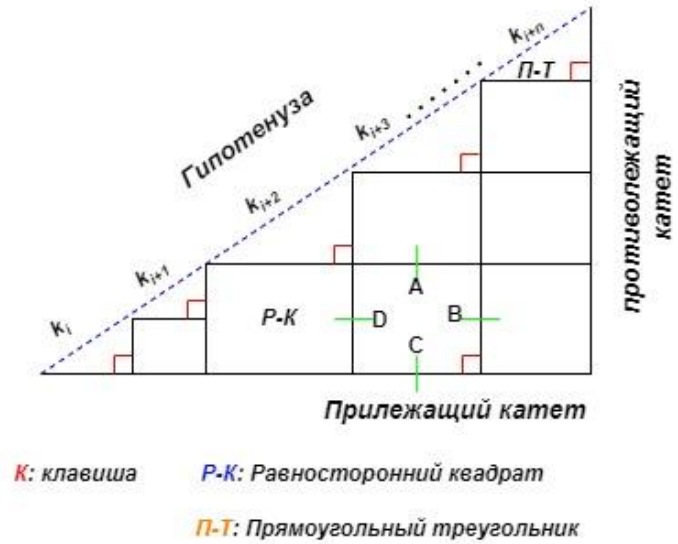

Рисунок 1 – Геометрическое формирование подхода пользователя к нажатию клавиш

Процесс построения модели пользователя на этапе обучения

$$d_{\text{euclidean}}\,(p,q) = \sqrt[2]{\sum_{i}^{n}(p_i - q_i\,/\,\alpha_i)^2}\,, \tag{2.1}$$

$$d_{manhattan}\,(p,q) = \sum_{i}^{n}|(p_i - q_i)|\,/\,\alpha_i\,, \tag{2.2}$$

$$d_{Chebyshev}(p,q) = lim_{a\to\infty}(\sum_{i}|p_i - q_i|^{a})^{\frac{1}{a}} = \max|p_i - q_i|\,, \tag{2.3}$$

где $d_{\text{euclidean}}$ – Евклидово расстояние; $d_{manhattan}$ – Манхэттенское расстояние; $d_{Chebyshev}$ – расстояние Чебышева; p_i –является первой клавшей; q_i –является второй клавшей; α – Количество нажатых и отпущенных клавиш на клавиатуре

$$a = c \,.\sin\alpha = \sqrt[2]{\sum_{i}^{n}(p_i - q_i)^2}\,.sin^{-1}, \tag{2.4}$$

$$b = c \,.\cos\beta = \sqrt[2]{\sum_{i}^{n}(p_i - q_i)^2}\,.cos^{-1}, \tag{2.5}$$

$$z = b \,.tg\ \delta = ma\,x|x_i - y_i|\,.tg^{-1}, \tag{2.6}$$

где α – катет, противолежащий углу; a – противолежащий катет; c – Гипотенуза; β– катет, прилежащий углу; b – прилежащий катет; δ – катет, прилежащий углу. z – противолежащий катет.

$$threshould = \frac{\sqrt{\left(\sum_{i=1}^{n}\alpha_{right\ triangle} + \sum_{i=1}^{n}\frac{\beta_{square}}{4}\right)}}{\mu_n}, \tag{2.7}$$

где $threshould$ – Пороговое значение; $\alpha_{right\ triangle}$ – Противоположный угол прямоугольного треугольника; β_{square} – Квадратный угол; μ –Количество нажатых и отпущенных клавиш на клавиатуре.

Процесс подтверждения модели пользователя на этапе тестирования

$$T = \frac{1}{2}ab = \frac{ma\,x|p_i - q_i|\,.\ \sum_{i=1}^{n}|p_i - q_i|}{2}, \tag{2.8}$$

$$A = l^2 = \ ma\,x|p_i - q_i|^2\,, \tag{2.9}$$

где a – основание, образованное от расстояния Чебышева; b – высота, образованная от Манхэттенского расстояния p , q – значение временной метки для каждой клавиши, набираемой на клавиатуре; l – основание, образованное от расстояния Чебышева.

$$area_{test} = \sum_{i}\left(\frac{\frac{ma\,x|p_i - q_i|\,.\ \sum_{i=1}^{n}|p_i - q_i|}{2} + \ ma\,x|p_i - q_i|^2}{\mu_n}\right), \tag{2.10}$$

где $area_{test}$ – общее пространство значений временных меток на этапе тестирования; μ_n–все клавиши, введенные на клавиатуре в процессе входа в систему и ввода пароля.

Для повышения точности определения руки, используемой для печати на клавиатуре, был предложен подход, основанный на разделении клавиатуры на восемь частей и использовании законов кинематики для определения скорости и местоположения каждой нажатой клавиши на клавиатуре, что ранее не использовался для решения этой проблемы. Повысилось качество аутентификации пользователей в среднем на 10% по сравнению с используемой в существующих работах стандартизацией признаков

Процесс построения модели пользователя на этапе обучения

Векторное расстояние для определения руки рассчитывается по формуле:

$$r_{towhand} = \sum_{z=1}^{n} key_z\,\vec{\imath} + key_z\,\vec{\jmath}\ , \tag{2.11}$$

$$r_{onehand} = \sum_{z=1}^{n} (key_z \vec{\imath} + key_z \vec{\jmath}) \,.\, |mk_{mc} - mk_{m+1\,c+1}| \ , \tag{2.12}$$

где $r_{towhand}$ – расстояние вектора положения двух рук; $r_{onehand}$ – расстояние вектора положения одной руки; $\vec{\imath}$ - вектор движения по оси X; $\vec{\jmath}$ – вектор движения по оси Y; key_z – клавиша при нажатии и отпускании; n– длина пароля.

Стандартная векторная скорость для обеих рук и одной рассчитывается по формуле:

$$|\vec{v}|_{towhand=}\sqrt{\dot{x}\vec{\imath} + \dot{y}\vec{\jmath}} = \sum_{i=1}^{n} \sqrt{\frac{r_{towhand}}{t_{i+1} - t_i}} = \frac{|\vec{v}|_{towhand}}{\Delta_t}, \tag{2.13}$$

$$|\vec{v}|_{onehand=}\sqrt{\dot{x}\vec{\imath} + \dot{y}\vec{\jmath}} = \sum_{i=1}^{n} \sqrt{\frac{r_{onehand}}{t_{i+1} - t_i}} = \frac{|\vec{v}|_{onehand}}{\Delta_t}, \tag{2.14}$$

где $|\vec{v}|_{towhand}$ – стандартная векторная скорость для обеих рук; $|\vec{v}|_{onehand}$ – стандартная векторная скорость для одной руки

Высчитывается расположение всех букв, которые были написаны обеими руками или одной рукой в качестве пароля, по формуле:

$$position_{towhand} = \frac{\sum_{i=1}^{n} r_{towhand}}{\mu}, \tag{2.15}$$

$$position_{onehand} = \frac{\sum_{i=1}^{n} r_{onehand}}{\mu}, \tag{2.16}$$

где $position_{towhand}$ – положение букв относительно пространства при письме двумя руками; $position_{onehand}$ – положение букв относительно пространства при письме одной руки μ– количество нажатых и отпущенных клавиш.

Процесс подтверждения модели пользователя на этапе тестирования

Прохождение тестирования зависит от определения скорости и пройденного расстояния при письме двумя руками и письме одной рукой. То есть скорость прохождения расстояния двумя руками больше скорости письма одной рукой. Скорость печати рассчитывается по формуле:

$$spd_{towhand} = |r_{towhand} - position_{towhand}|, \tag{2.17}$$

$$spd_{onehand} = \left|\frac{position_{onehand}}{\mu * 10}\right|, \tag{2.18}$$

Где $spd_{towhand}$ – скорость прохождения дистанции двумя руками; $spd_{onehand}$ – Скорость прохождения дистанции одной рукой;

На первом этапе аутентификации, основанном на движении мыши пользователя и его перемещении между текстовыми полями для ввода логина и пароля, что считается ограниченным движением и, таким образом, уровень ложного принятия высок. Для решения этой проблемы был предложен подход, зависящий от объединения Манхэттенского расстояния и расстояния Минковского и, таким образом, повышения точности измерения порогового значения на основе четверти кривой круга, который отличает каждого пользователя по его движению и повышает качество аутентификации пользователей в среднем на 2% по сравнению с используемой в существующих работах стандартизацией признаков.

Процесс построения модели пользователя на этапе обучения

Чтобы получить лучшее пороговое значение для динамики мыши, кривая в четверть круга рассчитывается с использованием расстояния Минковского. Экспериментально было определено значение p, чтобы найти лучшую кривую для порогового значения, которое составило 0,9.

$$D(X,Y) = s\left(\sum_{i=1}^{n}|x_i - y_i|^p\right)^{\frac{1}{p}} = \sqrt[p]{\sum_{i=1}^{n}|x_i - y_i|^p}\,, \tag{2.19}$$

$$curve_{c_{quadrant}} = D_{Minkowski}(X,Y) = \sqrt[0.9]{\sum_{i=1}^{n}|x_i - y_i|^{0.9}}\,, \tag{2.20}$$

где x, y – две точки в n-мерном пространстве; p – параметр, определяющий тип расстояния; $curve_{c\_quadrant}$ – Перемещение мыши между текстовыми полями.

Квадрант формируется следующим образом, площадь четверти круга рассчитывается с помощью Манхэттенского расстояния, чтобы вычислить значение радиуса четверти.

$$A_{quadrant} = \frac{1}{4}\pi R^2 = \frac{\pi}{4}.\frac{\sum_{i=1}^{n}|x_i - y_i|^2}{2}, \tag{2.21}$$

$$= \frac{\pi\ \sum_{i=1}^{n}|x_i - y_i|}{4}, \tag{2.22}$$

где $A_{quadrant}$ – площадь четверти круга; R – луч это одна из сторон четверти круга, и здесь он представляет собой Манхэттенское расстояние; x и y – операции с извлеченными характеристиками динамики мыши;

Пороговое значение динамики мыши в зависимости от площади четверти круга и ее окружности

$$threshould = \sqrt{\left(A_{quadrant} + R\right)} + \frac{\pi D}{4}, \tag{2.23}$$

$$= \sqrt{\left(A_{quadrant} + R\right)} + \frac{\pi 2R}{4}, \tag{2.24}$$

где $threshould$ – Пороговое значение; D– Окружность четверти круга.

В таблице 1 приведены оценки эффективности метода

Таблица 1. Анализ оценки эффективности предложенного метода

Показатель	**Известные методики**	**Разработанная методика**
Количество использованных биометрических систем	1-2	3
Количество извлечённых биометрических-поведенческих характеристик	4-8	21
Скорость обработки данных	~ 0.82 С	~ 0.37 С
Степень точности системы %	87.4% - 94.8%	97.18%
Снижение уязвимости от брутфорс атак	~ 20%	~ 2%

Результаты первого исследования были получены путем проведения реалистичного эксперимента по использованию первой части системы аутентификации. Результаты были получены проведено сравнение, которое показано в таблице 2.

Таблица 2. Анализ оценки эффективности экспериментального метода по кривой ROC

Методика	**FAR (доля неправильно принятых)**		**FRR (доля неправильно отклонённых)**		**ER (равная вероятность ошибок)**		**Точность**
Динамика нажатия клавиш	1.2%	0.79%	1.1%	0.11%	1.15%	0.45%	98.7262%
Динамика нажатия мыши	0.88%	0%	5.5%	1%	3.19%	0.51%	95.0216%
Определение руки	~0.20%	0.14%	~1.2%	0.86%	0.7%	0.523%	96.3639%

В третьей главе, В данном разделе проводилось исследование и разработка методики многофакторной аутентификации на основе поведенческой биометрии нажатий клавиш с использованием метода одноразовых паролей (OTP). Цель состоит в том, чтобы объединить фактор владения с фактором свойства, связав систему OTP с поведенческо-биометрическими характеристиками, чтобы создать систему многофакторной аутентификации, которая может добавить уровень защиты пользователей и затруднить взлом кода OTP. Это означает, что даже если хакер получит код OTP, он не сможет войти в систему, поскольку у него нет поведенческо-биометрических характеристик, которыми обладает действительный пользователь.

Этот подход не использовался в предыдущих исследованиях и показал многообещающие результаты в повышении уровня защиты и снижении фишинговых атак.

В результате проведенного исследования были достигнуты следующие результаты:

Предлагается подход к генерации случайного пароля из мастер-пароля, введенного пользователем на этапе проверки в первой части. В связи с этим, повышается точность выбора шаблона биометрических данных для проверки. Матрица случайных паролей располагается так, чтобы уменьшить процент разброса в вычислениях между ней и основной матрицей паролей.

Операции линейной алгебры используются с матрицами и объединяют их для облегчения процесса сравнения и упорядочивания случайной матрицы. Все элементы первой матрицы делятся на элементы второй матрицы по порядку, рассчитывается по формуле:

$$A = \sum_{i=1}^{n} \frac{M_{password_i}}{M_{random_i}}, \tag{3.1}$$

$$A = \begin{pmatrix} M_{pass_i}/M_{ran_i} & M_{pass_i}/M_{ran_{i+1}} & M_{pass_i}/M_{ran_{i+n}} \\ M_{pass_{i+1}}/M_{ran_i} & M_{pass_{i+1}}/M_{ran_{i+1}} & M_{pass_{i+1}}/M_{ran_{i+n}} \\ \vdots & \cdots & \cdots \\ M_{pass_n}/M_{ran_i} & M_{pass_n}/M_{ran_{i+1}} & M_{pass_n}/M_{ran_{i+n}} \end{pmatrix}, \tag{3.2}$$

где A – Представляет новую матрицу путем деления первой матрицы на вторую; M_{pass} – элементы основного массива паролей; M_{ran} – элементы случайного массива паролей;

Используя операции линейной алгебры, матрица А преобразуется в двоичную матрицу для облегчения процесса передачи и упорядочивания случайного пароля. Рассчитывается по

формуле:

$$A` = \left(A_i + \left(-1.\left(A_{i)}\right)\right)\right), \text{где } \forall A_i \ni]-\infty; 1[\cup]1; +\infty[, \tag{3.3}$$

$$A` = \begin{pmatrix} 0 & 1 & \cdots & A_n \\ 1 & 0 & \cdots & \vdots \\ 1 & 1 & \cdots & \vdots \end{pmatrix}, \tag{3.4}$$

где $A`$ – Матрица из двоичной системы счисления.

В случае логической матрицы, представляющей бинарное отношение R, транспонирование соответствует обратному отношению R^T. Рассчитывается по формуле:

$$A^T = \begin{pmatrix} 0 & 1 & \cdots & A_n \\ 1 & 0 & \cdots & \vdots \\ A_n & A_n & \cdots & \vdots \end{pmatrix}, \tag{3.5}$$

где A^T – Матрица переноса; i –Ряды; j – Колонны;

В матрице сортировки важно то, что двоичное значение один перемещается к ближайшему значению слева в каждой строке. Рассчитывается по формуле:

$$A_{mul_{ij}} = A`.A^T = A`_{i1}.A^T{}_{1j} + A`_{i2}.A^T{}_{2j} + \cdots + A`_{in}.A^T{}_{nj} = \sum_{k=1}^{n} A`_{ik}.A^T{}_{kj}, \tag{3.6}$$

$$A_{mul} = \begin{pmatrix} A_{mul_{ij}}/_n & A_{mul_{ij+1}}/_n & A_{mul_{ij+n}}/_n \\ A_{mul_{i+1,j}}/_n & A_{mul_{i+1j+1}}/_n & A_{mul_{i+1j+n}}/_n \\ \vdots & \cdots & \ldots \\ A_{mul_{i+n,j}}/_n & A_{mul_{i+n,j+1}}/_n & A_{mul_{i+n,j+n}}/_n \end{pmatrix}, \tag{3.7}$$

где A_{mul} – Матричное умножение между матрицей переноса и нулевой матрицей; k – Колонны;

Процесс перестановки строк и столбцов, если одно из значений всей строки равно нулю, и таким образом операции перестановки выполняются между следующей строкой так, чтобы результатом в итоге стала диагональная матрица с результатом единица.

$$A_{Switching} = A_{mul_{ij}} \rightarrow A_{mul_i-1,j-1}, \text{где } A_{mul_{ij}} = 0, \tag{3.8}$$

$$A_{Switching} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 & \ldots \end{pmatrix}, \tag{3.9}$$

где $A_{Switching}$– Диагональная матрица порядка для одного.

Случайная матрица упорядочивается согласно перестановке строк и столбцов матрицы. Из каждой строки берется место содержащее значение 1.

$$sort_{ran} = \left(A_{Switching_i}\ A_{Switching_{i+1}}\ \ldots\ A_{Switching_{i+n}}\right), A_{Switching} \supset \{1\}, \tag{3.10}$$

где $sort_{ran}$– матрица ранжирования.

Случаи рандомного расположения клавши:

– в первом случае расположения случайного массива упорядочены в соответствии с

положениями массива паролей, если клавиш и местоположение одинаковы в двух массивах по формуле массива:

$$time_{sort_{ran_1}} = \begin{pmatrix} time_{password_i} - time_{password_{i+1}} \\ time_{password_{i+1}} - time_{password_{i+2}} \\ \vdots \\ time_{password_{i+n}} - time_{password_{i+n+1}} \end{pmatrix}, \quad (3.11)$$

где $time_{sort_{ran\_1}}$ – первый случай вычисление ожидаемого значения расстояния для клавши;

– в втором случае клавиш повторяется последовательно в случайном массиве, пропорциональном расположению первого клавиша в массиве исходный пароль.

$$time_{sort_{ran_2}} = \begin{pmatrix} time_{sort_{ran_{i-1}}} - time_{sort_{ran_i}} \\ \vdots \\ time_{sort_{ran_{i-n}}} - time_{sort_{ran_n}} \end{pmatrix}, \quad (3.12)$$

где $time_{sort_{ran\_2}}$ – второй случай вычисление ожидаемого значения расстояния для клавши;

– в третьем случае расположение клавиш случайного массива не в порядке и несовместимо относительно расположено исходной матрицы паролей (рисунок 2).

$$time_{sort_{ran_3}} = \begin{pmatrix} (time_{password_i} - time_{password_{i+1}}) - time_{password_{i+2}} \\ \vdots \\ (time_{password_{i+n}} - time_{password_{i+n+1}}) time_{password_{i+n+2}} \end{pmatrix}, \quad (3.13)$$

где $time_{sort_{ran\_3}}$ – третий случай вычисление ожидаемого значения расстояния для клавши;

Пороговое значение для случайного пароля зависит от трех случаев расчета ожидаемого расстояния от исходного пароля

$$threshould_{ran} = \sqrt{\frac{\sum_{i=1}^{n} time_{sort_{ran-1}} + time_{sort_{ran-2}} + time_{sort_{ran-3}}}{\mu}}, \quad (3.14)$$

где $threshould_{ran}$ – пороговое значение Случайного пароля; μ – Случайная длина пароля.

Предлагается подход к проверке нажатия клавиш, основанный на расстоянии сходства Жаккара, позволяющий выбор Манхэттенского или Евклидово расстояния для выполнения процесса проверки. Повысилось качество аутентификации пользователей в среднем на 8% по сравнению с используемой в существующих работах стандартизацией признаков.

$$d_J(M_{password}, M_{random}) = 1 - J(M_{password}, M_{random}), \quad (3.15)$$

$$\frac{|M_{password} \cup M_{random}| - |M_{password} \cap M_{random}|}{|M_{password} \cup M_{random}|}, \quad (3.16)$$

$$\frac{\sum_{i=1}^{n} |key_{pass_i} \cup key_{ran_i}| - |key_{pass_i} \cap key_{ran_i}|}{\sum_{i=1}^{n} |key_{pass_i} \cup key_{ran_i}|}, \quad (3.17)$$

где $d_J(M_{password}, M_{random})$– расстояние Жаккара;

Если расстояние Жаккара больше 0.5, используется Манхэттенское расстояние. поскольку расстояние Манхэттена измеряет путь вдоль линий сети - самое длинное

расстояние, к которому можно получить доступ между двумя точками, чтобы избежать ложный коэффициент отклонения. Однако если расстояние Жаккара меньше или равно 0.5, будет использоваться Евклидово расстояние, поскольку оно измеряет прямой путь вдоль линий сетки, то есть кратчайшее расстояние, которого можно достичь между двумя точками, чтобы избежать ложный коэффициент принятия.

$$dis_{ran} = \begin{cases} \text{Евклидовое}, & 0.5 \leq d_J\left(M_{password}, M_{random}\right) \\ \text{Манхэттенское}, & 0.5 > d_J\left(M_{password}, M_{random}\right) \end{cases}, \tag{3.18}$$

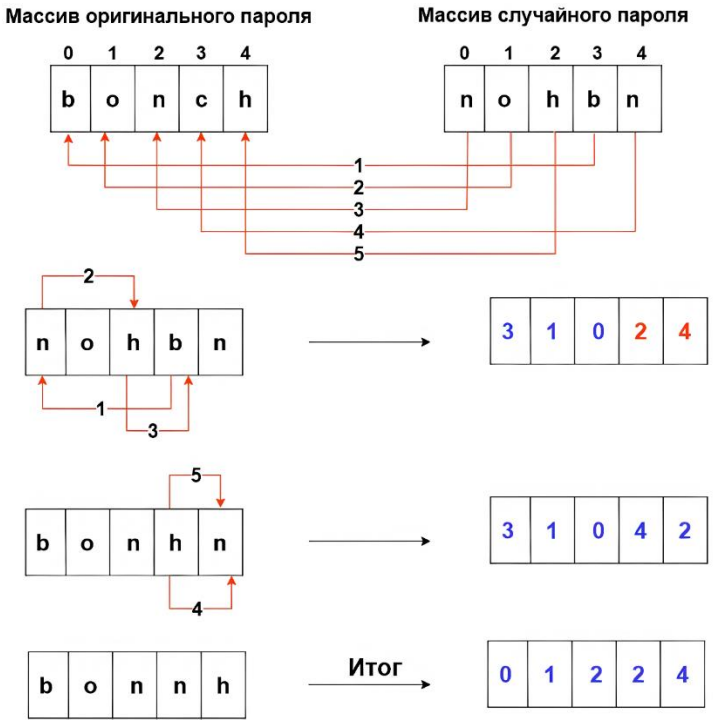

Рисунок 2 – Рандомизация случайного массива

Таблица 3 – Анализ оценки эффективности предложенного метода

Показатель	**Известные методики**	**Разработанная методика**
Количество факторов аутентификации	1	3
Снижение уязвимости от брутфорс атак	~ 15%	~ 6%
Степень защиты, %	90.38%	93.16%
Снижение уязвимости связи с фишинговыми атаками	~ 20%	~ 5%
Скорость обработки данных %	~ 0.31%	~ 0.12%

Была проведена серия экспериментов, в результате которой было подтверждено высокое качество работы предложенных алгоритмов. В результате их использования удалось достичь качества распознавания порядка 0.9316 ROC AUC, что значительно превосходит качество аутентификации пользователей при использовании методов, рассмотренных в существующих научных работах, как показано в Таблице 4.

Таблица 4 – Анализ оценки эффективности экспериментального метода

Метод	**FAR (доля неправильно принятых)**		**FRR (доля неправильно отклонённых)**		**ERR (равная вероятность ошибок)**	
Аутентификация, второй этап (Система динамики нажатия клавиш OTP)	7%	6.43%	2.8%	0.915%	4.9%	3.6725%

В четвертой главе исследования была разработана система непрерывной аутентификации пользователей на основе динамики мыши. Предложен подход разделения веб-страниц на сектора, с расстоянием между ними 19мм. На рисунке 3 показан каждый сектор является кодом клавиши по системе (ASCII), подразделяется четыре типа движения мыши, каждое из которых представляет: Перемещение из одной точки в другую по прямой линии; длинным прямоугольным движением; по кривой и зигзагообразными способом. Каждое из движений представляют соответствующие метрики Манхэттенского, Евклидова расстояния, расстояние Минковского и векторного расстояния с использованием расстояния Левенштейна, которое рассчитывает отличия между образованными строками на этапе обучения и тестирования при каждом моменте затишья.

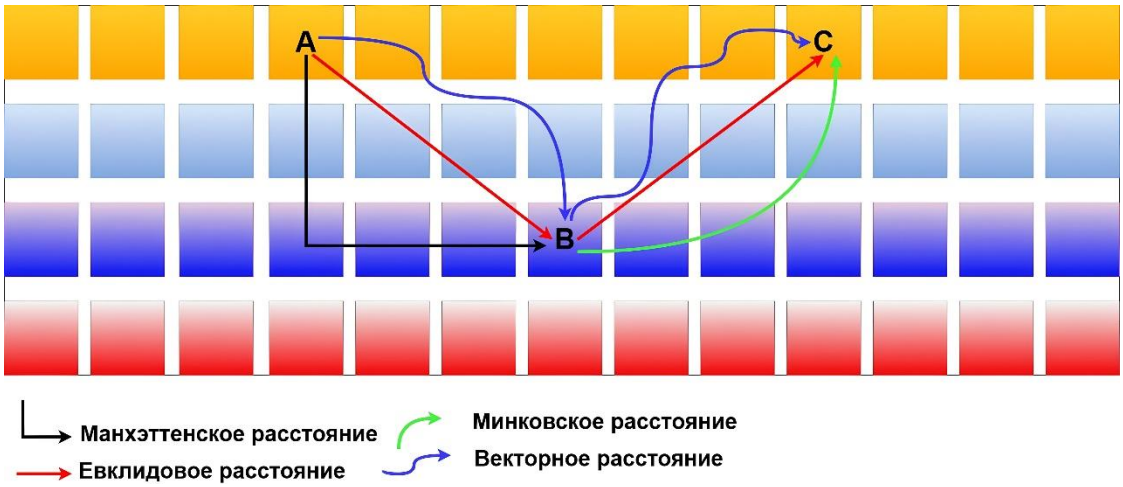

Рисунок 3 –типы движений по веб-странице

Процесс построения модели пользователя на этапе обучения

Расстояние между квадратами определяется при перемещении по веб-странице. Рассчитывается по формуле:

$$Square_{location} = \left| ms_{rp_i} - ms_{rp_{i+1}} \right|, \tag{4.1}$$

где $Square_{location}$ – расположение квадратов.

$$\vec{a}(t) = \lim_{\Delta t \to 0} \frac{\vec{a}(t + \Delta t) - \vec{v}(t)}{\Delta t} = \frac{\Delta \vec{v}}{\Delta t}, \tag{4.2}$$

где $\vec{a}(t)$ – стандартная векторная ускорения; Δt – количество временных меток между щелчками, отпусканием и движениями мыши; $\vec{v}(t)$ – стандартная векторная скорость

$$\overline{mva} = \frac{1}{n}\left(\sum_{i=1}^{n} \vec{a}_i\right) = \frac{\sum \vec{a}(t)_i - \vec{a}(t)_{i+1} - \cdots - \vec{a}(t)_{i+n}}{\mu - 1}, \tag{4.3}$$

где $\overline{mva}$ – среднее арифметическое значений ускорения; μ – длина строки, образуемой движением мыши.

$$e(ac) \sqrt[2]{\sum_{\boldsymbol{i}}^{\boldsymbol{n}} \left(\frac{\vec{a}(t)_i - \vec{a}(t)_i}{\overline{mva}}\right)^2}, \tag{4.4}$$

$$m(ac) = \frac{|\vec{a}(t)_i - \vec{a}(t)_{i+1}| + |\vec{a}(t)_{i+2} - \vec{a}(t)_{i+3}| + \cdots + |\vec{a}(t)_{i+n} - \vec{a}(t)_n|}{\mu - 1}, \tag{4.5}$$

$$mi(ac) = \sqrt[3]{\left|\frac{\vec{a}(t)_i - \vec{a}(t)_{i+1}}{\overline{mva}}\right|^3 + \left|\frac{\vec{a}(t)_{i+2} - \vec{a}(t)_{i+3}}{\overline{mva}}\right|^3 + \cdots + \left|\frac{\vec{a}(t)_{i+n} - \vec{a}(t)_n}{\overline{mva}}\right|^3}, \tag{4.6}$$

$$\overrightarrow{rv} = \sqrt[3]{\sum_{i=1}^{n} \frac{19mm\,.\,Square_{location}}{\overline{mva}}}, \tag{4.7}$$

где e – Евклидово расстояние при первом случае; α_i – среднее арифметическое ускорение; m – манхэттенское расстояние при первом случае; mi – расстояние Минковского при третьем случае; $\overrightarrow{rv}$ – векторное расстояние между точками кривизны при четвертом случае.

$$distance_{Total} = \sqrt{\frac{e(ac) + m(ac) + mi(ac) + \overrightarrow{rv}}{4}}, \tag{4.8}$$

где $distance_{Total}$ – общее расстояние, рассчитанное из четырех расстояний.

Расстояние Левенштейна рассчитывает отличия между строковым типом, образованным на этапах обучения и тестирования для того, чтобы увеличить свободу перемещения по веб-странице и не ограничивать пользователя фиксированным движением или определенным количеством щелчков мыши.

$$\mathrm{lev}(a,b) = \begin{cases} |a| & if\ |b| = 0 \\ |b| & if\ |a| = 0 \\ lev(tail(a), tail(b)) & if\ head\ (a) = head(b), \\ 1 + min \begin{cases} lev(tail(a), b) \\ lev\big(a, tail(b)\big) \\ lev\big(tail(a), tail(b)\big) \end{cases} & otherwise. \end{cases} \tag{4.9}$$

где lev– расстояние Левенштейна; a – номер строки в массиве.; b – номер столбца в матрице; $head\ (a)$ – первая буква ряда; $head\ (b)$ – первая буква столбца; $tail$– серия букв, за исключением первой буквы.

В используемом подходе было предложено вычислять пороговое значение на этапе

проверки, а не на этапе обучения, как в предыдущих исследованиях, чтобы снизить показатели ложного отвержения и ложного принятия. Предложен подход, который вычисляет пороговое значение периодически и многократно при каждой остановке движения с использованием расстояния Левенштейна. В отличие от предыдущих методов, процесс проверки выполняется многократно в пределах страницы и не основан на определенном времени или количестве движений мыши. Повышено качество аутентификации пользователей в среднем на 2% по сравнению с используемой в существующих работах стандартизацией признаков.

Случаи порогового значения относительно количества щелчков мыши рассчитываются по формуле:

$$threshould_i = \begin{cases} threshould_1, & \mu_{lev} > \mu_{Training} \\ threshould_2, & \mu_{lev} < \mu_{Training}, \\ threshould_3, & \mu_{lev} = \mu_{Training} \end{cases} \quad (4.10)$$

где $threshould_i$ – пороговое значение; μ_{lev} – длина букв и символов, сформированных на этапе тестирования; $\mu_{Training}$ – длина букв и символов, сформированных на этапе обучения;

– Если длина букв и символов, сформированных на этапе тестирования больше длины букв и символов, сформированных на этапе обучения, пороговое значение рассчитывается по формуле:

$$threshould_1 = \frac{distance_{Total}}{\mu_{lev} - (\mu_{lev} - \mu_{Training})}$$

– Если длина букв и символов, сформированных на этапе тестирования меньше длины букв и символов, сформированных на этапе обучения, пороговое значение рассчитывается по формуле:

$$threshould_2 = \frac{distance_{Total}}{\mu_{lev} + (\mu_{lev} - \mu_{Training})}$$

– Если длина букв и символов, сформированных на этапе тестирования равно длине букв и символов, сформированных на этапе обучения, пороговое значение рассчитывается по формуле:

$$threshould_3 = \frac{distance_{Total}}{\mu_{lev} + 1}$$

Таблица 5 – Анализ оценки эффективности предложенного метода

Показатель	**Известные методики**	**Разработанная методика**
Степень защиты, %	92.48%	97.2%
Быстрое обнаружение подозрительного поведения, %	90%	94%
Вероятность перехвата сеанса	7.52%	2.8%

Была проведена серия экспериментов, в результате которых было подтверждено высокое качество работы предложенных алгоритмов. В результате использования предложенной комбинации алгоритмов достигнуто качество распознавания порядка 0.9718 ROC AUC, что значительно превосходит качество аутентификации пользователей при использовании методов, рассмотренных в существующих научных работах. как показано в Таблице 6.

Таблица 6 – Анализ оценки эффективности экспериментого метода

Метод	**FAR (доля неправильно принятых)**		**FRR (доля неправильно отклонённых)**		**ERR (равная вероятность ошибок)**	
Непрерывная аутентификация	4.6%	3.4%	6.6%	1.8%	5.6%	2.6%

ЗАКЛЮЧЕНИЕ

Поставленная в диссертационном исследовании цель по обеспечению защиты от угроз безопасности в системах веб-приложений и по защите пользовательских данных от взлома, путем создания статической и непрерывной системы многофакторной биометрическо-поведенческой аутентификацией, достигнута. Для достижения цели были поставлены и выполнены задачи, получены научные результаты, составляющие следующие итоги исследования:

1. Разработана высокоточная система двухфакторной аутентификации (2FA), через анализ поведенческой модели для определения пользователя на основе динамики нажатия клавиш и мыши для аутентификации:

– Разработана модель аутентификации на основе динамики нажатия для выявления аномалий путем алгоритма на основе объединения трех расстояний: Манхэттенского расстояния, Евклидова расстояния и расстояния Чебышева, чтобы вычислить по теореме Пифагора угол прямоугольного треугольника, прилежащего к гипотенузе, как индивидуальное пороговое значение для пользователей, с целью уменьшения значения частоты ложного отклонения и принятия. Позволяет извлечь характеристики нажатых клавиш от всех случаев использования клавиатуры, включая не валидные к вводу пароля.

– Разработана модель аутентификации на основе динамики мыши, благодаря алгоритму использования расстояния Минковского, которое рассчитывается через кривую четверти круга, и Манхэттенского расстояния, которое находится через площадь четверти круга и длину дуги четверти круга. Исходя из полученных данных высчитывается пороговое значение для последующей аутентификации пользователя. Тестирование зависит от длины дуги, рассчитанной по расстоянию Минковского.

– Разработана модель идентификации количества использованных при печати рук (1 или 2), с применением законов движения кинематики, Предложен подход разделения клавиатуры на 8 частей для облегчения рассчитывания расстояния между клавишами.

2. Разработана система многофакторной аутентификации (MFA) пользователей и субъектов доступа для веб-приложения. Предложен подход генерации случайного слова от существующего пароля на основе его биометрических данных с помощью расстояние Жаккара, которое рассчитывает сходство между случайным словом и самим паролем для принятия решения, будут проходить последующие измерения через Манхэттенское или Евклидово расстояние. Отправка сообщение со случайным паролем происходит через библиотеку PHPMalier. Система позволяет объединить фактор знания, владения с фактором свойства, связав систему OTP с поведенческо-биометрической системой, позволяет добавить уровень защиты и затруднить взлом кода OTP.

3. Разработана система непрерывной аутентификации пользователей на основе динамики мыши. Предложен подход разделения веб-страниц на сектора, с расстоянием между ними 19мм. Каждый сектор является кодом клавиши по системе (ASCII), подразделяется четыре типа движения мыши, каждое из которых представляет: Перемещение из одной точки

в другую по прямой линии, Перемещение из одной точки в другую длинным прямоугольным движением, Движение из одной точки в другую по кривой и Движение из одной точки в другую зигзагообразными способом. Каждое из движений представляют соответствующие метрики Манхэттенское расстояние, Евклидово расстояние, расстояние Минковского и векторное расстояние с использованием расстояния Левенштейна, которое рассчитывает отличия между образованными строками на этапе обучения и тестирования при каждом моменте затишья. Благодаря этому вычисления порогового значения на этапе проверки, вместо этапа обучения, чтобы снизить показатели ложного отвержения и принятия. быстро выявлять аномалий с каждым моментом затишья.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных ВАК

1. Красов, А.В. Аутентификация и идентификация пользователя с использованием биометрической динамики нажатия клавиш на основе "манхэттенского и евклидовского расстояния" / А.В. Красов, Ю. Альотум, И.А. Ушаков, В.В. Максимов, А.В. Архипов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2023. – № 4. – С. 49–56. DOI: 10.46418/2079-8199_2023_4_10

2. Альотум, Ю.М.А.А. Мягкая биометрия для аутентификации и определения рук на основе использования клавиатуры / Ю.М.А.А. Альотум, А.В. Красов // Труды учебных заведений связи. – 2024. – Т. 10, – № 6. – С. 55–67. DOI 10.31854/1813-324X-2024-10-6-55-67

3. Альотум, Ю.М.А.А Создание железных ворот для аутентификации и идентификации пользователя с использованием биометрической динамики движения мыши на основе "Манхэттенского расстояния. / Ю.М.А.А. Альотум // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2024. – № 2. – С. 95–102. DOI: 10.46418/2079-8199_2024_2_18

4. Альотум, Ю.М.А.А. Непрерывная аутентификация и мониторинг пользователей с использованием биометрии динамики мыши / Ю.М.А.А. Альотум // Экономика и качество систем связи. – 2024. – № 4(34). – С. 172–180.

Программы для ЭВМ

5. Альотум Ю.М.А.А., Пешков А.И. Программа по многофакторной аутентификации пользователей на основе биометрических динамических методов: Свидетельство о регистрации программы для ЭВМ RU 2024664769, 24.06.2024.

Публикации в других изданиях

6. Yousef, M.A.A.A. Biometric and behavioral authentication and soft biometrics using keystroke and mouse dynamics // ICAIT 2023: Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 марта 2023 года. – Санкт-Петербург: СПбГУТ, 2023. – Т.1. – С. 70–75.

7. Альотум, Ю.М.А.А. Веб-сайт заказа здорового питания "Deliveryhealthy" // Цифровые технологии и защита информации в современном обществе: сборник докладов

Международной научно-практической конференции, Астрахань, 29–30 ноября 2021 года. – 2021. – С. 29–32.

8. Альотум, Ю.М.А.А. Метод одноразового пароля в механизме факторной аутентификации и возможность его использования в биометрической системе // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024): Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. – Санкт-Петербург: СПбГУТ, 2025. – С. 150–155.

9. Алотоум Ю.М.А.А. Биометрическая аутентификация и мягкая биометрика / Ю.М.А.А. Алотоум // Региональная информатика (РИ-2024). – СПб., 2024. – С. 428–429.

10. Алотоум Ю.М.А.А. Биометрическая и поведенческая аутентификация, а также мягкая биометрия с использованием динамики нажатия клавиш и мыши // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13. СПОИСУ. – СПб., 2024. – С.633–636.

11. Альотум, Ю.М.А.А. Биометрические данные и их возможности достижения многофакторной аутентификации методом одноразового пароля // 65-ая Научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС СПбГУТ). Сборник трудов. – СПб., 2025.

12. Альотум, Ю.М.А.А. Динамика нажатия клавиш и их роль в ненавязчивом обеспечении многофакторной аутентификации с помощью OTP // 65-ая Научно-техническая конференция профессорско-преподавательского состава, научных работников и асприрантов (НТК ППС СПбГУТ). Сборник трудов. – СПб., 2025.

Подписано в печать 24.04.2025. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1