TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа _Инженерная школа информационных технологий и робототехники_____
Направление подготовки _09.04.01 Информатика и вычислительная техника_____
ООП/ОПОП _Разработка интернет-приложений _____
Отделение школы (НОЦ) _Отделение информационных технологий _____

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРАНТА

Тема работы
Разработка системы динамической аутентификации пользователя на основе анализа его работы на клавиатуре компьютера

УДК 004.81:004.353.4

Обучающийся

Группа	ФИО	Подпись	Дата
8ВМ11	Очиров Жаргал Александрович		01.03.2023

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Кочегурова Е. А	к.т.н., доцент		01.03.2023

КОНСУЛЬТАНТЫ ПО РАЗДЕЛАМ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент, ОСГН ШБИП	Былкова Т. В	к.э.н., доцент		01.03.2023

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ООД ШБИП	Федорчук Ю. М	д.т.н., профессор		01.03.2023

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП, должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент, ОИТ ИШИТР	Кочегурова Е. А	к.т.н., доцент		01.06.2023

Томск – 2023 г.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ООП

по направлению 09.04.01 Информатика и вычислительная техника

Код компетенции	Наименование компетенции
Универсальные компетенции	
УК(У)-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК(У)-2	Способен управлять проектом на всех этапах его жизненного цикла
УК(У)-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК(У)-4	Способен применять современные коммуникативные технологии, в том числе на иностранном (-ых) языке (-ах), для академического и профессионального взаимодействия
УК(У)-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК(У)-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
Общепрофессиональные компетенции	
ОПК(У)-1	Способен самостоятельно приобретать, развивать и применять математические, естественно-научные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте
ОПК(У)-2	Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач
ОПК(У)-3	Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями
ОПК(У)-4	Способен применять на практике новые научные принципы и методы исследований
ОПК(У)-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК(У)-6	Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования
ОПК(У)-7	Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий
ОПК(У)-8	Способен осуществлять эффективное управление разработкой программных средств и проектов
Профессиональные компетенции	
ПК(У)-1	Способен разрабатывать и администрировать системы управления базами данных
ПК(У)-2	Способен проектировать сложные пользовательские интерфейсы
ПК(У)-3	Способен управлять процессами и проектами по созданию (модификации) информационных ресурсов
ПК(У)-4	Способен осуществлять руководство разработкой комплексных проектов на всех стадиях и этапах выполнения работ
ПК(У)-5	Способен проектировать и организовывать учебный процесс по образовательным программам с использованием современных образовательных технологий

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.01 Информатика и вычислительная техника
Отделение школы (НОЦ) Отделение информационных технологий

УТВЕРЖДАЮ:
Руководитель ООП/ОПОП
_____ _____ Кочегурова Е.А.
(Подпись) (Дата) (ФИО)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

Обучающийся:

Группа	ФИО
8ВМ11	Очиров Жаргал Александрович

Тема работы:

Разработка системы аутентификации пользователя на основе его анализа работы на клавиатуре компьютера	
Утверждена приказом директора (дата, номер)	от 06.04.2023 №96-61/с

Срок сдачи обучающимся выполненной работы:	01.06.2023

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Объектом исследования является система аутентификации пользователя на основе анализа его работы на клавиатуре компьютера.
Перечень разделов пояснительной записки подлежащих исследованию, проектированию и разработке	1. Исследование предметной области. 2. Изучение характеристик клавиатурного почерка. 3. Обзор методов аутентификации пользователей. 4. Разработка алгоритма аутентификации. 5. Разработка системы. 6. Тестирование и анализ результатов. 7. Раздел ВКР «Финансовый менеджмент

	ресурсоэффективность и ресурсосбережение». 8. Раздел ВКР «Социальная ответственность». 9. Раздел ВКР на английском языке.
Перечень графического материала	Презентация в формате *.pptx

Консультанты по разделам выпускной квалификационной работы	
Раздел	**Консультант**
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Доцент ОСГН, ШБИП к.э.н. Былкова Т.В.
Социальная ответственность	Профессор ООД, ШБИП д.т.н. Федорчук Ю.М.
Английский язык	Доцент ОИЯ, ШБИП к.ф.н. Степура С.Н.
Названия разделов, которые должны быть написаны на иностранном языке:	
Раздел 1	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	01.03.2023

Задание выдал руководитель

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент ОИТ ИШИТР	Кочегурова Е.А.	к.т.н., доцент		

Задание принял к исполнению обучающийся:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ11	Очиров Жаргал Александрович		

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.01 Информатика и вычислительная техника
Уровень образования Магистратура
Отделение школы (НОЦ) Отделение информационных технологий
Период выполнения (осенний / весенний семестр 2022/2023 учебного года)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Обучающийся:

Группа	ФИО
8ВМ11	Очиров Жаргал Александрович

Тема работы:

Разработка системы аутентификации пользователя на основе его анализа работы на клавиатуре компьютера

Срок сдачи обучающимся выполненной работы:	01.06.2023

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
01.06.2023	Основная часть	70
01.06.2023	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	10
01.06.2023	Социальная ответственность	10
01.06.2023	Приложение на английском языке	10

СОСТАВИЛ:
Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Кочегурова Е.А.	к.т.н., доцент		

СОГЛАСОВАНО:
Руководитель ООП/ОПОП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Кочегурова Е.А.	к.т.н., доцент		

Обучающийся

Группа	ФИО	Подпись	Дата
8ВМ11	Очиров Жаргал Александрович		

РЕФЕРАТ

Выпускная квалификационная работа выполнена на 107 страницах, содержит 37 рисунков, 23 таблицы, 40 источников, 1 приложение.

Ключевые слова: клавиатурный почерк, информационная безопасность, аутентификация, биометрия, динамические характеристики клавиатурного почерка.

Объектом исследования является разрабатываемая система аутентификации пользователя на основе его анализа работы на клавиатуре.

Цель работы – развитие задач теории распознавания пользователей на основе динамических характеристик клавиатурного почерка и разработка на этой основе алгоритмического и программного обеспечения системы аутентификации пользователя.

В процессе исследования проводились работы по изучению методов аутентификации пользователей по клавиатурному почерку. В ходе работы были рассмотрены существующие подходы к решению задачи аутентификации, а также предложены решения по оптимизации существующих алгоритмов.

В результате исследования было разработано программное приложение для аутентификации пользователя на основе динамических характеристик клавиатурного почерка. Были изучены, а также протестированы с точки зрения точности аутентификации алгоритмы распознавания пользователя на основе динамических характеристик клавиатурного почерка.

Область применения: аутентификация пользователей по динамическим характеристикам клавиатурного почерка, определение психофизиологического состояния пользователя, скрытый мониторинг пользователей корпоративной сети с целью определения подмены оператора.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире информационных технологий и интернет-сервисов, безопасность и защита персональных данных являются одной из наиболее актуальных и важных задач. По данным статистики, в 2020 году в мире было более 4,6 миллиарда пользователей интернета, которые использовали различные виды аутентификации для доступа к своим учетным записям, приложениям и сервисам. Однако, большинство из них имеют свои недостатки, такие как неудобство использования, возможность кражи или подделки, высокая стоимость оборудования и обслуживания.

В связи с этим, в последнее время все больше внимания уделяется разработке и применению так называемых поведенческих методов аутентификации, которые основаны на анализе индивидуальных особенностей поведения пользователя при работе с компьютером или мобильным устройством. Одним из таких методов является динамическая аутентификация пользователя на основе анализа его работы на клавиатуре компьютера.

Данный метод заключается в том, что при вводе текста на клавиатуре компьютера пользователь демонстрирует определенный стиль набора текста, который характеризуется различными параметрами, такими как скорость набора, длительность удержания клавиш, интервалы между нажатиями клавиш и т.д. Эти параметры формируют уникальный профиль пользователя, который может быть использован для его идентификации и аутентификации.

Данный метод имеет ряд преимуществ по сравнению с другими видами аутентификации, такие как удобство использования, низкая стоимость, высокая точность и невозможность подделки. Однако, он также имеет ряд недостатков и угроз, связанных с безопасностью и защитой персональных данных пользователя. Например, киберпреступники могут использовать различные способы для получения доступа к профилю пользователя или подмены его поведенческих характеристик. Такие способы могут включать

фишинг, кейлоггеры, имитацию стиля набора текста и т.д. Это может привести к утечке или компрометации данных пользователя или к нарушению его конфиденциальности.

Поэтому, для повышения безопасности и защиты персональных данных необходимо сочетать поведенческую аутентификацию и другие способы, такие как шифрование данных, обновление программного обеспечения, резервное копирование данных, использование надежных паролей и двухфакторной аутентификации.

Целью данной работы является изучение метода динамической аутентификации пользователя на основе анализа его работы на клавиатуре компьютера и оценка. Для достижения этой цели были поставлены следующие задачи:

- провести обзор существующих методов аутентификации пользователя и сравнить их с методом динамической аутентификации на основе работы на клавиатуре;
- изучить основные параметры и характеристики работы пользователя на клавиатуре компьютера и способы их измерения и анализа;
- подобрать набор данных для эксперимента
- разработать программное обеспечение обработки данных о работе пользователя на клавиатуре компьютера;
- провести экспериментальное тестирование метода динамической аутентификации пользователя на основе работы на клавиатуре компьютера;
- оценить точность и надежность метода динамической аутентификации пользователя на основе работы на клавиатуре компьютера;
- выявить возможные угрозы и риски для безопасности и защиты персональных данных пользователя при использовании данного метода аутентификации;
- предложить рекомендации по улучшению метода динамической аутентификации пользователя на основе работы на клавиатуре компьютера.

1 СОСТОЯНИЕ И АКТУАЛЬНОСТЬ КЛАВИАТУРНОЙ ИДЕНТИФИКАЦИИ

1.1 Вопросы клавиатурной аутентификации и идентификации

Вопросы клавиатурной аутентификации и идентификации относятся к области биометрии поведения, которая использует манеру и ритм набора текста на клавиатуре для определения личности пользователя. Клавиатурная аутентификация может быть основана на различных параметрах, таких как скорость набора, длительность нажатия клавиш, интервалы между клавишами и ошибки. Это показано на рисунке 1

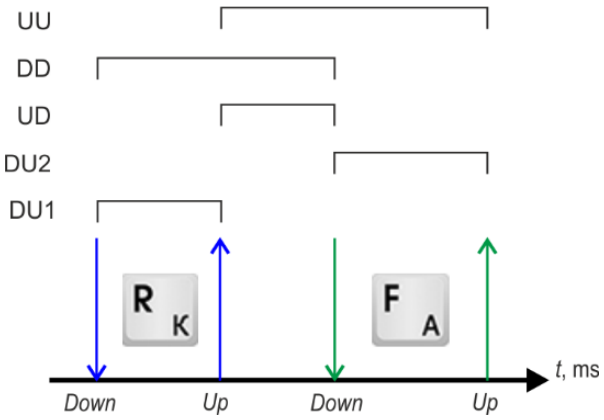

Рисунок 1 – Показатели клавиатурного подчерка

Где, DU – время удержания клавиши, UD – пауза между нажатиями, UU или DD интервал между нажатием или отпусканием одной клавиши и нажатием или отпусканием следующей клавиши соответственно.

Один из возможных способов защиты системы от несанкционированного доступа – использовать двухэтапный процесс верификации:

- Первичная идентификация личности
- Динамическая аутентификация личности

Однако у каждого человека есть индивидуальный ритм набора текста. Ввиду этой особенности биометрическая система распознавания личности

может использовать клавиатурный почерк. Для наглядности на рисунке 2 представлена скорость набора текста 8 пользователей из датасета KM.

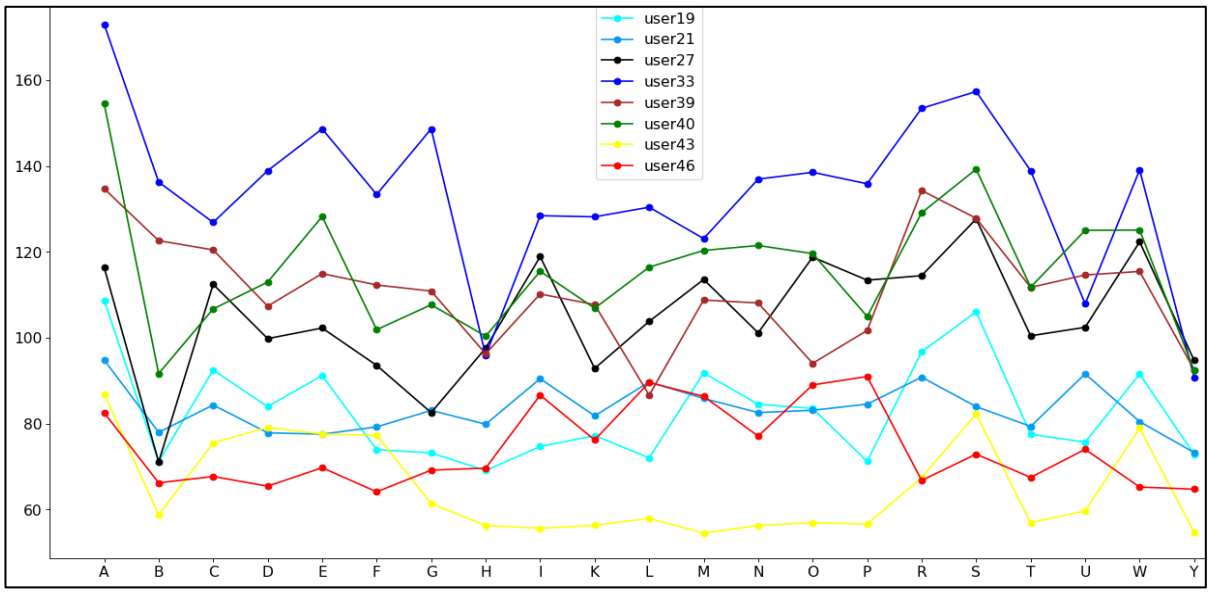

Рисунок 2 – Клавиатурные шаблоны пользователей

Визуальный анализ демонстрирует определенные расхождения между временами нажатия определенных букв на клавиатуре. Данный разброс как раз демонстрирует уникальность ритма нажатия клавиш каждого пользователя. С технической точки зрения, чем больше клавиш пользователь нажимает, тем более точно алгоритм может понять и воссоздать клавиатурный шаблон пользователя. Уникальность клавиатурного шаблона увеличивает точность системы распознавания.

Клавиатурная идентификация — это способ определения пользователя среди множества других потенциальных пользователей на основе того, как он печатает на клавиатуре. При этом учитываются различные факторы, влияющие на стиль набора, например, скорость печатания, ритм нажатия клавиш, длительность удержания клавиши и интервалы между нажатиями. Каждый человек имеет свой индивидуальный клавиатурный почерк, который отличает его от других и может быть использован как биометрический признак для его идентификации

Для реализации клавиатурной аутентификации и идентификации могут использоваться различные техники, от статистических методов до подходов искусственного интеллекта, таких как нейронные сети. Одним из преимуществ клавиатурной аутентификации является то, что она не требует специального оборудования, такого как сканеры отпечатков пальцев или лица, а может работать с любой стандартной клавиатурой. Однако клавиатурная аутентификация также имеет свои недостатки, такие как влияние физического или эмоционального состояния пользователя, изменение стиля набора во времени и возможность подделки или имитации.

Клавиатурная аутентификация и идентификация могут применяться для различных целей, таких как повышение безопасности входа в систему, контроль доступа к конфиденциальной информации, мониторинг поведения пользователей в сети или обнаружение вторжений. Клавиатурная идентификация также может использоваться для психологического анализа личности по ее способу печатания.

1.2 Методы аутентификации

Существует множество методов аутентификации пользователя. Методы можно условно разделить на четыре группы что показано на рисунке 3:

- На основе знания уникальной информации;
- На основе владения уникальным предметом;
- На основе биометрии
- И других признаках

Рисунок 3 – Методы аутентификации

Аутентификация на основе знаний личной информации (имени, пароля, секретного вопроса). Эти способы просты в использовании и недорогие. Однако, они обеспечивают низкий уровень безопасности [1].

Аутентификация на основе владения личными объектами пользователя, такими, как смарт-карты и ключи. Это наименее популярный метод в электронной аутентификации, потому что личные предметы могут быть украдены или скопированы [1].

Другие признаки аутентификации основаны на местоположении, временной зоне, IP-адресе и др. [1]

Биометрические признаки аутентификации разделяются на физиологические и поведенческие. Физиологические характеристики включают форму лица, радужную оболочку глаза, отпечатки пальцев и т.д. Поведенческие - голос, походка, подпись, движение мыши, рукописный и клавиатурный почерк. Аутентификация на основе физиологических признаков точна, но технические устройства распознавания довольно дороги [1]. Клавиатурный почерк относится к биометрии поведения.

Методы клавиатурного распознавания – это способы идентификации и аутентификации пользователя по его индивидуальному стилю набора текста на клавиатуре компьютера. Эти методы относятся к поведенческой биометрии и могут использоваться для статической или динамической (непрерывной) проверки подлинности пользователя.

Частота использования методов клавиатурного распознавания зависит от различных факторов, таких как тип вводимого текста (структурированный или свободный), язык текста (русский или английский), цель аутентификации (первичная или вторичная), алгоритм классификации (основанный на метрических расстояниях, статических методах или машинном обучении) и т.д.

Согласно обзору литературы [3], существует множество различных методов клавиатурного распознавания, которые можно разделить на три основные группы с точки распознавания образов:

- Оценка метрических расстояний
- Статистические методы
- Методы машинного обучения

Относительная частота использования разных методов клавиатурного распознавания представлена на рисунке 4 в порядке убывания [3].

Рисунок 4 – Относительная частота использования методов клавиатурного распознавания

Как видно из рисунка, наиболее часто используемыми методами клавиатурного распознавания являются те, которые основаны на оценке метрических расстояний между текущим и эталонным профилями пользователя. Эти методы просты в реализации и не требуют сложных вычислений. Однако, они также имеют свои недостатки, такие как низкая точность, высокая чувствительность к изменениям в поведении пользователя и необходимость выбора порогового значения для принятия решения.

Статические методы клавиатурного распознавания используют различные статические модели для описания распределения параметров клавиатурного распознавания и вычисления вероятности принадлежности текущего профиля к эталонному. Эти методы более точные и устойчивые к шумам и вариациям данных, но они также более сложные в реализации и требуют большего объема данных для обучения модели.

Методы машинного обучения клавиатурного распознавания применяют различные алгоритмы классификации, такие как нейронные сети, опорные вектора, дерево решения и т.д., для обучения модели классификатора на основе имеющихся данных и прогнозирования принадлежности текущего профиля к одному из заранее определенных классов (пользователей). Эти методы могут достигать высокой точности и адаптивности к новым данным, но они также требуют большого объема данных для обучения, а также подбора оптимальных параметров для каждого алгоритма.

В целом, можно сказать, что частота использования методов клавиатурного распознавания определяется различными факторами и зависит от конкретной задачи и условий аутентификации пользователя.

1.3 Режимы аутентификации

Наиболее обоснованный для системы распознавания и комфортный для пользователя способ аутентификации личности — это постоянный и скрытый мониторинг динамики его работы.

Динамические характеристики клавиатурного почерка более сложны для распознавания, нежели физиологические. Однако этот факт компенсируется более трудоемким процессом подмены пользователя, что благотворно сказывается на уровне защищенности системы. Кроме того, динамические характеристики могут отражать не только личность

пользователя, но и его эмоциональное состояние, что может быть полезно для анализа его поведения и мотивации.

Существует два вида аутентификации: статическая и динамическая. При статической аутентификации пользователю системы предоставляется определенный текст фиксированной длины, который пользователь должен ввести для подтверждения своей личности. Этот текст может быть паролем, ПИН-кодом или другой комбинацией символов. Преимуществом этого способа является простота реализации и проверки. Недостатком является возможность кражи или забывания текста, а также необходимость постоянного запоминания новых текстов при их изменении.

Динамическая аутентификация представляет собой более сложный процесс мониторинга нажатий клавиш пользователем. При определенном заданном условии, это может быть частое использование служебных символов, что не свойственно пользователю, либо слишком медленная печать, система может ограничить доступ к учетной записи и попросит повторно пройти процесс идентификации. Преимуществом этого способа является возможность непрерывной проверки подлинности пользователя в течение всей сессии работы с системой, а также отсутствие необходимости запоминать специальные тексты. Недостатком является сложность реализации и настройки параметров распознавания.

Оба способа могут дополнять друг друга в зависимости от поставленной организацией задачи. Например, статическая аутентификация может служить как первый уровень защиты. Динамическая аутентификация будет выступать в качестве второго. Таким образом, можно повысить надежность и безопасность системы распознавания личности.

1.4 Жизненный цикл аутентификации

Жизненный цикл клавиатурного распознавания – это последовательность этапов, которые необходимо выполнить для идентификации или аутентификации пользователя (рисунок 5).

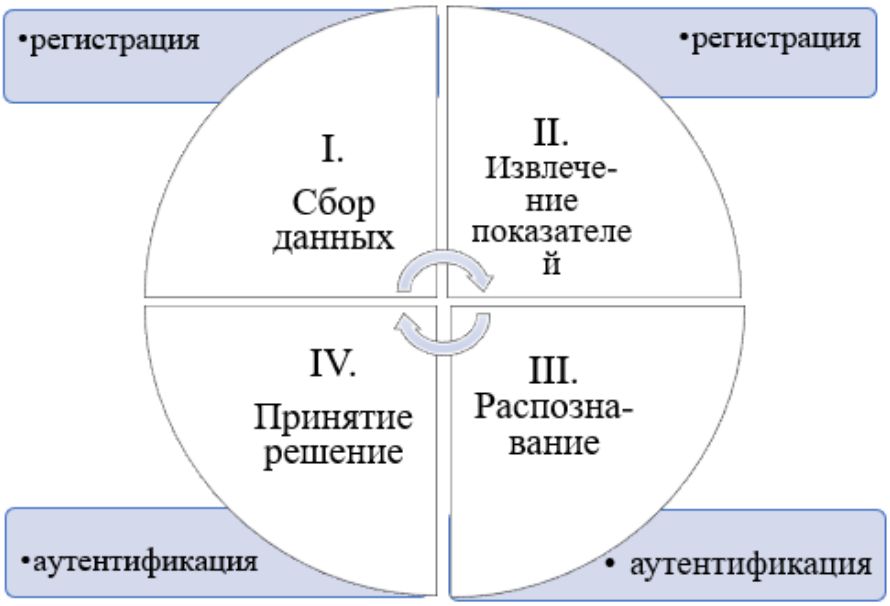

Рисунок 5 – Жизненный цикл аутентификации

Первый этап жизненного цикла распознавания является сбор данных о нажатиях клавиш пользователя – это первый и важный этап жизненного цикла клавиатурного распознавания. Этот этап заключается в том, что на компьютере пользователя устанавливается специальная программа или устройство, которое фиксирует и сохраняет нажатия клавиш, которые пользователь делает при вводе различных текстов. Эти тексты могут быть структурированными или свободными, на разных языках и т.д.

Существует два основных типа сбора данных о нажатиях клавиш пользователя:

- Аппаратный
- Программный

Аппаратный способ данных о нажатиях клавиш пользователя осуществляется с помощью специальных устройств, которые подключаются

между клавиатурой и компьютером или встраиваются в саму клавиатуру. Эти устройства записывают все данные, которые передаются от клавиатуры к компьютеру, во внутреннюю память или на внешний носитель. Примером такого устройства может быть так называемый keylogger, который показан на рисунке 6

Рисунок 6 – Аппаратный keylogger

Программный сбор данных о нажатиях клавиш пользователя осуществляется с помощью специальных программ, которые устанавливаются на компьютер пользователя и перехватывают все данные, которые поступают от клавиатуры к операционной системе или приложениям. Эти программы могут быть разными по уровню доступа и сложности реализации. Например, существуют программы, которые работают в пользовательском режиме и используют API-функции операционной системы для получения данных о нажатиях клавиш [6]. Также существуют программы, которые работают в ядре операционной системы и имеют прямой доступ к драйверам клавиатуры [6]. Примером такой программы может быть WhatPulse, который показан на рис.7

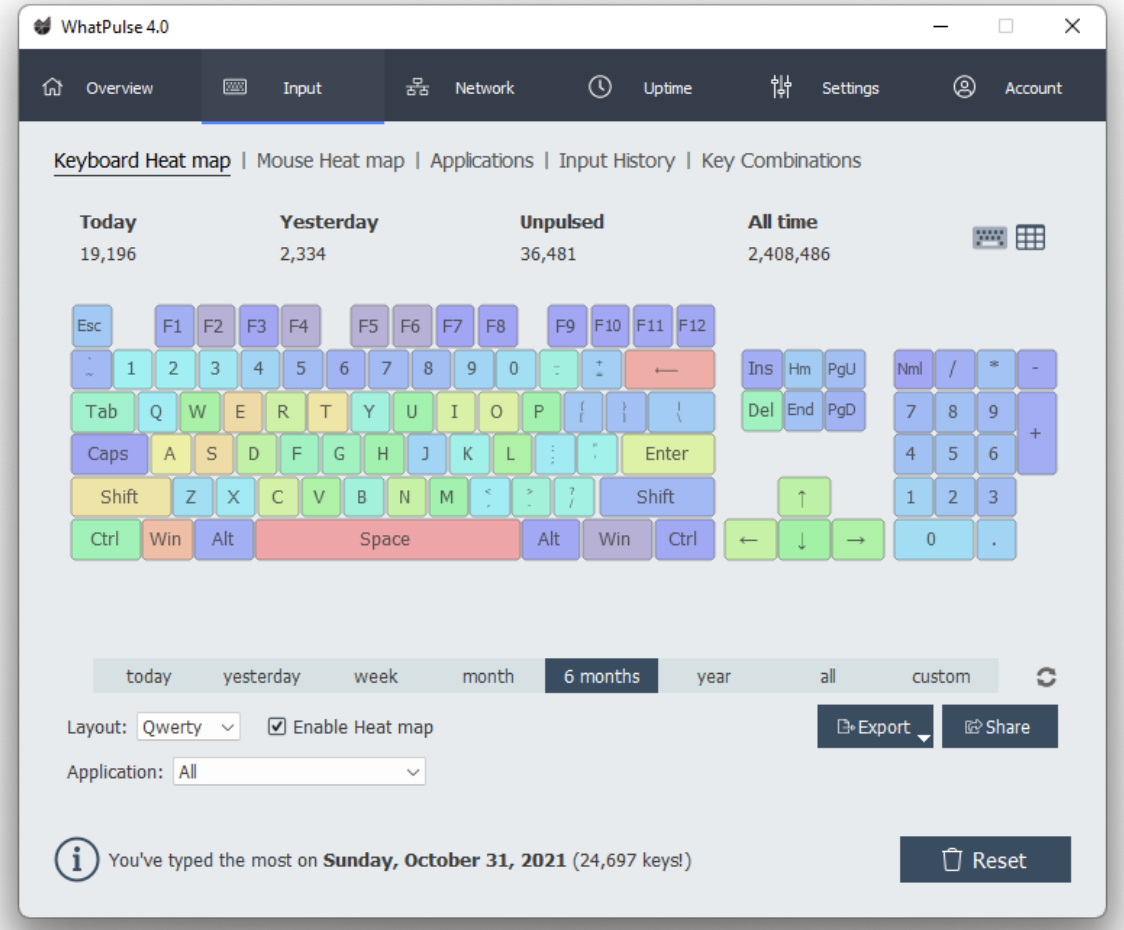

Рисунок 7 – Пример программного keylogger WhatPulse

Сбор данных о нажатиях клавиш пользователя имеет свои преимущества и недостатки. С одной стороны, он позволяет получить большой объем информации о стиле набора текста пользователя, который может быть использован для его идентификации и аутентификации. С другой стороны, он может нарушать приватность и безопасность пользователя, если эти данные попадут в руки злоумышленников или будут использованы без согласия пользователя.

Извлечение признаков клавиатурного почерка – это **второй этап** жизненного цикла клавиатурного распознавания. Этот этап заключается в том, что из собранных данных о нажатиях клавиш пользователя выделяются те характеристики, которые наилучшим образом отражают его

индивидуальный стиль набора текста и позволяют отличить его от других пользователей. Эти характеристики называются признаками клавиатурного почерка.

Существует много разных видов признаков клавиатурного почерка, которые могут быть извлечены из данных о нажатиях клавиш пользователя. Например существуют:

- Статистические признаки, которые описывают распределение и вариабельность различных параметров нажатий клавиш, таких как скорость набора, длительность удержания клавиши, интервалы между нажатиями клавиш и т.д.
- Символьные признаки, которые описывают частоту и последовательность использования разных символов на клавиатуре, такие как буквы, цифры, знаки препинания и т.д.

Этап распознавания – это **третий этап** жизненного цикла клавиатурного распознавания. Этот этап заключается в том, что извлеченные признаки клавиатурного почерка пользователя сравниваются с эталонными признаками или профилями других пользователей с помощью алгоритма классификации, который определяет, к какому классу или категории относится пользователь. Этот этап может быть реализован с помощью различных алгоритмов и методов, таких как:

- Методы основанные на оценки близости, которые основаны на оценке метрических расстояний между текущим и эталонным профилями пользователя.
- Метод опорных векторов (SVM), который находит оптимальную гиперплоскость, которая разделяет извлеченные признаки клавиатурного почерка пользователей.
- Нейронные сети, которые обучаются на извлеченных признаках клавиатурного почерка пользователя и выдают вектор вероятностей принадлежности пользователя к разным классам

Последние исследования, посвященные распознаванию пользователей по клавиатурному почерку, позволили обобщить данные об эффективности непрерывной аутентификации. Обобщенные данные приведены в Таблице 1. Данные получены и адаптированы из обзорных статей [20, 26] и адаптированы из обзорных статей [16,19, 21, 23, 25- 32].

Таблица 1 – Исследования динамической идентификации

Год	**Ссылка, автор**	**Параметр КП**	**Метод**	**Эффективность**
2005	[24] Gunetti	FT	Расстояние (R и A)	FAR-0.005%, FRR- 5%
2010	[30] Shimshon		Кластеризация	FAR 3,47% и FRR 0%
2011	[31] Messerman		Статистические, расстояние	FAR-2.02%, FRR-1.84%
2011	[35] Solami		Кластеризация	Точность 100%
2013	[26] Alsultan	дираф	Смешанная (Fusion)	FAR-21%, FRR- 17%
2014	[33] Ahmed	дираф	Нейронные сети	FAR-0.015%, FRR-4.82%
2015	[37] Antal	DT, FT	Статистические Метод опорных векторов Нейронные сети Дерево решений	93.04% Точность
2014	[38] Locklear		Статистические	EER 4,55-13,37%
2015	[39] Kang	DT, FT	Кластеризация, Расстояние	3.8% EER

Продолжение таблицы 1

2015	[40] Matsubara	дограф, DT	Расстояние	99% Точность
2016	[22] Morales	дограф, n-граф	k-NN ближайший сосед, Расстояние	90% Точность
2017	[30] Alsultan	дограф, DT	Метод опорных векторов	0.169 FAR, 0.423 FRR
2017	[27] Mondal Bours	дограф, DT	Расстояние	182 keystrokes
2017	[34] Goodkind	Contextual features	Наивный Байес	82.2% Точность
2017	[29] Ali		k-NN метод	EER 3,7%
2021	[32] Chang	DT, FT	CNN-GRU	Точность 99% EER 0,0690

Этап принятия решения **четвертый и заключительный этап** жизненного цикла клавиатурного распознавания. Этот этап заключается в том, что на основе результата этапа распознавания, то есть вектора вероятностей принадлежности пользователя, принимается окончательное решение о том, является ли пользователь подлинным или поддельным, эмоциональным или спокойным и т.д. Этот этап может быть реализован с помощью порогового решения (threshold decision), которое сравнивает вероятность принадлежности пользователя к определенному классу с заданным порогом и принимает решение в зависимости от того, больше или меньше вероятность порога.

1.5 Скрытый мониторинг и динамическое распознавание

Скрытый мониторинг по клавиатурному подчерку — это процесс анализа временных параметров нажатия клавиш пользователем для его

динамического распознавания (аутентификации и идентификации). Динамическое распознавание использует различные методы для сравнения текущего почерка пользователя с его эталоном для выдачи решения об аутентификации. Архитектура динамической (непрерывной) аутентификации (рисунок 8) включает в себя три подсистемы:

- Регистрация
- Аутентификация
- Адаптация

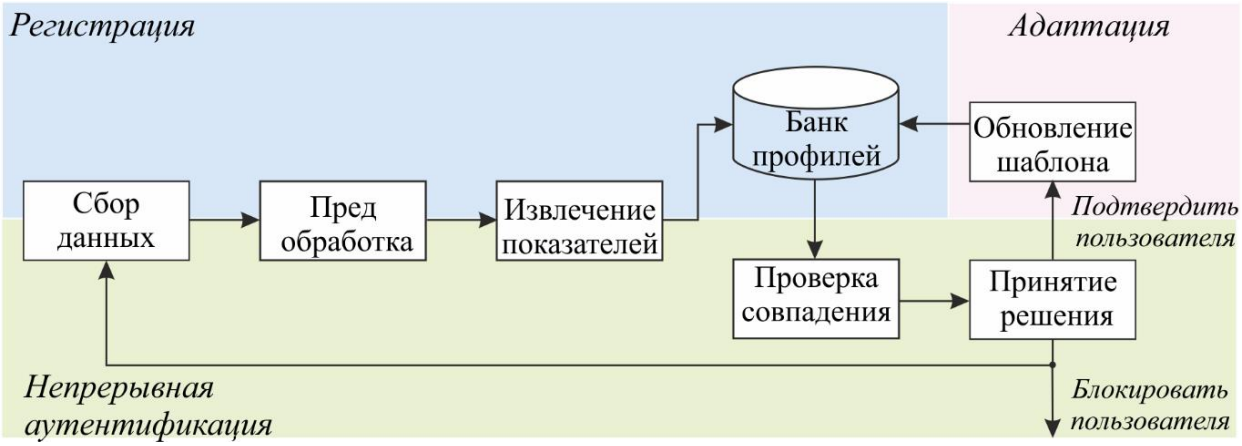

Рисунок 8 – Архитектура системы непрерывной аутентификации

Во время процесса регистрации происходит сбор данных о клавиатурных нажатиях, далее производится предобработка и извлечение показателей. Все эти действия ведут к пополнению банка профилей (шаблонов). Далее во время процесса непрерывной аутентификации происходит проверка совпадения шаблонов и принятие решения о допуске / отказе в допуске пользователю в систему. Обновление шаблона пользователя происходит при условии подтверждения его личности с последующим обновлением данных в банке профилей [1].

Для динамического распознавания пользователя необходимы следующие данные: временные характеристики набора текста, такие как скорость ввода, время удержания клавиши, интервалы между нажатиями и т.д.; эталонные образцы клавиатурного подчерка каждого пользователя

системы, которые были записаны ранее; алгоритмы распознавания, которые сравнивают введенный текст и его динамику с эталонными образцами и выдает решении об аутентификации пользователя.

Для проведения исследований по динамической аутентификации по клавиатурному почерку необходимы специальные наборы данных, содержащие информацию о скорости и ритме набора текста разными пользователями. Такие наборы данных можно получить двумя способами собрать их локально или скачать готовый датасет.

1.6 Оценки эффективности аутентификации

Для оценки эффективности системы аутентификации по клавиатурному подчерку используются различные показатели частоты ошибок.

Один из таких показателей – это False Rejection Rate (FRR), который означает оценку ложного отклонения или ошибку I рода. FRR определяет процент случаев, когда законный пользователь ошибочно отклоняется.

$$FRR = \frac{FR}{TA + FA + TR + FR} \quad (1)$$

Другой показатель – это False Acceptance Rate (FAR), который означает ошибку ложного принятия или ошибку II рода. FAR определяет процент случаев принятия нелегальных пользователей.

$$FAR = \frac{FA}{TA + FA + TR + FR} \quad (2)$$

В (1) и (2) приняты обозначения:

- True Accept (TA) – верный допуск в систему законного пользователя.

- True Reject (TR) – верный отказ в доступе незаконному пользователю.

- False Accept (FA) – ложный допуск незаконного пользователя.

- False Reject (FR) – ложный отказ в доступе законному пользователю.

Сумма вышеперечисленных показателей составляет общее количество попыток.

Гипотетически ошибки FRR и FAR варьируются в зависимости от уровня чувствительности алгоритма (порогового значения) и имеют противоположный характер: когда одна ошибка уменьшается, другая увеличивается.

Более высокие значения FAR обычно предпочтительнее в системах, где безопасность не имеет первостепенной важности, тогда как более высокие значения FRR являются предпочтительными в приложениях с высокой степенью защиты.

Еще один показатель – это Equal Error Rate (EER), который представляет значения ошибки, когда FAR и FRR принимают равные значения и не зависит от уровня чувствительности. ERR используется для определения общей точности системы распознавания.

Перечисленные показатели эффективности требуют дополнительного анализа при использовании в задачах аутентификации и идентификации пользователей. Принятия решения не может базироваться только на показателях FAR и FRR. Желательно иметь обобщенный пространственный показатель, дополненный пороговым значением (чувствительностью) и предельными значениями показателей.

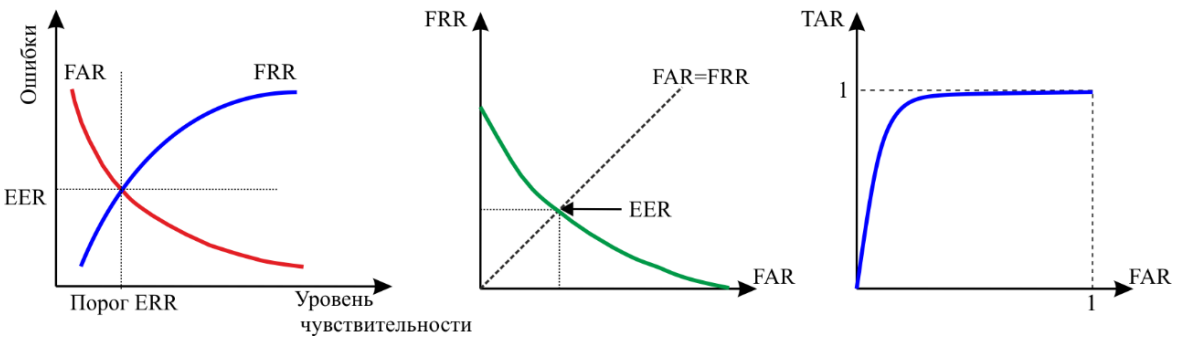

Рисунок 9 – Показатели эффективности клавиатурной аутентификации

2 ТЕХНОЛОГИИ КЛАВИАТУРНОЙ АУТЕНТИФИКАЦИИ

2.1 Этапы клавиатурной аутентификации

Этапы клавиатурной аутентификации - это процесс проверки подлинности пользователя по его способу набора текста на клавиатуре. Это один из видов биометрической аутентификации, которая основана на измерении уникальных физических или поведенческих характеристик человека.

Согласно некоторым источникам [2, 3], основные этапы клавиатурной аутентификации, следующие:

- Сбор информации о клавиатурных нажатиях пользователя во время ввода текста.
- Извлечение признаков клавиатурного почерка, таких как длительность нажатия и отпускания клавиш, интервалы между нажатиями и т.д.
- Сравнение признаков с заранее сохраненным шаблоном или эталоном для данного пользователя.
- Принятие решения об легитимности пользователя на основе выбранного алгоритма и порогового значения.

Некоторые системы также могут использовать дополнительные факторы, такие как частотность использования букв в текстах [3], географическое местоположение [2] или контекст ввода, для повышения точности и надежности распознавания.

2.2 Непрерывный сбор данных о клавиатурных нажатиях

Для достижения наилучших результатов при сборе данных необходимо осуществлять его в непрерывном режиме. Непрерывный сбор данных о клавиатурных нажатиях — это процесс отслеживания динамики набора текста пользователя в режиме реального времени для целей аутентификации. Это означает, что система не только проверяет пользователя при входе в систему, но и продолжает контролировать его поведение на клавиатуре в течение всей сессии его работы. Таким образом, система может обнаружить

и заблокировать несанкционированный доступ к компьютеру или приложению, если обнаружит аномалии в клавиатурном почерке пользователя.

Для непрерывного сбора данных о клавиатурных нажатиях необходимо использовать специальное программное обеспечение, которое может перехватывать и анализировать сигналы от клавиатуры. Такое ПО может быть установлено на компьютер пользователя или на удаленном сервере. В любом случае, ПО должно быть способно извлекать признаки клавиатурного почерка из любого введенного текста, независимо от его содержания и языка.

Непрерывный сбор данных о клавиатурных нажатиях имеет ряд преимуществ перед статической аутентификацией по паролю или одноразовому коду. Во-первых, он повышает уровень безопасности, так как затрудняет подбор или кражу пароля. Во-вторых, он повышает удобство использования, так как не требует от пользователя запоминать или вводить дополнительные данные для аутентификации. В-третьих, он повышает эффективность работы, так как не прерывает процесс ввода текста и не отвлекает пользователя от основной задачи [2].

2.3 Актуализация динамических наборов данных

Актуализация динамических наборов — это процесс обновления и коррекции эталонных шаблонов пользователей на основе их текущего поведения на клавиатуре. Это необходимо для повышения точности и надежности системы аутентификации по клавиатурному почерку, которая отслеживает динамику нажатия клавиш в режиме реального времени [3].

Актуализация динамических наборов позволяет учитывать изменения в клавиатурном почерке, вызванные различными факторами, такими как усталость, стресс, эмоции, здоровье и т.д. [4]. Для актуализации динамических наборов данных необходимо использовать специальные алгоритмы, которые могут определять степень сходства между текущим и

эталонным образцом клавиатурного почерка и вносить необходимые коррективы в шаблон [3, 4].

2.4 Данные для эксперимента

В качестве данных выступают наборы данных о клавиатурных нажатиях. Большинство исследований в научной среде использует готовые наборы данных.

В данном исследовании будут использованы данные, собранные для статьи [10] автором Nahuel Gonzalez.

Набор данных содержит CSV-файлы с характеристиками времени (время удержания и паузы) каждого нажатия клавиш в наборах свободного текста. Двадцать испытуемых выполнили сопоставимые задания на транскрипцию и свободное сочинение; реализованы два классификатора динамики нажатий клавиш; Каждый классификатор оценивался с использованием образцов как свободного состава, так и образцов транскрипции [10]. Нажатия клавиш были сгруппированы для каждого пользователя независимо от их сеансов. Таким образом, для каждого набора данных, пользователя, задачи, кода виртуальной клавиши и функции был создан профиль, состоящий из набора временных значений. Имена файлов указаны с использованием следующего соглашения: DATASET-TASK-USER-FEATURE-VK и организованы в папки в соответствии с их набором данных и задачей. Поскольку количество файлов превышает сто тысяч, они упаковываются в DISTRIBUTIONS.zip файл. Для иллюстрации соглашения об именовании добавлены пять файлов, которые также входят в комплект поставки. Например, KM-transcribed-USERs019-FT-VK32.csv содержит временные наблюдения за временем полета (FT) клавиши пробела (VK32, код виртуальной клавиши 32) при нажатии пользователем s019 в наборе данных KM, когда он выполняет задачу транскрипции.

В процессе сбора данных были получены данные о клавиатурных нажатиях по одной сессии для каждого из двадцати пользователей. Поскольку в дистрибутиве не предусмотрено разделение на сессии для одного пользователя, мы предположили, что каждый пользователь имеет только одну сессию. Ввиду малого количества данных, было принято решение смоделировать сессии полученных пользователей.

Для моделирования сессий было использовано десктопное приложение. При этом нужно учитывать, что полученные при моделировании выборки из одной генеральной совокупности с близким математическим ожиданием и средним квадратичным отклонением.

Моделирование сессий реальных пользователей было выполнено из расчета по 10 сессий на пользователя, каждая сессия содержит в себе 1000 символов. Диаграмма разброса значений сгенерированных сессий для пользователя user19 изображена на рисунке 10.

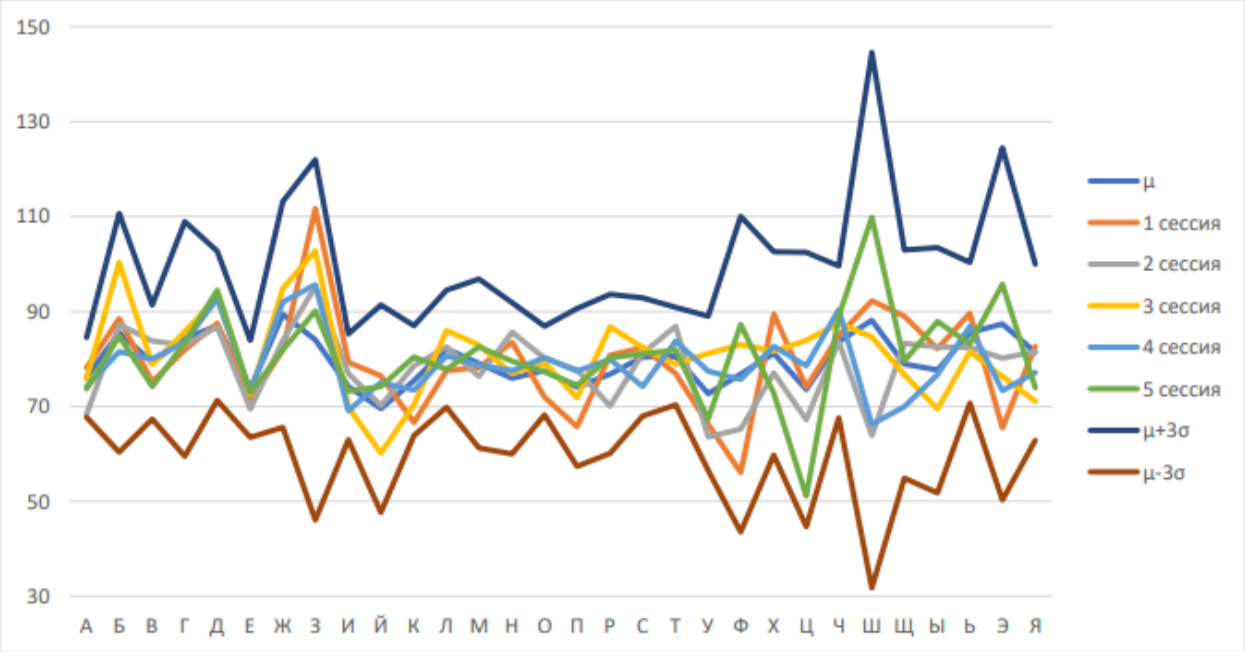

Рисунок 10 – Сгенерированные сессии

Собранные и смоделированные данные сохраняются в формате txt и имеют следующий вид рисунок 11.

Рисунок 11 – Данные формате txt

2.5 Формирование временного показателя

Формирование временного показателя клавиатурного подчерка — это процесс извлечения и анализа характеристик, связанных с длительностью и интервалами нажатия и отпускания клавиш при вводе текста. Эти характеристики отражают индивидуальный стиль и ритм набора пользователя, который может быть использован для его идентификации или аутентификации [3]. Формирование временного показателя клавиатурного подчерка требует специального программного обеспечения, которое может перехватывать сигналы от клавиатуры и измерять время между ними. Затем эти данные подвергаются статистическому анализу для выделения признаков, которые могут отличать одного пользователя от другого [5]. Формирование временного показателя клавиатурного подчерка имеет ряд преимуществ перед другими биометрическими методами, такими как отпечатки пальцев, распознавание лица или голоса. Во-первых, он не требует дополнительного оборудования, кроме обычной клавиатуры. Во-вторых, он не нарушает приватность пользователя, так как не собирает его личные данные. В-третьих, он является ненавязчивым и незаметным для пользователя, так как не требует от него специальных действий или поз [5].

В работе для повышения качества временных характеристик, была использована частотность букв английского алфавита. Использование

частотности позволяет оптимизировать алгоритм из-за нормирования значения отдельной буквы в шаблоне пользователя. Частотность английского алфавита изображена на рисанках.12 и 13

Рисунок 12 – Диаграмма частотность букв английского алфавита

Рисунок 13 – Диаграмма частотность букв английского алфавита, отсортированная по частоте использования

Как видно из рисунка, некоторые буквы используются пользователями довольно часто, некоторые же очень редко – менее 2%. В ходе исследования

было принято решение не использовать буквы чья частотность ниже 1%, этими буквами являются J, Q, V, Z.

2.6 Создание шаблонов пользователей

Создание шаблонов клавиатурного подчерка пользователей — это процесс формирования эталонных образцов, которые отражают индивидуальные особенности набора текста на клавиатуре. Эти образцы могут быть использованы для идентификации или аутентификации пользователей по их клавиатурному почерку. Создание шаблонов клавиатурного подчерка пользователей требует сбора и обработки данных о временных характеристиках нажатия и отпускания клавиш, а также о частотности использования букв в текстах [5]. Создание шаблонов клавиатурного подчерка пользователей имеет ряд преимуществ перед другими методами аутентификации, такими как пароли, отпечатки пальцев или распознавание лица. Во-первых, оно усиливает защиту паролей, так как добавляет дополнительный фактор аутентификации. Во-вторых, оно упрощает процесс аутентификации, так как не требует от пользователя запоминания сложных комбинаций. В-третьих, оно повышает удобство использования системы, так как не требует от пользователя ввода пароля каждый раз при доступе к ресурсам [3].

2.7 Алгоритмы и методы распознавания

Одни и те же методы применяется для динамической и статической аутентификации. Разделение методов распознавания на классы достаточно условно, но можно выделить методы машинного обучения, статистические методы и основанные на оценке метрических расстояний.

В работе были использованы следующие методы:

1. Метод на основе Евклидового расстояния. Это расстояние между двумя точками в евклидовом пространстве. Евклидово расстояние

вычисляется по теореме Пифагора, то есть как корень из суммы квадратов разностей координат точек

$$\rho(x, y) = \sqrt{\sum_{i}^{n} (x_i - y_i)^2} \quad (1)$$

2. Метод на основе городских кварталов (манхэттенское расстояние). Это расстояния между двумя точками в N-мерном векторном пространстве, которая равна сумме модулей разностей их координат.

$$\rho(x, y) = \sum_{i}^{n} | x_i - y_i | \quad (2)$$

3. Метод опорных векторов (SVM) – это метод машинного обучения, который используется для задач классификации и регрессии. Основная идея метода найти такую гиперплоскость в пространстве признаков, которая максимально разделяет объекты разных классов. Для этого метод опирается на некоторые объекты, называемые опорными векторами, которые лежат ближе всего к границе разделения. Для клавиатурного распознавания SVM может использоваться для классификации пользователей по их нажатиям клавиш на клавиатуре. Для этого необходимо собрать обучающую выборку, состоящую из набора признаков, описывающее каждое нажатие клавиши пользователем. Затем на основе этой выборки можно обучить SVM-классификатор, который будет классифицировать пользователей по их клавиатурному почерку.

3 ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СИСТЕМЫ

3.1 Функциональные возможности

Функциональными возможностями системы является способность проверять подлинность пользователя по его индивидуальному стилю набора текста. Для этого система анализирует различные параметры клавиатурного подчерка с помощью которых формирует вектор биометрических характеристик, которые сравнивается с эталонными образцами пользователей и принимает решение в зависимости от выбранного алгоритма распознавания.

3.2 Анализ и выбор инструментов

Для разработки веб-приложения были использованы следующие технологии и инструменты:

- Языки программирования: для клиентской части веб-приложения были использованы HTML и CSS, а для серверной части Python и Django. HTML определяет структуру и содержание страницы, CSS задает стили и оформление элементов. Python – это высокоуровневый язык программирования, который позволяет писать чистый и эффективный код. Django – это многофункциональный фреймворк для веб-разработки на Python, который предоставляет все необходимые инструменты для создания веб-приложения.
- Фреймворки и библиотеки: для упрощения и ускорения разработки веб-приложения были использованы разные фреймворки и библиотеки. Например, я использую Django для создания полноценного веб-сервера, sckit-learn для реализации различных алгоритмов машинного обучения, json для работы с данными и т.д.
- Инструменты разработки: для написания и отладки кода была использована интегрированная среда разработки PyCharm,

которая имеет множество полезных функций и расширений для работы с Python. Для контроля версий кода была использована система Git, которая позволяет отслеживать изменения, синхронизировать код с удаленным репозиторием на GitHub и сотрудничать с другими разработчиками

3.1 Архитектура приложения

Диаграмма классов приложения изображена на рисунке 14

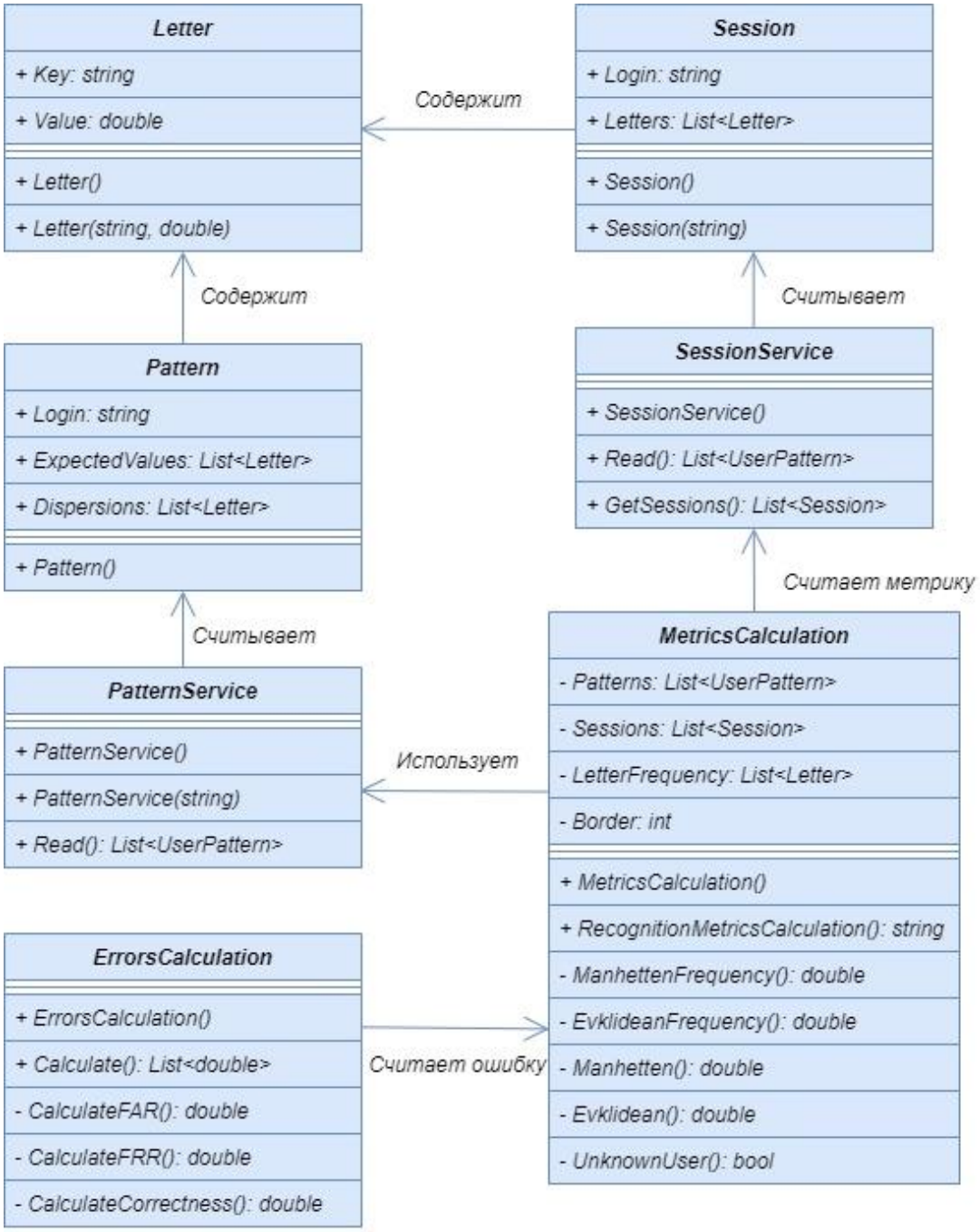

Рисунок 14 – Диаграмма классов приложения

Целью класса PatternService является извлечение шаблонов сессий из хранилища данных. Объекты класса Pattern представляют собой записи шаблонов сессий.

Класс SessionService отвечает за получение сессий из хранилища данных. Объекты класса Session содержат данные о сессиях.

Класс Letter описывает букву, которую нажал пользователь, и время удержания клавиши.

Класс MetricsCalculation решает задачу идентификации путем вычисления различных методов.

Класс ErrorsCalculation вычисляет ошибки методов.

На рисунке 15 представлена диаграмма использования веб-приложения.

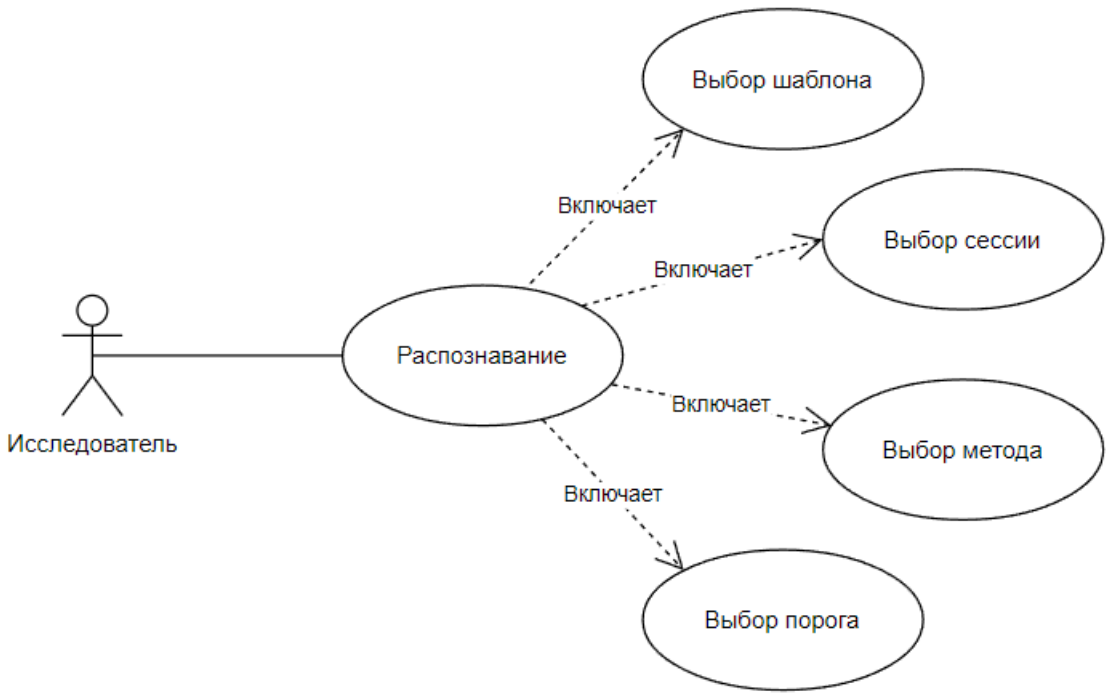

Рисунок 15 – Диаграмма использования

Пользователем веб-приложения является исследователь по клавиатурному распознаванию, он может использовать прецедент распознавание, которое включает выбор шаблона, сессии, метода, а также пороговое значение распознавания.

На следующем рисунке 16 представлена диаграмма деятельности для процесса распознавания. Исследователь выбирает файл с шаблонами пользователей и файл, содержащий сессии, далее он (исследователь) задает параметры распознавания такие как номер сессии для распознавания, значение порога и выбирает один из предложенных методов распознавания (Евклидово расстояние, Манхэттенское расстояние, Метод опорных векторов, евклидово или Манхэттенское расстояние с влиянием частотности букв). После всех, вышеперечисленных, действий пользователь системы получает результат идентификации выбранной сессии.

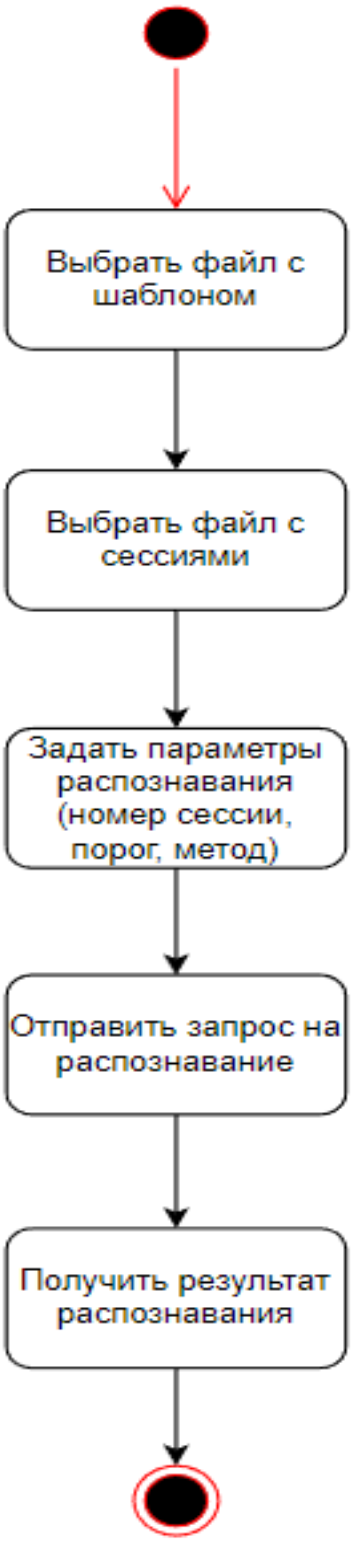

Рисунок 16 – Диаграмма деятельности

3.3 Интерфейс приложения

Приложение представлено в виде двух веб-страниц рисунок 17

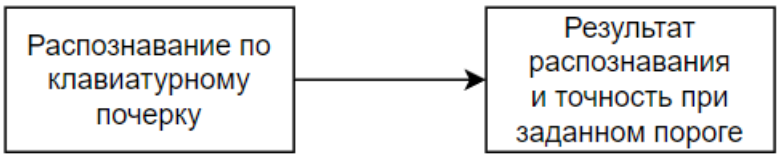

Рисунок 17 – Структура приложения

На рисунке 18 представлена веб-форма для заполнения параметров распознавания

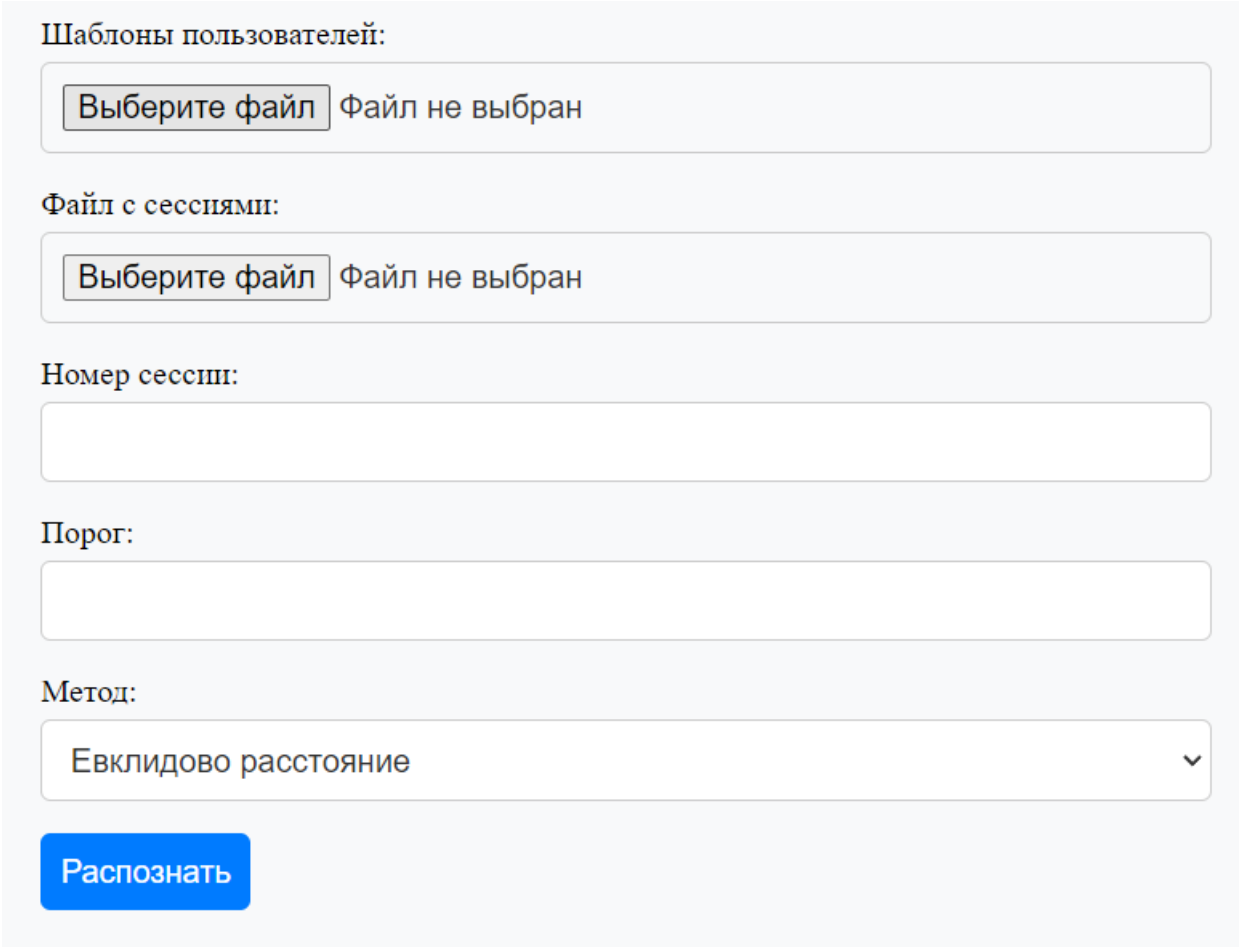

Рисунок 18 – Веб-форма для распознавания

Веб-форма в своем составе имеет:

1. Два поля ввода типа file для выбора файлов шаблонов пользователей и файл со сессиями пользователей.

2. Поле с номером сессии для распознавания

3. Поле для установки порога распознавания

4. Поле списка с методами для распознавания пользователя

Для начала процесса распознавания пользователю необходимо заполнить все поля формы перед нажатием кнопки «Распознать».

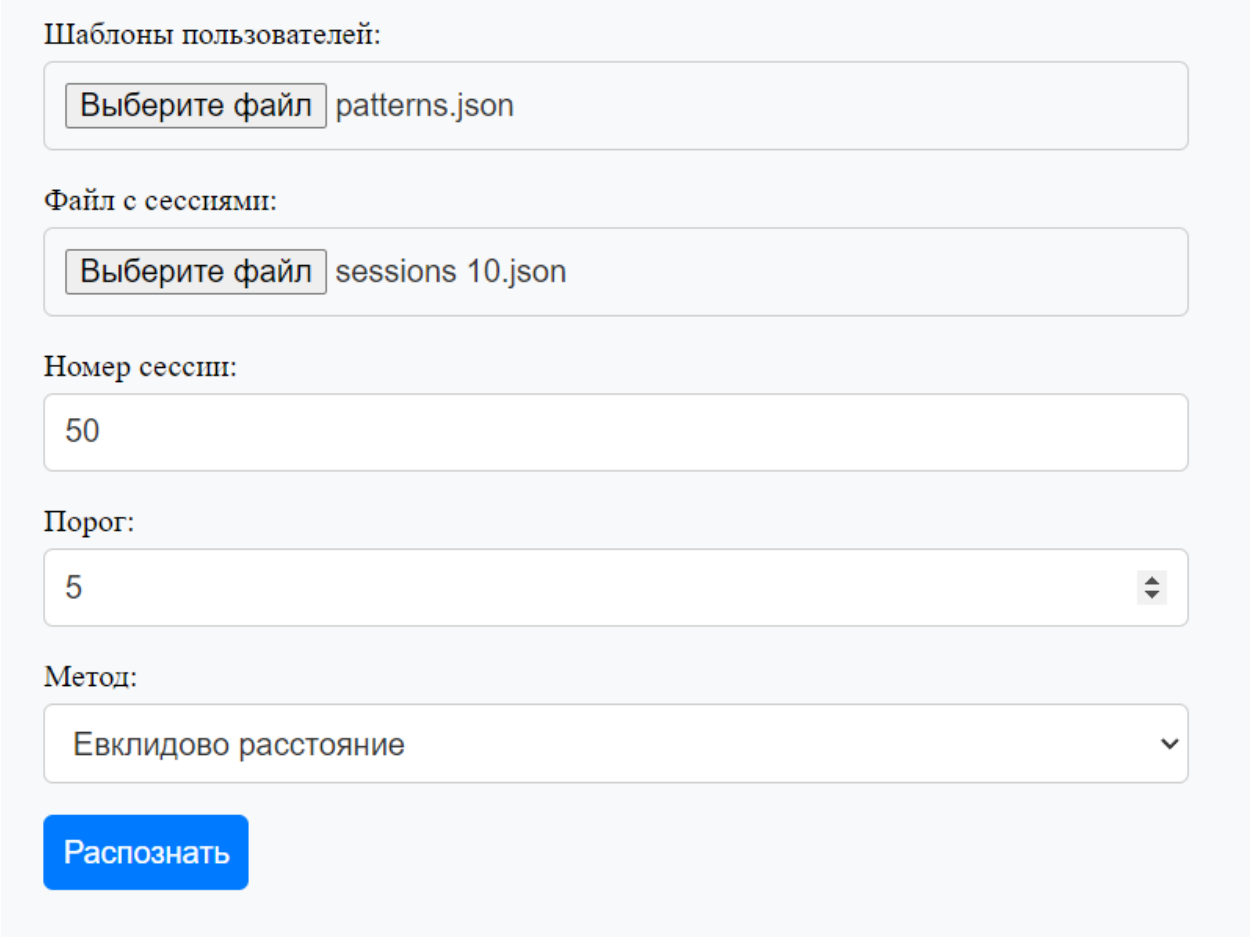

Рисунок 19 – Заполнение полей для начала процесса распознавания

Результат распознавания сессии номер 50, а также точность методов представлен на рисунке 20

Системой идентифицирован пользователь User27

Точность алгоритма

Метод	TAR	FAR	FRR	TRR
Евклидово расстояние	97	25	44	34
Манхэттенское расстояние	93	29	48	30
Евклидово расстояние + частотность	41	81	26	52
Манхэттенское расстояние + частотность	44	78	23	55
Метод опорных векторов	97	25	44	34

Рисунок 20 – Результат и точность методов распознавания

4 РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

Цикл непрерывной аутентификации пользователя состоит из двух основных этапов: регистрации данных и аутентификации личности. На первом этапе происходит постоянный сбор и анализ данных о клавиатурных нажатиях пользователя, на основе которых извлекаются характеристики его клавиатурной динамики.

Шаблоны пользователей являются динамическими, то есть адаптируются к изменениям в клавиатурном почерке пользователя, вызванным разными факторами, такими как психоэмоциональное состояние, усталость и т.д. Шаблоны формируются на основе случайных нажатий на клавиатуру во время работы с любыми приложениями операционной системы. Для проведения исследования был выбран датасет о клавиатурных нажатиях на английском языке КМ.

Следующим этапом система вычисляет среднее время удержания клавиши в текущем сеансе для каждой буквы и обновляет соответствующий шаблон в базе данных. Это позволяет повысить точность идентификации.

На рисунке 21 представлены визуальные отображения шаблонов пользователей банка данных КМ. По горизонтальной оси указаны буквы английского алфавита, по вертикали – время удержания клавиши в миллисекундах. Из рисунка видно, что шаблоны пользователей имеют различия

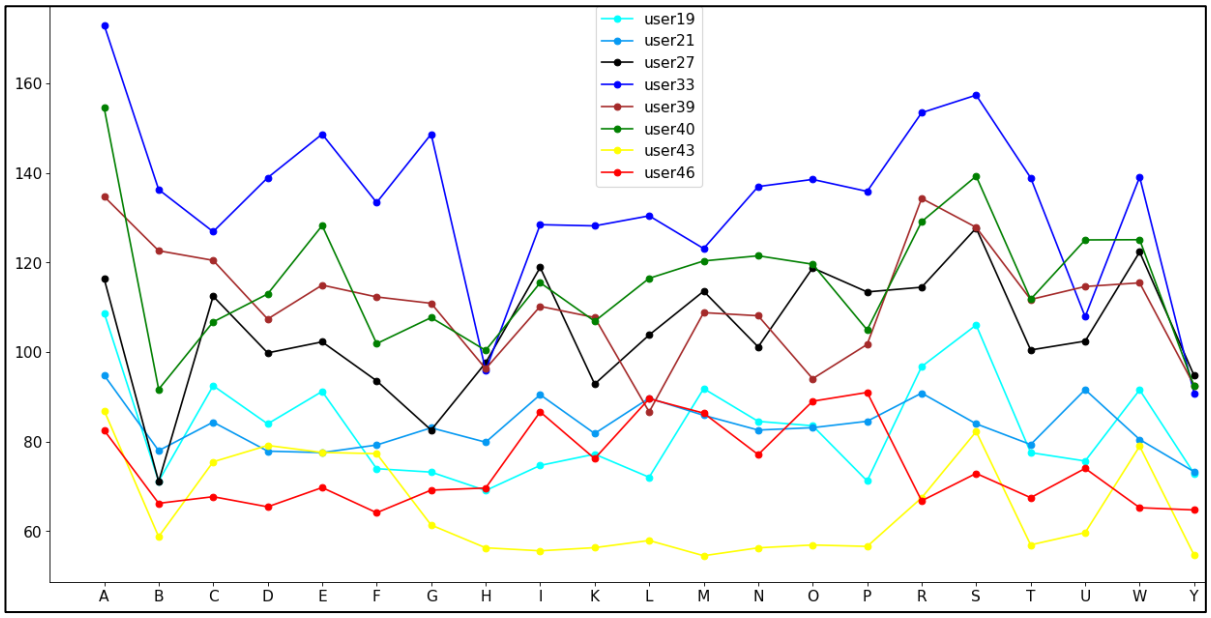

Рисунок 21 – Клавиатурные шаблоны датасета KM

Из рисунка следует, что каждый шаблон уникален, это происходит из-за различия скорости и ритма набора текста разными пользователями. Рисунок 22 показывает плотности распределения времени удержания клавиши

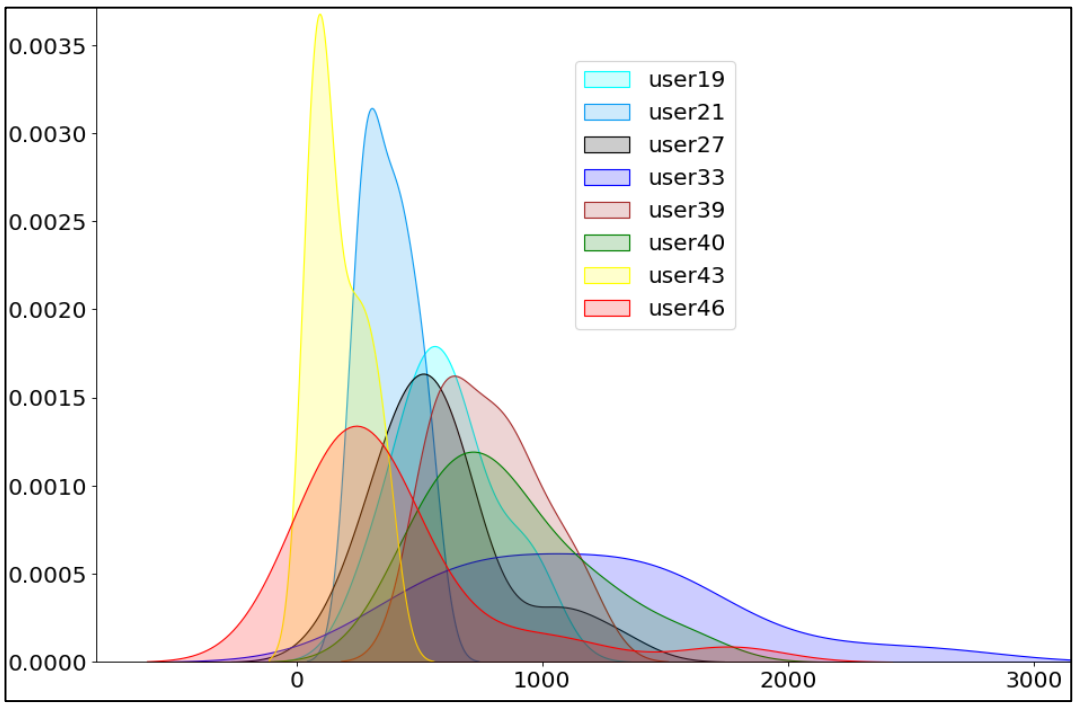

Рисунок 22 – Плотности распределения ВУКов пользователей

Анализ рисунка показывает различия в скорости и качестве набора текста у пользователей. User43 и User46 набирают текст быстрее всех (желтая и красная линии), но у User46 более равномерное время удержании клавиш для разных букв, что свидетельствует о лучших навыках работы с клавиатурой. User33 набирает медленнее всех (синяя линия) и имеет большой разброс времени удержания, что указывает на слабые навыки набора текста. Статический анализ также может выделить гендерные различия и психоэмоциональную нестабильность пользователя.

Для подтверждения легитимности пользователя системы сравниваются его текущий и сохраненный в базе данных шаблоны. Возможны два варианта:

- Шаблоны совпадают
- Шаблоны не совпадают

В этом исследовании для анализа совпадения шаблонов использовались метод опорных векторов (SVM) и Евклидова и Манхэттенская метрики расстояний.

В любом методе важно выбрать порог принятия решения в зависимости от поставленных задач. Низкий порог означает малую разницу между шаблонами и сложный доступ в систему. Высокий порог означает большую разницу между шаблонами и простой доступ в систему. На рисунке 23 показываются визуальные инструменты ошибок первого и второго рода для Манхэттенской метрики.

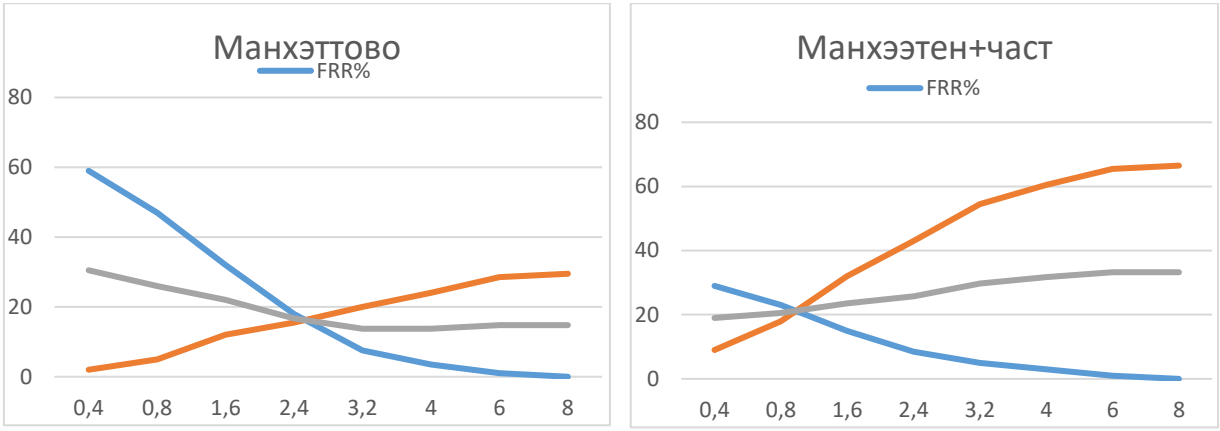

Рисунок 23 – Оценка эффективности распознавания пользователей

Как видно из рисунка, достигнуто уменьшение порогового значения примерно в 3 раза с 2,4 мс до 0,8 мс при незначительном увеличении ошибки.

В таблице 2 сведены результаты исследования по методам распознавания

Таблица 2 - Результаты исследования по методам

	расстояние				метод
	Евклидово		Манхэттенское		SVM
	частотность		частотность		
	-	+	-	+	
ERR, (0-100) %	12,25	21	16,75	20,5	14,75
порог (FAR=FRR), мс	2,5	0,9	2,6	0,8	2,3
Accuracy, (0-100) %	86,3	80,32	82,08	89,47	88,3
Precision, (0-1)	0,64	0,47	0,58	0,57	0,64
Recall, (0-1)	0,73	0,16	0,69	0,2	0,73

Сравнительный анализ показал, что показатели, полученные на основе Манхэттенской и Евклидовой метрик идентичные. Метод опорных векторов показал результат 14,75 % ERR при пороговом значении 2,3 мс.

Для распознавания легитимных пользователей и шпионов используется матрица соответствия ошибок, представленная в таблице 3. В ней отражены четыре возможных исхода распознавания:

– Верный допуск (TA)
– Верный отказ (TR)

– Ложный допуск (FA)

– Ложный отказ (FR)

Таблица 3 - Матрица соответствия ошибок

		Пользователь при распознавании	
		законный	**законный**
Фактический пользователь	**законный**	TA	FR
	незаконный	FA	TR

На основе этой матрицы можно вычислить следующие показатели качества распознавания:

– Accuracy – доля верных решений по всем пользователям

$$Accuracy = \frac{TA+TR}{TA+TR+FA+FR}. \quad (3)$$

– Precision – доля легитимных пользователей среди всех допущенных

$$Precision = \frac{TA}{TA+FA}. \quad (4)$$

– Recall – доля допущенных пользователей среди всех легитимных

$$Recall = \frac{TA}{TA+FR}. \quad (5)$$

Все три показателя отражают точность аутентификации «своего» пользователя, но с разными акцентами. Accuracy показывает общую точность верных допусков и отказов. Precision показывает, как часто система пропускает шпионов. Recall показывает, как часто система отказывает легитимным пользователям.

В данном исследовании для сравнения шаблонов пользователя были использованы метрические расстояния (Евклидово и Манхэттенское) и метод опорных векторов. Для оценки визуализации качества классификации распознавания были построены ROC и DET на рисунках 24 и 25.

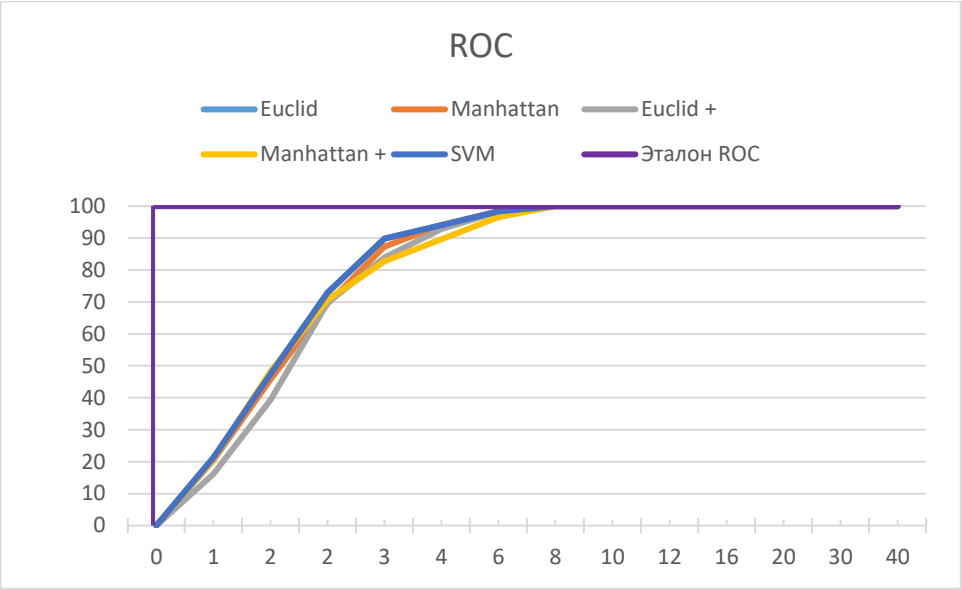

Рисунок 24 – График ROC

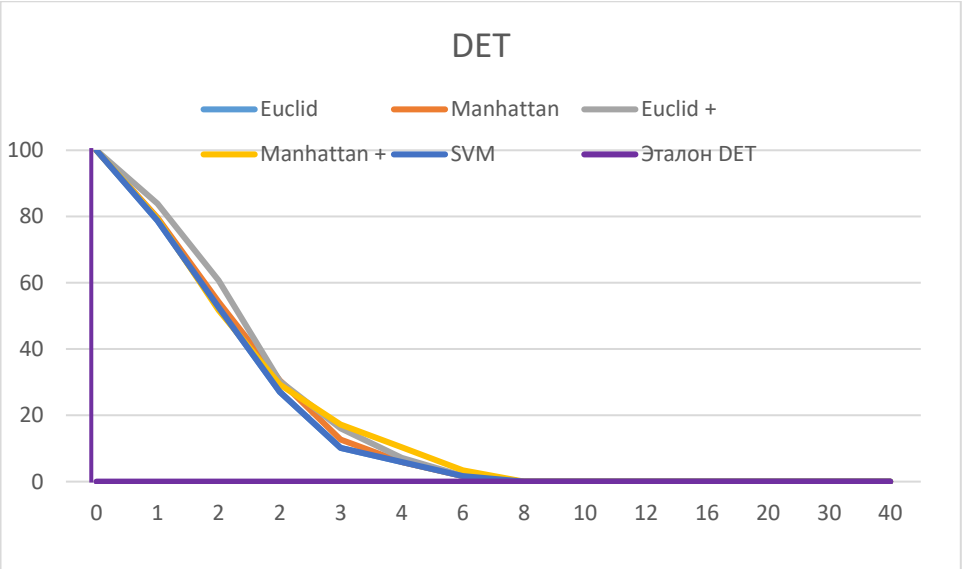

Рисунок 25 – График DET

На графике ROC видно, что метод опорных векторов имеет большую площадь по кривой (AUC), чем остальные алгоритмы, что означает что он лучше разделяет пользователей в отличие от остальных алгоритмов. На графике DET видно, что манхэттенское расстояние с поправкой на частотность имеет меньшую частоту ошибок обнаружения и пропуска при средних порогах классификации, чем остальные, что означает что он более точен и надежен.

Кроме того, для каждого метода аутентификации была создана таблица в Excel с результатами расчетов программы. На основе этих таблиц были построены графики зависимости ошибок FAR, FRR, ERR.

Результаты расчетов показали, что наименьшее значении Equal Error Rate имеет Евклидово расстояние, которое равно 12,25%. Следующим по возрастанию ERR – метод опорных векторов (SVM) со значением 14,75%. Затем идут Манхэттенское расстояние, Манхэттенское расстояние и Евклидово расстояние с поправкой на частотность букв английского алфавита 16,75%, 20,5% и 21% соответственно.

В ходе исследования выяснилось, что учет частотности букв английского языка значительно уменьшает время допуска путем повышения чувствительности в три раза, в ущерб точности распознавания в районе 5%. Допустимые значения ошибок первого и второго рода, а также значения ERR необходимо подбирать в зависимости от конкретной прикладной задачи.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ВМ11	Очиров Жаргал Александрович

Школа	ИШИТР	Отделение школы (НОЦ)	ОИТ
Уровень образования	Магистр	Направление/специальность	09.04.01 «Информатика и вычислительная техника»

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	Стоимость ресурсов определялась по средней рыночной стоимости, в соответствии с окладами сотрудников организации.
2. *Нормы и нормативы расходования ресурсов*	Тариф электроэнергии 2,73 руб. за кВт/ч Районный коэффициент 30%
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	Коэффициент отчислений на уплату во внебюджетные фонды 30%
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого и инновационного потенциала НТИ*	Провести предпроектный анализ
2. *Разработка устава научно-технического проекта*	Представить Устав научного проекта магистерской работы
3. *Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок*	Разработать план управления НТИ
4. *Определение ресурсной, финансовой, экономической эффективности*	Рассчитать сравнительную эффективность исследования
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. *Матрица сегментации рынка* 2. *Оценка конкурентоспособности технических решений* 3. *Матрица SWOT* 4. *График проведения и бюджет НТИ* 5. *Оценка ресурсной, финансовой и экономической эффективности НТИ* 6. *Потенциальные риски*	

Дата выдачи задания для раздела по линейному графику	01.03.2023 г.

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент ОСГН, ШБИП	Былкова Т.В.	к.э.н		01.03.2023 г.

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ11	Очиров Жаргал Александрович		01.03.2023 г.

5 ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ

Система аутентификации и идентификации на основе динамических характеристик клавиатурного подчерка предназначена для улучшения безопасности. Целевым рынком для системы являются предприятия и компании, которые хотят улучшить безопасность своих систем аутентификации. В качестве таких предприятий могут выступать банки, государственные учреждения, медицинские учреждения и другие организации, которые работают с конфиденциальной информацией.

Таким, образом целью раздела «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение» является определение перспективности и успешности научно-исследовательского проекта, разработка механизма управления и сопровождения конкретных проектных решений на этапе реализации.

Чтобы достичь поставленной цели необходимо решить задачи по организации работы над проектным решением, по планированию этапов разработки, оценить перспективность и коммерческий потенциал проекта, рассчитать бюджет, необходимый для реализации проекта, оценить социальную и экономическую эффективность проекта.

5.1 Оценка коммерческого и инновационного потенциала НТИ

5.1.1 Потенциальные потребители результатов исследования

Для системы аутентификации и идентификации на основе динамических характеристик клавиатурного подчерка возможны следующие варианты сегментации рынка:

- По размеру и сфере деятельности компаний. Этот критерий позволяет выделить те компании, которые имеют большое количество сотрудников, работающих с компьютерами, и которые заинтересованы в повышении безопасности своих систем и данных. Например, это могут быть банки, страховые компании, государственные учреждения и т.д.

- По уровню осведомленности и заинтересованности в системе. Этот критерий позволяет выделить те компании, которые уже знают о существовании такой системы и ее преимуществах, и которые готовы к ее внедрению или тестированию. Например, это могут быть инновационные компании, работающие в области информационных технологий или кибербезопасности.
- По готовности к оплате за систему. Этот критерий позволяет выделить те компании, которые имеют достаточный бюджет для приобретения или аренды системы, и которые видят в ней ценность для своего бизнеса. Например, это могут быть крупные или средние компании с высоким уровнем дохода или прибыли.

Таблица 4 – Матрица сегментации рынка

Сегмент	Размер и сфера деятельности	Уровень осведомленности и заинтересованности	Готовность к оплате
1	Банки, страховые компании, государственные учреждения	Высокий	Высокая
2	Инновационные компании в области IT или кибербезопасности	Высокий	Средняя
3	Малые и средние предприятия разных отраслей	Средний	Низкая
4	Частные лица, интересующиеся технологиями	Низкий	Низкая

В данном случае, наиболее прибыльным сегментом является первый, так как он имеет большой объем рынка, высокий уровень осведомленности и заинтересованности в системе аутентификации по клавиатурному подчерку и высокую готовность к оплате за нее.

5.1.2 Анализ конкурентных технических решений

Для оценки конкурентоспособности разработки проводится анализ существующих решений, по аутентификации с помощью клавиатурного подчерка. Для сравнительного анализа были выбраны:

1. Plurilock – это система аутентификации по клавиатурному подчерку, которая также использует другие поведенческие биометрические сигналы, такие как движение мыши, для создания сложного профиля пользователя. Она работает в фоновом режиме и не требует никакого дополнительного оборудования или действий пользователя
2. Bio-Sig-ID – это система аутентификации по клавиатурному подчерку, которая не требует никакого дополнительного оборудования или загрузки программ. Она аутентифицирует пользователя по его уникальным жестам, которые он совершает при вводе пароля.

Сравнение технических и экономических характеристик этих продуктов представлено в таблице 5. «Plurilock» обозначен К1, а «Bio-Sig-ID» - К2.

Таблица 5 – Анализ конкурентных технических решений

Критерий оценки	**Вес критерия**	**Баллы**			**Конкурентно-способность**		
		$Б_ф$	$Б_{к1}$	$Б_{к2}$	$К_ф$	$К_{к1}$	$К_{к2}$
Технические критерии оценки ресурсоэффективности							
• Удобство в эксплуатации	0,18	4	3	5	0,72	0,54	0,9
• Возможность подключения в сеть ЭВМ	0,11	4	1	5	0,44	0,11	0,55
• Потребность в ресурсах	0,27	5	5	2	1,35	1,35	0,54
• Функциональные возможности	0,25	3	2	3	0,75	0,5	0,75
• Быстродействие	0,1	5	5	4	0,5	0,5	0,4
• Возможность доработки	0,06	5	3	4	0,3	0,18	0,24
• Обслуживание после продажи	0,02	3	1	5	0,06	0,02	0,1
• Предполагаемый срок эксплуатации	0,01	5	3	4	0,05	0,03	0,04
Итого	**1**	**34**	**23**	**32**	**4,17**	**3,23**	**3,52**

Таким образом, разрабатываемая система имеет ряд преимуществ перед аналогами по следующим критериям:

1) Потребность в ресурсах памяти;
2) Быстродействие;
3) Предполагаемый срок эксплуатации;

4) Возможность подключения в сеть ЭКМ;
5) Удобство в эксплуатации.

Недостатками системы являются:

1) Функциональные возможности;
2) Послепродажное обслуживание.

В результате анализа было установлено, что система является более конкурентноспособной, чем К1 и К2. Следовательно, более целесообразно проводить дальнейшую разработку.

5.1.3 SWOT анализ

Матрица SWOT-анализа представлена в таблице 6.

Таблица 6 – Итоговая матрица SWOT-анализа

	Сильные стороны научно-исследовательского проекта: С1. Простота эксплуатации С2. Низкая стоимость разработки С3. Централизованное хранение данных С4. Низкие требования к аппаратно-программному обеспечению С5. Удобный интерфейс	**Слабые стороны научно-исследовательского проекта:** Сл1. Невысокая точность алгоритма распознавания клавиатурного почерка Сл2. Отсутствие кроссплатформенности Сл3. Длительная разработка
Возможности: В1. Реализация новых функций В2. Повышение отказоустойчивости программы В3. Увеличение спроса на продукт В4. Расширение команды разработчиков для ускорения реализации и поддержки продукта	1. В1С2С3 – Простота расширения функционала системы. 2. В2С2С3С4 – Простота изменения каналов связи. 3. В3С1С3С4С5 – Широкие возможности увеличения спроса за счет сильных сторон научно-исследовательского проекта. 4. В4С2 – Ускорение разработки.	1. В1Сл1Сл3 – Необходимость доработки и оптимизации алгоритма. 2. В2Сл3 – Модификация приложения требует времени. 3. В4Сл1Сл3 – Новые разработчики должны сначала исследовать существующий код и алгоритм.

Продолжение таблицы 6

Угрозы: У1. Увеличение конкуренции У2. Прекращение поддержки руководителей проекта У3. Отсутствие интереса к продукту на рынке	1. У3С2 – При выходе на рынок необходимо обеспечить мониторинг поведения потребителей, с целью совершенствования ценовой политики	1. У1Сл1Сл2Сл3 – Необходимо разработать ПО сходного функционала более быстро и качественно. 2. У3Сл1Сл2 – Необходимо улучшить точность алгоритмов распознавания, а также разработать приложение для других платформ.

5.1.4 Оценка готовности проекта коммерциализации

Для оценки готовности проекта были определены показатели по вопросам в таблице 9. Оценка проводится по пятибалльной шкале. При оценке научного проекта: 1 балл – не проработано, 2 балла – проработка слабая, 3 балла – выполнено, качество посредственное, 4 балла – удовлетворительное качество, 5 баллов – качество подтверждено сторонним специалистом. При оценке знаний разработчика: 1 балл – не знаю, 2 балла – только теоретические знания, 3 балла – теоретические знания с практическими примерами, 4 балла – умею, практикую, 5 баллов – могу консультировать по вопросу.

Таблица 7 – Таблица оценки готовности научного проекта к коммерциализации

№ п/п	Наименование	Степень проработанности научного проекта	Уровень имеющихся знаний у разработчика
1	Определён имеющийся научно-технический задел	4	4
2	Определены перспективные направления коммерциализации научно-технического задела	3	3
3	Определены отрасли и технологии (товары, услуги) для представления на рынок	4	5
4	Определена товарная форма научно-технического задела для представления на рынок	2	2

Продолжение таблицы 7

5	Определены авторы и осуществлена охрана их прав	3	3
6	Проведена оценка стоимости интеллектуальной собственности	3	3
7	Проведены маркетинговые исследования рынков сбыта	3	3
8	Разработан бизнес-план коммерциализации научной разработки	3	3
9	Определены пути продвижения научной разработки на рынок	2	2
10	Разработана стратегия реализации научной разработки	4	4
11	Проработаны вопросы международного сотрудничества и выхода на зарубежный рынок	2	2
12	Проработаны вопросы использования инфраструктуры поддержки, получения льгот	1	1
13	Проработаны вопросы финансирования коммерциализации научной разработки	2	3
14	Имеется команда для коммерциализации научной разработки	3	3
15	Проработан механизм реализации научной разработки	4	4
ИТОГО		43	45

Таким образом, готовность научного проекта к коммерциализации средняя. Уровень имеющихся знаний у разработчика немного выше, но также находится в категории выше среднего. В дальнейшем необходимо проработать международного сотрудничества и выхода на зарубежный рынок, вопросы использования инфраструктуры поддержки и получения льгот, вопросы финансирования коммерциализации научной разработки.

5.2 Инициация проекта

Устав проекта:

1. Цели и результаты проекта

Были определены заинтересованные стороны (таблица 5). Заинтересованные стороны – это лица или организации, которые активно заинтересованы и/или могут быть как положительно, так и отрицательно затронуты в результате проекта.

Таблица 8 – Заинтересованные в проекте стороны

Заинтересованные стороны проекта	**Ожидания заинтересованных сторон**
Разработчик системы	Получение знаний по специальности, пополнение портфолио, получение материальной выгоды
НИ ТПУ	Увеличение числа научных публикаций, дипломов на научно-практических конференциях.
Компании, желающие повысить свою кибербезопасноть	Увеличение контроля доступа к информации

В таблице 9 представим цель проекта

Таблица 9 – Цели и результаты проекта

Цель проекта:	Разработка системы аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка

Организационная структура проекта

В таблице 10 отражена организационная структура, роль и функции каждого члена команды.

Таблица 10 – Рабочая группа

№ п/п	ФИО, основное место работы, должность	Роль	Функции	Трудо-затраты, час.
1	Кочегурова Елена Алексеевна, Томский политехнический университет, доцент	Руководитель	Заверение документов, определение направления развития проекта.	36
2	Очиров Жаргал Александрович, Томский	Исполнитель	Разработка ПО, документирование результатов.	540

	политехнический университет, магистр			

5.3 Планирование управления НТИ

Иерархическая структура работ проекта

Для осуществления разработки, был сформирован ряд работ и назначены должности исполнителей для каждого этапа работы (таблица 11).

Таблица 11 – Перечень работ по проекту

№ работы	Наименование работы	Исполнители работы	Длительность работ в днях
1	Выбор научного руководителя магистерской работы	Очиров Ж.А.	5 дней
2	Составление и утверждение темы магистерской работы	Кочегурова Е.А., Очиров Ж.А.	7 дней
3	Составление календарного плана-графика выполнения магистерской работы	Кочегурова Е.А.	3 дня
4	Подбор и изучение литературы по теме магистерской работы	Очиров Ж.А.	12 дней
5	Анализ предметной области	Очиров Ж.А.	15 дней
6	Разработка методики и алгоритма распознавания	Очиров Ж.А.	16 дней
7	Проектирование системы распознавания пользователя по клавиатурному почерку	Очиров Ж.А.	15 дней
8	Сбор и моделирование тестовых данных	Очиров Ж.А.	14 дней
9	Разработка системы распознавания пользователя по клавиатурному почерку	Очиров Ж.А.	15 дней
10	Тестирование системы	Очиров Ж.А.	7 дней
11	Оценка эффективности полученных результатов	Очиров Ж.А.	3 дня
12	Согласование выполненной работы с научным руководителем	Кочегурова Е.А., Очиров Ж.А.	3 дня
13	Выполнение других частей работы (финансовый менеджмент, социальная	Очиров Ж.А.	14 дней

	ответственность)		
14	Подведение итогов, оформление работы	Очиров Ж.А.	4 дня

5.3.1. План проекта

В виде диаграммы Ганта был составлен линейный график работ по проекту, в котором отражены даты начала и окончания, длительность ответственных лиц по каждому этапу работ рисунок 26.

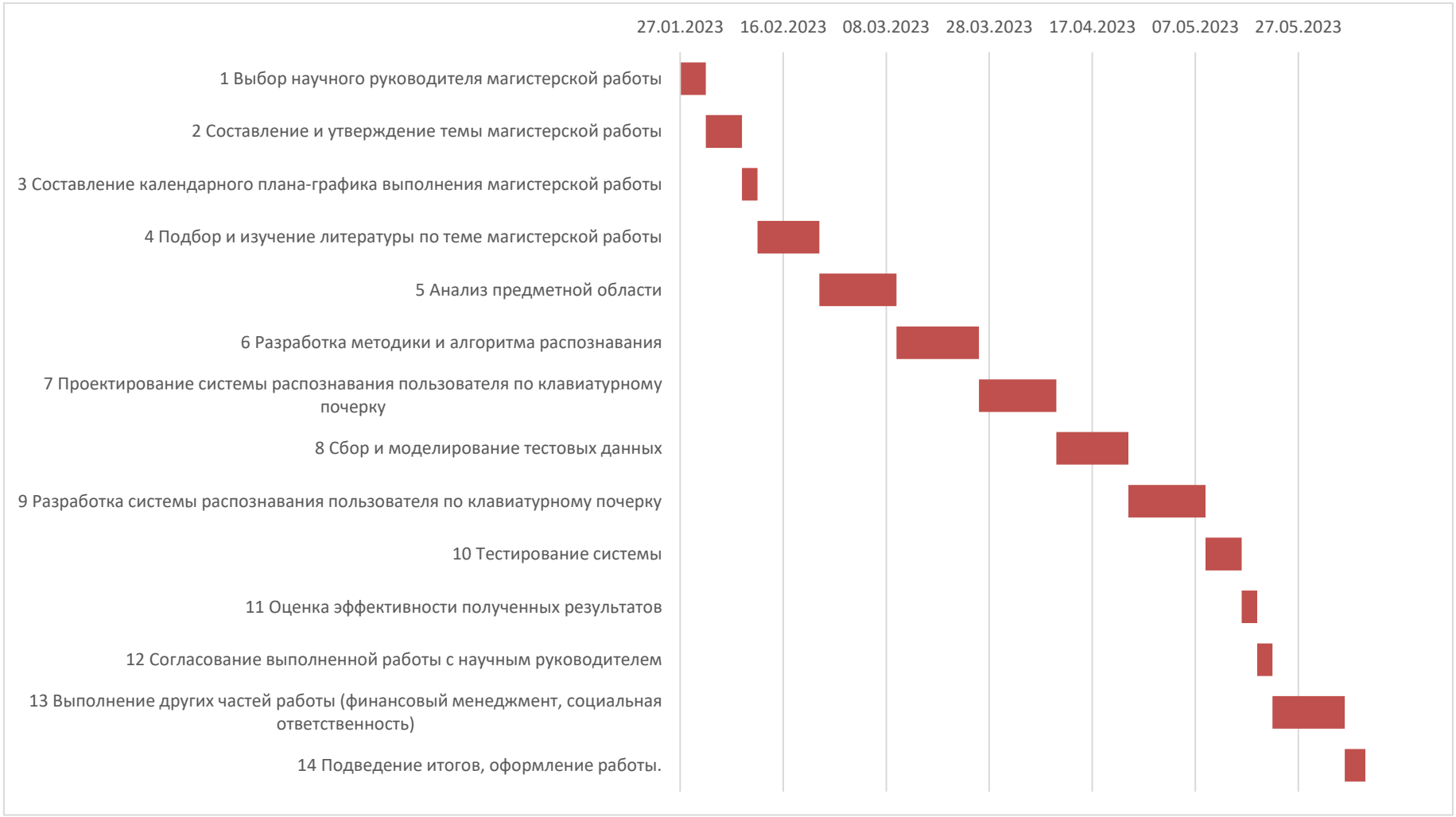

Рисунок 26 – Диаграмма Ганта

5.3.2. Бюджет НТИ

Статьи, рассчитанные в предыдущих пунктах, сведены в таблице 9.

Таблица 12 – Итоговый бюджет НТИ

Статьи					
Варианты исполнения	Сырье и материалы, руб.	Специальное оборудование, руб.	Основная заработная плата, руб.	Отчисления на социальные нужды, руб.	Итого
1	6000	60000	298634,16	89590,2	454224,4
2	6000	80000	298634,16	89590,2	474224,4

Сырьё и материалы

Сырьем и материалами в нашем случае являются оплата за электричество и интернет. Тарифный план за свет 2,73 рубля за кВт, по приблизительным усредненным показателям, компьютер потребляет около 200 Вт. Оплата за интернет составляет 350 рублей. Траты на сырье и материалы за год составят 6000 рублей

Специальное оборудование

Таблица 13 - Специального оборудования

Вариант исполнения	**Наименование**	**Кол-во, шт.**	**Цена единицы, руб.**	**Общая стоимость, руб.**
1	ПК	1	60000	60000
	Операционная система Linux	1	0	0
	Среда разработки	1	0	0
Итог:				**60000**
2	ПК	1	60000	60000,00
	Операционная система Linux	1	0	4000
	Среда разработки	1	0	16000
Итог:				**80000**

Основная заработная плата

Основная заработная плата ($З_{осн}$) руководителя (лаборанта, инженера) от предприятия (при наличии руководителя от предприятия) рассчитывается по следующей формуле:

$$З_{осн} = З_{дн} \cdot T_p . \quad (6)$$

Где $З_{осн}$ – основная заработная плата одного работника, руб.;

$Т_р$ – продолжительность работ, выполняемых научно-техническим работником, раб. дн. (таблица);

$З_{дн}$ – среднедневная заработная плата работника, руб.

Среднедневная заработная плата рассчитывается по формуле:

$$З_{дн} = \frac{З_м \cdot М}{F_д} . \quad (7)$$

Где $З_м$ – месячный должностной оклад работника, руб.;

М – количество месяцев работы без отпуска в течение года: при отпуске в 48 раб. дня М =10,4 месяца, 6-дневная неделя;

$F_д$ – действительный годовой фонд рабочего времени научно-технического персонала, рабочие дни (таблица 11).

Таблица 14 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Студент
Календарное число дней	365	365
Количество нерабочих дней - выходные дни - праздничные дни	118	118
Действительный годовой фонд рабочего времени	247	247

Месячный должностной оклад работника:

$$З_м = З_{тс} \cdot (1 + k_{пр} + k_д) \cdot k_р . \quad (8)$$

Где $З_{тс}$ – заработная плата по тарифной ставке, руб.;

$k_{пр}$ – премиальный коэффициент, равный 0,3 (т.е. 30% от $З_{тс}$);

$k_д$ – коэффициент доплат и надбавок составляет примерно 0,2 – 0,5 (в НИИ и на промышленных предприятиях – за расширение сфер

обслуживания, за профессиональное мастерство, за вредные условия: 15-20 % от $З_{тс}$);

$k_р$ – районный коэффициент, равный 1,3 (для Томска).

Для предприятий, не относящихся к бюджетной сфере, тарифная заработная плата (оклад) рассчитывается по тарифной сетке, принятой на данном предприятии. Расчёт основной заработной платы приведён в таблице 16.

Величина отчислений во внебюджетные фонды определяется исходя из следующей формулы:

$$З_{внеб} = k_{внеб} \cdot (З_{осн} + З_{доп}), \quad (9)$$

где $k_{внеб}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования, в фонд социального страхования, всего 30%).

Таблица 15 – Расчёт основной заработной платы

Исполнители	$З_{тс}$, руб	$k_{пр}$	$k_д$	$k_р$	$З_м$, руб	$З_{дн}$, руб	$Т_р$, раб. дн.	$З_{осн}$, руб	Отчисления в социальные внебюджетные фонды
Руководитель	33664,00	0,3	0,15	1,3	63456,64	2671,86	13	34734,16	10420,2
Студент	25000,00	0,3	0,15	1,3	47125,00	1984.21	133	263900,00	79170
Итого								**298634,16**	**89590,2**

5.3.3. Реестр рисков проекта

Риски проекта включают в себя различные неопределенные события, которые могут возникнуть в проекте и вызвать негативные последствия. Риски представлены в таблице 16.

Таблица 16 – Реестр рисков проекта

№	Риск	Потенциальное воздействие	Вероятность наступления (1-5)	Влияние риска (1-5)	Уровень риска*	Способы смягчения риска	Условия наступления
1	Несоответствие модели реальным процессам	Увеличение сроков разработки	2	4	Средний	Составление плана реализации проекта	Неверное планирование времени

Продолжение таблицы 16

2	Недостаток знаний не позволит создать продукт, отвечающий требованиям	Продукт ненадлежащего качества	2	5	Средний	Изучение специализированной литературы	Недостаток знаний у разработчика
3	Создание продукта, не соответствующего ожиданиям заказчика	Не востребованность системы	2	2	Низкий	Тщательное изучение требований и проектирование системы	Изменение требований к системе

5.4 Определение ресурсной (ресурсосберегающей), финансовой эффективности исследования

Сравнительная эффективность разработки выражается в интегральном показателе эффективности. Этот показатель состоит из двух средневзвешенных величин:

Определение интегральных показателей эффективности проведём в сравнении со вариантом исполнения 2.

Интегральный финансовый показатель разработки определяется как:

$$I_{\text{финр}}^{исп.i} = \frac{\Phi_{pi}}{\Phi_{max}}. \quad (10)$$

Где $I_{\text{финр}}^{\text{исп.i}}$ – интегральный финансовый показатель разработки;

Φ_{pi} – стоимость *i*-го варианта исполнения;

Φ_{max} – максимальная стоимость исполнения научно-исследовательского проекта.

Результаты вычислений приведены в таблице 17.

Таблица 17 – Расчёт интегрального финансового показателя

Вариант исполнения	Φ_{pi}	Φ_{max}	$I_{\text{финр}}^{исп.i}$
1	454224,4	474224,4	0,95
2	474224,4		1

Интегральный показатель ресурсоэффективности вариантов исполнения объекта исследования можно определить следующим образом:

$$\mathrm{I_{pi}} = \sum a_i \cdot b_i \,. \qquad (11)$$

Где I_{pi} – интегральный показатель ресурсоэффективности для i-го варианта исполнения разработки;

a_i – весовой коэффициент *i*-го варианта исполнения разработки;

b_i – бальная оценка *i*-го варианта исполнения разработки, устанавливается экспертным путем по выбранной шкале оценивания;

n – число параметров сравнения.

Расчёт показателя приведён в таблице 18.

Таблица 18 – Сравнительная оценка характеристик продуктов

Критерии	Весовой коэффициент параметра	1 вариант исполнения	2 вариант исполнения
1. Надежность алгоритмов	0,3	3	5
2. Быстродействие	0,3	3	3
3. Удобство	0,1	4	4
4.Функциональность	0,2	3	4
5. Интерфейс	0,1	4	4
ИТОГО	1	3,4	4

Интегральный показатель эффективности вариантов исполнения разработки ($I_{ucni.}$) определяется на основании интегрального показателя ресурсоэффективности и интегрального финансового показателя по формуле:

$$I_{исп.1} = \frac{I_{р-исп1}}{I_{финр}^{исп.1}}, \quad I_{исп.1} = \frac{I_{р-исп1}}{I_{финр}^{исп.1}} \text{ и т.д.} \qquad (12)$$

Сравнение интегрального показателя эффективности вариантов исполнения разработки позволит определить сравнительную эффективность проекта (таблица 19) и выбрать наиболее целесообразный вариант из предложенных.

Таблица 19 – Расчёт интегрального показателя эффективности

	$I_{\text{финр}}^{исп.i}$	$I_{р-исп}$	$I_{исп}$
1 вариант исполнения	0,95	3,4	3,58
2 вариант исполнения	1	4	4

Сравнительную эффективность проекта определим по следующей формуле:

$$Э_{ср} = \frac{I_{исп.1}}{I_{исп.2}}.; \quad (13)$$

где $Э_{ср}$ – сравнительная эффективность проекта;

$I_{исп.1}$ – интегральный показатель первого варианта исполнения разработки, описанной в ВКР;

$I_{исп.2}$ – интегральный показатель второго варианта исполнения, описанной в ВКР.

Таким образом сравнительная эффективность проекта с вариантом разработки номер 2 составила 0.895. Отсюда следует что вариант разработки номер 2 является предпочтительным в плане эффективности.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ВМ11	Очиров Жаргал Александрович

Тема магистерской диссертации:

«Разработка системы динамической аутентификации пользователя на основе анализа его работы на клавиатуре компьютера»

Школа	ИШИТР	Отделение	ОИТ
Уровень образования	Магистратура	**Направление/специальность**	09.04.01 «Информатика и вычислительная техника»

Исходные данные к разделу «Социальная ответственность»	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	Объект исследования: система аутентификации пользователя на основе его анализа на клавиатуре Область применения: финансовые сферы, информационные системы. Рабочее место: офис с персональным компьютером. Количество и наименование оборудования рабочей зоны: персональный компьютер.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность: 1.1. Анализ выявленных вредных факторов • Природа воздействия • Действие на организм человека • Нормы воздействия и нормативные документы (для вредных факторов) • СИЗ коллективные и индивидуальные 1.2. Анализ выявленных опасных факторов • Термические источники опасности • Электробезопасность • Пожаробезопасности	1. Вредные факторы: 1.1. Недостаточная освещенность; 1.2. Нарушения микроклимата, оптимальные и допустимые параметры; 1.3. Шум, ПДУ, СКЗ, СИЗ; 1.4. Повышенный уровень электромагнитного излучения, ПДУ, СКЗ, СИЗ; 2.Опасные факторы: 2.1.Электроопасность; класс электроопасности помещения, безопасные номиналы I, U, $R_{заземления}$, СКЗ, СИЗ; 2.2.Пожароопасность, категория пожароопасности помещения, марки огнетушителей, их назначение и ограничение применения; Приведена схема эвакуации.
2. Экологическая безопасность: • Выбросы в окружающую среду • Решения по обеспечению экологической безопасности	Наличие промышленных отходов (бумага-черновики, перегоревшие люминесцентные лампы, оргтехника) и способы их утилизации;

3. Безопасность в чрезвычайных ситуациях: 1.перечень возможных ЧС при разработке и эксплуатации проектируемого решения; 2.разработка превентивных мер по предупреждению ЧС; 3.разработка действий в результате возникшей ЧС и мер по ликвидации её последствий.	Рассмотрены 2 ситуации ЧС: 1) природная – сильные морозы зимой, (аварии на электро-, тепло-коммуникациях, водоканале, транспорте); 2) техногенная – несанкционированное проникновение посторонних на рабочее место (возможны проявления вандализма, диверсии, промышленного шпионажа), представлены мероприятия по обеспечению устойчивой работы производства в том и другом случае.
4.Перечень нормативно-технической документации.	– ГОСТы, СанПиНы, СНиПы

Дата выдачи задания для раздела по линейному графику	01.03.2023 г.

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ТПУ	Федорчук Ю.М.	д.т.н.		01.03.2023 г.

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ11	Очиров Жаргал Александрович		01.03.2023 г.

6 СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Введение

Социальная ответственность - ответственность отдельного ученого и научного сообщества перед обществом. Первостепенное значение при этом имеет безопасность применения технологий, которые создаются на основе достижений науки, предотвращение или минимизация возможных негативных последствий их применения, обеспечение безопасного как для испытуемых, как и для окружающей среды проведения исследований.

Разработанный проект в рамках магистерской диссертации представляет собой программно-вычислительную систему, направленную на построение моделей для прогнозирования температурных величин, тем самым повышая предсказуемость этих параметров во времени. Работа выполнялась в лаборатории кибернетического центра ТПУ с использованием компьютера. Раздел также включает в себя оценку условий труда на рабочем месте, анализ вредных и опасных факторов труда, разработку мер защиты от них.

6.1 Производственная безопасность

6.1.1. Вредные производственные факторы

6.1.1.1. Недостаточная освещенность рабочей зоны

Для обеспечения требуемой освещенности необходимо использовать совмещенное освещение, создаваемое сочетанием естественного и искусственного освещения. При данном этапе развития осветительной техники целесообразно использовать люминесцентные лампы, которые по сравнению с лампами накаливания имеют большую светоотдачу на ватт потребляемой мощности и более естественный спектр.

Минимальный уровень средней освещенности на рабочих местах с постоянным пребыванием людей должен быть не менее 200 лк.

В расчётном задании должны быть решены следующие вопросы:

– выбор системы освещения;
– выбор источников света;
– выбор светильников и их размещение;
– выбор нормируемой освещённости;
– расчёт освещения методом светового потока.

В данном расчётном задании для всех помещений рассчитывается общее равномерное освещение.

Таблица 20. Параметры помещения.

Параметр	Обозначение	Значение, м
Длина	A	7
Ширина	B	6
Высота помещения	H	3,5
Свес	h_c	0,4
Высота Р.П.	$h_{рп}$	0,8
Высота от светильника до Р.П.	h	$H- h_{рп} - h_c$
Коэффициент отражения стен	$\rho_{ст}$	70 %
Коэффициент отражения потолка	$\rho_п$	70
Коэффициент запаса	Kз	1.5
Коэффициент неравномерности	Z	1.1

Расчёт общего равномерного искусственного освещения горизонтальной рабочей поверхности выполняется методом коэффициента светового потока, учитывающим световой поток, отражённый от потолка и стен.

Световой поток лампы определяется по формуле:

$$\Phi_{рас} = \frac{E_н * S * K_з * Z}{N * \eta}$$

Где $E_н$ – нормируемая минимальная освещённость по СНиП 23-05-95, лк; S – площадь освещаемого помещения, м^2; $K_з$ – коэффициент запаса, учитывающий загрязнение светильника (источника света, светотехнической арматуры, стен и пр., т. е. отражающих поверхностей), наличие в атмосфере

цеха дыма, пыли; Z – коэффициент неравномерности освещения, отношение $E_{\text{ср}}/E_{\min}$. Для люминесцентных ламп при расчётах берётся равным 1,1; N – число ламп в помещении; η – коэффициент использования светового потока.

Коэффициент использования светового потока показывает, какая часть светового потока ламп попадает на рабочую поверхность. Он зависит от индекса помещения i, типа светильника, высоты светильников над рабочей поверхностью h и коэффициентов отражения стен ρ_c и потолка ρ_n.

Индекс помещения определяется по формуле:

$$i = S / h\ (\text{A} + B)$$

Проведем расчет индекса помещения:

Площадь помещения:

$$S = A * B = 7 * 6 = 42\ m^2$$

Индекс:

$$\text{i} = \frac{S}{\text{h} * (A + B)} = \frac{42}{(3.5 - 0.8 - 0.4) * (8 + 7)} = 1.4$$

Согласно этим данным, коэффициент использования светового потока будет равен 48 % или в долях = 0,48.

Коэффициенты отражения оцениваются субъективно (табл. 4.10) [БЖД Практикум 2009-2020].

Согласно указанной методике, выбираем тип источника света.

Наиболее подходящим вариантом является 40 ваттная лампа ЛБ, у которой Ф=2800 лм. Для выбранного типа лампы подходит светильник ОД-2-40 с размерами: длина = 1230 мм, ширина = 266 мм.

Количество ламп для помещения:

$$N = \frac{E_н * S * K_з * Z}{Ф * \eta} = \frac{200 * 42 * 1.5 * 1.1}{2800 * 0.48} = 10.3$$

Принимаем N=12 лампы или 6 светильников.

Размещаем светильники в 2 ряда по 3 светильников в ряду с соблюдением условий: L – расстояние между соседними светильниками или рядами (если по длине (А) и ширине (В) помещения расстояния различны, то они обозначаются L_A и L_B), l – расстояние от крайних светильников или рядов до стены.

Оптимальное расстояние l от крайнего ряда светильников до стены рекомендуется принимать равным $L/3$.

Сначала определим световой поток расчетный.

$$Ф = \frac{E_н * S * K_з * Z}{N * \eta} = \frac{200 * 42 * 1.5 * 1.1}{12 * 0.48} = 2406 \text{ лм};$$

Теперь определим расстояния между светильниками по длине помещения.

$$7000 = 2 * L_A + 3 * 1230 + 2/3 * L_A \; ; \; L_A = (7000 - 3690) * 3/8 = 1241 \text{ мм}$$

$$L_A / 3 = 414 \text{ мм}$$

$$6000 = L_B + 2 * 266 + 2/3 * L_B \; ; \; L_B = (6000 - 532) * 3/5 = 3281 \text{ мм}$$

$$L_B / 3 = 1094 \text{ мм}$$

Рисуем схему размещения светильников на потолке для обеспечения общего равномерного освещения.

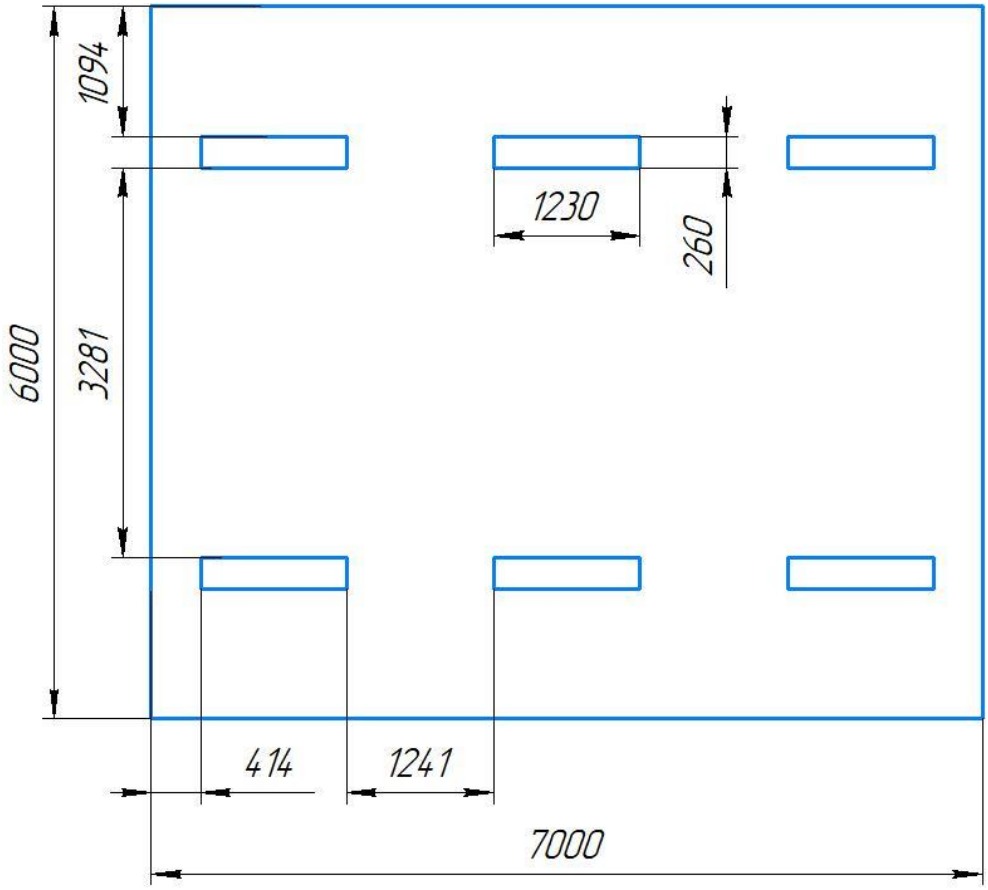

Рисунок 27 – План размещения светильников на потолке.

Проведем проверку выполнения условия соответствия:

$$-10\% \le \frac{\Phi_{л.станд} - \Phi_{л.расч}}{\Phi_{л.станд}} * 100\% \le +20\%$$

$$-10\% \le \frac{2800 - 2406}{2800} * 100\% \le +20\%$$

$$-10\% \le +14\% \le +20\%$$

Результат расчета укладывается в поле допуска.

Определим мощность осветительной установки:

$$P = N * P_i = 12 * 40\ Вт = 480\ Вт$$

6.1.1.2. Отклонение показателей микроклимата в помещении

Проанализируем микроклимат в помещении, где находится рабочее место. Микроклимат производственных помещений определяют следующие параметры: температура, относительная влажность, скорость движения воздуха. Эти факторы влияют на организм человека, определяя его самочувствие.

Оптимальные параметры микроклимата на рабочих местах должны соответствовать величинам, приведенным таблицах 21, 22.

Таблица 26- Оптимальные нормы микроклимата

Период года	Температура воздуха, С°	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	19-23	40-60	0.1
Теплый	23-25		0.2

Таблица 22 - Допустимые нормы микроклимата

Период года	Температура воздуха, С°		Относительная влажность воздуха, %	Скорость движения воздуха, м/с
	Нижняя допустимая граница	Верхняя допустимая граница		
Холодный	15	24	20-80	<0.5
Теплый	22	28	20-80	<0.5

Общая площадь рабочего помещения составляет 42м^2, объем составляет 147м^3. По СанПиН 2.2.2/2.4.1340-03 санитарные нормы составляют 6,5 м^2 и 20 м^{3}объема на одного человека. Исходя из приведенных выше данных, можно сказать, что количество рабочих мест соответствует размерам помещения по санитарным нормам.

После анализа габаритных размеров рассмотрим микроклимат в этой комнате. В качестве параметров микроклимата рассмотрим температуру, влажность воздуха, скорость ветра.

В помещении осуществляется естественная вентиляция посредством наличия легко открываемого оконного проема (форточки), а также дверного проема. По зоне действия такая вентиляция является общеобменной. Основной недостаток - приточный воздух поступает в помещение без предварительной очистки и нагревания. Согласно нормам, СанПиН 2.2.2/2.4.1340-03 объем воздуха необходимый на одного человека в помещении без дополнительной вентиляции должен быть более 40м^3[1]. В нашем случае объем воздуха на одного человека составляет 42 м^3, из этого следует, что дополнительная вентиляция не требуется. Параметры микроклимата поддерживаются в холодное время года за счет систем водяного отопления с нагревом воды до 100°С, а в теплое время года – за счет кондиционирования, с параметрами согласно [2]. Нормируемые параметры микроклимата, ионного состава воздуха, содержания вредных веществ должны соответствовать требованиям [3].

6.1.1.3. Превышение уровней шума

Одним из наиболее распространенных в производстве вредных факторов является шум. Он создается вентиляционным и рабочим оборудованием, преобразователями напряжения, рабочими лампами дневного света, а также проникает снаружи. Шум вызывает головную боль, усталость, бессонницу или сонливость, ослабляет внимание, память ухудшается, реакция уменьшается.

Основным источником шума в комнате являются компьютерные охлаждающие вентиляторы и. Уровень шума варьируется от 35 до 42 дБА. Согласно СанПиН 2.2.2 / 2.4.1340-03, при выполнении основных работ на ПЭВМ уровень шума на рабочем месте не должен превышать 80 дБА [4].

При значениях выше допустимого уровня необходимо предусмотреть средства индивидуальной защиты (СИЗ) и средства коллективной защиты (СКЗ) от шума.

Средства коллективной защиты:

1. устранение причин шума или существенное его ослабление в источнике образования;
2. изоляция источников шума от окружающей среды (применение глушителей, экранов, звукопоглощающих строительных материалов, например любой пористый материал – шамотный кирпич, микропористая резина, поролон и др.);
3. применение средств, снижающих шум и вибрацию на пути их распространения;

Средства индивидуальной защиты;

1. применение спецодежды и защитных средств органов слуха: наушники, беруши, антифоны.

6.1.1.4. Повышенный уровень электромагнитных излучений

Источником электромагнитных излучений в нашем случае являются дисплеи ПЭВМ. Монитор компьютера включает в себя излучения рентгеновской, ультрафиолетовой и инфракрасной области, а также широкий диапазон электромагнитных волн других частот.

Согласно СанПиН 2.2.2/2.4.1340-03 напряженность электромагнитного поля по электрической составляющей на расстоянии 50 см вокруг ВДТ не должна превышать 25В/м в диапазоне от 5Гц до 2кГц, 2,5В/м в диапазоне от 2 до 400кГц [1]. Плотность магнитного потока не должна превышать в диапазоне от 5 Гц до 2 кГц 250нТл, и 25нТл в диапазоне от 2 до 400кГц. Поверхностный электростатический потенциал не должен превышать 500В [1].

В ходе работы использовалась ПЭВМ типа ASUS GL703VD со следующими характеристиками: напряженность электромагнитного поля 3В/м; поверхностный потенциал составляет 560 В (основы противопожарной защиты предприятий ГОСТ 12.1.004 и ГОСТ 12.1.010 – 76.)[5].

При длительном постоянном воздействии электромагнитного поля (ЭМП) радиочастотного диапазона при работе на ПЭВМ у человеческого организма сердечно-сосудистые, респираторные и нервные расстройства, головные боли, усталость, ухудшение состояния здоровья, гипотония, изменения сердечной мышцы проводимости. Тепловой эффект ЭМП характеризуется увеличением температуры тела, локальным селективным нагревом тканей, органов, клеток за счет перехода ЭМП на теплую энергию.

Предельно допустимые уровни (ПДУ) облучения (по ОСТ 54 30013-83):

а) до 10 мкВт/см2, время работы (8 часов);

б) от 10 до 100 мкВт/см2, время работы не более 2 часов;

в) от 100 до 1000 мкВт/см2, время работы не более 20 мин. при условии пользования защитными очками;

г) для населения в целом ППМ не должен превышать 1 мкВт/см2.

Защита человека от опасного воздействия электромагнитного излучения осуществляется следующими способами:

СКЗ

1. защита временем;
2. защита расстоянием;
3. снижение интенсивности излучения непосредственно в самом источнике излучения;
4. заземление экрана вокруг источника;

5. защита рабочего места от излучения;

СИЗ

1. Очки и специальная одежда, выполненная из металлизированной ткани (кольчуга). При этом следует отметить, что использование СИЗ возможно при кратковременных работах и является мерой аварийного характера. Ежедневная защита обслуживающего персонала должна обеспечиваться другими средствами.

2. Вместо обычных стекол используют стекла, покрытые тонким слоем золота или диоксида олова (SnO_2).

6.1.2. Опасные производственные факторы

6.1.2.1. Поражение электрическим током

К опасным факторам можно отнести наличие в помещении большого количества аппаратуры, использующей однофазный электрический ток напряжением 220 В и частотой 50Гц. По опасности электропоражения комната относится к помещениям без повышенной опасности, так как отсутствует повышенная влажность, высокая температура, токопроводящая пыль и возможность одновременного соприкосновения токоведущих элементов с заземленными металлическими корпусами оборудования [6].

Лаборатория относится к помещению без повышенной опасности поражения электрическим током. Безопасными номиналами являются: $I < 0{,}1$ А; $U < (6\text{-}42)$ В; $R_{заз} < 4$ Ом.

Для защиты от поражения электрическим током используют СКЗ и СИЗ.

Средства коллективной защиты:

1. — защитное заземление, зануление;
2. — малое напряжение;
3. — электрическое разделение сетей;
4. — защитное отключение;

5. — изоляция токоведущих частей;

6. — оградительные устройства.

Использование щитов, барьеров, клеток, ширм, а также заземляющих и шунтирующих штанг, специальных знаков и плакатов.

Средства индивидуальной защиты:

1. — диэлектрические перчатки, изолирующие клещи и штанги;

2. — слесарные инструменты с изолированными рукоятками;

3. — указатели величины напряжения, калоши, боты, подставки и коврики.

6.1.2.2. Пожароопасность

По взрывопожарной и пожарной опасности помещения подразделяются на категории А, Б, В1-В4, Г и Д.

Согласно НПБ 105-03 лаборатория относится к категории В – горючие и трудно горючие жидкости, твердые горючие и трудно горючие вещества и материалы, вещества и материалы, способные при взаимодействии с водой, кислородом воздуха или друг с другом только гореть, при условии, что помещения, в которых находится, не относятся к категории наиболее опасных А или Б.

По степени огнестойкости данное помещение относится к 1-й степени огнестойкости по СНиП 2.01.02-85 (выполнено из кирпича, которое относится к трудно сгораемым материалам).

Возникновение пожара при работе с электронной аппаратурой может быть по причинам как электрического, так и неэлектрического характера.

Причины возникновения пожара неэлектрического характера:

а) халатное неосторожное обращение с огнем (курение, оставленные без присмотра нагревательные приборы, использование открытого огня);

Причины возникновения пожара электрического характера: короткое замыкание, перегрузки по току, искрение и электрические дуги, статическое электричество и т. п.

Для локализации или ликвидации загорания на начальной стадии используются первичные средства пожаротушения. Первичные средства пожаротушения обычно применяют до прибытия пожарной команды.

Огнетушители водо-пенные (ОХВП-10) используют для тушения очагов пожара без наличия электроэнергии. Углекислотные (ОУ-2) и порошковые огнетушители предназначены для тушения электроустановок, находящихся под напряжением до 1000В. Для тушения токоведущих частей и электроустановок применяется переносной порошковый огнетушитель, например ОП-5.

В общественных зданиях и сооружениях на каждом этаже должно размещаться не менее двух переносных огнетушителей. Огнетушители следует располагать на видных местах вблизи от выходов из помещений на высоте не более 1,35 м. Размещение первичных средств пожаротушения в коридорах, переходах не должно препятствовать безопасной эвакуации людей.

Для предупреждения пожара и взрыва необходимо предусмотреть:

1. специальные изолированные помещения для хранения и разлива легковоспламеняющихся жидкостей (ЛВЖ), оборудованные приточно-вытяжной вентиляцией во взрывобезопасном исполнении - соответствии с ГОСТ 12.4.021-75 и СНиП 2.04.05-86;

2. специальные помещения (для хранения в таре пылеобразной канифоли), изолированные от нагревательных приборов и нагретых частей оборудования;

3. первичные средства пожаротушения на производственных участках (передвижные углекислые огнетушители ГОСТ 9230-77, пенные

огнетушители ТУ 22-4720-80, ящики с песком, войлок, кошма или асбестовое полотно);

4. автоматические сигнализаторы (типа СВК-3 М 1) для сигнализации о присутствии в воздухе помещений предвзрывных концентраций горючих паров растворителей и их смесей.

Лаборатория полностью соответствует требованиям пожарной безопасности, а именно, наличие охранно-пожарной сигнализации, плана эвакуации, изображенного на рисунке 1, порошковых огнетушителей с поверенным клеймом, табличек с указанием направления к запасному (эвакуационному) выходу.

Рисунок 28 – План эвакуации. Исполнитель в аудитории 105, сплошные линии − основной выход, штриховые линии − запасный выход.

6.2 Экологическая безопасность

В компьютерах огромное количество компонентов, которые содержат токсичные вещества и представляют угрозу, как для человека, так и для окружающей среды.

К таким веществам относятся:

- свинец (накапливается в организме, поражая почки, нервную систему);
- ртуть (поражает мозг и нервную систему);
- никель и цинк (могут вызывать дерматит);
- щелочи (прожигают слизистые оболочки и кожу);

Поэтому компьютер требует специальных комплексных методов утилизации.

Таким образом утилизацию компьютера можно провести следующим образом:

- отделить металлические детали от неметаллов;

- разделить углеродистые металлы от цветмета;

- пластмассовые изделия (крупногабаритные) измельчить для уменьшения объема;

- копир-порошок упаковать в отдельную упаковку, точно также, как и все проклассифицированные и измельченные компоненты оргтехники, и после накопления на складе транспортных количеств отправить предприятиям и фирмам, специализирующимся по переработке отдельных видов материалов.

Люминесцентные лампы утилизируют следующим образом. Не работающие лампы немедленно после удаления из светильника должны быть упакованы в картонную коробку, бумагу или тонкий мягкий картон, предохраняющий лампы от взаимного соприкосновения и случайного

механического повреждения. После накопления ламп объемом в 1 транспортную единицу их сдают на переработку на соответствующее предприятие. Недопустимо выбрасывать отработанные энергосберегающие лампы вместе с обычным мусором, превращая его в ртутьсодержащие отходы, которые загрязняют ртутными парами

6.3 Безопасность в чрезвычайных ситуациях

Природная чрезвычайная ситуация – обстановка на определенной территории или акватории, сложившейся в результате возникновения источника природной чрезвычайной ситуации, который может повлечь или повлек за собой человеческие жертвы, ущерб здоровью людей и (или) окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Производство находится в городе Томске с континентально-циклоническим климатом. Природные явления (землетрясения, наводнения, засухи, ураганы и т. д.), в данном городе отсутствуют.

Возможными ЧС на объекте в данном случае, могут быть сильные морозы и диверсия (вандализм, хулиганство, шпионаж).

Для Сибири в зимнее время года характерны морозы. Достижение критически низких температур приводит к авариям систем тепло- и водоснабжения, сантехнических коммуникаций и электроснабжения, приостановке работы. В этом случае при подготовке к зиме следует предусмотреть

а) газобаллонные калориферы (запасные обогреватели),

б) дизель или бензо-электрогенераторы;

в) запасы питьевой и технической воды на складе (не менее 30 л на 1 человека);

г) теплый транспорт для доставки работников на работу и с работы домой в случае отказа муниципального транспорта. Их количества и мощности должно хватать для того, чтобы работа на производстве не прекратилась.

В лаборатории кибернетического центра наиболее вероятно возникновение чрезвычайных ситуаций (ЧС) техногенного характера.

Для предупреждения вероятности осуществления вышесказанных диверсии предприятие необходимо оборудовать системой видеонаблюдения, круглосуточной охраной, пропускной системой, надежной системой связи, а также исключения распространения информации о системе охраны объекта, расположении помещений и оборудования в помещениях, системах охраны, сигнализаторах, их местах установки и количестве. Должностные лица раз в полгода проводят тренировки по отработке действий на случай экстренной эвакуации.

ЗАКЛЮЧЕНИЕ

В рамках магистерской работы был изучен способ решения проблемы подтверждения личности пользователя на основе анализа его работы на клавиатуре.

Было выявлено, что аутентификация пользователя может осуществляется на основе непрерывного контроля его клавиатурных нажатий в любой программной среде. На основе проведенных исследований были сформулированы следующие выводы:

- Необходимо корректировать образцы клавиатурного почерка при использования динамической аутентификации пользователя по клавиатурному почерку.
- Улучшение качества данных, собираемых системой, а также выделение устойчивых признаков клавиатурного почерка существенно влияют на последующие вычисления и, в конечном итоге, на способность системы правильно подтверждать законность пользователя.
- Внедрение в систему частотности букв значительно влияет на чувствительность аутентификации.
- Использованный в исследовании метод опорных векторов (SVM) показал средний результат уступив только распознаванию на основе Евклидова расстояния.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Кочегурова Е.А., Очиров Ж. А. МОНИТОРИНГ ПОЛЬЗОВАТЕЛЯ ДИСТАНЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК КЛАВИАТУРНОГО ПОЧЕРКА // Сборник научных статей по материалам III Всероссийской конференции. - Курск: Курский государственный университет, 2022. - С. 122-131.
2. Аутентификация // Википедия URL: https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F (дата обращения: 12.05.2023).
3. Кочегурова Е.А., Мартынова Ю.А. Особенности непрерывной идентификации пользователей на основе свободных текстов в режиме скрытого мониторинга // Программирование. 2020. № 1. С. 15-28.
4. Довгаль В.А. Особенности захвата параметров клавиатурного почерка // Научный журнал НИУ ИТМО. Серия «Процессы управления и автоматизация». 2017. № 4 (28). С. 57-61.
5. Аюпова А.Р., Якупов А.Р., Шабалкина А.А. Аутентификация по клавиатурному почерку: выгоды и проблемы использования // Международный научно-исследовательский журнал. 2017. № 1. С. 167-171.
6. What is a keylogger // csoonline URL: https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html (дата обращения: 26.05.2023).
7. Killourhy K.S., Maxion R.A. Comparing anomaly-detection algorithms for keystroke dynamics // IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). – Lisbon, Portugal, Jun. 2009.

8. Mondal S., Bours P., Chandran V. Latent semantic indexing-based authentication for free text keystroke dynamics // Pattern Recognition Letters. – 2019. – Vol. 125. – P. 86-93.
9. Gunetti D., Picardi C. Keystroke analysis of free text // ACM Transactions on Information and System Security (TISSEC). – 2005. – Vol. 8, no. 3. – P. 312–347.
10. González N., Calot E.P., Ierache J.S., Hasperué W. On the shape of timings distributions in free-text keystroke dynamics profiles // Heliyon. – 2021. – Vol. 7, no. 11. – e08413. – DOI: 10.1016/j.heliyon. 2021.e08413.
11. Stylios I., Kokolakis S., Thanou O., Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: A survey // Information Fusion. – 2021. – Vol. 66. – P. 76-99. – DOI: 10.1016/j.inffus.2020.08.021
12. Toosi R, Akhaee MA. Time–frequency analysis of keystroke dynamics for user authentication Future Generation. Computer Systems 2021; 115: 438-447. doi.org/10.1016/j.future.2020.09.027.
13. Hazan I., Margalit O., Rokach L. Supporting unknown number of users in keystroke dynamics models // Knowledge-Based Systems. – 2021. – Vol. 221. – P. 106982. – DOI: 10.1016/j.knosys.2021.106982.
14. Parkinson S., Khan S., Crampton A., Xu Q., Xie W., Liu N., Dakin K. Password policy characteristics and keystroke biometric authentication // IET Biometrics . – 2021 .– Vol .10 (2). – P .163-178 .– DOI: 10 .1049 / bme2 .12017.
15. Singh S., Inamdar A., Kore A., Pawar A.Analysis of Algorithms for User Authentication using Keystroke Dynamics // 2020 International Conference on Communication and Signal Processing (ICCSP). – 2020 .– P .0337-0341 .– DOI: 10 .1109 / ICCSP48568 .2020 .9182115.
16. Kim J., Kim H., Kang P .Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature

extraction and novelty detection // Applied Soft Computing .– 2018 .– Vol .62 .– P .1077–1087 .– DOI: 10 .1016 / j.asoc .2017 .09 .045.

17. Lu X., Zhang S., Hui P., Lio P.Continuous authentication by free-text keystroke based on CNN and RNN // Computers & Security .– 2020 .– Vol .96 .– P .01861.– DOI: 10 .1016 / j.cose .2020 .101861.
18. Dargan S., Kumar M.A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities // Expert Systems with Applications.– 2020.– Vol.–143.– P.–113114.– DOI:10.–1016/j.eswa.–2019.–113114.
19. Kochegurova E.A., Martynova Y.A.Aspects of continuous user identification based on free texts and hidden monitoring // Program Comput Softw.– 2020.– Vol.–46 (1).– P.–12-24.– DOI:10.–1134/S036176882001003X.
20. Zaidi A.Z., Chong C.Y., Jin Z., Parthiban R., Sadiq A.S.Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities // J Network Comput Appl.– 2021.– Vol.–191.– P.–103162.– DOI:10.–1016/j.jnca.–2021.–103162.
21. Teh P.S., Teoh A.B.J., Yue S.A survey of keystroke dynamics biometrics // Sci World J.–2013;–2013:1-24;–DOI:10;–1155/2013/408280.
22. Morales A., Fierrez J., Tolosana R.Ortega-Garcia J.Galbally J.Gomez-Barrero M.Anjos A.Marcel S.KBOC: Keystroke biometrics OnGoing competition // 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS).–2016;–DOI:10;–1109/BTAS;–2016;–7791180.
23. Pisani P.H.Lorena A.C.A systematic review on keystroke dynamics // J Braz Comput Soc;–2013;–19(4):573-587.
24. Gunetti D.Picardi C.;Keystroke analysis of free text // ACM Trans Inf Syst Secur;–2005;–8(3):312-347;–DOI:10;–1145/1085126;1085129.

25. Kochegurova E.Luneva E.Gorokhova E.On continuous user authentication via hidden free-text based monitoring // Adv Intell Sys Comput;–2019;–875:66-75;–DOI:10;1007/978-3-030-01821-4_8.
26. Alsultan A.Warwick K.Non-conventional keystroke dynamics for user authentication // Pattern Recogn Lett;–2017;89:53-59;doi:10;1016/j.patrec;2017;02;010.
27. Mondal S.Bours P.A study on continuous authentication using a combination of keystroke and mouse biometrics // Neurocomputing;–2017;(230):1-22;DOI:10;1016/j.neucom;2016;11;031.
28. Zhong Y.Deng Y.A survey on keystroke dynamics biometrics: approaches, advances, and evaluations // Recent Advances in User Authentication Using Keystroke Dynamics Biometrics;2015;(2):1-22.DOI:10;15579/gcsr.vol2.ch1.
29. Ali M.L., Monaco J.V., Tappert C.C. et al. Keystroke Biometric Systems for User Authentication // J Sign Process Syst. – 2017. – P. 175–190. – DOI: 10.1007/s11265-016-1114-9.
30. Alsultan A., Warwick K., Wei H. Non-conventional keystroke dynamics for user authentication // Pattern Recogn Lett. – 2017. – Vol. 89. – P. 53-59. – DOI: 10.1016/j.patrec.2017.02.010..
31. Messerman T., Mustafić T., Camtepe S.A., Albayrak S.Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics // 2011 International Joint Conference on Biometrics (JCB).– 2011.– P.–1–8.– DOI:10.–1109/IJCB.–2011.–6117552.
32. Chang HC, Li J, Wu C, Stamp M. Machine Learning and Deep Learning for Fixed-Text Keystroke Dynamics. arXiv:2107.07409v1 [cs. LG]; 2021. doi.org/10.48550/arXiv.2107.07409.
33. Ahmed AA, Traore I. Biometric recognition based on free-text keystroke dynamics/ Cybern. IEEE Trans 2014; 44(4): 458–472. DOI:10.1109/TCYB.2013.2257745.

34. Goodkind A, Brizan DG, Rosenberg A. Utilizing overt and latent linguistic structure to improve keystroke-based authentication. Image and Vision Computing 2017; 58: 230-238. DOI:10.1016/j.imavis.2016.06.003.
35. Al Solami E, Boyd C, Clark A, Ahmed I. User-representative feature selection for keystroke dynamics. 5th International Conference on Network and System Security (NSS'11) 2011: 229–233. DOI:10.1109/ICNSS.2011.6060005.
36. Eberz S, Rasmussen KB, Lenders V, Martinovic I. Evaluating behavioral biometrics for continuous authentication: challenges and metrics. 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). 2017: 386-399. DOI:10.1145/3052973.3053032.
37. Antal M, Szabó LZ, Laszlo I. Keystroke dynamics on Android platform. Procedia Technology 2015; 19: 820-826. DOI:10.1016/j.protcy.2015.02.118.
38. Locklear H, Govindarajan S, Sitova Z, и др. Continuous authentication with cognition-centric text production and revision features. IEEE/IAPR international joint conference on biometrics (IJCB 2014); 2014. DOI:10.1109/BTAS.2014.6996227.
39. Kang P, Cho S. Keystroke dynamics-based user authentication using long and free text strings from various input devices. Inf Sci 2015; 308: 72-93. DOI:10.1016/j.ins.2014.08.070.
40. Matsubara Y, Samura T, Nishimura H. Keyboard Dependency of Personal Identification Performance by Keystroke Dynamics in Free Text Typing. Journal of Information Security 2015; 6: 229-240. DOI: 10.4236/jis.2015.63023.

Из социальной

1. ГОСТ 54 30013-83. Электромагнитные излучения СВЧ. Предельно допустимые уровни облучения. Требования безопасности.
2. ГОСТ 12.4.154-85. “ССБТ. Устройства экранирующие для защиты от электрических полей промышленной частоты”.
3. ГН 2.2.5.1313-03. Предельно допустимые концентрации (ПДК) вредных веществ в воздухе рабочей зоны.
4. СанПиН 2.2.4/2.1.8.055-96. "Электромагнитные излучения радиочастотного диапазона (ЭМИ РЧ)".
5. СанПиН 2.2.4.548-96. Гигиенические требования к микроклимату производственных помещений.
6. ГОСТ Р 12.1.019-2009. Электробезопасность. Общие требования и номенклатура видов защиты.
7. ГОСТ 12.4.123-83. Средства коллективной защиты от инфракрасных излучений. Общие технические требования.
8. ГОСТ Р 12.1.019-2009. Электробезопасность. Общие требования и номенклатура видов защиты.
9. ГОСТ 12.1.030-81. Электробезопасность. Защитное заземление. Зануление.
10. ГОСТ 12.1.004-91. Пожарная безопасность. Общие требования.
11. ГОСТ 12.2.037-78. Техника пожарная. Требования безопасности.
12. СанПиН 2.1.6.1032-01. Гигиенические требования к качеству атмосферного воздуха.
13. ГОСТ 30775-2001. Ресурсосбережение. Обращение с отходами. Классификация, идентификация и кодирование отходов.
14. СНиП 21-01-97. Противопожарные нормы.

Приложение А
(справочное)

STATE AND RELEVANCE OF KEYBOARD IDENTIFICATION

Студент

Группа	ФИО	Подпись	Дата
8ВМ11	Очиров Жаргал Александрович		

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Кочегурова Е.А.	к.т.н., доцент		

Консультант-лингвист отделения иностранных языков ШБИП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИЯ ШБИП	Степура С.Н.	к.ф.н.		

1 STATE AND RELEVANCE OF KEYBOARD IDENTIFICATION

1.1 Keyboard authentication and identification issues

Keyboard authentication and identification issues belong to the field of behavioral biometrics, which uses the manner and rhythm of typing text on the keyboard to determine the user's identity. Keyboard authentication can be based on various parameters, such as typing speed, duration of key presses, intervals between keys and errors. This is shown in Figure 1

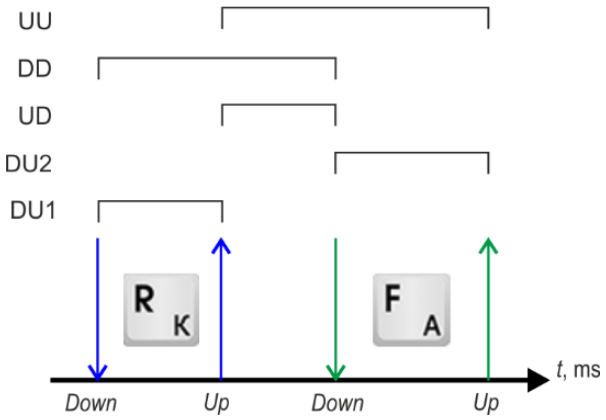

Figure A.1 - Keyboard stroke indicators

Where, DU - key hold time, UD - pause between presses, UU or DD interval between pressing or releasing one key and pressing or releasing the next key respectively.

How to protect the system from unauthorized access? One of the possible ways is to use a two-step verification process:

- Primary identity identification
- Dynamic identity authentication

However, each person has an individual rhythm of typing text. Due to this feature, a biometric system for recognizing a person's identity can use keyboard handwriting. For clarity, Figure 2 shows the typing speed of 8 users from the KM dataset.

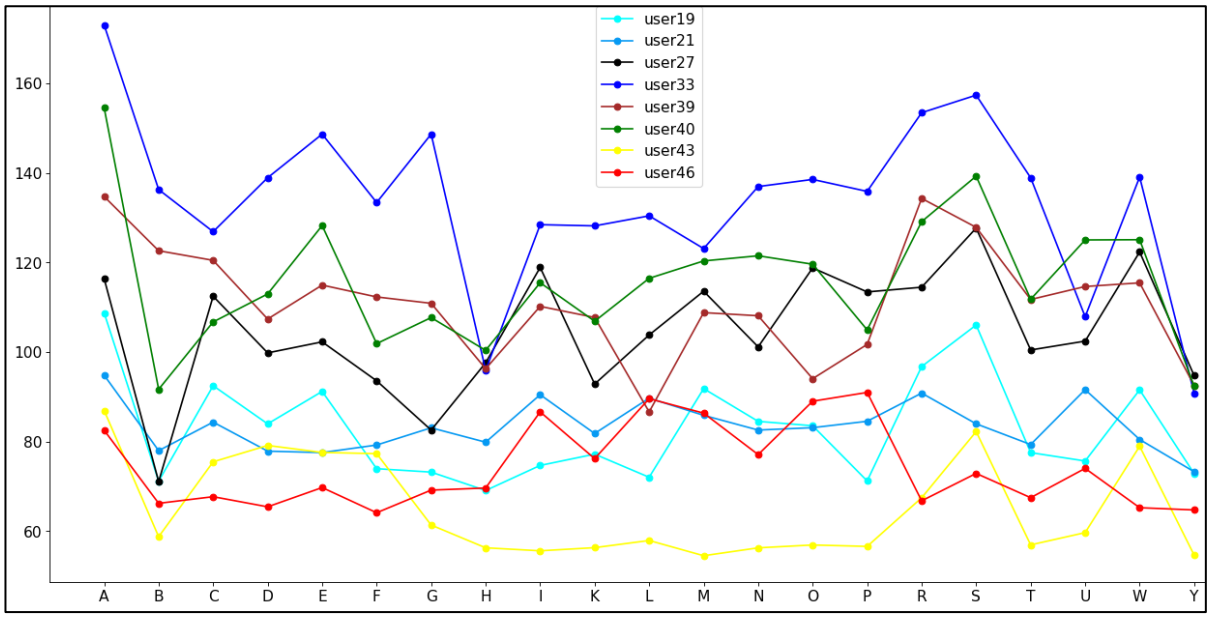

Figure A.2 - Keyboard templates for users

Visual analysis demonstrates certain discrepancies between the times of pressing certain letters on the keyboard. This scatter demonstrates exactly the uniqueness of the rhythm of pressing keys for each user. From a technical point of view, the more keys a user presses, the more accurately an algorithm can understand and recreate a user's keyboard template. The uniqueness of the keyboard template increases the accuracy of the recognition system.

Keyboard identification is a way of determining the user among many other potential users based on how he types on the keyboard. This takes into account various factors that affect the style of typing, such as typing speed, rhythm of key presses, duration of key holding and intervals between presses. Each person has their own individual keyboard handwriting, which distinguishes them from others and can be used as a biometric feature for their identification.

Various techniques can be used to implement keyboard authentication and identification, from statistical methods to artificial intelligence approaches, such as neural networks. One of the advantages of keyboard authentication is that it does not require special equipment, such as fingerprint or face scanners, but can work with any standard keyboard. However, keyboard authentication also has its

drawbacks, such as the influence of physical or emotional state of the user, change in typing style over time and possibility of forgery or imitation.

Keyboard authentication and identification can be used for various purposes, such as enhancing login security, access control to confidential information, monitoring user behavior in the network or detecting intrusions. Keyboard identification can also be used for psychological analysis of personality by its way of typing.

1.2 Authentication methods

There are many methods of user authentication. The methods can be conditionally divided into four groups as shown in Figure 3:

- Based on knowledge of unique information;
- Based on possession of a unique object;
- Based on biometrics
- And other features

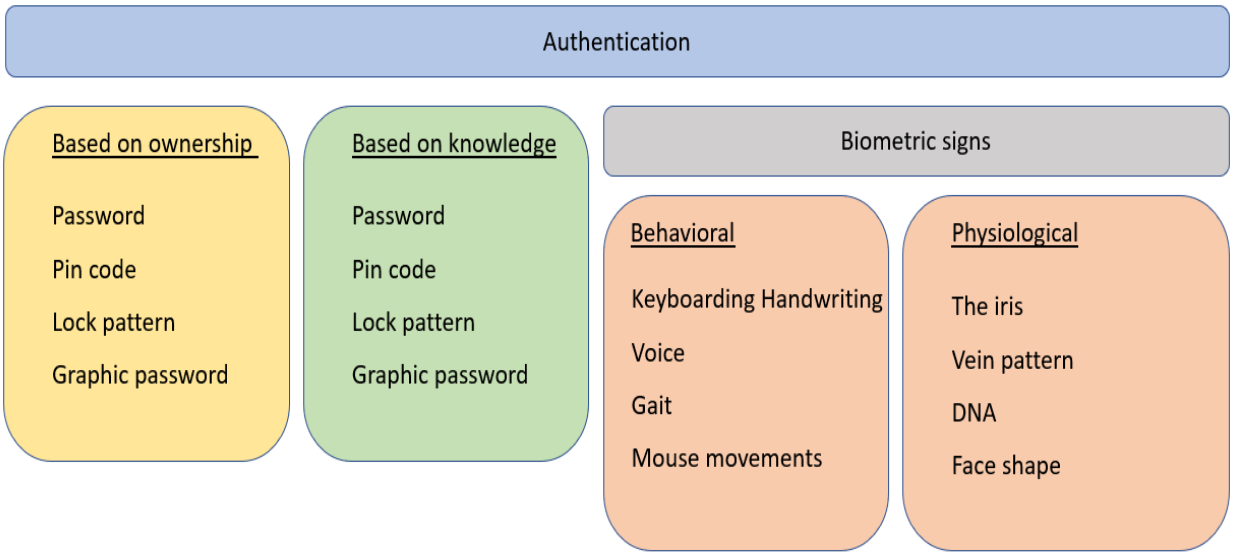

Figure A.3 - Authentication methods

Authentication based on knowledge of personal information (name, password, secret question). These methods are simple to use and inexpensive. However, they provide a low level of security [1].

Authentication based on possession of personal objects user, such as smart cards and keys. This is the least popular method in electronic authentication, because personal items can be stolen or copied [1].

Other authentication features are based on location, time zone, IP address, etc. [1].

Biometric authentication features are divided into physiological and behavioral. Physiological characteristics include shape face, iris of the eye, fingerprints, etc. Behavioral - voice, gait, signature, mouse movement, handwriting and keyboard handwriting. Authentication based on physiological features is accurate, but technical recognition devices are quite expensive [1]. Keyboard handwriting belongs to behavioral biometrics.

Keyboard recognition methods are ways of identifying and authenticating a user by his individual style of typing text on computer keyboard. These methods belong to behavioral biometrics and can be used for static or dynamic (continuous) verification user authenticity.

The frequency of use of keyboard recognition methods depends on from various factors, such as the type of input text (structured or free), text language (Russian or English), authentication purpose (primary or secondary), classification algorithm (based on metric distances, static methods or machine learning), etc.

According to a literature review [3], there are many different keyboard recognition methods that can be divided into three main groups from the point of view of pattern recognition:

- Evaluation of metric distances
- Statistical methods
- Machine learning methods

The relative frequency of use of different keyboard recognition methods is presented in Figure 4 in descending order [3].

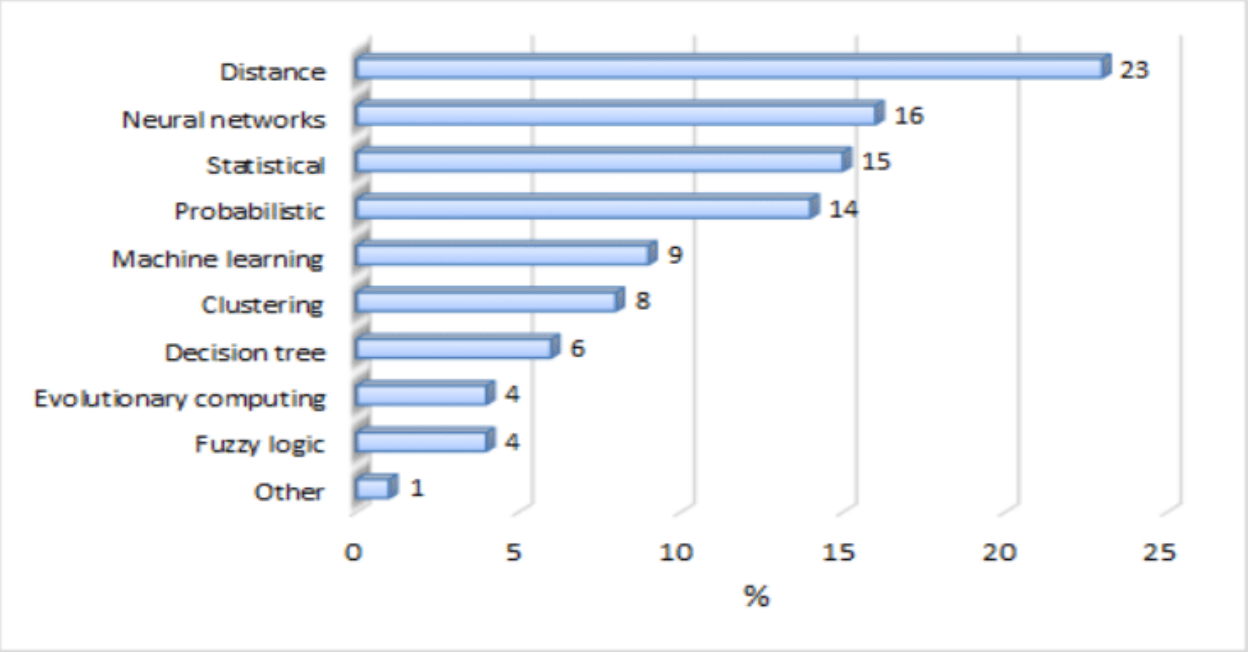

Figure A.4 - Relative frequency of use of keyboard recognition methods

As can be seen from the figure, the most frequently used keyboard recognition methods are those that are based on estimating metric distances between the current and reference user profiles. These methods are simple in implementation and do not require complex calculations. However, they also have their drawbacks, such as low accuracy, high sensitivity to changes in user behavior and the need to choose a threshold value for decision making.

Static keyboard recognition methods use various static models to describe the distribution of keyboard parameters recognition and calculation of the probability of belonging of the current profile to reference. These methods are more accurate and robust to noise and variations in data, but they are also more complex in implementation and require more data for training the model.

Machine learning keyboard recognition methods apply various classification algorithms, such as neural networks, support vectors, decision tree, etc., for training a classifier model based on existing data and predicting the belonging of the current profile to one of the predefined classes (users). These methods can achieve high accuracy and adaptability to new data, but they also require a large

amount of data for training, as well as selection of optimal parameters for each algorithm.

In general, it can be said that the frequency of use of keyboard recognition methods is determined by various factors and depends on specific task and conditions of user authentication.

1.3 Authentication modes

The most justified for the recognition system and comfortable for the user way of authentication is constant and hidden monitoring of the dynamics of his work.

Dynamic characteristics of keyboard handwriting are more difficult to recognize than physiological ones. However, this fact is compensated by a more labor-intensive process of replacing the user, which has a beneficial effect on the level of security of the system. In addition, dynamic characteristics can reflect not only the user's personality, but also his emotional state, which can be useful for analyzing his behavior and motivation.

There are two types of authentication: static and dynamic. In static authentication, the system user is provided with a certain text of fixed length, which the user must enter to confirm his identity. This text can be a password, pin code or another combination of symbols. The advantage of this method is simplicity of implementation and verification. The disadvantage is the possibility of theft or forgetting the text, as well as the need for constant memorization of new texts when they change.

Dynamic authentication is a more complex process of monitoring key presses by the user. Under certain given condition, this can be frequent use of service symbols, which is not characteristic of the user, or too slow typing, the system can restrict access to the account and ask to go through the identification process again. The advantage of this method is the possibility of continuous verification of user authenticity throughout the session with the system, and also

the absence of the need to remember special texts. The disadvantage is the complexity of implementation and configuration of recognition parameters.

Both methods can complement each other depending on the task set by the organization. For example, static authentication can serve as the first level of protection. Dynamic authentication will act as the second one. Thus, it is possible to increase the reliability and security of the identity recognition system.

1.4 Authentication lifecycle

The keyboard recognition lifecycle is a sequence of steps that need to be performed to identify or authenticate a user (Figure 5).

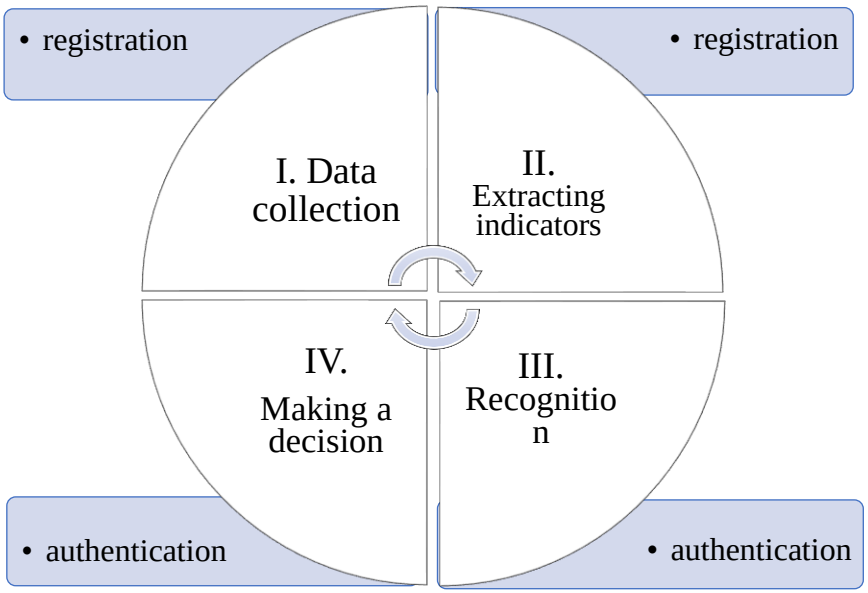

Figure A.5 - Authentication lifecycle

The first stage of the keyboard recognition lifecycle is data collection about the user's keystrokes - this is the first and important stage of the keyboard recognition lifecycle. This stage consists in the fact that on the user's computer a special program or device is installed that records and saves keystrokes that the user makes when entering different texts. These texts can be structured or free, on different languages, etc.

There are two main types of data collection about keystrokes user:

- Hardware
- Software

Hardware way of collecting data about keystrokes of a user is carried out using special devices that are connected between the keyboard and computer or built into the keyboard itself. These devices record all data that is transmitted from the keyboard to the computer, in internal memory or on an external medium. An example of such a device can be a so-called keylogger, which is shown in Figure 6

Figure A.6 - Hardware keylogger

Software data collection about keystrokes of a user is carried out using special programs that are installed on the user's computer and intercept all data that comes from the keyboard to the operating system or applications. These programs can be different in terms of access level and complexity of implementation. For example, there are programs that work in user mode and use API functions of the operating system to get data about keystrokes [6]. There are also programs that work in the kernel of the operating system and have direct access to keyboard drivers [6]. An example of such a program can be «WhatPulse», which is shown in Figure 7

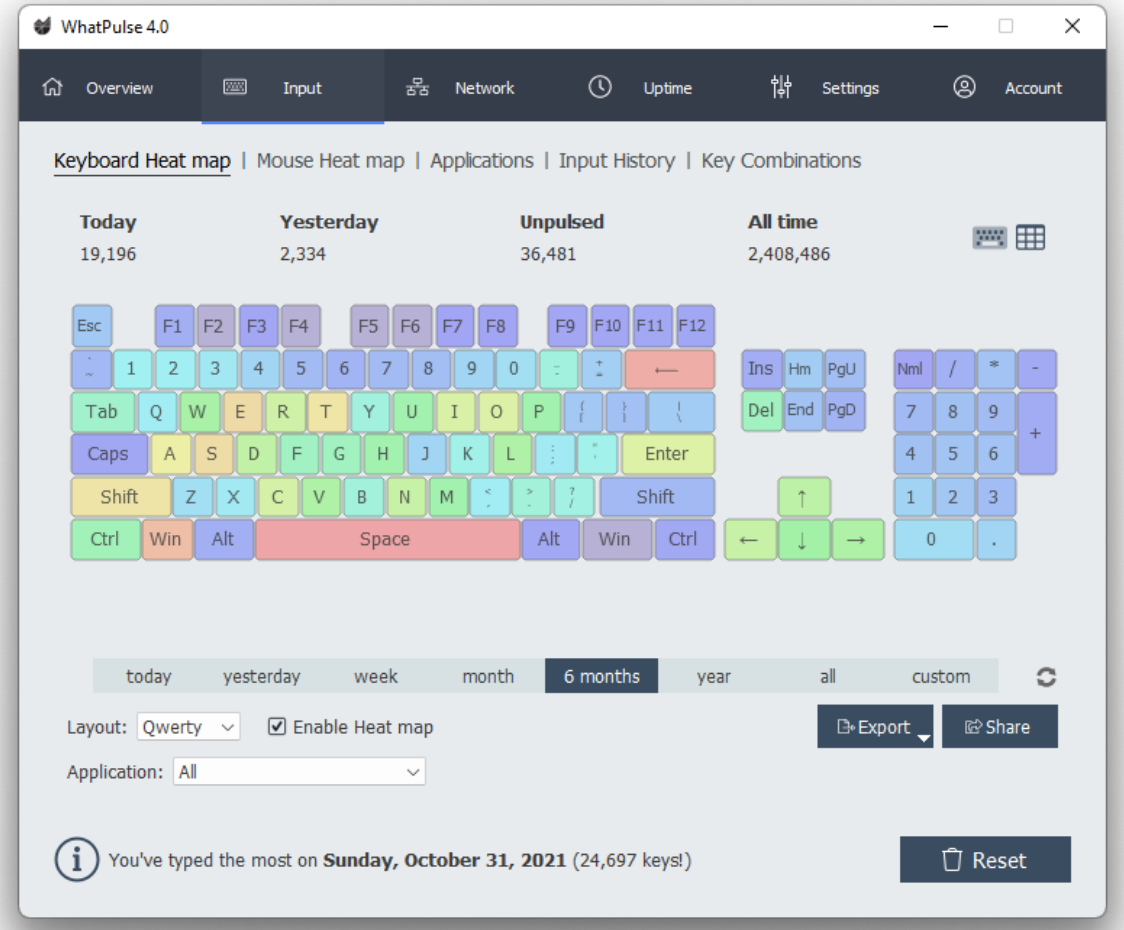

Figure A.7 - Example of software keylogger WhatPulse

Data collection about keystrokes of a user has its own advantages and disadvantages. On the one hand, it allows you to get a large amount of information about the style of typing text by the user, which can be used for his identification and authentication. On the other hand, it can violate privacy and security of the user, if these data fall into the hands of attackers or will be used without the consent of the user.

Extracting features of keyboard handwriting - this is the second stage of the keyboard recognition lifecycle. This stage consists in extracting those characteristics from the collected data about keystrokes of a user that best reflect his individual style of typing text and allow him to distinguish him from other users. These characteristics are called features of keyboard handwriting.

There are many different types of features of keyboard handwriting that can be extracted from data about keystrokes of a user. For example, there are:

- Statistical features that describe the distribution and variability of various parameters of keystrokes, such as typing speed, duration of holding a key, intervals between keystrokes, etc.
- Symbolic features that describe the frequency and sequence of using different symbols on the keyboard, such as letters, numbers, punctuation marks, etc.

Recognition stage - this is the third stage of the keyboard recognition lifecycle. This stage consists in comparing extracted features of keyboard handwriting with reference features or profiles of other users using an algorithm classification that determines which class or category belongs to user. This stage can be implemented using various algorithms and methods, such as:

- Methods based on proximity assessment, which are based on estimating metric distances between current and reference profiles user.
- Support vector method (SVM), which finds an optimal hyperplane that separates extracted features of keyboard handwriting users.
- Neural networks that learn from extracted features of keyboard handwriting and output a vector of probabilities belonging to different classes

Recent research on keyboard handwriting recognition has made it possible to generalize data on continuous authentication efficiency. The generalized data are presented in Table 1. The data were obtained based on research by my supervisor [20, 26] and adapted from review articles [17, 22, 24, 27- 33].

Table A.1 - Dynamic Identification Studies

Year	**Reference, author**	**KD Parameter**	**Method**	**Effectiveness**
2005	[25] Gunetti	FT	Distance (R and A)	FAR-0.005%, FRR- 5%
2010	[32] Shimshon		Clustering	FAR 3,47% и FRR 0%
2011	[33] Messerman		Statistical, distance	FAR-2.02%, FRR-1.84%
2011	[37] Solami		Clustering	Accuracy 100%
2013	[27] Alsultan	Digraph	Fusion	FAR-21%, FRR- 17%
2014	[35] Ahmed	Digraph	Neural networks	FAR-0.015%, FRR-4.82%
2015	[39] Antal	DT, FT	Statistical Reference Vector Method Neural Networks Decision Tree	93.04% Accuracy
2014	[40] Locklear		Statistical	EER 4,55-13,37%
2015	[41] Kang	DT, FT	Clustering, Distance	3.8% EER
2015	[42] Matsubara	Digraph, DT	Distance	99% Accuracy
2016	[23] Morales	Digraph, n-Grath	k-NN nearest neighbor, Distance	90% Accuracy
2017	[31] Alsultan	Digraph, DT	Reference vector method	0.169 FAR, 0.423 FRR
2017	[28] Mondal Bours	Digraph, DT	Distance	182 keystrokes
2017	[36] Goodkind	Contextual features	Naive Bayes	82.2% Accuracy
2017	[30] Ali		k-NN method	EER 3,7%
2021	[34] Chang	DT, FT	CNN-GRU	Accuracy 99% EER 0,0690

The decision-making stage is the fourth and final stage keyboard recognition lifecycle. This stage consists in the fact that based on the result of the recognition

stage, that is, the vector of probabilities user belonging, a final decision is made about whether the user is authentic or fake, emotional or calm, etc. This stage can be implemented using a threshold decision (threshold decision), which compares the probability of user belonging to a certain class with a given threshold and makes a decision depending on whether the probability is greater or less than the threshold.

1.5 Hidden monitoring and dynamic recognition

Hidden monitoring by keyboard handwriting is a process analysis of the temporal parameters of keystrokes by the user for his dynamic recognition (authentication and identification). Dynamic recognition uses various methods to compare the current handwriting of the user with his reference for issuing an authentication decision. The architecture of dynamic (continuous) authentication (Figure 8) includes three subsystems:

- Registration
- Authentication
- Adaptation

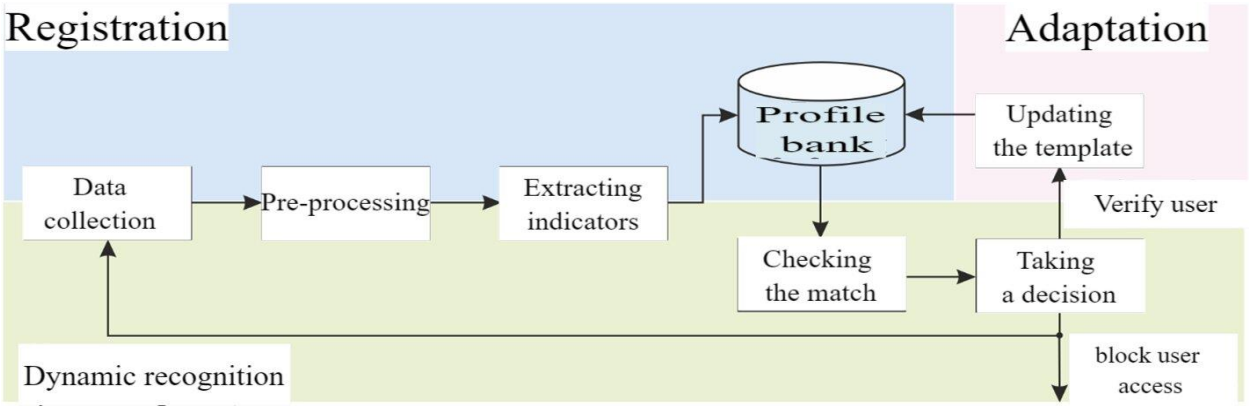

Figure A.8 - Architecture of a continuous authentication system

During the registration process, data collection takes place about keyboard keystrokes, then preprocessing and extraction are performed indicators. All these actions lead to replenishment profile bank (templates). Next, during the process of continuous authentication the matching of templates and making a decision about admission / refusal in accessing the user to the system. Updating the user's

template occurs when confirmation of his identity with subsequent updating of data in the bank profiles [1].

For dynamic recognition of a user, the following data are required: temporal characteristics of typing, such as typing speed, holding time key, intervals between keystrokes, etc.; reference samples of keyboard handwriting of each user of the system, which were recorded earlier; recognition algorithms that compare the entered text and its dynamics with reference samples and issue a decision about user authentication.

For conducting research on dynamic authentication by keyboard handwriting, special data sets are required that contain information about the speed and rhythm of typing by different users. Such data sets can be obtained in two ways collect them locally or download a ready-made dataset.

1.6 Authentication efficiency assessment

Various error rate indicators are used to assess the effectiveness of the keyboard handwriting authentication system.

One of these indicators is False Rejection Rate (FRR), which means an estimate of false rejection or error of type I. FRR determines the percentage of cases when a legitimate user is erroneously rejected.

$$FRR = \frac{FR}{TA + FA + TR + FR} \tag{1}$$

Another indicator is False Acceptance Rate (FAR), which means an error of false acceptance or error of type II. FAR determines the percentage of cases of acceptance of illegal users.

$$FAR = \frac{FA}{TA + FA + TR + FR} \tag{2}$$

In (1) and (2) the following notations are adopted:

- True Accept (TA) - correct admission to the system of a legitimate user.

- True Reject (TR) - correct denial of access to an illegal user.
- False Accept (FA) - false admission of an illegal user.
- False Reject (FR) - false denial of access to a legitimate user.

The sum of the above indicators makes up the total number of attempts.

Hypothetically, FRR and FAR errors vary depending on the level of sensitivity of the algorithm (threshold value) and have an opposite character: when one error decreases, the other increases.

Higher FAR values are usually preferable in systems where security is not a priority, while higher FRR values are preferable in applications with a high degree of protection.

Another indicator is Equal Error Rate (EER), which represents error values when FAR and FRR take equal values and do not depend on the level of sensitivity. ERR is used to determine the overall accuracy of the recognition system.

The listed performance indicators require additional analysis when used in authentication and identification tasks. users. Decision making cannot be based solely on FAR and FRR indicators. It is desirable to have a generalized spatial indicator, supplemented by a threshold value (sensitivity) and limit values of indicators.

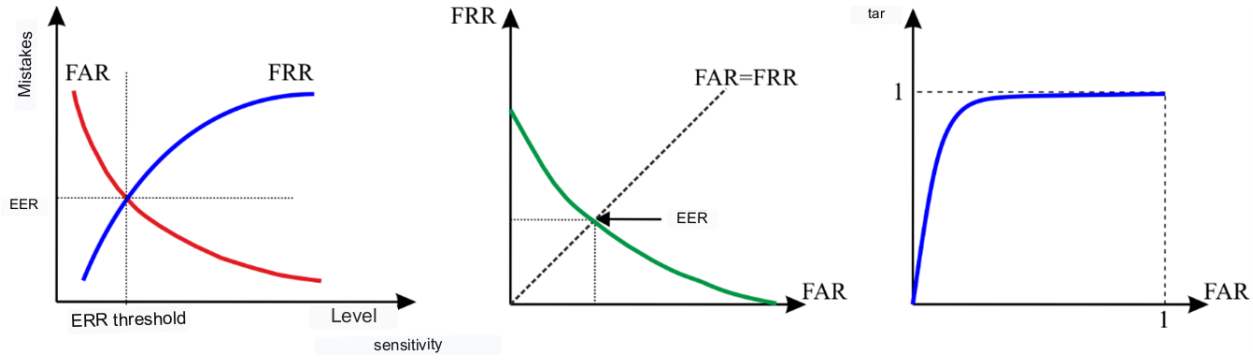

Figure A.9 - Indicators keyboard authentication efficiency