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
Специальность 09.04.01 Информатика и вычислительная техника
ООП Разработка интернет-приложений
Отделение школы (НОЦ) Отделение информационных технологий

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРА

Тема работы
Разработка системы аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка

УДК 004.85.056.5:004.93'1

Обучающийся

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

Руководитель ВКР

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

КОНСУЛЬТАНТЫ ПО РАЗДЕЛАМ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ОСГН ШБИП	Жиронкин С.А.	д.э.н, профессор		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ООД ШБИП	Федоренко О.Ю.	д.м.н., профессор		

ДОПУСТИТЬ К ЗАЩИТЕ:

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

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, социальноэкономические 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) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

ВКР магистра

Студенту:

Группа	**ФИО**
8ВМ01	Затееву Роману Павловичу

Тема работы:

Разработка системы аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка	
Утверждена приказом директора (дата, номер)	№ 34-64/с от 03.02.2022

Срок сдачи студентом выполненной работы:	01.06.2022

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Объектом исследования является система аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка

Перечень подлежащих исследованию, проектированию и разработке вопросов	1. Исследование предметной области; 2. Изучение динамических характеристик клавиатурного почерка; 3. Обзор методов аутентификации пользователей по клавиатурному почерку; 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	Профессор ОСГН ШБИП, д.э.н,. Жиронкин С.А.
Социальная ответственность	Профессор ООД ШБИП, д.м.н., Федоренко О.Ю.
Английский язык	Доцент ОИЯ ШБИП, к.пед.н., Сидоренко Т.В.

Названия разделов, которые должны быть написаны на иностранном языке:

Раздел 2

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	01.03.2022

Задание выдал руководитель:

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

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

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 2021 /2022 учебного года)

Форма представления работы:

ВКР магистра

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Обучающегося:

Группа	ФИО
8ВМ01	Затеева Романа Павловича

Тема работы:

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

Срок сдачи студентом выполненной работы:	01.06.2022

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
01.06.2022	Основная часть	70
01.06.2022	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	10
01.06.2022	Социальная ответственность	10
01.06.2022	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

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

Обучающийся

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ВМ01	Затееву Роману Павловичу

Школа	Инженерная школа информационных технологий и робототехники	**Отделение школы (НОЦ)**	Отделение автоматизации и робототехники
Уровень образования	Магистратура	**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	Бюджет проекта – не более 600 000 руб., в т.ч. затраты по оплате труда – не более 150000 руб. Стоимость материальных и интеллектуальных ресурсов определялась согласно прейскурантам компаний
2. Нормы и нормативы расходования ресурсов	Оклад студента-программиста – 25000 р. 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	Анализ потенциальных потребителей результатов исследования; Анализ конкурентных технических решений; SWOT анализ; Оценка готовности проекта к коммерциализации
2. Разработка устава научно-технического проекта	Цели и результатов проекта; Организационная структура проекта;
3. Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок	Структура работ; План проекта; Бюджет научного исследования; Риски проекта;
4. Определение ресурсной, финансовой, экономической эффективности	Абсолютная эффективность исследования; Сравнительная эффективность исследования;
Перечень графического материала:	
1. «Портрет» потребителя результатов НТИ 2. Сегментирование рынка 3. Оценка конкурентоспособности технических решений	

4. Матрица SWOT 5. График проведения и бюджет НТИ 6. Оценка ресурсной, финансовой и экономической эффективности НТИ 7. Потенциальные риски
Дата выдачи задания для раздела по линейному графику |

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ОСГН ШБИП ТПУ	Жиронкин Сергей Александрович	д.э.н, профессор		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА

«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа		ФИО	
8ВМ01		Затееву Роману Павловичу	
Школа	Инженерная школа информационных технологий и робототехники	**Отделение (НОЦ)**	Отделение информационных технологий
Уровень образования	Магистратура	**Направление/ специальность**	09.04.01 Информатика и вычислительная техника

Тема ВКР:

Разработка системы аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка	
Исходные данные к разделу «Социальная ответственность»:	
Введение – Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика) и области его применения. – Описание рабочей зоны (рабочего места) при разработке проектного решения/при эксплуатации	Объект исследования разрабатываемая система аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка. Область применения: информационные системы Рабочая зона: офис Размеры помещения :6*8м Технические параметры помещения: Центральное отопление, естественная непринудительная вентиляция, освещение искусственное в виде люминесцентных ламп и естественное (2 окна размером 1,5*2м) Количество и наименование оборудования рабочей зоны: персональные компьютер в количестве 3 штук Рабочие процессы, связанные с объектом исследования, осуществляющиеся в рабочей зоне: Разработка приложения с использованием компьютера
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Правовые и организационные вопросы обеспечения безопасности при разработке проектного решения – специальные (характерные при эксплуатации объекта исследования, проектируемой рабочей зоны) правовые нормы трудового законодательства; – организационные мероприятия при компоновке рабочей зоны.	– ГОСТ 12.1.006-84 «Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля» – Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 09.03.2021); ГОСТ 12.0.003-2015 Опасные и вредные производственные факторы. Классификация. Перечень опасных и вредных факторов. – СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания, – СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95, – ГОСТ 12.1.003-83 Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности. Рабочее место при выполнении работ в положении сидя должно соответствовать требованиям ГОСТ 12.2.032-78. – ТОИ Р-45-084-01 «Типовая инструкция по охране труда при работе на персональном компьютере»,

	– ГОСТ 12.1.030-81 Система стандартов безопасности труда (ССБТ). Электробезопасность. Защитное заземление. Зануление. – ГОСТ 12.1.038-82 Система стандартов безопасности труда (ССБТ). Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов, – ГОСТ 12.1.004-91 Система стандартов безопасности труда (ССБТ). Пожарная безопасность. Общие требования/ ГОСТ 17.4.3.04-85 Охрана природы (ССОП). Почвы. Общие требования к контролю и охране от загрязнения/
2. Производственная безопасность при разработке проектного решения: – Анализ выявленных вредных и опасных производственных факторов – Расчет уровня опасного или вредного производственного фактора	Вредные факторы: – недостаточная освещённость рабочей зоны; отсутствие или недостаток естественного света; – повышенный уровень шума; – повышенный уровень электромагнитных излучений; – повышенная напряжённость электрического поля; – повышенная или пониженная влажность воздуха; Опасные факторы: – электрический ток (источником является ПК); – короткое замыкание; – статическое электричество; Требуемые средства коллективной и индивидуальной защиты от выявленных факторов: наушники, устройства для вентиляции и очистки воздуха, источники света, устройства улавливания и очистки воздуха и жидкостей; Расчет: расчет уровня шума в помещении
3. Экологическая безопасность при разработке проектного решения	Воздействие объекта на атмосферу, гидросферу, селитебную зону не происходит. В работе проведён анализ воздействия на литосферу (образование отходов при выходе из строя ПК, возникновения отходов при печати и утилизации ламп).
4. Безопасность в чрезвычайных ситуациях при разработке проектного решения	Возможные ЧС: Природные катастрофы, например, ураган Геологические воздействия (землетрясения, оползни, обвалы, провалы территории и т.д.); Техногенные аварии (пожар) Наиболее типичная ЧС: пожар
Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ООД ШБИП	Федоренко Ольга Юрьевна	д.м.н, профессор		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

РЕФЕРАТ

Выпускная квалификационная работа выполнена на 101 странице, содержит 29 рисунков, 36 таблиц, 26 источников, 2 приложения.

Ключевые слова: клавиатурный почерк, информационная безопасность, аутентификация, биометрия, дистанционное обучение.

Объектом исследования является разрабатываемая система аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка.

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

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 свои 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 корпоративной сети, скрытый мониторинг пользователей корпоративной сети с целью определения подмены оператора.

Оглавление

Введение

События последних лет оказали большой влияние на развитие всех сфер жизни человечества. Многие организации по всему миру ввели удаленный режим работы, а также и другие ограничительные меры, для избежания увеличения количества заболевших сотрудников. Своими действиями они ускорили развитие процессов цифровизации, дистанционного обучения, телемедицины, интернет-торговли и других жизненно важных процессов.

Однако, ускоренное развитие ИТ-отрасли за последние годы привело к неизбежному росту киберпреступности. В 2020 году начала пандемии в мире зафиксирован сильный рост количества преступлений в сфере компьютерной безопасности. В 2021 г в мире зафиксировано резкое увеличение умышленных утечек информации (82% от общего количества) и утечек от действий внешних киберпреступников (до 63%).

Интересным является факт, что доля умышленных утечек данных при участии внутренних нарушителей за 2020 год так же увеличилась больше, чем в 2 раза. При этом Россия по-прежнему занимает лидирующую позицию в мире по количеству утечек информации. Число кибератак в России за 2021 год согласно статистике компании Ivideon выросло на 54 %, при том, что средний показатель по миру 40 %.

Проблема информационной безопасности становится все более актуальной в нынешних реалиях, несмотря на постоянное увеличение способов защиты информации.

Область образования относится к более уязвимым с точки зрения кибербезопасности. Это привлекает университеты для атак хакеров.

С другой стороны, эпидемия привела к сильному сбою функционирования классических систем институтского и школьного образования. Онлайн тесты и экзамены имеют большое значение в электронном обучении. Они позволяют преподавателю получать обратную связь от обучаемого. Этот факт в свою очередь совершенствует процесс

обучения. Однако, бывают случаи, когда студенты используют ряд методов академического мошенничества во время прохождения онлайн тестов. К сожалению, на сегодня не существуют простых методов обнаружения таких подмен.

1 Обзор возможностей использования клавиатурного почерка в онлайн обучении

Резкий переход очного образования в дистанционный формат послужил большому всплеску количества случаев академического мошенничества: подмена личности экзаменуемого, фальсификация результатов, плагиат и т.д. Помимо традиционных способов противодействия академическому мошенничеству, существуют так же негласные рекомендации, которым следуют преподаватели:

- Увеличить индивидуальность заданий
- Заменить тесты на открытые вопросы
- Чаще использовать форматы эссе
- Увеличить количество проверок во время прохождения экзамена

Предложенные выше меры позволяют незначительно снизить количество нарушений, при этом они заметно увеличивают нагрузку на преподавателя.

Альтернативным решением проблемы несанкционированного доступа является использование клавиатурного почерка обучаемого в качестве средства непрерывной аутентификации.

1.1 Система дистанционного обучения Moodle

Moodle относится к свободно распространяемому программному обеспечению (по Стандартной общественной лицензии GNU, созданной в рамках проекта по свободному распространению программного обеспечения). В основном это означает, что Moodle охраняется авторскими правами, но имеются дополнительные права. Разрешается копировать, использовать и модифицировать Moodle при условии, что вы согласны:

– предоставлять ваши дополнения другим;

– не модифицировать и не удалять оригинальную лицензию и авторские права;

– применять эту же лицензию к любым вторичным работам;

Moodle может быть инсталлирована на любом компьютере или сервере, который может запустить веб-сервер, PHP и может поддерживать базы данных типа SQL (например, MySQL). Он может быть запущен под операционными системами Windows и Mac и многих разновидностях Linux.

Архитектура Moodle типична для приложений подобного масштаба и назначения и состоит из 3 слоёв: слоя пользовательского интерфейса (UI), набора библиотек для работы (Libraries) и библиотеки для работы с базой данных и юридическими файлами, которые по сути являются расширениями php (DB libs, File libs).

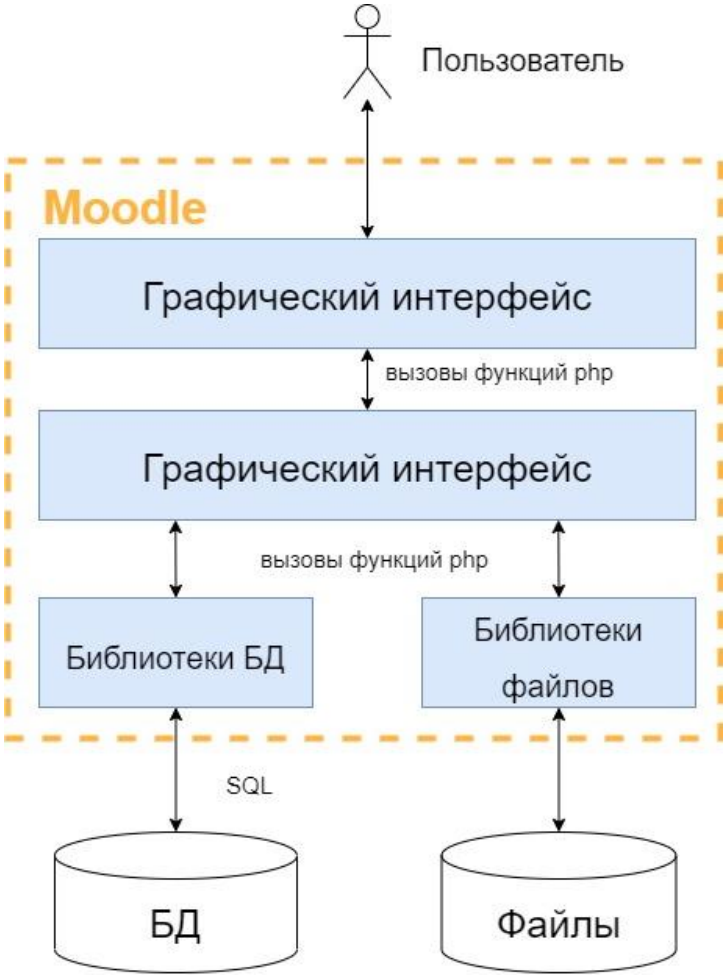


Рисунок 1.1 – Архитектура Moodle

1.2 Прокторинг

В русскоязычном сообществе понятие прокторинг встречается крайне редко. Ввиду этого, у пользователей зачастую отсутствует понимание принципа работы этого инструмента. Прокторинг по своей сути является

отличным инструментом, позволяющим значительно улучшить качество дистанционного образования. Плюсы дистанционного обучения неоспоримы – это минимальные временные затраты на перемещение между домом и место учебы, ввиду этого также снижаются финансовые затраты студентов и преподавателей и т.д. Однако для закрепления полученных знаний обучающимся необходимо выполнять так называемые контрольные срезы. Это могут быть тестирования, контрольные работы, экзамены и далее по списку. Прокторинг позволяет проходить аттестацию так же в режиме онлайн. Существуют виды прокторинга, позволяющие проводить контрольные срезы даже без участия третьего лица – экзаменатора.

Прокторинг — это процедура контроля на онлайн-экзамене или тестировании, где за всем процессом наблюдает администратор — проктор. Администратор наблюдает действиями за действиями экзаменуемого с помощью веб-камеры и видит, что происходит на мониторе его компьютера.

Со времен появления прокторинга технологии не стояли на месте, и сейчас, в наших реалиях, прокторинг проводится тремя способами:

проктор-человек — проктор наблюдает за процессом сдачи экзамена через экран, фиксируя замечания собственноручно.

автопрокторинг — данный способ характеризуется наличием программы, которая автоматически следит на экзаменуемым в реальном времени. Программа может анализировать любые активности пользователя – движения его глаз, рук, головы, анализ звуков в помещении. При этом она автоматически фиксирует нарушения и на их основе готовит отчет. На рынке уже есть готовые решения программ автопрокторинга. Платформы онлайн-образования, при желании, могут внедрять их в свои системы. Плюсом внедрения данных платформ является снижение нагрузки с преподавателей, которые, зачастую, принимают огромное количество экзаменов в период сессии.

человек и программа — третий способ прокторинга, который объединяет в себе два предыдущих. По своей сути он берет все лучшее из

описанных выше способов. Программа позволяет проктору принимать экзамен сразу у нескольких обучаемых. При этом программа автоматически фиксирует некоторые нарушения, которые, по какой-то причине преподаватель не заметил.

1.3 Сценарий взаимодействия разрабатываемой системы и платформы онлайн-обучения Moodle

Для интеграции с платформой Moodle потенциально может быть разработан специальный API, который построен таким образом, чтобы можно было гибко настраивать протокол обмена данными между системой и Moodle в формате JSON.

Сценарий взаимодействия:

1. Студент проходит авторизацию на платформе stud.lms.tpu.ru путем ввода корпоративного логина и пароля.

2. Студент попадает в интерфейс платформы и заполняет обязательные поля в своем профиле. Обязательность заполнения профиля зависит от требований конкретной образовательной организации. В профиль загружается фото, заполняются текстовые поля и загружаются дополнительные документы при необходимости. В профиле студент должен будет заполнить поле «Клавиатурный шаблон», путем ввода текста длиной минимум 1000 символов.

3. После этого студент сразу может приступить к выполнению экзамена. При этом на протяжении всего экзамена будет осуществляться скрытый мониторинг. Если программа зафиксирует подозрительные действия со стороны экзаменуемого –то есть его клавиатурный почерк сильно отличается от его клавиатурного шаблона, то система уведомляет преподавателя о попытке академического мошенничества.

2 Вопросы клавиатурной аутентификации и идентификации

Зачастую для в качестве способа защиты системы от несанкционированного доступа используется двухэтапный процесс верификации:

- Первичная идентификация личности
- Динамическая аутентификация личности

У каждого человека есть индивидуальный ритм набора текста. Ввиду этой особенности клавиатурный почерк может быть использован в биометрической системе распознавания личности. Для наглядности на рисунке представлена клавиатурная динамика 6 пользователей домена университета. Визуальный анализ демонстрирует определенные расхождения между временами нажатия определенных букв на клавиатуре. Данный разброс как раз демонстрирует уникальность клавиатурного ритма 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.

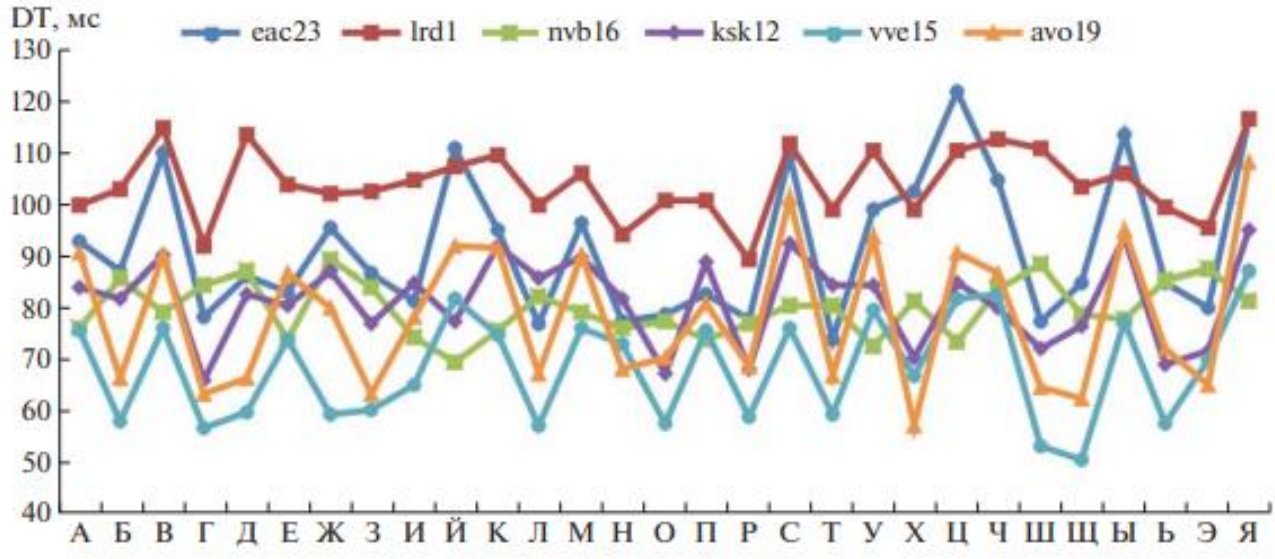


Рисунок 2.1 – Среднее время удержания клавиш пользователями домена, мс.

2.1 Методы аутентификации

Аутентификация — процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Существует большое количество методов аутентификации пользователя. Методы можно разделить на три основные категории, исходя из следующих парадигм [10]:

- что вы знаете (например, пароль, PIN-код)
- чем вы владеете (например, токен, смарт-карта)
- кем вы являетесь (например, отпечатки пальцев)

Последняя парадигма «кем вы являетесь» тесно связана с понятием биометрия. Существуют физиологические (сканер радужной оболочки глаза, сканер лица, отпечаток пала и т.д.) и поведенческие (клавиатурный почерк, шаблон перемещения компьютерной мыши и т.д.)

Аутентификация пользователей по клавиатурному почерку является одним из самых доступных способов предотвращения утечки данных. Данный способ защиты информации сочетает в себе два основных достоинства – это отсутствие необходимости в наличии дополнительного оборудования и низкая стоимость по сравнению с остальными методами биометрии. Все, что требуется от пользователя это наличие стандартной клавиатуры, при этом раскладка не имеет большого значения, и наличие установленное программное приложение. Данный способ аутентификации позволяет осуществлять скрытый мониторинг действий пользователя, то есть пользователь работает в комфортном ему режиме, а программа автоматически считывает его нажатия по клавиатуре. Клавиатурный почерк формируется путем анализа скорости набора, ритма, нажатия клавиш. Важно иметь ввиду, что клавиатурный почерк, как и другие методы биометрии, имеют тенденцию меняться со временем у каждого человека. Однако, вероятность подмены пользователя путем имитации его клавиатурного почерка практически

нереальна. Основные преимущества и недостатки методов аутентификации приведены в таблице ниже

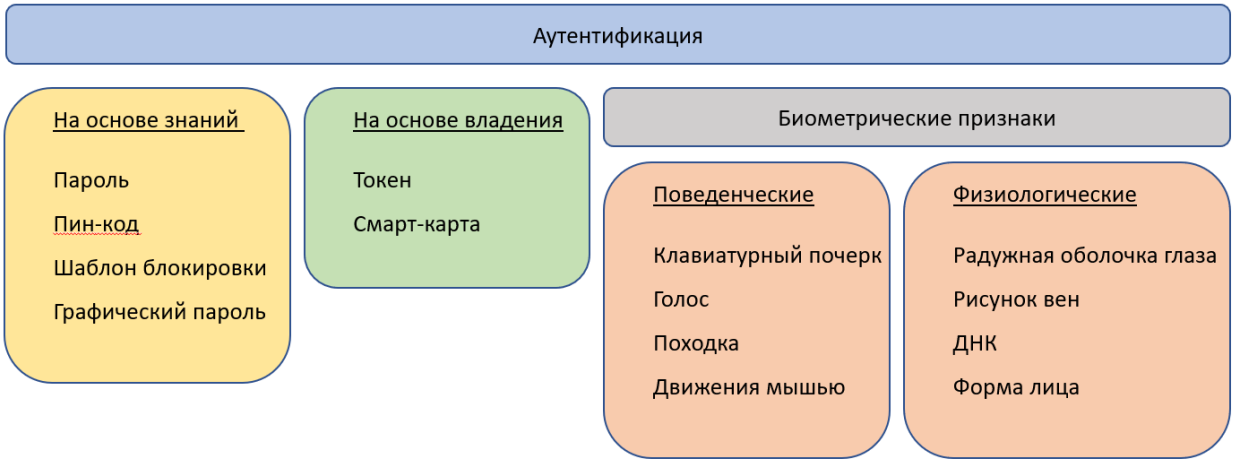


Рисунок 2.2 – Методы аутентификации личности

Таблица 1 – Характеристики методов аутентификации

Метод	Достоинства	Недостатки	Пример
Парольный	1. Простая реализация 2. Однозначное распознавание	1. Может быть забыт или украден	1. Пароль 2. ПИН-код
Атрибутный	1. Простая реализация 2. Не требует затрат	1. Может быть потерян или украден	1. Ключ 2. Смарт-карта 3. Токен
Биометрический	1. Уникальность 2. Невозможно забыть/потерять	1. Стоимость реализации 2. Изменчивость данных независимо от человека	1. Отпечаток пальца 2. Голос 3. Клавиатурный почерк

2.2 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.

Существует два вида аутентификации: статическая и динамическая. При статической аутентификации пользователю системы предоставляется определенный текст фиксированной длинны, который пользователь должен

ввести для подтверждения своей личности. 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.

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.

2.3 Жизненный цикл аутентификации

Непрерывная аутентификация пользователя на основе КП имеет фазу регистрации и фазу аутентификации, как показано на рисунке 2.3.

В процессе этапа регистрации система фиксирует данные о нажатых на клавиатуре клавишах. На следующем шаге система производит вычленение характеристик клавиатурного почерка из собранной статистики – длительности нажатий, пауз между ними, наличия служебных клавиш и так далее. На основе собранных данных формируется или обновляется клавиатурный шаблон пользователя. Далее шаблон сверяется с хранящимся в базе данных происходит процесс аутентификации.

Рисунок 2.3 – Процесс жизненного цикла непрерывной аутентификации

Жизненный цикл непрерывной аутентификации пользователя по динамическим характеристикам клавиатурного почерка включает 4 основных этапа:

I. Сбор данных о динамике нажатия клавиш

Во время первого этапа происходит процесс сбора пользовательских данных при работе с клавиатурой.

Для перехвата сообщений в операционной системе Windows используется технология Windows-hook. Данная технология позволяет фиксировать любые нажатия пользователя на клавиатуре. Точность клавиатурных нажатий измеряется в миллисекундах.

II. Извлечение классификационных признаков

Собранные в процессе первого этапа данные необходимо нормализовать – очистить от недостоверных значений, выбросов, фантомных нажатий и т.д. На основании полученной выборки уже имеет смысл рассчитать скорость набора, паузы, пользовательский ритм. Все эти показатели являются уникальными поведенческими характеристиками.

Показателей КП довольно много, но наиболее популярны у исследователей диаграммы (диграфы) – тайминг двух состояний клавиши [17, 21-23].

На рисунке 2.4 приведены некоторые наиболее часто используемые временные и частотные показатели тайминга.

- DU или время удержания клавиши характеризуется временным интервалом между нажатием и отпусканием клавиши.

- UD или пауза характеризуется временным интервалом между нажатием следующей клавиши и отпусканием предыдущей.

- UU или DD интервал между нажатием или отпусканием одной клавиши и нажатием или отпусканием следующей клавиши соответственно.

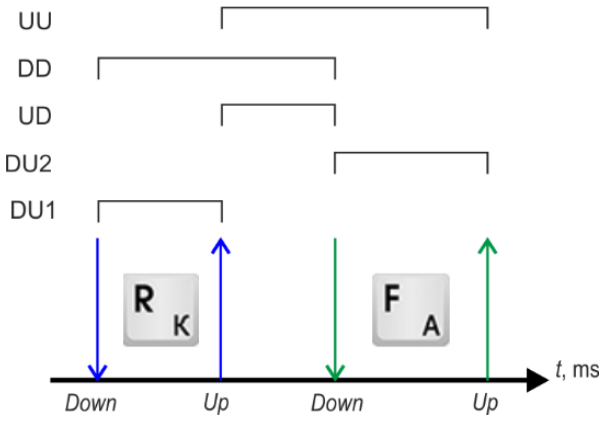


Рисунок 2.4 – Показатели нажатия клавиш в нотации Down Time/Up Time

Подсистемы предварительной обработки данных о тайминге и извлечения характеристик клавиатурного почерка создают массив требуемых значений о любом нажатии кнопки юзером. Дальше на базе массива генерируется клавиатурный профиль юзера для его размещения в базе данных.

III. Распознавание пользователя

Аутентификация — это задача классификации зарегистрированных в системе пользователей. Основные методы и алгоритмы, применяемые для решения задачи классификации пользователей одинаковы как для статической, так и для динамической аутентификации. Их можно разделить на три группы:

- на основе оценки близости;
- методы машинного обучения.
- статистические;

Последние исследования, посвященные распознаванию пользователей по клавиатурному почерку, позволили обобщить данные об эффективности непрерывной аутентификации. Обобщенные данные приведены в Таблице 2. Данные получены на основе собственных исследований [20, 26] и адаптированы из обзорных статей [17, 22, 24, 27- 33].

Таблица 2 – Исследования динамической идентификации

Год	**Ссылка, автор**	**Параметр КП**	**Метод**	**Эффективность**

2005	[25] Gunetti	FT	Расстояние (R и A)	FAR- 0.005%, FRR- 5%
2010	[32] Shimshon		Кластеризация	FAR 3,47% и FRR 0%
2011	[33] Messerman		Статистические, расстояние	FAR- 2.02%, FRR- 1.84%
2011	[37] Solami		Кластеризация	Точность 100%
2013	[27] Alsultan	дираф	Смешанная (Fusion)	FAR- 21%, FRR- 17%
2014	[35] Ahmed	дираф	Нейронные сети	FAR- 0.015%, FRR- 4.82%
2015	[39] Antal	DT, FT	Статистические Метод опорных векторов Нейронные сети Дерево решений	93.04% Точность
2014	[40] Locklear		Статистические	EER 4,55-13,37%
2015	[41] Kang	DT, FT	Кластеризация, Расстояние	3.8% EER
2015	[42] Matsubara	дираф, DT	Расстояние	99% Точность
2016	[23] Morales	дираф, n-граф	k-NN ближайший сосед, Расстояние	90% Точность
2017	[31] Alsultan	дираф, DT	Метод опорных векторов	0.169 FAR, 0.423 FRR
2017	[28] Mondal Bours	дираф, DT	Расстояние	182 keystrokes
2017	[36] Goodkind	Contextual features	Наивный Байес	82.2% Точность
2017	[30] Ali		k-NN метод	EER 3,7%
2021	[34] Chang	DT, FT	CNN-GRU	Точность 99% EER 0,0690

IV. Принятие решения о легитимности пользователя

Данный этап полностью преследует посвящен решению задачи аутентификации пользователя по клавиатурному почерку.

В процессе динамической аутентификации ключевой задачей непрерывного мониторинга является возможность зарегистрированного пользователя постоянно иметь доступ к ресурсам приложения.

Преследуя поставленную цель, было принято решение постоянно отслеживать вероятности возникновения ошибок первого и второго рода – ложного доступа и ложного отказа:

- False Rejection Rate (FRR) – частота ложного отказа в доступе законному (зарегистрированному) пользователю:

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

- False Acceptance Rate (FAR) – частота ложного допуска к системе незаконных 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.

На получаемые значения ошибок FAR и FRR коренным образом влияет чувствительность алгоритма. Путем контроля чувствительности администратор приложения способен принять решение о допуске либо недопуске пользователя в систему. Если система требует высокой степени защиты, тогда будет необходимо выставлять максимально высокие значения чувствительности. В данном случае будут получены большие значения ложно отклоненных пользователей. Если же требуется более упрощенный доступ к

системе, то администратором выставляется маленькие значения чувствительности алгоритма – это соответствует небольшим значениям FRR. Данный компромисс приходится разрешать индивидуально для каждой прикладной задачи.

Следующим по популярности является показатель Equal Error Rate (EER). Данный показатель соответствует значению, получающемуся на пересечении графиков FAR и FRR. При помощи регулирования показателя EER можно контролировать степень защищенности системы в целом.

Вышеописанные показатели являются самыми популярными в научной среде при решении задачи динамической аутентификации по клавиатурному почерку.

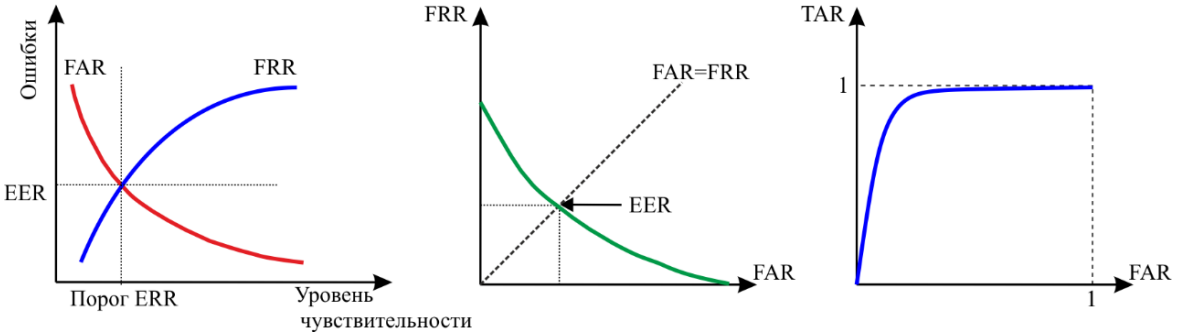


Рисунок 2.5 – Показатели эффективности клавиатурной аутентификации

3 Скрытый мониторинг в дистанционной образовательной системе

Многие учебные заведения ввиду последних событий начали вводить системы управления онлайн-обучением, постепенно перенося уже имеющиеся курсы в онлайн. Итоговая оценка студента за такой курс складывается из его активности в течение семестра и за прохождение экзамена/тестирований в формате онлайн. Однако, на данном этапе возникает вероятность, что студент попытается нелегальным образом улучшить результат своей итоговой оценки. Ряд исследований подтверждает, что успех дистанционного формата обучения коренным образом зависит от использования платформой систем контроля биометрии пользователей во время прохождения онлайн-экзаменов. В частности, использование клавиатурной динамики позволяет максимально точно провести динамическую аутентификацию пользователя, что несомненно, делает огромный вклад в уровень объективность получаемых на экзамене результатов.

3.1 Структура системы непрерывной аутентификации

Особенности непрерывной аутентификации, которые были изложены выше, позволяют рассматривать ее в качестве метода вторичной аутентификации залогиненного пользователя. При этом аутентификация проводится путем скрытого мониторинга действий пользователя в период его работы. Данные методы взяты за основу для дополнительной проверки обучаемого в период онлайн тестирования.

Были выполнены исследования возможности использования непрерывной аутентификации личности. Архитектура экспериментальной системы отображена на рисунке 3.1. Как видно на рисунке, в состав системы входит 3 основных составляющих: регистрация, адаптация и непрерывная аутентификация. При этом составляющие системы работают в непрерывном режиме. Во время процесса регистрации происходит сбор данных, далее предобработка и извлечение показателей. Все эти действия ведут к пополнению банка профилей. Далее во время процесса непрерывной

аутентификации происходит проверка совпадения и принятие решения о допуске либо не допуске пользователя в систему. Обновление шаблона пользователя включается при условии подтверждения его личности с последующим обновлением данных в банке профилей.

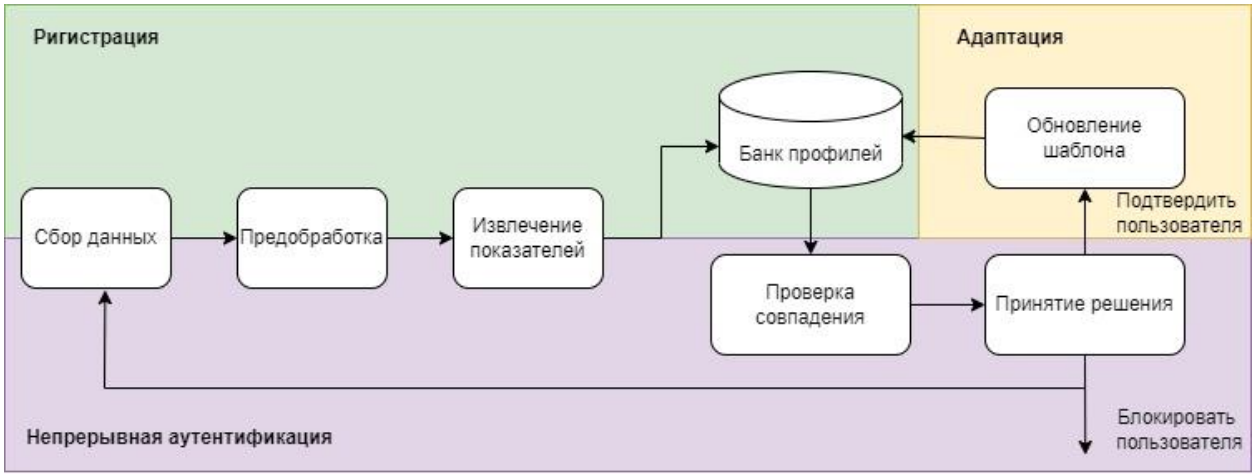


Рисунок 3.1 –Структура системы непрерывной аутентификации

3.1.1Данные для эксперимента

В качестве данных для эксперимента выступают наборы клавиатурных нажатий. Большинство исследований в научной среде использует готовые наборы данных.

В данном исследовании будут использованы данные, собранные на домене университета. Для этой задачи было разработано специальной программное приложение для ОС Windows.

В процессе сбора данных всего было собрано около 10 сессий для 6 пользователей корпоративной сети. Ввиду слишком малого количества исходных данных для эксперимента было принято решение смоделировать сессии уже имеющихся пользователей.

Для моделирования данных было использовано приложение, разработанное в процессе написания выпускной бакалаврской работы. 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 100 сессий на пользователя, каждая сессия содержит в себе 1000 символов. Диаграмма разброса значений сгенерированных сессий для юзера nvb16 изображена на рисунке 3.2.

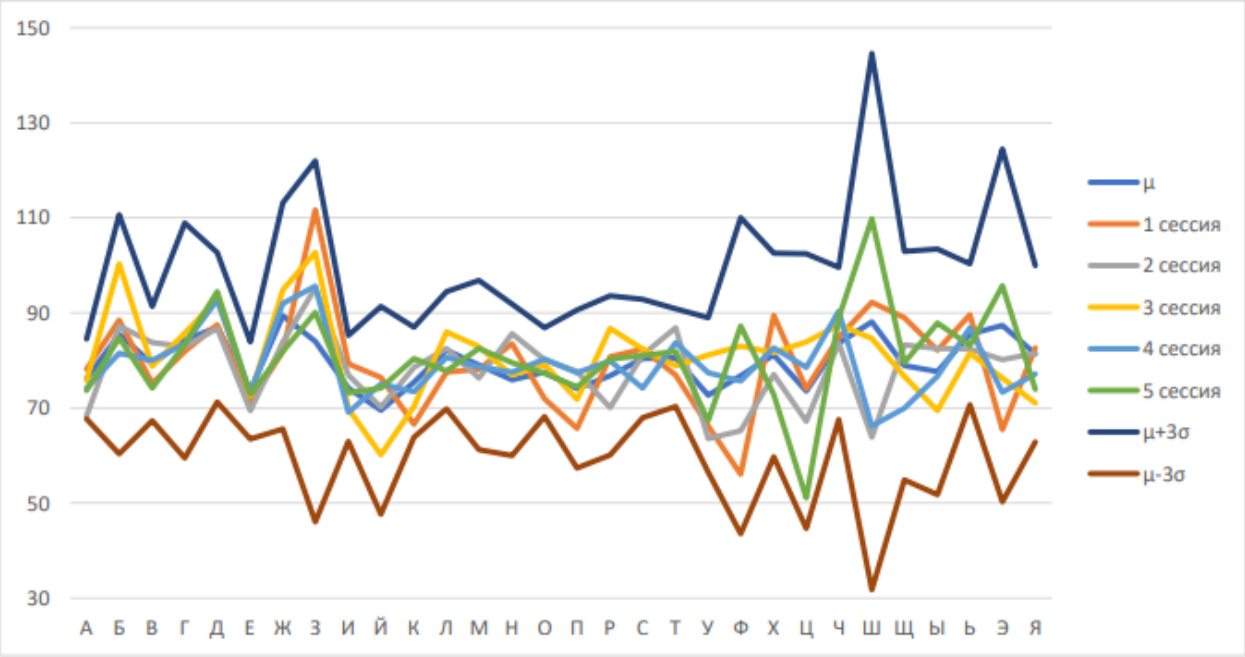


Рисунок 3.2 – Диаграмма разброса значений сгенерированных сессий для пользователя nvb16

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

Рисунок 3.3 – Данные в формате txt

Остальной функционал приложения реализован на сервере. Подобное разделение заметно снижает риски утери данных на менее защищенных клиентских машин.

3.1.2Предварительная обработка данных

Предварительная обработка данных предполагает очистку данных от нежелательных, фантомных нажатий. Подобные данные сильно увеличивают разброс клавиатурных показателей пользователя, что негативно сказывается на качестве работы алгоритма. Слишком короткие сессии, в которых количество набранных символов менее 1000 так же подлежат очистке ввиду отсутствия смысла в их дальнейшей обработке. Одним из важнейших этапов первичной обработки данных является выбор оптимального количества символов для работы. В исследованиях последних лет встречаются различные методики разбиения. В данной работе используется методика «скользящее окно», при этом минимальный размер сессии оставляет 600 символов.

3.1.3Формирование клавиатурных шаблонов

В данном исследовании данные о клавиатурной динамике последнего сеанса конкретного пользователя поступают на сервер в формате txt. Дальше делаются вычисления необходимых статистических характеристик. Результатом данного этапа являются сформированные клавиатурные шаблоны залогиненного пользователя. Если пользователь новый, его клавиатурный шаблон добавляется на сервер. Шаблон же ранее зарегистрированного пользователя обновляется. На серверной части программы шаблоны хранятся в формате .json.

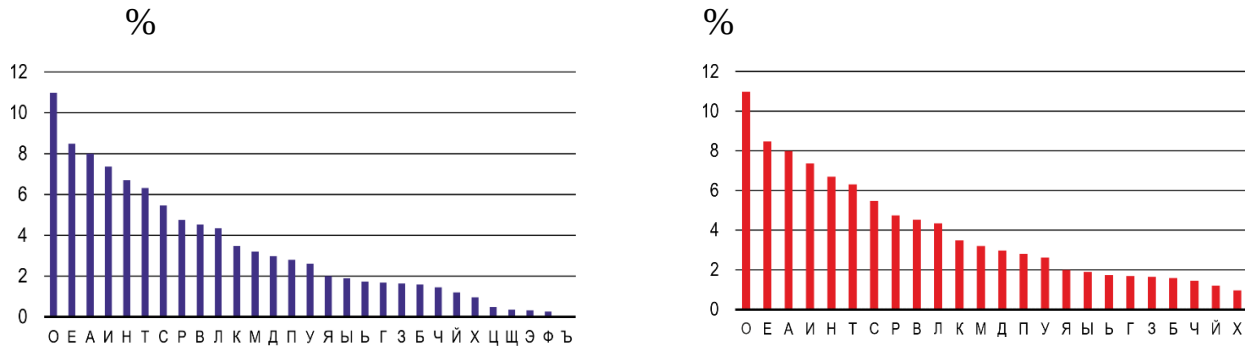
3.1.4Формирование векторного показателя

Этап формирования векторного показателя необходим для повышения достоверности и информативности шаблонов пользователей. С точки зрения алгоритмизации приложения, векторный показатель является наиболее доступным, понятный и простым. Он состоит из средних значений удержания клавиш пользователем.

Дополнительные методы оптимизации

В данной работе для повышения качества временных характеристик, следовательно и алгоритма, была использована частотность букв русского алфавита. Использование частотности позволяет еще больше оптимизировать

алгоритм, ввиду нормирования значения каждой отдельной буквы в клавиатурном шаблоне пользователя. Частотность букв русского алфавита изображена на рисунке 3.4. Как видно из рисунка, некоторые буквы используются русскоязычными пользователями довольно часто, некоторые же очень редко – менее 2% исходя из минимального размера сессии в 1000 символов. В исследовании было принято решение ограничить допустимый порог частоты использования букв, равный 0.5 %. Это означает, что в шаблон пользователя не включены буквы Ц, Щ, Э, Ф, Ъ, Ё, рисунок 3.4, б.



а) б)

Рисунок 3.4 – Частота использования букв русского алфавита

Таким образом, полученный векторный показатель клавиатурного почерка включает в себя 27 букв, средняя частота использования которых не менее 0.5 %.

3.1.5Распознавание легитимных пользователей

Статическая и динамическая аутентификация преследует цель проверки уже аутентифицированного пользователя в сети. Принципиальное различие между этими методами заключается в условии обработки введенного пользователем текста. В статической текст уже заранее предопределен, от пользователя лишь требуется ввести его во время нахождения в своей учетной записи. Динамическая аутентификация проходит полностью скрытно. Пользователь работает в привычном ему формате, в привычных приложениях и в произвольное для него время.

Стоит отметить, что данное исследование принадлежит к решению задачи одноклассовой классификации ввиду отсутствия у системы данных о новом пользователе.

Методы распознавания динамической и статической аутентификации одинаковы. Результаты краткого обзора методов динамической аутентификации на основании исследований последнего десятилетия представлены в таблице 3. Разделение методов распознавания на классы достаточно условно, но можно выделить методы машинного обучения, статистические методы и основанные на оценке метрических расстояний.

В данной работе были использованы следующие методы:

1. Наиболее распространенная функция расстояния. Представляет собой геометрическим расстоянием в многомерном пространстве:

$$\rho(x, y) = \sqrt{\sum_{i}^{n} (x_i - y_i)^2} \tag{1.1}$$

2. Расстояние городских кварталов (манхэттенское расстояние)

Это расстояние является средним разностей по координатам. В большинстве случаев эта мера расстояния приводит к таким же результатам, как и для обычного расстояния Евклида. Однако для этой меры влияние отдельных больших разностей (выбросов) уменьшается (т.к. они не возводятся в квадрат). Формула для расчета манхэттенского расстояния:

$$\rho(x, y) = \sum_{i}^{n} | x_i - y_i | \tag{1.3}$$

3. Метод K-ближайшего соседа

Один из методов решения задачи классификации. В основе метода лежит следующее правило: объект считается принадлежащим тому классу, к которому относится большинство его ближайших соседей. При использовании метода необходимо уметь определять, насколько объекты близки друг к другу. В данном исследовании расстояние было рассчитано между шаблоном пользователя и «новой» сессией. Расстояние рассчитывается исходя из количества ближайших букв.

4 Разработка

4.1 Функциональные возможности системы

Приложение предназначено для решения задачи аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка.

4.1.1Архитектура приложения

Диаграмма классов приложения изображена на рисунке 4.1.

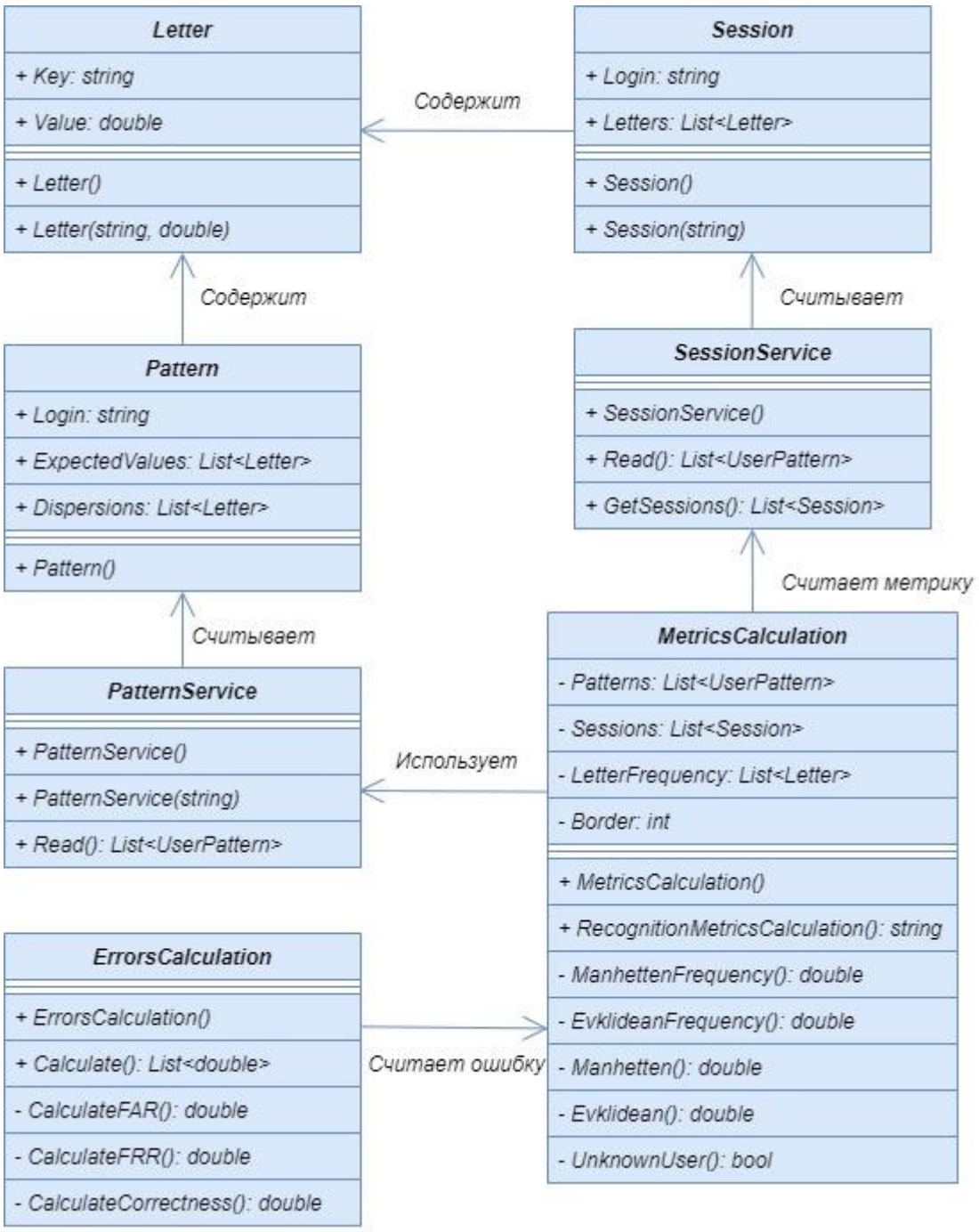


Рисунок 4.1 – Диаграмма классов

Класс PatternService предназначен для получения шаблонов сессий из хранилища данных. Шаблоны сессий записываются в объекты класса Pattern.

Класс SessionService предназначен для получения сессий из хранилища данных. Шаблоны сессий записываются в объекты класса Session.

Класс Letter используется для описания буквы, нажатой пользователем, и временем удержания клавиши.

Класс MetricsCalculation используется для решения задачи идентификации путем расчета различных методов.

Класс ErrorsCalculation предназначен для расчета ошибок методов.

На рисунке 4.2 изображена диаграмма процесса «Идентификация».

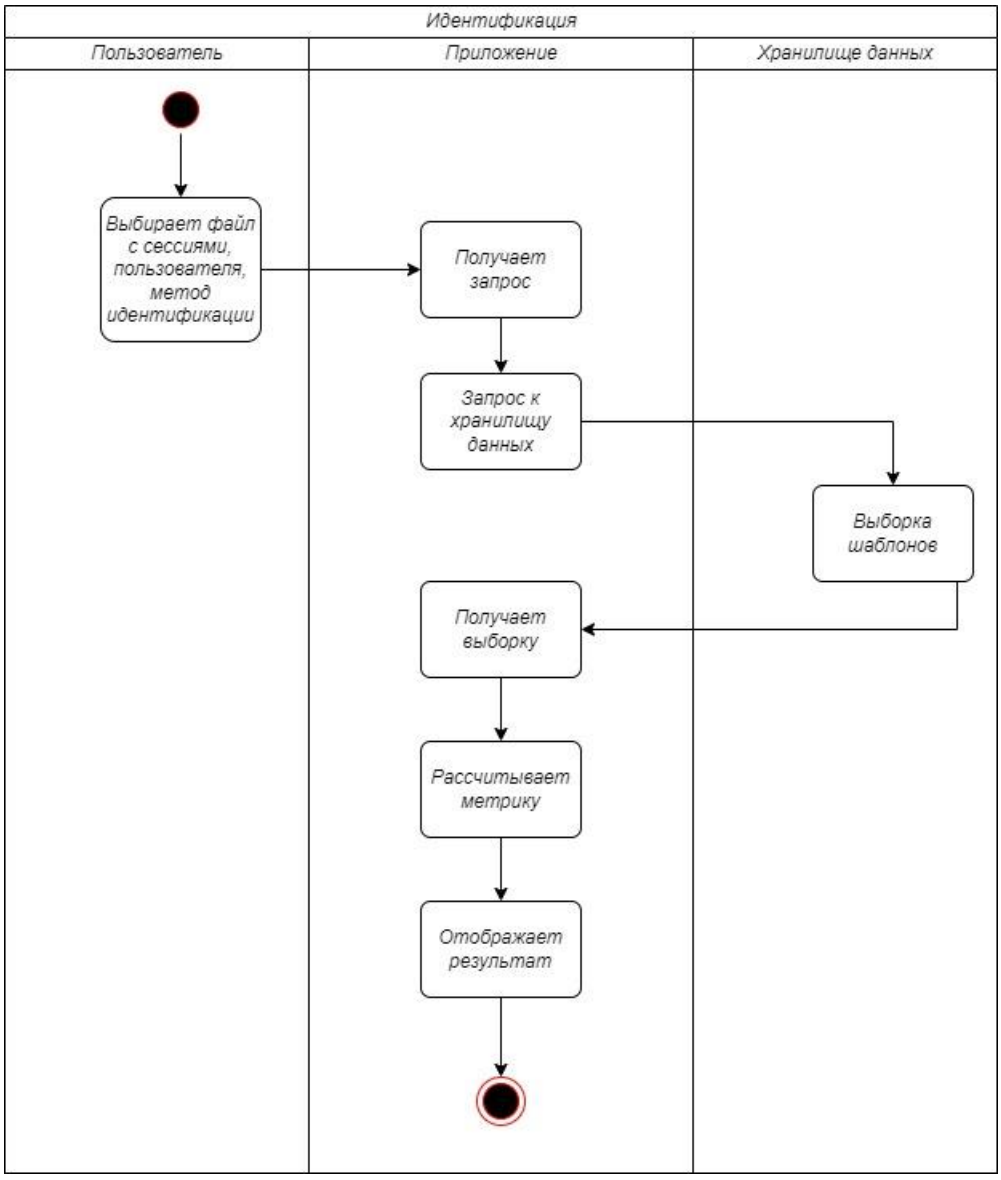


Рисунок 4.2 – Диаграмма процесса «Идентификация»

4.1.2Интерфейс приложения

В состав приложения входят три окна (рисунок 4.3).

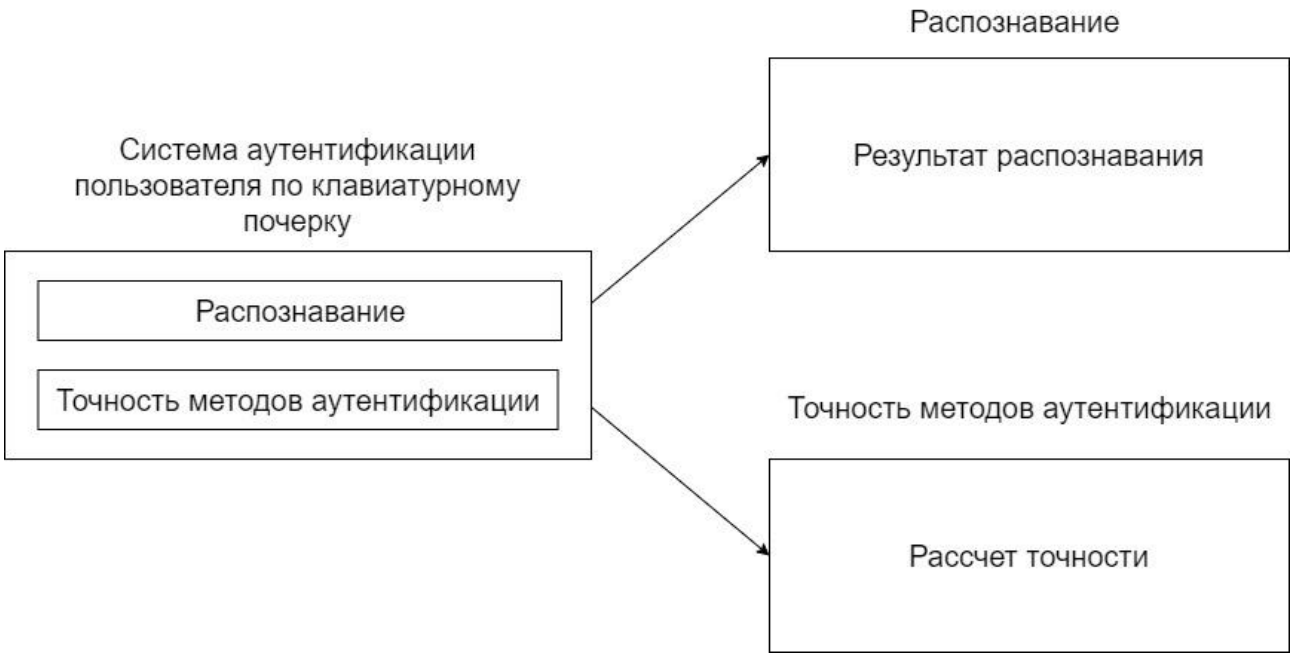


Рисунок 4.3 – Структура приложения

На рисунке 4.4 отображено основное окно приложения.

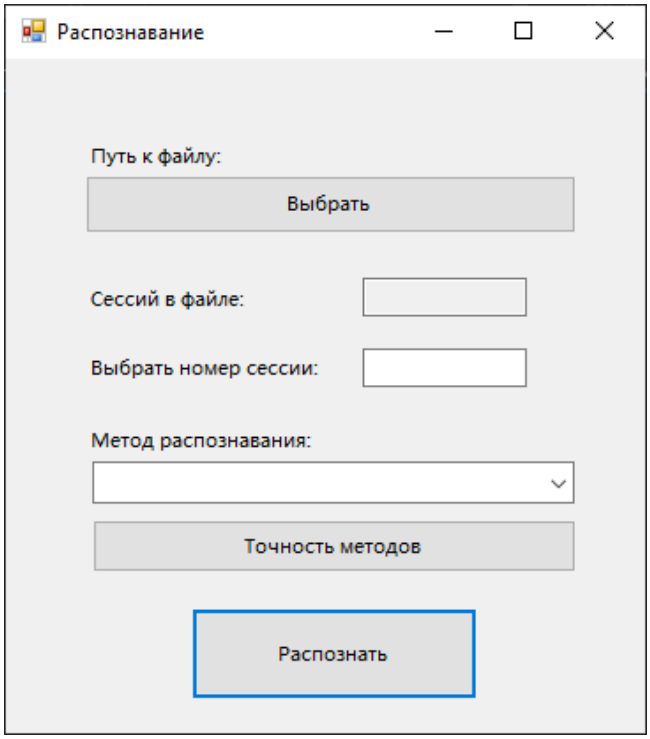


Рисунок 4.4 – Основное окно приложения

Окно приложения имеет в своем составе:

1. Кнопка «Выбрать», предназначена для выбора файла с сессиями пользователей.

2. Поле «Сессий в файле» отображает количество сессий в выбранном файле.

3. Поле «Номер сессии» предназначено для ввода номера сессии для запуска процесса распознавания.

4. Поле «Метод распознавания» предназначено для выбора метода распознавания.

5. Кнопка «Точность методов» при нажатии вызывает форму «Точность методов».

6. Кнопка «Распознать» запускает режим распознавания сессии пользователя.

Для запуска процесса распознавания пользователю необходимо выбрать файл с сессиями, затем выбрать номер сессии, выбрать метод распознавания и нажать на кнопку «Распознать» (рисунок 4.5).

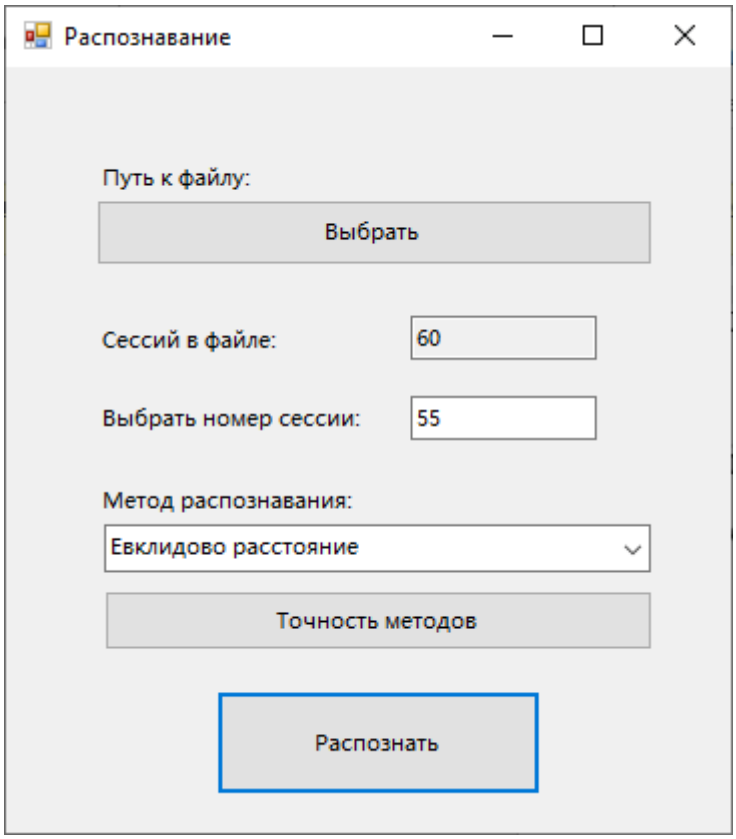


Рисунок 4.5 – Ввод значений для запуска процесса распознавания

Результат распознавания сессии изображен на рисунке 4.6.

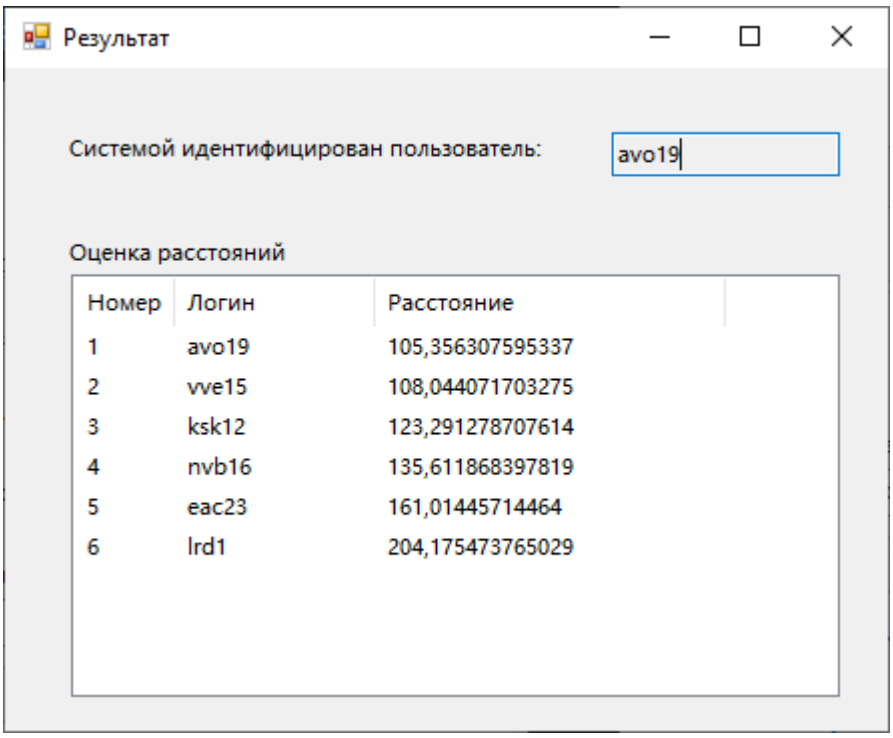


Рисунок 4.6 – Результат распознавания сессии

Для просмотра точности методов распознавания пользователю необходимо нажать на кнопку «Точность методов». После нажатия появится окно (рисунок 4.7).

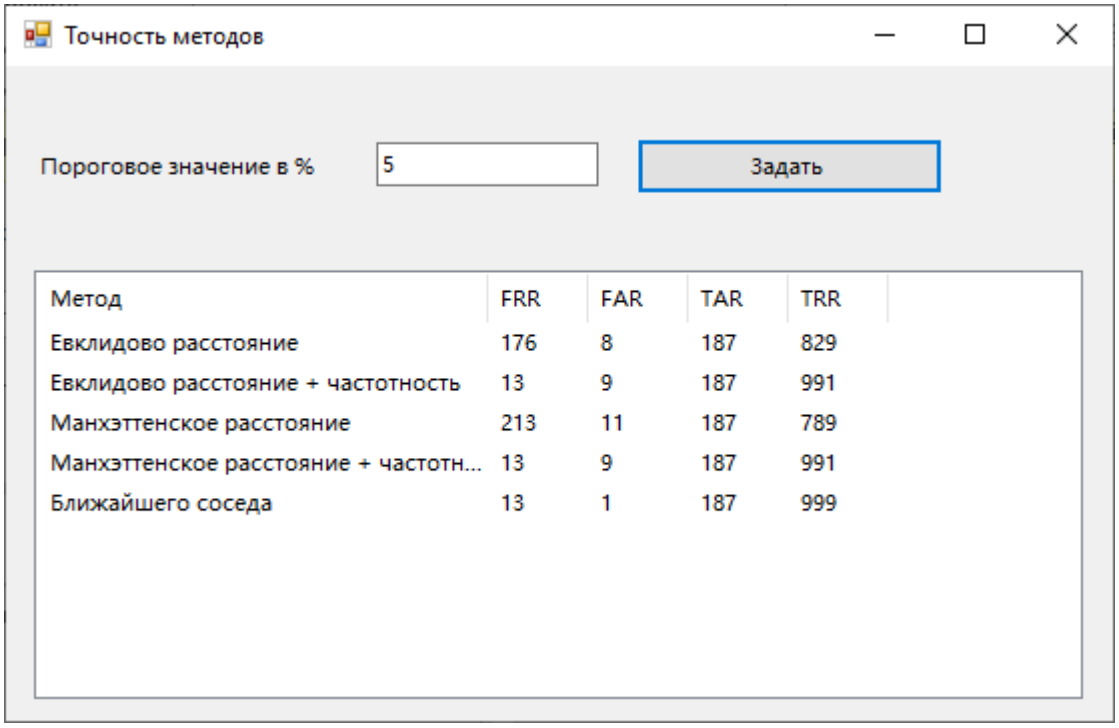


Рисунок 4.7 – Окно «Точность методов» при пороговом значении 5%

На рисунке 4.8 изображено, как задать «Пороговое значение». Для этого необходимо в поле «Граница окрестности шаблона» ввести число от 0 до 100 и нажать на кнопку «Задать».

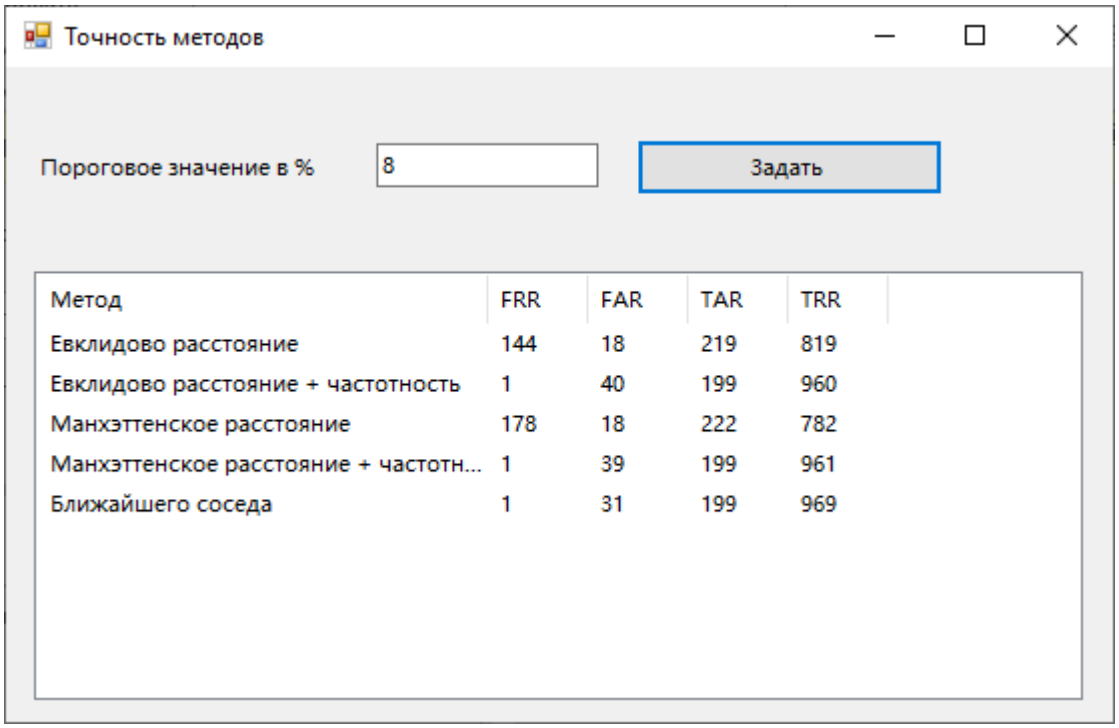


Рисунок 4.8 – Окно «Точность методов» при пороговом значении 8%

4.2 Анализ результатов

Ведущими процессами цикла непрерывной аутентификации юзера при интернет-обучении считаются рубежи регистрации данных и аутентификации личности обучаемого. При регистрации выполняется постоянный сбор данных о клавиатурных нажатиях и дальнейшее извлечение характеристик клавиатурной динамики.

Шаблоны юзеров домена динамические, так как они сформированы на базе мониторинга случайных нажатий на клавиатуру и не связаны с определенными приложениями операционной системы. Изучения проведены на основе домена государственного института.

Северная часть системы рассчитывает средние значения ВУК в текущем сеансе для каждой буквы и обновляет шаблон в базе данных. Для каждого юзера в базе данных хранятся шаблоны его 10 последних сеансов. Данный подход позволяет выслеживать изменения клавиатурного почерка,

связанный различным психоэмоциональным состоянием, пользователя, усталостью и т.д.

Рисунок 4.9 отображает шаблоны пользователей университетского домена. По оси абсцисс расположены буквы русского алфавита. По оси ординат расположены времена удержания клавиш в миллисекундах. Данная визуализация позволяет наглядно увидеть клавиатурные шаблоны шести пользователей домена.

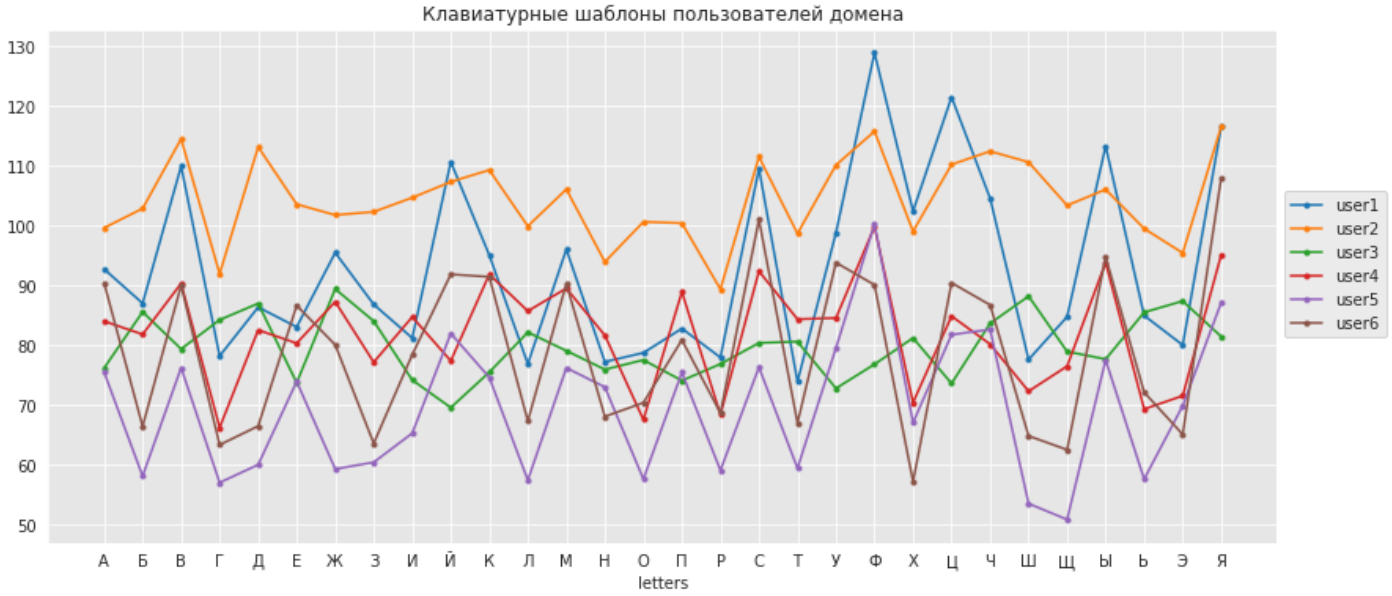


Рисунок 4.9 – Визуализация шаблонов пользователей домена

Как видно из рисунка, каждый клавиатурный шаблон уникален. Это исходит из того, что у каждого пользователя своя скорость и ритм набора печатных символов на клавиатуре. Рисунок 4.10 иллюстрирует плотности распределения времен удержания клавиш.

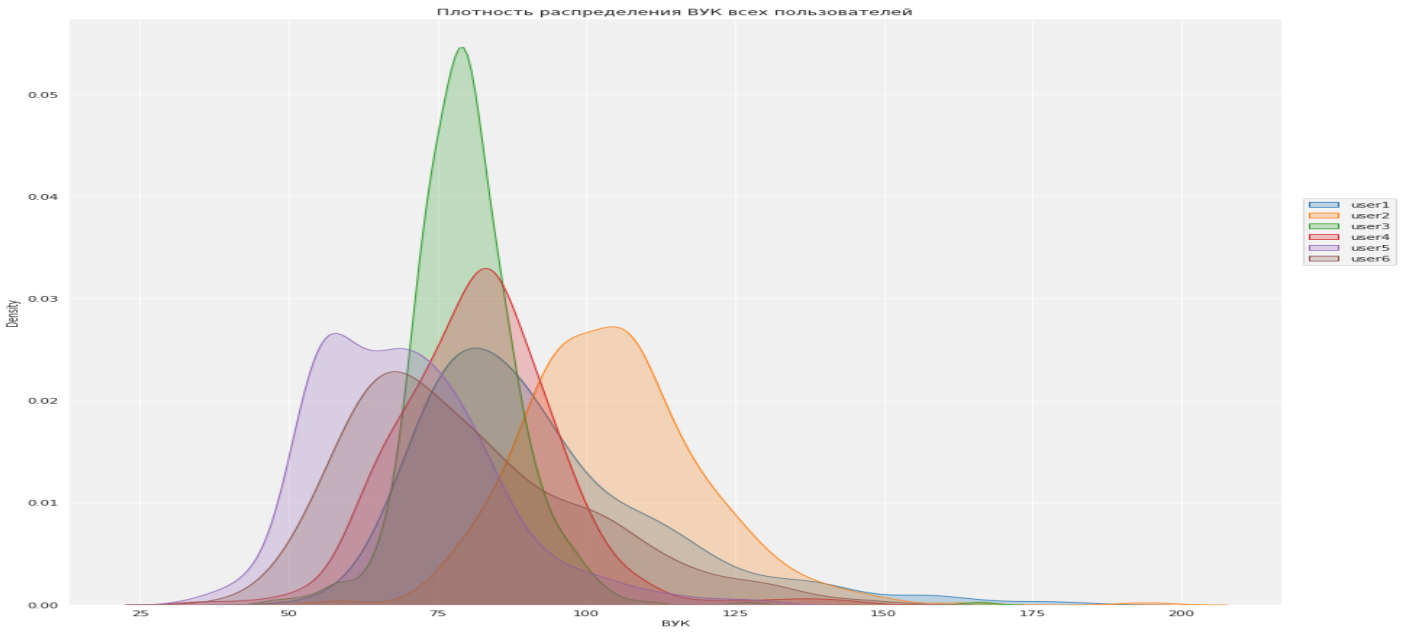


Рисунок 4.10 – Плотность распределения

У пользователя User5, как показывают рисунки 4.9 и 4.10, хорошо развиты навыки работы с клавиатурой. При этом, у него, как у большинства пользователей, владеющих навыками быстрой печати, встречаются наложения, когда предыдущая клавиша еще не отпущена, а следующая уже нажата.

Гистограмма пользователя User03 отличается малым разбросом и средней скоростью набора. Это полностью совпадает с картиной на рисунке 19 и подтверждается малыми отклонениями между модой и медианой ряда.

Из рисунков 4.9, 4.10 следует, что средние значения пользователей User04 и User01 примерно равны. При этом распределение пользователя User01 имеет «тяжелые хвосты», то есть мода и медиана для этого ряда значительно различаются между собой, как и для пользователя User06.

На следующем этапе распознавания производится подтверждение легитимности пользователя системы. Для этого происходит сопоставление шаблона зарегистрированного пользователя с его шаблоном, хранящимся в базе данных. При этом возможны два исхода:

- шаблон текущего сеанса пользователя совпадает с его шаблоном из базы данных;

- шаблон текущего сеанса пользователя не совпадает с его шаблоном из базы данных.

В данном исследовании совпадение шаблонов проанализировано с использованием метода k-ближайших соседей и оценки расстояний на основе Евклидовой и Манхэттенской метрик.

Важнейшей характеристикой в любом методе является порог принятия решения. Пороговое значение выбирается исходя из приоритета поставленных задач. Низкие пороговые значения, соответствуют малой разнице между текущем и хранящимся в базе данных шаблоном. Это обеспечивает сложный доступ всех пользователей в систему. Высокие порог обеспечивает более простой доступ в систему для всех пользователей. Основные визуальные инструменты ошибок первого и второго рода для метрики «Расстояние городских кварталов» приведены на рисунке 4.11.

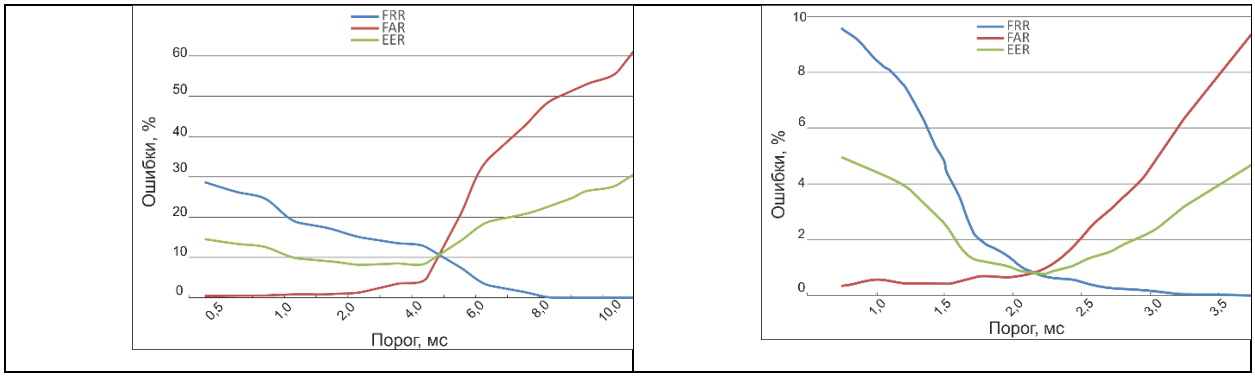


Рисунок 4.11 – Оценка эффективности распознавания пользователей

На рисунке 4.11-б) FAR, FRR и EER представлены с учетом поправки на частотность букв русского алфавита, 4.11-а) – без учета. Как видно из рисунка, достигнуто заметное уменьшение ошибок, в среднем на порядок при разных пороговых значениях. В таблице 3 приведено сравнение ключевых значений данного исследования.

Таблица 3. Сравнительный анализ показателей эффективности новый

	расстояние				метод
	Евклидово		Манхэттенское		kNN
	частотность		частотность		
	-	+	-	+	
ERR, (0-100)%	10,8	0,99	10,1	0,79	0,54
порог (FAR=FRR), мс	4,8	2,3	4,8	2,2	2,8
Accuracy, (0-100)%	90,87	99,20	90,41/83,41	99,20/99,4	99,45

Precision, (0-1) Recall, (0-1)	0,83 0,71	0,98 0,83	0,83/0,73 0,68/0,74	0,98/0,98 0,83/0,94	0,98 0,96

Сравнительный анализ показал, что показатели, полученные на основе Манхэттенской и Евклидовой метрик, мало отличаются между собой. Метод kNN показал немного лучшие показатели ERR=0.54 % при пороговом значении 2,8 мс. Такие результаты потребовали длительного подбора параметров алгоритма.

Полезным инструментом для понимания событий при распознавании легитимных пользователей и шпионов является матрица соответствия, таблица 4. На пересечении строк и столбцов матрицы показаны возможные верные (T) или ложные (F) исходы распознавания: принять (A) или отклонить (R) пользователя. Столбцы соответствуют исходу распознавания, строки – реальным пользователям.

Таблица 4. Матрица соответствия ошибок

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

Указанные в таблице 3 показатели, вычисляются следующим образом:

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

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

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

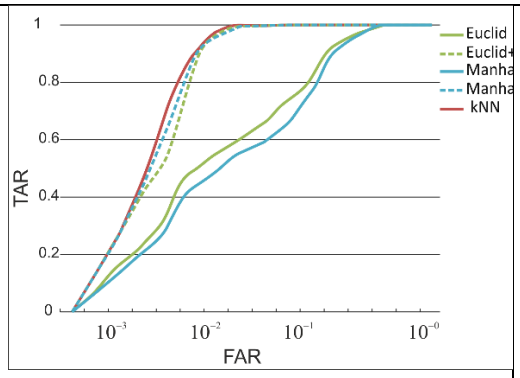
Все три показателя отражают точность аутентификации «своего» пользователя. Однако, акценты каждого показателя разные.

- Accuracy – показывает точность верных допусков и отклонений.
- Precision – показывает отношение верно допущенных пользователей ко всем принятым системой.

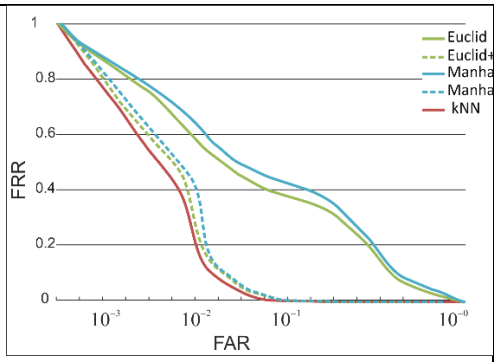
- Recall – показывает долю допущенных пользователей из всех легитимных.

Показатель Accuracy выражать в процентах, а Precision и Recall изменяются в диапазоне (0-1).

На рисунке 4.12 представлены кривые DET и ROC для каждого метода, использованного в исследовании.



а) ROC



б) DET

Рисунок 4.12 – Оценка эффективности распознавания пользователей

Данные для DET и ROC-кривых представлены в логарифмическом масштабе, что позволяет оценить порядок погрешностей для достижения целевых значений. Так, 100 % подтверждение легитимности (TAR=1) достигнуто при FAR=10-2, т.е. на уровне 1-9 % ошибочно принятых системой с учетом частотности алфавита и KNN-метода. Без учета частотности этот показатель много хуже до 50 % FAR. Такие же закономерности по ошибкам и методам подтверждает и DET-кривая.

В ходе практической части для каждого метода аутентификации была также создана таблица в Excel, куда были занесены результаты расчетов программы. На основе полученных таблиц были построены графики зависимости ошибок распознавания друг от друга. Расчеты удовлетворяют условию:

$$TRR + FRR + TAR + FAR = 1200 \quad (6)$$

На основе полученных таблиц были построены графики ошибок FAR, FRR и ERR (Приложение Б).

Результаты расчетов показали самое маленькое значение Eual Error Rate у методов «Евклидово расстояние с поправкой на частотность букв русского языка» и «Манхэттенское расстояние с поправкой на частотность букв русского языка». При этом EER составил 12.8 мс. Следом по возрастанию EER идет метод «K-ближайших соседей» со значением 14.7 мс. Дальше идет метод «Евклидово расстояние» со значением EER равным 25 мс. Заключающим стал метод «Манхэттенское расстояние» при EER равным 26 мс.

В ходе исследования выяснилось, что частотность букв русского языка значительно повышает точность методов распознавания. У методов «Евклидово расстояние» и «Манхэттенское расстояние значения» EER уменьшились в два раза, что существенно упрощает процесс аутентификации. Допустимые значения ошибок первого и второго рода, а также значения EER необходимо подбирать исходя из конкретной прикладной задачи.

5 Финансовый менеджмент

Введение

Система аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка предназначена для защиты информации от несанкционированного доступа. Ввиду последних событий переход к дистанционному обучению резко увеличил спрос на платформы, предназначенные для онлайн обучения. Целевым рынком для системы являются компании, заинтересованные в контроле доступа к информации: военные предприятия, производственные предприятия, софтверные компании, торговые компании, научно-исследовательские центры, учебные заведения и т.д.

Цель раздела данного раздела – оценка эффективности, рисков, экономической успешности проекта.

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.

Цель данной НИР спроектировать и разработать систему аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка.

5.1 Оценка коммерческого и инновационного потенциала НТИ

Перед планированием работы, определением ресурсного и экономического потенциала разработки программно-алгоритмического комплекса, следует уделить особое внимание оценки коммерческого потенциала и перспективности новой разработки в целом, дать характеристику и определить сегмент рынка, на который будет ориентироваться компания, при продаже данной продукции.

5.1.1Потенциальные потребители результатов исследования

Сегментацию рынка возможно провести по следующим критериям.

Размер предприятия

1) Крупные;
2) Средние;
3) Малые;

Степень секретности информации

1) Высокая;
2) Средняя;
3) Низкая;

Карта сегментирования рынка следующая (т 5).

Таблица 5 – Карта сегментирования рынка продаж

Степень защиты информации / Размер компании	Высокая	Средняя	Низкая
Крупные			
Средние			
Малые			

Coursera	ТПУ	Репетитор

В качестве наиболее значимых были выбраны следующие критерии: степень секретности информации и размер предприятия. Пользователи образовательной платформы Coursera

В результате анализа конкурентных программных продуктов было установлено, что относительно небольшая конкуренция наблюдается в случае, если предприятие малое и степень секретности информации низкая либо средняя.

5.1.2Анализ конкурентных технических решений

Для оценки конкурентоспособности разработки проводится анализ существующих решений, позволяющих анализировать и распознавать клавиатурный почерк. Для сравнительного анализа были выбраны:

1. Облачное приложение «CleverControl» для контроля активности сотрудников на компьютерах в режиме реального времени
2. Система мониторинга работы подчиненных «StaffCop», включающая в себя модуль для анализа клавиатурного почерка

Сравнение технических и экономических характеристик этих продуктов представлено в таблице 6. «CleverControl» обозначен К1, а «StaffCop» - К2.

Таблица 6 – 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							
1. Удобство в эксплуатации	0,18	4	1	5	0,72	0,18	0,9
2. Возможность подключения в сеть ЭВМ	0,11	4	1	5	0,44	0,11	0,55
3. Потребность в ресурсах	0,07	5	5	2	0,35	0,35	0,14
4. Функциональные возможности	0,15	3	1	5	0,45	0,15	0,75
5. Быстродействие	0,1	5	5	4	0,5	0,5	0,4
Экономические критерии оценки эффективности							
1. Возможность доработки	0,06	5	3	4	0,3	0,18	0,24
2. Цена	0,2	4	5	1	0,8	1	0,2
3. Уровень проникновения на рынок	0,1	1	2	4	0,1	0,2	0,4
4. Обслуживание после продажи	0,02	3	1	5	0,06	0,02	0,1
5. Предполагаемый срок эксплуатации	0,01	5	3	4	0,05	0,03	0,04
Итого	**1**	**39**	**27**	**39**	**3,77**	**2,72**	**3,72**

Таким образом, разрабатываемая система распознавания клавиатурного почерка имеет преимущества перед аналогами по следующим критериям:

1) Цена;
2) Потребность в ресурсах памяти;
3) Быстродействие;
4) Предполагаемый срок эксплуатации;
5) Возможность подключения в сеть ЭКМ;
6) Удобство в эксплуатации.

Недостатками системы являются:

1) Уровень проникновения на рынок;
2) Функциональные возможности;
3) Послепродажное обслуживание.

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

5.1.3SWOT анализ

SWOT-анализ используется для выявления сильных и слабых сторон проекта, а также его возможностей и угроз выполнения.

На первом этапе SWOT-анализа были описаны сильные и слабые стороны проекта, возможности и угрозы реализации. Матрица SWOT-анализа представлена в таблице 7.

Таблица 7 – SWOT-анализ

	Сильные стороны научно-исследовательского проекта:	**Слабые 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 С6. Графическое представление данных	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 В5. Реализация версий программы для Linux и MacOS		
Угрозы: У1. Увеличение конкуренции У2. Прекращение поддержки руководителей проекта У3. Отсутствие интереса к продукту на рынке		

Второй этап SWOT-анализа включает выявление соответствий между сильными и слабыми сторонами проекта и окружающей средой. Интерактивные матрицы соответствия представлены в таблицах 8-11.

Таблица 8 – Интерактивная матрица соответствия сильных сторон и возможностей

Сильные стороны проекта							
Возможности проекта		Сл1	Сл2	Сл3	Сл4	С5	С6
	В1	-	+	+	0	-	+
	В2	-	+	+	+	-	-
	В3	+	-	+	+	+	+
	В4	-	+	-	-	-	-
	В5	0	+	-	+	-	-

Таблица 9 – Интерактивная матрица соответствия сильных сторон и угроз

Сильные стороны проекта							
Угрозы проекта		Сл1	Сл2	Сл3	Сл4	С5	С6
	У1	-	-	-	-	0	-
	У2	-	-	-	-	-	-
	У3	-	+	-	-	-	-

Таблица 10 – Интерактивная матрица соответствия слабых сторон и возможностей

Слабые стороны проекта				
Возможности проекта		Сл1	Сл2	Сл3
	В1	+	-	+
	В2	-	-	+
	В3	-	-	-
	В4	+	-	+
	В5	-	+	+

Таблица 11 – Интерактивная матрица соответствия слабых сторон и угроз

Слабые стороны проекта				
Угрозы проекта		Сл1	Сл2	Сл3
	У1	+	+	+
	У2	+	-	+
	У3	+	+	-

Третий этап включает в себя составление итоговой матрицы SWOT-анализа на основе полученной таблицы SWOT-анализа и интерактивных таблиц (таблица 12).

Таблица 12 – Итоговая матрица SWOT-анализа

	Сильные стороны научно-исследовательского проекта:	**Слабые 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 С6. Графическое представление данных	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 В5. Реализация версий программы для Linux и MacOS	1. В1С2С3С6 – Простота расширения функционала системы. 2. В2С2С3С4 – Простота и низкая стоимость изменения каналов связи. 3. В3С1С3С4С5С6 – Широкие возможности для увеличения спроса. 4. В4С2 – Ускорение разработки. 5. В5С2С4 – Расширение рынка сбыта.	1. В1Сл1Сл3 – Необходимость доработки и оптимизации алгоритма. 2. В2Сл3 – Модификация приложения требует времени. 3. В4Сл1Сл3 – Новые разработчики должны сначала исследовать существующий код и алгоритм. 4. В5Сл2Сл3 – Реализация поддержки новой ОС потребует
Угрозы: У1. Увеличение конкуренции У2. Прекращение поддержки руководителей проекта У3. Отсутствие интереса к продукту на рынке	1. У3С2 – Недостаточно системный подход к разработке ПО	1. У1Сл1Сл2Сл3 – Конкуренты смогут разработать ПО сходного функционала более быстро и качественно. 2. У2Сл1Сл3 – Руководитель проекта недоволен реализацией. 3. У3Сл1Сл2 – Продукт не удовлетворяет ожидания пользователей.

5.1.4Оценка готовности проекта к коммерциализации

Для оценки готовности проекта были определены показатели по вопросам в таблице 13. 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 13 – 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
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 выше среднего. 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 Инициализация проекта

В данном этапе фиксируются начальные цели, содержание и финансовые ресурсы. Определяются заинтересованы стороны, которые могут повлиять на конечный результат проекта. Эта информация закрепляется в уставе проекта.

5.2.1Цели и результаты проекта

Были определены заинтересованные стороны (14). Заинтересованные стороны – это лица или организации, которые активно заинтересованы и/или могут быть как положительно, так и отрицательно затронуты в результате проекта.

Таблица 14 – 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.
Платформы онлайн-образования	Увеличение контроля качества результатов тестирований и экзаменов

В таблице 15 представим цель и результаты проекта, а также критерии их достижения и требования к результатам.

Таблица 15 – Цели и результаты проекта

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

Ожидаемые результаты:	Функционирующая система аутентификации пользователя по клавиатурному почерку
Критерии приёмки результатов:	Точность распознавания составляет не менее 95%
Требования к результатам:	1. Разработать систему аутентификации пользователя по клавиатурному почерку 2. Точность алгоритмов аутентификации должна составлять не менее 95%

5.2.2Организационная структура проекта

В таблице 16 отражена организационная структура, роль и функции каждого члена команды.

Таблица 16 – 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	Затеев Роман Павлович, Томский политехнический университет, магистр	Исполнитель	Разработка ПО, документирование результатов.	540

5.2.3Ограничения и допущения

При разработке системы необходимо учитывать некоторые ограничивающие факторы. Они представлены в таблице 17.

Таблица 17 – Ограничения проекта

Фактор	**Ограничения / допущения**
Бюджет	100 000
Источники	Личные средства разработчика
Сроки	27.01.2022 – 04.06.2022

Дата утверждения плана управления проектом	27.01.2022
Дата завершения	04.06.2022
Прочие ограничения	Время работы участников проекта не может превышать 4 часа в день

5.3 Планирование управления НТИ

Для организации и систематизации работы выпускника был сформирован план работ. Данный этап обеспечил своевременное и эффективное выполнение задания выпускной квалификационной работы.

Для осуществления разработки, был сформирован ряд работ и назначены должности исполнителей для каждого этапа работы (таблица 18).

Таблица 18 – Перечень работ по проекту

№ работы	Наименование работы	Исполнители работы
1	Выбор научного руководителя магистерской работы	Затеев Р.П..
2	Составление и утверждение темы магистерской работы	Кочегурова Е.А., Затеев Р.П..
3	Составление календарного плана-графика выполнения магистерской работы	Кочегурова Е.А.
4	Подбор и изучение литературы по теме магистерской работы	Затеев Р.П..
5	Анализ предметной области	Затеев Р.П..
6	Разработка методики и алгоритма распознавания	Затеев Р.П..
7	Проектирование системы распознавания пользователя по клавиатурному почерку	Затеев Р.П..
8	Сбор и моделирование тестовых данных	Затеев Р.П..
9	Разработка системы распознавания пользователя по клавиатурному почерку	Затеев Р.П..
10	Тестирование системы	Затеев Р.П..
11	Оценка эффективности полученных результатов	Затеев Р.П..
12	Согласование выполненной работы с научным руководителем	Кочегурова Е.А., Затеев Р.П..

13	Выполнение других частей работы (финансовый менеджмент, социальная ответственность)	Затеев Р.П..
14	Подведение итогов, оформление работы	Затеев Р.П..

5.3.1План проекта

В виде диаграммы Ганта был составлен линейный график работ по проекту, в котором отражены даты начала и окончания, длительность и ответственных лиц по каждому этапу работ (рис.5.1).

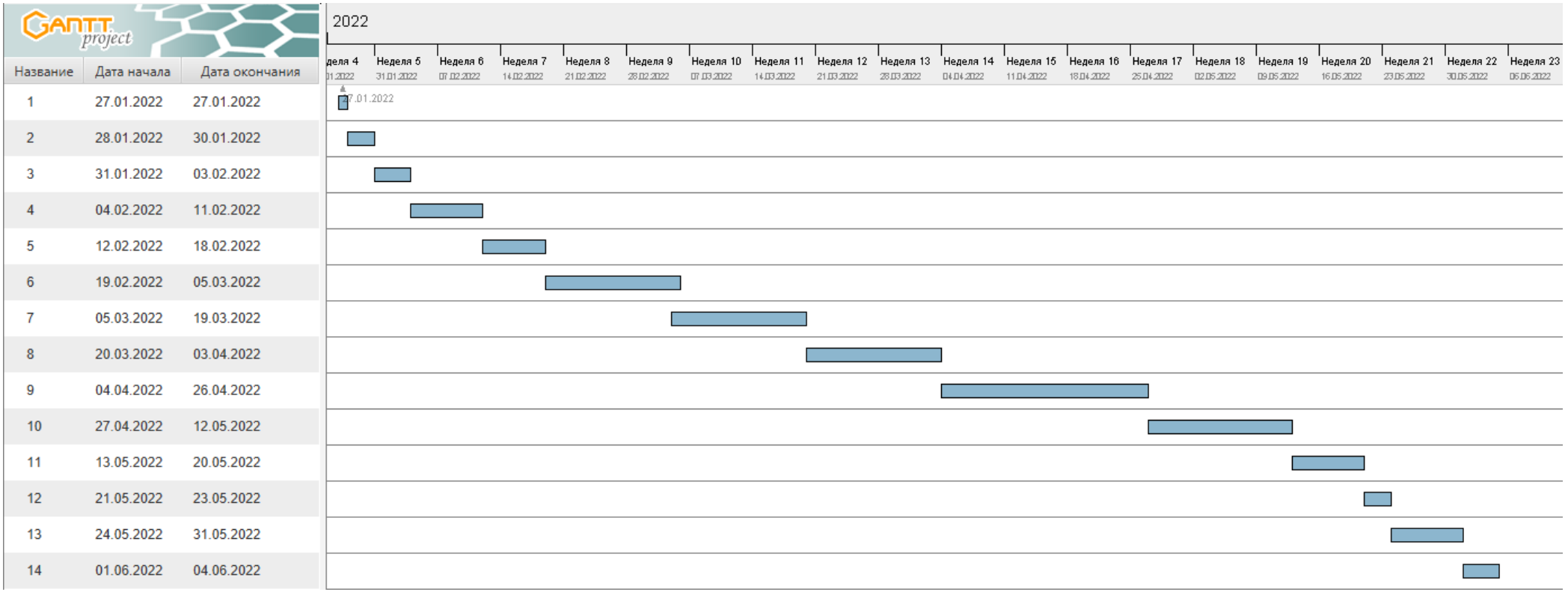


Рисунок 5.1 – Диаграмма Ганта

5.3.2Бюджет НТИ

Бюджет научного исследования должен в полной мере отражать все планируемые расходы на его выполнение. Бюджет формируется по следующим статьям: сырьё и материалы, специальное оборудование, основная заработная плата, дополнительная заработная плата, отчисления в социальные фонды, командировки, оплата работ сторонних организаций.

Сырьё и материалы

Данная статья затрат включает в себя затраты на приобретение сырья, материалов, полуфабрикатов и комплектующих со стороны. Также в эту статью включаются транспортные расходы, равные 15 % от общей стоимости материальных затрат.

Общая сумма материальных затрат включает в себя только затраты на канцелярские принадлежности (300 руб.), для которых не учитываются транспортные расходы.

Таким образом, общая сумма материальных затрат составляет 300 руб.

Специальное оборудование

В качестве специального оборудования подразумеваются лицензии на ПО и затраты на приобретение ПК для разработки.

№ п/п	Наименование	Кол-во, шт.	Цена единицы, руб.	Общая стоимость, руб.
1	ПК	1	50000,00	50000,00
Итог:				50000.00

Основная заработная плата

Заработная плата работника включает основную заработную плату, и дополнительную заработную плату:

$$З_{зп} = З_{осн} + З_{доп}.$$ **(Ошибка! Используйте вкладку "Главная" для применения**

мой_заголовок_1 к тексту, который должен здесь отображаться..1)

Где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата (12-20 % от $З_{осн}$).

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

$$З_{осн} = З_{дн} \cdot T_p .$$

(Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..2)

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:

$$З_{дн} = \frac{З_м \cdot М}{F_д} .$$

(Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..3)

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 19).

Таблица 19 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Студент
Календарное число дней	365	365
Количество нерабочих дней - выходные дни - праздничные дни	118	118
Потери рабочего времени - отпуск - невыходы по болезни	48	48
Действительный годовой фонд рабочего времени	199	199

Месячный должностной оклад работника:

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

(Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..4)

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 20.

Таблица 20 – Расчёт основной заработной платы

Исполнители	$З_{тс}$, руб.	$k_{пр}$	$k_д$	$k_р$	$З_м$, Руб	$З_{дн}$, руб.	$Т_р$, раб.	$З_{осн}$, руб.
Руководитель	33 664,00	0,3	0,15	1,3	63 456,64	3 316,33	14	46 428,58
Студент	25 000,00	0,3	0,15	1,3	43 750,50	2286.45	60	137187.49
Итого:								183616.07

Дополнительная заработная плата

Расчет дополнительной заработной платы ведется по следующей формуле:

$$З_{доп} = k_{доп} \cdot З_{осн}.$$ (**Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться.**.5)

Где $k_{доп}$ – коэффициент дополнительной заработной платы (на стадии проектирования принимается равным 0,12 – 0,15).

Примем коэффициент равный 0,12. Результаты расчета приведены в таблице 21.

Таблица 21 – Расчёт дополнительной заработной платы

Исполнители	Дополнительная заработная плата, руб
Руководитель	5 571,43
Студент	15 101,98
Итого	20 673,41

Отчисления во внебюджетные фонды

Величина отчислений во внебюджетные фонды определяется исходя из следующей формулы:

$$З_{внеб} = k_{внеб} \cdot (З_{осн} + З_{доп}).$$ (**Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться.**.6)

Где $k_{внеб}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования и пр.).

Результаты расчета приведены отчислений и общий итог по фонду заработной платы приведены в таблице 22.

Таблица 22 – Общий итог по зарплатному фонду

Исполнитель	**Коэффициент отчислений во внебюджетные фонды**	**Основная заработная плата, руб.**	**Дополнительная заработная плата, руб.**	**Отчисления во внебюджетные фонды**
Руководитель проекта	0,3	46 428,58	5 571,43	15 600,00
Студент		137187,49	15 101,98	45686.84
Итог:		183616.07	20 673,41	61286.84

Научные и производственные командировки

Данный вид работ не запланирован, расчёт статьи расходов не требуется.

Контрагентные расходы

Привлечение сторонних организаций не запланировано, расчёт статьи расходов не требуется.

Накладные расходы

Накладные расходы учитывают прочие затраты организации, не попавшие в предыдущие статьи расходов: печать и ксерокопирование материалов исследования, оплата услуг связи, электроэнергии, почтовые и телеграфные расходы, размножение материалов и т.д. Их величина определяется по следующей формуле:

$$З_{накл} = k_{накл} \cdot (З_{осн} + З_{доп}) .$$

(Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен

здесь отображаться..7)

Где $k_{накл}$ – коэффициент, учитывающий накладные расходы.

Примем коэффициент равным 0,8. Таким образом сумма накладных расходов составит (таблица 23):

Таблица 23 – Расчёт накладных расходов

Исполнитель	**Коэффициент учёта накладных расходов**	**Основная заработная плата, руб.**	**Дополнительная заработная плата, руб.**	**Накладные расходы**
Руководитель проекта	0,8	46 428,58	5 571,43	41 600,00
Студент		137187,49	15 101,98	121831.57
Итог:		183616.07	20 673,41	163431.57

Бюджет НТИ

Статьи, рассчитанные в предыдущих пунктах, сведены в таблице 24.

Таблица 24 – Итоговый бюджет НТИ

	Статьи						
Сырье и материалы, руб.	Специальное оборудование, руб.	Основная заработная плата, руб.	Дополнительная заработная плата, руб.	Отчисления на социальные нужды, руб.	Научные и производственные, руб.	Контрагентные расходы, руб.	Накладные расходы, руб
300,00	50000,00	183616.07	20 673,41	61286.84	0,00	0,00	163431.57
	Итог:						479307,89

5.3.3Риски проекта

Риски проекта включают в себя различные неопределенные события, которые могут возникнуть в проекте и вызвать негативные последствия. Риски представлены в таблице 25.

Таблица 25 – 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
2	Недостаток знаний не позволит создать продукт, отвечающий требованиям	Продукт ненадлежащего качества	1	5	Средний	Изучение специализированной литературы	Недостаток знаний у разработчика
3	Создание продукта, не соответствующего ожиданиям заказчика	Не востребованность системы	1	2	Низкий	Тщательное изучение требований и проектирование системы	Изменение требований к системе

5.4 Определение ресурсной, финансовой, экономической эффективности

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

Определение интегральных показателей эффективности проведём в сравнении со следующими аналогами:

1. Система онлайн прокторинга ProctorEdu;
2. Система онлайн прокторинга Examus.

Интегральный финансовый показатель разработки определяется как:

$$I_{\text{финр}}^{исп.i} = \frac{\Phi_{\text{р}i}}{\Phi_{\max}}.$$ (**Ошибка! Используйте**

вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..8)

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 26.

Таблица 26 – Расчёт интегрального финансового показателя

Продукт	Φ_{pi}	Φ_{max}	$I_{\text{финр}}^{исп.i}$
НТИ	500 000,00	3 500 000,00	0,14
ProctorEdu	1 300 000,00		0,37
Examus	3 500 000,00		1

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

$$I_{pi} = \sum a_i \cdot b_i .$$

(Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..9)

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 27.

Таблица 27 – Сравнительная оценка характеристик продуктов

Критерии	Весовой коэффициент параметра	НТИ	ProctorEdu	Examus
1. Надежность алгоритмов	0,3	3	5	5
2. Быстродействие	0,3	3	3	4
3. Удобство	0,1	4	4	5
4. Функциональность	0,2	3	4	5
5. Интерфейс	0,1	4	4	5
ИТОГО	1	3,4	4	4,8

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

$$I_{исп.1} = \frac{I_{р-исп1}}{I^{исп.1}_{финр}}, \quad I_{исп.1} = \frac{I_{р-исп1}}{I^{исп.1}_{финр}} \text{ и т.д.}$$

(Ошибка! Используйте вкладку "Главная" для применени

я мой_заголовок_1 к тексту, который должен здесь отображаться..10)

Сравнение интегрального показателя эффективности вариантов исполнения разработки позволит определить сравнительную эффективность проекта (таблица 28) и выбрать наиболее целесообразный вариант из предложенных.

Таблица 28 – Расчёт интегрального показателя эффективности

	$I_{\text{финр}}^{исп.i}$	$I_{р-исп}$	$I_{исп}$
НТИ	0,14	3,4	24,29
ProctorEdu	0,37	4	10,81
Examus	1	4,8	4,8

Сравнительную эффективность проекта определим по следующей формуле:

формуле:

$$Э_{ср} = \frac{I_{финр}^{р}}{I_{финр}^{а}};$$ (**Ошибка! Используйте**

вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться..11)

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

$I^{p}_{mэ}$ – интегральный показатель разработки;

$I^{a}_{mэ}$ – интегральный технико-экономический показатель аналога.

Таким образом сравнительная эффективность проекта с аналогами:

1. В сравнении с ProctorEdu $Э_{ср} = 2.25$;
2. В сравнении с Examus $Э_{ср} = 5.06$;

Вывод

В ходе работы были выявлены направления возможного развития проекта для повышения его конкурентоспособности. Разработка данного проекта является целесообразной с точки зрения экономической успешности, эффективности и рисков.

6 Социальная ответственность

Введение

Объектом исследования данной ВКР является система распознавания пользователя по клавиатурному почерку. Как разработка системы, так и её эксплуатация происходит в офисном помещении. Офис, а также находящаяся в нем компьютерная и оргтехника, оказывают неблагоприятное воздействие на окружающую среду. Кроме того, при несоблюдении санитарных норм и правил, возможно, негативное влияние на здоровье сотрудников офиса.

Данный раздел посвящен вопросам производственной безопасности и гигиене труда, соблюдению санитарных норм и защиты сотрудников от негативного воздействия среды. Рассматриваются меры по охране окружающей среды и ресурсосбережению. Предлагается ряд решений для исключения возникновения несчастных случаев при разработке и эксплуатации системы распознавания клавиатурного почерка.

Также исследуются правовые вопросы обеспечения безопасности, связанные с использованием разработанной системы.

6.1 Правовые и организационные вопросы обеспечения безопасности

6.1.1Особенности законодательного регулирования проектных решений

Режим труда и отдыха для вида трудовой деятельности на ПЭВМ регламентируется ТК РФ [0], СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания [0] и ТОИ Р-45-084-01 «Типовая инструкция по охране труда при работе на персональном компьютере» [13].

Работа в офисе относится ко второй категории тяжести труда – работы выполняются при оптимальных условиях внешней производственной среды и при оптимальной величине физической, умственной и нервно-эмоциональной

нагрузки. Продолжительность рабочего дня работников не должна превышать 40 часов в неделю.

Продолжительность непрерывной работы за компьютером без регламентированного перерыва не должна превышать 1 час.

Рекомендуется делать перерывы в работе за ПК продолжительностью 10-15 минут через каждые 45-60 минут работы.

Во время регламентированных перерывов целесообразно выполнять комплексы упражнений и осуществлять проветривание помещения.

Эффективными являются нерегламентированные перерывы (микропаузы) длительностью 1-3 минуты. Регламентированные перерывы и микропаузы целесообразно использовать для выполнения комплекса упражнений и гимнастики для глаз, пальцев рук, а также массажа. Комплексы упражнений целесообразно менять через 2-3 недели.

Не рекомендуется работать за компьютером более 6 часов за смену. Для того чтобы ПЭВМ соответствовали нормам, осуществляется производственный контроль и надзор внутри предприятия-производителя. Эксплуатирующие предприятия также следят за характеристиками используемой аппаратуры.

6.1.2Организационные мероприятия при компоновке рабочей зоны

В соответствии с ГОСТ 12.2.032-78 Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования [0] рабочий стол может быть любой конструкции, отвечающей современным требованиям эргономики и позволяющей удобно разместить на рабочей поверхности оборудование с учетом его количества, размеров и характера выполняемой работы. Выполнение требований на данном рабочем месте отражено ниже в таблице 29, согласно СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы [**Ошибка! Источник**

ссылки не найден.] и ГОСТ 12.2.032-78 Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования [0].

Таблица 29 – Требования к организации рабочего места при работе с ПЭВМ

Требование	**Требуемое значение**	**Значение параметров в помещении**
Высота рабочей поверхности стола	Регулируемая высота (680-800мм) Нерегулируемая высота (725мм)	Соответствует
Рабочий стул	Подъемно-поворотный, регулируемый по высоте и углу наклона спинки	Соответствует
Расположение монитора от глаз пользователя	600-700мм	Соответствует

Данные требования выполняются на текущем рабочем месте.

6.2 Производственная безопасность

Ниже приведен перечень опасных и вредных факторов, характерных для производственной среды в виде таблицы (таблица 30).

Таблица 30 – Опасные и вредные факторы при выполнении работ по разработке программно-алгоритмического комплекса планирования производственных процессов.

Факторы (ГОСТ 12.0.003-2015) [0]	Нормативные документы
Недостаточная освещённость	СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95 [0]

рабочей зоны; отсутствие или недостаток естественного света	
Повышенный уровень шума	ГОСТ 12.1.003-83 Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности [0]
Повышенный уровень электро-магнитных излучений	ГОСТ 12.1.006-84 «Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля» [0]
Повышенная или пониженная влажность воздуха	СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания [0]
Статические перегрузки, умственные перегрузки, перегрузки анализаторов;	МР 2.2.9.2311 – 07 «Профилактика стрессового состояния работников при различных видах профессиональной деятельности» [0]
Электрический ток	ГОСТ 12.1.030-81 Система стандартов безопасности труда (ССБТ). Электробезопасность. Защитное заземление. Зануление [0]
Короткое замыкание	ГОСТ 12.1.030-81 Система стандартов безопасности труда (ССБТ). Электробезопасность. Защитное заземление. Зануление [0]
Статическое электричество	ГОСТ 12.1.038-82 Система стандартов безопасности труда (ССБТ). Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов [0]

6.2.1Недостаточная освещённость рабочей зоны; отсутствие или недостаток естественного света

Рабочее место находится на 2 этаже здания. Естественное освещение в кабинете присутствует. Основное освещение в аудитории производится посредством общего искусственного освещения.

В процессе разработки, разработчик все время работы пользуется ПК. При этом согласно СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95 [0] освещение не создает бликов на поверхности экрана ПЭВМ, а освещенность экрана не более 300 лк. Кроме того, работа за ПЭВМ относится к категории зрительных работ к разряду Б зрительных работ (восприятие информации).

6.2.2Повышенный уровень шума

Звуковые колебания, издаваемые движущимися частями механизмов и приборов, могут воздействовать на здоровье человека. Громкие звуки, могут стать причиной проблем со слухом, а длительное воздействие шума более 80 дБ может стать причиной его потери ли ухудшения. Чувствительность к монотонным звукам является индивидуальным показателем. Но постоянно повторяющиеся шумы на рабочем месте провоцируют проблемы, связанные с нервной системой и органами слуха.

В данной работе основным источником шума является системный блок ПК, внутри которого работает система охлаждения, состоящая из вентиляторов, воспроизводящих непрерывный шелест или гудение.

Постоянный уровень шума влияет на работоспособность и сосредоточенность человека. Рабочее место соответствует нормам ГОСТ 12.1.003-83 «Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности» [0] и является помещением с минимальным уровнем шума при программировании и разработке программного обеспечения планирования производственных процессов. Кроме того, каждый академический час в работе делается перерыв, который позволяет отключить

компьютер и/или выйти из помещения для разгрузки нервной системы и органов слуха.

Характеристикой постоянного шума на рабочем месте является уровень звукового давления, определяемый по формуле:

$$L_{\text{а}} = 20\lg\frac{P_a}{P_0}.$$

(**Ошибка! Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться.**.1)

Где P_a среднеквадратичная величина звукового давления;

P_0 – исходное звуковое давление в воздухе, равное $2\cdot10^{-5}$ Па

Замеры звукового давления на рабочем месте показали $P_a = 385\cdot10^{-5}$. Согласно формуле (Ошибка! **Используйте вкладку "Главная" для применения мой_заголовок_1 к тексту, который должен здесь отображаться.**.1:

$$L_{\text{а}} = 20\lg\frac{385\cdot10^{-5}}{2\cdot10^{-5}} = 37.73;$$

Предельно допустимые уровни звука на рабочих местах с учётом тяжести труда представлены в таблице 31.

Таблица 31 – Допустимые уровни звука на рабочем месте

Категория напряженности трудового процесса	Категория тяжести трудового процесса				
	Легкая физическая нагрузка	Средняя физическая нагрузка	Тяжелый труд 1 степени	Тяжелый труд 2 степени	Тяжелый труд 3 степени
Напряженность легкой степени	80	80	75	75	75

Напряженность средней степени	70	70	65	65	65
Напряженный труд 1 степени	60	60	-	-	-
Напряженный труд 2 степени	60	60	-	-	-

Уровень звука, при этом не превышает 40дБ, следовательно, данный уровень шума допустим для лёгкой физической нагрузки и напряжённого труда.

6.2.3Повышенный уровень электромагнитных излучений

Уровень электромагнитных излучений регулируется ГОСТ 12.1.006-84 «Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля» [0].

В повседневной жизни для людей не заметно воздействия электромагнитных излучений. Мощность источника излучения должна быть достаточно большой, чтобы это отражалось на здоровье и самочувствие организма.

Основные излучающие электромагнитное поле части ПЭВМ – это системный блок, в котором находится процессор, и экран монитора.

На рабочем месте установлены ПЭВМ, оснащённые жидкокристаллическим монитором. Они излучают электромагнитные волны, которые не причиняют человеку вреда, даже при длительной работе.

6.2.4Повышенная напряжённость электрического поля

Работа ПЭВМ, кроме электромагнитных излучений сопровождается электростатическим полем, которое может деионезировать окружающую воздушную оболочку. Согласно ГОСТ 12.1.006-84 «Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля»

[0] для обеспечения безопасности рабочего персонала и оборудования необходимо проводить ионизацию воздуха, путём установки ионизаторов или обеспечения проветривания помещения.

6.2.5Повышенная или пониженная влажность воздуха

Согласно СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания [0] давление, температура и влажность воздуха влияют на здоровье работников, следовательно, он влияют на общее самочувствие, работоспособность и выполнение поставленных задач.

Рабочее место из-за своего расположения может быть слишком влажным. Поэтому в стенах аудитории установлена механическая вентиляция, оснащенная вентилятором и отводящая воздух из помещения. Это снижает влажность в помещении. Кроме того, аудитория подключена к системе центрального городского отопление. Это помогает регулировать температуру в период зимних месяцев.

6.2.6Статические перегрузки

В современном мире, почти каждая работа, так или иначе, связанна с работой за компьютером. Разработчикам программ, инженерам и всем, кто учится, приходится проводить за ПВЭМ многие часы. При этом пользователь вынужден принимать одну и ту же позу в течение длительного времени, тем самым создавая в работе мышечного корсета статические перегрузки. Неудобная поза, нахождение центра тяжести в одном месте, постоянный наклон вперед вызывают боли в шее и спине.

Работа с ПЭВМ подразумевает обработку большого количества информации. Анализ данных, инженерные исследования, расчеты и разработка программных продуктов требуют высокой концентрации внимания. При работе с визуальной информацией напрягаются глаза, которые являются зрительными анализаторами человека. Расстояние расположения предмета постоянного визуального контроля не меняется в процессе работы,

из-за этого устают глазные мышцы, из-за этого снижается острота зрения. При длительных контактах с дисплеем, постоянного наблюдения схожей по структуре зрительной информации, человек начинает испытывать стресс.

Согласно МР 2.2.9.2311 – 07 «Профилактика стрессового состояния работников при различных видах профессиональной деятельности» [0], разработка программно-алгоритмического комплекса относится к группе В, I категории (до 2х часов) – творческая работа в режиме диалога с ПЭВМ. При выполнении разных групп работ в течение смены за основную принимают такую, которая занимает не менее 50% времени рабочего дня. Для обеспечения оптимальной работоспособности и сохранения здоровья пользователей на протяжении рабочей смены должны устанавливаться регламентированный перерыв, при 8-ми часовом рабочем дне 30 минут. Продолжительность непрерывной работы с ПК не должна превышать 2 часов. Для I категории работ - через 2 часа от начала работы и через 1,5 - 2 часа после обеденного перерыва продолжительностью 15 минут каждый.

Во время регламентированных перерывов с целью сохранения высокой работоспособности выполняется комплекс упражнений. С целью уменьшения отрицательного влияния монотонности целесообразно чередование операций осмысленного текста и числовых данных, чередование редактирования текстов и ввода данных (изменение содержания работы).

Работа над разработкой программного продукта требует сосредоточенности и частого переключения между использованием нескольких программ одновременно. Поэтому для того чтобы зрительные анализаторы работали на нужном уровне каждый академический час проводится перерыв в 5-10 минут, а в каждый второй академический час перерыв в 20 минут. Во время перерыва есть возможность выйти из аудитории и выключить на время ПЭВМ.

6.2.7Электробезопасность

Электробезопасность – система организационных и технических мероприятий и средств, обеспечивающих защиту людей от вредного и опасного воздействия электрического тока, электрической дуги, электромагнитного поля и статического электричества.

Согласно ГОСТ 12.1.030-81 «Система стандартов безопасности труда (ССБТ). Электробезопасность. Защитное заземление. Зануление» [0] помещение, в котором находится рабочее место, относится к категории помещений без повышенной опасности. Его можно охарактеризовать, как сухое, непыльное, с токонепроводящими полами и нормальной температурой воздуха. Температурный режим, влажность воздуха, химическая среда не способствуют разрушению изоляции электрооборудования.

Защита от электрического тока на рабочем месте производится с помощью изоляции токопроводящих частей (все провода изолированы). Электрические устройства, в частности процессор от ПЭВМ расположен в защитном коробе.

Короткое замыкание – это соединение двух точек с разным потенциалом с последующим увеличением тока и выделением большого количества тепла. Вследствие чего короткое замыкание может стать причиной пожара в помещении, при коротком замыкании от электрического тока могут пострадать люди, находящиеся в непосредственной близости от источника возникновения.

На рабочем месте короткое замыкание может быть вызвано либо неисправностью в проводке, либо при работе с компьютером, когда внутри корпуса создается разность фаз и ток может так же повредить всю электросеть.

Для защиты электрической сети от короткого замыкания предусмотрены устройства защитного отключения (УЗО), оснащенные устройствами автоматического отключения – автоматами и предохранителями. Кроме того, в помещении установлены датчики дыма,

которые при возникновении возгорания, вызванного коротким замыканием, оповещают все здание о начавшемся пожаре. Таким образом, рабочее место полностью защищено от возможного короткого замыкания.

6.2.8Статическое электричество

В рабочем пространстве находится много устройств, которые работают от электрического тока и сделаны из материалов, которые, так или иначе, накапливают на себе статически заряд. Может возникнуть разность потенциалов от статического электричества, и прикосновение человека к заряду может вызвать травмы, ожоги или пожар.

Для защиты оборудования и персонала применяется общее заземление электропроводки и увлажняющие устройства.

6.3 Экологическая безопасность

6.3.1Воздействие на литосферу

Вышедшее из строя ПЭВМ и сопутствующая оргтехника относится к IV классу опасности и подлежит специальной утилизации. Для оказания наименьшего влияния на окружающую среду, необходимо проводить специальную процедуру утилизации ПЭВМ и оргтехники, при которой более 90% отправится на вторичную переработку и менее 10% будут отправлены на свалки. При этом она должна соответствовать процедуре утилизации ГОСТ Р 53692-2009 Ресурсосбережение. Обращение с отходами. Этапы технологического цикла отходов [0].

При выходе из строя, а также устаревании компонентов, ПЭВМ и сопутствующая оргтехника начинает представлять собой источник второсортного сырья и относится к IV классу опасности. Каждый ПЭВМ содержит цветные металлы и целый набор опасных для окружающей среды веществ. Это производные газов, тяжелые металлы, среди которых кадмий, ртуть и свинец. Попадая на свалку, все эти вещества под воздействием внешней среды постепенно проникают в почву.

Люминесцентные лампы при перегорании становятся источником загрязнения. Лампы содержат внутри себя ртуть, которая загрязняет окружающую среду. Кроме того, их корпус состоит преимущественно из стеклянной трубки, которая при неосторожном обращении может разбиться на мелкие осколки.

Документы, перенесенные на бумагу, становятся источником бумажных отходов. Такие отходы медленнее разлагаются из-за предварительной обработки бумаги, а также содержат на себе следы краски, которая, попадая в почву ее загрязняет.

Согласно ГОСТ 17.4.3.04-85 «Охрана природы (ССОП). Почвы. Общие требования к контролю и охране от загрязнения» [0] юридические лица имеют право утилизировать оргтехнику только при прохождении процедуры полного списания, подтвержденного актом.

Томский политехнический университет является юридическим лицом, поэтому перегоревшие люминесцентные лампы собираются техническим персоналом, а затем передаются в центр по переработке таких ламп, у которого имеется лицензия на право сбора и переработки люминесцентных ламп. Для макулатуры существуют специально установленные контейнеры, в которые помещаются отработавшие печатные издания, офисная бумага и другие изделия из переработанной целлюлозы. Они отвозятся в пункты по сбору макулатуры, где утилизируются.

6.4 Безопасность в чрезвычайных ситуациях

6.4.1Пожарная безопасность

Пожарная безопасность может быть обеспечена мерами пожарной профилактики и активной пожарной защиты. Пожарная профилактика включает комплекс мероприятий, направленных на предупреждение пожара или уменьшение его последствий. Возникновение пожара в помещении аудитории может привести к большим материальным потерям и возникновению чрезвычайной ситуации. Чрезвычайные ситуации приводят к

полной потере информации и большим трудностям восстановления всей информации в полном объёме.

Согласно ГОСТ 12.1.004-91 «Система стандартов безопасности труда (ССБТ). Пожарная безопасность. Общие требования» [0], рабочее помещение относится к категории В (производства, связанные с обработкой или применением твердых сгораемых веществ и материалов).

В случае возникновения пожара необходимо отключить электропитание, вызвать по телефону пожарную команду, произвести эвакуацию и приступить к ликвидации пожара огнетушителями. При наличии небольшого очага пламени можно воспользоваться подручными средствами с целью прекращения доступа воздуха к объекту возгорания. Покидать помещение необходимо согласно плану эвакуации.

Пожар является чрезвычайной ситуацией для людей, находящихся в помещении. При возникновении пожара сработают датчики дыма, которые подадут сигнал общего оповещения всего здания.

На рисунке 6.1 представлен план эвакуации людей при пожаре и других ЧС для учебного корпуса № 10 ТПУ, расположенного по адресу пр. Ленина 2.

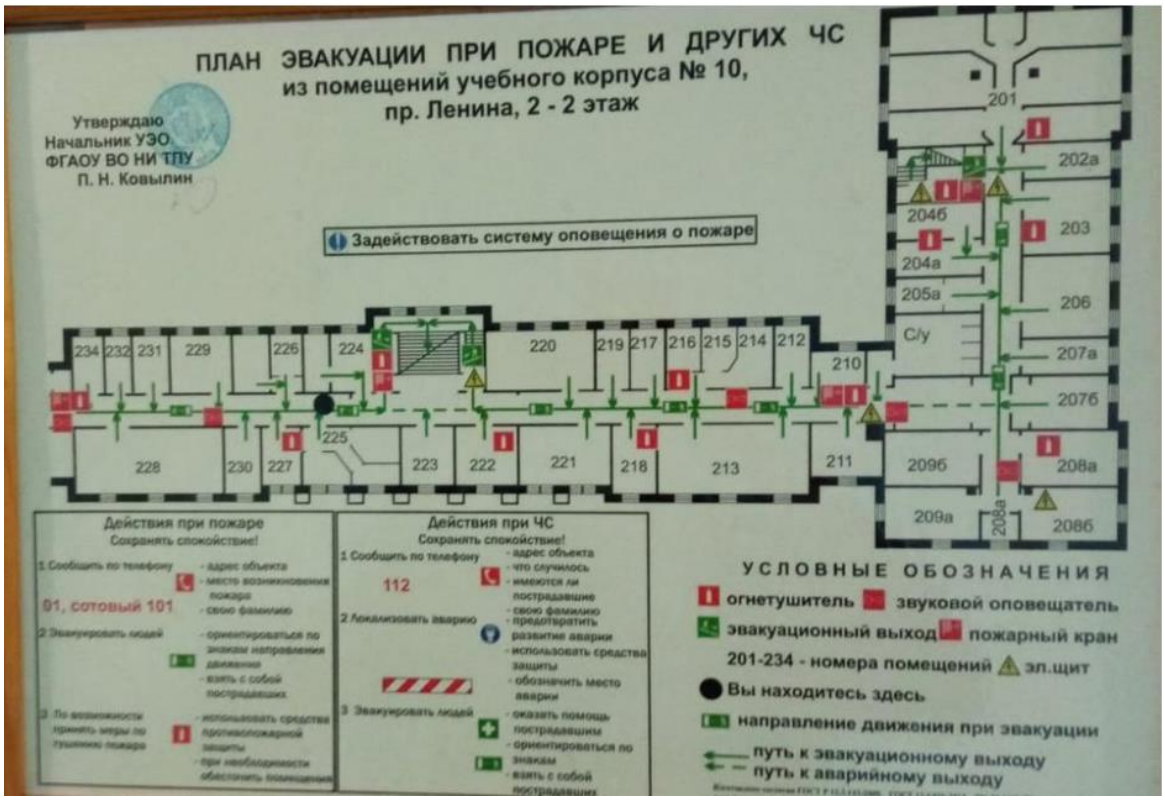


Рисунок 6.1ы – План эвакуации людей при пожаре и других ЧС

Выводы

В ходе выполнения работы над разделом «Социальная ответственность» были выявлены опасные и вредные факторы, воздействию которых может подвергнуться человек, занимающийся разработкой системы аутентификации пользователей на основе динамических характеристик клавиатурного почерка.

При работе в офисном помещении производятся отходы: бумага, канцелярские принадлежности, люминесцентные лампы и т.д. При надлежащей утилизации этих отходов (с помощью специальных фирм, имеющих лицензию на осуществление утилизации) загрязнение окружающей среды относительно мало.

В разделе были проведены расчеты допустимого уровня шума, которые показали, что рабочее место удовлетворяет требованиям безопасности.

Была рассмотрена наиболее распространенная чрезвычайная ситуация – пожар. Пожар может быть следствием короткого замыкания или неверной

эксплуатации электроприборов, а также несоблюдения техники безопасности. Именно для этого сотрудники офиса проходят инструктаж по правилам пожарной безопасности, проходят учебные эвакуации. В разделе была приведена схема эвакуации при пожаре и других ЧС.

Правовые и организационные вопросы обеспечения безопасности регулируются государственными органами. Правила и нормы для обеспечения нормальных условий труда всех сотрудников устанавливаются на государственном уровне.

Заключение

В ходе магистерской диссертации был рассмотрен подход к решению задачи аутентификации слушателя дистанционного обучения на основе динамических характеристик клавиатурного почерка.

Было установлено, что аутентификация пользователя может проходить на основе непрерывного мониторинга его клавиатурных нажатий в любой программной среде. На основании проведенных исследований были сделаны следующие выводы.

1. Необходимо корректировать образцы клавиатурного почерка при условии использования динамической аутентификации пользователя по клавиатурному почерку.

2. Улучшение качества собираемых системой данных, а также выделение стабильных признаков клавиатурного почерка коренным образом влияет на дальнейшие вычисления, и в конечном счете, на способность системы правильно подтверждать легитимность пользователя.

3. Внедрение в систему частотности букв русского алфавита значительным образом повлияло на качество аутентификации. При этом, у двух используемых методов – Евклидова расстояния и расстояния городских кварталов качество распознавания улучшилось в два раза.

4. Использованный в исследовании метод классификации k-NN при этом показал средний результат. Однако при отсутствии без внедрения в систему частотности букв русского алфавита метод занимает первое место по качеству аутентификации.

5. В ходе исследования выяснилось, что основной эффект использования частотности букв алфавита состоит в том, что отпадает необходимость в использовании сложных методов машинного обучения отсутствии ввиду одинаковости показателей эффективности распознавания.

Conclusion

In the course of the master's thesis an approach to solving the problem of authentication of a distance learning listener based on the dynamic characteristics of keyboard handwriting was considered.

It was found that user authentication can take place on the basis of continuous monitoring of his keyboard keystrokes in any software environment. The following conclusions were made based on the research conducted.

1. Keyboard handwriting samples must be corrected if dynamic user authentication by keyboard handwriting is used.

2. Improving the quality of the data collected by the system, as well as the identification of stable keyboard handwriting features, has a profound effect on further calculations, and ultimately on the system's ability to correctly validate the user's legitimacy.

3. The introduction of the frequency of letters of the Russian alphabet into the system had a significant impact on the quality of authentication. At the same time, the two methods used - Euclidean distance and city block distance - improved the quality of recognition in two times.

4. The k-NN classification method used in the study showed an average result. However, in the absence of the frequency of the letters of the Russian alphabet without implementation in the system, the method ranks first in terms of the quality of authentication.

5. In the course of the study it turned out that the main effect of using the frequency of letters of the alphabet is that there is no need to use complex methods of machine learning due to the uniformity of recognition performance.

Список литературы

1. Затеев Р. П. Непрерывная идентификация пользователей на основе динамических характеристик клавиатурного почерка и методов Data Mining : бакалаврская работа / Р. П. Затеев ; Национальный исследовательский Томский политехнический университет (ТПУ), Инженерная школа информационных технологий и робототехники (ИШИТР), Отделение информационных технологий (ОИТ) ; науч. рук. Е. А. Кочегурова. — Томск, 2020.

2. Прокторинг в онлайн-экзаменах: как это работает? [Электронный ресурс] / habr. URL: https://habr.com/ru/company/stepic/blog/329420/, дата обращения: 11.05.2022

3. Кочегурова Е.А., Мартынова Ю.А. Особенности непрерывной идентификации пользователей на основе свободных текстов в режим скрытого мониторинга // Программирование. - 2020. - №1. - С. 15-28.

4. Залучёнова О.М. Онлайн-образование: проблемы и перспективы развития. Вестник университета «Туран». 2020;(3):276-279. https://doi.org/10.46914/1562-2959-2020-1-3-276-279

5. Fenu G, Marras M, Boratto L. A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters 2018; 113: 83-92. doi.org/10.1016/j.patrec.2017.03.027.

6. Ngqondi T, Maoneke PB, Mauwa L. A secure online exams conceptual framework for South African universities. Social Sciences & Humanities Open. 2021; 3(1): 100132. doi.org/10.1016/j.ssaho.2021.100132.

7. Затеев Р. П., Кочегурова Е. А. Непрерывная идентификация пользователей на основе динамических характеристик клавиатурного почерка // Современные технологии, экономика и образование: сборник материалов II Всероссийской научно-методической конференции, Томск, 2-4 Сентября 2020. - Томск: ТПУ, 2020 - С. 60-62

8. Затеев Р. П. Непрерывная идентификация пользователей на основе динамических характеристик клавиатурного почерка и методов Data Mining:

бакалаврская работа / Р. П. Затеев; Национальный исследовательский Томский политехнический университет (ТПУ), Инженерная школа информационных технологий и робототехники (ИШИТР), Отделение информационных технологий (ОИТ) ; науч. рук. Е. А. Кочегурова. — Томск, 2020.

9. Махонченко С. С. , Затеев Р. П. Защита корпоративной информационной системы на базе распознавания клавиатурного почерка пользователей // Молодежь и современные информационные технологии: сборник трудов XVI Международной научно- практической конференции студентов, аспирантов и молодых ученых, Томск, 3-7 Декабря 2018. - Томск: ТПУ, 2019 - С. 94-95

10. Репина Е. Ю., У Д. -., Затеев Р. П. К вопросу оптимизации параметров сглаживающего сплайна // Молодежь и современные информационные технологии: сборник трудов XVI Международной научно-практической конференции студентов, аспирантов и молодых ученых, Томск, 3-7 Декабря 2018. - Томск: ТПУ, 2019 - С. 116-117

11. ГОСТ 12.0.003-2015 Опасные и вредные производственные факторы. Классификация. Перечень опасных и вредных факторов;

12. ГОСТ 12.1.003-83 «Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности»;

13. ГОСТ 12.1.004-91 «Система стандартов безопасности труда (ССБТ). Пожарная безопасность. Общие требования»;

14. ГОСТ 12.1.006-84 «Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля»;

15. ГОСТ 12.1.030-81 «Система стандартов безопасности труда (ССБТ). Электробезопасность. Защитное заземление. Зануление»;

16. ГОСТ 12.1.038-82 Система стандартов безопасности труда (ССБТ). Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов;

17. ГОСТ 12.2.032-78 Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования;

18. ГОСТ 17.4.3.04-85 «Охрана природы (ССОП). Почвы. Общие требования к контролю и охране от загрязнения»;

19. ГОСТ ISO 9612-2016 Акустика. Измерения шума для оценки его воздействия на человека. Метод измерений на рабочих местах (с Поправкой);

20. ГОСТ Р 53692-2009 Ресурсосбережение. Обращение с отходами. Этапы технологического цикла отходов.

21. МР 2.2.9.2311 – 07 «Профилактика стрессового состояния работников при различных видах профессиональной деятельности»;

22. СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания;

23. ТОИ Р-45-084-01 «Типовая инструкция по охране труда при работе на персональном компьютере».

24. СП 12.13130.2009 Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности;

25. СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95;

26. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 25.02.2022).

Приложение А

Раздел 2

Keyboard authentication and identification issues

Обучающийся:

Группа	ФИО	Подпись	Дата
8ВМ01	Затеев Роман Павлович		

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	Сидоренко Т. В.	к.пед.н., доцент		

1 Keyboard authentication and identification issues

Often a two-step verification process is used as a way to protect the system from an unauthorized access:

- primary identity authentication,
- dynamic identity authentication.

Each person has an individual typing rhythm. In view of this, keyboard handwriting can be used in a biometric identity recognition system. For illustration, figure 1 shows the keyboard dynamics of 6 university domain users. The visual analysis demonstrates a certain variation between the times of pressing certain letters on a keyboard. This variation just demonstrates the uniqueness of each user's keyboard rhythm. Technically, the more keys a user presses, the more accurately the algorithm can understand and recreate a user's keyboard pattern. The uniqueness of the keyboard pattern increases the accuracy of the recognition system.

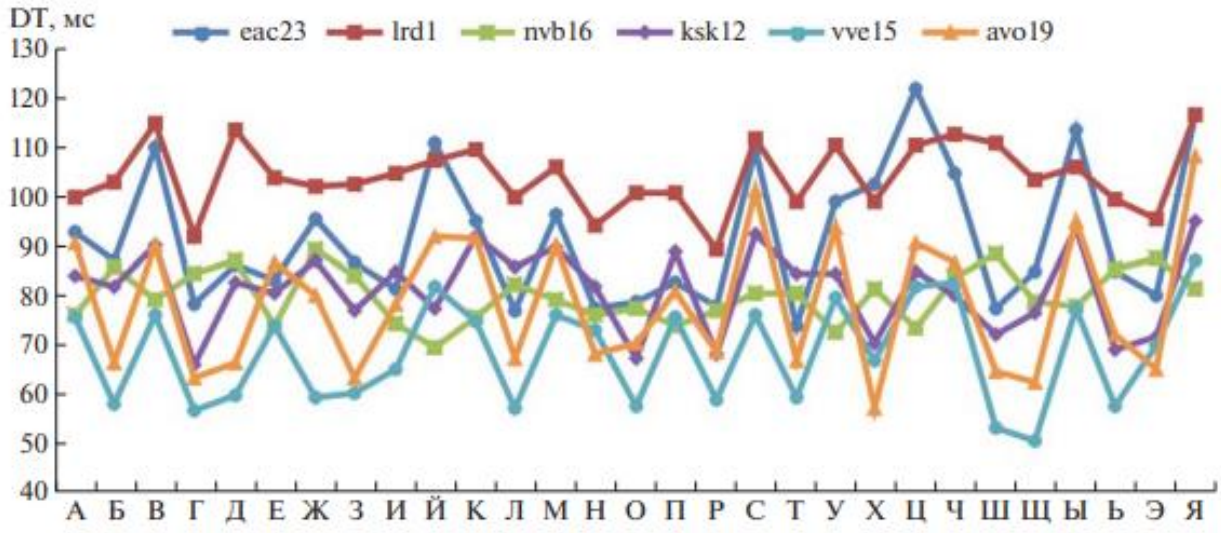


Figure A.1 – Average time of keyholding by domain users, ms.

1.1 Authentication methods

Authentication is an authentication procedure, such as checking the authenticity of a user by comparing a password he/ she entered with the password stored in database. There are a large number of user authentication methods. The methods can be divided into three main categories based on the following paradigms [10]:

- what you know (e.g., password, PIN),

- what you possess (e.g., a token, a smart card),

- who you are (e.g. fingerprints).

The last paradigm of "who you are" is closely related to the concept of biometrics. There are physiological (iris scanner, face scanner, palm print, etc.) and behavioral (keyboard handwriting, computer mouse movement pattern, etc.).

Keyboard handwriting-based user authentication is one of the most affordable ways to prevent data leakage. This method of information protection combines two main advantages - there is no need for additional equipment and low cost compared to other methods of biometrics. All that is required from the user is the presence of a standard keyboard, and the layout does not matter, and the presence of installed software application. This method of authentication allows you to monitor the hidden actions of the user, that is, the user works in his comfortable mode, and the program automatically reads his keystrokes on the keyboard. Keyboard handwriting is formed by analyzing typing speed, rhythm, keystrokes. It is important to keep in mind that keyboarding, like other biometric methods, tends to change over time with each individual. However, the likelihood of a user being spoofed by imitating their keyboard handwriting is virtually unrealistic. The main advantages and disadvantages of authentication methods are shown in the table below.

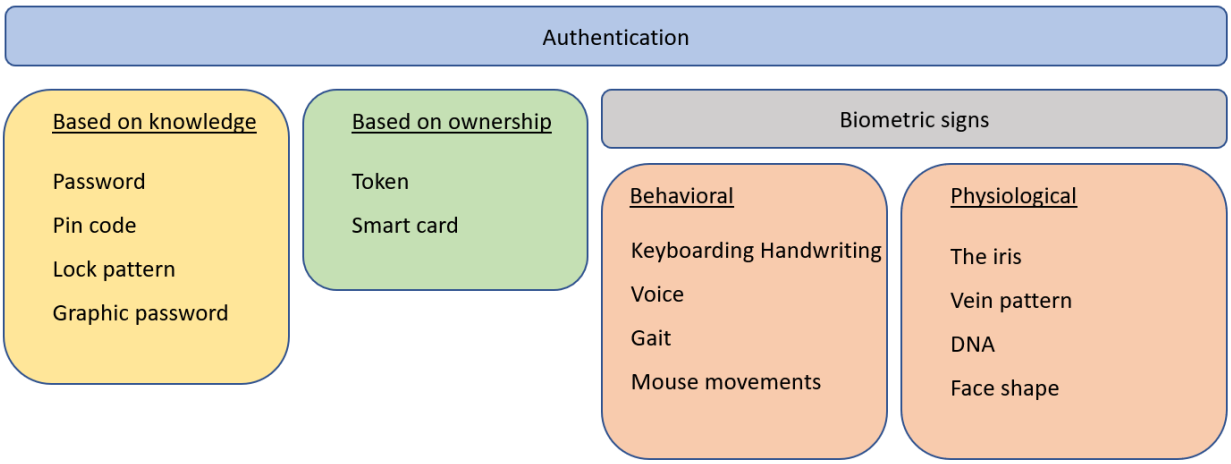


Figure A.2 – Identity authentication methods

Table A.1 - Characteristics of authentication methods

Method	Advantages	Disadvantages	Example

Password	1. Simple implementation 2. Unambiguous recognition	1. Can be forgotten or stolen	1. Password 2. PIN
Attribute	1. Easy implementation 2. No cost	1. Can be lost or stolen	1. Key 2. Smart card 3. Token
Biometric	1. Uniqueness 2. Impossible to forget/lose	1. Cost of implementation 2. Variability of data regardless of the person	1. Fingerprint 2. Voice 3. Keyboard handwriting

1.2 Authentication modes

The most reasonable for the recognition system and the most comfortable way for the user to authenticate his identity is to constantly and covertly monitor the dynamics of his work. Dynamic characteristics of keyboard handwriting are more difficult to recognize than physiological ones. However, this fact is compensated for by the more time-consuming process of user spoofing, which has a beneficial effect on the level of system security.

There are two types of authentication: static and dynamic. With static authentication, the system user is presented with a certain fixed-length text, which the user must enter to verify his identity. Dynamic authentication is a more complex process of monitoring the user's keystrokes. If a certain condition is set, such as frequent use of service characters, which is not typical of the user, or printing is too slow, the system may restrict access to the account and ask to go through the authentication process again. 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 security. Dynamic authentication would serve as the second.

1.3 Authentication Lifecycle

Continuous user authentication based on the CA has a registration phase and an authentication phase, as shown in Figure 3. During the registration phase, the system records data about the keys pressed on the keyboard. In the next step, the system extracts characteristics of the keyboard handwriting from the collected statistics - the duration of presses, pauses between them, the presence of service keys, and so on. Based on the collected data, the system generates or updates a user's

keystroke pattern. Next, the pattern is checked against the stored in the database authentication process takes place.

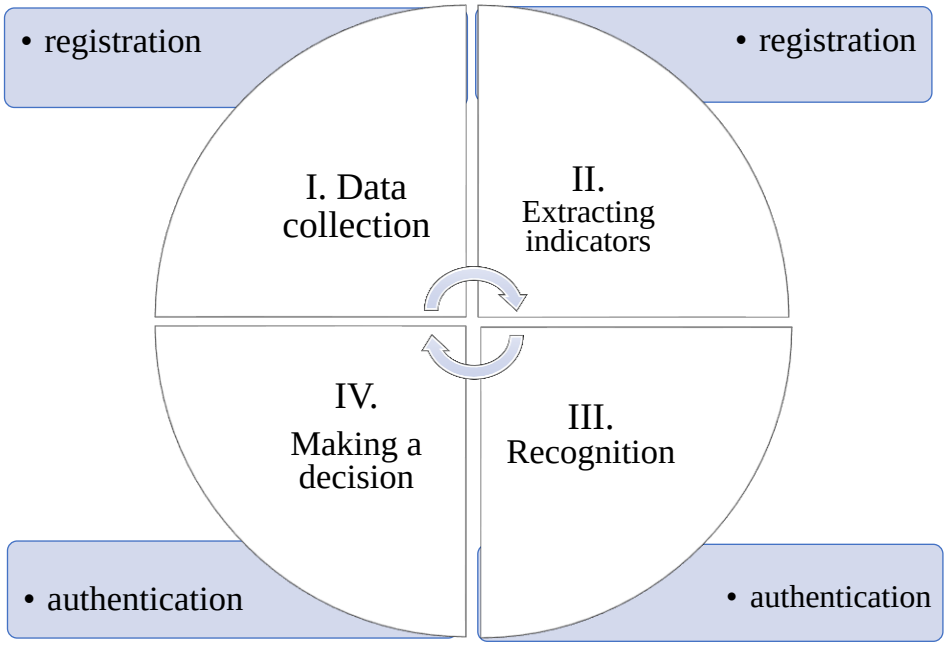


Figure A.3 - Continuous Authentication Lifecycle Process

The lifecycle of continuous user authentication by dynamic characteristics of keyboard handwriting includes 4 main stages:

I. Collecting data on the dynamics of key presses

During the first stage, the process of collecting user data when using the keyboard takes place. The Windows operating system uses Windows-hook technology to intercept messages. This technology allows to capture any user's keystrokes on the keyboard. Accuracy of keyboard keystrokes is measured in milliseconds.

II. Extracting classification attributes

The data collected during the first stage should be normalized - cleaned of unreliable values, outliers, phantom presses, etc. Based on the sample obtained, it already makes sense to calculate the dial rate, pauses, and user rhythm. All of these indicators are unique behavioral characteristics.

There are quite a lot of KP indicators, but the most popular among researchers are diagrams (digraphs) - timing of two key states [17, 21-23]. Figure 6 shows some of the most commonly used timings and frequencies.

- DU or key hold time is characterized by the time interval between pressing and releasing a key.

- UD or pause is characterized by the time interval between pressing the next key and releasing the previous one.

- UU or DD The interval between pressing or releasing one key and releasing or releasing the next key, respectively.

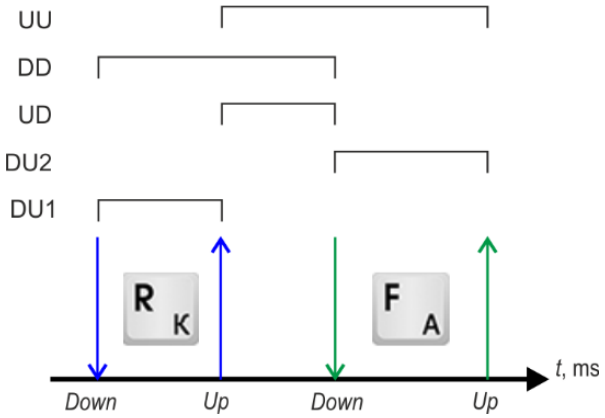


Figure A.4 - Key press indicators in Down Time/Up Time notation

Subsystems of the pre-processing of timing data and extraction of keyboard handwriting characteristics create an array of the required values of any user's button presses. Then, a user's keyboard profile is generated based on the array and placed in the database.

III. User recognition

Authentication is the task of classifying users registered in the system. The basic methods and algorithms used to solve the problem of user classification are the same for both static and dynamic authentication. They can be divided into three groups:

- based on proximity estimation;

- machine learning methods.

- statistical;

Recent studies on user recognition by keyboard handwriting have summarized data on the effectiveness of continuous authentication. The data are summarized in Table 2. The data are derived from our own studies [20, 26] and adapted from review articles [17, 22, 24, 27- 33].

Table A.2 - 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

IV. Deciding on the user's legitimacy

This stage is entirely dedicated to solving the problem of user authentication by keyboard handwriting. In the process of dynamic authentication, the key objective of continuous monitoring is the ability of a registered user to access application resources at all times. In pursuit of this goal, it was decided to continuously monitor the probabilities of first- and second-order errors - false access and false denial:

- False Rejection Rate (FRR) - the rate of false denial of access to a legitimate (registered) user:

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

- False Acceptance Rate (FAR) - False Acceptance Rate of illegal users:

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

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

- True Accept (TA) - True admittance to a legitimate user.

- True Reject (TR) - True denial of access to an illegal user.

- False Accept (FA) - False Access for an illegal user.

- False Reject (FR) - False denial of access to a legitimate user.

The sum of the above indicators is the total number of attempts.

The resulting FAR and FRR errors are fundamentally affected by the sensitivity of the algorithm. By controlling the sensitivity, the application administrator is able to decide whether or not to allow a user into the system. If the system requires a high degree of protection, then it will be necessary to set the highest possible sensitivity values. This will result in high false user rejections. If more simplified access to the system is required, then the administrator sets small values of sensitivity of the algorithm - this corresponds to a small value of FRR. This compromise has to be resolved individually for each application.

The next most popular indicator is Equal Error Rate (EER). This indicator corresponds to the value obtained at the intersection of the FAR and FRR graphs. By adjusting the EER, you can control the degree of security of the system as a

whole. The indicators described above are the most popular in the scientific community when solving the problem of dynamic authentication by keyboard handwriting.

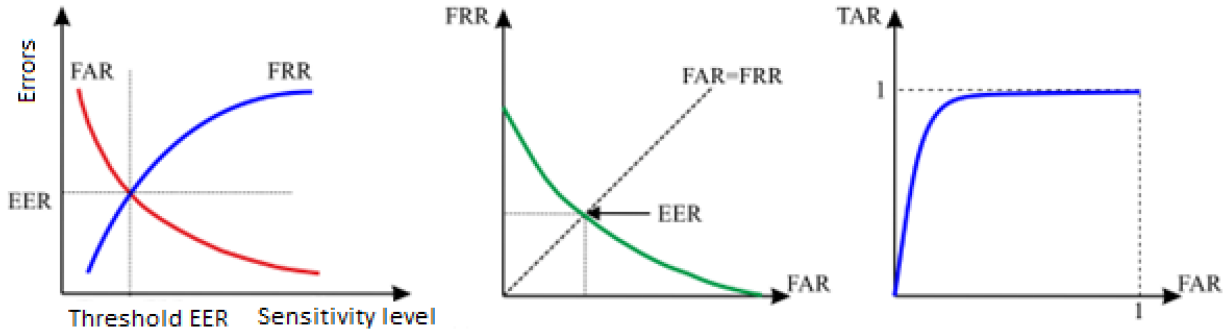


Figure A.5 - Keyboard authentication performance indicators

Приложение Б

Таблица Б.1 – Расчеты для метода «Евклидово расстояние»

№	Порог мс	Порог %	FRR	FAR	TAR	TRR	sum
1	0,004	0,01	362	0	1	837	1200
2	0,2	0,5	335	1	28	836	1200
3	0,4	1	307	5	56	832	1200
4	0,6	1,5	278	7	85	830	1200
5	0,8	2	252	7	111	830	1200
6	1,6	4	185	7	178	830	1200
7	2,4	6	167	8	196	829	1200
8	3,2	8	144	18	219	819	1200
9	4	10	119	68	244	769	1200
10	6	15	27	450	336	387	1200
11	8	20	0	631	363	206	1200
12	10	25	0	715	363	122	1200
13	12	30	0	836	363	1	1200
14	16	40	0	837	363	0	1200
15	20	50	0	837	363	0	1200
16	30	75	0	837	363	0	1200
17	40	100	0	837	363	0	1200
18	80	200	0	837	363	0	1200

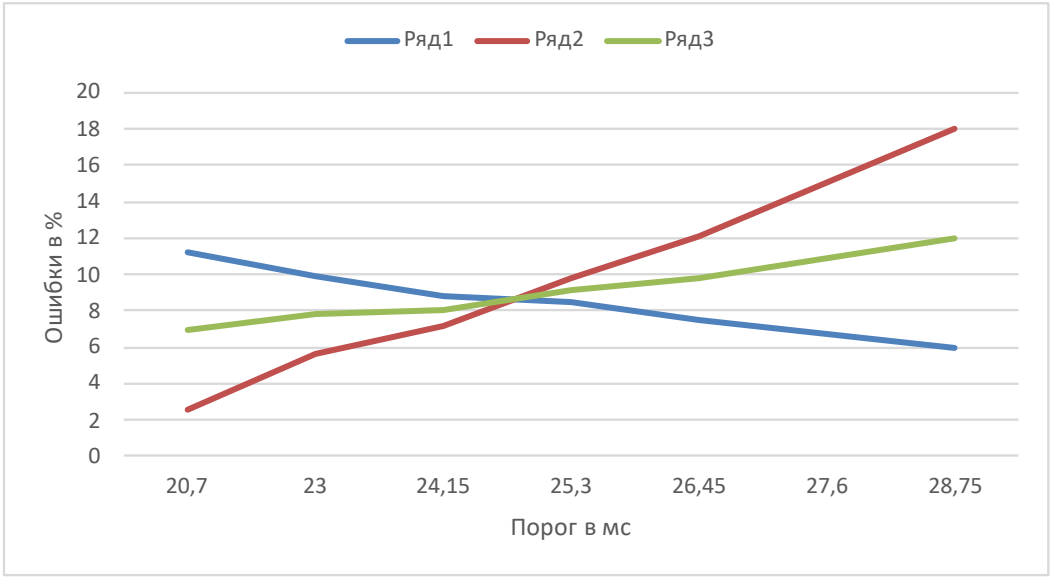


Рисунок Б.1 – Оценка эффективности распознавания пользователей методом «Евклидово расстояние»

Таблица Б.2 – Расчеты для метода «Евклидово расстояние с поправкой на частотность букв русского языка»

№	Порог мс	Порог %	FRR	FAR	TAR	TRR	sum
1	0,004	0,01	199	0	1	1000	1200
2	0,2	0,5	172	1	28	999	1200
3	0,4	1	144	2	56	998	1200
4	0,6	1,5	115	4	85	996	1200
5	0,8	2	89	4	111	996	1200
6	1,6	4	22	8	178	992	1200
7	2,4	6	7	13	193	987	1200
8	3,2	8	1	40	199	960	1200
9	4	10	0	114	200	886	1200
10	6	15	0	589	200	411	1200
11	8	20	0	794	200	206	1200
12	10	25	0	878	200	122	1200
13	12	30	0	999	200	1	1200
14	16	40	0	1000	200	0	1200
15	20	50	0	1000	200	0	1200
16	30	75	0	1000	200	0	1200
17	40	100	0	1000	200	0	1200
18	80	200	0	1000	200	0	1200

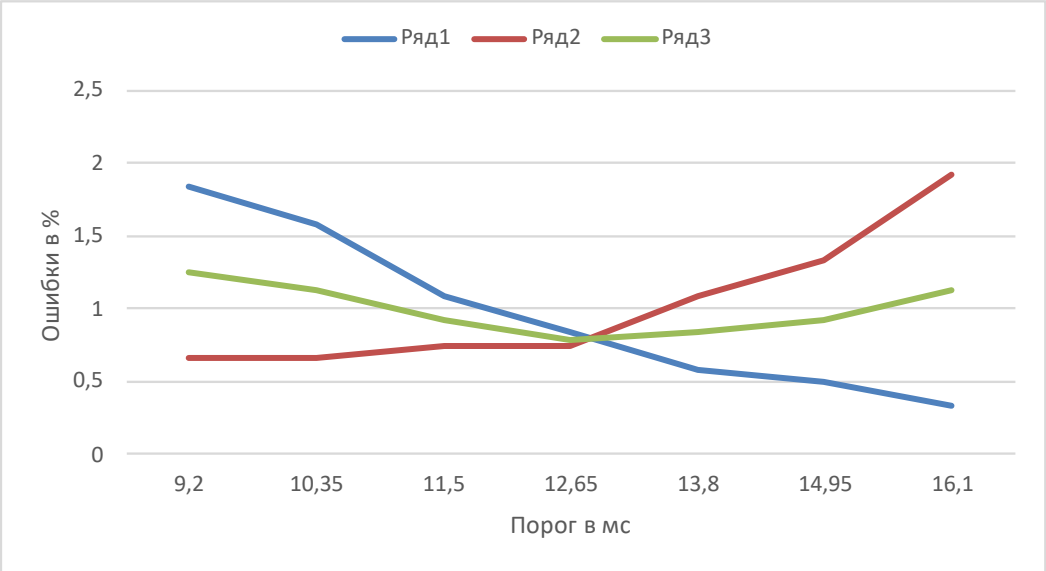


Рисунок Б.2 – Оценка эффективности распознавания пользователей методом «Евклидово расстояние с поправкой на частотность букв русского языка»

Таблица Б.3 – Расчеты для метода «Манхэттенское расстояние»

№	Порог мс	Порог %	FRR	FAR	TAR	TRR	sum
1	0,004	0,01	399	0	1	800	1200
2	0,2	0,5	372	1	28	799	1200
3	0,4	1	344	5	56	795	1200
4	0,6	1,5	315	6	85	794	1200
5	0,8	2	289	7	111	793	1200
6	1,6	4	222	10	178	790	1200
7	2,4	6	204	11	196	789	1200
8	3,2	8	178	18	222	782	1200
9	4	10	148	63	252	737	1200
10	6	15	35	422	365	378	1200
11	8	20	0	594	400	206	1200
12	10	25	0	678	400	122	1200
13	12	30	0	799	400	1	1200
14	16	40	0	800	400	0	1200
15	20	50	0	800	400	0	1200
16	30	75	0	800	400	0	1200
17	40	100	0	800	400	0	1200
18	80	200	0	800	400	0	1200

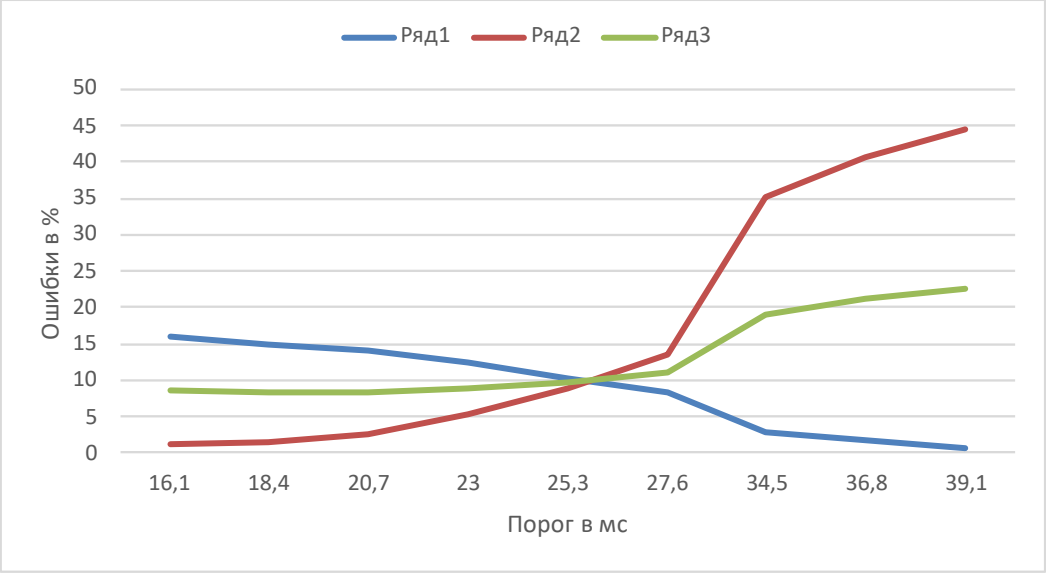


Рисунок Б.3 – Оценка эффективности распознавания пользователей методом «Манхэттенское расстояние»

Таблица Б.4 – Расчеты для метода «Манхэттенское расстояние с поправкой на частотность букв русского языка»

№	Порог мс	Порог %	FRR	FAR	TAR	TRR	sum
1	0,004	0,01	399	0	1	800	1200
2	0,2	0,5	372	1	28	799	1200
3	0,4	1	344	5	56	795	1200
4	0,6	1,5	315	6	85	794	1200
5	0,8	2	289	7	111	793	1200
6	1,6	4	222	10	178	790	1200
7	2,4	6	204	11	196	789	1200
8	3,2	8	178	18	222	782	1200
9	4	10	148	63	252	737	1200
10	6	15	35	422	365	378	1200
11	8	20	0	594	400	206	1200
12	10	25	0	678	400	122	1200
13	12	30	0	799	400	1	1200
14	16	40	0	800	400	0	1200
15	20	50	0	800	400	0	1200
16	30	75	0	800	400	0	1200
17	40	100	0	800	400	0	1200
18	80	200	0	800	400	0	1200

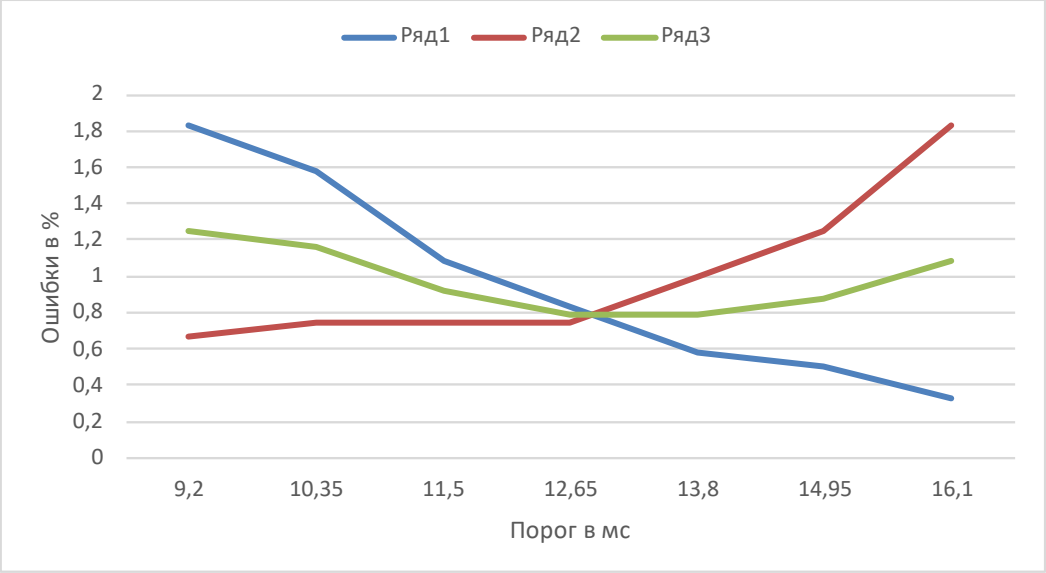


Рисунок Б.4 – Оценка эффективности распознавания пользователей методом «Манхэттенское расстояние с поправкой на частотность букв русского языка»

Таблица Б.5 – Расчеты для метода «K-ближайших соседей»

№	Порог мс	Порог %	FRR	FAR	TAR	TRR	sum
1	0,004	0,01	399	0	1	800	1200
2	0,2	0,5	372	1	28	799	1200
3	0,4	1	344	5	56	795	1200
4	0,6	1,5	315	6	85	794	1200
5	0,8	2	289	7	111	793	1200
6	1,6	4	222	10	178	790	1200
7	2,4	6	204	11	196	789	1200
8	3,2	8	178	18	222	782	1200
9	4	10	148	63	252	737	1200
10	6	15	35	422	365	378	1200
11	8	20	0	594	400	206	1200
12	10	25	0	678	400	122	1200
13	12	30	0	799	400	1	1200
14	16	40	0	800	400	0	1200
15	20	50	0	800	400	0	1200
16	30	75	0	800	400	0	1200
17	40	100	0	800	400	0	1200
18	80	200	0	800	400	0	1200

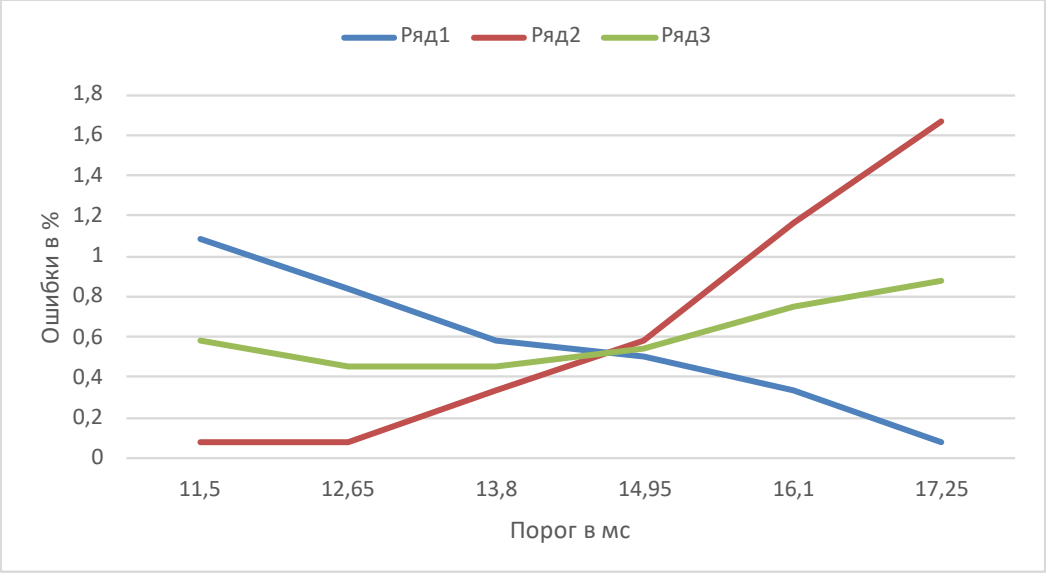


Рисунок Б.5 – Оценка эффективности распознавания пользователей методом «K-ближайших соседей»