МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество Казахский «Национальный исследовательский технический университет имени К. И. Сатпаева»

SATBAYEV UNIVERSITY

Институт автоматики и информационных технологий

Кафедра «Робототехники и технических средств автоматики»

Бекташов Айбек Шаукатұлы

ДИПЛОМНАЯ РАБОТА

Тема: Разработка программного средства для контроля посещаемости студентов на основе биометрических данных сканера отпечатков пальцев

Специальность 6В07113 – Робототехника и Мехатроника

Алматы 2023

Некоммерческое акционерное общество Казахский «Национальный исследовательский технический университет имени К. И. Сатпаева»

SATBAYEV UNIVERSITY

Институт автоматики и информационных технологий

Кафедра «Робототехники и технических средств автоматики»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой РТиТСА
кандидат технических наук
Ожикенов К. А.
«29» мая 2023 г.

ДИПЛОМНАЯ РАБОТА

Тема: «Разработка программного средства для контроля посещаемости студентов на основе биометрических данных сканера отпечатков пальцев»

по специальности 6B07113 – Робототехника и Мехатроника

Выполнил Бекташов Айбек Шаукатулы

Рецензент
Проректор по науке и сотрудничеству
АО «Академия логистики и транспорта»
PhD, ассоциированный профессор
_____ Балбаев Г.К.
подпись ФИО
«26» май 2023 ж.

Научный руководитель
Магистр технических наук,
старший преподаватель
_____ Бигалиева Ж.С.
«26» май 2023 ж.

Алматы 2023

Некоммерческое акционерное общество Казахский «Национальный исследовательский технический университет имени К. И. Сатпаева»

SATBAYEV UNIVERSITY

Институт автоматики и информационных технологий

Кафедра «Робототехники и технических средств автоматики»

6В07113 – Робототехника и Мехатроника

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой РТиТСА
кандидат технических наук
_____ Ожикенов К. А.
«29» мая 2023 г.

ЗАДАНИЕ
на выполнение дипломной работы

Обучающемуся Бекташов Айбек Шаукатұлы
1. Тема: «Разработка программного средства для контроля посещаемости студентов на основе биометрических данных сканера отпечатков пальцев.»
Утверждена приказом Ректора Университета № 408ПП от «18» 11. 2022 г
2. Срок сдачи студентом законченной работы «30» мая 2023 г.
3. Исходные данные к работе (законы, литературные источники, лабораторно-производственные данные)
а) Теоретические материалы по ЯП Kotlin.
б) Теоретические материалы по аппаратно-программной среды Android Studio, Arduino.
в) Теоретические материалы по объектно-реляционной системе управления БД, SQLite.
г) Теоретические материалы по использованию модуля распознавания отпечатков пальцев FPM10A
4. Перечень вопросов, подлежащих к разработке в дипломной работе (проекте)
а) Определить и раскрыть понятие «идентификации» и «аутентификации» личности и изучить методы распознавания личности используемых в системах контроля посещаемости
б) Рассмотреть и проанализировать имеющеюся базу систем для контроля и мониторинга посещаемости и выявить достоинство и недостатки
в) Обосновать необходимость системы мониторинга посещаемости образовательных учреждений.
г) Программно реализовать ПС, с использованием биометрических данных
д) Избрать необходимые программные и аппаратные средства для разработки
5. Перечень графических материалов (чертежи, таблицы, диаграммы и т. д.)
Представлены 11 слайдов презентации работы
6. Перечень основной рекомендуемой литературы: 32 страниц

ГРАФИК

подготовки дипломной работы (проекта)

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю и консультантам	Примечание
Сбор материалов для подготовки дипломной работы	24.01.23	выполнен
Подготовка теоретической части дипломной работы	27.02.23	выполнен
Подготовка аналитической части дипломной работы	25.03.23	выполнен
Завершение чернового варианта полного текста дипломной работы	27.03.23	выполнен

Подписи

консультантов и нормоконтролера на законченную дипломную работу (проект) с указанием относящихся к ним разделов работы (проекта)

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	Игембай Е. А., магистр техники и технологии	26.05.23	

Научный руководитель _____ Бигалиева Ж.С.

Задание принял к исполнению обучающийся _____ Бекташов А.Ш.

Дата "26" мая 2023г.

АННОТАЦИЯ

Программное обеспечение для учета посещаемости студентов, основанное на биометрических данных со сканеров отпечатков пальцев, является инновационным решением, предназначенным для автоматизации процесса учета посещаемости в образовательных учреждениях. Система использует биометрическую технологию и хранит уникальные биометрические данные студентов.

Это программное средство использует биометрические данные для обеспечения высокой точности и быстрой проверки посещаемости. Это позволяет эффективно контролировать посещаемость студентов и предоставлять точные отчеты администрации учебного заведения.

АҢДАТПА

Саусақ ізін сканерлеуге арналған биометриялық бағдарлама білім беру ұйымдарындағы сабаққа қатысу процесін автоматтандыруға арналған инновациялық шешім болып табылады. Жүйе биометриялық технологияларды пайдаланады және оқушылардың бірегей биометриялық деректерін сақтайды.

Бұл бағдарламалық құрал жоғары дәлдік пен жылдам қатысуды тексеру үшін биометрияны пайдаланады. Бұл студенттердің сабаққа қатысуын тиімді бақылауға және оқу орнының әкімшілігіне сенімді есеп беруге мүмкіндік береді.

ABSTRACT

Student attendance software based on biometric data from fingerprint scanners is an innovative solution designed to automate the attendance accounting process at educational institutions. The system uses biometric technology and stores unique biometric data of students.

This software tool uses biometric data to provide high accuracy and fast attendance verification. This allows for effective monitoring of student attendance and providing accurate reports to the institution's administration.

Содержание

ВВЕДЕНИЕ 7
1. Анализ современных методов биометрических данных 9
1.1 Преимущества и недостатки имеющихся систем 10
1.2 Понятие и типология «идентификации» и «аутентификации» личности 12
1.3 Системы мониторинга контроля посещаемости в сфере образования 14
2 Программные и аппаратные средства для разработки «Student’s attendance system» 16
2.1 Языки программирования Kotlin, C++; 17
2.2 Интегрированные среды разработки Android Studio, Arduino; 18
2.3 Модуль распознавания отпечатков пальцев FPM10A 19
3 Тестирование и эксплуатация программного средства 27
3.1 Эргономичность использования программного средства «Student attendance system» 27
3.2 Инструкция по эксплуатации 28
ЗАКЛЮЧЕНИЕ 33
СПИСОК СОКРАЩЕНИИ 34
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 35
ПРИЛОЖЕНИЕ А 37
ПРИЛОЖЕНИЕ Б 38
ПРИЛОЖЕНИЕ В 39

ВВЕДЕНИЕ

Сегодня онлайновые системы управления работой позволяют управлять организациями точно и эффективно. Деловая активность, успеваемость учеников в классе, поведение сотрудников в рамках рабочего графика и другие внутренние и внешние операции компании должным образом учитываются с помощью различных методов мониторинга.

В организационной структуре поведение сотрудников оценивается на основе выполнения работы, а определенные функции оценки контролируются с помощью ежедневной посещаемости.

Тот же сценарий можно наблюдать при оценке успеваемости студентов в классе. Учащиеся должны соблюдать требуемую посещаемость и расписание, что помогает педагогам оценить слабые и сильные стороны каждого ученика в классе, что обеспечивает целостность информации, в которой заинтересованы и могут узнать родители и другие внешние заинтересованные стороны.

Как вы знаете, технологии оказывают значительное влияние на обучение и преподавание. Будущая роль технологий в содействии обучению заключается в том, чтобы облегчить жизнь людей, чтобы контроль посещаемости можно было осуществлять одним щелчком мыши [1].

Актуальность темы, рассматриваемой в данной работе, заключается в том, что, несмотря на значительные изменения во всех странах, сфера образования в нашей стране сталкивается с проблемой использования примитивных и традиционных методов учета и контроля посещаемости занятий, таких как проверка, перекличка, имена, подписание документов и создание коллективного журнала посещаемости. Это происходит потому, что. Этот процесс отнимает много времени и иногда дает неверные оценки посещаемости. Это увеличивает нагрузку на учителя при оценке успеваемости учеников. Это привело к разработке программной системы управления посещаемостью учеников на основе биометрических данных со сканеров отпечатков пальцев, основанной на концепции веб-сервиса, взаимодействующего с базой данных на удаленном сервере. Преимущества реализации данного проекта заключаются в следующем

- Сокращение бумажной работы и экономия времени
- Устранение дублирующего ввода данных и ошибок при учете посещаемости;
- Повышение безопасности и конфиденциальности благодаря настройкам авторизации на основе ролей пользователей.

Целью данной работы является разработка программного инструмента для контроля посещаемости студентов на основе биометрических данных со сканеров отпечатков пальцев.

Предметом исследования является мониторинг посещаемости студентов, т.е. сектор образования.

Объектом исследования является ПС на основе биометрических данных со сканеров отпечатков пальцев.

Для достижения поставленной цели в данном исследовании были поставлены следующие задачи

- Провести теоретический анализ современных биометрических методов;
- Определить и уточнить понятия "идентификация" и "аутентификация";
- Изучить методы идентификации, используемые в системах учета посещаемости;
- Изучить и проанализировать существующие системы управления и мониторинга посещаемости и выявить их преимущества и недостатки; и
- Объяснить необходимость создания системы контроля посещаемости.
- Выбрать программное и аппаратное обеспечение, необходимое для разработки программных средств.
- Разработать и внедрить программное средство для управления посещаемостью учеников на основе биометрических данных сканера отпечатков пальцев.
- Протестировать разработанное программное средство "Система мониторинга посещаемости учащихся".

При написании данной работы был использован широкий спектр общелогических и специальных методов исследования. Так, при исследовании и определении термина "аутентификация личности" использовались общие методы анализа, синтеза и обобщения информации на основе использованной литературы и материалов.

Основные источники, использованные в данной работе, можно разделить на несколько категорий. Первая - теоретический материал. Сюда входят все документы PL и IDE. Вторая - официальные сайты международных организаций и исследовательских центров.

Научная новизна данной работы заключается в использовании биометрических данных как средства контроля и мониторинга посещаемости в образовательных учреждениях.

Теоретическая значимость работы заключается в актуальности изучения информационных технологий в образовании, т.е. совместного использования аппаратного и программного обеспечения.

Практическая значимость данной работы заключается в том, что PS может быть усовершенствована как инструмент для контроля посещаемости лекций в высших учебных заведениях и как средство учета посещаемости сотрудников в компаниях.

Работа имеет традиционную структуру и состоит из введения, трех глав, заключения, списка литературы и приложения. Во введении описывается актуальность темы исследования, цели и задачи диссертации, а также структура и план глав.

1. Анализ современных методов биометрических данных

Биометрия — это метод измерения физических характеристик человека для подтверждения его личности. Это могут быть физиологические характеристики, такие как отпечатки пальцев или глаз, или поведенческие характеристики, такие как уникальные способы решения головоломок аутентификации безопасности. Чтобы биометрические данные были полезными, они должны быть уникальными, постоянными и собираемыми. После измерения информация сравнивается и сопоставляется в базе данных.

Каждый раз, когда вы разблокируете экран своего смартфона с помощью системы распознавания лиц, запрашиваете у Siri прогноз погоды или входите в свой банковский онлайн-счет с помощью отпечатка пальца, вы используете биометрические данные. Возможно, вы используете эту технологию каждый день для подтверждения своей личности и связи с вашими персональными устройствами, но есть и множество других применений биометрии.

Например, полиция может собирать ДНК и отпечатки пальцев на месте преступления, а система видеонаблюдения может анализировать походку и голос подозреваемого. В медицинском секторе проверка здоровья может включать сканирование сетчатки глаза и генетическое тестирование. Кроме того, при использовании кредитной карты в кассе эмитент часто предоставляет подпись, которая может быть проанализирована, если эмитент подозревает подделку.

Типы биометрических данных существуют различные типы биометрических данных. Ниже описаны шесть из них:

– Распознавание лица. Измеряет уникальный рисунок лица человека путем сравнения и анализа контуров лица. Используется службами безопасности и правоохранительными органами в качестве метода аутентификации личности и разблокировки устройств, таких как смартфоны и ноутбуки;

– Распознавание радужной оболочки глаза. Определяет уникальный рисунок радужной оболочки глаза, цветную область вокруг зрачка. Широко используется в системах безопасности, но обычно не применяется на потребительском рынке;

– Сканеры отпечатков пальцев. Захватывают уникальный рисунок гребней и впадин пальцев. Многие смартфоны и некоторые ноутбуки используют эту технологию в качестве пароля для разблокировки экрана;

– Распознавание голоса. Измеряет уникальные звуковые волны в вашем голосе, когда вы говорите в устройство. Эта технология используется банками для проверки личности при звонке по поводу счета, а также умными колонками, такими как Amazon Alexa, для передачи инструкций;

– Ручная геометрия. Измеряет и записывает длину, толщину, ширину и площадь поверхности руки человека. Эти устройства появились еще в 1980-х годах и широко использовались в системах безопасности;

– Поведенческие свойства. Анализирует взаимодействие с компьютеризированными системами. Нажатия клавиш, почерк, манера ходьбы, использование мыши и другие виды поведения могут быть использованы для оценки того, кто вы или насколько хорошо знакомы с вводимой вами информацией.

ПС на основе биометрических данных в настоящее время широко распространены на рынке информационных технологий.

1.1 Преимущества и недостатки имеющихся систем

Системы мониторинга контроля посещаемости:

1. сетевая система мониторинга посещаемости:

Считаясь одной из самых инновационных технологий автоматизации контроля посещаемости студентов (сотрудников), эта система контроля посещаемости эффективна и экономит время. Отсутствует риск потери данных о посещаемости, а эффективный вывод результатов позволяет легко добиваться различных видов повторной посещаемости. Система позволяет пользователям просто зарегистрировать свою идентификационную информацию (например, имя, факультет, номер студента и т.д.) и автоматически ввести время входа; недостатком PS является то, что в случае ошибки при входе в систему может быть введена недействительная дата и время посещения. Для решения проблем такого рода вокруг объектов в компаниях и университетах устанавливаются системы мониторинга для повышения безопасности и предотвращения аномалий в организации.

Примеры SAR

– Schoology [5];
– ClassDojo [6];
– GoGuardian Teacher [7];
– SAP Litmos [8];
– Platonus [9].

2. RFID (радиочастотная идентификация):

RFID определяется как радиочастотная идентификация и была разработана в 1985 году и первоначально использовалась для отслеживания и доступа. Известная как система беспроводных устройств, она является бесконтактной, считываемой и эффективно присутствует в производственных и других агрессивных средах, где нет этикеток со штрих-кодами [10].

RFID на самом деле не является новой технологией, но в последнее время она быстро завоевала внимание благодаря своей низкой стоимости и достижениям в других областях вычислительной техники, которые открывают больше возможностей для применения RFID сочетает в себе радиочастотную и микрочиповую технологии для идентификации, мониторинга, защиты и инвентаризации объектов интеллектуальные системы, которые могут быть использованы для идентификации, мониторинга, защиты и инвентаризации

объектов. В простейших системах RFID используется небольшой чип, называемый меткой, который содержит идентифицирующую информацию и передается на RFID-считыватель; системы контроля посещаемости на основе RFID имеют потенциал для предоставления большего количества услуг по автоматизации процессов в образовательных учреждениях. Интеграция с другими обществами в кампусе легко автоматизируется и контролируется [12].

Слабые стороны радиочастотного SAR, которые касаются обновления системы и упаковки компонентов. Информация об отслеживании обновляется только тогда, когда манера находится в пределах досягаемости и возможна связь с системой. Существует также возможность фальсификации посещаемости. Радиочастотные SAR:

– RF-Campus [13];

– uAttend [14].

3. ПС на основе биометрии.

В мире инновационных технологий биометрия проложила путь к более совершенной идентификации и в итоге стала широко использоваться для автоматической идентификации. Для каждой конкретной системы, описанной ниже, используются различные биометрические параметры.

Биометрические системы идентифицируют человека только один раз, поскольку использование биометрии считается безопасным подходом при контроле посещаемости. Их можно разделить на следующие категории: отпечатки пальцев, голос, ладонь, ДНК, радужная оболочка глаза, подпись или распознавание лица.

Идентификация отпечатков пальцев человека известна как одна из самых передовых биометрических технологий и широко используется в криминалистических лабораториях и подразделениях идентификации [15, 16]. В настоящее время она также используется на предприятиях, в научных учреждениях и всеми расширенными пользователями в системах контроля посещаемости и безопасности.

Голосовые методы аутентификации - это еще один вид биометрической защиты, который устраняет возможность фальсификации посещаемости с помощью других биометрических и не биометрических методов контроля посещаемости. Он также служит в качестве защиты паролем при входе в помещение и не может быть подделан одним голосовым признаком. Стоит дорого и обычно подходит для крупных предприятий [17].

Другой популярной биометрической технологией является процесс распознавания ладони, особенно в мониторинге посещаемости. Благодаря прочности и другим генетическим характеристикам, методики определения точности ладони способствуют развитию и повышению надежности биометрической безопасности. Также были предложены методы определения формы ладони [18], которые могут применяться в различных ситуациях (например, при контроле посещаемости, уголовных расследованиях, медицинских осмотрах).

Информация о ДНК (дезоксирибонуклеиновой кислоте) и профилирование проложили путь к вкладу профилирования в идентификацию и распознавание. Уникальность ДНК человека отражает физические и поведенческие характеристики различных пользователей, что делает мошенничество и аномалии менее вероятными, особенно при организационном наблюдении и контроле.

В настоящее время рассматриваются другие системы многофакторной аутентификации, сочетающие в себе биометрию лица, радужную оболочку глаза и распознавание зубов, которые являются отличительными чертами систем наблюдения за идентификацией личности. В некоторых организациях распознавание лица пользователя может выступать в качестве автоматического ключа для доступа к внутренней среде или просто для входа в системы, требующие сложных сенсорных камер.

Яркие примеры ПС контроля посещаемости на основе биометрии включают:

– Биометрическая система учета рабочего времени и посещаемости, Mantra [19].

1.2 Понятие и типология «идентификации» и «аутентификации» личности

Традиционные методы аутентификации, такие как надежное имя пользователя и пароль, аутентификация на основе знаний и двухфакторная аутентификация на основе SMS, вышли из употребления из-за ряда уязвимостей безопасности, начиная от перехвата учетных записей и заканчивая фишингом и социальной инженерией. В результате ИТ-отделы ищут более надежные системы аутентификации, которые снижают вероятность кражи и мошенничества.

Биометрическая аутентификация - это процесс безопасности, который использует уникальные биологические особенности, такие как сетчатка глаза, голос, черты лица и отпечатки пальцев, для проверки личности пользователя. Системы биометрической аутентификации хранят эти биометрические данные для проверки личности пользователя при доступе к его счету. Поскольку эти данные уникальны для каждого отдельного пользователя, биометрическая аутентификация, как правило, более безопасна, чем традиционная многофакторная аутентификация.

Идентификацию и аутентификацию нелегко отличить друг от друга, особенно когда они происходят в одной и той же транзакции. Хотя они могут показаться синонимами, это два разных процесса. Основное различие между ними заключается в том, что идентификация подразумевает предоставление идентификатора, в то время как аутентификация подразумевает проверки, проводимые для обеспечения достоверности заявленного идентификатора.

Проще говоря, процесс идентификации подразумевает утверждение личности, а процесс аутентификации - подтверждение этой личности.

Наиболее распространенные и традиционные методы идентификации и аутентификации в существующих ПС:

– Идентификация пользователя: это наиболее стандартная форма идентификации и наиболее часто используемый метод идентификации в организациях для отличия пользователей от других пользователей. Каждый раз, когда пользователь вводит идентификатор пользователя в процессе аутентификации, он сообщает системе, что хочет быть распознанным по этому идентификатору, инициируя процесс аутентификации пользователя и предоставляя ему соответствующие ресурсы;

– MAC-адрес: каждому компьютеру присваивается 48-битное число, называемое адресом управления доступом к среде (MAC), для уникальной идентификации. Ранее MAC-адрес был встроен в аппаратное обеспечение устройства и не мог быть изменен конечным пользователем. Однако теперь MAC-адрес большинства сетевых устройств настраивается в программном обеспечении и может быть изменен пользователем. Таким образом, они больше не считаются уникальными и безопасными идентификаторами;

– IP-адреса: MAC-адрес помогает определить физическое местоположение компьютера, а IP-адрес помогает определить логическое местоположение системы; IP-адреса распределяются между всеми системами, использующими сетевой протокол TCP/IP; IP-адреса используются для идентификации IP-адресов в пулах адресов. диапазон пулов адресов, так что они могут быть разделены для формирования подсетей. Различные системы в разных подсетях могут иметь одинаковые IP-адреса, но они должны быть уникальными в пределах одной подсети устройств. Он также не является надежным идентификатором, поскольку может быть легко изменен пользователем;

– Персональный идентификационный номер (ПИН): ПИН предоставляется пользователю, чтобы определить, имеет ли пользователь право выполнять какие-либо действия в системе. Этот метод наиболее часто встречается в банковских операциях и является второй формой идентификации пользователя;

– Идентификационные бейджи: идентификация может быть как физической, так и электронной. Например, организации используют бейджи для идентификации сотрудников. Это означает именной бейдж с именем пользователя и его фотографией. Это делается для того, чтобы предотвратить вход людей, которые не работают в данном учреждении, и процесс аутентификации в этом случае происходит в самой точке входа в организацию. Хотя этот метод аутентификации может показаться эффективным, во многих случаях он используется персоналом неправильно, и охранники иногда могут ошибиться, сравнивая фотографию человека с бейджем;

– Электронная почта: в последние годы новые формы идентификации, такие как адреса электронной почты, также стали уникальными формами

идентификации. Однако они являются уникальными лишь условно и не должны использоваться как элемент, заслуживающий доверия. Поскольку адреса электронной почты можно легко подделать, организации должны использовать другие факторы аутентификации, чтобы связать адрес электронной почты с пользователем.

Традиционные методы аутентификации, такие как надежное имя пользователя и пароль, аутентификация на основе знаний и двухфакторная аутентификация на основе SMS, вышли из употребления из-за целого ряда уязвимостей безопасности, от перехвата учетных записей до фишинга и социальной инженерии. В результате ИТ-отделы ищут более надежные системы аутентификации, которые снижают вероятность кражи и мошенничества.

Биометрическая аутентификация – это процесс безопасности, использующий уникальные биологические особенности, такие как сетчатка глаза, голос, черты лица и отпечатки пальцев, для проверки личности пользователя. Системы биометрической аутентификации хранят эти биометрические данные для проверки личности пользователя при доступе к его счету. Поскольку эти данные уникальны для каждого отдельного пользователя, биометрическая аутентификация, как правило, более безопасна, чем традиционная многофакторная аутентификация.

1.3 Системы мониторинга контроля посещаемости в сфере образования

Мировой рынок программного обеспечения для учета рабочего времени и посещаемости сегментируется по типу, организационной структуре и географии. По типу рынок делится на карты учета рабочего времени, бесконтактные карты, бейджи, брелоки, биометрию, веб-станции входа и интерактивный голосовой ответ (IVR) [3].

Автоматизированные системы могут быть разных типов. Электронные метки, бейджи со штрих-кодом, биометрия, такая как распознавание пальцев, рук и глаз, использование карт с магнитной полосой и различные типы сенсорных экранов - вот лишь несколько примеров из множества систем, используемых сегодня. Эти системы работают очень хорошо с точки зрения регистрации поведения сотрудников и в то же время оповещения менеджеров, когда это необходимо [4].

Независимо от того, ручной это процесс или автоматический, основной процесс передачи данных остается неизменным, как это видно на примере контроля посещаемости. Процесс ввода позволяет сотрудникам и ученикам вводить идентификационные данные путем нажатия на табель учета рабочего времени, прикосновения к идентификатору или введения пальца в аппарат получателя. При обработке дат, полученных на этапе ввода, система мониторинга времени и посещаемости проверяет информацию и отправляет ее другим функциям системы мониторинга. На этапе вывода на экран

выводятся результаты обработки данных, которые называются тайм-аутом студента. Это показано на рисунке 1 ниже:

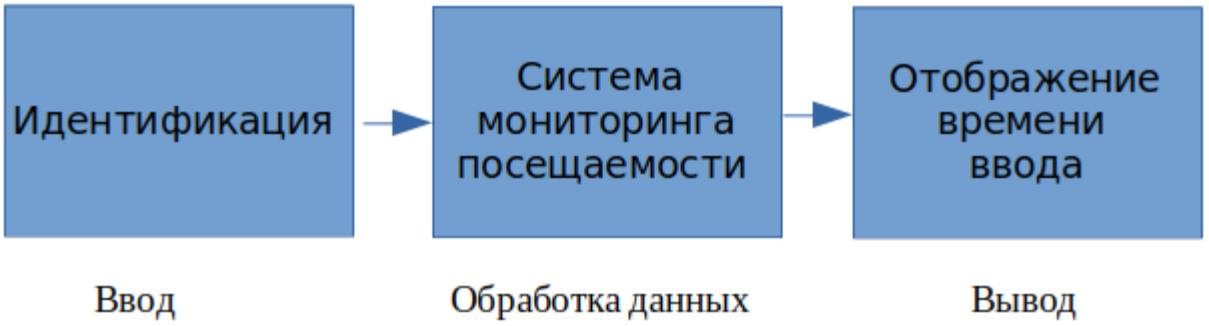

Рисунок 1.3.1 - Базовая структура системы мониторинга посещаемости.

В некоторых случаях фаза завершения завершается сообщением или уведомлением об обновлениях конечному пользователю. В случае со студентами некоторые учебные заведения внедрили в свои системы мониторинга посещаемости функцию уведомления родителей о статусе посещаемости через SMS. Такие механизмы могут мотивировать студентов активно посещать занятия в соответствии с заранее установленным расписанием учебного заведения.

Каждая КС мониторинга имеет свои уникальные особенности и характеристики. Вот некоторые из основных характеристик мощной системы мониторинга посещаемости

– Безопасность: необходимо иметь надежную систему безопасности, чтобы обеспечить конфиденциальность и безопасность передачи данных;

– Надежность: вся информация должна быть корректной и объективной, чтобы предоставлять достоверную информацию для организации в целом и особенно для конечных пользователей; и

– Эффективность: биометрия является хорошим примером эффективной системы контроля посещаемости. Она позволяет биометрическим сканерам обеспечивать квалифицированный уровень выдачи данных целевому пользователю, поскольку отпечаток пальца или руки человека, используемый при входе в систему, является уникальным;

– Точность и своевременность: все данные, вводимые в систему контроля посещаемости, должны быть точными и своевременными. Наличие своевременной информации имеет решающее значение.

1.4 Описания использования биометрических данных сканера отпечатков пальцев

Идентификация по отпечаткам пальцев предполагает считывание рисунка на кончике пальца. Существуют различные подходы к сопоставлению отпечатков пальцев. Некоторые из них имитируют традиционные

полицейские методы считывания рисунка, другие используют устройства прямого считывания, а третьи являются немного более уникальными, например, муаровые полоски или ультразвуковые функции. Устройства идентификации по отпечаткам пальцев используются чаще, чем любая другая биометрическая технология.

Системы идентификации по отпечаткам пальцев преобразуют люминесцентное изображение отпечатка пальца в цифровой код, который используется в программном обеспечении для регистрации (регистрация отпечатков пальцев) и верификации (аутентификация и сопоставление зарегистрированных пользователей).

Сканеры используют датчики изображения для получения высококонтрастных изображений с высоким разрешением и практически без искажений. Ряд мощных алгоритмов извлекает данные из изображения и отображает отличительные особенности отпечатков пальцев.

Эти данные преобразуются в закодированную двоичную строку, известную как цифровой рисунок, и сохраняются в базе данных. Само изображение отпечатка пальца никогда не сохраняется. Чтобы идентифицировать или проверить отпечаток пальца, уникальный алгоритм сопоставления сравнивает ранее сохраненный образец с новым шаблоном, созданным на основе особенностей, извлеченных из входного отпечатка пальца на оптическом модуле. Весь процесс сопоставления занимает примерно одну секунду. Аутентификация может быть выполнена локально на устройстве или на сервере, в зависимости от конфигурации системы.

В данной статье описывается разработка программного инструмента для управления посещаемостью на основе биометрических данных, а именно отпечатков пальцев. По сравнению с вышеперечисленными методами, система биометрических данных на основе отпечатков пальцев признана лучшей и наиболее защищенной от фальсификации данных пользователя.

2 Программные и аппаратные средства для разработки «Student’s attendance system»

Для разработки ПС «Student’s attendance system» необходимы следующие программные и аппаратные средства:

– Языки программирования Kotlin,C++;

– Интегрированные среды разработки Android Studio, Arduino;

– Модуль распознавания отпечатков пальцев FPM10A.

2.1 Языки программирования Kotlin, C++;

Kotlin – это статически типизированный язык программирования, который был создан в 2011 году в компании JetBrains. Он работает на платформе Java Virtual Machine (JVM) и может быть использован для разработки мобильных приложений для Android, веб-приложений и серверных приложений.

Kotlin является языком с открытым исходным кодом и имеет синтаксис, похожий на языки Java и C#. Он предоставляет множество возможностей для создания безопасного, высокопроизводительного и легко поддерживаемого кода, таких как проверка на нулевые значения, расширения функций и инлайн-функции.

Kotlin также поддерживает функциональное программирование и имеет многочисленные расширения для разработки асинхронного кода, например, асинхронных функций и корутин.

Кроме того, Kotlin имеет хорошую интеграцию с другими языками, такими как Java, JavaScript и Swift, что делает его привлекательным для использования в комбинации с другими технологиями.

Kotlin становится все более популярным языком программирования, особенно в области разработки мобильных приложений для Android, и считается одним из лучших языков для начала изучения программирования.

В разрабатываемой мной ПС «Student’s attendance system» ЯП Kotlin используется для написания бэкенда и фронтона, так как данный ЯП особенно хорошо подходит для создания инфраструктуры, такой как сетевые серверы, инструменты и системы.

C++ является одним из языков программирования, который можно использовать для программирования на платформе Arduino. Arduino - это небольшая платформа, которая используется для создания электронных проектов. Платформа содержит микроконтроллер, который управляет внешними устройствами и датчиками.

В Arduino используется язык программирования Wiring, который основан на C++. Язык Wiring имеет многие особенности C++, такие как классы и наследование, но также имеет упрощенный синтаксис для работы с микроконтроллером.

Для программирования Arduino на C++ необходимо использовать интегрированную среду разработки (IDE) Arduino, которая предоставляет все необходимые инструменты для создания и отладки программ.

В Arduino можно использовать многие функции C++, такие как ввод-вывод, работа с памятью, управление потоками и многие другие. Кроме того,

с помощью библиотек, которые предоставляются в Arduino IDE, можно упростить процесс разработки и добавления функциональности к вашим проектам.

Если вы уже знакомы с языком программирования C++, то переход на программирование Arduino на этом языке может быть относительно легким и позволит создавать более сложные проекты. Однако, если вы новичок в программировании, то может потребоваться некоторое время, чтобы изучить основы программирования на C++ и работу с платформой Arduino.

2.2 Интегрированные среды разработки Android Studio, Arduino;

Android Studio — это официальная интегрированная среда разработки (IDE) для разработки приложений на платформе Android. Эта IDE основана на среде разработки IntelliJ IDEA от JetBrains и предоставляет инструменты для создания, сборки, отладки и развертывания приложений на Android.

Некоторые из функций, доступных в Android Studio, включают в себя:

1. Редактор кода: Android Studio предоставляет редактор кода с функциями подсветки синтаксиса, автозаполнения, рефакторинга, контекстной помощи и другими инструментами, которые позволяют разработчикам писать и отлаживать код на языках программирования Java и Kotlin.

2. Инструменты разработки пользовательского интерфейса: Android Studio предоставляет визуальный редактор макетов, который позволяет разработчикам создавать и настраивать макеты пользовательского интерфейса. Визуальный редактор макетов позволяет быстро создавать интерфейсы, используя перетаскивание и редактирование элементов интерфейса.

3. Сборка и запуск: Android Studio позволяет легко собирать и запускать приложения на эмуляторе или на реальном устройстве. Приложения могут быть собраны в разных режимах, таких как отладочный или релизный режим.

4. Отладка: Android Studio предоставляет инструменты отладки, которые помогают разработчикам находить и исправлять ошибки в коде. Эти инструменты включают в себя возможность установки точек останова, просмотра значений переменных и выполнения шаг за шагом.

5. Инструменты управления проектом: Android Studio предоставляет

инструменты для управления проектом, такие как система контроля версий и инструменты сборки проекта.

6. Поддержка многопоточности: Android Studio предоставляет инструменты для управления потоками и синхронизации, которые помогают разработчикам создавать приложения, которые работают быстро и эффективно.

Android Studio является одной из самых популярных IDE для разработки приложений на платформе Android, и предоставляет разработчикам все необходимые инструменты для создания высококачественных приложений.

Arduino

«Arduino — это электронная платформа с открытым исходным кодом, основанная на простом в использовании аппаратном и программном обеспечении. Он предназначен для всех, кто делает интерактивные проекты. Arduino воспринимает окружающую среду, получая входные данные от многих датчиков, и воздействует на окружающую среду, управляя освещением, двигателями и другими приводами.» [23].

Выбор данного IDE можно аргументировать как его необходимость для написания функционального кода для совместной работы устройств сканера отпечатка пальца, т. е. датчика отпечатка пальца FPM10A и Arduino Uno.

2.3 Модуль распознавания отпечатков пальцев FPM10A

Модули идентификации отпечатков пальцев FPM10A широко используются в системах безопасности. Эти датчики содержат микросхему, которая обрабатывает изображение и выполняет вычисления, необходимые для определения соответствия между записанными и текущими данными. При наличии соответствующего программного обеспечения изображение отпечатка пальца, может быть, даже выведено на дисплей. Замечательно, что существует отдельная библиотека для Arduino, с помощью которой можно легко и быстро настроить датчики.

Датчик имеет шесть контактов, которые обозначены на рисунке 2 ниже:

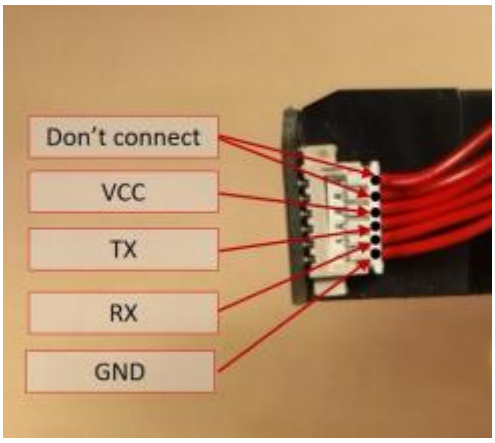

Рисунок 2.3.1 - Входные и выходные контакты модуля FPM10A

VCC – напряжение 5V (так же 3.3V)
TX – RX (цифровой вывод 2, последовательный программный код)
RX – TX (цифровой вывод 3, последовательный программный код)
GND – GND

Для программирования этого датчика необходимо скачать библиотеку AFS library[24]

Библиотек AFS — предназначена для облегчения работы с датчика отпечатка пальцев. Она имеет большой диапазон функций, для чтения/записи, удаления, пересохранения, обновления, а также иллюстрации. В разработке аппаратной чатси ПС работе будут использоваться следующие функции:

–TempleteNum;
– GenImg;
– Img2Tz;
– Store;
– и основные функции Arduino.

Эти функции необходимы для того, чтобы была возможность параллельное использования нескольких датчиков и передачи информации между ними по средство ПС. Вышеперечисленный функционал библиотеки AFS, позволяет реализовать сбор данных во внешнем хранилище, при использовании дополнительных ПО.

Схема использования данного модуля с МК Arduino Uno, достаточна проста, следовательно использования данного датчика позволяет сократить время и уменьшить расходы. Схема подключения к Arduino на рисунке 3:

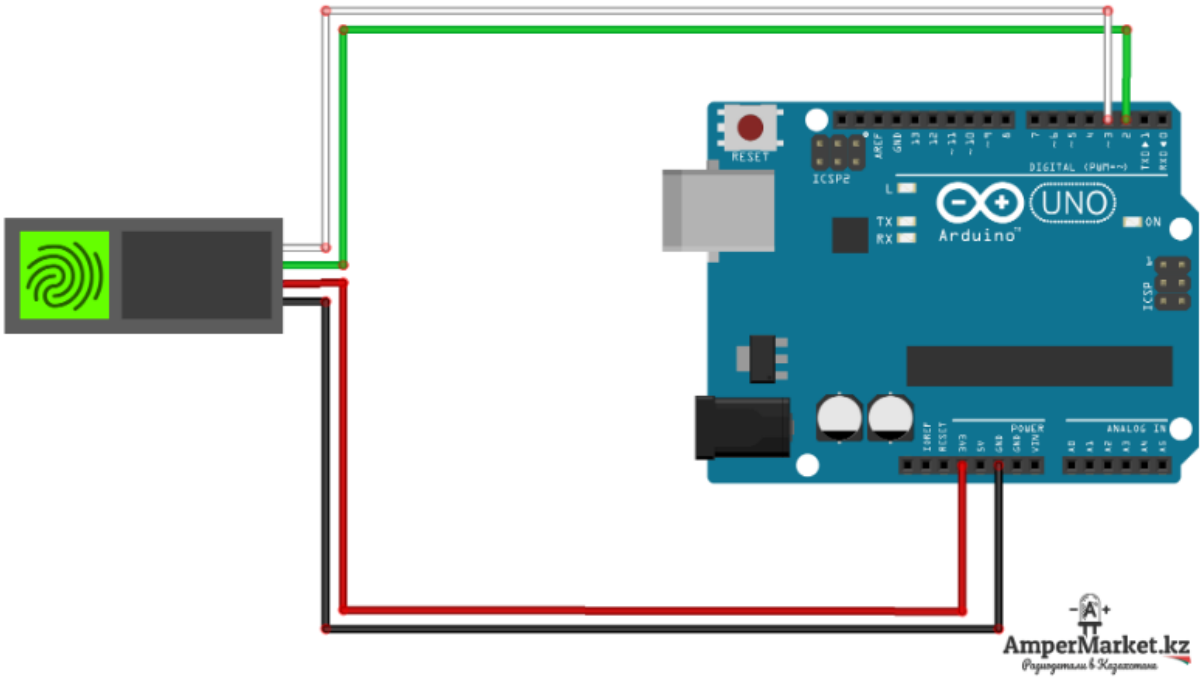

Рисунок 2.3.2 - Схема подключения датчика отпечатка пальца FPM10A к микроконтроллеру Arduino Uno[25]

Код подключения в предоставляет собой 3 блока:

– объявления входных пинав и импортирование библиотек;

– функция void setup ()— инициализируем датчик отпечатков пальцев переменные;

– функция loop () – код постоянно проверяет наличие отпечатков пальцев. Если датчик обнаруживает сохраненный отпечаток пальца, Arduino сохраняет соответствующий идентификатор в переменной ID.

2.4 Практическая часть — реализация программного средства «Student's attetndance system», для контроля посещаемости студентов на основе биометрических данных

В мире технологий биометрия играет эффективную роль в идентификации людей. Биометрические данные или характеристики тесно связаны с человеком и не могут быть забыты, переданы, украдены или легко взломаны. Поскольку биометрия может лучше решать проблемы контроля доступа, мошенничества и кражи, все больше и больше организаций рассматривают биометрию как решение своих проблем безопасности.

Характеристики могут однозначно идентифицировать человека, заменяя или дополняя традиционные методы безопасности, предоставляя два

основных улучшения: личную биометрию нельзя легко украсть, и человеку не нужно запоминать пароли или коды.

Моя биометрическая система посещаемости учащихся на базе Android обеспечивает безопасность, контроль доступа, надежность, эффективность и лучшую производительность. Система будет иметь данные о каждом ученике и проверять ежедневную посещаемость каждого ученика, использующего устройство. В этом проекте интерфейс использует XML, Android-Kotlin, а сервер —SQLite. В качестве IDE используется Android Studio.

Структура БД для ПС «Student’s attendance system»:

Система для хранения пользовательских сведений, данных по посещаемости, а так же отпечатков пальцев использует БД SQLite.

Архитектура пользователей иллюстрирована на рисунке 4. В проекте используется 3 user-a, (1 админ, 2 типа пользователей)

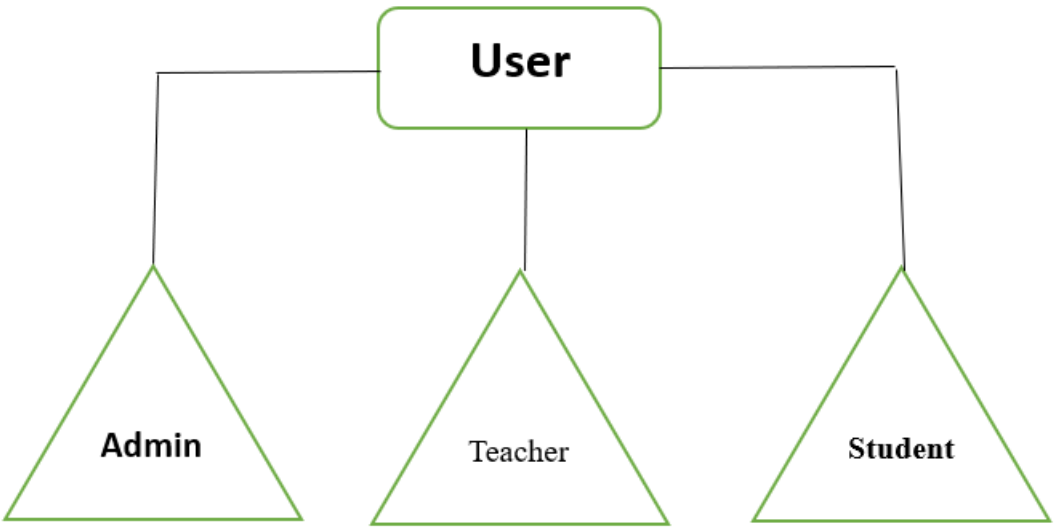

Рисунок 2.4.1- Пользовательская структура системы

а) имеет доступ только к индивидуальных данным

б) возможность мониторинга посещений, курсов (при условии преподавания данного занятия)

в) неограниченный доступ

Разработка аппаратной части программы:

Предлагаемый мной система состоит из трех основных частей, чтобы сделать систему более гибкой и подходящей для использования в любом институте в зависимости от необходимости. Частями предлагаемой системы являются считыватель отпечатков пальцев (FPM10A), блок управления

(Arduino Uno) и Приложение, который соединяется с Интернетом, как показано на рисунке 5:

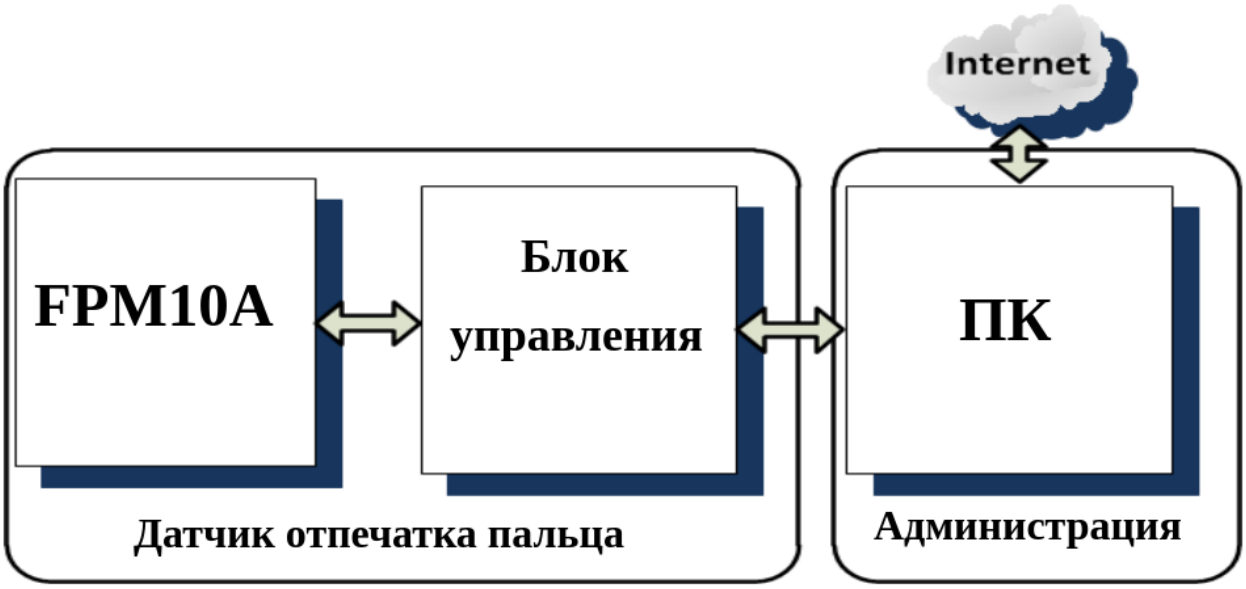

Рисунок 2.4.2 - Структурная схема предлагаемой системы

Устройство для считывания отпечатков пальцев. Это устройство работает путем записи и сопоставления отпечатков пальцев человека. Оно интегрируется с блоком управления для создания устройства, называемого считывателем отпечатков пальцев. Устройство считывания отпечатков пальцев должно быть установлено в классе и подключено к ПК или серверу управления.

Блок управления. Это устройство управляет устройством идентификации отпечатков пальцев и взаимодействует с сервером для загрузки и выгрузки данных. Блок управления состоит из микроконтроллера Arduino Uno. Блок управления имеет интерфейс для работы считывателя отпечатков пальцев.

Приложение используется для управления системой учета посещаемости по отпечаткам пальцев и ее приложениями. Как правило, она состоит из системы сбора данных (система зачисления). Вначале студентов просят записать свои отпечатки пальцев во время процесса регистрации. Они просто прикладывают палец к считывателю отпечатков пальцев. Затем система автоматически отправляет имя студента вместе с датой и временем на блок управления. Система имеет удобный интерфейс для регистрации и проверки отпечатков пальцев. Однако наиболее важными являются отпечатки пальцев и идентификационный номер ученика. После первоначальной регистрации предоставленные данные можно использовать в качестве списка посещаемости лекций.

Блок-схемы Основные блок-схемы, объясняющие принцип работы системы, показаны на рисунках 6 и 8, причем две блок-схемы описывают

основные функции, такие как зачисление новых отпечатков пальцев и зачисление студенческих событий, используемых для проверки посещаемости. Рисунок 6 называется таблицей регистрации студентов и используется серверным приложением для регистрации отпечатков пальцев студента. Это используется для регистрации посещаемости студента в классе. Как показано на рисунке 3, когда ученик инициирует регистрацию отпечатков пальцев, система генерирует первый шаблон, запрашивает повторную регистрацию и создает второй шаблон. Затем эти два шаблона сравниваются, чтобы убедиться в правильности регистрации, и шаблон отпечатка пальца сохраняется в базе данных вместе с информацией об ученике.

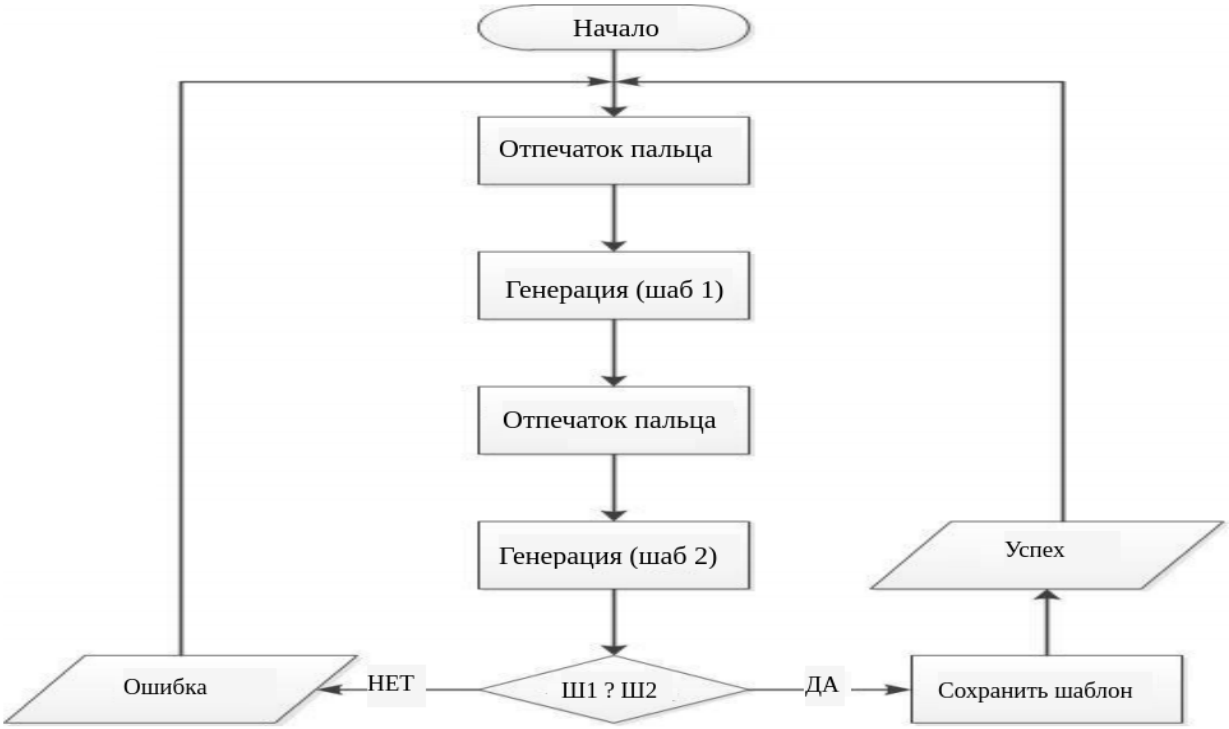

Рисунок 2.4.3 - Блок-схема зачисления студентов

Ш1 — первый отпечаток пальца пользователя (студента)

Ш2 — второй отпечаток пальца пользователя (студента)

Отпечаток пальца сохраняется в базе в виде байт кода для у эффективного сравнения. Перед тем как попасть в основное БД, шаблон считывается с serial-монитора на Arduino IDE. Дальше происходит декодирования данного файла в основанном ПС, и после корректного выполнения вышеперечисленных действий шаблон попадает в базу и присваивается к студенту. Алгоритм показан на рисунке 7.

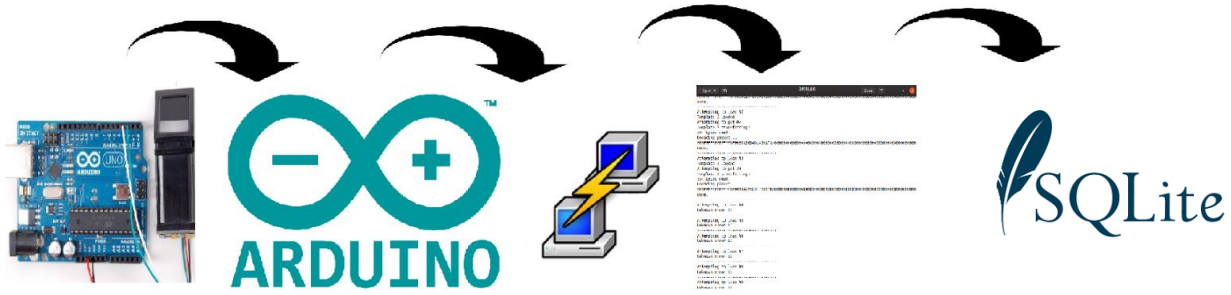

Рисунок 2.4.4 - Программный алгоритм регистрации биометрических данных

На рисунке 9 показан процесс регистрации посещаемости. Он начинается с того, что отпечатки пальцев студента совпадают с ранее зарегистрированным шаблоном отпечатков пальцев. Когда текущий шаблон отпечатка пальца совпадает с ранее зарегистрированным и сохраненным шаблоном отпечатка пальца, устройство идентификации отпечатков пальцев регистрирует посещение по академическому идентификатору студента, дате и времени. Алгоритм схемы на рисунке 8 используется устройством идентификации по отпечаткам пальцев.

Рисунок 2.4.5 - Блок-схема регистрации посещаемости

Ш1 — идентификатор отпечатка пальца от FPM10A
Ш2 — идентификатор отпечатка пальца из БД

Для выполнения программной части второго блока имеется 2 способа:

– запись в хранилища датчика внешних данных, а именно биометрических данных студентов;

– записывать отпечаток пальца и после получения шаблонов, в ПС выполнить сравнение.

При котором на Arduino IDE, вовремя запуски программы для получения отпечатков пальца, заполняется хранилище датчика FPM10A. На рисунке 9 иллюстрирована реализация данного алгоритма.

Рисунок 2.4.6 - Запись шаблонов в хранилище FPM10A

Во втором случае повторяется порядок действий регистрации, но единственным отличием является, сохранение времени в дополнении к байт-коду. Интерфейс состоит из 3 пользовательского доступа, страницы разделены по области разрешения.

3 Тестирование и эксплуатация программного средства

3.1 Эргономичность использования программного средства «Student attendance system»

Эргономика — это совокупность знаний о возможностях, ограничениях и других характеристиках человека, относящихся к проектированию. Эргономический дизайн — это применение этих знаний для проектирования инструментов, машин, систем, задач, рабочих мест и сред, которые безопасны, удобны и эффективны для использования человеком.

Программная эргономика — это подкатегория эргономики, которая занимается проектированием программных систем, а не аппаратного обеспечения. Эргономика программного обеспечения включает в себя понимание потребностей пользователя, проектирование интерфейса, поддержку пользователя и тестирование удобства использования.

"Система управления посещаемостью учащихся на основе биометрических данных отпечатков пальцев" - это программное обеспечение, предназначенное для управления ежедневной посещаемостью учащихся в образовательных учреждениях. Разработанная ПС сокращает ручной труд и позволяет избежать ненужных данных.

Предлагаемый проект системы учета посещаемости на основе отпечатков пальцев решает проблему посещаемости следующими способами

- Учет посещаемости ведется во время лекций, что исключает участие преподавателя и потерю времени;
- Система гибко подстраивается под расписание университета, а управление посещаемостью автоматизировано; и
- отсутствует возможность ложной посещаемости;
- Посещаемость студентов может быть оценена автоматически.

Система также может быть легко использована преподавателями для контроля состояния дисциплины преподавателей в дни лекций. Она также может быть расширена для отображения всей информации о студентах в режиме онлайн.

Основным преимуществом предлагаемой системы является ее низкая стоимость. Рынок биометрических датчиков широк, а датчики на основе отпечатков пальцев в настоящее время являются самыми дешевыми и простыми в использовании, т. е. высокий спрос на этот продукт повлиял на развитие и совершенствование данного типа модуля. К программным преимуществам модулей на основе отпечатков пальцев относятся:

– Простота внедрения;
– Возможность перепрограммирования;
– Перезапись данных;
– Выборочное удаление данных;
– Очистка хранилища;

– Шаблоны могут быть записаны с внешних запоминающих устройств, что позволяет параллельно работать с несколькими датчиками;

– Повышенная безопасность: возможность фальсификации отпечатков пальцев близка к нулю.

3.2 Инструкция по эксплуатации

Программный инструмент 'Student Attendance System' состоит из двух основных частей:

– Программная часть;

– Аппаратная часть.

Программная часть представляет собой приложение для мониторинга и анализа данных. Аппаратная часть состоит из сканера отпечатков пальцев. Для работы с аппаратной частью пользователям, т. е. администраторам и учителям, необходимо иметь следующее (Рисунок 11)

– сканер отпечатков пальцев

– Блок питания для ПК или ноутбука;

– Arduino IDE (опционально, для удаленной передачи данных, реализуя Ethernet или беспроводную связь с аппаратной частью датчика).

Рисунок 3.2.1 - Необходимое оборудование и программное обеспечение

Пользователю (ученику или учителю) не нужно иметь никакого дополнительного программного или аппаратного обеспечения для работы этого программного обеспечения. С другой стороны, у администраторов есть два варианта работы:

– Развернуть локальную базу данных, т. е. SQLite;

– Приобрести или арендовать онлайновый хост;

– Arduino IDE.

При запуске программы, т. е. открытии приложении, первой страницей, которая открывается, независимо от пользователя, является страница 'login'. Эта страница имеет следующие функции

– Определение типа пользователя

– Определение пользователя

– Вход в систему.

После выполнения страницы входа в систему программа начинает генерировать страницы пользователей по типу пользователя и назначать права доступа по вложению. Страница входа в систему показана на рисунке 12.

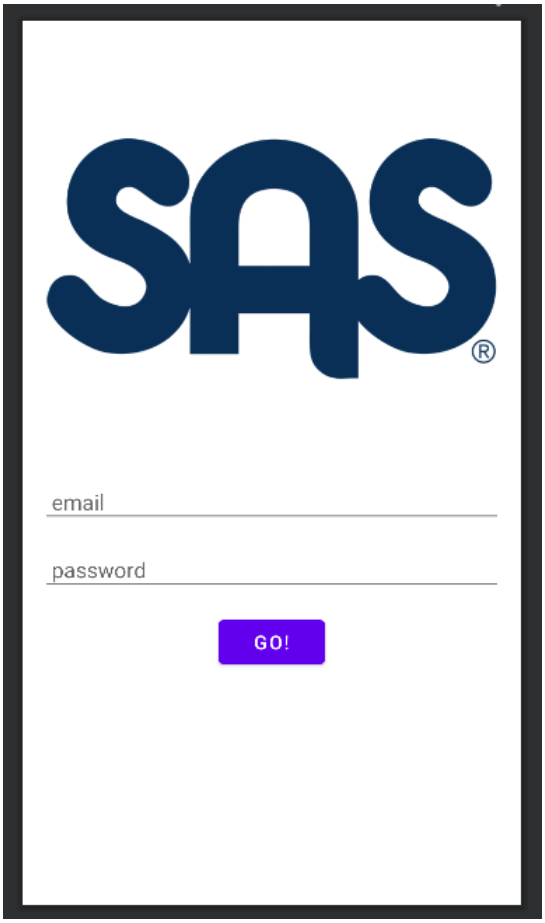

Рисунок 3.2.2 - Вход в систему

Вход в систему выполняется, стандартным образом, вводом логина и порол. После того как заполнены входные поля, программа выполняет проверку правильности введенных данных, при возникновении ошибки

выводит сообщение на экран в виде «Problem». Если все пользовательские данные производится успешно, то в приложении переходит на следующий экраны:

- при вводе данных для открытия страницы админа, открывается экран Admin Activity, на рисунке 13;

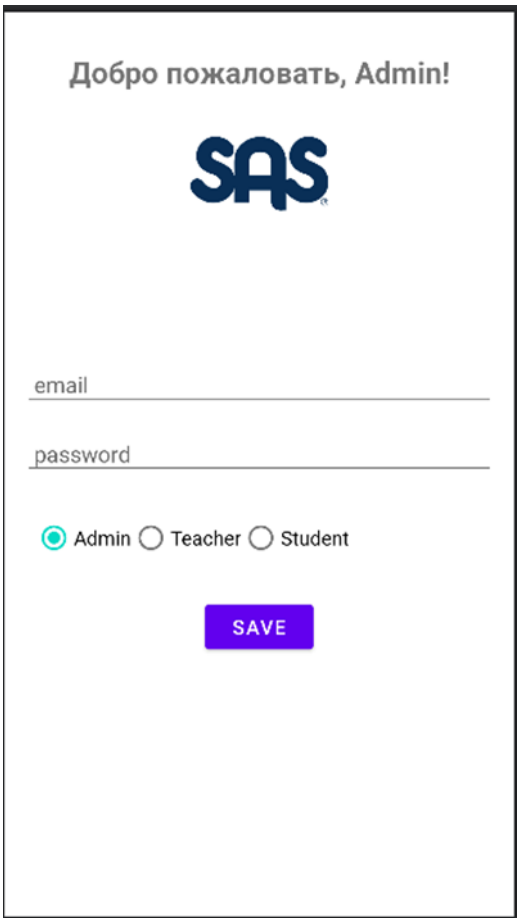

Рисунок 3.2.3 - Admin Activity

Данный экран позволяет добавить пользователя:

– личная информация (почта, фамилия, имя и отчество);

– пароль

– выбрать тип пользователя (админ, преподаватель и студент);

В этом экране пользователь Админ, может добавлять новых пользователь (преподавателей, студентов) и сохранять их в базу данных, чтобы пользователи (преподаватель и студент) могли войти. После заполнение всех полей, на экране отображается сообщение «Пользователь успешно сохранен», при не заполнении одного поля отображается сообщение «Заполните поля». Если все данные были введены правильно, то нажимаем кнопку назад, для того чтобы войти как пользователь (преподаватель, студент).

– при вводе данных студента, открывается экран Student Activity на рисунке 14;

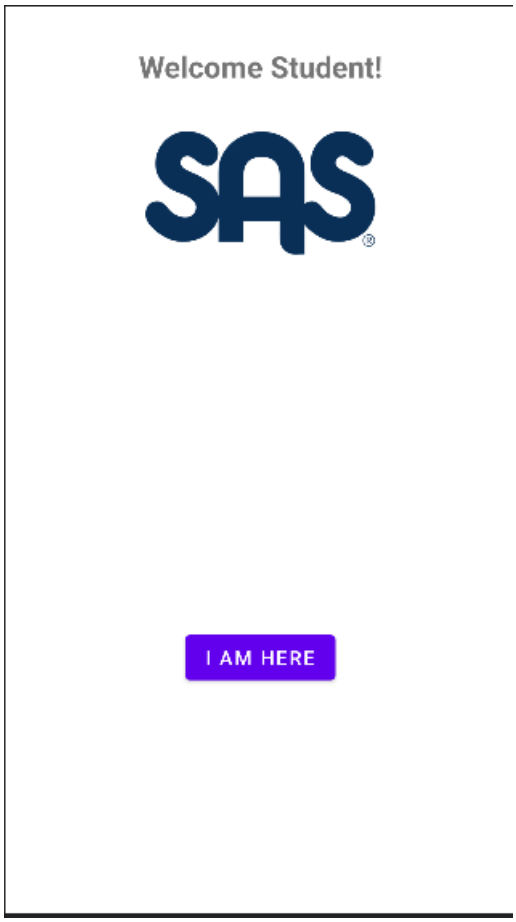

Рисунок 3.2.4 - Student Activity

В данном экране имеется кнопка с надписью «Я, здесь!», кнопка нужен чтобы отметиться на занятии. После того как студент нажмет на кнопку, присутствие студента поступает в базу данных и сохраняется, где учитель может посмотреть статус студента.

– при вводе данных преподавателя, открывается экран Teacher Activity на рисунке 15;

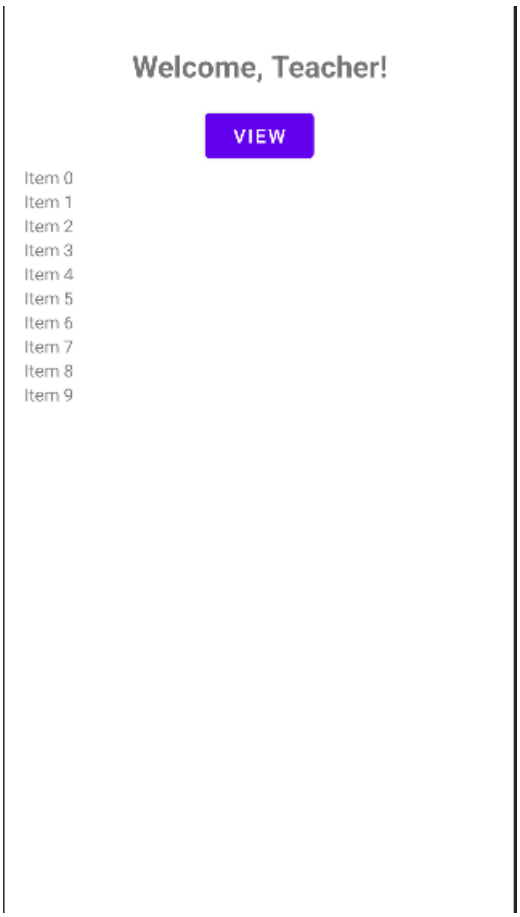

Рисунок 3.2.5 - Teacher Activity

В данном экране имеется кнопка «Просмотр», для отображения списка студентов, которые присутствует на занятии. Где записана элементы “item”, вместо него появляется список студентов. На этом экране отображается таблица в котором имеется имя студента и статус.

Также Админ может открывать полный список пользователей в базе данных и может изменять тип пользователя, на рисунке 16;

	username	password	role
1	admin	admin	ADMIN
2	aibek	1234	TEACHER
3	Bektashov	NULL	STUDENT

Рисунок 3.2.6 – таблица база данных

ЗАКЛЮЧЕНИЕ

Сегодня, когда системы онлайн-управления внедряются во все сферы бизнеса с целью совершенствования методов управления, сектор образования остается нетронутым, то есть нет возможности развивать его организационную структуру. Причина этого в том, что в странах СНГ структура введения контроля за учащимися является традиционной и не претерпела значительных изменений с советских времен. В результате возникли следующие проблемы

– Административная работа трудоемка и занимает много времени;

– частые ошибки при заполнении журналов посещаемости

– отсутствие безопасности, вызванное фальсификацией данных о посещаемости.

Посещаемость — это действие или факт посещения школы или учебного заведения. Учет посещаемости также используется в учебных заведениях для отслеживания того, сколько человек присутствует на занятиях в данный день.

Разработанные ПС могут внедрять системы мониторинга в электронном виде, а не традиционным способом, т.е. записывая их на бумаге и отражая в сервисе; ПС позволяет пользователям экономить время при выполнении своих обязанностей, в данном случае преподавания студентам и административных задач.

Уникальной особенностью данного проекта является использование биометрических данных для обеспечения расширенного управления посещаемостью. Затраты на этот проект окупились благодаря низкой цене устройства и тому факту, что одно устройство с 3-сторонним хранением (запись, чтение и удаление) может использоваться в течение длительного периода времени.

В будущем этот ПС может быть модернизирован для еще более эффективной работы. Добавление Ethernet или беспроводной связи к сканеру отпечатков пальцев улучшило бы аппаратное обеспечение, позволив ему передавать данные, используя только источник питания.

СПИСОК СОКРАЩЕНИИ

ЯП – Язык программирования

IDE – Интегрированная среда разработки

ПС – Программное средство

ТЗ – Техническое задание

БД — База данных

ID - Идентификатор, уникальный признак объекта

MAC - от англ. Media Access Control — управление доступом к среде

IP-адрес - Internet Protocol Address «адрес Интернет-протокола»

TCP / IP - от анг. Transmission Control Protocol /Internet Protocol - протокол управления передачей

ПИН - Персональный идентификационный номер

IVR — от анг. Interactive Voice Response - интерактивное голосовое меню

RFID — от анг. Radio Frequency Identification - радиочастотная идентификация

ДНК - Дезоксирибонуклеиновая кислота

IT — от анг. Information Technology — Информационные Технолоигии

МК — микроконтроллер

ТТЛ - Транзисторно-транзисторная логика

AFS - Adafruit Fingerprint Sensor

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 http://hubpages.com/technology/What-Is-The-Role-And-Importance-Of-Attendance-Monitoring-System, (дата обращения: 12.02.2023)

2 https://www.ibm.com/support/knowledgecenter/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm , (дата обращения 12.10.2019)

3 Time and Attendance Software Market by Type (Time Cards; Proximity Cards, Badges, and Key Fobs; Biometric; Web-based Login Stations; and Interactive Voice Response (IVR)) and Organization Structure (Small, Medium, and Large) - Global Opportunity Analysis and Industry Forecast, 2020-2027. [Electronic resource]. - Mode of access: https://www.alliedmarketresearch.com/time-and-attendance-software-market — Caps. from the screen.

4 http://www.hiral.com/attendance-management-system.aspx, (дата обращения: 15.02.2023)

5 https://www.schoology.com/, (дата обращения 17.02.2023)

6 https://www.classdojo.com/, (дата обращения 17.02.2023)

7 https://www.goguardian.com/teacher/, (дата обращения 17.02.2023)

8 http://www.biometricsystem.in/Attendance-Recorder.html, (дата обращения: 17.02.2023)

9 https://www.litmos.com/, (дата обращения 17.02.2023)

10 Dawes A.T. (2004),” Is RFID Right for Your Library”, Journal of Access Services, Volume 2(4), pp 7-13.

11 R. Patel, N. Patel and M. Gujar, “Online Students ‘Attendance Monitoring System in Classroom Using Radio Frequency Identification Technology: A Proposed System Framework”, International Journal of Emerging Technology and Advanced Engineering, vol. 2, Issue 2, - 2012 - February, pp. 61-66.

12 H. C. Lee and R. E. Gansler (eds.), “Advances in Fingerprint Technology”, Second Edition, CRC Press, New York, (2001)

13 T. Nawaz, S. Pervaiz, A. Koranic and Ashar-ud-din, “Development of Academic Attendance Monitoring System Using Fingerprint Identification” International Journal of Computer Science and Network Security, vol. 9, no. 5, (2009) May.

14 J. Baig, P. Bharne and T. Chauhan, “Automated Attendance Monitoring System Using Face Recognition”, International Journal for Research in

Emerging Science and Technology, vol. 2, Special Issue 1, (2015) March, pp. 108-112.

15 O. O. V. Villegas, H. d. O. Domínguez, V. G. C. Sánchez, L. O. Maynez and H. M. Orozco, “Biometric Human Identification of Hand Geometry Features Using Discrete Wavelet Transform”, Discrete Wavelet Transforms-Biomedical Applications, www.intechopen.com, (2011), pp. 251-266

16 https://developer.android.com/studio, (дата обращение 20.02.2023)

17 https://www.mantratec.com/Solutions/Biometrics-Attendance-System, (дата обращения 18.02.2023)

18 https://www.arduino.cc/, Arduino official web site (дата обращения 02.03.2023)

19 https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library, official library (дата обращения 02.03.2023)

20 https://ampermarket.kz/, (дата обращения 02.03.2023)

ПРИЛОЖЕНИЕ А

Техническая характеристика модуля отпечатка пальцев FPM10A DY50

Напряжение питания	DC 3.6 ~ 6.0 В / 3.3 В
Ток питания	120 мА
Пиковый ток	140 мА
Время обработки изображения отпечатка	<1 сек
Размер окна	14 мм x 18 мм
Режим соответствия	1 : 1
Режим поиска	(1 : N)
Файл ПО	256 байт
Емкость	300
Количество уровней безопасности	5
Ложный коэффициент отклонений (FRR)	<1.0% (при уровне безопасности 3)
Время поиска	<1.0 сек (1: 500, среднее)
Интерфейс ПК	UART (TTL Logic Level) или usb2.0 / USB1.1
Скорость передачи (UART)	(9600 × N) BPS где N = 1 ~ 12 (значение по умолчанию N = 6, 57600bps)
Рабочая температура	-20 °C…+50 °C

ПРИЛОЖЕНИЕ Б

а) Исходный код для подключения Arduino Uno FPM10A, сохранение отпечатка пальца и отправление на Android устройства

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
// Установка пинов для SoftwareSerial
const uint8_t RX_PIN = 2;
const uint8_t TX_PIN = 3;
// Создание объекта SoftwareSerial
SoftwareSerial mySerial (RX_PIN, TX_PIN);

// Создание объекта сканера отпечатков пальцев
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup() {
  // Настройка сканера отпечатков пальцев
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) { delay(1); }
  }
}
void loop() {
  // Ожидание считывания отпечатка пальца
  uint8_t p = finger.getImage();
  if (p == FINGERPRINT_OK) {
    Serial.println("Image taken");
    // Обработка отпечатка пальца
    p = finger.image2Tz();
    if (p == FINGERPRINT_OK) {
      Serial.println("Image converted");
      // Считывание и отправка ID отпечатка пальца на Android-устройство через
USB-порт
      int id = finger.fingerID;
      Serial.print("ID: ");
      Serial.println(id);
      Serial.write(id);
    } else {
      Serial.println("Failed to convert image");
    }
  } else {
    Serial.println("Failed to take image");
  }
  delay(1000);
}
```

ПРИЛОЖЕНИЕ В

Описание таблиц: Структура база данных

-«users» - учетные данные:

```
companion object{
    private const val DATABASE_NAME = "user.db"
    private const val DATABASE_VERSION = 1

    private const val TABLE_NAME = "users"
    private const val COLUMN_USERNAME = "username"
    private const val COLUMN_PASSWORD = "password"
    private const val COLUMN_ROLE = "role"

    private const val CREATE_TABLE_QUERY =
        "CREATE TABLE $TABLE_NAME ($COLUMN_USERNAME TEXT PRIMARY KEY, " +
                "$COLUMN_PASSWORD TEXT, $COLUMN_ROLE TEXT)"
}
```

-«attendance» - показ список студентов:

```
companion object {
    private const val DATABASE_VERSION = 1
    private const val DATABASE_NAME = "attendance.db"
    // Table Names
    private const val TABLE_ATTENDANCE = "attendance"
    // Common column names
    private const val KEY_ID = "id"
    // ATTENDANCE Table - column names
    private const val KEY_STUDENT_NAME = "student_name"
    private const val KEY_DATE = "date"
    private const val KEY_STATUS = "status"
    private const val COLUMN_IS_PRESENT = "isPresnt"

    // Table Create Statements
    private const val CREATE_TABLE_ATTENDANCE = ("CREATE TABLE "
            + TABLE_ATTENDANCE + "(" + KEY_ID + " INTEGER PRIMARY KEY," +
            KEY_STUDENT_NAME
            + " TEXT," + KEY_DATE + " TEXT," +
            KEY_STATUS + " INTEGER," + COLUMN_IS_PRESENT + "INTEGER")
}
```