Государственное бюджетное общеобразовательное

учреждение города Москвы

«Школа № 627 имени генерала Д.Д. Лелюшенко» г. Москвы

**Проектная работа**

**«Аутентификация с помощью биометрического классификатора данных лица для доступа к шкафчикам»**

**Выполнили**:

Ученик 10Б класса Школы № 627 имени

генерала Д.Д. Лелюшенко

**Похлестов Андрей Дмитриевич**

Ученик 10Б класса Школы № 627 имени генерала Д.Д. Лелюшенко

**Зуев Михаил Константинович**

**Руководители проекта:**

Учитель технологии ГБОУ Школы №627 имени генерала Д.Д. Лелюшенко

**Ломоносов Антон Владимирович**

Москва, 2024 год

Оглавление

[**Введение** 5](#_Toc184152376)

[**Глава 1. Сравнительный анализ других биометрических технологий** 6](#_Toc184152377)

[**1.1. Дактилоскопия** 6](#_Toc184152378)

[1.1.1. Принципы работы 6](#_Toc184152379)

[1.1.2. Преимущества 6](#_Toc184152380)

[1.1.3. Недостатки 6](#_Toc184152381)

[**1.2. Идентификация по радужной оболочке глаза** 7](#_Toc184152382)

[1.2.1. Принципы работы 7](#_Toc184152383)

[1.2.2. Преимущества 7](#_Toc184152384)

[1.2.3. Недостатки 7](#_Toc184152385)

[**1.3. Голосовая биометрия** 7](#_Toc184152386)

[1.3.1. Принципы работы 7](#_Toc184152387)

[1.3.2. Преимущества 7](#_Toc184152388)

[1.3.3. Недостатки 7](#_Toc184152389)

[**1.4. Распознавание лиц** 8](#_Toc184152390)

[1.4.1. Преимущества 8](#_Toc184152391)

[1.4.2. Недостатки 8](#_Toc184152392)

[**1.5. Вывод** 8](#_Toc184152393)

[**Глава 2. Теоретические основы распознавания лиц** 8](#_Toc184152394)

[**2.1. Основы распознавания лиц** 8](#_Toc184152395)

[**2.2. Применение в системах безопасности** 9](#_Toc184152396)

[**2.3. OpenCV и его возможности** 10](#_Toc184152397)

[**Глава 3. Описание системы и её компонентов** 11](#_Toc184152398)

[**3.1. Общая структура системы** 11](#_Toc184152399)

[**3.2. Аппаратные компоненты** 12](#_Toc184152400)

[3.2.1. Платформа OrangePI 12](#_Toc184152401)

[3.2.2. Камера 13](#_Toc184152402)

[3.2.3. Механизм управления дверью 13](#_Toc184152403)

[3.2.4. Источник питания 14](#_Toc184152404)

[**3.3. Программные компоненты** 14](#_Toc184152405)

[3.3.1. OpenCV для обработки изображений 14](#_Toc184152406)

[3.3.2. Алгоритмы распознавания лиц 15](#_Toc184152407)

[3.3.3. Интерфейс управления 15](#_Toc184152408)

[**3.4. База данных лиц** 16](#_Toc184152409)

[**3.5. Протоколы безопасности** 16](#_Toc184152410)

[**Глава 4. Алгоритмы распознавания лиц** 16](#_Toc184152411)

[**4.1 Принципы работы алгоритмов распознавания лиц** 16](#_Toc184152412)

[**4.2. Алгоритм Haar-cascade** 17](#_Toc184152413)

[4.2.1. Принципы работы алгоритма 18](#_Toc184152414)

[4.2.2. Применение в проекте 18](#_Toc184152415)

[**4.3. Алгоритм LBPH (Local Binary Patterns Histograms)** 18](#_Toc184152416)

[4.3.1. Принципы работы алгоритма 19](#_Toc184152417)

[4.3.2. Применение в проекте 19](#_Toc184152418)

[**4.4. Методы глубокого обучения** 20](#_Toc184152419)

[4.4.1. Принципы работы сверточных нейронных сетей 20](#_Toc184152420)

[4.4.2. Применение в проекте 20](#_Toc184152421)

[**4.5. Оценка точности алгоритмов** 21](#_Toc184152422)

[**Глава 5. Экономическая рентабельность** 21](#_Toc184152423)

[**5.1. Структура затрат** 21](#_Toc184152424)

[5.1.1. Капитальные затраты (CAPEX) 21](#_Toc184152425)

[5.1.2. Операционные затраты (OPEX): 22](#_Toc184152426)

[5.1.3. Итоговая стоимость проекта 22](#_Toc184152427)

[**5.2. Экономическая выгода** 23](#_Toc184152428)

[5.2.1. Сокращение текущих издержек 23](#_Toc184152429)

[5.2.2. Повышение безопасности 23](#_Toc184152430)

[5.2.3. Удобство для пользователей 23](#_Toc184152431)

[**5.3. Анализ рентабельности** 23](#_Toc184152432)

[5.3.1. Срок окупаемости (Payback Period) 23](#_Toc184152433)

[5.3.2. Чистая приведённая стоимость (NPV) 24](#_Toc184152434)

[5.3.3. Внутренняя норма доходности (IRR) 24](#_Toc184152435)

[**5.4. Потенциальные риски и их минимизация** 24](#_Toc184152436)

[5.4.1. Риски завышения капитальных затрат 24](#_Toc184152437)

[5.4.2. Технические сбои 24](#_Toc184152438)

[5.4.3. Низкая пользовательская вовлечённость 24](#_Toc184152439)

[**Глава 6. Этические и юридические аспекты биометрии** 25](#_Toc184152440)

[**6.1. Юридические аспекты использования биометрии** 25](#_Toc184152441)

[6.1.1. Биометрические данные как объект правового регулирования 25](#_Toc184152442)

[6.1.2. Обработка биометрических данных в образовательных учреждениях 26](#_Toc184152443)

[**6.2. Аргументы в пользу исключения проекта из сферы действия законодательства** 26](#_Toc184152444)

[6.2.1. Принцип локальной обработки данных 26](#_Toc184152445)

[6.2.2. Отсутствие персонификации данных 26](#_Toc184152446)

[6.2.3. Неприменимость норм о Единой биометрической системе (ЕБС) 27](#_Toc184152447)

[6.2.4. Соблюдение принципа добровольного согласия 27](#_Toc184152448)

[6.2.5. Система контроля доступа как образовательный инструмент 27](#_Toc184152449)

[**6.3. Этика и защита прав пользователей** 27](#_Toc184152450)

[6.3.1. Минимизация сбора данных 27](#_Toc184152451)

[6.3.2. Шифрование и защита базы данных 27](#_Toc184152452)

[6.3.3. Прозрачность работы системы 27](#_Toc184152453)

[6.3.4. Срок хранения данных 28](#_Toc184152454)

## **Введение**

В условиях повышенных требований к безопасности и автоматизации образовательных учреждений использование биометрических технологий представляет особый интерес. В современном мире технологии распознавания лиц находят широкое применение в области контроля доступа и идентификации личности.

Применение биометрических методов идентификации для обеспечения автоматического доступа к личным шкафчикам учащихся в школе является инновационным решением, которое позволяет обеспечить безопасность, исключить использование ключей и карт доступа, а также значительно повысить удобство пользователей.

Данный проект направлен на разработку системы доступа к шкафчику, использующей алгоритмы компьютерного зрения для идентификации лиц учащихся. Реализация выполняется на базе одноплатного компьютера Orange Pi и библиотеки компьютерного зрения OpenCV.

Цель работы: Разработка и тестирование системы автоматического доступа к школьному шкафчику, функционирующей на основе технологии распознавания лиц, для повышения уровня безопасности и удобства в учебном заведении.

Задачи исследования:

* Исследовать текущие алгоритмы и методы распознавания
* Исследовать теоретические основы распознавания лиц
* Разработать систему и создать макет
* Оценить экономическую рентабельность и эффективность продукта

# **Глава 1. Сравнительный анализ других биометрических технологий**

Биометрические системы идентификации включают широкий спектр технологий, каждая из которых основывается на уникальных физиологических или поведенческих характеристиках человека. В данном разделе проводится сравнительный анализ технологии распознавания лиц с альтернативными биометрическими методами, такими как дактилоскопия (анализ отпечатков пальцев), идентификация по радужной оболочке глаза и голосовая биометрия.

## **1.1. Дактилоскопия**

### 1.1.1. Принципы работы

Метод основан на уникальности кожных рисунков пальцев, которые преобразуются в цифровой шаблон для последующего сравнения.

### 1.1.2. Преимущества

* Высокая точность при низких затратах на оборудование.
* Устойчивость к большинству внешних факторов, включая освещение и угол касания.
* Компактность устройств, позволяющая их интеграцию в малогабаритные системы.

### 1.1.3. Недостатки

* Снижение точности при повреждении кожи (царапины, ожоги).
* Контактный характер системы, что приводит к повышенным санитарным рискам.
* Зависимость от чистоты сенсоров, что делает систему менее надёжной в условиях высокой проходимости.

## **1.2. Идентификация по радужной оболочке глаза**

### 1.2.1. Принципы работы

Распознавание осуществляется путём анализа уникального узора радужной оболочки, который остаётся неизменным на протяжении всей жизни.

### 1.2.2. Преимущества

* Исключительная точность идентификации, превышающая показатели большинства альтернативных методов.
* Минимальное влияние внешних факторов, включая освещённость и возраст пользователя.

### 1.2.3. Недостатки

* Высокая стоимость аппаратуры, требующей инфракрасных сенсоров высокого разрешения.
* Необходимость точного позиционирования пользователя перед камерой.

## **1.3. Голосовая биометрия**

### 1.3.1. Принципы работы

Метод включает анализ акустических характеристик речи, таких как частота, тембр и тональность, с последующим созданием цифрового голосового шаблона.

### 1.3.2. Преимущества

* Удобство использования в условиях отсутствия визуального контакта (например, в телефонных системах).
* Возможность удалённой идентификации без специализированного оборудования.

### 1.3.3. Недостатки

* Высокая чувствительность к изменениям голоса из-за болезней или окружающего шума.
* Уязвимость к атакам путём воспроизведения записанных голосов.

## **1.4. Распознавание лиц**

### 1.4.1. Преимущества

* Бесконтактность, исключающая санитарные риски и повышающая удобство.
* Возможность интеграции в системы видеонаблюдения для обеспечения непрерывного мониторинга.
* Высокая скорость обработки изображений в реальном времени.

### 1.4.2. Недостатки

* Чувствительность к освещённости и углу съёмки.

## **1.5. Вывод**

На основании проведённого анализа распознавание лиц представляет собой сбалансированное решение для применения в системах школьных шкафчиков. Метод сочетает достаточную точность с удобством бесконтактного использования, что особенно актуально в образовательных учреждениях.

# **Глава 2. Теоретические основы распознавания лиц**

## **2.1. Основы распознавания лиц**

Распознавание лиц — это биометрическая технология, использующая уникальные характеристики человеческого лица для идентификации или верификации личности. Основным преимуществом данного метода является его бесконтактность, что делает его удобным и эффективным для применения в различных сферах, включая системы безопасности. Основой распознавания лиц является извлечение специфических признаков, таких как расстояния между ключевыми точками лица, форма контуров, линии глаз и рта, а также структура кожи. Эти параметры образуют так называемый "лицевой шаблон", который затем используется для сравнения с базой данных для подтверждения или отказа в доступе.

В рамках данного проекта распознавание лиц будет использоваться для автоматической идентификации пользователей при доступе к шкафчику, что позволит исключить необходимость использования физических ключей или карт. Наиболее распространённым методом распознавания лиц является использование алгоритмов классификации, которые работают по принципу сопоставления извлечённых признаков с заранее подготовленными моделями, полученными на основе тренировочных данных. Алгоритм распознавания лиц может быть разделён на несколько этапов: предварительная обработка изображения, извлечение признаков, сопоставление с базой данных и принятие решения о верификации или идентификации.

Наиболее популярные алгоритмы включают Haar-cascade классификаторы, метод LBPH (Local Binary Patterns Histograms), а также методы, основанные на глубоком обучении. Алгоритм Haar-cascade, например, использует каскад классификаторов, которые способны распознавать объекты (в данном случае лица) в реальном времени с минимальными затратами вычислительных ресурсов. LBPH применяет текстурные признаки для анализа изображений, что позволяет повысить точность распознавания, даже если лицо человека частично закрыто или изображение деформировано. Методы на основе глубоких нейронных сетей (например, использование сверточных нейронных сетей, CNN) способны достигать высокой точности распознавания, но требуют значительных вычислительных мощностей и большого объёма данных для обучения.

## **2.2. Применение в системах безопасности**

Технологии распознавания лиц нашли широкое применение в различных системах безопасности, начиная от установок в аэропортах и банках, и заканчивая более мелкими приложениями, такими как системы контроля доступа в здания и помещения. Преимущества таких технологий заключаются в их способности эффективно и точно идентифицировать личности, при этом исключая необходимость в физическом взаимодействии с устройствами (например, использование карт или паролей).

Особое внимание в последнее время уделяется внедрению биометрических систем в образовательных учреждениях, где распознавание лиц может существенно повысить безопасность, упрощая процессы контроля доступа и мониторинга. Например, такие системы могут быть использованы для автоматического открытия шкафчиков, доступ к которым будет предоставляться только тем пользователям, чьи лица зарегистрированы в системе. Это позволяет избежать потери ключей и идентификационных карт, а также предотвращает несанкционированный доступ. Кроме того, интеграция распознавания лиц с другими системами, например, с учётными системами для отслеживания посещаемости или контроля за выходом из учебных заведений, также является важным аспектом в повышении общей безопасности.

## **2.3. OpenCV и его возможности**

Одним из главных преимуществ систем распознавания лиц является их высокая скорость работы в реальном времени. Алгоритмы, основанные на OpenCV, позволяют достигать быстрого отклика при обработке изображений, что критически важно в таких задачах, как контроль доступа и мониторинг в местах с высоким потоком людей.

OpenCV (Open Source Computer Vision Library) — это мощная библиотека с открытым исходным кодом, предназначенная для разработки приложений, использующих методы компьютерного зрения, обработки изображений и машинного обучения. Среди множества функций и инструментов, предоставляемых OpenCV, наиболее важными для разработки системы распознавания лиц являются:

Алгоритмы для детекции лиц: Одним из наиболее эффективных методов является использование Haar-cascade классификаторов, которые обучаются на большом количестве примеров лиц. Этот метод позволяет быстро и с высокой точностью находить лица в изображении, даже если они частично скрыты или находятся под углом.

Методы для распознавания лиц: Использование алгоритмов, таких как LBPH (Local Binary Patterns Histograms), позволяет не только обнаружить лицо, но и провести его идентификацию, сравнив извлечённые признаки с базой данных. LBPH особенно эффективен в условиях изменяющегося освещения или низкого качества изображения.

Возможности работы с видео: OpenCV предоставляет мощные инструменты для обработки видеопотока, что является критически важным для реализации системы распознавания лиц в реальном времени. Библиотека поддерживает работу с различными камерами и видеопотоками, что позволяет легко интегрировать её в систему контроля доступа.

Интеграция с аппаратными платформами: OpenCV активно используется в проектах, основанных на различных одноплатных компьютерах, таких как Raspberry Pi и OrangePI. Эти платформы, благодаря своей компактности и мощности, идеально подходят для проектов, где требуется реальное распознавание лиц с использованием камер высокого разрешения.

Алгоритмы OpenCV позволяют значительно ускорить процесс разработки систем на основе распознавания лиц, снижая потребность в написании собственных сложных алгоритмов обработки изображений. Библиотека также предоставляет удобные средства для оптимизации и ускорения вычислений, что важно при работе с устройствами с ограниченными вычислительными ресурсами, как в случае с OrangePI.

# **Глава 3. Описание системы и её компонентов**

## **3.1. Общая структура системы**

Система автоматического контроля доступа на основе распознавания лиц включает несколько ключевых компонентов, каждый из которых играет свою роль в процессе обработки данных и принятия решений о доступе. Главные элементы системы: аппаратная платформа, программное обеспечение, компоненты для захвата изображений, база данных лиц и интерфейс для управления доступом. Система должна обеспечивать быструю обработку изображений, точное распознавание лиц, а также надёжность и безопасность на всех этапах работы.

*Основные задачи системы заключаются в том, чтобы:*

* Обнаружить лицо пользователя с помощью камеры.
* Сравнить извлечённые признаки лица с записями в базе данных.
* Принять решение о предоставлении доступа в реальном времени.

Для решения этих задач используется интеграция аппаратных и программных компонентов. В качестве платформы для реализации системы используется OrangePI, которая является альтернативой Raspberry Pi и обеспечивает достаточную вычислительную мощность для обработки изображений в реальном времени при низкой стоимости.

## **3.2. Аппаратные компоненты**

### 3.2.1. Платформа OrangePI

OrangePI — это одноплатный компьютер, который обладает множеством характеристик, подходящих для реализации проектов, связанных с распознаванием лиц. В отличие от стандартных ПК или серверов, OrangePI представляет собой компактное решение с хорошими вычислительными способностями и энергоэффективностью. Он оснащён процессором Allwinner H3 с четырьмя ядрами ARM Cortex-A7, что позволяет эффективно работать с различными задачами компьютерного зрения и машинного обучения. Модели OrangePI поддерживают различное количество оперативной памяти (от 512 МБ до 2 ГБ), что даёт возможность выбрать подходящую версию в зависимости от требований к системе.

Платформа имеет несколько портов для подключения внешних устройств, включая USB-порты для камер, а также GPIO (General Purpose Input/Output) для подключения других компонентов, например, механизмов открывания дверей. OrangePI поддерживает несколько операционных систем, включая Linux и Android, что позволяет гибко настроить систему под нужды проекта.

### 3.2.2. Камера

Для захвата изображений и проведения распознавания лиц используется камера с высоким разрешением. USB-камеры с разрешением 1080p или выше являются оптимальным выбором для проекта, поскольку они обеспечивают достаточное качество изображения для точного распознавания лиц. Камера должна быть подключена к OrangePI через USB-порт, и её размещение вблизи дверей шкафчика будет критически важным для корректной работы системы.

Для повышения точности распознавания лиц рекомендуется использовать камеры с функциями автофокуса, которые могут адаптироваться к изменениям в положении лица, а также камеры, способные работать при различных уровнях освещенности.

### 3.2.3. Механизм управления дверью

Для автоматического открытия дверцы шкафчика используется приводной механизм, управляемый через платформу OrangePI. Наиболее часто в таких системах применяются электромагнитные замки или серводвигатели, которые подключаются к GPIO-портам. Электромагнитный замок с блокировкой может быть активирован программным обеспечением системы, что позволяет открыть шкафчик только при успешной верификации лица. Для точного управления замком используется система команд, которая учитывает данные о успешной или неуспешной идентификации пользователя.

### 3.2.4. Источник питания

Для бесперебойной работы всей системы необходимо обеспечение стабильного источника питания. В качестве источников питания могут использоваться адаптеры переменного тока с выходным напряжением 5 В (для OrangePI) и соответствующие источники для подключения камеры и других устройств. Важно предусмотреть наличие резервного питания или системы с батарейным питанием для обеспечения работы в случае отключения основного источника.

## **3.3. Программные компоненты**

Программное обеспечение, используемое для распознавания лиц, включает два основных блока: обработку изображений и алгоритмы распознавания лиц, а также интерфейс для взаимодействия с аппаратной частью системы.

### 3.3.1. OpenCV для обработки изображений

В качестве основного инструмента для обработки изображений используется библиотека OpenCV, которая предоставляет набор готовых функций для захвата изображений с камеры, обработки и анализа этих изображений, а также для распознавания лиц. OpenCV включает следующие ключевые возможности для проекта:

Детекция лиц: с помощью алгоритмов, таких как Haar-cascade классификаторы или LBPH, можно обнаружить лицо в кадре и провести его идентификацию. Эти алгоритмы эффективно работают даже при наличии шума, освещении или изменении угла наклона головы.

Программирование алгоритмов распознавания: OpenCV предоставляет средства для реализации алгоритмов, таких как SVM (Support Vector Machine) или KNN (K-Nearest Neighbors) для сравнения лиц и принятия решения о верификации.

Предобработка изображений: перед выполнением распознавания лицо должно быть подготовлено с помощью таких операций, как преобразование в оттенки серого, выравнивание освещенности, уменьшение шума. Это позволяет улучшить точность и скорость обработки.

### 3.3.2. Алгоритмы распознавания лиц

Для распознавания лиц на основе извлечённых признаков используется алгоритм LBPH (Local Binary Patterns Histograms). Этот метод является эффективным для работы с изображениями, где могут быть изменения в освещении или наклоне головы. Алгоритм работает, преобразуя изображение лица в локальные бинарные паттерны, что позволяет значительно уменьшить чувствительность к изменениям в фоновом освещении или позе.

Также возможно использование методов глубокого обучения, если для обучения имеются большие базы данных изображений. В случае такого подхода может быть применён TensorFlow или Keras, что позволит повысить точность системы, однако это потребует большего объёма вычислительных ресурсов.

### 3.3.3. Интерфейс управления

Интерфейс управления системой должен быть простым и удобным для использования. Это может быть как веб-интерфейс для администрирования базы данных лиц, так и локальная консоль для настройки системы. Для взаимодействия с пользователем система должна выводить сообщения о статусе распознавания, например, "Доступ разрешён" или "Лицо не распознано", и в зависимости от этого активировать механизмы открытия или блокировки дверцы шкафчика.

## **3.4. База данных лиц**

База данных лиц хранит уникальные изображения пользователей, которые были зарегистрированы в системе. Каждое изображение должно быть заранее обработано и преобразовано в шаблоны признаков, которые затем используются для сравнения при каждом новом обращении. База данных может быть реализована как локальная система хранения на платформе OrangePI или как удалённая база данных, если система требует масштабируемости.

## **3.5. Протоколы безопасности**

В процессе работы системы важно учитывать аспекты безопасности. Данные о лицах пользователей должны быть защищены от несанкционированного доступа. Для этого можно использовать методы шифрования, такие как AES для хранения данных в базе данных, а также обеспечить защищённые каналы связи при передаче данных, если система работает в сети.

Система должна поддерживать надёжную аутентификацию и защиту от подмены данных, что обеспечивается через шифрование изображений и использование защищённых алгоритмов распознавания.

# **Глава 4. Алгоритмы распознавания лиц**

## **4.1 Принципы работы алгоритмов распознавания лиц**

Распознавание лиц в рамках рассматриваемого проекта основывается на использовании компьютерного зрения и обработки изображений для идентификации лица пользователя. Задача распознавания лиц делится на несколько этапов: от захвата изображения и его предобработки до принятия решения о предоставлении или отказе в доступе. Важнейшей частью системы является выбор и использование алгоритма распознавания, который будет обеспечивать максимальную точность, а также работоспособность в реальном времени при ограниченных вычислительных ресурсах.

*Алгоритмы распознавания лиц функционируют в несколько этапов:*

* *Детекция лица*: на этом этапе система должна выявить лицо на изображении или видеопотоке. Для этого используются различные методы, которые позволяют точно обнаруживать лица, независимо от угла наклона, освещенности или частичной блокировки.
* *Извлечение признаков*: после того как лицо обнаружено, производится извлечение характеристик, которые могут быть использованы для его идентификации. Эти признаки могут включать расстояние между глазами, форму подбородка, контуры лица, текстуры кожи и другие уникальные особенности.
* *Сравнение признаков с базой данных*: на этом этапе система сравнивает извлечённые признаки с заранее зарегистрированными лицами в базе данных, используя различные методы сравнения и классификации.

Принятие решения: на основе полученных результатов сравнений принимается решение о том, предоставить ли доступ пользователю или отказать.

В рамках этого проекта особое внимание уделяется выбору эффективных алгоритмов для выполнения каждой из этих задач. Ниже рассматриваются основные методы, используемые для распознавания лиц.

## **4.2. Алгоритм Haar-cascade**

Один из наиболее известных и широко используемых алгоритмов для распознавания лиц в реальном времени — это алгоритм Haar-cascade, который был разработан Пауло Виолы и Михалом Джонсом в 2001 году. Этот метод основан на использовании каскада простых классификаторов для определения наличия объектов на изображении, в частности, лиц.

### 4.2.1. Принципы работы алгоритма

Алгоритм Haar-cascade использует набор Хаара-признаков, которые представляют собой различие интенсивности пикселей в определённых областях изображения. Эти признаки моделируют определённые текстуры, такие как границы между носом и глазами, которые легко идентифицируются на изображениях лиц. Каскад классификаторов обучается на большом наборе положительных и отрицательных примеров, чтобы эффективно классифицировать части изображения как лицо или не лицо.

Характерной особенностью данного метода является его способность работать в реальном времени, благодаря быстрой вычислительной реализации. Haar-cascade классификаторы могут быть использованы как для распознавания лиц, так и для обнаружения других объектов, таких как глаза или автомобили.

### 4.2.2. Применение в проекте

В рамках системы автоматического контроля доступа Haar-cascade будет использоваться для детекции лиц на видеопотоке, поступающем с камеры. После того как лицо будет обнаружено, система будет переходить к следующему этапу — извлечению признаков лица и сравнению их с базой данных зарегистрированных пользователей.

Этот алгоритм выбран, потому что он достаточно эффективен для использования в реальном времени, с минимальной нагрузкой на вычислительные ресурсы, что критично для работы на платформе OrangePI.

## **4.3. Алгоритм LBPH (Local Binary Patterns Histograms)**

Алгоритм LBPH (Local Binary Patterns Histograms) используется для распознавания лиц и является альтернативой методу Haar-cascade, обеспечивая более высокую точность в условиях плохой освещенности и изменяющихся углов взгляда. Этот метод работает путём преобразования изображения в набор текстурных признаков, которые затем используются для сравнения лиц.

### 4.3.1. Принципы работы алгоритма

*LBPH представляет собой комбинацию двух методов:*

* Локальные бинарные паттерны (LBP) — это текстурные признаки, которые описывают локальные различия в интенсивности пикселей, сравнивая каждый пиксель с его соседями. Полученная бинарная матрица преобразуется в десятичное число, которое затем используется для дальнейшей обработки.
* Гистограммы — после того как локальные бинарные паттерны были вычислены, они группируются в гистограмму, которая представляется как вектор признаков для каждого лица.

*Процесс включает несколько этапов:*

* Преобразование изображения в оттенки серого.
* Вычисление LBP для каждого региона изображения.
* Построение гистограммы для каждого лица.
* Сравнение гистограмм для определения сходства.

### 4.3.2. Применение в проекте

Алгоритм LBPH будет использоваться для распознавания лиц после их детекции. После извлечения лиц с помощью Haar-cascade система будет применять LBPH для получения текстурных признаков каждого лица, которые затем будут сравниваться с лицами в базе данных. Этот алгоритм выбран за счёт своей высокой устойчивости к изменениям освещенности и углов наклона головы.

Также LBPH используется для работы в условиях, где изображения могут быть размытыми или шумными, что улучшает общую точность системы в условиях реальной эксплуатации.

## **4.4. Методы глубокого обучения**

Системы распознавания лиц могут быть улучшены с использованием методов глубокого обучения. Одним из самых распространённых подходов является использование сверточных нейронных сетей (CNN), которые позволяют значительно повысить точность распознавания.

### 4.4.1. Принципы работы сверточных нейронных сетей

Сверточные нейронные сети — это класс нейронных сетей, специально разработанных для обработки данных в виде изображений. Они применяют несколько слоёв свертки и подвыборки, что позволяет выявлять более сложные закономерности и особенности изображения, чем традиционные методы, такие как LBPH. В случае с распознаванием лиц, CNN могут быть обучены на большом наборе изображений, чтобы выявлять и классифицировать лица с высокой точностью.

*Процесс обучения свёрточной нейронной сети включает следующие этапы:*

* Обучение сети на большом объёме данных, используя методы оптимизации для минимизации ошибки распознавания.
* Применение обученной сети для классификации новых изображений лиц.

### 4.4.2. Применение в проекте

Для этого проекта использование CNN в качестве дополнительного метода распознавания лиц может быть полезным в случаях, когда точность распознавания должна быть максимальной. Однако стоит учитывать, что использование глубокого обучения требует значительных вычислительных ресурсов, поэтому этот метод может быть менее применим для платформ с ограниченными возможностями, таких как OrangePI. Тем не менее, методы глубокого обучения могут быть полезны для улучшения точности системы, если она будет расширяться и запускаться на более мощных вычислительных устройствах.

## **4.5. Оценка точности алгоритмов**

Для оценки точности распознавания лиц применяются различные метрики, такие как достоверность, чувствительность и специфичность. Также важно учитывать скорость распознавания, особенно в реальных условиях, когда система должна работать в реальном времени.

* Достоверность измеряет процент правильных идентификаций среди всех попыток.
* Чувствительность отражает способность системы обнаруживать лица среди всех лиц, которые должны быть распознаны.
* Специфичность показывает способность системы избегать ложных срабатываний, то есть, когда лицо не должно быть распознано, но система ошибочно его идентифицирует.

# **Глава 5. Экономическая рентабельность**

Экономическая эффективность внедрения биометрической системы доступа к школьным шкафчикам оценивается через анализ затрат на разработку, внедрение и эксплуатацию системы, а также расчёт её влияния на уменьшение текущих издержек, повышение удобства и безопасности. Данная глава детализирует все аспекты экономической оценки, включая статические и динамические показатели рентабельности, потенциальные риски и способы их минимизации.

## **5.1. Структура затрат**

### 5.1.1. Капитальные затраты (CAPEX)

#### Аппаратные компоненты:

* Одноплатный компьютер (OrangePI): 2500–3000 рублей за единицу.
* Камера высокого разрешения (1080p): 3500–4500 рублей.
* Электромагнитный замок: 1500–2000 рублей.
* Источник питания: 1000 рублей.
* Прочие комплектующие (кабели, крепления): 500 рублей.
* Итого на один шкафчик: 9000–11000 рублей.

#### Программное обеспечение:

* Разработка пользовательского интерфейса и алгоритмов: 100 000 рублей.
* Тестирование и отладка: 20 000 рублей.

#### Инфраструктура:

* Серверное оборудование для хранения базы данных: 50 000 рублей (на 500 шкафчиков).
* Лицензирование программных компонентов: 15 000 рублей (если используется коммерческая версия).

### 5.1.2. Операционные затраты (OPEX):

#### Электроэнергия:

* Одноплатный компьютер: 5 Вт × 8 часов/день × 0,5 руб./кВт⋅ч = 7,5 руб./мес. на шкафчик.
* Камера: 3 Вт × 8 часов/день = 4,5 руб./мес.
* Средняя стоимость работы системы на один шкафчик: ~12 рублей/мес.

#### Обслуживание:

* Проверка оборудования, обновление ПО: 20 000 рублей/год для всей системы.
* Ремонтные работы (замена замков, камер): 2% от капитальных затрат/год.

### 5.1.3. Итоговая стоимость проекта

#### Для школы с 500 шкафчиками:

* Капитальные затраты: 100 шкафчиков × 10 000 руб. + серверное оборудование + ПО = 1 165 000 рублей.
* Операционные затраты: ~300 000 рублей/год.

## **5.2. Экономическая выгода**

### 5.2.1. Сокращение текущих издержек

#### Исключение расходов на изготовление и замену ключей:

* Один комплект ключей: 500 руб. × 500 шкафчиков × 2 комплекта/год = 500 000 руб./год.

#### Сокращение времени на выдачу ключей:

* Средняя зарплата сотрудника (кладовщика): 25 000 руб./мес.
* Высвобождение ~40% рабочего времени: экономия ~120 000 руб./год.

### 5.2.2. Повышение безопасности

#### Снижение затрат на урегулирование спорных ситуаций (утеря ключей, кражи):

* Прямые потери от взлома шкафчиков составляют 50 000–100 000 руб./год, что полностью устраняется при внедрении системы.

### 5.2.3. Удобство для пользователей

Увеличение скорости доступа к шкафчику: экономия времени учащихся и персонала.

Повышение удовлетворённости родителей благодаря внедрению современной технологии.

## **5.3. Анализ рентабельности**

Для оценки рентабельности проекта используются основные экономические показатели

### 5.3.1. Срок окупаемости (Payback Period)

* Общие вложения: 1 165 000 руб.
* Ежегодная экономия: ~620 000 руб.
* Срок окупаемости: 1 165 000 / 620 000 ≈ 1,9 года.

### 5.3.2. Чистая приведённая стоимость (NPV)

NPV = ∑ (CFₜ / (1 + r)ᵗ) − CAPEX,

*где:*

* CFₜ — годовой денежный поток (~620 000 руб.).
* r — ставка дисконтирования (10%).
* t — количество лет.

*При расчёте на 5 лет:*

NPV = (620 000 / 1,1¹) + (620 000 / 1,1²) + (620 000 / 1,1³) + (620 000 / 1,1⁴) + (620 000 / 1,1⁵) − 1 165 000 = ~1 256 000 руб.

### 5.3.3. Внутренняя норма доходности (IRR)

IRR ≈ 34%, что значительно превышает среднюю ставку доходности инвестиций.

## **5.4. Потенциальные риски и их минимизация**

### 5.4.1. Риски завышения капитальных затрат

#### Оптимизация выбора оборудования:

* Использование более дешёвых альтернатив при сохранении качества.
* Закупка компонентов оптом.

### 5.4.2. Технические сбои

* Регулярное обслуживание и мониторинг.
* Использование резервного источника питания.

### 5.4.3. Низкая пользовательская вовлечённость

* Организация обучения для школьного персонала и учащихся.
* Упрощение интерфейса системы.

Экономическая оценка показывает высокую рентабельность проекта, при которой срок окупаемости составляет менее двух лет, а показатели NPV и IRR подтверждают инвестиционную привлекательность. Система обеспечивает не только финансовую выгоду, но и значительное повышение уровня безопасности и удобства. Внедрение биометрической технологии является стратегически обоснованным шагом, способным повысить имидж образовательного учреждения и обеспечить долговременную экономию средств.

# **Глава 6. Этические и юридические аспекты биометрии**

Биометрические технологии, включая системы распознавания лиц, активно внедряются в различных сферах деятельности, вызывая вопросы, связанные с соблюдением прав на защиту персональных данных, обеспечением информационной безопасности и соответствием законодательным нормам. Настоящий проект, направленный на автоматизацию доступа к школьным шкафчикам, был спроектирован таким образом, чтобы минимизировать юридические риски и соответствовать основополагающим этическим принципам. В данной главе осуществляется детальный анализ применимого правового регулирования в Российской Федерации, а также обосновывается исключение проекта из сферы действия законодательства о биометрии.

## **6.1. Юридические аспекты использования биометрии**

### 6.1.1. Биометрические данные как объект правового регулирования

Согласно статье 11 Федерального закона №152-ФЗ "О персональных данных", биометрическими данными признаются сведения, характеризующие физиологические и биологические особенности человека, позволяющие установить его личность, и используемые оператором для идентификации субъекта данных. Примером таких данных являются изображения лица, отпечатки пальцев, параметры радужной оболочки глаза и голосовой отпечаток.

Правовой статус биометрических данных обусловлен их уникальностью и высокой степенью конфиденциальности, что требует строгого соблюдения оператором принципов обработки, таких как:

* Законность и справедливость обработки.
* Целевое назначение использования данных.
* Минимизация объёма обрабатываемой информации.

### 6.1.2. Обработка биометрических данных в образовательных учреждениях

В условиях образовательной среды использование биометрических данных чаще всего сопряжено с необходимостью их применения для контроля доступа, автоматизации учёта посещаемости или других внутренних процессов. Законодательство требует соблюдения особых условий:

* Получение осознанного письменного согласия со стороны учащихся или их законных представителей (пункт 1 статьи 11 Федерального закона №152-ФЗ).
* Гарантия локального хранения и обработки данных без передачи их третьим лицам.
* Соответствие методам защиты данных положениям статьи 19 закона №152-ФЗ, включая использование сертифицированных средств криптографической защиты.

## **6.2. Аргументы в пользу исключения проекта из сферы действия законодательства**

### 6.2.1. Принцип локальной обработки данных

В рамках настоящего проекта обработка биометрических данных осуществляется исключительно локально на оборудовании, расположенном в школе, без использования облачных хранилищ, интернет-соединений или сторонних баз данных. Это исключает проект из-под действия норм, регулирующих передачу биометрии через открытые каналы связи.

### 6.2.2. Отсутствие персонификации данных

База данных системы хранения лица учащихся и их идентификаторов не привязывается к паспортным или иным идентификационным данным. Система функционирует исключительно в режиме верификации: «лицо в базе – лицо перед камерой». Это означает, что даже в случае компрометации данных они не могут быть использованы для установления личности.

### 6.2.3. Неприменимость норм о Единой биометрической системе (ЕБС)

Поскольку система разработана для внутренних нужд образовательного учреждения, данные не подлежат обязательной передаче в ЕБС в соответствии с Федеральным законом №482-ФЗ. Более того, отсутствие коммерческой цели исключает необходимость использования сертифицированного оператором канала связи.

### 6.2.4. Соблюдение принципа добровольного согласия

Сбор и обработка биометрических данных учащихся осуществляются только после получения письменного согласия родителей (законных представителей), оформленного в строгом соответствии с требованиями статьи 9 Федерального закона №152-ФЗ. В согласии указываются:

* Цель обработки (обеспечение доступа к шкафчикам).
* Способы хранения данных (локально на устройстве).
* Порядок удаления данных (после окончания обучения).

### 6.2.5. Система контроля доступа как образовательный инструмент

Система распознавания лиц выполняет функцию не только автоматизации, но и обучения учащихся современным технологиям. Этот образовательный аспект не подпадает под коммерческое или публичное использование, которое требует строгой сертификации.

## **6.3. Этика и защита прав пользователей**

### 6.3.1. Минимизация сбора данных

Система ограничивается сбором только тех данных, которые необходимы для функционирования. Дополнительные данные о пользователе (возраст, пол, гражданство) не собираются.

### 6.3.2. Шифрование и защита базы данных

Для защиты биометрических шаблонов используется алгоритм AES-256, соответствующий международным стандартам безопасности. База данных защищена паролем и доступна только администратору системы.

### 6.3.3. Прозрачность работы системы

Родители и учащиеся имеют право в любой момент запросить информацию о сохранённых данных, получить их копию или потребовать удаления.

### 6.3.4. Срок хранения данных

Данные хранятся в течение учебного года и удаляются по окончании обучения либо по запросу родителей.

Настоящий проект разработан с учётом строгих юридических и этических норм. Его исключение из-под действия законодательства о биометрии базируется на отсутствии персонификации данных, локальной обработке и ограниченном функциональном применении. Соблюдение всех принципов обработки данных гарантирует защиту прав пользователей, минимизацию юридических рисков и соответствие текущему законодательству.