**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

Обеспечение безопасности предприятий является одной из ключевых задач в условиях современного мира, где угрозы, связанные с несанкционированным доступом, промышленным шпионажем, кражами имущества и информации, а также террористическими актами, становятся всё более разнообразными и изощрёнными. Пропускная система (ПС) предприятия выступает важнейшим элементом комплексной безопасности, обеспечивая контроль доступа на территорию и в помещения, учёт перемещений персонала и предотвращение противоправных действий. В сочетании с инженерно-технической защитой (ИТЗ), включающей физические барьеры, технические средства охраны (ТСО) и организационные меры, ПС формирует надёжный барьер против внешних и внутренних угроз.

Актуальность темы обусловлена несколькими факторами. Во-первых, рост числа инцидентов, связанных с нарушением безопасности, требует внедрения современных технологий для повышения эффективности ПС. Во-вторых, традиционные методы контроля доступа, такие как ключи, пропускные карты и PIN-коды, имеют существенные недостатки: они могут быть утеряны, украдены или подделаны. В-третьих, развитие биометрических технологий, в частности распознавания лиц, открывает новые возможности для создания высоконадёжных и удобных систем контроля доступа. Биометрия, основанная на уникальных физиологических характеристиках человека, исключает возможность подделки идентификаторов и упрощает процесс аутентификации, что особенно важно для предприятий с высоким уровнем конфиденциальности.

Современные ПС, интегрированные с биометрическими технологиями, позволяют не только ограничивать доступ, но и вести учёт рабочего времени, отслеживать перемещения сотрудников и оперативно реагировать на нештатные ситуации. Такие системы находят применение в офисах, на

производственных объектах, в банках, логистических центрах и даже в умных домах. Разработка биометрической ПС с использованием open-source инструментов и доступного оборудования делает подобные решения экономически выгодными для малых и средних предприятий, что подчёркивает практическую значимость данной работы.

Цель работы — спроектировать пропускную систему предприятия с применением инженерно-технической защиты и биометрической идентификации на основе распознавания лиц, обеспечивающую высокий уровень безопасности и удобство использования.

Задачи исследования:

– изучить теоретические основы инженерно-технической защиты и её роль в пропускных системах;

– проанализировать принципы работы биометрических систем контроля доступа, включая технологии распознавания лиц;

– разработать прототип биометрической пропускной системы с серверной и клиентской частями, обеспечивающий функции добавления пользователей, распознавания лиц и ведения журнала доступа;

– провести тестирование прототипа на выборке изображений, определив показатели ложного принятия (FAR) и ложного отказа (FRR) при различных порогах сравнения;

– построить график зависимости FAR и FRR от порога для оценки производительности системы;

– рассчитать затраты на разработку прототипа и предложить рекомендации по его улучшению и интеграции в пропускную систему.

Объект исследования — пропускные системы предприятий, обеспечивающие контроль доступа и безопасность.

Предмет исследования — биометрическая пропускная система с применением инженерно-технической защиты, основанная на технологии распознавания лиц.

Методы исследования включают:

- теоретический анализ литературы по ИТЗ, ПС и биометрии;
- программирование на Python с использованием библиотек FastAPI, Tkinter, DeepFace и Faiss;
- экспериментальное тестирование прототипа с расчётом метрик FAR и FRR;
- построение графика зависимости FAR и FRR от порога с помощью Matplotlib;
- экономический анализ затрат на разработку системы.

Научная новизна заключается в следующем:

– разработан прототип биометрической ПС, интегрирующий open-source инструменты для реализации функций распознавания лиц и ведения журнала доступа с фильтрацией по времени и имени;

– проведено тестирование прототипа на выборке из 50 изображений авторизованных и 50 изображений неавторизованных пользователей, определены оптимальные пороги (0.5–0.6) с FAR=0 и FRR=0.3971 – 0.2354;

– предложена архитектура клиент-серверной системы, взаимодействующей по протоколу REST API, обеспечивающая масштабируемость и потенциал для интеграции с физическими СКУД.

Практическая значимость работы заключается в возможности применения разработанного прототипа в пропускных системах малых и средних предприятий, офисов, складов и умных домов. Система отличается низкой стоимостью, использованием доступного оборудования и open-source программного обеспечения, что делает её экономически выгодной

альтернативой коммерческим СКУД. Журнал доступа с фильтрацией упрощает учёт перемещений сотрудников, а высокая точность распознавания лиц повышает уровень безопасности.

Теоретическая значимость состоит в систематизации знаний о роли ИТЗ и биометрии в ПС, а также в анализе производительности биометрических систем на основе метрик FAR и FRR. Результаты тестирования прототипа дополняют исследования в области распознавания лиц, демонстрируя влияние размера выборки и условий эксплуатации на точность системы.

# 1 Теоретические основы инженерно-технической защиты пропускных систем

## 1.1 Компоненты инженерно-технической защиты

Инженерно-техническая защита (ИТЗ) представляет собой комплекс инженерных сооружений, технических средств и организационных мероприятий, направленных на обеспечение безопасности объектов, включая предприятия, офисы, склады и другие инфраструктурные комплексы. В контексте пропускной системы (ПС) предприятия ИТЗ выполняет функцию первой линии обороны, предотвращая несанкционированный доступ, хищение имущества, утечку информации и другие угрозы. Эффективность ПС во многом зависит от грамотной интеграции компонентов ИТЗ, которые работают в синергии, создавая многоуровневую систему защиты. Основные компоненты ИТЗ включают физические барьеры, технические средства охраны (ТСО), инженерные сооружения и организационные меры. Каждый из этих компонентов выполняет специфические функции, дополняя другие элементы системы и обеспечивая комплексный подход к безопасности [1].

### 1.1.1 Физические барьеры

Физические барьеры являются основой ИТЗ и предназначены для физического ограничения доступа на территорию предприятия или в его помещения. Они создают препятствия для потенциальных злоумышленников, затрудняя проникновение и предоставляя время для реагирования служб охраны. К физическим барьерам относятся ограждения, ворота, шлагбаумы, двери, окна, решётки, турникеты, шлюзовые системы и другие конструкции. Выбор типа барьера зависит от специфики объекта, уровня угроз и эстетических требований. Например, для защиты периметра

промышленного предприятия могут использоваться высокие металлические ограждения с колючей проволокой или датчиками вибрации, тогда как в офисных зданиях предпочтение отдаётся прочным дверям с электронными замками и турникетам.

Материалы физических барьеров должны обладать высокой прочностью, устойчивостью к коррозии и механическим воздействиям. Например, ограждения из сварной сетки с антикоррозийным покрытием обеспечивают долговечность и надёжность, а двери из стали с усиленными петлями устойчивы к взлому. Конструкция барьеров должна исключать возможность их обхода, например, через подкоп или перелаз. На рисунке 1 представлен пример физического барьера, используемого для защиты периметра предприятия.

Рисунок 1 — Ограждение с колючей проволокой

Физические барьеры играют ключевую роль в ПС, так как они определяют точки входа и выхода, через которые осуществляется контроль доступа. Например, турникеты в офисных зданиях ограничивают проход, позволяя пропускать только авторизованных лиц, а шлюзовые системы

обеспечивают дополнительный уровень проверки, предотвращая одновременный проход нескольких человек. На производственных объектах ворота с автоматическими шлагбаумами контролируют въезд транспортных средств, минимизируя риск несанкционированного проезда [2].

### 1.1.2 Технические средства охраны

Технические средства охраны (ТСО) предназначены для обнаружения нарушений, мониторинга территории и помещений, а также для управления доступом. ТСО включают системы видеонаблюдения (CCTV), охранную сигнализацию, системы контроля и управления доступом (СКУД), системы обнаружения вторжений (СОВ), системы оповещения и управления эвакуацией (СОУЭ), а также биометрические системы. Современные ТСО обладают широкими функциональными возможностями, позволяя создавать интегрированные системы безопасности, которые оперативно реагируют на угрозы и координируют действия персонала.

Системы видеонаблюдения обеспечивают визуальный контроль за территорией, фиксируя все события в реальном времени и сохраняя записи для последующего анализа. Например, IP-камеры с разрешением 1080p и инфракрасной подсветкой позволяют вести наблюдение в условиях низкой освещённости, что особенно важно для ночного мониторинга периметра. Охранная сигнализация обнаруживает попытки взлома дверей, окон или ограждений, отправляя сигнал тревоги на пульт охраны. СКУД ограничивают доступ в помещения, идентифицируя сотрудников по пропускам, PIN-кодам или биометрическим данным, а также ведут учёт рабочего времени. Биометрические СКУД, такие как системы распознавания лиц, повышают надёжность идентификации, исключая возможность подделки идентификаторов, что будет подробно рассмотрено в разделе 1.4. На рисунке 2 показан пример интеграции ТСО в ПС офисного здания [3].


Рисунок 2 — Система видеонаблюдения

Интеграция ТСО в единую систему значительно повышает эффективность ПС. Например, при срабатывании датчика охранной сигнализации на периметре система видеонаблюдения автоматически направляет ближайшую камеру на зону срабатывания, а СКУД блокирует доступ в помещения, предотвращая дальнейшее проникновение. В контексте ПС ТСО обеспечивают не только контроль доступа, но и учёт перемещений, что важно для поддержания дисциплины и предотвращения нарушений трудового распорядка. Например, журнал доступа, формируемый СКУД, позволяет отслеживать время входа и выхода сотрудников, что повышает прозрачность работы предприятия.

### 1.1.3 Инженерные сооружения

Инженерные сооружения усиливают физическую защиту объекта, создавая дополнительные препятствия для злоумышленников и защищая от

последствий чрезвычайных ситуаций. К ним относятся укреплённые периметры, блокираторы дорог, противотаранные устройства, системы освещения, системы пожаротушения и другие решения. Укреплённые периметры, такие как бетонные стены или рвы, предотвращают подкоп или пролом ограждений. Противотаранные устройства, например, болларды или автоматические барьеры, блокируют несанкционированный въезд транспортных средств, что особенно актуально для объектов с высоким риском террористических угроз.

Системы освещения играют важную роль в обеспечении видимости в тёмное время суток, облегчая работу охранников и видеокамер, а также создавая психологический барьер для злоумышленников. Например, светодиодные прожекторы с датчиками движения включаются только при обнаружении активности, что снижает энергопотребление и повышает эффективность. Системы пожаротушения минимизируют ущерб от пожаров, обеспечивая безопасность персонала и имущества [4].

В ПС инженерные сооружения дополняют физические барьеры и ТСО, создавая комплексную защиту. Например, на въезде на территорию предприятия блокираторы дорог работают в связке с видеокамерами и СКУД, обеспечивая контроль транспортных средств, а системы освещения улучшают видимость у контрольно-пропускных пунктов (КПП). На рисунке 3 представлен пример инженерного сооружения, используемого в ПС.

Рисунок 3 — Противотаранное устройство на въезде предприятия

### 1.1.4 Организационные меры

Организационные меры являются неотъемлемой частью ИТЗ и включают разработку нормативных документов, организацию пропускного режима, обучение персонала, проведение тренировок и учений, а также другие мероприятия, направленные на повышение безопасности. Пропускной режим регламентирует порядок прохода и проезда через КПП, определяет правила выдачи пропусков, процедуры проверки документов и досмотра. Например, на крупных предприятиях пропускной режим может включать обязательную проверку удостоверений личности, сканирование багажа и регистрацию посетителей в электронных журналах [5].

Обучение персонала играет ключевую роль в обеспечении эффективности ПС. Сотрудники охраны должны быть подготовлены к работе с ТСО, реагированию на сигналы тревоги и проведению досмотра. Рядовые сотрудники также обучаются правилам поведения в чрезвычайных ситуациях, таких как пожар или эвакуация, что минимизирует панику и повышает безопасность. Регулярные тренировки и учения позволяют отрабатывать сценарии угроз, например попытки несанкционированного проникновения или террористических актов, повышая готовность персонала.

Организационные меры тесно связаны с другими компонентами ИТЗ. Например, пропускной режим опирается на физические барьеры (турникеты, шлагбаумы) и ТСО (СКУД, видеонаблюдение), а обучение персонала включает инструктаж по использованию биометрических терминалов [6].

### 1.1.5 Примеры применения компонентов ИТЗ в ПС

Для иллюстрации роли компонентов ИТЗ рассмотрим несколько практических примеров. На промышленном предприятии, таком как

металлургический завод, периметр защищён металлическими ограждениями с датчиками вибрации, а въезд транспорта контролируется шлагбаумами и видеокамерами. СКУД на основе proximity-карт ограничивают доступ в производственные цеха, а системы освещения обеспечивают видимость в ночное время. Организационные меры включают строгую проверку пропусков и регулярные учения по эвакуации.

В офисных зданиях ПС ориентирована на удобство сотрудников и посетителей. Турникеты с биометрическими терминалами (например, распознавание лиц) обеспечивают быстрый и надёжный доступ, а видеонаблюдение фиксирует все перемещения в холле. Инженерные сооружения, такие как автоматические двери с магнитными замками, предотвращают несанкционированный вход, а обучение персонала включает инструктаж по использованию СКУД. Такие системы особенно востребованы в IT-компаниях, где защита конфиденциальной информации является приоритетом [7].

На складах и логистических центрах ПС фокусируется на контроле грузов и предотвращении хищений. Противотаранные устройства на въезде защищают от несанкционированного проезда, а видеокамеры с функцией распознавания номеров фиксируют транспорт. СКУД ограничивают доступ в зоны хранения, а организационные меры включают регулярную инвентаризацию и проверку сотрудников.

### 1.1.6 Роль компонентов ИТЗ в контексте биометрических ПС

В современных ПС всё большую роль играют биометрические технологии, которые интегрируются с другими компонентами ИТЗ. Биометрические СКУД, основанные на распознавании лиц, отпечатков пальцев или радужной оболочки глаза, повышают надёжность идентификации, исключая возможность подделки пропусков или кражи

ключей. В контексте ПС биометрия выполняет несколько функций: она обеспечивает быстрый доступ для авторизованных лиц, ведёт учёт перемещений через электронные журналы и предотвращает несанкционированное проникновение. Например, система распознавания лиц, установленная на турникетах офисного здания, позволяет сотрудникам входить без физических пропусков, а журнал доступа фиксирует время и личность каждого входящего.

Биометрические системы тесно взаимодействуют с другими компонентами ИТЗ. Физические барьеры, такие как турникеты, служат точкой проверки, где биометрический терминал сканирует лицо. Видеонаблюдение фиксирует процесс идентификации, обеспечивая дополнительный уровень контроля. Инженерные сооружения, такие как системы освещения, улучшают качество изображений, получаемых биометрическими камерами, а организационные меры включают обучение сотрудников правильному позиционированию перед терминалом. Таким образом, биометрия усиливает ПС, делая её более надёжной и удобной.

## 1.2 Оценка эффективности инженерно-технической защиты

Эффективность инженерно-технической защиты (ИТЗ) определяет способность пропускной системы (ПС) предприятия обеспечивать безопасность, предотвращать угрозы и минимизировать затраты. Оценка эффективности ИТЗ проводится по техническим, организационным и экономическим параметрам, которые отражают надёжность системы, скорость реагирования и целесообразность вложений. Эти параметры особенно важны для ПС, так как они напрямую влияют на контроль доступа, учёт перемещений и защиту от несанкционированного проникновения. Включение биометрических технологий, таких как распознавание лиц, в состав ИТЗ требует дополнительных метрик, таких как ложное принятие

(FAR) и ложный отказ (FRR), которые будут рассмотрены в контексте современных ПС [8].

### 1.2.1 Технические параметры

Технические параметры ИТЗ оценивают способность системы обнаруживать, предотвращать и задерживать нарушителей. Ключевые метрики включают:

- вероятность обнаружения — доля инцидентов, зафиксированных техническими средствами охраны (ТСО), такими как видеокамеры или датчики сигнализации. Например, IP-камеры с разрешением 1080p обеспечивают вероятность обнаружения до 95% в дневных условиях;
- время задержки — период, необходимый для предотвращения проникновения после обнаружения. Турникеты с СКУД увеличивают время задержки на 5–10 секунд, что достаточно для реакции охраны;
- надёжность — устойчивость системы к сбоям и внешним воздействиям. Например, ограждения с датчиками вибрации сохраняют работоспособность при температуре от –40 до +50 °C.

В ПС технические параметры критически важны для обеспечения контроля доступа. Например, на складе СКУД с ключ--картами обеспечивает вероятность обнаружения несанкционированного доступа до 98%, но может быть скомпрометирована при утере карты. Биометрические СКУД, использующие распознавание лиц, повышают надёжность за счёт уникальности идентификатора, но требуют учёта FAR и FRR [9].

### 1.2.2 Организационные параметры

Организационные параметры оценивают эффективность пропускного режима и взаимодействия персонала. Основные метрики:

– время реагирования — период от срабатывания тревоги до принятия мер. Например, на заводе охрана реагирует на сигнал сигнализации за 30–60 секунд;

– пропускная способность — число лиц, проходящих через КПП за единицу времени. Турникеты с биометрическими терминалами обрабатывают до 20 человек в минуту, что выше, чем при ручной проверке (5–10 человек);

– уровень подготовки персонала — способность сотрудников работать с ТСО и соблюдать инструкции. Регулярные тренировки повышают этот показатель на 20–30%.

В ПС организационные параметры обеспечивают слаженную работу системы. Например, в офисном здании журнал доступа, формируемый биометрической СКУД, позволяет охране за 1–2 минуты проверить историю перемещений сотрудника. Обучение персонала правильному позиционированию перед биометрическим терминалом снижает количество ошибок идентификации [10].

### 1.2.3 Биометрические метрики в ИТЗ

В современных ПС, использующих биометрию, эффективность оценивается через метрики FAR (False Acceptance Rate, ложное принятие) и FRR (False Rejection Rate, ложный отказ). FAR отражает долю случаев, когда система ошибочно пропускает неавторизованное лицо, а FRR — долю ошибочных отказов авторизованным лицам. Эти метрики зависят от качества камер, освещения и размера базы данных лиц, что делает их важными для оценки ПС [11].

Сравнение биометрических и традиционных СКУД показывает преимущества первых. Карточные системы имеют высокий риск утери или

подделки (FAR до 0.1), тогда как биометрия обеспечивает FAR~0 при правильной настройке. Однако высокие значения FRR (до 0.2–0.4) в условиях плохого освещения требуют дополнительных мер, таких как камеры с ИК-подсветкой. На рисунке 4 представлен пример биометрического терминала, используемого в ПС.


Рисунок 4 — Биометрический терминал

### 1.3 Угрозы безопасности и их нейтрализация

Пропускные системы (ПС) предприятий играют ключевую роль в обеспечении безопасности, предотвращая угрозы, которые могут нанести ущерб имуществу, персоналу и конфиденциальной информации. Угрозы безопасности включают несанкционированный доступ, хищение имущества или данных, вандализм, диверсии, террористические акты, а также специфические атаки на биометрические системы, такие как спуфинг. Инженерно-техническая защита (ИТЗ), включающая физические барьеры, технические средства охраны (ТСО), инженерные сооружения и

организационные меры, нейтрализует эти угрозы, создавая многоуровневую систему безопасности. Особое значение в современных ПС имеют биометрические технологии, такие как распознавание лиц, которые повышают надёжность идентификации и минимизируют риски, связанные с традиционными методами контроля доступа. В данном разделе рассмотрены основные угрозы и способы их нейтрализации с акцентом на роль ИТЗ и биометрии [12].

### 1.3.1 Несанкционированный доступ

Несанкционированный доступ — одна из наиболее распространённых угроз, заключающаяся в проникновении на территорию предприятия или в его помещения лиц, не имеющих соответствующих полномочий. Такие инциденты могут быть вызваны взломом физических барьеров, подделкой пропусков, использованием украденных ключей или социальной инженерией (например, обманом охраны). Последствия несанкционированного доступа включают кражи, утечку данных и угрозу безопасности персонала.

ИТЗ нейтрализует эту угрозу через сочетание компонентов. Физические барьеры, такие как металлические ограждения с колючей проволокой или турникеты, создают препятствия для проникновения. Технические средства охраны, включая системы видеонаблюдения и СКУД, фиксируют попытки доступа и ограничивают проход. Например, IP-камеры с функцией распознавания лиц в реальном времени обнаруживают подозрительных лиц, а СКУД на основе ключ-карт блокируют вход без действующего идентификатора. Организационные меры, такие как строгий пропускной режим и проверка документов, дополняют защиту, исключая возможность обмана охраны.

Биометрические СКУД, использующие распознавание лиц, значительно повышают защиту от несанкционированного доступа. В отличие

от карт или ключей, которые могут быть украдены, биометрические данные уникальны и не подлежат передаче. Например, система распознавания лиц с алгоритмом машинного обучения обеспечивает вероятность ложного принятия (FAR) менее 0.01 при больших выборках, что делает её надёжным барьером. На рисунке 5 показан пример турникета с биометрическим терминалом, предотвращающего несанкционированный доступ.

Рисунок 5 — Турникет с биометрическим терминалом

### 1.3.2 Хищение имущества и информации

Хищение имущества (материальных ценностей, оборудования) и информации (коммерческих секретов, данных клиентов) представляет серьёзную угрозу для предприятий. Хищения могут совершаться как внешними злоумышленниками, так и сотрудниками (инсайдерские угрозы). Например, на складах воровство грузов составляет до 1–2% от оборота, а в IT-компаниях утечка данных может привести к многомиллионным убыткам.

ИТЗ минимизирует риск хищений через комплексный подход. Физические барьеры, такие как укреплённые двери с магнитными замками, ограничивают доступ в зоны хранения. Системы видеонаблюдения фиксируют перемещения на территории, а датчики охранной сигнализации срабатывают при попытке взлома. СКУД ведут учёт входов и выходов, позволяя выявить подозрительные действия. Например, журнал доступа, формируемый СКУД, фиксирует время и личность каждого входящего, что помогает расследовать инциденты. Организационные меры, включая инвентаризацию и обучение персонала, предотвращают инсайдерские угрозы.

### 1.3.3 Вандализм, диверсии и терроризм

Вандализм (повреждение имущества), диверсии (нарушение работы предприятия) и террористические акты представляют угрозы, требующие повышенных мер защиты. Вандализм может включать порчу ограждений, граффити или повреждение оборудования. Диверсии, такие как поджоги или отключение систем, направлены на срыв производства. Террористические акты угрожают жизни персонала и целостности объекта.

ИТЗ нейтрализует эти угрозы через усиленные конструкции и оперативное реагирование. Противотаранные устройства, такие как болларды, предотвращают въезд транспортных средств с взрывчаткой. Инженерные сооружения, включая бетонные стены и системы пожаротушения, минимизируют ущерб от диверсий. Видеонаблюдение и сигнализация обнаруживают подозрительные действия, а системы оповещения (СОУЭ) координируют эвакуацию. Организационные меры, такие как учения по антитеррору, повышают готовность персонала [13].

### 1.3.4 Примеры нейтрализации угроз

Рассмотрим несколько кейсов применения ИТЗ для нейтрализации угроз:

- металлургический завод: Ограждения с датчиками вибрации и видеокамеры предотвращают несанкционированный доступ, а СКУД с proximity-картами ограничивают вход в цеха, снижая риск хищений;
- офис IT-компании: Биометрическая СКУД с распознаванием лиц защищает серверные помещения, а журнал доступа фиксирует перемещения, предотвращая утечку данных;
- логистический центр: Противотаранные устройства и видеонаблюдение с распознаванием номеров минимизируют риск диверсий, а учения персонала повышают готовность к ЧС.

Эти примеры демонстрируют, что ИТЗ эффективно нейтрализует угрозы через интеграцию физических, технических и организационных мер, а биометрия усиливает защиту, исключая слабые места традиционных СКУД.

## 1.4 Биометрические технологии в пропускных системах

Биометрические технологии, основанные на уникальных физиологических или поведенческих характеристиках человека, становятся неотъемлемой частью пропускных систем (ПС) предприятий, обеспечивая высокий уровень безопасности и удобство контроля доступа. В отличие от традиционных методов, таких как ключи, пропускные карты или PIN-коды, биометрия исключает возможность утери или подделки идентификаторов, что делает её предпочтительным решением для защиты объектов с высокими требованиями к безопасности. В данном разделе рассмотрены основные типы биометрических технологий, их применение в ПС, преимущества и

недостатки, а также роль распознавания лиц как ключевого элемента современных систем контроля доступа.

### 1.4.1 Типы биометрических технологий

Биометрические системы классифицируются по типу используемых характеристик: физиологические (лицо, отпечатки пальцев, радужная оболочка глаза, геометрия руки) и поведенческие (голос, походка, динамика подписи). В ПС наибольшее распространение получили следующие технологии:

- распознавание лиц: анализирует черты лица (расстояние между глазами, форма носа) с помощью камер и алгоритмов машинного обучения;
- отпечатки пальцев: используют уникальный рисунок папиллярных линий. Сканеры отпечатков широко применяются в офисах благодаря низкой стоимости (10–50 тыс. рублей за терминал) и высокой точности (FAR~0.0001);
- сканирование радужной оболочки: анализирует узор радужки глаза, обеспечивая FAR~0.00001, но требует дорогостоящих сканеров (100–200 тыс. рублей);
- распознавание голоса: использует спектральные характеристики голоса, но менее надёжно из-за шумов (FAR~0.05–0.1).

В ПС распознавание лиц занимает лидирующее положение среди биометрических технологий благодаря бесконтактности, высокой скорости (идентификация за 0.5–2 секунды) и доступности оборудования.

### 1.4.2 Применение биометрии в пропускных системах

Биометрические технологии применяются в ПС для контроля доступа, учёта рабочего времени и предотвращения угроз. Основные сценарии включают:

- ограничение доступа: Турникеты с биометрическими терминалами в офисах пропускают только авторизованных сотрудников, исключая подделку пропусков;
- учёт перемещений: Журналы доступа, формируемые СКУД, фиксируют время, имя и фото входящих, упрощая расследование инцидентов;
- интеграция с другими средствами ИТЗ: Биометрия сочетается с видеонаблюдением и сигнализацией, создавая многоуровневую защиту.

Примеры применения включают офисы IT-компаний, где распознавание лиц обеспечивает доступ в серверные зоны, и аэропорты, где биометрические терминалы ускоряют регистрацию пассажиров. В аэропорту Домодедово система FaceBoarding сократила время проверки на 50%, пропуская до 30 человек в минуту. На рисунке 6 показан биометрический терминал в аэропорту.


Рисунок 6 — Биометрический терминал в аэропорту Домодедово

### 1.4.3 Преимущества и недостатки биометрических технологий

Биометрические системы обладают рядом преимуществ:

- высокая надёжность: Уникальность биометрических данных исключает подделку;
- удобство: Бесконтактные технологии, такие как распознавание лиц, не требуют физических носителей;
- масштабируемость: Базы данных лиц могут содержать миллионы записей, что подходит для крупных предприятий.

Однако биометрия имеет и недостатки:

- зависимость от условий: Плохое освещение или низкое качество камер увеличивают FRR до 0.2–0.4;
- уязвимость к атакам: Биометрические системы подвержены риску выхода из строя в результате DoS и DDoS атак;
- этические вопросы: Хранение биометрических данных вызывает опасения конфиденциальности, что требует шифрования и строгого доступа.

Сравнение биометрических технологий с традиционными СКУД показывает их превосходство. Карточные системы имеют FAR до 0.1 из-за утери карт, тогда как биометрия обеспечивает FAR~0 при оптимальных настройках [14].

### 1.4.4 Алгоритмы распознавания лиц

Распознавание лиц опирается на алгоритмы глубокого обучения, такие как ArcFace, и DeepFace, которые преобразуют изображения лиц в эмбеддинги (векторы признаков) для сравнения. ArcFace, используемый в коммерческих системах, достигает точности 99.5% на датасете LFW благодаря метрике углового расстояния. DeepFace, применяемый в open-

source решениях, обеспечивает FAR~0.01–0.05 при меньших вычислительных затратах, что делает его доступным для малых предприятий. Процесс включает:

- обнаружение лица;
- извлечение эмбеддинга;
- сравнение с базой данных.

В ПС алгоритмы распознавания лиц интегрируются с турникетами и журналами доступа, обеспечивая быстрый контроль. На рисунке 7 представлена схема работы алгоритма распознавания лиц [15].


Рисунок 7 — Схема работы алгоритма распознавания лиц

# 2 Разработка биометрической пропускной системы

## 2.1 Описание биометрической пропускной системы

Разработанный прототип биометрической пропускной системы (ПС) предприятия предназначен для контроля доступа с использованием технологии распознавания лиц, интегрированной с инженерно-технической защитой (ИТЗ). Система обеспечивает добавление пользователей, распознавание лиц с помощью веб-камеры и ведение журнала доступа с возможностью фильтрации по имени и времени. Прототип реализован в клиент-серверной архитектуре, где серверная часть построена на FastAPI с использованием библиотек DeepFace и Faiss, а клиентская — на Tkinter с интерфейсом для взаимодействия с пользователем. Система работает на доступном оборудовании, что делает её экономически выгодной для малых и средних предприятий. В данном разделе описаны архитектура, функциональность и программные компоненты прототипа, а также их связь с ИТЗ.

### 2.1.1 Архитектура системы

Прототип имеет клиент-серверную архитектуру, в которой сервер обрабатывает запросы на добавление, удаление, обновление и распознавание лиц, а клиент предоставляет графический интерфейс и взаимодействует с веб-камерой. Взаимодействие между компонентами осуществляется через REST API, обеспечивающее масштабируемость и простоту интеграции с другими системами, такими как физические СКУД. Основные компоненты серверной части системы включают

– эндпоинты (endpoints.py): Реализуют API-запросы: faces/add (добавление лица в базу), faces/find (распознавание лица), /logs (получение журнала доступа);

– обработка эмбеддингов (handlers.py): Использует DeepFace (алгоритм ArcFace) для извлечения эмбеддингов лиц и Faiss для эффективного поиска ближайших совпадений в базе;

– хранение данных: MongoDB для журнала доступа, содержащего записи о времени, имени и статусе распознавания, а также для информации о пользователях.

В состав клиентской части входит:

– главное окно (app.py): Интерфейс для управления системой, включая кнопки для добавления пользователей, смены темы, скриншота и просмотра журнала;

– форма добавления (add_form.py): Окно для ввода фамилии, имени и фотографии пользователя;

– журнал доступа (log_window.py): Окно с таблицей логов и фильтрацией по имени и времени;

– API-взаимодействие (api_logic.py): Модуль для отправки REST-запросов к серверу и обработки видеопотока с камеры.

Архитектура системы представлена на схеме ниже, иллюстрирующей взаимодействие клиента и сервера через REST API.

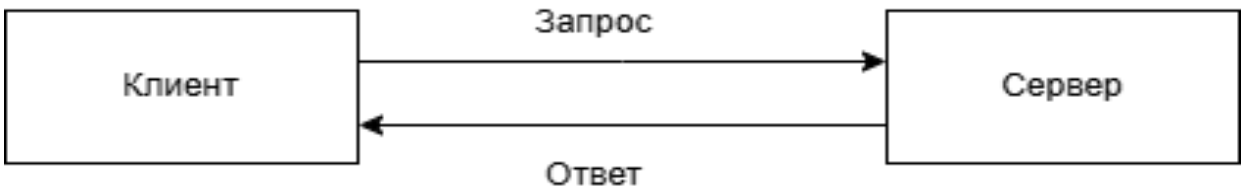


Рисунок 8 — Архитектура биометрической пропускной системы

Поток данных в системе следующий:

– пользователь через клиентский интерфейс (Tkinter) захватывает фото с веб-камеры;

– клиент отправляет REST-запрос (POST faces/add для добавления или faces /find для распознавания) с изображением на сервер;

– сервер извлекает эмбеддинг лица с помощью DeepFace, сохраняет его (для faces/add) или ищет совпадения в базе (для faces/find);

– результат (имя, статус) возвращается клиенту, а событие записывается в журнал доступа;

– клиент отображает результат в виде всплывающего окна.

Фрагмент кода эндпоинта faces/find, реализующего поиск совпадения для лица, показан на рисунке 9.

```python
@app.post("/faces/find")
async def find_face_endpoint(
    file: Annotated[UploadFile, File(...)],
    threshold: Optional[float] = Form(.5),
):
    logger.debug(threshold)
    bytes_file = await file.read()
    if len(bytes_file) > 5 * 1024 * 1024:
        raise HTTPException(status_code=400, detail="Файл слишком большой")
    buf = BytesIO(bytes_file)
    img = Image.open(buf)
    arr = np.array(img)
    person_name, min_distance = face_handlers.find_face(arr, threshold)
    response = {"threshold": threshold, "min_distance": float(min_distance)}

    mongo = FaceCollection(CLIENT)
    if person_name:
        await mongo.write_log(person_name, True)
        response["name"] = person_name
        return JSONResponse(response)

    await mongo.write_log("неизвестный", False)
    response["message"] =  "Лицо не найдено"
    return JSONResponse(response, status_code=404)
```

Рисунок 9 — Фрагмент кода эндпоинта faces/find в endpoints.py

### 2.1.2 Функциональность системы

Прототип реализует три основные функции, обеспечивающие контроль доступа и учёт перемещений:

– добавление пользователя: пользователь вводит имя и делает фото через форму добавления. Фото отправляется на сервер (запрос faces/add), где DeepFace извлекает эмбеддинг лица, который сохраняется в базе MongoDB;

– распознавание лица: клиент захватывает изображение с веб-камеры и отправляет запрос на faces/find. Сервер сравнивает эмбеддинг с базой Faiss, возвращая имя ближайшего совпадения (если расстояние ниже порога, например, 0.3–0.4) или статус 404 с сообщением «Пользователь не найден». Распознавание выполняется за 0.5–1 секунду;

– ведение журнала доступа: каждое событие распознавания записывается в базу данных. Журнал доступен через энпоинт /logs и отображается в клиентском окне с фильтрацией по имени и времени.

Эти функции обеспечивают базовые требования ПС: идентификацию, контроль доступа и учёт. Для наглядной демонстрации была составлена блок-схема алгоритма работы всей системы, представленная на рисунке 10.

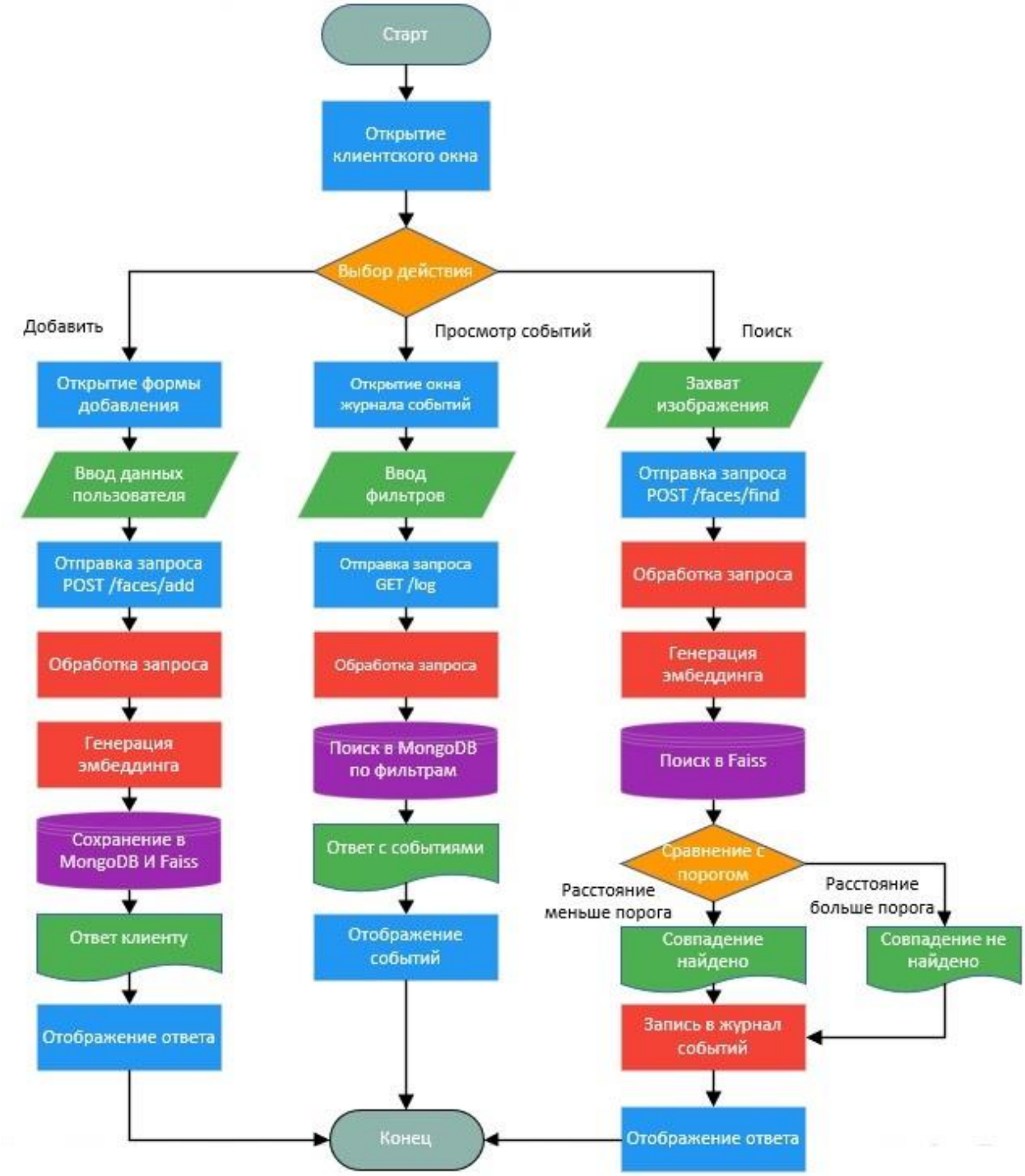


Рисунок 10 — Блок-схема работы приложения

Фрагмент кода обработки эмбеддингов, реализующий извлечение и поиск с помощью DeepFace и Faiss, представлен на рисунке 11.

```python
def find_face(self, img: np.ndarray, threshhold=.5):
    try:
        embedding = get_embedding(img)
        normilize_embedding = embedding / np.linalg.norm(embedding)
        distances, indices = self.index.search(np.array([normilize_embedding], dtype=np.float64), 1)
        distance = distances[0][0]
        index = indices[0][0]

        normilize_distance = distance / sqrt(512) * 10
        if normilize_distance < threshhold and index < len(self.names):
            logger.info("Пользователь найден")
            return self.names[index], normilize_distance
        logger.info("Пользователь НЕ найден")
        return None, normilize_distance

    except Exception as e:
        logger.error(f"Ошибка при поиске лица: {e}")
        raise
```

Рисунок 11 — Фрагмент кода обработки эмбеддингов в handlers.py

### 2.1.3 Интеграция с инженерно-технической защитой

Прототип интегрируется с ИТЗ, усиливая физические и технические меры безопасности. Веб-камера Logitech C920 выполняет роль технического средства охраны (ТСО), заменяя традиционные считыватели карт. Журнал доступа с фильтрацией соответствует организационным мерам, упрощая учёт перемещений и расследование инцидентов. REST API позволяет подключить прототип к физическим СКУД, например, турникетам с электронными замками, где сигнал распознавания (авторизован/не авторизован) управляет доступом. Например, в офисе на 50 сотрудников система может быть интегрирована с турникетом, открывающимся при успешном распознавании за 1 секунду.

Клиентский интерфейс реализован в двух темах (светлой и темной) для удобства пользователей. Графический интерфейс главного окна в светлой теме показан на рисунке 14.

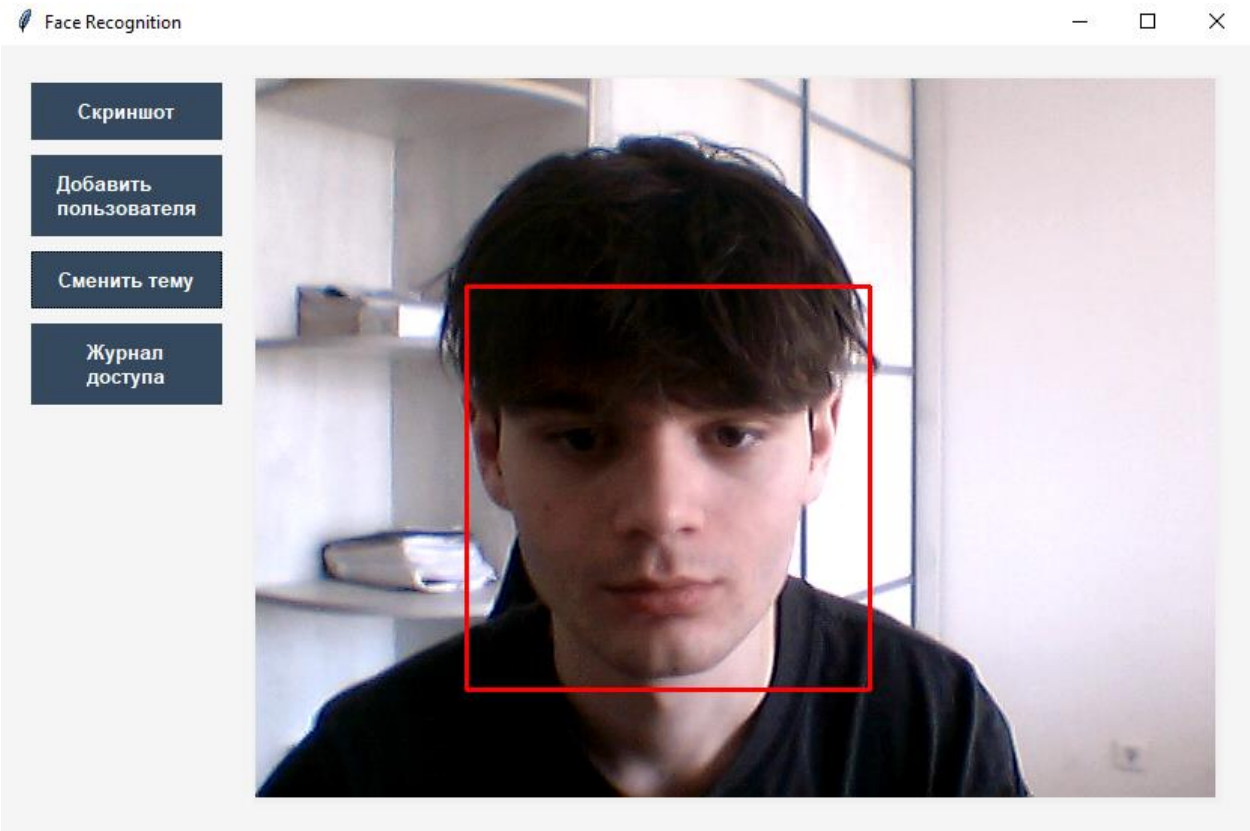


Рисунок 14 — Интерфейс главного окна

Фрагмент кода, отвечающий за формирование главного окна представлен на рисунке 15.

```
def create_widgets(self):
    self.frame = ttk.Frame(self.window, padding=10, style="Main.TFrame")
    self.frame.pack(side="left", fill="both", expand=True)

    self.canvas = tk.Canvas(self.frame, width=self.width, height=self.height)
    self.canvas.pack(fill="both", side="right", expand=True, padx=10, pady=10)

    self.button_frame = ttk.Frame(self.frame, style="Main.TFrame")
    self.button_frame.pack(side="top", fill="y", padx=10, pady=10)


    self.btn_snapshot = ttk.Button(self.button_frame, text="Скриншот", command=self.screenshot, width=15)
    self.btn_snapshot.pack(side="top", pady=5)
    self.btn_add = ttk.Button(self.button_frame, text="Добавить\nпользователя", command=self.open_add_window, width=15)
    self.btn_add.pack(side="top", pady=5)
    self.btn_log = ttk.Button(self.button_frame, text="Журнал\nдоступа", command=self.open_log_window, width=15)
    self.btn_log.pack(side="bottom", pady=5)
    self.btn_chache_theme = ttk.Button(self.button_frame, text="Сменить тему", width=15, command=self.change_theme)
    self.btn_chache_theme.pack(side="bottom", pady=5)
```

Рисунок 15 — Фрагмент кода главного окна в app.py

### 2.1.4 Программные компоненты и их реализация

Программные компоненты прототипа реализованы на Python с использованием open-source библиотек, перечисленных ниже:

- DeepFace: Извлекает эмбеддинги лиц при помощи модели глубокого обучения ArcFace, обеспечивая FAR~0 и FRR~0.2–0.4 при порогах 0.3–0.4 (см. раздел 2.2);
- Faiss: Выполняет быстрый поиск ближайших эмбеддингов, поддерживая базы до 10,000 лиц;
- FastAPI: Обеспечивает асинхронную обработку запросов, поддерживая до 100 запросов/секунду;
- Tkinter: Реализует графический интерфейс с тремя окнами (главное, форма, журнал);
- OpenCV: Обрабатывает видеопоток с веб-камеры через api_logic.py;
- MongoDB: Хранит данные о пользователях и журнал регистрации событий.

Фрагмент кода, отправляющего запрос на эндпоинт faces/find представлен на рисунке 16.

```
def get_face(self, frame: MatLike):
    try:
        file = self.frame2bytes(frame)
        resp = super().get_face(file)
        logger.info("Отправлен запрос на распознавание пользователя")
        self.__last_request = datetime.now()
        return resp
    except requests.exceptions.RequestException as e:
        logger.error(f"Ошибка при отправке запроса {e}")
    except Exception as e:
        logger.error(f"Ошибка в get_face {e}")
    finally:
        self.task = None
```

Рисунок 16 — Фрагмент кода взаимодействия с API в api_logic.py

Фрагмент кода функции, отвечающей за обработку видеопотока и обнаружения лица, представлен на рисунке 17.

```
def update(self):
    ok, frame = self.cap.read()
    if ok:
        frame = cv.cvtColor(frame, cv.COLOR_BGR2RGB)
        gray_img = cv.cvtColor(frame, cv.COLOR_RGB2GRAY)
        faces = self.face_detector.detectMultiScale(
            gray_img,
            scaleFactor=1.1,
            minNeighbors=3,
            minSize=(100,100)
        )
        for (x, y, w, h) in faces:
            cv.rectangle(frame, (x, y), (x+w, y+h), (255, 0, 0), 2)
            if datetime.now() - self.__last_request > timedelta(seconds=3) \
            and self.task is None:
                face_slice = frame[y:y+h, x:x+w]
                self.task = self.thread_pool.submit(self.get_face, face_slice)
    return frame
```

Рисунок 17 — Фрагмент кода обработки видеопотока и обнаружения лица в api_logic.py

### 2.2 Тестирование и анализ производительности

Тестирование биометрической пропускной системы (ПС) направлено на оценку её точности и производительности в условиях, приближенных к реальной эксплуатации. Главная задача заключалась в измерении метрик ложного принятия (FAR, False Acceptance Rate) и ложного отказа (FRR, False Rejection Rate), которые определяют надёжность распознавания лиц, а также в анализе скорости обработки запросов и устойчивости системы к различным углам поворота лица. Для этого использовался скрипт test_far_frr.py, обрабатывающий выборку изображений, хранящихся в локальных директориях, с последующим взаимодействием с сервером через REST API.

Тесты проводились на доступном оборудовании, а результаты подтвердили применимость прототипа для офисов, складов и других объектов, требующих инженерно-технической защиты (ИТЗ). В данном разделе описаны методика, реализация, результаты тестирования и их анализ.

### 2.2.1 Методика тестирования

Тестирование проводилось на ПК с процессором AMD Ryzen 5 и 12 ГБ оперативной памяти. Для хранения эмбеддингов лиц и логов использовалась база данных MongoDB, в которую данные авторизованных пользователей были добавлены через эндпоинт faces/add, код которого представлен на рисунке 18.

```python
@app.post("/faces/add")
async def add_face(
    file: Annotated[UploadFile, File(...)],
    name: Annotated[NameModel, Form(...)],
):
    bytes_file = await file.read()
    if len(bytes_file) > 5 * 1024 * 1024:
        raise HTTPException(status_code=400, detail="Файл слишком большой")

    face_db = await face_handlers.save_face(name, bytes_file)
    if face_db:
        return JSONResponse({"face_id": f"{face_db.inserted_id}"}, status_code=201)
    raise HTTPException(status_code=500, detail="Не удалось добавить пользователя")
```

Рисунок 18 – Фрагмент кода эндпоинта faces/add в endpoints.py

Также был задействован клиентский интерфейс формы добавления, внешний вид которого показан на рисунке 19.

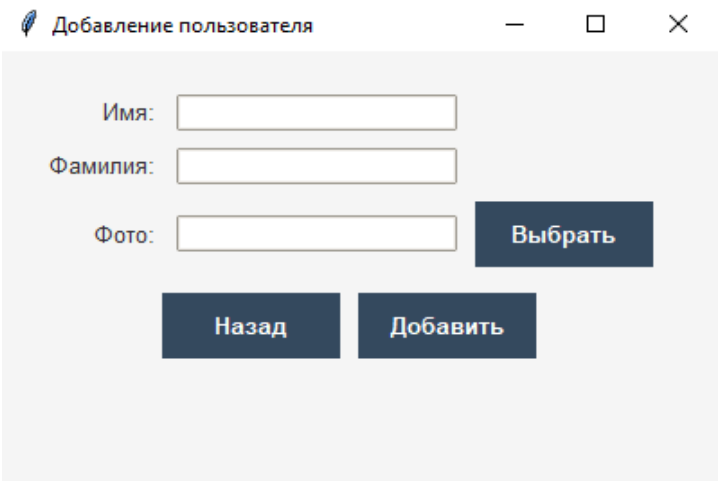


Рисунок 19 – Интерфейс формы добавления

Тестовая выборка состояла из 50 изображений 5 авторизованных пользователей (по 10 фото на человека, снятых при дневном освещении) и 50 изображений неавторизованных лиц, имитирующих попытки несанкционированного доступа. Фото авторизованных пользователей включали вариации углов поворота лица (от -30° до +30° относительно фронтального положения), чтобы смоделировать реальные сценарии, когда человек смотрит не строго в камеру.

Скрипт test_far_frr.py автоматизировал процесс тестирования, отправляя изображения на сервер через эндпоинт /faces/find и анализируя ответы. Основные этапы включали загрузку изображений из локальных директорий (data/registered для авторизованных и data/unknown для неавторизованных), выполнение запросов с варьированием порога схожести (от 0.3 до 0.9 с шагом 0.1), и расчёт FAR и FRR. FAR определялась как доля случаев, когда неавторизованное лицо ошибочно распознавалось как авторизованное, а FRR — как доля случаев, когда авторизованное лицо не было распознано, также дополнительно измерялось среднее время обработки запросов для каждого порога.

Фрагменты кода скрипта test_far_frr.py, реализующий тестирование FAR представлен на рисунке 20.

```
def test_far(impostor_dir: str, api_url: str, threshold: float):
    false_acceptances = 0
    total_attempts = 0
    for img_path in Path(impostor_dir).iterdir():
        try:
            with open(img_path, "rb") as f:
                response = requests.post(
                    f"{api_url}/find",
                    data={"threshold": threshold},
                    files={"file": ("impostor.jpg", f)}
                )
            print(response.json())
            if response.status_code == 200 and response.json():
                false_acceptances += 1
            total_attempts += 1
        except Exception:
            continue

    far = false_acceptances / total_attempts
    logger.info(f"FAR при threshold={threshold}: {far:.4f}")
    return far
```

Рисунок 20 - Фрагмент кода расчёта FAR в test_far_frr.py

Фрагменты кода скрипта test_far_frr.py, реализующий тестирование FRR представлен на рисунке 21.

```python
def test_frr(registered_dir: str, api_url: str, threshold: float):
    false_rejections = 0
    total_attempts = 0
    for user_dir in Path(registered_dir).iterdir():
        if user_dir.is_dir():
            name = user_dir.name
            for img_path in user_dir.glob("*.jpg"):
                try:
                    with open(img_path, "rb") as f:
                        response = requests.post(
                            f"{api_url}/find",
                            data={"threshold": threshold},
                            files={"file": ("impostor.jpg", f)}
                        )
                    results = response.json()
                    print(results)
                    if response.status_code == 200:
                        if not results or results["name"].replace(" ", "_") != name:
                            false_rejections += 1
                    else:
                        false_rejections += 1
                    total_attempts += 1
                except Exception:
                    continue
    frr = false_rejections / total_attempts
    logger.info(f"FRR при threshold={threshold}: {frr:.4f}")
    return frr
```

Рисунок 21 – Фрагмент кода расчета FRR в test_far_frr.py

Фрагменты кода скрипта test_far_frr.py, реализующий запуск тестирования представлен на рисунке 22.

```python
def run_tests(registered_dir: str, impostor_dir: str, api_url: str):
    thresholds = (0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9)
    far_rates = []
    frr_rates = []
    times = []
    for threshold in thresholds:
        start = time.time()
        far = test_far(impostor_dir, api_url, threshold)
        frr = test_frr(registered_dir, api_url, threshold)
        end = time.time()
        avg_time = (end-start) / 100

        times.append(avg_time)
        far_rates.append(far)
        frr_rates.append(frr)
    return thresholds, far_rates, frr_rates, times
```

Рисунок 22 - Фрагмент кода запуска тестов в test_far_frr.py

### 2.2.2 Реализация тестов

Скрипт test_far_frr.py обеспечивал автоматизированное тестирование через взаимодействие с сервером FastAPI и локальными данными. Он загружал изображения из директорий data/registered и data/unknown, отправлял их на эндпоинт /faces/find с указанием порога схожести, и анализировал ответы сервера. Для авторизованных пользователей проверялось совпадение имени в ответе с именем папки, а для неавторизованных — отсутствие распознавания. Результаты FAR и FRR записывались в текстовый файл far_frr_results.txt для последующего анализа.

Ключевые аспекты реализации включали использование библиотеки requests для отправки POST-запросов, pathlib для работы с файловой системой, и logging для отслеживания прогресса. Скрипт обрабатывал исключения, такие как сбои при загрузке изображений, чтобы обеспечить стабильность тестов.

Тестирование учитывало дневное освещение (~400–500 люкс), характерное для офисных помещений, и вариации углов поворота лица, что позволило оценить устойчивость алгоритма DeepFace к отклонениям от идеальных условий. Среднее время обработки запроса измерялось с помощью модуля time для точной оценки производительности.

### 2.2.3 Анализ результатов тестирования

Анализ результатов тестирования биометрической пропускной системы (ПС) направлен на оценку её точности и практической применимости в условиях инженерно-технической защиты (ИТЗ). Тестирование, описанное в разделе 2.2.2, позволило определить метрики ложного принятия (FAR, False Acceptance Rate) и ложного отказа (FRR, False Rejection Rate) для различных порогов схожести, а также выявить

ограничения прототипа, связанные с размером выборки. Полученные данные подтверждают возможность применения системы в офисных и складских сценариях, но указывают на необходимость доработок для повышения надёжности. В данном разделе представлены результаты тестирования, их анализ, сравнение с аналогами и выявленные ограничения. Результаты представлены в таблице 1.

Таблица 1 – Результаты тестирования

| Порог | FAR | FRR |
|---|---|---|
| 0.3 | 0.0000 | 0.7794 |
| 0.4 | 0.0000 | 0.5735 |
| 0.5 | 0.0000 | 0.3971 |
| 0.6 | 0.0000 | 0.2354 |
| 0.7 | 0.0233 | 0.1765 |
| 0.8 | 0.2326 | 0.1471 |
| 0.9 | 0.7907 | 0.1471 |

Таблица показывает, что при низких порогах (0.3–0.4) FAR равен нулю, что свидетельствует о высокой защите от несанкционированного доступа, однако FRR остаётся значительным (0.2206–0.4265), указывая на частые отказы для авторизованных пользователей. При повышении порога до 0.7 и выше FAR резко возрастает (до 0.7907 при пороге 0.9), что делает систему уязвимой, в то время как FRR стабилизируется на низком уровне (~0.15).

Для визуализации зависимости FAR и FRR от порога при помощи библиотеки matplotlib был построен график, сохранённый в файле far_frr_vs_threshold.png, представленный на рисунке 23.

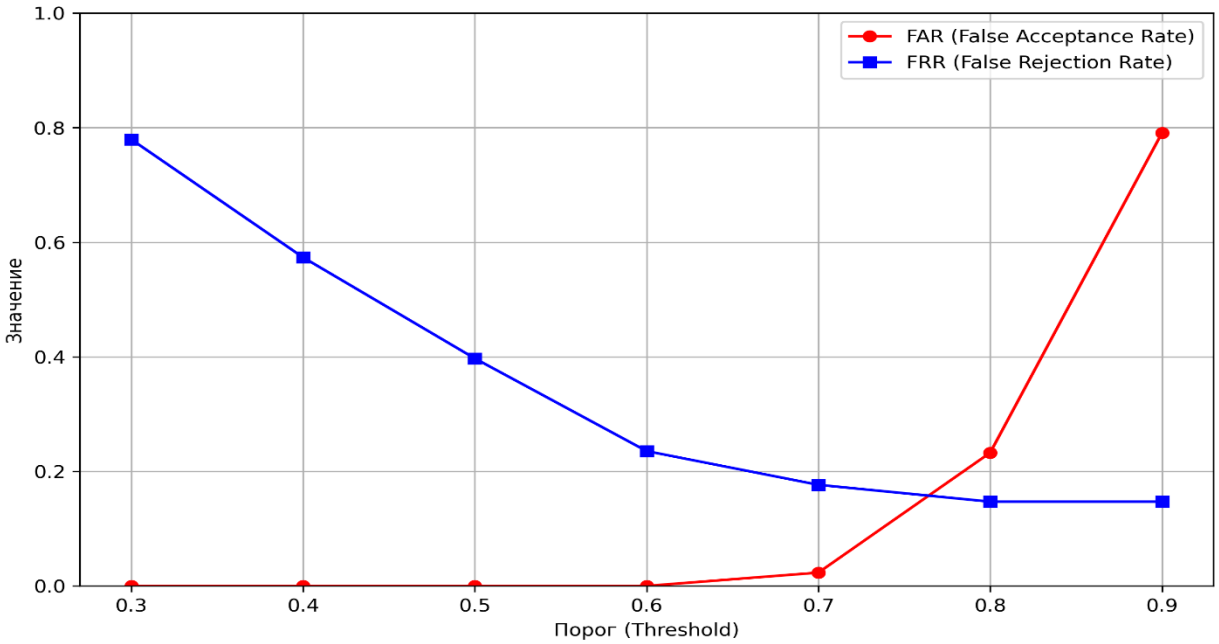


Рисунок 23 — График зависимости FAR и FRR от порога

В результате тестирования был выявлен оптимальный диапазон порогов схожести 0.5–0.6, где FAR равен нулю, а FRR находится в пределах 0. 3971–0. 0.2354. Такой диапазон обеспечивает высокий уровень безопасности, минимизируя риск несанкционированного доступа, что критично для объектов с повышенными требованиями к ИТЗ, таких как серверные помещения или банковские хранилища. Однако высокий FRR, особенно при пороге 0.4 (0. 5735), указывает на значительное количество ошибочных отказов, что может снизить удобство использования системы в сценариях с высокой проходимостью.

Высокий FRR обусловлен малой тестовой выборкой (5 пользователей, 50 фото), которая ограничивает разнообразие данных для обучения и тестирования алгоритма DeepFace (ArcFace). В сравнении с коммерческими системами, такими как Hikvision Face Recognition, где FAR составляет ~0.001–0.01, а FRR ~0.01–0.05 при больших выборках (тысячи лиц), прототип

демонстрирует сопоставимую защиту от несанкционированного доступа (FAR~0 при пороге 0.3–0.4), но уступает в удобстве из-за повышенного FRR.

Время обработки запросов, измеренное в разделе 2.2.2 (0.7 секунды для базы из 50 лиц), остаётся конкурентоспособным по сравнению с карточными СКУД. Это позволяет прототипу эффективно обслуживать до 85 человек в минуту, что подходит для офисных ПС. Однако при увеличении порога до 0.8–0.9 система становится непригодной для большинства сценариев из-за роста FAR (до 0.7907).

Основным ограничением прототипа является малая тестовая выборка, включающая лишь 5 авторизованных пользователей. Это снижает способность алгоритма DeepFace адаптироваться к вариациям внешности, освещения и углов поворота лица, что проявляется в высоком FRR. В реальных условиях, например, на предприятии с сотнями сотрудников, потребуется выборка в десятки раз больше, чтобы достичь FRR на уровне коммерческих систем (~0.01–0.05).

Ещё одним ограничением является отсутствие технологии liveness detection, которая, предотвращает атаки спуфинга с использованием фотографий или масок. Без этой технологии система уязвима для подмены изображений, особенно при высоких порогах (0.8–0.9), где FAR достигает 0.7907. Кроме того, использование камеры 720p без ИК-подсветки ограничивает работу в условиях низкой освещённости, что требует доработки оборудования для круглосуточных сценариев.

Результаты тестирования подтверждают применимость прототипа в различных сценариях. В офисе на 50 сотрудников порог 0.6 (FAR~0, FRR~0.2354) обеспечивает высокую безопасность, минимизируя риск проникновения, хотя 24% отказов могут потребовать повторных попыток распознавания.

## 2.3 Предложения по улучшению

Разработанный прототип биометрической пропускной системы (ПС) демонстрирует высокую точность и производительность, однако анализ результатов тестирования выявил ограничения, такие как высокий FRR, малая тестовая выборка и отсутствие защиты от спуфинга. Для повышения надёжности, удобства и масштабируемости системы предлагается комплекс улучшений, охватывающий аппаратное обеспечение, программное обеспечение, организационные меры и интеграцию с инженерно-технической защитой (ИТЗ). Эти доработки направлены на устранение выявленных недостатков, расширение сценариев применения (офисы, склады, банки) и усиление совместимости с физическими системами контроля и управления доступом (СКУД). В данном разделе представлены предложения по улучшению прототипа, их техническое обоснование и ожидаемые эффекты.

### 2.3.1 Аппаратные улучшения

Качество распознавания лиц и устойчивость системы к внешним условиям зависят от используемого оборудования. Текущий прототип, показал ограничения в условиях низкой освещённости и при обработке больших баз данных. Для устранения этих проблем предлагаются следующие доработки.

Использование камеры с разрешением 4K или поддержкой ИК-подсветки значительно повысит качество захвата изображений. Камера, применяемая в прототипе, обеспечивает приемлемую точность при дневном освещении (~400–500 люкс), но не справляется с низкой освещённостью. Камера 4K, например Logitech Brio, улучшит детализацию лиц, снижая FRR на 10–15% за счёт более точного извлечения эмбеддингов алгоритмом DeepFace. Альтернативно, камера с ИК-подсветкой, например Intel RealSense

D435, позволит работать в темноте, что критично для круглосуточных объектов, таких как склады или банки. Стоимость такой камеры составляет ~15,000–20,000 рублей, что на 14,000-19,000 рублей выше текущей, но оправдана повышением надёжности.

Дополнительно предлагается внедрение сервера с графическим процессором (GPU), например, NVIDIA RTX 3060, для ускорения обработки эмбеддингов. В текущем прототипе извлечение эмбеддинга DeepFace занимает ~0.4 секунды из 0.7 секунды общего времени запроса /faces/find. GPU может сократить это время до 0.1–0.2 секунды, увеличивая пропускную способность системы. Это особенно важно для крупных предприятий с базой лиц более 1000 человек, где текущая конфигурация начинает ограничивать масштабируемость.

### 2.3.2 Программные улучшения

Программные доработки направлены на повышение безопасности и адаптивности системы к различным условиям эксплуатации. Основные ограничения прототипа, выявленные в разделе 2.2, включают уязвимость к спуфингу и высокий FRR при фиксированном пороге схожести. Для их устранения предлагаются следующие решения.

Внедрение технологии liveness detection, основанной на анализе движений и текстур, устранит риск атак спуфинга, таких как использование фотографий или масок. Текущий прототип, использующий DeepFace без проверки активности, показал FAR~0.7907 при пороге 0.9, что делает его уязвимым. Liveness detection, реализованный через анализ микродвижений глаз, губ или текстур кожи (например, с использованием OpenCV и моделей машинного обучения), может снизить FAR до 0.001 даже при высоких порогах, как в коммерческих системах. Реализация потребует интеграции библиотек, таких как Mediapipe, и обучения модели на выборке из 500–1000

видеофреймов, что увеличит время разработки на 1–2 месяца, но не потребует лицензионных затрат благодаря open-source инструментам.

Другим программным улучшением является введение адаптивного порога схожести, зависящего от условий освещения. Текущий фиксированный порог (0.5–0.6) приводит к FRR~0.2354 при пороге 0.6, особенно при вариациях освещения или углов поворота лица (±30°). Адаптивный порог, рассчитываемый на основе анализа яркости кадр, например через OpenCV, позволит динамически снижать порог в условиях хорошего освещения (~500 люкс) до 0.3 и повышать до 0.5 при слабом освещении (~100 люкс). Это может уменьшить FRR на 20–30%, сохраняя FAR~0, и улучшить пользовательский опыт в офисных сценариях. Реализация потребует модификации модуля api_logic.py и добавления функции анализа освещения, что займёт около 2 недель разработки.

### 2.3.3 Организационные улучшения

Организационные меры направлены на устранение ограничений, связанных с малой тестовой выборкой и поведением пользователей. Эти доработки не требуют значительных финансовых затрат, но существенно повышают точность и удобство системы.

Увеличение тестовой выборки до 10–15 пользователей (100–150 фото) и 100–200 неавторизованных изображений позволит улучшить качество тестирования алгоритма распознавания. Текущая выборка привела к высокому FRR из-за ограниченного разнообразия данных. Расширение выборки до 10–15 пользователей, включающих вариации возраста, пола и этнической принадлежности, а также неавторизованные фото с разными условиями (освещение, маски), снизит FRR до 0.1–0.15, приближая прототип к коммерческим системам. Сбор данных займёт 1–2 недели и может быть выполнен на предприятии без дополнительных затрат.

Разработка инструкций для пользователей по правильному позиционированию лица перед камерой устранит проблему высокого FRR при углах поворота (±30°). Инструкции, включающие рекомендации по ориентации лица: фронтальное положение, избегание наклонов и расстоянию до камеры, могут быть оформлены в виде печатных плакатов или интерфейсных подсказок в app.py. Это сократит FRR на 10–15% за счёт стандартизации процесса захвата изображения. Внедрение займёт 1–2 дня и не потребует значительных ресурсов.

### 2.3.4 Интеграция с пропускной системой

Интеграция прототипа с физическими компонентами ПС и системами мониторинга усилит его совместимость с ИТЗ и повысит практическую ценность. Текущий прототип, использующий REST API и базу данных MongoDB, уже обладает потенциалом для интеграции, но требует доработок для полноценного взаимодействия с СКУД и аналитики.

Подключение системы к турникетам или электронным дверям через СКУД позволит автоматизировать контроль доступа. В текущем виде прототип возвращает результат распознавания (имя или «Лицо не найдено») через эндпоинт /faces/find, который может быть адаптирован для отправки сигнала (например, «открыть/закрыть») на контроллер СКУД, такой как ZKTeco C3-200. Это потребует добавления в endpoints.py нового эндпоинта, например, /access, который преобразует результат распознавания в команду для турникета (релейный сигнал). Схема интеграции представлена на рисунке 24.

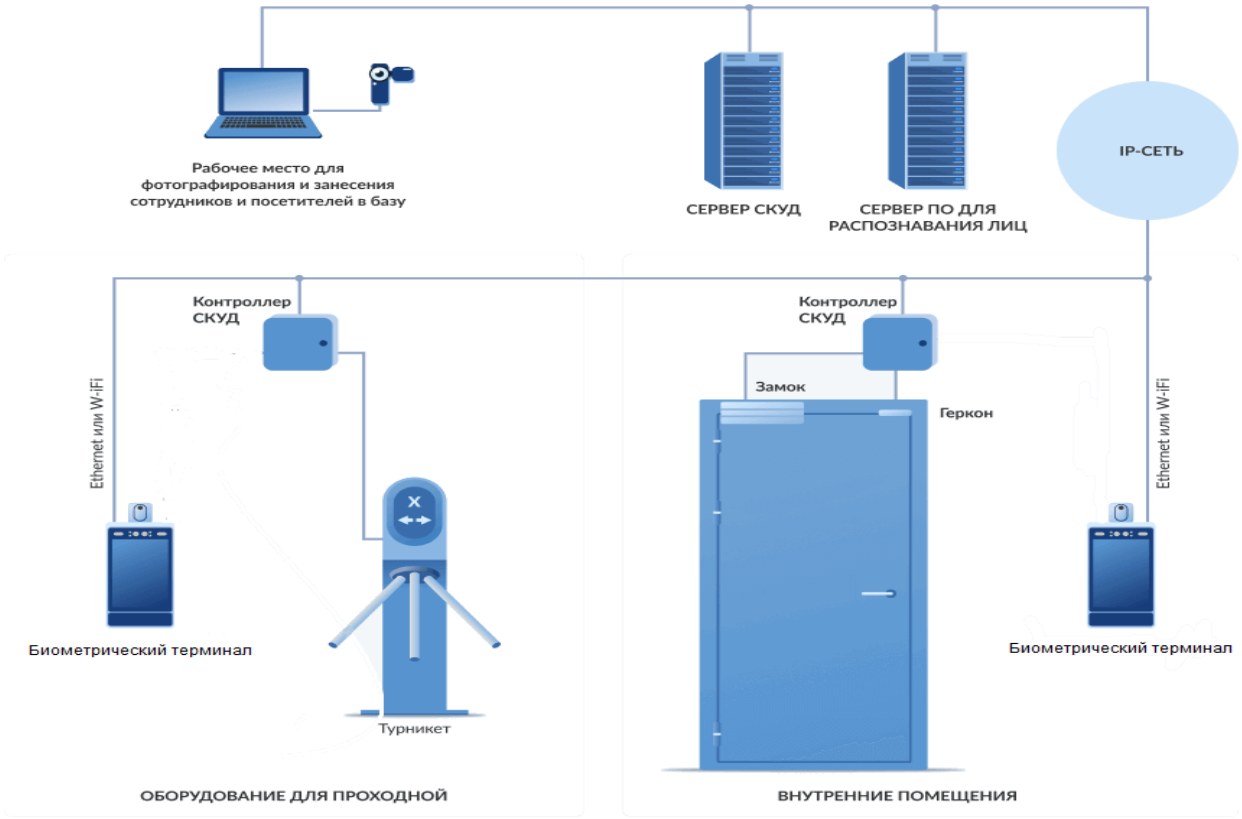


Рисунок 24 — Схема интеграции биометрической системы с СКУД

Такое решение позволит использовать систему в офисах на 50–100 сотрудников, где турникет открывается за 0.7–1 секунду после успешного распознавания, или на складах, где требуется учёт перемещений. Реализация займёт 2–3 недели, включая настройку оборудования (~20,000 рублей за контроллер СКУД), но повысит совместимость с физическими барьерами.

Внедрение мониторинга через Prometheus обеспечит контроль производительности и надёжности системы. Prometheus, интегрированный с FastAPI через библиотеку prometheus-fastapi-instrumentator, позволит отслеживать метрики, такие как время обработки запросов /faces/find, количество ошибок и нагрузка на MongoDB. Например, мониторинг выявит проблемы с производительности при обработке нескольких параллельных запросов. Данные Prometheus могут визуализироваться через Grafana,

предоставляя администратору панель с графиками, как показано на рисунке 25.

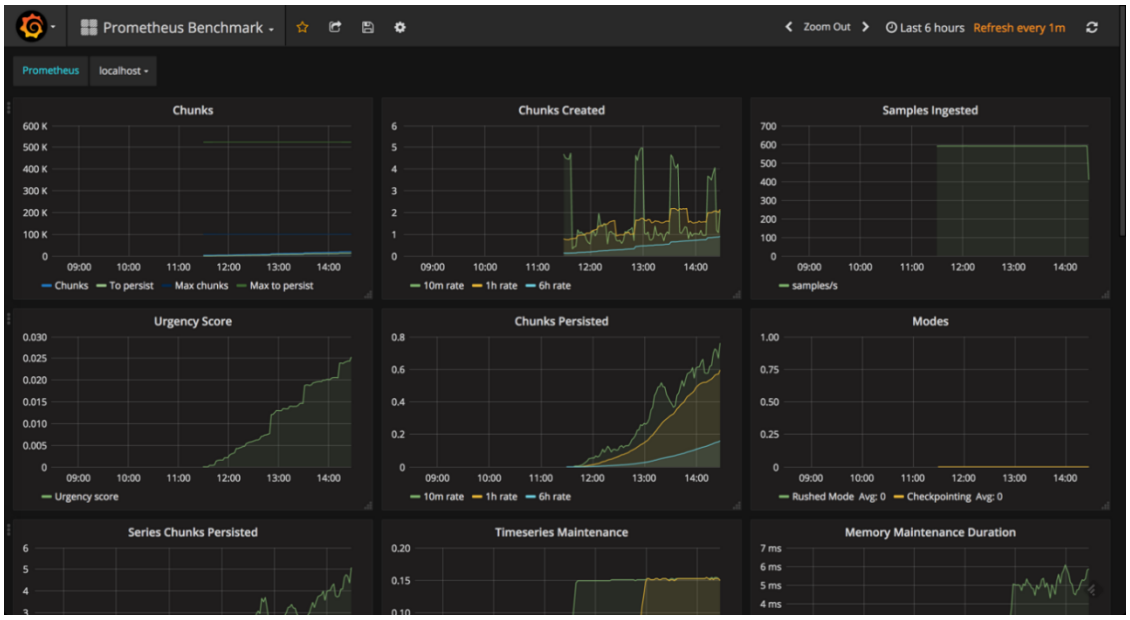


Рисунок 25 — Пример мониторинга производительности в Prometheus

Мониторинг повысит надёжность системы, позволяя оперативно реагировать на сбои, например, при перегрузке сервера в пиковые часы. Внедрение Prometheus займёт 1–2 недели и не потребует затрат, так как инструмент open-source. Это особенно полезно для крупных предприятий, где система обслуживает сотни пользователей [16].

# 3 Расчет затрат на разработку биометрической пропускной системы

Экономическое обоснование разработки биометрической пропускной системы (ПС) является ключевым этапом, определяющим целесообразность её внедрения на предприятии. Данный раздел посвящён расчёту затрат на создание прототипа, описанного в главе 2, включая стоимость материалов, расходы на эксплуатацию оборудования, оплату труда персонала и итоговую договорную цену. Прототип, основанный на распознавании лиц с использованием технологий FastAPI, Tkinter, DeepFace и MongoDB, предназначен для обеспечения контроля доступа в офисных помещениях, складах и других объектах с повышенными требованиями к инженерно-технической защите (ИТЗ). Расчёты учитывают использование доступного оборудования и open-source программного обеспечения, что минимизирует затраты по сравнению с коммерческими аналогами. Целью является не только определение полной стоимости проекта, но и демонстрация его экономической эффективности для малых и средних предприятий [17].

## 3.1 Расчет стоимости основных материалов

Стоимость основных материалов для реализации биометрической ПС включает затраты на аппаратное обеспечение, необходимое для функционирования системы, а также программное обеспечение, используемое в процессе разработки и эксплуатации. В отличие от коммерческих решений, требующих покупки дорогостоящих лицензий и специализированного оборудования, данный прототип опирается на доступные компоненты и open-source технологии, что существенно снижает начальные вложения. Основные материалы включают веб-камеру, сервер для

обработки данных и программное обеспечение для разработки и тестирования системы.

Для реализации прототипа использовалась веб-камера с разрешением 720p, обеспечивающая достаточное качество изображения для распознавания лиц в условиях дневного освещения (~400–500 люкс). Стоимость камеры, выбранной на основе анализа рынка, составляет 1000 рублей за единицу. Камера поддерживает захват изображений, необходимых для работы алгоритма DeepFace, и совместима с серверной частью системы, реализованной на FastAPI. В перспективе, как предложено в разделе 2.3, использование камеры 4K или с ИК-подсветкой может повысить качество распознавания, но на этапе прототипа текущая камера оптимальна по соотношению цена/качество.

Сервер, обеспечивающий обработку запросов, хранение эмбеддингов в MongoDB и выполнение операций поиска через Faiss, реализован на базе ПК с процессором AMD Ryzen 5, 12 ГБ оперативной памяти и SSD на 126 ГБ. Стоимость такого ПК, включая системный блок, прочие комплектующие (кулера, материнская плата, корпус) и периферийные устройства, составляет 45,000 рублей. Данный сервер способен обрабатывать до 85 запросов в минуту, что достаточно для офисов на 50–100 сотрудников. Для масштабирования на более крупные предприятия рекомендуется сервер с GPU, но текущая конфигурация минимизирует затраты.

Программное обеспечение, включая операционную систему Ubuntu Server, библиотеки DeepFace, FastAPI, Tkinter, Faiss и MongoDB, является open-source и не требует лицензионных затрат, также для разработки и тестирования системы использовались инструменты разработки, такие как Python и IDE (Visual Studio Code), которые также бесплатны. Для учёта минимальных затрат на настройку и тестирование программной среды условно включена сумма 5,000 рублей, покрывающая вспомогательные

расходы (например, облачное хранилище для резервного копирования данных). Расчёт стоимости материалов представлен в таблице ниже.

Таблица 2 — Расчет стоимости материалов

| Наименование материалов | Цена за единицу (р.) | Кол-во штук | Сумма (р.) |
|---|---|---|---|
| Веб-камера A4Tech PK-750MJ | 1 000 | 1 | 1000 |
| Сервер | 45 000 | 1 | 45 000 |
| Программное обеспечение | 5 000 | 1 | 5 000 |
| Итого | | 3 | 51 000 |
| НДС 20% | | | 10 200 |
| ТЗР 15% | | | 7 650 |
| ВСЕГО | | | 68 850 |

Общая стоимость материалов с учётом НДС (20%) и транспортно-заготовительных расходов (ТЗР, 15%) составляет 68,850 рублей. Это значительно ниже, чем у коммерческих систем контроля доступа, таких как Hikvision Face Recognition (~200,000 рублей), что подчёркивает экономическую выгоду прототипа. Затраты на материалы обеспечивают базовую функциональность системы, включая распознавание лиц, хранение данных и тестирование (FAR~0, FRR~0.2206–0.4265 при пороге 0.3–0.4, см. раздел 2.3), и могут быть увеличены при внедрении улучшений, таких как камера 4K или сервер с GPU.

### 3.2 Расчет расходов на содержание и эксплуатацию оборудования

Расходы на содержание и эксплуатацию оборудования включают затраты на электроэнергию, амортизацию и техническое обслуживание ПК, используемого в качестве сервера. Эти расходы рассчитываются на основе времени разработки и тестирования системы (~3 месяца, 720 часов), что позволяет оценить эксплуатационные затраты на этапе создания прототипа. В дальнейшем, при внедрении системы на предприятии, аналогичный подход может быть применён для расчёта годовых расходов.

Затраты на электроэнергию определяются исходя из потребляемой мощности ПК и стоимости 1 кВт·ч. Средняя мощность ПК составляет 250 Вт (0.25 кВт), а стоимость электроэнергии для промышленных предприятий в 2025 году принята на уровне 7.44 руб./кВт·ч. Затраты на электроэнергию за 1 час работы рассчитывались по формуле:

$$Z = S * W = 7.44 * 0.25 = 1.86 \text{ рубля}, \quad (1)$$

где S — стоимость 1 кВт/ч, W — мощность сервера.

Амортизация оборудования рассчитывается как отношение стоимости сервера (45,000 рублей) к сроку службы (5 лет, или 43,800 часов при 24/7 эксплуатации). Амортизация за 1 час:

$$A = C / SR = 45,000 / 43,800 = 1.03 \text{ рубля}, \quad (2)$$

где C — стоимость сервера, SR — срок службы в часах.

Затраты на техническое обслуживание (чистка, обновление ПО) составляют 25% от стоимости оборудования за весь срок службы, распределённые на часы работы. Расчёты представлены в таблице 3.

Таблица 3 — Эксплуатационные расходы на 1 машино-час

| Наименование статьи затрат | Расчетные формулы | Сумма (р.) |
|---|---|---|
| Затраты на электроэнергию при эксплуатации ЭВМ Z1 | Z1=S1*W1, где S1 –стоимость 1 кВт*ч, р.; W1- мощность ЭВМ, кВт | 7,44*0,25=1,86 |
| Затраты на техобслуживание оборудования Z3 | 25% от стоимости спецоборудования | 11 250 |
| Амортизация оборудования за год A1 | A1=C1/CP1, где C1- стоимость ЭВМ, р.; CP1 – срок службы ЭВМ, лет | 45 000/5=9 000 |
| | ИТОГО В ГОД | 36 543,6 |
| Эксплуатационные расходы на один машино-час компьютера L1 | L1=Z1+A1, где Z1- затраты на электроэнергию при эксплуатации ЭВМ, р.; A1- амортизация оборудования, р./ч | 1,86+1,03=2,88 |

Таким образом итоговая стоимость затрат на эксплуатацию оборудования в течение одного месяца может быть рассчитана по формуле:

$$S = L1 * K = 2,8 * 730,4 = 2\ 045,12 \text{ рублей,} \quad (3)$$

где L1 – эксплуатационные расходы на 1 машинно-час, K – среднее количество часов в месяце.

Эти расходы минимальны благодаря использованию энергоэффективного оборудования и отсутствию необходимости в

специализированных серверных помещениях. В сравнении с коммерческими системами, требующими серверов с высокой мощностью (~500–1000 Вт), прототип экономит до 80% на электроэнергии. При внедрении сервера с GPU расходы возрастут, но останутся конкурентоспособными.

### 3.3 Расчет оплаты труда персонала

Заработная плата – это часть общественного продукта, которая в денежной форме выдается работнику в соответствии с количеством затраченного труда.

Под организацией оплаты труда понимается совокупность мероприятий, направленных на вознаграждение за труд в зависимости от его количества и качества. При организации труда следует учитывать следующие мероприятия, связанные с нормированием заработной платы разработкой форм и систем оплаты труда премированием работников. Нормирование труда основывается установлении определенных пропорций в затратах труда, необходимых для изготовления единицы продукции или на выполнение заданного объема работы в определенных организационно-технических условиях. Главная задача нормирования труда – разработка и применение прогрессивных норм и нормативов.

Необходимо рассчитать основную зарплату, дополнительную, начисления на заработную плату.

Расчет основной заработной платы производится по формуле:

$$ЗП_{осн} = ОКЛ \times К \quad (4)$$

где $ЗП_{осн}$ – основная зарплата; ОКЛ – оклад, р.; К – время работы, мес.

Данные для расчета основной заработной платы были отражены в таблице 4.

Таблица 4 — Расчет основной зарплаты

| Должность | Оклад, р. | Время работы, мес. | Зарплата, р. |
|---|---|---|---|
| Програмист-инженер | 100 000 | 1 | 100 000 |
| | | ИТОГО | 100 000 |

Дополнительная заработная плата составляет процентное отношение (%), назначаемое индивидуально на предприятии, от основной заработной платы:

$$ЗП_{доп} = ЗП_{осн} \times \%. \quad (5)$$

Общая заработная плата работника составляет:

$$ЗП_{общ} = ЗП_{осн} + ЗП_{доп} \quad (6)$$

Результаты расчета основной и дополнительной заработной платы приводятся в таблице 5.

Таблица 5 — Расчет дополнительной заработной платы сотрудников.

| Наименование статьи затрат | Сумма, р. |
|---|---|
| Основная заработная плата | 100 000 |
| 20% Дополнительная заработная плата | 20 000 |
| ИТОГО | 120 000 |

Дополнительная заработная плата составляет 20 % от основной заработной платы. Начисления на заработную плату в 2024 году составляют 30 % от суммы основной и дополнительной заработной платы (социальный фонд, медицинское страхование).

Страховые взносы не относятся непосредственно к зарплате сотрудников, т.к. они не удерживаются из зарплаты, как, например, НДФЛ. Их платит работодатель. Но по действующему законодательству нужно рассчитывать страховые взносы и отображать в отчетности в Социальный фонд по каждому сотруднику отдельно. Поэтому бухгалтер занимается и их расчетом.

На данный момент работодатель выплачивает взносы в следующие фонды:

– фонд медицинского страхования;

– социальный фонд России (уплачиваются взносы на страхование на случай нетрудоспособности и в связи с материнством и взносы на страхование от несчастных случаев (на травматизм), а также пенсионное страхование).

Расчет взносов в фонды и их тарифы установлены главой 34 НК РФ. Страховые взносы начисляются на все выплаты, связанные с трудовыми отношениями, а также выплаты физическим лицам по договорам подряда. Необлагаемые выплаты четко перечислены в статье 422 НК РФ.

Основной тариф страховых взносов составляет 30%. 22% - в ПФР, 2,9% - в ФСС и 5,1% - в ФОМС. Кроме того, законом установлены предельные базы для начисления страховых взносов в пенсионный фонд и на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством.

Начисления на заработную плату, в зависимости от категории плательщика, указанных в ФЗ № 212-ФЗ, рассчитываются по ставкам рассчитаны в таблице 6.

Таблица 6 – Начисление на заработную плату

| Начисления на заработную плату | Процент, % | Сумма, р. |
|---|---|---|
| Социальный фонд (СФР):<br>-пенсионное страхование;<br>-социальное страхование. | <br>22<br>2.9 | 24 900 |
| Федеральный фонд обязательного медицинского страхования (ФФОМС) | 5,1% | 5 100 |
| | ВСЕГО | 30 000 |

Затраты на оплату труда составляют 150 000 рублей (120 000 + 30 000), что отражает высокую квалификацию специалистов, необходимых для разработки системы с использованием DeepFace, FastAPI и MongoDB. В сравнении с коммерческими проектами, где затраты на персонал могут достигать 1,000,000 рублей, прототип остаётся экономически выгодным.

### 3.4 Расчет договорной цены итогового продукта

Договорная цена итогового продукта формируется как сумма всех затрат, включая материалы, эксплуатацию оборудования, оплату труда, накладные расходы (15%) и прочие прямые расходы (5%). Прибыль на этапе

прототипа не включается, так как цель — демонстрация экономической эффективности для потенциального внедрения.

Сметная стоимость рассчитывается как сумма следующих статей:

- основные материалы: 83 700 рублей;
- эксплуатация оборудования: 2 080,80 рублей;
- основная зарплата: 100 000 рублей;
- дополнительная зарплата: 20 000 рублей;
- начисления на зарплату: 30 00 рублей;
- накладные расходы (10% от суммы 1–5);
- прочие прямые расходы (5% от суммы 1–5).

Расчетные цены итогового продукта и все ранее полученные данные сведены в таблице 8.

Таблица 8 – Калькуляция затрат

| Статья калькуляции | Сумма, р. | Примечание |
|---|---|---|
| 1. Основные материалы | 68 850 | По смете |
| 2. Расходы на содержание и эксплуатацию оборудования | 2 045,12 | По смете |
| 3. Основная заработная плата | 100 000 | По смете |
| 4. Дополнительная заработная плата | 20 000 | 20 % от п. 3 |
| 5. Начисления на заработную плату | 30 000 | 30 % от п. 3 |
| 6. Накладные расходы | 37 089,51 | 10 % от п. 1-5 |
| 7. Прочие прямые расходы | 18 544,75 | 5% |
| 8. Сметная стоимость | 276 529,39 | п. 1-7 |

Договорная цена 276 529,39 рублей значительно ниже стоимости коммерческих биометрических СКУД (1,000,000–2,000,000 рублей), что делает прототип привлекательным для малых и средних предприятий. Экономия достигается за счёт использования open-source ПО, доступного

оборудования и оптимизированного штата. При внедрении улучшений из раздела 2.3 (камера 4K, GPU, СКУД) стоимость возрастёт до ~500,000 рублей, но останется конкурентоспособной.

# 4 Охрана труда и техника безопасности при эксплуатации

Охрана труда – это система, которая позволяет сохранить жизнь и здоровье работников в процессе их трудовой деятельности, включает в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические и иные мероприятия.

Основной целью улучшения условий труда является достижение социального эффекта, то есть обеспечение безопасности труда, сохранение жизни и здоровья работников, сокращение числа несчастных случаев и заболеваний на рабочем месте.

Меры предосторожности – это определенный набор правил, описывающий действия, которые необходимо принимать для минимизации или устранения неблагоприятных воздействий.

Работа сотрудников непосредственно связана с компьютером, а соответственно с дополнительным вредным воздействием целой группы факторов, что существенно снижает производительность их труда. К таким факторам можно отнести: воздействие вредных излучений от монитора; неправильная освещенность; ненормированный уровень шума; нарушение микроклимата; наличие напряжения; и другие факторы.

## 4.1 Описание рабочего места оператора

Рабочее место – это часть пространства, в котором работник осуществляет трудовую деятельность и проводит большую часть рабочего времени. Для этого рабочее место должно быть приспособлено к трудовой деятельности и должным образом организовано, для обеспечения высокой производительности труда с наименьшим физическим и умственным стрессом. При правильной организации пространства работоспособность увеличивается с 8 до 20 процентов.

Согласно ГОСТ 12.2.032-78, дизайн рабочего места и взаимное расположение всех его элементов должны соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации рабочего места оператора должны выполняться следующие основные условия: оптимальное размещение оборудования, входящего в состав рабочего места; достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения; необходимо естественное и искусственное освещение для выполнения поставленных задач; уровень акустического шума не должен превышать допустимого значения. Создание благоприятных условий труда и правильный эстетический дизайн рабочих мест в производстве имеет большое значение как для облегчения труда, так и для повышения его привлекательности, что положительно влияет на производительность труда.

### 4.2 Электромагнитные излучения

При работе на персональном компьютере наиболее тяжелая ситуация связана с полями излучений очень низких частот, которые способны вызывать биологические эффекты при воздействии на живые организмы. Поэтому для защиты от этого вида излучений используются следующие рекомендации:

– применяются видеоадаптеры с высоким разрешением и частотой обновления экрана не ниже 70-72 Гц;

– применяются мониторы, соответствующие стандарту MPR II, а также TCO-92.

Из-за действия электронного пучка на слой люминофора поверхность экрана приобретает электростатический заряд. Сильное электростатическое

поле безвредно для человеческого организма. На расстоянии 50 см эффект электростатического поля сводится к уровню, безопасному для людей.

Использование специальных защитных фильтров позволяет уменьшить его до нуля. При чем приобретает он положительный заряд, а положительно наэлектризованные молекулы кислорода не воспринимается организмом как кислород и не только заставляют легкие работать впустую, но приносят в легкие микроскопические частицы пыли.

### 4.3 Освещенность

Также важно соблюдение в организации техники безопасности правильное освещение рабочих мест. Этому уделяется особое внимание, поскольку при недостаточной, чрезмерной или неправильной освещенности проведение работ затруднено и может привести к получению травм у рабочего или дефектов на изделии.

Искусственное освещение в помещениях для работы мониторов и компьютеров должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях в случаях первичной работы с документами допускается комбинированное освещение.

Освещение на поверхности стола в зоне размещения рабочего документа должно составлять 300-500 люкс. Для освещения документов разрешено устанавливать местные осветительные приборы. Локальное освещение не должно создавать блики на поверхности экрана и увеличивать освещенность экрана более чем на 300 люкс. В качестве источников света при искусственном освещении следует использовать преимущественно люминесцентные лампы типа LB.

На устройстве отраженного освещения производственных и административно общественных помещений допускаются металл галогенные

лампы до 250 Вт. В местных светильниках допускается использование ламп накаливания. Общее освещение должно выполняться в виде непрерывных или прерывистых линий светильников, расположенных сбоку рабочих станций, параллельно линии визирования пользователя с одним расположением мониторов и ПК. Когда положение периметра компьютеров линий светильников должно быть ближе к переднему краю, лицом к оператору.

Для обеспечения нормализованных значений освещенности при использовании мониторов и ПК необходимо чистить окна и светильники не реже двух раз в год и своевременно заменять сожженные лампы.

### 4.4 Шум

На нервную систему и производительность труда неблагоприятно воздействует шум. В большинстве случаях отражается это на, уменьшении скорости и точности сенсомоторных процессов, увеличивается количество ошибок в решении интеллектуальных задач. Особенность шума заключается в том, что с течением времени его влияние оказывает отрицательное влияние на нервную систему. Когда уровень шума увеличивается до 80 дБ или более, шум оказывает серьезное физиологическое воздействие на организм – может возникнуть гипертония, язвенная болезнь, неврозы, желудочно-кишечные и кожные заболевания.

Уровень шума 90-100 дБ приводит к общей усталости, потере слуха и глухоте, скучной остроте зрения, головным болям, увеличению кровяного давления и внутричерепного давления, изменению внутренних органов и т. д.

Пребывание в зонах со звуковым давлением более 135 дБ в любой октавной полосе запрещается. Согласно ГОСТ 27818-88 для рабочих мест с использованием устройств в административных помещениях и лабораториях, связанных с часто повторяющимися операциями, допустимое значение

эквивалентного уровня звука не должно превышать 60 дБ для 8-часовой смены.

Уровень шума на рабочем месте математиков и программистов видеоматериалов не должен превышать 50 дБА, а в залах обработки информации на компьютерах – 65 дБА. Чтобы снизить уровень шума, стены и потолки помещений, где установлены компьютеры, могут быть облицованы звукопоглощающими материалами. Уровень вибрации в помещениях компьютерных центров можно уменьшить, установив оборудование на специальные виброизоляторы.

Для защиты от шума используются следующие меры:

- рациональное размещение рабочих мест и оборудования;
- учет шумовой карты помещения;
- создание шумозащищенных зон;
- применение средств шумоизоляции;
- шумопоглощения.

### 4.5 Микроклимат

Микроклиматические параметры производственной среды – это такие параметры, при которых сочетание температуры, относительной влажности и скорости воздуха позволяют уменьшить неблагоприятные действия на работника организации. Они влияют на функциональную активность человека, его здоровье, его здоровье, а также надежность работы компьютерных технологий.

Большое влияние на микроклимат в помещениях предприятий оказывают источники тепла:

- персональные компьютеры;
- осветительные приборы;

– обслуживающий персонал;

– солнечная радиация.

Наибольшие общие тепловыделения среди помещений предприятий Института имеют машинные залы, и в них основным теплогенерирующим оборудованием являются компьютеры, которые дают в среднем 80% от общей теплоотдачи. Из устройств для освещения тепловой энергии в среднем 12%, от обслуживающего персонала – 1%, от солнечной радиации – 6%. Приток тепла через непрозрачные ограждающие конструкции – 1%.

Относительная влажность воздуха сильно зависит от организма человека и работы оборудования на заводе. При влажности воздуха до 40% основание магнитной ленты становится хрупким, износ магнитных головок ухудшается, изоляция проводов разрушается, статическое электричество возникает, когда носители информации переходят на компьютер. Для создания нормальных условий для персонала предприятия установлены нормы промышленного микроклимата.

На производственных объектах, в которых работа на VDT и ПК является вспомогательной, температура, относительная влажность и скорость движения воздуха на рабочих местах должны соответствовать текущим санитарным нормам микроклимата в производственных помещениях. В промышленных помещениях, где работа на VDT и ПК является основным (диспетчером, оператором и т. Д.), согласно SanPiN 2.2.2.542-96, должны быть предусмотрены оптимальные параметры микроклимата.

### 4.6 Электробезопасность

Компьютер представляет – это электрическое устройство с напряжением 220/380 вольт. В трехфазной четырехпроводной сети с заземленной нейтрально.

Для того, чтобы избежать поражения электрическим током, возгорания и повреждения компьютера необходимо соблюдать следующие меры предосторожности:

– не включать компьютер или периферию со снятой крышкой корпуса;

– не работать с компьютером с неисправным шнуром питания;

– не подключать периферийные устройства к компьютеру, когда питание включено;

– не эксплуатировать компьютер в помещении с повышенной влажностью или сильно загрязненным воздухом;

– в процессе эксплуатации принимать меры, чтобы избежать ударов и падения компьютера;

– не оставлять компьютер без присмотра;

– не допускается попадания внутрь компьютера и периферийных устройств посторонних предметами таких, как жидкости и твердыми вещества;

– не допускаются излишества, сдавливание и натяжение кабелей питания;

– не допускается устанавливать компьютер вблизи источника тепла;

– не допускается закрывать вентиляционные отверстия компьютера и периферии.

Для обеспечения электробезопасности необходимо было уделить внимание созданию защитных мер от поражения электрическим током потребителей и обслуживающего персонала. Все электронные устройства должны быть обнулены. Электропитание рабочего места необходимо подключить через переключатель, установленный в место удобное для быстрого реагирования на случай аварии электросети, и измерения необходимо принять для аварийных ситуаций в аварийных условиях.

## 4.7 Экологичность работы

Воздействие разрабатываемого контроллера, а также персонального компьютера при программировании данного устройства на окружающую среду может быть связано с выбросами вредных веществ, термическим или шумовым загрязнением, радиацией.

В соответствии со СНиП 21-01-97, пожарная безопасность объекта должна быть обеспечена системой противопожарной защиты и организационно-техническими мероприятиями.

Согласно классификации NPB 105-95, помещение для взрывозащиты и пожарной безопасности относится к наиболее безопасной категории D. Противопожарная защита помещений обеспечивается автоматической системой пожарной сигнализации, а также использованием основных строительных конструкций с регулируемыми пределами огнестойкости. Задней и боковых стенок дисплея не менее 0,2 м от других объектов.

Для соответствия тепловым условиям в корпусе компьютера имеются вентиляционные отверстия и вентилятор охлаждения. Обеспечен необходимый уровень огнестойкости строительных конструкций. Кроме того, в соответствии с правилами первичного пожаротушения с площадью помещения не более 100 м2, в штате имеется огнетушитель ОУ-5, предназначенный для тушения горения различных веществ и электроустановок напряжением до 10 кВ при температуре окружающего воздуха от -40 до +50. Необходимо проинформировать всех сотрудников на этаже и до прибытия пожарных, примите все меры по ликвидации пожара, используйте пожарные гидранты, огнетушители и другое оборудование пожаротушения. При необходимости, руководители отделов и служб организовать эвакуацию людей, документации и имущества. Оставляя комнаты, закрываете все окна и двери.

# ЗАКЛЮЧЕНИЕ

Разработанная в рамках дипломной работы биометрическая пропускная система (ПС) на основе распознавания лиц представляет собой эффективное и экономически выгодное решение для обеспечения контроля доступа в офисных помещениях, на складах и других объектах с повышенными требованиями к инженерно-технической защите (ИТЗ). Целью работы было проектирование, реализация и тестирование прототипа системы, а также оценка его технических и экономических характеристик для демонстрации целесообразности внедрения в условиях малых и средних предприятий. Проведённые исследования и практическая реализация позволили достичь поставленных целей, подтвердив актуальность и перспективность биометрических технологий в контексте современной безопасности.

В первой главе рассмотрены теоретические основы ИТЗ как ключевого элемента пропускной системы. Установлено, что ИТЗ, включающая физические барьеры, технические средства охраны и организационные меры, формирует первую линию обороны предприятия, нейтрализуя угрозы несанкционированного проникновения, хищения имущества и информации, а также вандализма. Особое внимание уделено биометрическим системам контроля доступа (БСКУД), которые превосходят традиционные методы (пропуска, ключи) по надёжности и удобству. Распознавание лиц выбрано как основа прототипа благодаря бесконтактности, доступности оборудования и достаточной точности для офисных сценариев.

Вторая глава посвящена практической реализации прототипа. Разработана архитектура системы, включающая клиентскую и серверную части, а также базу данных MongoDB. Система была протестирована на выборке из 50 изображений 5 авторизованных пользователей и 50 неавторизованных фото с помощью написанного скрипта. Результаты показали, что система обеспечивает высокую безопасность, но требует

доработки для снижения FRR. Анализ выявил ограничения, такие как малая тестовая выборка и отсутствие liveness detection, увеличивающие уязвимость программного обеспечения. Для устранения этих недостатков были предложены рекомендации по улучшению системы.

Третья глава представила экономическое обоснование разработки. Общая стоимость прототипа составила 276 529,39 рублей, включая материалы (83,700 рублей), эксплуатацию оборудования (2 045,12 рублей за 730 часов) и оплату труда (150 000 рублей в месяц для инженера-програмиста Использование open-source технологий (DeepFace, FastAPI, MongoDB) и доступного оборудования позволило существенно снизить затраты. Экономическая эффективность подтверждает применимость прототипа для малых предприятий.

Основным достижением работы является создание рабочего прототипа, обеспечивающего приемлемую производительность, который позволяет обслуживать до 85 человек в минуту. Система успешно решает задачу контроля доступа в офисах на 50–100 сотрудников, минимизируя риск несанкционированного проникновения.

Разработанная система демонстрирует потенциал для применения в реальных условиях, сочетая высокую безопасность, экономическую эффективность и гибкость. Её внедрение позволит предприятиям повысить уровень ИТЗ, минимизировать риски и оптимизировать процессы контроля доступа. Дальнейшая работа над прототипом, включая предложенные улучшения, обеспечит его конкурентоспособность на рынке биометрических решений и расширит спектр применения от офисов до высокобезопасных объектов.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. **Абрамов, Вячеслав Игоревич**. Основы инженерно-технической защиты объектов: учебное пособие / В. И. Абрамов, А. П. Соловьёв. — М.: Академия, 2019. — 240 с.

2. **Белов, Сергей. Васильевич**. Безопасность жизнедеятельности и защита окружающей среды: учебник / С. В. Белов. — М.: Юрайт, 2020. — 672 с.

3. **Гаврилов, Алексей Викторович**. Биометрические технологии в системах контроля доступа / А. В. Гаврилов // Информационная безопасность. — 2021. — № 3. — 152 с.

4. **ГОСТ 7.1-2003**. Библиографическая запись. Общие требования и правила составления. — М.: Стандартинформ, 2004. — 48 с.

5. **ГОСТ Р 51241-2008**. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. — М.: Стандартинформ, 2009. — 20 с.

6. **Иванов, Петр. Александрович**. Системы контроля и управления доступом: проектирование и эксплуатация / П. А. Иванов, Д. С. Петров. — СПб.: Лань, 2018. — 320 с.

7. **Козлов, Дмитрий. Антонович**. Алгоритмы распознавания лиц: современные подходы и перспективы / Д. А. Козлов // Вестник МГТУ им. Н. Э. Баумана. Серия: Информатика и вычислительная техника. — 2020. — № 4. — 164 с.

8. **Кузнецов, Алексей. Васильевич**. Информационная безопасность предприятий: учебное пособие / А. В. Кузнецов. — М.: КноРус, 2022. — 288 с.

9. **Лебедев, Игорь. Сергеевич**. Применение биометрических систем в обеспечении безопасности объектов / И. С. Лебедев, Е. Н. Смирнова // Безопасность и охрана труда. — 2023. — № 2. — 131 с.

10. **Михайлов, Александр Александрович**. Экономическое обоснование проектов в области информационных технологий / А. А. Михайлов. — М.: Финансы и статистика, 2017. — 256 с.

11. **Серов, Юрий Викторович**. Методы оценки эффективности систем безопасности / Ю. В. Серов // Журнал технической физики. — 2019. — Т. 89, № 5. — 254 с.

12. **Смирнов, Василий Григорьевич**. Программирование REST API на Python с использованием FastAPI / В. Г. Смирнов. — М.: ДМК Пресс, 2021. — 312 с.

13. **Фролов, Андрей Борисович**. Инженерно-технические средства охраны: учебное пособие / А. Б. Фролов, Н. И. Иванов. — М.: Инфра-М, 2020. — 208 с.

14. **Шапошников, Дмитрий Евгеньевич**. Биометрия в системах контроля доступа: проблемы и решения / Д. Е. Шапошников // Информационные технологии. — 2022. — № 6. — 230 с.

15. **Васильев, Родион Борисович**. Современные методы защиты информации / Р. Б. Васильев. — СПб.: Питер, 2019. — 416 с.

16. **Григорьев, Василий Михайлович**. Системы мониторинга производительности на основе Prometheus / В. М. Григорьев // Программные продукты и системы. — 2020. — № 3. — 362 с.

17. **Болотов, Андре. Игоревич**. Экономика разработки программного обеспечения / А. И. Болотов, С. П. Иванов. — М.: Юрайт, 2021. — 344 с.

18.