

**Бюджетное Учреждение Высшего Образования
Ханты-Мансийского автономного округа – Югры
«СУРГУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Политехнический институт

Кафедра автоматизированных систем обработки информации и управления

Курсовой проект по дисциплине «Проектирование и эксплуатация ИЭС»

Тема курсовой работы:

**«Проектирование системы обнаружения присутствия человека в
опасной зоне с учётом прохождения контрольных точек»**

Выполнил: студент группы 606-12

Речук Дмитрий Максимович

Проверил: Доцент кафедры АСОИУ, к. т. н.

Гавриленко Тарас Владимирович

Сургут, 2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1. ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ.....	6
1.1. Опасные зоны	6
1.2. Технологии обнаружения.....	7
1.3. Искусственные нейронные сети.....	7
2. ОБЗОР АНАЛОГОВ	9
2.1. Существующие решения.....	9
2.2. Сравнительный анализ аналогов	12
2.3. Выводы по обзору аналогов.....	13
3. ТЕХНИЧЕСКОЕ ЗАДАНИЕ.....	15
3.1. Общие сведения	15
3.2. Назначение и цели разработки	15
3.3. Требования к системе	16
3.4. Основные пользователи	19
4. ПРОЕКТИРОВАНИЕ СИСТЕМЫ.....	20
4.1. BPMN-диаграмма.....	20
4.2. Диаграмма IDEF0.....	22
4.3. DFD диаграмма	23
4.4. Схема интерфейса	24
5. ВИДЫ ОБЕСПЕЧЕНИЯ.....	26
5.1. Лингвистическое обеспечение.....	26
5.2. Математическое обеспечение.....	26
5.3. Программное обеспечение	28
5.4. Техническое обеспечение	28
5.5. Алгоритмическое обеспечение.....	29
5.6. Информационное обеспечение	30
5.6.1. ER-диаграмма базы данных.....	30
5.6.2. Логическая модель базы данных.....	32
ЗАКЛЮЧЕНИЕ	34

ВВЕДЕНИЕ

В современном мире обеспечение безопасности на производственных и инфраструктурных объектах приобретает всё большую значимость. Опасные зоны, характеризующиеся наличием сложного оборудования, высоких температур, химических веществ или радиации, представляют серьёзную угрозу для здоровья и жизни персонала. Традиционные методы контроля присутствия человека в таких зонах, основанные на визуальном наблюдении или использовании простых сигнальных систем, часто оказываются недостаточно эффективными из-за человеческого фактора, ограниченности оперативности реагирования и невозможности точного учёта всех аспектов безопасности. Это стимулирует разработку автоматизированных систем, способных повысить надёжность мониторинга и минимизировать риски несчастных случаев.

Современные технологии, такие как радиочастотная идентификация (RFID), компьютерное зрение и искусственные нейронные сети (ИНС), открывают новые возможности для создания систем, которые не только фиксируют присутствие человека в опасной зоне, но и учитывают прохождение контрольных точек и наличие защитного оборудования. Такие системы имеют потенциал снизить вероятность ошибок, связанных с невнимательностью или усталостью персонала, а также обеспечить оперативное реагирование на нарушения правил безопасности. Особое внимание уделяется применению методов искусственного интеллекта, которые позволяют анализировать сложные данные с камер и датчиков, обеспечивая высокую точность обнаружения и классификации объектов.

Данная работа посвящена разработке автоматизированной системы обнаружения присутствия человека в опасной зоне с учётом прохождения контрольных точек и наличия защитного оборудования. Система направлена на повышение безопасности сотрудников путём интеграции современных технологий мониторинга и анализа данных. Особое внимание уделяется учёту

таких факторов, как идентификация персонала, контроль маршрутов перемещения и проверка средств индивидуальной защиты, что делает задачу комплексной и многогранной.

Актуальность темы обусловлена следующими факторами:

1. **Рост сложности производственных процессов:** Современные предприятия используют всё более сложное оборудование и технологии, что повышает риски для персонала и требует точного контроля опасных зон.
2. **Ограниченность традиционных методов:** Ручной контроль и базовые системы сигнализации не способны обеспечить высокий уровень точности и оперативности в условиях динамичной среды.
3. **Развитие технологий автоматизации:** Прогресс в области компьютерного зрения, RFID и искусственного интеллекта создаёт основу для разработки эффективных систем безопасности.
4. **Потребность в комплексном подходе:** Необходимость учёта не только присутствия человека, но и его маршрута и защитной экипировки требует интеграции различных технологий.
5. **Снижение рисков и затрат:** Автоматизация контроля позволяет уменьшить количество инцидентов и связанные с ними экономические потери, повышая общую эффективность управления безопасностью.

Цель исследования: разработка и исследование автоматизированной системы обнаружения присутствия человека в опасной зоне, обеспечивающей надёжный контроль прохождения контрольных точек и наличия защитного оборудования с использованием современных технологий.

Задачи исследования:

1. Исследование предметной области, включая анализ существующих технологий и методов обнаружения.
2. Изучение инструментов и подходов к проектированию автоматизированных систем мониторинга.
3. Проектирование системы: разработка архитектуры, алгоритмов и интерфейса взаимодействия.
4. Анализ эффективности применения компьютерного зрения и RFID для фиксации присутствия человека и проверки защитного оборудования.
5. Разработка программного обеспечения для интеграции данных с датчиков и камер.
6. Оценка надёжности системы в условиях реальных или смоделированных сценариев.
7. Формирование рекомендаций по внедрению системы на предприятиях.

Выполнение указанных задач позволит достичь поставленной цели и создать систему, способную повысить уровень безопасности на объектах с повышенным риском.

1. ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

При разработке автоматизированной системы обнаружения присутствия человека в опасной зоне с учётом прохождения контрольных точек и наличия защитного оборудования крайне важно тщательно исследовать предметную область. Это позволяет определить ключевые аспекты, необходимые для проектирования эффективного решения. В первую очередь необходимо рассмотреть следующие элементы: опасные зоны, технологии обнаружения и искусственные нейронные сети как инструмент анализа данных.

1.1. Опасные зоны

Опасные зоны представляют собой участки производственных или инфраструктурных объектов, где существуют факторы риска для здоровья и жизни человека. К таким факторам относятся работа тяжёлого оборудования (например, станков, кранов), воздействие высоких температур, радиации, токсичных веществ или электричества. Опасные зоны могут быть как статическими (например, фиксированные участки цеха), так и динамическими (временные зоны, возникающие при проведении ремонтных работ). Основной задачей в контексте таких зон является контроль присутствия человека, поскольку его нахождение в них без соблюдения правил безопасности может привести к травмам или авариям.

Контрольные точки в опасных зонах — это заранее определённые места, такие как входы, выходы или промежуточные участки маршрута, прохождение которых фиксируется системой. Это позволяет отслеживать перемещения персонала и выявлять нарушения, например, несанкционированное проникновение в зону без прохождения обязательных этапов. Наличие защитного оборудования (шлемов, жилетов, перчаток и т.д.) является ещё одним критическим аспектом, так как оно снижает риск травматизма и является обязательным требованием на большинстве предприятий.

1.2. Технологии обнаружения

Для фиксации присутствия человека и контроля соблюдения требований безопасности используются различные технологии. Рассмотрим основные из них:

- **Радиочастотная идентификация (RFID):** Персонал оснащается RFID-метками, которые считываются антеннами, установленными в контрольных точках или по периметру зоны. Это позволяет идентифицировать сотрудника и фиксировать его перемещения. Метки могут быть интегрированы в защитное оборудование, что даёт возможность проверять его наличие.
- **Компьютерное зрение:** Камеры, установленные в опасных зонах, анализируют видеопоток в реальном времени. С помощью алгоритмов обработки изображений система определяет присутствие человека, его маршрут и наличие защитной экипировки (например, распознавание шлема по форме и цвету).
- **Датчики:** Инфракрасные, ультразвуковые или лазерные датчики фиксируют пересечение границ зоны или прохождение контрольных точек. Они могут дополнять другие технологии, повышая точность системы.

Каждая из технологий имеет свои особенности. Например, RFID обеспечивает точную идентификацию, но требует наличия меток у каждого сотрудника. Компьютерное зрение позволяет анализировать сложные сцены, но зависит от условий освещения. Датчики просты в установке, но не всегда могут идентифицировать конкретного человека. В рамках данной работы предполагается комбинированный подход для достижения максимальной надёжности.

1.3. Искусственные нейронные сети

Искусственные нейронные сети (ИНС) являются ключевым инструментом для обработки данных, поступающих от камер и датчиков. Они

широко применяются в задачах обнаружения объектов, классификации и анализа изображений. В контексте данной работы ИНС используются для:

- Определения присутствия человека в зоне на основе видеоданных.
- Распознавания защитного оборудования (например, шлемов, жилетов) по изображениям.
- Анализа маршрутов перемещения и фиксации прохождения контрольных точек.
- Наиболее перспективными архитектурами ИНС являются:
- **Сверточные нейронные сети (CNN):** применяются для анализа изображений с камер, выявляя признаки объектов (например, контуры шлема или силуэт человека).
- **Архитектуры для детектирования объектов (YOLO, SSD):** позволяют не только классифицировать объекты, но и определять их координаты в пространстве, что полезно для отслеживания перемещений.

Проведённый анализ предметной области показывает, что комбинирование технологий обнаружения с применением ИНС позволяет создать систему, способную эффективно решать задачу контроля безопасности в опасных зонах. Это обеспечивает основу для дальнейшего проектирования и разработки.

2. ОБЗОР АНАЛОГОВ

В области автоматизированного контроля присутствия человека в опасных зонах существует ряд решений, использующих различные технологии, такие как радиочастотная идентификация (RFID), компьютерное зрение, датчики и искусственный интеллект. Эти системы применяются для повышения безопасности на производственных объектах, в строительстве, энергетике и других отраслях с повышенным риском. В данном разделе рассматриваются основные аналоги, их функциональные возможности, преимущества и недостатки, а также проводится сравнительный анализ для определения перспективного подхода к разработке системы.

2.1. Существующие решения

1. Системы на основе RFID

Технология радиочастотной идентификации активно используется для отслеживания перемещений сотрудников в опасных зонах. Примером может служить система контроля доступа, применяемая на промышленных предприятиях. Сотрудники оснащаются RFID-метками, которые считываются антеннами, установленными в контрольных точках (например, на входах и выходах). Такие системы способны фиксировать присутствие человека и проверять наличие защитного оборудования, если оно также оснащено метками.

Преимущества:

- Высокая точность идентификации персонала.
- Простота интеграции в существующие системы безопасности.
- Возможность работы без прямой видимости.

Недостатки:

- Ограниченная дальность действия пассивных меток (до 10 м).
- Высокая стоимость активных меток и считывающих устройств.

- Отсутствие возможности анализа сложных сценариев (например, распознавания экипировки без меток).

2. Системы компьютерного зрения

Примером является система видеоаналитики, используемая на заводах для мониторинга безопасности. Камеры фиксируют видеопоток, а алгоритмы компьютерного зрения, такие как YOLO или SSD, анализируют изображения для обнаружения людей и проверки наличия защитного оборудования (например, шлемов или жилетов). Такие решения часто применяются в реальном времени и интегрируются с системами оповещения.

Преимущества:

- Высокая точность обнаружения объектов в зоне видимости.
- Возможность анализа сложных сцен и распознавания защитной экипировки.
- Гибкость в настройке под конкретные задачи.

Недостатки:

- Зависимость от условий освещения и угла обзора камер.
- Высокие вычислительные требования для обработки видео.
- Необходимость установки множества камер для полного покрытия зоны.

3. Системы на основе датчиков

Примером служат решения с использованием инфракрасных или лазерных датчиков, которые фиксируют пересечение границ опасных зон. Такие системы часто применяются в автоматизированных складах или на строительных площадках для контроля доступа в зоны риска.

Преимущества:

- Низкая стоимость и простота установки.
- Высокая надёжность в условиях плохой видимости.
- Быстрая реакция на пересечение границ.

Недостатки:

- Ограниченная функциональность (невозможно идентифицировать человека или проверить экипировку).
- Возможность ложных срабатываний из-за внешних факторов (например, животных или объектов).
- Отсутствие данных о маршрутах перемещения.

4. Комбинированные системы с искусственным интеллектом

Примером является система видеоаналитики NtechLab, используемая в городской среде для контроля доступа и распознавания лиц. Аналогичные решения адаптируются для промышленности, комбинируя RFID для идентификации, камеры для анализа экипировки и нейронные сети для обработки данных. Такие системы способны не только фиксировать присутствие, но и анализировать соблюдение правил безопасности.

Преимущества:

- Комплексный подход к мониторингу (идентификация, контроль экипировки, отслеживание маршрутов).
- Высокая адаптивность к изменяющимся условиям.
- Возможность интеграции с другими системами управления.

Недостатки:

- Высокая стоимость разработки и внедрения.
- Сложность настройки и обучения нейронных сетей.
- Зависимость от качества входных данных (видео, сигналов RFID).

2.2. Сравнительный анализ аналогов

Для оценки существующих решений ниже приведена таблица, в которой сравниваются ключевые характеристики систем по основным критериям.

Таблица 1. Сравнение аналогов

Функциональная возможность	RFID	Компьютерное зрение	Датчики	Комбинированные системы
Точность обнаружения	Высокая	Высокая	Средняя	Высокая
Идентификация персонала	Да	Нет	Нет	Да
Проверка защитного оборудования	Ограниченно (с метками)	Да	Нет	Да
Учёт контрольных точек	Да	Ограниченно	Да	Да
Адаптивность к условиям	Средняя	Низкая	Высокая	Высокая
Вычислительная сложность	Низкая	Высокая	Низкая	Высокая
Стоимость внедрения	Средняя	Высокая	Низкая	Высокая

- **Точность обнаружения:** Компьютерное зрение и комбинированные системы обеспечивают высокую точность благодаря анализу изображений, тогда как датчики могут быть менее надёжными из-за ложных срабатываний.

- **Идентификация персонала:** RFID и комбинированные системы позволяют точно определять, кто находится в зоне, что недоступно для датчиков и чистого компьютерного зрения.
- **Проверка защитного оборудования:** Компьютерное зрение и комбинированные системы превосходят другие подходы благодаря возможности анализа внешнего вида экипировки.
- **Учёт контрольных точек:** RFID и датчики эффективно фиксируют пересечение границ, тогда как компьютерное зрение требует дополнительных алгоритмов для отслеживания маршрутов.
- **Адаптивность:** Комбинированные системы лучше справляются с изменяющимися условиями благодаря ИИ, в отличие от компьютерного зрения, зависящего от освещения.
- **Стоимость:** Датчики являются наиболее экономичным решением, тогда как комбинированные системы требуют значительных вложений.

2.3. Выводы по обзору аналогов

Анализ существующих решений показывает, что ни одна из технологий в отдельности не решает задачу комплексного контроля присутствия человека в опасной зоне с учётом всех требований (идентификация, проверка экипировки, фиксация контрольных точек). Системы на основе RFID эффективны для идентификации и учёта маршрутов, но ограничены в анализе экипировки без дополнительных меток. Компьютерное зрение обеспечивает высокую точность распознавания объектов, но зависит от внешних условий и не идентифицирует персонал. Датчики просты и надёжны, но не предоставляют полной картины. Комбинированные системы с использованием искусственного интеллекта демонстрируют наибольший потенциал, объединяя преимущества всех подходов, однако их внедрение связано с высокой стоимостью и сложностью.

Для разработки системы в рамках данной работы целесообразно ориентироваться на комбинированный подход, интегрирующий RFID для идентификации и учёта контрольных точек, компьютерное зрение для проверки защитного оборудования и нейронные сети для обработки данных. Это позволит достичь высокой точности, надёжности и функциональности, необходимых для обеспечения безопасности в опасных зонах.

3. ТЕХНИЧЕСКОЕ ЗАДАНИЕ

3.1. Общие сведения

3.1.1. Наименование темы (проекта)

Полное наименование: «Разработка автоматизированной системы обнаружения присутствия человека в опасной зоне с учётом прохождения контрольных точек и наличия защитного оборудования».

3.1.2. Основания для разработки

- Курсовая работа в рамках Сургутского государственного университета.
- Письменное задание научного руководителя от «01» марта 2025 г.
- Цель разработки — создание системы, обеспечивающей надёжный контроль присутствия человека в опасных зонах, фиксацию прохождения контрольных точек и проверку наличия защитного оборудования с использованием современных технологий.

3.1.3. Исполнители

- Студент: Речук Дмитрий Максимович, группа 606-12.
- Научный руководитель: Гавриленко Тарас Владимирович, доцент кафедры АСОИУ, к.т.н.

3.1.4. Дата начала и дата окончания работ

- Начало работ: «__» _____ 2025 г.
- Окончание работ: «__» _____ 2025 г.

3.2. Назначение и цели разработки

3.2.1. Назначение

Разрабатываемая автоматизированная система предназначена для мониторинга присутствия человека в опасных зонах производственных или инфраструктурных объектов. Система обеспечивает фиксацию прохождения контрольных точек (входов, выходов, промежуточных участков), идентификацию персонала и проверку наличия защитного оборудования (шлемов, жилетов, перчаток и т.д.) в реальном времени. Решение направлено

на повышение безопасности сотрудников и снижение рисков несчастных случаев.

3.2.2. Цели и задачи

Главная цель: разработка и исследование автоматизированной системы, обеспечивающей надёжное обнаружение присутствия человека в опасной зоне с учётом прохождения контрольных точек и наличия защитного оборудования.

Основные задачи:

1. Исследование предметной области и анализ существующих технологий обнаружения.
2. Определение требований к системе и выбор подходящих инструментов для реализации.
3. Проектирование архитектуры системы, включая интеграцию RFID, компьютерного зрения и датчиков.
4. Разработка программного обеспечения для обработки данных с камер, RFID-меток и датчиков.
5. Реализация алгоритмов анализа видеопотока для проверки наличия защитного оборудования.
6. Тестирование системы в смоделированных условиях с оценкой точности и надёжности.
7. Формирование отчёта с результатами тестирования и рекомендациями по внедрению.

3.3. Требования к системе

3.3.1. Функциональные требования

1. Идентификация персонала
 - Регистрация сотрудников с использованием RFID-меток.
 - Сохранение данных о каждом сотруднике (ID, время входа/выхода).
2. Фиксация присутствия в опасной зоне

- Обнаружение человека в реальном времени с помощью камер и датчиков.
 - Генерация уведомлений при несанкционированном проникновении.
3. Контроль прохождения контрольных точек
- Отслеживание маршрута сотрудника через заданные точки (вход, выход, промежуточные участки).
 - Запись времени прохождения каждой точки.
4. Обработка и анализ данных
- Интеграция данных с RFID-антенн, камер и датчиков в единую систему.
 - Классификация событий (нарушение, нормальная работа) с использованием нейронных сетей.
5. Визуализация и уведомления
- Отображение текущего состояния зоны (присутствие людей, статус экипировки) на интерфейсе.
 - Генерация звуковых и визуальных сигналов при выявлении нарушений.
6. Хранение данных
- Ведение базы данных с информацией о сотрудниках, событиях и результатах анализа.
 - Возможность экспорта отчётов в форматах PDF.
- 3.3.2. Нефункциональные требования
1. Точность
- Точность обнаружения присутствия человека — не менее 95%.
2. Производительность
- Время реакции системы на событие (обнаружение, нарушение) — не более 1 секунды.

- Обработка видеопотока в реальном времени (не менее 15 кадров в секунду).

3. Надёжность

- Устойчивость к сбоям оборудования (камер, датчиков, RFID-антенн).
- Возможность работы в условиях плохого освещения или помех.

4. Масштабируемость

- Поддержка мониторинга нескольких опасных зон одновременно.
- Возможность добавления новых датчиков и камер без изменения архитектуры.

5. Интерфейс

- Простота использования для операторов (интуитивно понятный дизайн).
- Поддержка русского языка.

3.3.3. Требования к программному обеспечению

- Языки программирования: C#, Python (для нейронных сетей и анализа данных).
- Среда разработки: Visual Studio 2022.
- Библиотеки: OpenCV (обработка изображений), TensorFlow/PyTorch (нейронные сети).
- СУБД: PostgreSQL для хранения данных о сотрудниках и событиях.

3.3.4. Требования к аппаратному обеспечению

- Камеры: Разрешение не менее 1080p.
- RFID-оборудование: Антенны с радиусом действия 5–10 м, метки (активные/пассивные).
- Сервер: Процессор 4 ядра (Intel i5 или выше), 16 ГБ ОЗУ, SSD 256 ГБ.
- Операционная система: Windows 10/11.

3.4. Основные пользователи

- Операторы безопасности: Персонал, ответственный за мониторинг зон и реагирование на нарушения.
- Инженеры: Специалисты по настройке и обслуживанию системы.

4. ПРОЕКТИРОВАНИЕ СИСТЕМЫ






Для проектирования системы необходимо построить BPMN диаграмму для описания бизнес-процесса, DFD диаграмму для описания потока данных, IDEF0 диаграмму для описания общей структуры системы, схема интерфейса для определения концепции взаимодействия с пользователем.

4.1. BPMN-диаграмма

Первым этапом в проектировании системы является построение BPMN диаграммы. BPMN-диаграмма отражает детальное описание бизнес-процессов. Диаграмма представлена ниже (рис. 1).

Далее представлена таблица обозначений нотации BPMN:

Таблица 2. Обозначения в нотации BPMN

Объект	Описание
	Начало работы системы
	Конец работы системы
	Процесс
	Хранилище данных
	Комментарий к процессу
	Обозначение глобального процесса
	Документ/отчет
	Условное разветвление бизнес-процесса

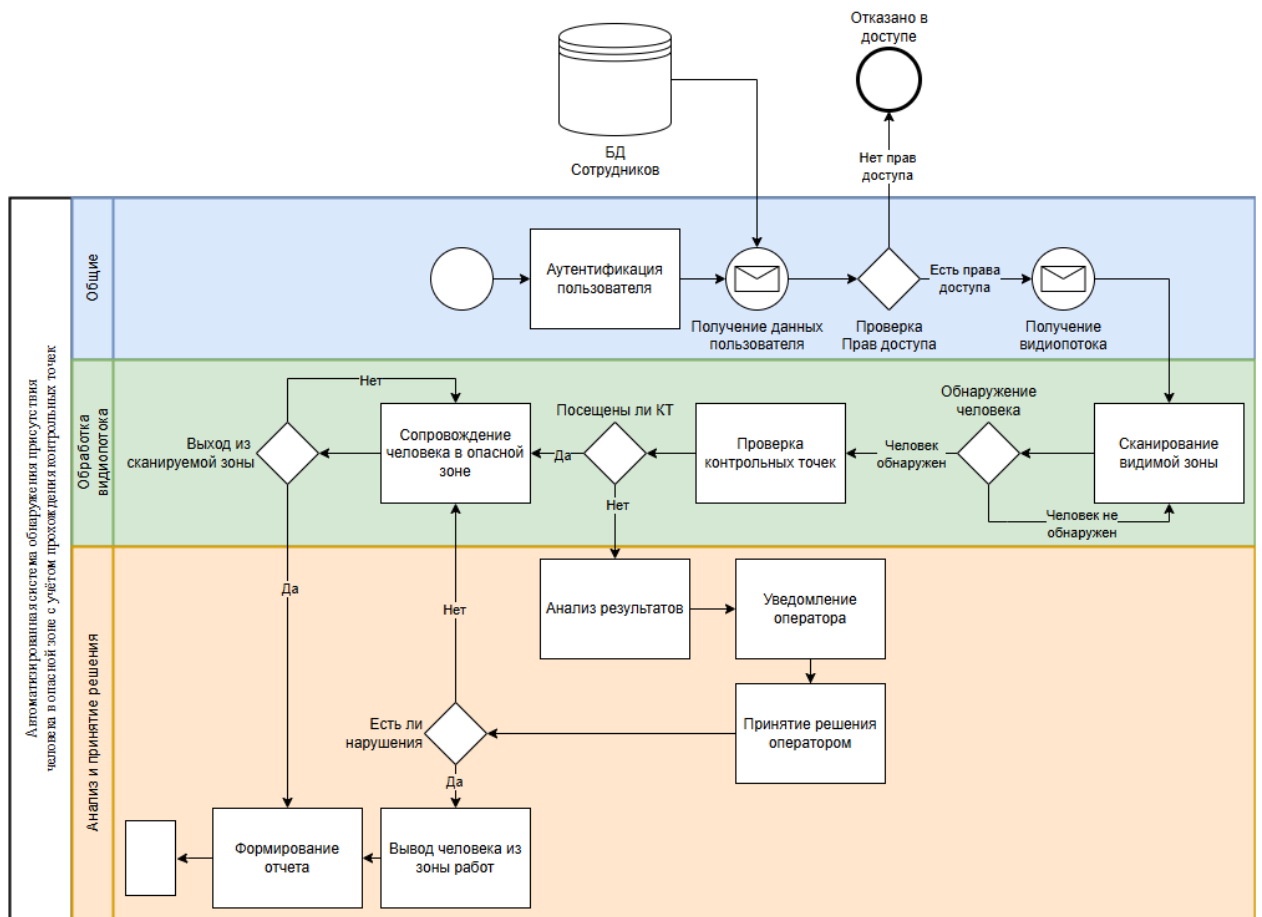


Рисунок 1. BPMN диаграмма системы

Глобально всю систему можно разделить на три модуля – идентификация и мониторинг, проверка экипировки, анализ и уведомления.

В блоке идентификации и мониторинга при запуске системы пользователь (оператор) может самостоятельно настроить параметры мониторинга, такие как границы опасной зоны, контрольные точки и требования к защитному оборудованию. Также он может загрузить из базы данных (БД сотрудников) уже существующие параметры, которые использовались ранее. После этого происходит инициализация системы и запуск мониторинга опасной зоны. Система начинает сбор данных с камер, RFID-антенн и датчиков для обнаружения присутствия человека и фиксации прохождения контрольных точек.

После этого в работу включается модуль проверки экипировки, который выполняется в заданном порядке. Сначала система идентифицирует сотрудника с помощью RFID-метки, чтобы определить его личность и

проверить допуск к работе в опасной зоне. Далее данные с камер передаются в нейросетевой модуль для анализа видеопотока. Нейросеть определяет наличие защитного оборудования (шлемов, жилетов и т.д.) у сотрудника. На основании этой информации система фиксирует, соответствует ли экипировка требованиям безопасности.

На последнем этапе включается в работу модуль анализа и уведомлений, который обрабатывает собранные данные. Анализатор проверяет, были ли соблюдены все требования: прохождение контрольных точек, наличие экипировки, допуск сотрудника. Если обнаруживаются нарушения (например, отсутствие шлема или непрохождение контрольной точки), формируется уведомление для оператора. Также создаётся отчёт с результатами мониторинга, включающий данные о сотрудниках, времени входа/выхода, прохождении контрольных точек и выявленных нарушениях.

Также на протяжении всего процесса мониторинга ведётся сбор необходимой информации для сохранения в БД. Это данные о сотрудниках (ID, время входа/выхода), результаты проверки экипировки, информация о прохождении контрольных точек, а также итоговый отчёт и уведомления о нарушениях.

Данная диаграмма позволяет в полной мере отразить процессы, происходящие в системе.

4.2. Диаграмма IDEF0

Следующий этап проектирования – это построение IDEF0 диаграммы. Диаграмма верхнего уровня обеспечивает наиболее общее или абстрактное описание объекта моделирования. Диаграмма представлена на рисунке ниже.

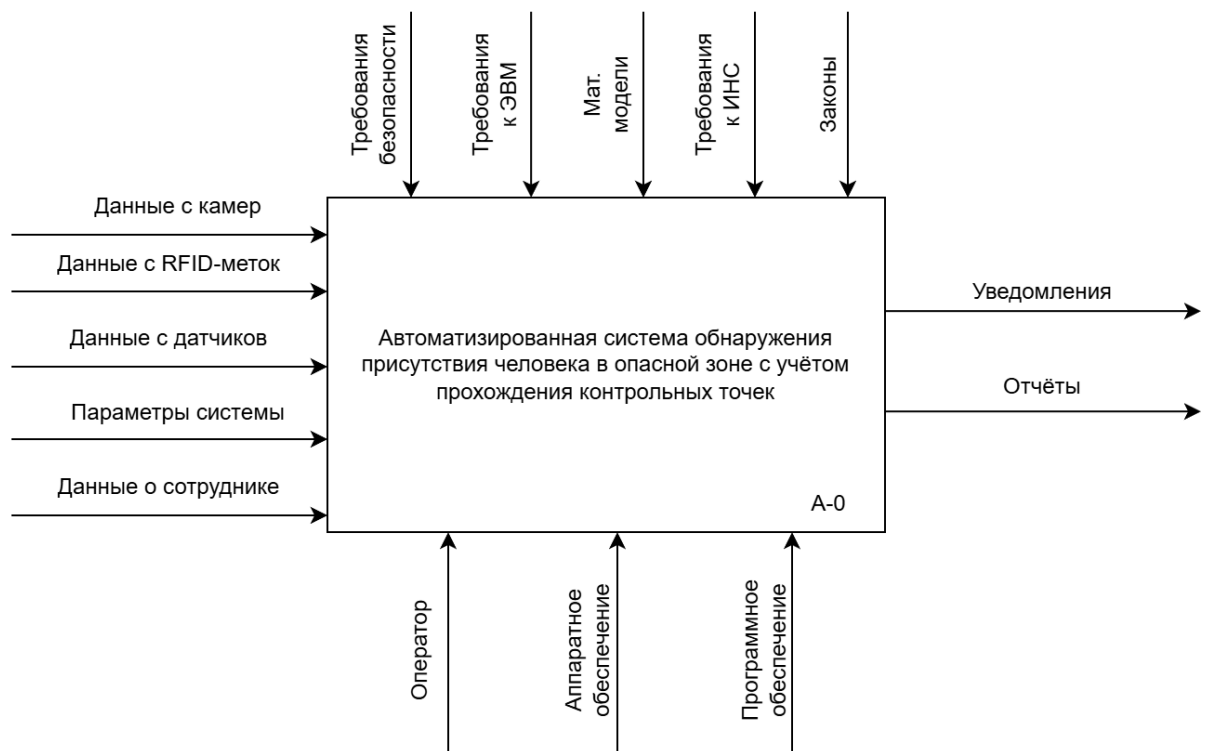


Рисунок 2. IDEF0 диаграмма системы

4.3. DFD диаграмма

Следующим же этапом проектирования стало построение DFD диаграммы. Данная диаграмма отображает потоки данных между системами, базами данных. Ключевыми элементами являются входные/выходные данные, системы, точки хранения и сбора данных. Она представлена на рисунке ниже.

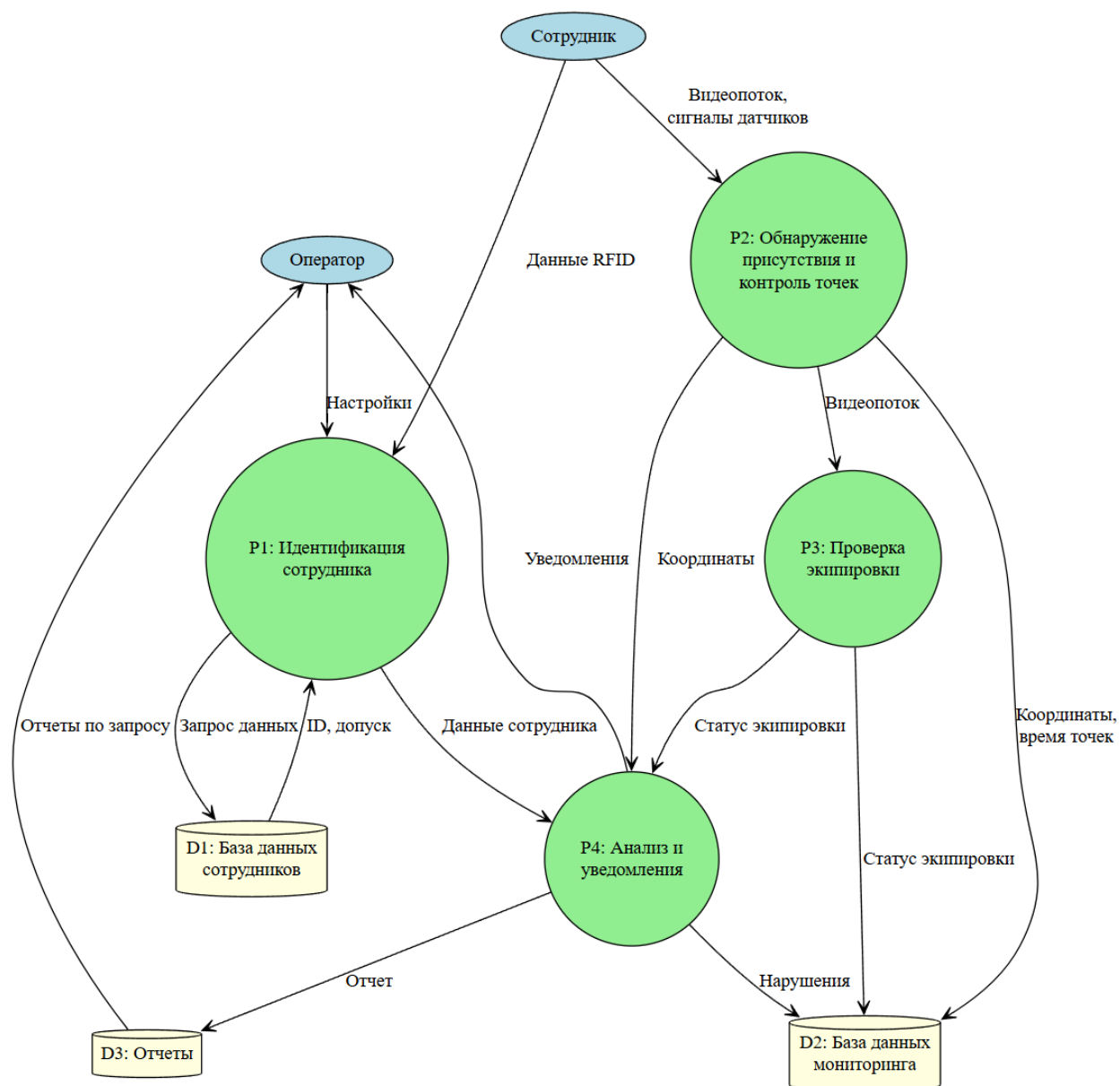


Рисунок 3. DFD диаграмма системы

4.4. Схема интерфейса

Ниже приведена схема интерфейса системы.

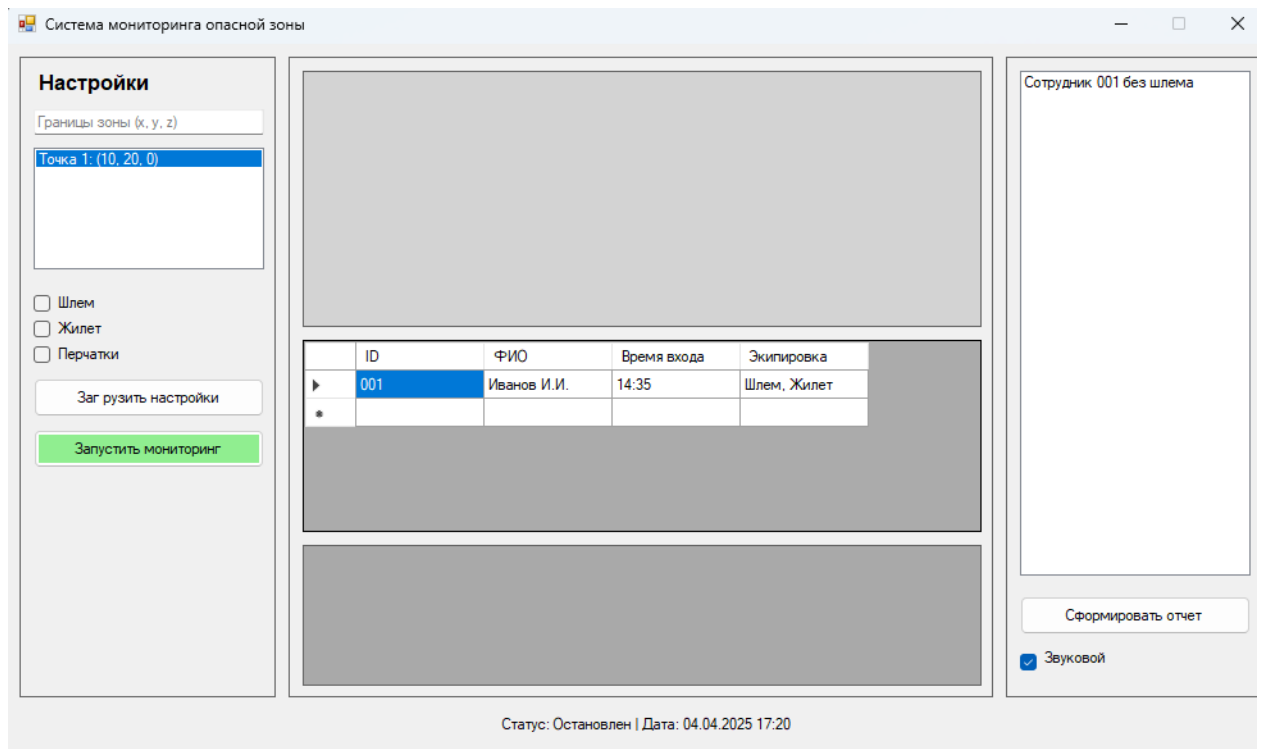


Рисунок 4. Схема интерфейс системы

5. ВИДЫ ОБЕСПЕЧЕНИЯ

5.1. Лингвистическое обеспечение

В качестве основного языка программирования для реализации системы был выбран **C#** и является удобным для создания приложений с графическим интерфейсом. Среда разработки — **Visual Studio 2022** для написания программ на языке **C#**.

Помимо этого, был использован язык программирования **Python** для обработки данных с камер и реализации нейросетевых алгоритмов. Python применяется для анализа видеопотока, классификации объектов (например, распознавания защитного оборудования) и интеграции с библиотеками машинного обучения.

Также был использован язык запросов **SQL** в СУБД **PostgreSQL** для управления базой данных, в которой хранятся данные о сотрудниках, событиях, контрольных точках и результатах мониторинга.

Ниже представлено описание некоторых профессиональных терминов, используемых в проекте:

- **RFID-метка:** Устройство, используемое для радиочастотной идентификации, которое позволяет идентифицировать сотрудника и фиксировать его перемещения.
- **Контрольная точка:** заранее определённый участок (например, вход или выход из опасной зоны), прохождение которого фиксируется системой для отслеживания маршрута сотрудника.
- **Компьютерное зрение:** Технология, позволяющая анализировать видеопоток для обнаружения объектов, в данном случае — для проверки наличия защитного оборудования.

5.2. Математическое обеспечение

Для реализации системы используются математические методы и алгоритмы, обеспечивающие обработку данных и принятие решений.

1. Обработка данных с RFID

Для определения местоположения сотрудника на основе сигналов RFID используется метод триангуляции. Расстояние между RFID-меткой и антенной рассчитывается по формуле:

$$d = \frac{P_r}{P_t G_t G_r \left(\frac{\lambda}{4\pi}\right)^2}$$

где d — расстояние, P_r — мощность принятого сигнала, P_t — мощность передатчика, G_t и G_r — коэффициенты усиления антенн, λ — длина волны. Этот метод позволяет определить координаты сотрудника в опасной зоне.

2. Обработка видеопотока

Для анализа видеопотока с камер используется сверточная нейронная сеть (CNN). Нейросеть обучается на датасете изображений, содержащих сотрудников с защитным оборудованием (шлемы, жилеты) и без него. Для классификации объектов применяется функция активации Softmax:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^n e^{z_j}}$$

где $P(y_i)$ — вероятность принадлежности объекта к классу i , z_j — выходной сигнал нейрона для класса i , n — количество классов (например, «шлем есть», «шлема нет»).

3. Фиксация контрольных точек

Для определения пересечения контрольных точек используется алгоритм пересечения луча с плоскостью. Если сотрудник пересекает контрольную точку, его координаты (x , y , z) сравниваются с координатами плоскости точки:

$$t = \frac{(\text{planeOrigin} - \text{origin}) \cdot n}{\text{planeNormal} \cdot n}$$

где t — параметр пересечения, n — нормаль плоскости, planeNormal — направление луча, planeOrigin — вектор от начала луча до плоскости. Если $t > 0$, фиксируется прохождение контрольной точки.

5.3. Программное обеспечение

Для реализации системы используются следующие программные средства:

- **Visual Studio 2022:** для разработки на C# с поддержкой .NET Framework версии 4.7.2 и выше.
- **Python 3.9+:** для реализации нейросетевых алгоритмов с использованием библиотек **TensorFlow** и **OpenCV**.
- **PostgreSQL 15:** для управления базой данных.

Сборка приложения доступна для операционных систем Windows, с поддержкой 32-разрядных и 64-разрядных архитектур.

5.4. Техническое обеспечение

Требования к операционной системе:

- Windows 10/11 (64-разрядные версии).

Минимальные требования для системы:

- Процессор: 4 ядра (Intel Core i3 или AMD Ryzen 3, начиная с 2015 года).
- Оперативная память: 8 ГБ.
- Видеокарта: NVIDIA GT 1030 или встроенная графика Intel HD Graphics 620 и выше.
- Свободное место на диске: 50 ГБ (рекомендуется SSD).

Рекомендуемые требования для системы:

- Процессор: 6 ядер (Intel Core i5 или AMD Ryzen 5, начиная с 2018 года).
- Оперативная память: 16 ГБ.
- Видеокарта: NVIDIA GTX 1060 6 ГБ или выше.
- Свободное место на диске: 100 ГБ (SSD).

Аппаратное обеспечение:

- Камеры: Разрешение 1080p, с поддержкой инфракрасного режима для работы в условиях плохого освещения.

- RFID-оборудование: Антенны с радиусом действия 5–10 м, активные и пассивные метки.
- Датчики: Инфракрасные или лазерные с дальностью действия до 20 м.

5.5. Алгоритмическое обеспечение

1. Алгоритм идентификации сотрудника:

- Считывание данных с RFID-метки.
- Запрос информации о сотруднике из БД (ID, допуск).
- Сохранение времени входа в опасную зону.

2. Алгоритм обнаружения присутствия:

- Сбор данных с камер и датчиков.
- Анализ видеопотока с помощью нейросети для обнаружения человека.
- Сравнение координат человека с границами опасной зоны.

3. Алгоритм фиксации контрольных точек:

- Определение координат сотрудника с помощью RFID-триангуляции.
- Проверка пересечения с плоскостью контрольной точки.
- Сохранение времени и места прохождения в БД.

4. Алгоритм проверки защитного оборудования:

- Анализ видеопотока с помощью сверточной нейронной сети (CNN).
- Классификация объектов (шлем, жилет, перчатки).
- Сравнение с требованиями безопасности.

5. Алгоритм анализа и уведомлений:

- Сбор данных о присутствии, контрольных точках и экипировке.
- Проверка на наличие нарушений (отсутствие экипировки, непрохождение КТ).

- Генерация уведомлений для оператора.
- Формирование отчёта в формате CSV.

5.6. Информационное обеспечение

5.6.1. ER-диаграмма базы данных

Представленная ER-диаграмма (рис. 5) отображает информационную модель системы для мониторинга присутствия человека в опасной зоне. Диаграмма иллюстрирует основные сущности, их атрибуты и связи между ними.

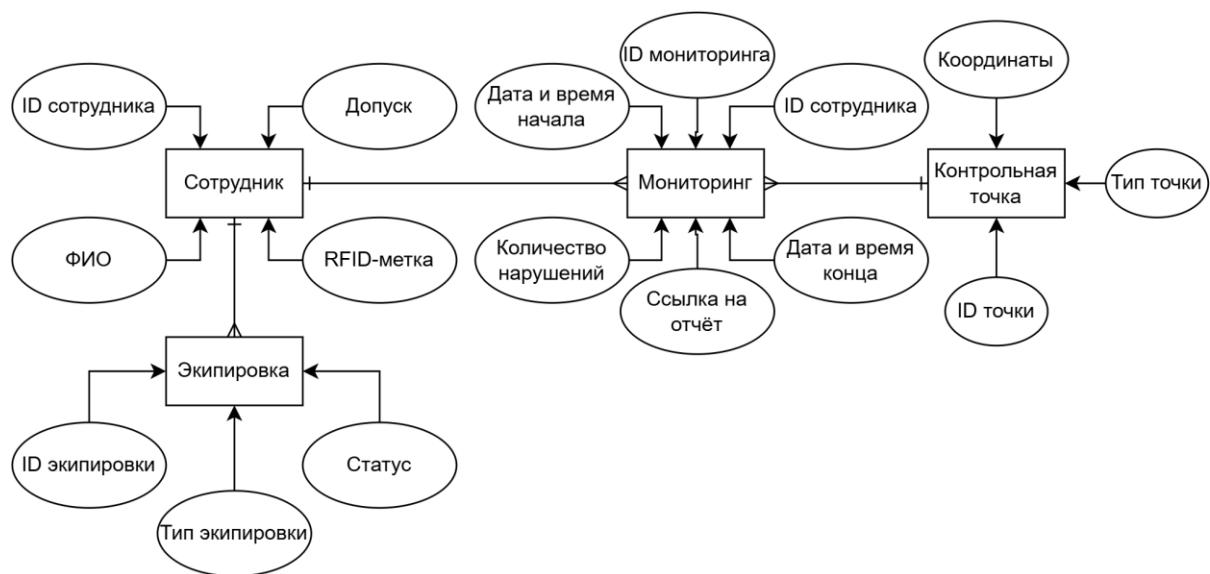


Рисунок 5. ER-диаграмма базы данных

Основные сущности:

1. **Мониторинг** — центральная сущность, представляющая процесс мониторинга.

Таблица 3. Описание сущности "Мониторинг"

№	Наименование	Назначение
1	ID мониторинга	Уникальный идентификатор процесса мониторинга
2	ID сотрудника	Ссылка на сотрудника, участвующего в мониторинге
3	Дата и время начала	Фиксация момента старта мониторинга

4	Дата и время конца	Фиксация момента завершения мониторинга
5	Ссылка на отчёт	Указатель на документ с результатами мониторинга
6	Количество нарушений	Статистический показатель выявленных нарушений

2. **Сотрудник** — сущность, описывающая данные о сотрудниках.

Таблица 4. Описание сущности "Сотрудник"

№	Наименование	Назначение
1	ID сотрудника	Уникальный идентификатор сотрудника
2	ФИО	Полное имя сотрудника
3	RFID-метка	Уникальный код RFID-метки
4	Допуск	Информация о допуске к работе в опасной зоне

3. **Контрольная точка** — сущность, представляющая контрольные точки.

Таблица 5. Описание сущности "Контрольная точка"

№	Наименование	Назначение
1	ID точки	Уникальный идентификатор контрольной точки
2	Координаты	Координаты точки в пространстве (x, y, z)
3	Тип точки	Тип точки (вход, выход, промежуточная)

4. **Экипировка** — сущность, описывающая защитное оборудование.

Таблица 6. Описание сущности "Экипировка"

№	Наименование	Назначение
1	ID экипировки	Уникальный идентификатор элемента экипировки

2	Тип экипировки	Тип элемента (шлем, жилет, перчатки)
3	Статус	Наличие элемента у сотрудника (да/нет)

Связи между сущностями:

- Мониторинг — Сотрудник: связь "многие-к-одному" (M:1).
- Мониторинг — Контрольная точка: связь "многие-к-одному" (M:1).
- Сотрудник — Экипировка: связь "один-ко-многим" (1:M).

5.6.2. Логическая модель базы данных

Логическая модель базы данных описывает структуру данных для системы мониторинга. Она представлена на рисунке ниже (рис. 6).

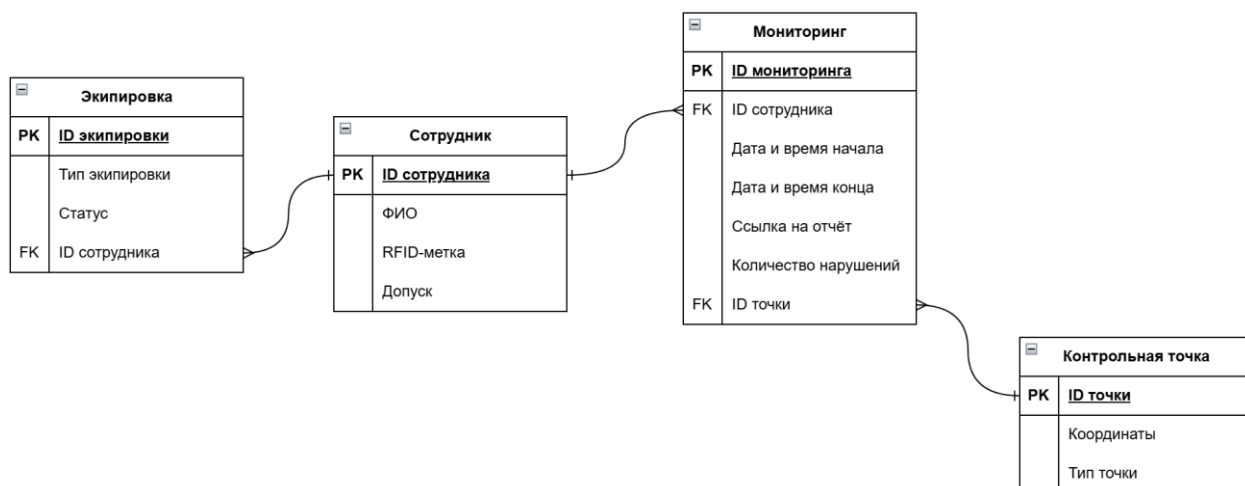


Рисунок 6. Логическая модель базы данных

Сущности и их атрибуты:

1. Мониторинг (Monitoring)

- ID_мониторинга (PK) — уникальный идентификатор.
- ID_сотрудника (FK) — внешний ключ к таблице сотрудников.
- Дата_время_начала — временная метка начала мониторинга.
- Дата_время_конца — временная метка завершения мониторинга.
- Ссылка_на_отчёт — путь к файлу отчёта.
- Количество_нарушений — счётчик нарушений.

2. Сотрудник (Employee)

- ID_сотрудника (PK) — уникальный идентификатор.

- ФИО — полное имя сотрудника.
- RFID_метка — код RFID-метки.
- Допуск — информация о допуске.

3. Контрольная точка (Checkpoint)

- ID_точки (PK) — уникальный идентификатор.
- Координаты — координаты точки (x, y, z).
- Тип_точки — тип точки (вход, выход, промежуточная).

4. Экипировка (Equipment)

- ID_экипировки (PK) — уникальный идентификатор.
- Тип_экипировки — тип элемента (шлем, жилет, перчатки).
- Статус — наличие элемента (да/нет).
- ID_сотрудника (FK) — внешний ключ к таблице сотрудников.

Связи между таблицами:

- Мониторинг → Сотрудник: связь "многие-к-одному" (M:1).
- Мониторинг → Контрольная точка: связь "многие-к-одному" (M:1).
- Сотрудник → Экипировка: связь "один-ко-многим" (1:M).

Данная логическая модель обеспечивает эффективное хранение и обработку данных для системы мониторинга, позволяя структурировать информацию о сотрудниках, контрольных точках, экипировке и результатах мониторинга.

ЗАКЛЮЧЕНИЕ

В рамках данной работы была разработана автоматизированная система обнаружения присутствия человека в опасной зоне с учётом прохождения контрольных точек и наличия защитного оборудования. Эта задача имеет высокую актуальность в условиях роста сложности производственных процессов и повышения требований к безопасности персонала на предприятиях. Использование современных технологий, таких как радиочастотная идентификация (RFID), компьютерное зрение и искусственный интеллект, позволило создать решение, способное минимизировать риски несчастных случаев и снизить влияние человеческого фактора на соблюдение норм безопасности.

В ходе выполнения работы были решены следующие задачи:

1. Проведён анализ предметной области, в рамках которого изучены опасные зоны, технологии обнаружения и методы применения искусственного интеллекта. Определены ключевые аспекты, такие как необходимость учёта контрольных точек и проверки защитного оборудования.
2. Выполнен обзор аналогов, который показал, что существующие решения (RFID-системы, компьютерное зрение, датчики) имеют свои преимущества и недостатки. На основе анализа был обоснован выбор комбинированного подхода, объединяющего несколько технологий для достижения максимальной эффективности.
3. Разработано техническое задание, включающее функциональные и нефункциональные требования к системе, а также этапы её реализации. Определены основные пользователи системы и требования к аппаратному и программному обеспечению.
4. Спроектирована система с использованием BPMN-диаграммы, которая описывает бизнес-процессы мониторинга, проверки экипировки и анализа данных. Диаграмма отражает взаимодействие между

оператором, системой мониторинга и модулем анализа, включая фиксацию контрольных точек и генерацию уведомлений.

5. Описаны виды обеспечения системы.

Разработанная система позволяет в реальном времени фиксировать присутствие человека в опасной зоне, отслеживать его перемещения через контрольные точки и проверять наличие защитного оборудования. Применение нейронных сетей для анализа видеопотока обеспечивает высокую точность распознавания экипировки, а использование RFID-технологии гарантирует надёжную идентификацию сотрудников. Генерация уведомлений при выявлении нарушений (например, отсутствие шлема или непрохождение контрольной точки) позволяет оперативно реагировать на потенциальные угрозы.

Однако система имеет потенциал для дальнейшего совершенствования.

В перспективе возможно:

- Интеграция с системами автоматического управления оборудованием для немедленной остановки работы при выявлении нарушений.
- Расширение функционала для мониторинга нескольких опасных зон одновременно с использованием облачных технологий.
- Применение адаптивных нейронных сетей для повышения точности распознавания в условиях плохой видимости или сложной среды.
- Разработка мобильного приложения для операторов, что упростит доступ к уведомлениям и отчётам.

Таким образом, разработанная система представляет собой эффективное решение для повышения безопасности на производственных объектах. Её внедрение может значительно снизить риски несчастных случаев, улучшить контроль соблюдения норм безопасности и повысить общую эффективность управления производственными процессами.