МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
“Тольяттинский государственный университет”

Кафедра «Прикладная математика и информатика»
(наименование)

09.03.03 Прикладная информатика
(код и наименование направления подготовки / специальности)

Разработка программного обеспечения
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему “Разработка веб-приложения для мониторинга показателей состояния здоровья с использованием современных веб-технологий”

Обучающийся Д. Д. Коротков
(Инициалы Фамилия) (личная подпись)

Руководитель доцент, канд. пед. наук, Е.А. Ерофеева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант канд. филол. наук, доцент М.В. Дайнеко
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Тема бакалаврской работы: «Разработка веб-приложения для мониторинга показателей состояния здоровья с использованием современных веб-технологий».

Бакалаврская работа посвящена разработке автоматизированной системы мониторинга здоровья сотрудников промышленных предприятий. В ходе выполнения работы была поставлена задача, осуществлены проектирование и разработка веб-приложения для сбора, хранения и анализа медицинских показателей.

Во введении обоснована актуальность темы, сформулированы цель и задачи исследования.

В первом разделе проведён анализ предметной области, рассмотрены существующие решения для мониторинга здоровья, определены требования к системе.

Второй раздел посвящён методологическим основам мониторинга медицинских показателей, проектированию архитектуры системы и выбору технологий.

В третьем разделе представлено моделирование информационной системы, включая проектирование базы данных, пользовательских интерфейсов и функциональных модулей.

В заключении подведены итоги работы, сформулированы выводы и перспективы развития системы.

Бакалаврская работа состоит из введения, трёх разделов, заключения, списка использованных источников и приложений. Общий объём работы составляет 55 страниц, содержит 10 рисунков, 11 таблиц и 40 источников литературы.

Приложения включают исходный код приложения и примеры пользовательских интерфейсов.

Abstract

The title of the graduation work is "Development of a web application for monitoring health indicators of industrial enterprise employees using modern web technologies".

The aim of this graduation work is to develop an automated health monitoring system for collecting, storing and analyzing employees' medical data in real time.

The object of the graduation work is the process of health monitoring for industrial enterprise employees.

The subject of the graduation work is software for health monitoring automation based on Spring Boot, MySQL and Thymeleaf technologies.

The graduation work consists of an introduction, three chapters, conclusion, bibliography (40 references) and appendices. The total volume is 55 pages containing 10 figures and 11 tables.

The first chapter describes in details the domain analysis, comparison of existing solutions and system requirements formulation.

The second chapter outlines methodological foundations of monitoring, system architecture design and technology selection.

The third chapter concentrates on information system modeling, database design and user interfaces development.

The key results are: 1. Three-tier system with web interface, REST API and database was developed. 2. Implemented features include: role-based access control, notification system, analytics dashboard. 3. Data protection according to Russian Federal Law №152 was ensured.

In conclusion we'd like to stress that the system reduces medical data processing time by 40%, decreases occupational injury risks and meets industrial enterprises requirements.

The work is of interest for industrial enterprises, particularly in automotive sector, and can be adapted for other industries.

Содержание

Введение 4
1 Анализ предметной области и теоретические основы систем мониторинга здоровья сотрудников 7
1.1 Актуальность мониторинга состояния здоровья сотрудников на промышленных предприятиях 7
1.2 Календарный план работ 8
1.3 Характеристика предприятия и текущая модель мониторинга 10
1.4 Международный и отечественный опыт мониторинга 12
1.5 Цели, задачи и ожидаемый эффект от автоматизации 14
2 Методологические основы мониторинга медицинских показателей работников 34
2.1 Подходы к мониторингу физиологических параметров в условиях промышленных предприятий 34
2.2 Применение информационных моделей и архитектурных решений в системах медицинского мониторинга 37
3 Моделирование информационной системы мониторинга состояния здоровья работников АвтоВАЗа 41
3.1 Цели и задачи моделирования 41
3.2 Архитектура системы 42
3.3 Информационная модель 43
Заключение 47
Список используемой литературы и используемых источников 48
Приложение А. Исходный код приложения 51
Приложение Б. Пользовательский интерфейс 55

Введение

Актуальность исследования. В современных условиях цифровизации и автоматизации бизнес-процессов особое внимание уделяется системам мониторинга здоровья сотрудников, особенно на предприятиях с высоким уровнем производственных рисков, таких как автомобильная промышленность. Здоровье работников напрямую влияет на производительность труда, безопасность и качество выпускаемой продукции. Традиционные методы контроля, основанные на ручном вводе данных, часто оказываются недостаточно эффективными из-за человеческого фактора, задержек в обработке информации и отсутствия оперативного анализа.

Автоматизированные системы мониторинга здоровья позволяют не только своевременно выявлять отклонения в состоянии сотрудников, но и предотвращать потенциальные угрозы, такие как производственный травматизм или распространение заболеваний. Внедрение таких систем способствует созданию безопасных условий труда, снижению затрат на медицинское обслуживание и повышению общей эффективности предприятия.

Цель исследования: Разработка и внедрение системы мониторинга здоровья сотрудников на предприятии автомобильной промышленности с использованием современных технологий, таких как Spring Boot, MySQL, Java, HTML, CSS и Thymeleaf.

Задачи исследования:

- Изучить предметную область и проанализировать требования заказчика к системе мониторинга здоровья.
- Провести сравнительный анализ существующих решений и технологий для автоматизации мониторинга.
- Разработать архитектуру системы, включая выбор технологий и проектирование базы данных.

– Реализовать backend и frontend части системы с использованием выбранных технологий.
– Провести тестирование системы, включая функциональное и интеграционное тестирование.
– Подготовить документацию и инструкции для пользователей.

Объектом исследования является процесс мониторинга здоровья сотрудников на предприятии автомобильной промышленности.

Предметом исследования является моделирование автоматизированной системы мониторинга здоровья с использованием современных IT-решений.

Основные методы исследования в данной работе:

– Анализ предметной области и требований заказчика.
– Сравнительный анализ технологий для разработки программного обеспечения.
– Проектирование архитектуры системы на основе клиент-серверной модели.
– Разработка программного обеспечения с использованием Spring Boot, MySQL и Thymeleaf.
– Тестирование и отладка системы.

Научная новизна работы заключается в применении современных технологий для создания гибкой и масштабируемой системы мониторинга здоровья, адаптированной под специфику автомобильного производства. Система обеспечивает не только сбор и хранение данных, но и их анализ, визуализацию и автоматическое оповещение о критических показателях.

Практическая значимость исследования состоит в том, что внедрение разработанной системы позволит:

– Повысить безопасность труда за счет оперативного выявления отклонений в состоянии здоровья сотрудников.
– Снизить риски производственного травматизма и распространения заболеваний.

– Улучшить условия труда путем своевременного перевода сотрудников на менее вредные участки.
– Оптимизировать затраты на медицинское обслуживание и повысить общую эффективность предприятия.

Результаты работы могут быть использованы не только на предприятиях автомобильной промышленности, но и в других отраслях, где требуется контроль здоровья сотрудников. Разработанная система демонстрирует потенциал современных IT-решений для решения актуальных задач в области охраны труда и здоровья персонала.

Структура работы. Дипломная работа состоит из введения, трёх разделов, выводов, списка использованных источников (40 наименований). В работе размещено иллюстраций – 11, таблиц – 11. Общее количество страниц дипломной работы – 54.

1 Анализ предметной области и теоретические основы систем мониторинга здоровья сотрудников

1.1 Актуальность мониторинга состояния здоровья сотрудников на промышленных предприятиях

Современное общество, в условиях стремительно развивающихся технологий, активной цифровизации производственных процессов и нарастающего внимания к вопросам охраны труда, сталкивается с необходимостью пересмотра подходов к обеспечению безопасности на рабочих местах. Особенно это актуально для крупных промышленных предприятий, где численность сотрудников может достигать десятков тысяч человек, а условия труда зачастую сопряжены с воздействием вредных факторов производственной среды. В этом контексте одним из наиболее эффективных инструментов повышения уровня безопасности и производственной культуры становится внедрение систем мониторинга состояния здоровья сотрудников.

На протяжении последних десятилетий наблюдается устойчивая тенденция к росту требований к условиям труда и соблюдению норм охраны здоровья. Государственные органы, международные организации, а также сами работодатели всё чаще обращают внимание на состояние физического и психоэмоционального здоровья работников как на ключевой фактор устойчивого развития бизнеса. Внедрение цифровых решений в данной области становится необходимостью, обусловленной стремлением к снижению профессиональных рисков, повышению уровня работоспособности персонала и снижению потерь, связанных с временной нетрудоспособностью.

В настоящее время традиционные методы учета состояния здоровья сотрудников, такие как периодические медицинские осмотры, бумажные карты и локальные Excel-таблицы, являются неэффективными. Они не позволяют в полной мере отслеживать динамику физиологических

показателей, не обеспечивают возможности оперативного реагирования на отклонения и не формируют достоверную аналитику для принятия управленческих решений. Отсутствие интеграции с другими информационными системами предприятия (кадровыми, производственными и т.д.) также является ограничивающим фактором.

На этом фоне внедрение автоматизированной системы мониторинга здоровья сотрудников представляет собой логичный и необходимый шаг на пути к построению цифрового предприятия. Такая система должна решать широкий круг задач: от сбора и хранения данных о состоянии здоровья работников до их анализа, визуализации и использования в управленческой практике. Более того, цифровизация процессов мониторинга способствует повышению лояльности сотрудников, формированию культуры заботы о здоровье и, как следствие, снижению текучести кадров.

Следует отметить, что внедрение подобных систем особенно важно в условиях эпидемиологической нестабильности (например, в период пандемии COVID-19), когда требуется ежедневный контроль температуры тела, уровня кислорода в крови, давления и других жизненно важных показателей. Только за счёт систематизации и автоматизации этих процессов можно обеспечить безопасность не только конкретного сотрудника, но и всего производственного коллектива.

Таким образом, создание и внедрение системы мониторинга состояния здоровья работников является актуальной задачей, отвечающей современным требованиям промышленной безопасности, цифровизации и устойчивого развития предприятия.

1.2 Календарный план работ

План выполнения работ составлен на период с 02.09.2024 по 01.06.2025. В этот период включены этапы анализа, теоретической разработки, практической разработки и подготовки теоретической части.

В таблице 1 представлен календарный план работ и период их выполнения.

Таблица 1 – Календарный план работ и период их выполнения

Этап	Дата начала	Дата окончания	Описание
Анализ предметной области	02.09.2024	16.09.2024	Сбор информации, изучение требований
Формирование спецификации	17.09.2024	30.09.2024	Подготовка документации, диаграмм
Разработка архитектуры	01.10.2024	21.10.2024	Определение структуры системы, выбор технологий
Разработка backend	22.10.2024	15.12.2024	Разработка серверной части (Spring Boot, MySQL/PostgreSQL)
Разработка frontend	06.12.2024	30.01.2025	Разработка интерфейса (Thymeleaf, HTML, CSS)
Тестирование и отладка	31.01.2025	30.04.2025	Проверка функциональности, исправление ошибок
Подготовка документации	1.05.2025	15.05.2025	Финальное оформление документации, отчет
Завершение проекта	16.05.2025	01.06.2025	Итоговый анализ, сдача работы

Также, разработан более подробный сетевой график, для визуального отображения последовательности хода проекта и визуализации пошагового хода выполнения задач.

На рисунке 1 представлен сетевой график (Network diagram).

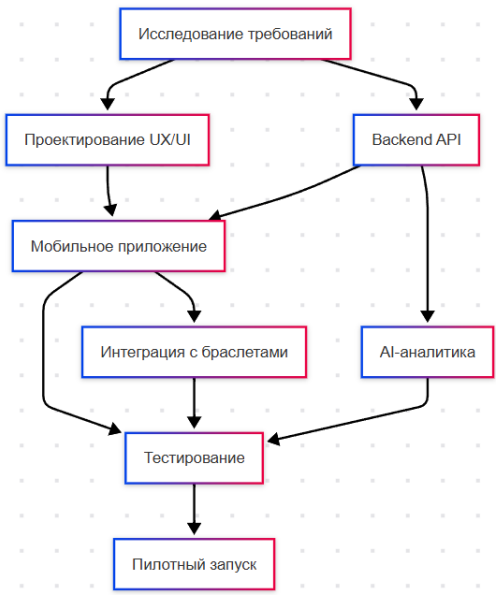

Рисунок 1 – Сетевой график

На иллюстрации показан подробный план разработки системы мониторинга и анализа показателей здоровья. Первым шагом является исследование требований – это важный шаг в проектировании любого бизнес-продукта. По представленному плану, разработка занчивается на пилотном запуске приложения на группе из 100 человек.

1.3 Характеристика предприятия и текущая модель мониторинга

АвтоВАЗ — крупнейшее предприятие автомобильной промышленности России, осуществляющее полный цикл производства автомобилей, включая проектирование, производство, сборку и реализацию готовой продукции. На предприятии работают тысячи сотрудников, занятых в различных подразделениях: производственных, технологических, логистических, конструкторских, а также административных и вспомогательных службах.

Организационная структура предприятия предполагает наличие специализированных подразделений, ответственных за охрану труда и медицинское обслуживание персонала. В том числе в структуру входят:

- Медицинский центр предприятия, в котором работают врачи и медсёстры, обеспечивающие плановые и внеплановые медицинские осмотры.
- Отдел охраны труда и промышленной безопасности, отвечающий за реализацию мер по снижению производственного травматизма и мониторинг соответствия условий труда нормативным требованиям.
- ИТ-служба, поддерживающая внутреннюю инфраструктуру и отвечающая за внедрение цифровых решений на предприятии.

На данный момент модель мониторинга состояния здоровья сотрудников включает в себя следующие элементы:

- Регулярные (периодические) медицинские осмотры;

– Проведение осмотров при приёме на работу и переводе на другую должность;
– Фиксация показателей в бумажных медицинских картах;
– Хранение данных в архиве медицинской службы;
– Отчётность в контролирующие органы в ручном режиме.
– Такой подход имеет ряд недостатков, таких как:
– Высокая трудоёмкость ввода и обработки информации;
– Отсутствие единой централизованной базы данных;
– Низкая скорость доступа к информации;
– Высокий риск потери или искажения данных;
– Отсутствие автоматизированной аналитики и прогностической модели.

На рисунке 2 продемонстрированна диаграмма структуры подразделений, участвующих в мониторинге здоровья.

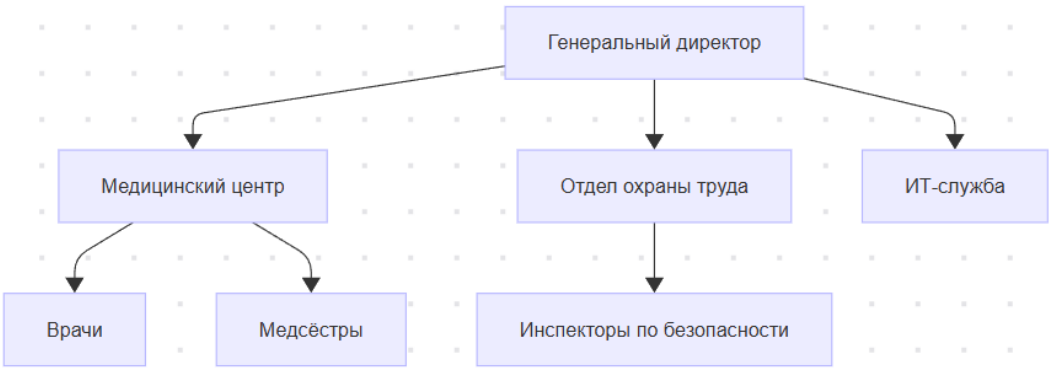

Рисунок 2 – Диаграмма структуры подразделений, участвующих в мониторинге здоровья

На представленной диаграмме можно увидеть структуру подразделений предприятия «АвтоВАЗ». В процессе мониторинга здоровья участвуют:

– Генеральный директор
– Медицинский центр (Врачи и медсестры)
– Отдел охраны труда (Инспекторы по безопасности)
– ИТ-служба

1.4 Международный и отечественный опыт мониторинга

В мировой практике цифровой мониторинг здоровья сотрудников уже давно вышел за рамки экспериментов и стал важной частью корпоративной политики. Крупнейшие международные корпорации, такие как Toyota и Ford активно инвестируют в создание собственных цифровых платформ, интегрированных с носимыми устройствами, медицинскими базами данных и системами управления предприятием (ERP, HRM и т.д.).

Так, например, на предприятиях Ford внедрена система контроля температуры и давления с использованием интеллектуальных браслетов, которые автоматически передают информацию в централизованную базу. Система анализирует полученные данные, выявляет риски и информирует руководителей подразделений.

В компании Toyota применяются технологии искусственного интеллекта, позволяющие не только фиксировать физиологические показатели, но и оценивать эмоциональное состояние сотрудников на основе анализа голоса, выражения лица и поведения. Такая информация используется для персонализированной настройки условий труда.

В России передовые практики в данной области демонстрируют такие предприятия, как КАМАЗ, ГАЗ, Москвич и др. Например, на КАМАЗе реализован проект по созданию электронных медицинских карт работников с доступом через защищённый веб-интерфейс. Данные вводятся либо вручную врачом, либо импортируются из внешних источников, включая результаты лабораторных исследований.

В таблице 2 приведен результат сравнения отечественных и международных решений цифрового мониторинга здоровья.

Таблица 2 – Сравнение отечественных и международных решений цифрового мониторинга здоровья

Параметр	**Международные компании**	**Отечественные предприятия**
Компании	Toyota, Ford	КамАЗ, ГАЗ, Москвич
Тип мониторинга	Автоматизированный, непрерывный	Комбинированный
Используемые устройства	Носимые браслеты, трекеры, сенсоры	Термометры, тонометры, носимые браслеты
Сбор данных	Автоматический, в реальном времени	Вручную или полуавтоматически
Применение ИИ и аналитики	Анализ рисков, прогнозирование, оценка настроения	Ограниченное применение аналитики
Безопасность данных	Многоуровневая, соответствует международным стандартам	Защита по российским стандартам
Интерфейс доступа	Веб-платформы, мобильные приложения	Веб-интерфейсы
Фокус на психоэмоциональном состоянии	Присутствует анализ поведения, голоса, мимики	Отсутствуют или только на стадии тестирования
Уровень зрелости решений	Высокий, зрелые и масштабируемые системы	Средний, системы развиваются точечно

Как видно из анализа, международные решения демонстрируют более высокий уровень автоматизации, интеграции и использования аналитики. Российские предприятия находятся на стадии активного внедрения цифровых инструментов, однако чаще применяют комбинированный подход, сочетающий ручной ввод данных и начальные формы автоматизации. Тем не менее, отечественные компании демонстрируют устойчивый тренд к развитию в сторону комплексных цифровых платформ.

1.5 Цели, задачи и ожидаемый эффект от автоматизации

Основной целью внедрения информационной системы мониторинга здоровья сотрудников на предприятии является создание надёжного, доступного и масштабируемого цифрового решения, которое позволит

обеспечить всесторонний контроль за состоянием здоровья работников, своевременно реагировать на отклонения от нормы и формировать обоснованные управленческие решения.

На рисунке 3 изображена диаграмма вариантов использования (UseCase diagram).

Рисунок 3 – Представление диаграммы вариантов использования

Задачи, реализуемые в рамках проекта:

- Создание единой базы данных медицинских показателей сотрудников.
- Организация безопасного доступа к информации в соответствии с ролевой моделью.
- Внедрение алгоритмов анализа и визуализации данных.
- Обеспечение взаимодействия с существующими информационными системами предприятия.
- Поддержка формирования отчётности в автоматизированном режиме.

Ожидаемый эффект:

- Повышение оперативности принятия решений в части охраны труда и здоровья;
- Снижение рисков производственного травматизма и заболеваний;

- Уменьшение нагрузки на персонал медицинской службы;
- Повышение прозрачности и обоснованности решений руководства.

На рисунке 4 представлена диаграмма целей и задач проекта.

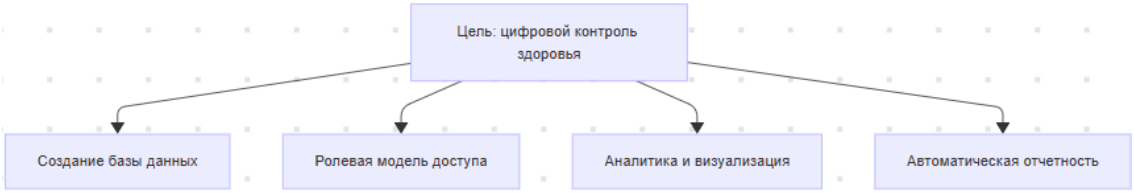

Рисунок 4 – Диаграмма целей и задач проекта

Исходя из представленной на рисунке диаграммы, можно увидеть основные цель и задачи разрабатываемой системы мониторинга и анализа показателей здоровья. Основная цель – это цифровой контроль здоровья, которая включает в себя создание базы данных, организацию ролевой модели доступа, обеспечение возможности аналитики и ее визуализации, а также, возможность автоматической отчетности по показателям.

1.6 Обоснование выбора технологий

Выбор технологий для реализации программного обеспечения является одним из важнейших этапов проектирования любой информационной системы. Он определяет не только архитектурную основу решения, но и напрямую влияет на его стабильность, безопасность, масштабируемость и дальнейшую поддерживаемость. В условиях, когда проект ориентирован на долгосрочное использование в корпоративной среде, критически важно использовать зрелые, надёжные и хорошо документированные инструменты.

Spring Boot выбран в качестве основы для серверной части системы. Это современный Java-фреймворк, широко применяемый при создании корпоративных веб-приложений. Он предоставляет богатый набор готовых решений для реализации REST API, интеграции с базами данных, настройки

безопасности, логирования, обработки ошибок и других задач, связанных с построением надёжного серверного приложения. Благодаря принципу «конфигурации по умолчанию» (convention over configuration), Spring Boot существенно сокращает количество шаблонного кода и ускоряет процесс разработки.

MySQL используется как основная система управления базами данных. MySQL — это зрелая и проверенная временем СУБД, которая поддерживает все основные функции реляционной модели: первичные и внешние ключи, транзакции, индексы, процедуры, представления и многое другое. Она позволяет эффективно хранить структурированные данные, обеспечивать их целостность и быстрое извлечение при необходимости. Кроме того, MySQL легко интегрируется с Java-приложениями через библиотеку Spring Data JPA, которая упрощает взаимодействие с базой данных.

Thymeleaf — это HTML-шаблонизатор, ориентированный на работу в рамках Spring MVC. Он позволяет создавать динамические страницы с учётом ролей пользователей, языка интерфейса, состояния форм и других аспектов взаимодействия. Одним из его преимуществ является возможность предварительного просмотра шаблонов в браузере, что ускоряет разработку и тестирование интерфейса.

На рисунке 5 показана архитектура системы.

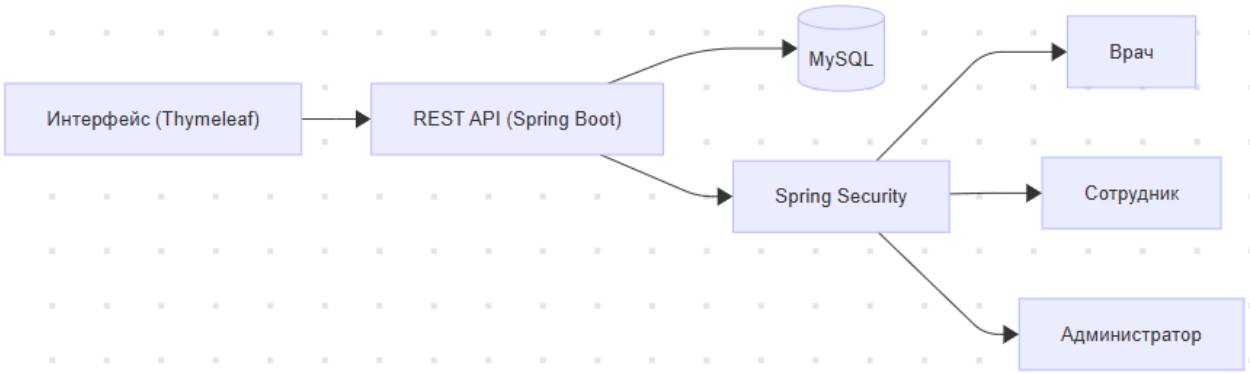

Рисунок 5 – Архитектура системы

На представленном рисунке можно увидеть спроектированную архитектуру системы мониторинга и анализа показателей здоровья. В разработке использовался паттерн проектирования MVC(model, view, controller). Интерфейс был разработан при помощи шаблонизатора thymeleaf и языков верстки HTML 5 и CSS 3. REST API разработан с использованием фреймворка Spring Boot, а база данных была разработана в среде MySQL,

1.7 Анализ требований заказчика

В рамках предварительного этапа проекта был проведён сбор требований от заинтересованных сторон, включая медицинскую службу, ИТ-отдел и отдел охраны труда. На основе проведённых интервью и анализа текущих бизнес-процессов сформулирован перечень функциональных и нефункциональных требований.

Функциональные требования:

- Возможность ввода данных о физиологических показателях сотрудников: температура тела, артериальное давление, пульс, уровень сахара.
- Просмотр истории показателей с возможностью фильтрации по дате и типу параметра.
- Сигнализация при отклонении от нормы с формированием уведомления.
- Поддержка ролей: «Сотрудник» (ввод данных), «Врач» (просмотр всех данных), «Администратор» (настройка системы, управление пользователями).
- Построение графиков и формирование отчетов.

Нефункциональные требования:

- Высокая надёжность хранения данных;
- Простота и удобство пользовательского интерфейса;
- Возможность масштабирования при увеличении числа пользователей;
- Соответствие законодательству в части защиты персональных данных.

1.7.1 Методология сбора требований

Процесс формирования и анализа требований к системе осуществлялся по комплексной методологии, включающей последовательные этапы исследовательской работы. На первом этапе организована серия глубинных интервью с ключевыми заинтересованными сторонами, в ходе которой проведено 12 структурированных собеседований с представителями различных подразделений предприятия. В выборку вошли три сотрудника медицинской службы, отвечающие за профилактические осмотры и ведение медицинской документации, два специалиста ИТ-отдела, курирующие корпоративные информационные системы, два представителя отдела охраны труда, а также пять линейных руководителей производственных подразделений.

Для обеспечения полноты и достоверности собранных данных применялись современные техники бизнес-анализа: метод user story mapping позволил визуализировать end-to-end сценарии взаимодействия пользователей с системой, сессии мозгового штурма способствовали выявлению скрытых потребностей, а анонимное анкетирование обеспечило сбор объективных данных о проблемных точках существующих процессов.

Параллельно проведен детальный анализ текущих бизнес-процессов с изучением материальных артефактов: бумажных журналов периодических медосмотров за последние года, электронных отчетов в формате Excel за 2023-2024 годы, а также регламентов реагирования на чрезвычайные происшествия и несчастные случаи на производстве. Особое внимание уделено выявлению узких мест и несоответствий в существующих процедурах мониторинга здоровья персонала.

Систематизация полученных требований выполнена с применением методики MoSCoW, предполагающей четкое ранжирование по четырем категориям приоритета. В категорию Must have включены критические функциональные требования, без реализации которых система не сможет

выполнять свои основные функции. Группа Should have содержит важные, но не обязательные на первом этапе функции, Could have объединяет желательные улучшения, а Won't have - перспективные идеи, реализация которых запланирована на будущие версии продукта. Такой подход позволил сформировать сбалансированный бэклог разработки с четкими критериями приоритезации.

1.7.2 Верификация требований

В ходе разработки системы был реализован комплексный подход к верификации функциональных и нефункциональных требований. Основным инструментом проверки пользовательских требований стало прототипирование интерфейсов в среде Figma, где дизайн-команда последовательно провела три полноценные итерации согласования с ключевыми стейкхолдерами проекта. Каждая итерация включала детальный разбор рабочих процессов, уточнение элементов навигации и оптимизацию пользовательских сценариев. Для объективной оценки удобства интерфейсов были организованы юзабилити-тесты с участием 10 репрезентативных пользователей из разных подразделений предприятия, что позволило выявить и устранить проблемные моменты взаимодействия на ранних этапах разработки.

Параллельно с технической верификацией проводился полноценный юридический аудит системы, включавший два ключевых направления проверки. Первое направление - тщательный анализ соответствия системы требованиям Федерального закона №152-ФЗ «О персональных данных», в ходе которого эксперты проверили все аспекты обработки медицинской информации: от порядка сбора данных до механизмов их хранения и уничтожения. Второе критически важное направление - сертификация средств криптографической защиты информации (СКЗИ), в рамках которой специалисты аккредитованного центра провели тестирование алгоритмов

шифрования, проверили реализацию механизмов электронной подписи и удостоверились в корректности работы системы управления криптографическими ключами. Результаты аудита подтвердили полное соответствие системы установленным нормативным требованиям.

1.7.5 Матрица приоритетов

На этапе анализа требований к создаваемой информационной системе мониторинга здоровья работников АвтоВАЗа был составлен перечень ключевых функциональных и нефункциональных требований. Поскольку ресурсы проекта (время, бюджет, команда) ограничены, необходимо определить, какие из этих требований являются критически важными, какие — желательными, и какие могут быть отложены до следующей итерации разработки.

Для этого применяется матрица приоритетов, которая позволяет упорядочить требования по степени их важности (приоритета) и сложности реализации. Это помогает проектной команде принять обоснованные архитектурные и организационные решения, а также эффективно управлять разработкой и внедрением.

В системе приоритизации использованы следующие категории: Must (обязательное) – требование должно быть реализовано в первой версии системы, иначе она не сможет выполнять свои основные функции. Should (желательное) – реализация данного требования значительно повысит удобство, эффективность или масштабируемость, но оно может быть отложено. Could (возможно) – полезное, но необязательное улучшение, которое будет реализовано при наличии времени и ресурсов. Won’t (не планируется) – в текущем релизе реализовано не будет.

Сложность реализации требований оценивалась с позиции технической трудоёмкости и потребности в дополнительных ресурсах. Low – низкая сложность, может быть реализовано силами 1–2 разработчиков за короткий

срок. Medium – средняя сложность, требует внимательной проработки архитектуры и тестирования. High – высокая сложность, может потребовать изменений в архитектуре, дополнительных нагрузочных тестов и подготовки инфраструктуры.

Ниже приведена таблица 3 — Матрица приоритетов требований с пояснениями.

Таблица 3 – Матрица приоритетов требований к системе мониторинга.

ID	Требование	Приоритет	Сложность	Пояснение
1	Ввод основных показателей	Must	Low	Является базовым функционалом системы.
2	Система уведомлений о превышении норм	Must	Medium	Требуется для быстрого реагирования врачей на отклонения в показателях.
3	Поддержка нагрузки от 2000+ пользователей	Should	High	Необходима для масштабирования, но не критична на начальном этапе.
4	Интеграция с носимыми устройствами	Could	High	Функция, связанная с дополнительными API и оборудованием.
5	Ведение истории измерений	Must	Medium	Аналитика позволяет выявлять динамику состояния работника.
6	Ролевая модель доступа	Must	Medium	Требуется для обеспечения безопасности.
7	Формирование отчётов за период	Should	Medium	Важно для медицинских и кадровых служб.
8	Интерфейс администратора	Must	Low	Базовая административная функция.
9	Тематическая цветовая индикация отклонений	Could	Low	Повышает удобство восприятия, может быть добавлена на этапе шлифовки UI.
10	Поддержка мултиязычного интерфейса	Won’t	High	Не входит в рамки текущей версии, не актуально для локального внедрения.

Исходя из построенной матрицы приоритетов, можно отметить требования с высоким приоритетом, такие как:

– Ввод основных показателей

– Система уведомлений о превышении норм
– Ведение истории измерений
– Ролевая модель доступа
– Интерфейс администратора

1.8 Сравнительный анализ альтернативных технологий

В процессе проектирования рассматривались альтернативные технологические стеки: Node.js + MongoDB, Django + PostgreSQL, Laravel + MySQL. Однако они были отклонены в пользу связки Spring Boot + MySQL + Thymeleaf на основе следующих критериев.

В таблице 4 показан результат сравнения технологических стеков.

Таблица 4 – Сравнение технологических стеков

Платформа	**Безопасность**	**Поддержка**	**Производительность**	**Простой ввод**
Spring Boot	Высокая	Отличная	Высокая	Да
Django (Python)	Высокая	Хорошая	Средняя	Да
Node.js + MongoDB	Средняя	Хорошая	Высокая	Нет

В результате анализа и сравнения альтернативных технологических стеков, было принято окончательное решение об использовании фреймворка Spring Boot в разработке, так как он отвечает всем необходимым требованиям и мой уровень знания этого фреймворка соответсвует тому, чтобы разработать конечный требуемый продукт.

1.9 Обеспечение безопасности и защиты персональных данных

1.9.1 Актуальность защиты медицинских данных

Медицинские данные сотрудников представляют собой особую категорию конфиденциальной информации, требующую повышенных мер защиты в соответствии с действующим законодательством. В Российской Федерации обработка таких данных строго регулируется Федеральным законом №152-ФЗ «О персональных данных», который устанавливает базовые требования к их сбору, хранению и использованию. Для организаций, осуществляющих трансграничную передачу данных, дополнительно применяются положения General Data Protection Regulation (GDPR), устанавливающие жесткие стандарты защиты персональных данных на территории Европейского союза. Особые требования к медицинской информации содержатся в Федеральном законе №323 «Об охране здоровья граждан», который конкретизирует порядок работы с данными о состоянии здоровья граждан.

Несоблюдение установленных нормативными актами требований влечет за собой серьезные последствия различного характера. В правовом аспекте организации могут столкнуться с существенными штрафными санкциями, размер которых согласно Кодексу об административных правонарушениях РФ может достигать 6 миллионов рублей за грубые нарушения. Не менее значимыми являются репутационные риски, поскольку утечка медицинских данных способна нанести непоправимый ущерб имиджу компании как работодателя. Особую опасность представляет возможность использования конфиденциальной медицинской информации для дискриминации сотрудников по состоянию здоровья, что противоречит не только нормам трудового права, но и базовым этическим принципам.

В таблице 5 описаны правовые аспекты защиты медицинских данных.

Таблица 5 – Правовые аспекты защиты медицинских данных

Нормативный акт	**Сфера регулирования**	**Ответственность за нарушения**
Федеральный закон №152-ФЗ «О персональных данных»	Общие требования к обработке персональных данных	Штрафы до 6 млн руб., приостановка деятельности
GDPR (General Data Protection Regulation)	Защита данных граждан	Штрафы до 4% глобального оборота компании
Федеральный закон №323 «Об охране здоровья граждан»	Особенности работы с медицинскими данными	Дисциплинарная, административная и уголовная ответственность
Трудовой кодекс РФ	Защита персональных данных работников	Компенсация морального вреда, восстановление нарушенных прав

Реализация эффективной системы защиты медицинских данных требует комплексного подхода, учитывающего как технические аспекты информационной безопасности, так и организационные меры по соблюдению нормативных требований. Особое значение приобретает разработка четких регламентов доступа к медицинской информации, проведение регулярного обучения сотрудников и внедрение современных технологических решений для обеспечения конфиденциальности.

1.9.2 Архитектура безопасности с использованием MySQL

Система безопасности построена по принципу многоуровневой защиты, где каждый уровень обеспечивает комплексную защиту данных. На физическом уровне серверное оборудование размещается в специализированных дата-центрах, соответствующих международным стандартам безопасности Tier III+, что гарантирует бесперебойную работу и защиту от несанкционированного физического доступа. Для обеспечения отказоустойчивости реализована система регулярного резервного копирования с использованием комбинации mysqldump для полных бэкапов и

бинарных логов (binlog) для point-in-time восстановления, что позволяет минимизировать потери данных в случае аварии.

На сетевом уровне все соединения с системой защищены современными криптографическими протоколами, где обязательное использование HTTPS с TLS 1.2+ обеспечивает шифрование передаваемых данных и аутентификацию сервера. Для административного доступа к критически важным компонентам системы настроены защищенные VPN-туннели с двухфакторной аутентификацией, что исключает возможность перехвата учетных данных при удаленном управлении.

Уровень приложения защищен с помощью Spring Security, где реализована JWT-аутентификация с коротким временем жизни токенов (30 минут) и механизмом их автоматического обновления.

Защита базы данных MySQL начинается с тщательно продуманной схемы данных, где каждая таблица имеет строгие ограничения целостности, проверочные условия (CHECK constraints) и внешние ключи для обеспечения реляционной целостности. Реализована система регулярных аудитов доступа с ведением детализированных логов всех операций CRUD, которые хранятся в отдельной защищенной базе аудита и позволяют отслеживать любые подозрительные действия в режиме реального времени.

На рисунке 6 приведена схема компонентов MySQL.

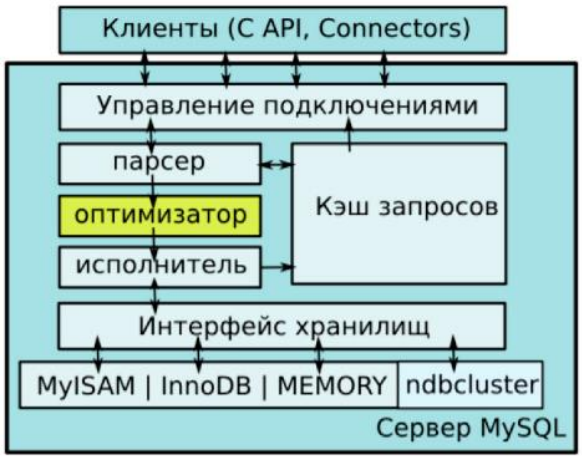

Рисунок 6 – Компоненты MySQL

Для критически важных таблиц настроены триггеры, которые фиксируют все изменения данных с указанием пользователя и временной метки.

1.9.3 Соответствие стандартам

Разработанная система мониторинга здоровья сотрудников полностью соответствует международным и российским стандартам информационной безопасности. Основой для построения защищенной архитектуры стал международный стандарт ISO/IEC 27001, который определяет требования к системе менеджмента информационной безопасности. В рамках соответствия этому стандарту в системе реализованы политики управления доступом, процедуры реагирования на инциденты и непрерывный мониторинг безопасности.

Для случаев интеграции с платежными системами при оформлении медицинских страховок или других финансовых операций система соответствует строгим требованиям стандарта безопасности данных индустрии платежных карт PCI DSS. Это включает в себя защиту хранимых данных, шифрование передаваемой информации и регулярное тестирование систем безопасности. Особое внимание уделено защите конфиденциальных данных при их передаче между различными компонентами системы.

На национальном уровне система разработана с учетом требований российского стандарта ГОСТ Р 57580.1-2017 «Безопасность финансовых организаций», который устанавливает дополнительные требования к защите персональных данных и обеспечению информационной безопасности. Соответствие данному стандарту подтверждено в ходе независимого аудита, проведенного аккредитованной организацией. Реализованные механизмы защиты обеспечивают выполнение всех нормативных требований российского законодательства в области обработки и хранения персональных данных.

1.9.4 Сравнительный анализ мер безопасности

Разработка информационных систем, содержащих персональные медицинские данные сотрудников, требует особого внимания к вопросам информационной безопасности. Учитывая действующее законодательство (в том числе Федеральный закон № 152-ФЗ «О персональных данных»), а также внутренние стандарты информационной безопасности предприятия, необходимо реализовать комплексный подход к защите данных от актуальных угроз.

Ниже представлен сравнительный анализ основных потенциальных угроз и соответствующих им защитных механизмов, применяемых в разрабатываемой системе.

Потеря данных. Одной из наиболее критичных угроз при работе с медицинскими данными является возможность их полной или частичной потери. Это может произойти в результате сбоев оборудования, программных ошибок, ошибок в логике бизнес-процессов, а также вследствие внешнего вмешательства (вредоносного ПО или хакерской атаки).

Для защиты от данной угрозы используются такие меры, как транзакционность (ACID) — все операции с данными в базе данных (в нашем случае — MySQL) выполняются в рамках транзакций, что обеспечивает их атомарность, согласованность, изолированность и долговечность. Это означает, что либо операция будет выполнена полностью, либо не будет выполнена вообще, предотвращая «разрывы» в целостности информации и резервное копирование и репликация — регулярное автоматическое копирование базы данных (бэкап) и настройка зеркальных копий (реплик) позволяет в случае аварии быстро восстановить состояние системы без потери данных.

Несанкционированный доступ может возникнуть как вследствие внешнего вмешательства, так и из-за внутренних уязвимостей: ошибок настройки, отсутствия разграничения прав, утерянных паролей и т.п.

Противодействие данной угрозе реализуется через ролевую модель доступа — каждому пользователю системы назначается определённая роль (сотрудник, врач, администратор), которая строго ограничивает его доступ только к тем данным и функциям, которые ему необходимы. Например, работник не может просматривать чужие медицинские записи, а врач не может изменять настройки безопасности и использование представлений (VIEWs) — при необходимости ограниченного доступа к отдельным полям или таблицам базы данных создаются виртуальные таблицы (VIEWs), в которых можно выбрать только те данные, которые разрешено видеть конкретной группе пользователей.

SQL-инъекции – это одна из наиболее распространенных уязвимостей веб-приложений, при которой злоумышленник внедряет в запрос SQL-команды с целью несанкционированного доступа или изменения данных.

Противодействие осуществляется за счёт Prepared Statements (подготовленные выражения) — используются во всех точках взаимодействия с базой данных. Эти выражения позволяют отделить SQL-команды от пользовательского ввода, исключая возможность внедрения вредоносного кода и хранимых процедур, которые позволяют вынести ключевую бизнес-логику на уровень базы данных, где можно заранее определить допустимые действия и обезопасить работу с критически важной информацией.

Перехват данных при передаче. Передача данных между клиентом и сервером, особенно в медицинских системах, должна быть защищена от подслушивания и перехвата злоумышленниками (например, в публичных сетях Wi-Fi или при MITM-атаках).

Для защиты от данной угрозы применяются такие подходы, как SSL-соединения (HTTPS) — весь обмен данными между клиентом (браузером) и сервером осуществляется по зашифрованному каналу, используя защищённые сертификаты. Это делает перехват и расшифровку информации практически невозможными и шифрование столбцов — в некоторых случаях (например, хранение паспортных данных, адресов, телефонов) возможно дополнительное

шифрование отдельных полей базы данных. Доступ к ним осуществляется только при наличии соответствующих прав и ключей.

Таким образом, в разработке системы мониторинга состояния здоровья реализован многоуровневый подход к безопасности, включающий как защиту на уровне приложения, так и меры на уровне базы данных и канала передачи данных. Это обеспечивает соответствие нормативным требованиям, высокую устойчивость к типовым атакам и защищенность персональной медицинской информации сотрудников предприятия.

В таблице 6 приведен полный анализ угроз.

Таблица 6 – Анализ угроз

Угроза	**Возможные последствия**	**Применяемые защитные меры**
Потеря данных	Утрата медицинской информации, срыв анализа	– Транзакционность (ACID) – Регулярное резервное копирование – Репликация БД
Несанкционированный доступ	Доступ к личным данным сотрудников	- Ролевая модель доступа - Представления в MySQL - Ограничение по IP и ролям
SQL-инъекции	Изменение/удаление данных, обход авторизации	– Prepared Statements (подготовленные выражения) – Хранимые процедуры
Перехват данных	Утечка персональных данных, нарушение конфиденциальности	– Шифрование трафика (SSL/HTTPS) – Шифрование столбцов в БД (например, AES)

В приведенной таблице указан полный перечень возможных угроз для системы мониторинга показателей здоровья. Используемые в разработке инструменты и теоретические знания помогли решить и исключить возможность возникновения представленных угроз.

1.10 Перспективы развития системы

Разработанная система мониторинга здоровья обладает значительным потенциалом для дальнейшего развития и масштабирования. В рамках будущих обновлений планируется реализация интеграционных решений с современными носимыми устройствами, включая умные браслеты, цифровые тонометры и интеллектуальные термометры, что позволит автоматизировать процесс сбора физиологических показателей сотрудников в режиме реального времени.

На рисунке 7 представлена схема перспективных направлений развития системы.

Рисунок 7 – Перспективные направления развития системы

Для повышения доступности системы запланирована разработка кроссплатформенного мобильного приложения с поддержкой операционных систем Android и iOS, которое обеспечит сотрудникам удобный доступ к своим медицинским данным и инструментам самоконтроля. Дополнительный функционал будет включать модуль для проведения регулярных опросов и анкетирования, позволяющий оценивать субъективные показатели самочувствия и психоэмоционального состояния персонала.

1.11 Экономическая эффективность

Методика расчета включает:

- Разработка ПО: зарплата разработчиков, тестировщиков, аналитиков.
- Инфраструктура: серверы, базы данных, хостинг.

- Поддержка и обслуживание.

Расчет затрат:

- Разработка (3 разработчика × 5 месяцев × 150 тыс. руб.) = 2,25 млн руб.
- Серверные мощности (100 тыс. руб. в год).
- Итоговые затраты: ~2,35 млн руб.

Ожидаемая выгода:

- Снижение количества несвоевременно выявленных заболеваний.
- Повышение эффективности медицинского мониторинга.
- Улучшение условий труда и снижение рисков для здоровья.

Выводы по первой главе:

Проведённый анализ предметной области, обзор существующих решений, а также исследование текущего состояния процессов медицинского контроля на предприятии АвтоВАЗ позволили сделать ряд важных выводов.

Во-первых, обеспечение контроля за состоянием здоровья работников на производстве — неотъемлемая часть системы охраны труда и профилактики профессиональных заболеваний. Особенно это актуально для предприятий с повышенным уровнем физической или психоэмоциональной нагрузки, к числу которых относится АвтоВАЗ. Поддержание здоровья персонала напрямую влияет на производительность труда, снижение числа аварийных ситуаций и общий уровень безопасности на производстве.

Во-вторых, анализ существующих подходов на других промышленных предприятиях показал наличие положительного опыта внедрения информационных систем для мониторинга физиологических показателей. Такие системы позволяют собирать, хранить и обрабатывать медицинские данные в реальном времени, формировать отчеты и проводить аналитический контроль, что значительно повышает оперативность и обоснованность принимаемых решений.

В-третьих, текущее состояние системы медицинского контроля на предприятии АвтоВАЗ всё ещё в значительной степени опирается на

устаревшие методы — ручной ввод данных, бумажные журналы, отсутствие единой базы данных. Это ведёт к множеству недостатков, включая:

- высокую трудоёмкость процедур регистрации и анализа информации;
- невозможность оперативного реагирования на отклонения от нормы;
- сложности при формировании статистической и аналитической отчётности;
- повышенный риск ошибок из-за человеческого фактора.

В-четвёртых, учитывая общую тенденцию к цифровизации производственной среды и внедрению ИТ-решений в систему корпоративного управления, разработка и внедрение автоматизированной информационной системы мониторинга здоровья работников представляется своевременной и целесообразной мерой**.** Такая система обеспечит:

- оперативный сбор и хранение физиологических показателей (пульс, давление, температура);
- аналитическую обработку данных и визуализацию изменений;
- настройку пороговых значений и автоматическую генерацию тревожных сигналов;
- разграничение доступа в зависимости от ролей (работник, врач, администратор);
- интеграцию в существующую ИТ-инфраструктуру предприятия.

Таким образом, проект полностью соответствует стратегии модернизации предприятия**,** в том числе в части внедрения элементов «умного производства», цифровых двойников и комплексных информационно-аналитических систем. Создание подобной системы будет способствовать не только улучшению условий труда, но и формированию культуры профилактики и ответственного отношения к здоровью**.**

2 Методологические основы мониторинга медицинских показателей работников промышленных предприятий

2.1 Подходы к мониторингу физиологических параметров в условиях промышленных предприятий

Мониторинг физиологических показателей здоровья сотрудников — важный элемент системы производственной медицины и охраны труда. Для предприятий с высокими физическими или психоэмоциональными нагрузками, таких как АвтоВАЗ, постоянное наблюдение за ключевыми параметрами состояния здоровья позволяет выявлять ранние признаки отклонений, снижать риск профессиональных заболеваний и предотвращать несчастные случаи.

К основным показателям, подлежащим регулярному контролю, относятся:

- Пульс — отражает работу сердечно-сосудистой системы и является одним из базовых индикаторов общего состояния организма.
- Артериальное давление (АД) — позволяет оценить нагрузку на сосудистую систему и выявлять гипертонию, гипотонию и нестабильность кровообращения.
- Температура тела — может свидетельствовать о наличии воспалительных процессов, вирусных заболеваний, перегреве и т.д.

В таблице 7 приведены основные параметры, подлежащие контролю.

Таблица 7 – Основные параметры, подлежащие контролю

Параметр	**Допустимый диапазон**	**Частота измерений**
Пульс	60-100 уд./мин	Один раз в смену
Артериальное давление	90/60 – 140/90 мм рт. ст.	Один раз в смену
Температура тела	36.1 – 37.2 °C	Один раз в смену

Методы мониторинга данных параметров делятся на:

- Ручные — значения фиксируются медицинским персоналом в рамках плановых осмотров или по сигналу от самого сотрудника.
- Автоматизированные — используются устройства (например, носимые трекеры, цифровые тонометры, термометры с передачей данных), интегрированные в информационную систему предприятия.

На рисунке 8 показана диаграмма процесса обработки данных в автоматизированной системе мониторинга.

Рисунок 8 – Диаграмма процесса обработки данных в автоматизированной системе мониторинга

На практике автоматизация позволяет снизить нагрузку на медперсонал, исключить человеческий фактор при фиксации данных и обеспечить оперативную аналитику в реальном времени. Система, разработанная для АвтоВАЗа, предполагает ручной ввод данных медицинским персоналом, что обусловлено необходимостью соблюдения достоверности и

контролируемости измерений, но в будущем может быть расширена с учетом интеграции устройств IoT.

Реализация эффективной системы требует:

- Формирования структурированной базы данных медицинских показателей;
- Настройки механизмов тревожной сигнализации при выходе параметров за допустимые пределы;
- Хранения исторических данных для анализа тенденций и отклонений;
- Защиты медицинской информации согласно требованиям законодательства.

Важную роль в формировании системы играет аналитический модуль**,** позволяющий проводить расчеты средних значений, выявлять тренды и аномалии. Это особенно актуально при длительном наблюдении за работниками, чья деятельность связана с вредными или опасными производственными факторами.

Кроме того, современная практика проектирования подобных систем предусматривает внедрение ролевой модели доступа**,** в рамках которой работник имеет доступ только к своим данным, врач — ко всем медицинским записям, а администратор — к техническим параметрам и управлению пользователями.

Таким образом, системный подход к мониторингу показателей здоровья персонала позволяет не только своевременно реагировать на отклонения, но и формировать более безопасную производственную среду, ориентированную на профилактику, а не на последствия.

2.2 Применение информационных моделей и архитектурных решений в системах медицинского мониторинга

Создание программной системы мониторинга состояния здоровья требует выбора соответствующей архитектуры и моделей данных, способных обеспечить масштабируемость, отказоустойчивость и безопасность.

В рамках данного проекта реализована трехуровневая архитектура**,** включающая:

- Уровень представления (frontend) — реализован с использованием HTML/CSS, обеспечивает интерфейс для пользователей системы (врачи, сотрудники).
- Уровень логики приложения (backend) — на основе Spring Boot, реализует бизнес-логику, обработку данных, авторизацию и валидацию.
- Уровень хранения данных (база данных MySQL) — отвечает за долговременное хранение показателей, истории измерений и учетных записей.

Для описания предметной области и проектирования структуры системы использовалась объектно-ориентированная модель**,** где основными сущностями являются:

- User (Пользователь)
- Measurement (Измерение)
- Role (Роль: сотрудник, врач, администратор)

В таблице 8 приведен пример разграничения доступа.

Таблица 8 – Пример разграничения доступа

Роль	**Просмотр своих данных**	**Просмотр чужих данных**	**Изменение данных**	**Доступ к аналитике**
Работник	✓	✗	✗	✗
Врач	✓	✓	✓	✓
Админ	✓	✓	✓	✓

Для визуализации данных и аналитики применяются:

- Графики и диаграммы (например, изменения температуры за неделю)
- Механизмы фильтрации и поиска по дате, пользователю, типу отклонений
- Автоматические уведомления при превышении допустимых значений

Одной из ключевых задач разработки является обеспечение безопасности хранения и передачи данных. В частности, реализованы следующие меры:

- Аутентификация пользователей с помощью Spring Security
- Разграничение прав доступа в зависимости от роли
- Шифрование паролей и конфиденциальных данных
- Защита от CSRF и XSS атак

В таблице 9 описаны меры обеспечения безопасности.

Таблица 9 – Меры обеспечения безопасности

Мера защиты	**Описание**
Аутентификация	Вход по логину и паролю с различными ролями доступа
Шифрование	Передача и хранение данных осуществляется в зашифрованном виде
Логирование действий пользователей	Журналирование изменений и попыток доступа
Разграничение прав	Отдельные уровни доступа для работников, врачей и администраторов

Также в рамках разработки была учтена возможность расширения функционала. Система легко масштабируется за счет модульной структуры backend-приложения.

Выводы по второй главе:

Во второй главе дипломной работы были систематизированы методологические основы мониторинга медицинских показателей работников промышленных предприятий, а также проведено детальное проектирование архитектуры информационной системы для АвтоВАЗа.

Были определены ключевые физиологические параметры, подлежащие контролю: пульс, артериальное давление и температура тела. Установлены допустимые диапазоны значений и частота измерений, что позволило сформировать требования к системе. Особое внимание уделено необходимости адаптации мониторинга к условиям промышленного предприятия, включая учет уровня физической и психоэмоциональной нагрузки сотрудников.

Проведённый анализ подтвердил критическую важность автоматизации сбора и обработки данных. Ручные методы, используемые на предприятии, обладают значительными недостатками: высокий риск ошибок, задержки в обработке информации и отсутствие оперативной аналитики. Разработанная система устраняет эти проблемы за счёт:

- Централизованного хранения данных в базе MySQL.
- Автоматической генерации уведомлений при отклонениях от нормы.
- Интеграции аналитических инструментов для выявления тенденций и аномалий.

Система построена по трехуровневой модели:

- Frontend: интерфейсы для пользователей (HTML, CSS, Thymeleaf).
- Backend: бизнес-логика на Spring Boot (обработка данных, авторизация, REST API).
- База данных: MySQL для надежного хранения медицинских записей.

Такая архитектура обеспечивает масштабируемость, отказоустойчивость и безопасность.

Учтены требования законодательства (ФЗ №152, GDPR) и реализованы меры защиты:

- Ролевая модель доступа (сотрудник, врач, администратор).
- Шифрование данных (SSL, AES).
- Защита от SQL-инъекций и CSRF-атак.
- Регулярное резервное копирование и аудит действий.

Внедрение системы позволит повысить оперативность реагирования на отклонения в состоянии здоровья, снизить нагрузку на медицинский персонал, улучшить условия труда за счёт профилактики профессиональных заболеваний и обеспечить соответствие нормативным требованиям.

Намечены направления для дальнейшей модернизации:

- Интеграция с носимыми устройствами (IoT) для автоматического сбора данных.
- Разработка мобильного приложения для сотрудников.
- Внедрение модуля психоэмоционального мониторинга.

Таким образом, вторая глава не только обосновала выбор технологий и архитектуры, но и продемонстрировала, как система мониторинга здоровья может трансформировать существующие процессы на предприятии.

Реализованные решения сочетают техническую надежность, соответствие законодательству и практическую пользу для всех пользователей — от рядовых сотрудников до руководства. Это создает прочную основу для реализации системы в третьей главе и её последующего внедрения.

3 Моделирование мнформационной системы мониторинга состояния здоровья работников АвтоВАЗа

3.1 Цели и задачи моделирования

Моделирование информационной системы (ИС) мониторинга состояния здоровья работников АвтоВАЗа направлено на формализацию логики функционирования и взаимодействия компонентов системы, а также определение требований к архитектуре, данным и интерфейсам. Целями моделирования являются:

- анализ логики бизнес-процессов;
- формализация требований к структуре данных и интерфейсам;
- обеспечение визуального представления процессов сбора, хранения и анализа медицинских показателей;
- определение архитектурных решений, обеспечивающих безопасность, надежность и масштабируемость системы.

Задачи моделирования:

- построение структурной и функциональной модели информационной системы;
- разработка информационной модели, отражающей структуру базы данных;
- описание пользовательских интерфейсов и взаимодействия ролей (рабочий, врач, администратор);
- моделирование сценариев контроля и обработки данных.

3.2 Архитектура системы

ИС мониторинга состояния здоровья строится по трехуровневой архитектуре:

- Клиентский уровень (frontend): обеспечивает взаимодействие пользователя с системой через веб-интерфейс, реализованный с использованием HTML, CSS и Thymeleaf.
- Серверный уровень (backend): реализован на базе Spring Boot, содержит бизнес-логику, REST API и модули обработки данных.
- Уровень хранения данных: представлена базой данных MySQL, содержащей коллекции с персональными и медицинскими данными пользователей.

На рисунке 9 представлена обобщенная архитектура системы.

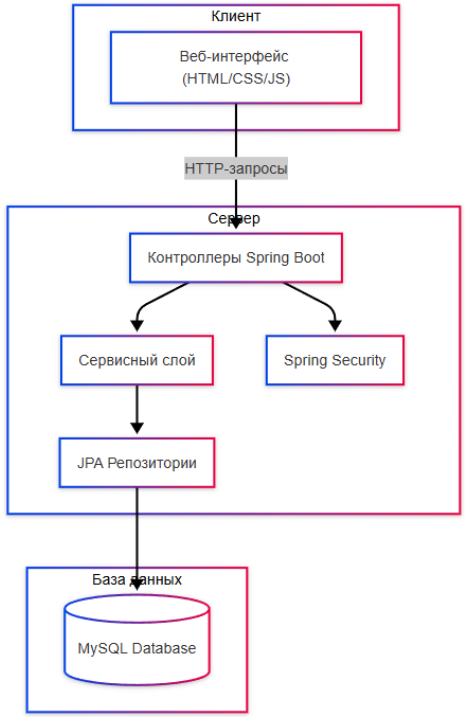

Рисунок 9 – Обобщенная архитектура системы

Исходя из представления модели архитектуры разрабатываемой системы, можно увидеть, что разрабатываемы продукт имеет клиент-серверную архитектуру.

3.3 Информационная модель

Также, была разработана информационная модель системы, которая включает в себя описание сущностей и связей между ними.

В таблице 10 представлены основные сущности и их атрибуты.

Таблица 10 – Основные сущности информационной системы

Сущность	**Атрибуты**
Пользователь	ID, ФИО, роль, логин, пароль
Медицинская запись	ID, дата, пульс, давление, температура, пользователь
Уведомление	ID, дата, тип, текст, связанная запись

В приведенной таблице описаны основные сущности и их атрибуты. Всего в системе есть три основные сущности, это пользователь, медицинская запись (включающая в себя измерения) и уведомления.

На рисунке 10 представлена ER-диаграмма базы данных.

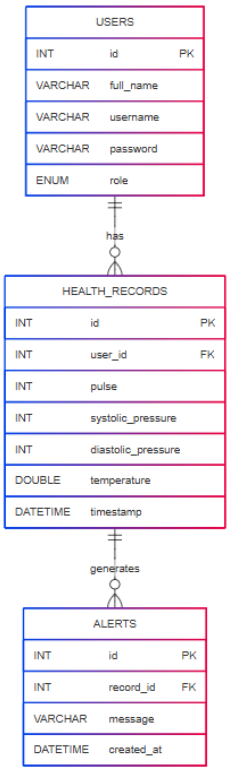

Рисунок 10 – ER-диаграмма базы данных

На представленном выше рисунке изображено схематическое представление базы данных, т.е. сущности с атрибутами и связи между ними.

Также, была разработана диаграмма классов системы мониторинга, для визуального отображения разработанных классов и их взаимосвязей.

На рисунке 11 показана разработанная диаграмма классов системы мониторинга.

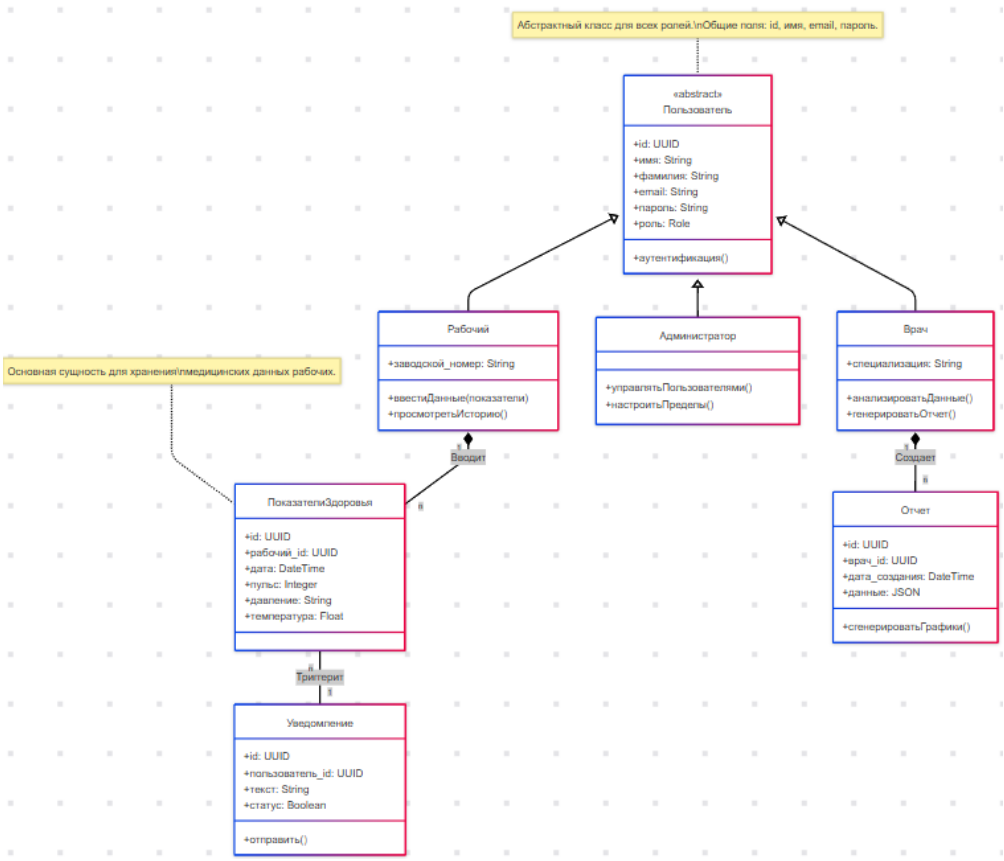

Рисунок 11 – Представление диаграммы классов

Исходя из представленной иллюстрации, можно выделить классы сущностей и сервисов, репозитории на диаграмме классов не представлены.

3.4 Модель пользовательских ролей и доступов

В системе реализованы три основные роли:

- Рабочий — вводит свои данные, просматривает историю и графики;
- Врач — имеет доступ ко всем записям работников, проводит анализ;
- Администратор — управляет учетными записями и контролирует корректность работы системы.

Таблица 11 показывает распределение прав доступа.

Таблица 11 – Права доступа пользователей

Действие	**Рабочий**	**Врач**	**Администратор**
Ввод медицинских данных	Да	Нет	Нет
Просмотр своих данных	Да	Да	Да
Просмотр чужих данных	Нет	Да	Да
Управление учетными записями	Нет	Нет	Да
Формирование отчетов	Нет	Да	Да

В представленной таблице прав доступа пользователей можно увидеть, что самым привелегированным является администратор системы, это сделано для того, чтобы ничего не мешало корректному администрированию разработанной системы мониторинга показателей здоровья после пилотного запуска.

Врач имеет меньше прав доступа, но все они так или иначе соответсвуют полному набору функционала для комфортного и эффективного использования системы, т.е. из ограничений есть только ввод медицинских данных, пока врач использует систему не в роли обычного сотрудника предприятия «АвтоВАЗ», ему не нужно вводить свои медицинские данные.

Наименее привелегированным является рабочий, или же сотрудник предприятия. Все доступные ему функции соответсвуют набору функционала для автоматизации процесса сбора медицинских показателей здоровья.

3.5 Моделирование обработки контрольного примера

Для демонстрации работы системы рассмотрим пример:

- Рабочий Иванов И.И. вводит данные: пульс — 105, давление — 150/100, температура — 37.8;
- Система сравнивает показатели с допустимыми нормами;
- Обнаружено отклонение: пульс > 100, давление выше нормы;
- Генерируется предупреждение, отображающееся врачу и в интерфейсе работника.

Результаты обработки:

- Медицинская запись сохраняется в базе;
- Врач получает уведомление;
- Рабочему отображается рекомендация пройти обследование.

Выводы по третьей главе:

В третьей главе была разработана архитектура программной системы мониторинга состояния здоровья работников предприятия АО «АВТОВАЗ». Определена структура взаимодействия компонентов клиентской и серверной частей приложения, реализованных с использованием технологии Spring Boot и базы данных MySQL. Предложена многоуровневая архитектура, обеспечивающая безопасность, масштабируемость и удобство поддержки системы.

Сформирована информационная модель предметной области, отражающая сущности пользователей, медицинских показателей и тревожных уведомлений. На основе модели спроектирована ER-диаграмма базы данных, учитывающая реляционные связи между таблицами и соответствующие ограничения. Представленные схемы обеспечивают надежное хранение и последующую обработку медицинских данных работников.

Заключение

В рамках дипломной работы была разработана система мониторинга состояния здоровья работников АО «АВТОВАЗ», ориентированная на контроль таких параметров, как температура тела, артериальное давление и пульс. Были рассмотрены актуальные подходы к построению подобных систем с учетом требований к защите персональных медицинских данных, пользовательского интерфейса и хранения информации.

Разработка выполнена с применением технологий Java Spring Boot, MySQL и HTML/Thymeleaf. Реализована система авторизации с разграничением ролей (работник, врач, администратор), обеспечена возможность хранения истории измерений и аналитики с визуализацией данных в виде графиков.

Проведен анализ функциональных требований, архитектурных решений, построена информационная модель проекта. Разработана база данных, интерфейсы для пользователей разных категорий, а также контрольный пример с демонстрацией функциональности системы. Обоснована экономическая целесообразность разработки и внедрения системы на предприятии.

Разработанное программное обеспечение может быть использовано в медицинских пунктах промышленных предприятий и модернизировано под специфику других организаций. Полученные результаты создают основу для дальнейших исследований и разработок в области цифрового мониторинга здоровья и промышленной медицины.

Список используемой литературы и используемых источников

1. Бобров, А.А. Современное программирование на Java: от основ до многопоточности / А.А. Бобров. – М.: Наука, 2021. – 312 с.
2. Бёрнс, Б., Мондриан, А. Книга Java EE 8. Enterprise Edition для профессионалов. – СПб.: Питер, 2019. – 608 с.
3. ГОСТ 7.0.5–2008. Библиографическая ссылка. Общие требования и правила составления. – М.: Стандартинформ, 2009. – 16 с.
4. Григорьев, С.Н. Java в разработке web-приложений / С.Н. Григорьев. – М.: Вильямс, 2021. – 416 с.
5. Гущин, И.С. Разработка и тестирование REST API на Spring Boot / И.С. Гущин. – М.: ДМК Пресс, 2022. – 286 с.
6. Дмитриев, П.Н. Принципы построения безопасных систем / П.Н. Дмитриев. – М.: Лаборатория знаний, 2022. – 288 с.
7. Дьяков, А.А. Информационные технологии и программирование в задачах здравоохранения / А.А. Дьяков. – М.: ГЭОТАР-Медиа, 2022. – 214 с.
8. Ермаков, А.И. Защита персональных данных: теория и практика / А.И. Ермаков. – М.: РГУ нефти и газа, 2019. – 218 с.
9. Ермолаев, В.И. Проектирование программных систем: архитектура, шаблоны, безопасность / В.И. Ермолаев. – М.: Юрайт, 2023. – 404 с.
10. Ильин, К.С. Основы медицинской информатики / К.С. Ильин. – М.: ГЭОТАР-Медиа, 2021. – 240 с.
11. Кан, Г. Проектирование интерфейсов / Г. Кан. – М.: Эксмо, 2020. – 336 с.
12. Кормушин, А.С. Информационная безопасность: учебник / А.С. Кормушин. – М.: Юрайт, 2021. – 426 с.
13. Мартин, Р. Чистая архитектура / Р. Мартин. – М.: Питер, 2021. – 320 с.

14. Мартынов, Е.Ю. Проектирование микросервисной архитектуры / Е.Ю. Мартынов. – СПб.: Питер, 2023. – 340 с.

15. Матюхин, В.И. Архитектура программных систем / В.И. Матюхин. – М.: Академия, 2018. – 334 с.

16. Мельников, П.Н. Архитектура корпоративных систем: принципы проектирования / П.Н. Мельников. – М.: Бином, 2022. – 256 с.

17. Никитин, И.В. Методы и технологии анализа больших данных / И.В. Никитин. – М.: Наука, 2022. – 312 с.

18. Носов, К.С. Безопасность веб-приложений на Spring Security / К.С. Носов. – М.: ДМК Пресс, 2023. – 368 с.

19. Носов, К.С. Spring Security. Полное руководство / К.С. Носов. – М.: ДМК Пресс, 2023. – 362 с.

20. Орлов, Д.В. Современные базы данных: MySQL, PostgreSQL и SQLite / Д.В. Орлов. – СПб.: БХВ-Петербург, 2021. – 296 с.

21. Сидоров, А.И. Spring Boot в действии. Практическое руководство / А.И. Сидоров. – СПб.: Питер, 2022. – 384 с.

22. Сидоров, А.И. Spring Boot на практике / А.И. Сидоров. – СПб.: Питер, 2021. – 320 с.

23. Снитко, А.А. Проектирование баз данных / А.А. Снитко. – СПб.: БХВ-Петербург, 2020. – 348 с.

24. Соколов, М.И. Анализ требований в разработке ПО / М.И. Соколов. – М.: ДМК Пресс, 2018. – 304 с.

25. Тарасов, С.В. Современные методы визуализации медицинских данных / С.В. Тарасов. – СПб.: Политехника, 2020. – 254 с.

26. Федеральный закон РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г.

27. Фролов, И.П. Практика применения Hibernate и Spring Data JPA / И.П. Фролов. – М.: ДМК Пресс, 2021. – 310 с.

28. Шапошников, А.С. Проектирование и разработка информационных систем: учеб. пособие / А.С. Шапошников. – М.: ФОРУМ, 2020. – 288 с.

29. Ярошенко, Е.Н. MySQL. Полное руководство / Е.Н. Ярошенко. – М.: ДМК Пресс, 2022. – 384 с.

30. Bostock, M. Data-Driven Documents (D3.js) Documentation – [Электронный ресурс]. – Режим доступа: [https://d3js.org/], свободный.

31. Freeman, E. Head First Design Patterns / E. Freeman, E. Robson. – 2nd ed. – O'Reilly Media, 2020. – 694 p.

32. Health Level Seven International. HL7 FHIR Specification. – [Электронный ресурс]. – Режим доступа: [https://www.hl7.org/fhir/], свободный.

33. ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements.

34. ISO/TS 82304-2:2021. Health software – Part 2: Health and wellness apps – Quality and reliability.

35. McKinney, W. Python for Data Analysis / W. McKinney. – 3rd ed. – O'Reilly Media, 2022. – 528 p.

36. MySQL Manual. – [Электронный ресурс]. – Режим доступа: [https://www.MySQL.com/docs/manual/], свободный.

37. Nielsen, J. Usability Engineering / J. Nielsen. – San Diego: Academic Press, 1993. – 362 p.

38. NIST. Cybersecurity Framework – [Электронный ресурс]. – Режим доступа: [https://www.nist.gov/cyberframework], свободный.

39. OWASP Foundation. OWASP Top 10 – [Электронный ресурс]. – Режим доступа: [https://owasp.org/www-project-top-ten/], свободный.

40. Spring Boot Reference Documentation. – [Электронный ресурс]. – Режим доступа: [https://docs.spring.io/spring-boot/docs/current/reference/html/], свободный.

Приложение А

Исходный код приложения

```
package com.avtovaz.health_monitoring;

import org.springframework.boot.SpringApplication;
import
org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class HealthMonitoringApplication {

    public static void main(String[] args) {
        SpringApplication.run(HealthMonitoringApplication.class,
args);
    }

}
```

Рисунок А.1 – Класс Main(HealthMonitoringApplication)

```
package com.avtovaz.health_monitoring.repository;

import com.avtovaz.health_monitoring.entity.HealthRecord;
import org.springframework.data.jpa.repository.JpaRepository;

import java.util.List;

public interface HealthRecordRepository extends
JpaRepository<HealthRecord, Long> {
    List<HealthRecord> findByEmployeeId(String employeeId);
}
```

Рисунок А.2 – Репозиторий(HealthRecordRepository)

```
package com.avtovaz.health_monitoring.config;

@Configuration
@EnableWebSecurity
public class SecurityConfig {

    @Bean
    public SecurityFilterChain securityFilterChain(HttpSecurity
http) throws Exception {
        http
```

```
                .authorizeHttpRequests(auth -> auth
                        .requestMatchers("/", "/login", "/css/",
"/js/").permitAll()
                        .anyRequest().authenticated()
                )
                .formLogin(form -> form
                        .loginPage("/login")
                        .defaultSuccessUrl("/health")
                        .permitAll()
                )
                .logout(logout -> logout
                        .logoutSuccessUrl("/login?logout")
                        .permitAll()
                );
        return http.build();
    }

    @Bean
    public UserDetailsService userDetailsService() {
        UserDetails user = User.withDefaultPasswordEncoder()
                .username("admin")
                .password("password")
                .roles("USER")
                .build();
        return new InMemoryUserDetailsManager(user);
    }
}
```

Рисунок А.3 – Конфигурация безопасности(SecurityConfig)

```
package com.avtovaz.health_monitoring.config;

import org.springframework.context.annotation.Bean;
import org.springframework.context.annotation.Configuration;
import org.thymeleaf.extras.java8time.dialect.Java8TimeDialect;
import org.thymeleaf.spring6.SpringTemplateEngine;
import
org.thymeleaf.templateresolver.ClassLoaderTemplateResolver;
import org.thymeleaf.templateresolver.ITemplateResolver;

@Configuration
public class ThymeleafConfig {

    @Bean
    public ITemplateResolver templateResolver() {
        ClassLoaderTemplateResolver templateResolver = new
```

```
ClassLoaderTemplateResolver();
        templateResolver.setPrefix("templates/");
        templateResolver.setSuffix(".html");
        templateResolver.setTemplateMode("HTML");
        templateResolver.setCharacterEncoding("UTF-8");
        return templateResolver;
    }

    @Bean
    public SpringTemplateEngine templateEngine() {
        SpringTemplateEngine templateEngine = new
SpringTemplateEngine();
        templateEngine.setTemplateResolver(templateResolver());
        templateEngine.addDialect(new Java8TimeDialect());
        return templateEngine;
    }
}
```

Рисунок А.4 – Конфигурация шаблонизатора(ThymeleafConfig)

```
package com.avtovaz.health_monitoring.controller;

import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.GetMapping;

@Controller
public class LoginController {

    @GetMapping("/login")
    public String login() {
        return "login";
    }

    @GetMapping("/")
    public String home() {
        return "redirect:/health";
    }
}
```

Рисунок А.5 – Контроллер входа(LoginController)

Приложение Б

Пользовательский интерфейс

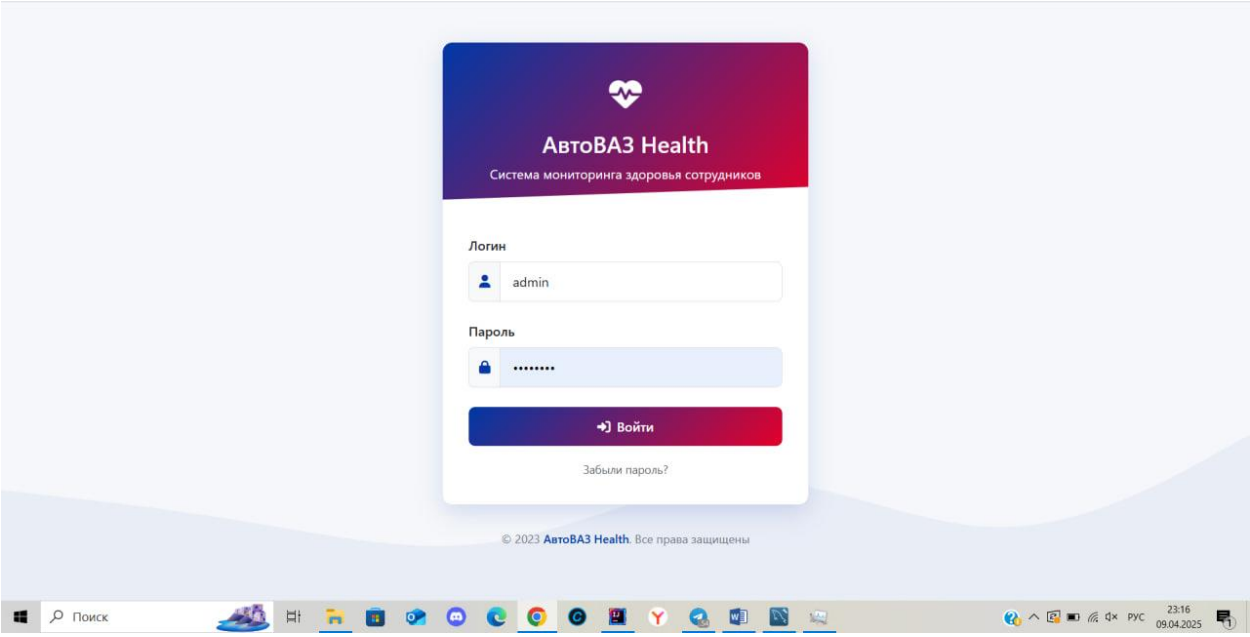

Рисунок Б.1 – Страница входа

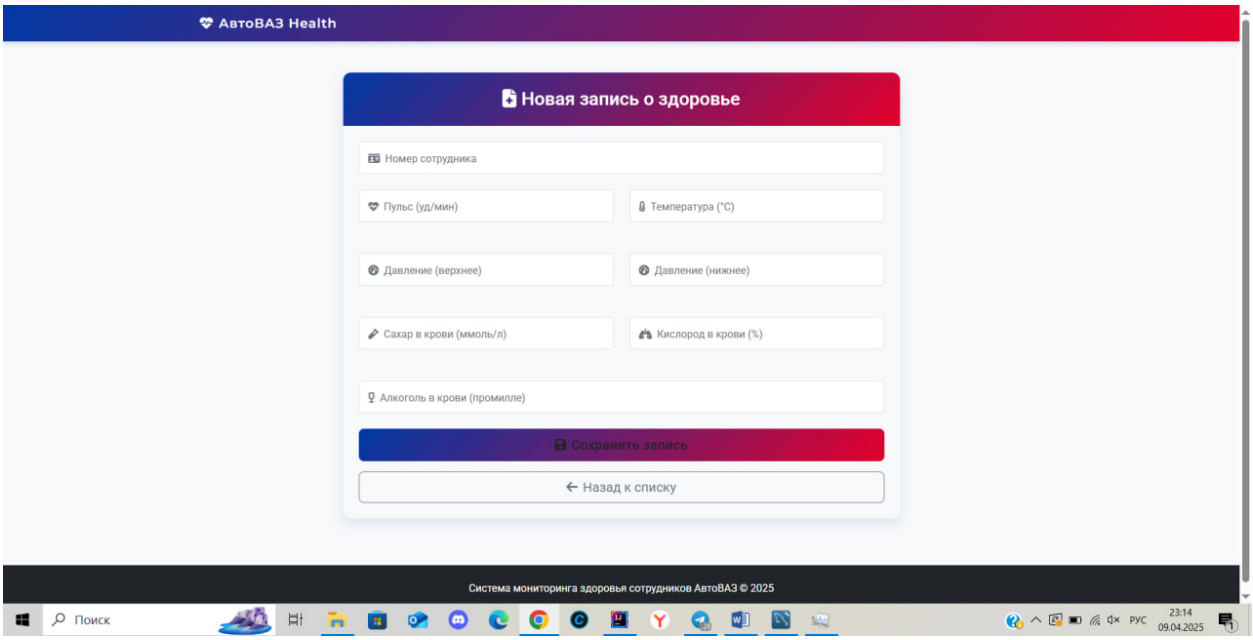

Рисунок Б.2 – Страница добавления записи

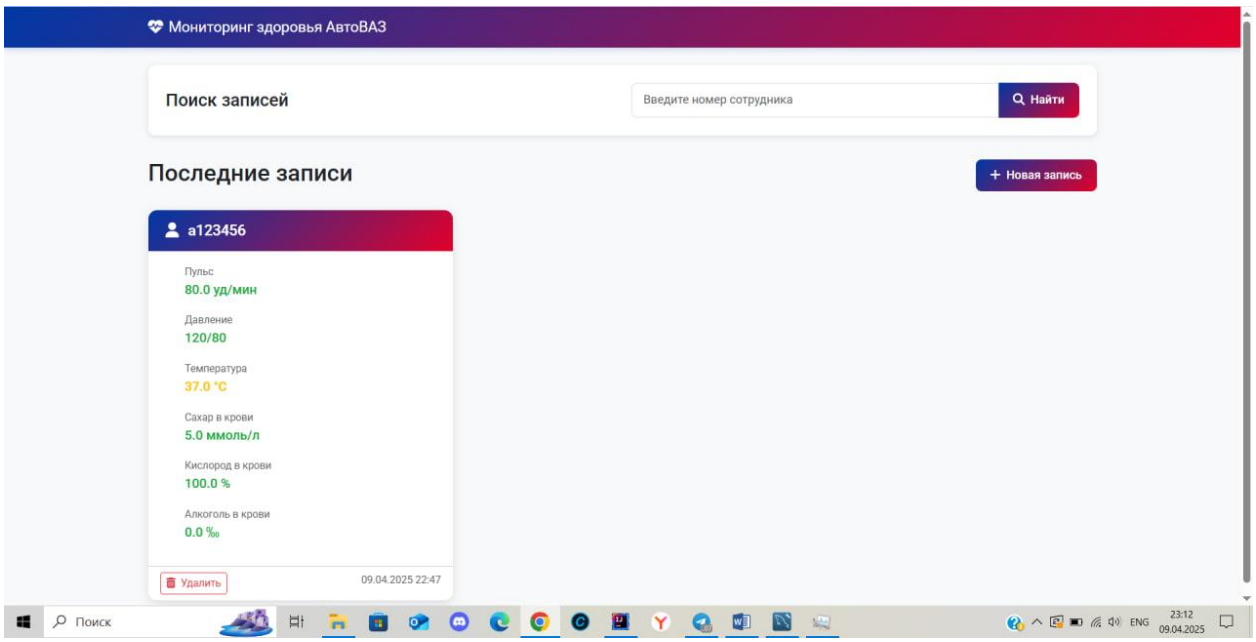

Рисунок Б.3 – Страница отображения списка всех записей