МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

Кафедра системного анализа и
автоматического управления

# РАЗРАБОТКА ПРИЛОЖЕНИЯ НА МИКРОСЕРВИСНОЙ АРХИТЕКТУРЕ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студентки 5 курса 551 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Мишуниной Евы Вадимовны

Научный руководитель
к. ф.-м. н., доцент _____ И. Е. Тананко

Заведующий кафедрой
к. ф.-м. н., доцент _____ И. Е. Тананко

Саратов 2025

# ВВЕДЕНИЕ

**Актуальность темы.** Современное программное обеспечение сталкивается с большим количеством задач, связанных с масштабируемостью, надежностью и безопасностью. Одним из передовых подходов для их решения является использование микросервисной архитектуры. Микросервисы позволяют разбить приложения на отдельные, управляемые компоненты, что обеспечивает гибкость разработки, упрощение сопровождения и масштабируемость системы.

**Цель бакалаврской работы** – разработка программного обеспечения на основе микросервисной архитектуры в защищенном исполнении, используя такие технологии, как Spring Boot, Spring Cloud и Docker. Код будет написан на Java, что дает возможности для использования обширного и мощного инструментария для создания надежных и устойчивых к сбоям приложений.

Поставленная цель определила **следующие задачи**:

- изучение и анализ подходов к реализации микросервисной архитектуры;
- исследование принципов и практик разделения приложения на микросервисы;
- анализ существующих решений и библиотек для обеспечения коммуникации и координации между микросервисами;
- разработка и внедрение микросервисного приложения с использованием Spring Boot и Spring Cloud;
- проектирование и реализация нескольких микросервисов, обеспечивающих выполнение различных функциональных задач;
- организация взаимодействия между микросервисами с использованием Spring Cloud;
- обеспечение защищенного исполнения микросервисного приложения с использованием Docker;
- создание и настройка Docker-контейнеров для каждого микросервиса;
- обеспечение безопасности микросервисного взаимодействия и защиты данных при их передаче между контейнерами;
- анализ нормативно-правовых актов в сфере информационной безопасности;
- разработка документации по безопасности.

При выполнении данной выпускной квалификационной работы основное внимание будет уделено практическим аспектам разработки и внедрения микросер-

висной архитектуры, а также вопросам обеспечения безопасности и надежности системы. Результаты работы могут быть полезны для разработчиков программного обеспечения и специалистов, занимающихся проектированием и поддержкой распределенных систем.

**Методологические основы** разработки программного обеспечения в защищенно исполнении представлены в работах С. Ньюмена, Р. Митра, А. Хоффман.

**Теоретическая и практическая значимость бакалаврской работы**. Теоретическая значимость данной бакалаврской работы заключается в углубленном исследовании вопросов безопасности микросервисной архитектуры, что является актуальной темой. При разработке приложения с использованием особое внимание уделено вопросам угроз и уязвимостей. В работе была разработана комплексная документация по безопасности, что способствует пониманию процессов обеспечения защиты персональных данных и противодействия различным видам атак.

Практическая значимость работы проявляется в контексте перехода российских компаний на отечественное программное обеспечение, что обусловлено как требованиями государства, так и необходимостью повышения уровня защищенности данных в условиях современных киберугроз. Разработка приложения на основе микросервисной архитектуры с внедрением систем безопасности и механизмов контроля доступа, предоставляет реальные решения для бизнес-структур, стремящихся улучшить защиту своих данных. Кроме того, практическое применение полученных результатов может способствовать улучшению безопасности и эффективности функционирования отечественных информационных систем, что в свою очередь влияет на повышение доверия к внутреннему ПО со стороны пользователей и компаний, создавая таким образом условия для более широкого внедрения современных технологий.

**Структура и объем работы**. Бакалаврская работа состоит из введения, трех разделов, заключения, списка использованных источников и одного приложения. Общий объем работы – 50 страниц, из них 43 страницы – основное содержание, включая 13 рисунков и одну таблицу, цифровой носитель в качестве приложения, список использованных источников информации – 22 наименования.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

**Первый раздел «Анализ актуальности выпускной квалификационной работы»** посвящен обзору микросервисной архитектуры, преимуществам и недостаткам микросервисной архитектуры, обзору нормативно-правовой базы РФ в области безопасности персональных данных.

**Преимущества микросервисной архитектуры:**

- Высокая отказоустойчивость: при выходе из строя одного из сервисов, все остальные остаются в строю. Таким образом, неполадки в отдельных сервисах не помешают всему рабочему процессу;
- Гибкость: можно быстро внедрить новую технологию. Это будет значительно быстрее и, при неудаче, отменить изменения просто. Меняя локально один из сервисов, мы не рискуем всей системой, и время, требующееся для изменений, меньше;
- Простота: чем меньше кода (а каждый отдельный сервис представляет собой цельную систему), тем проще и быстрее программистам разобраться в работе приложения;
- Лёгкость выведения написанного кода в работу: небольшое количество кода обеспечивает быстрое развертывание;
- Масштабируемость: самые необходимые и нужные сервисы можно дополнить и расширить, когда появится такая необходимость. Вся система при этом остается прежней.

Разработка приложений требует соблюдения норм и стандартов, касающихся безопасности данных. В условиях постоянного роста числа киберугроз и утечек информации, вопросы защиты персональных данных становятся особенно актуальными. Поэтому в данном разделе представлен обзор нормативно правовой базы Российской Федерации, регулирующей безопасность персональных данных. Это важно, так как при разработке приложения с акцентом на защиту информации, необходимо учитывать все действующие законы и требования, которые могут влиять на архитектуру и реализацию приложения. Обзор нормативных актов позволит не только глубже понять текущие стандарты безопасности, но и обосновать выбор определенных технологий и подходов, обеспечивающих соответствие законодательным требованиям и защиту данных пользователей.

По сравнению с монолитной, микросервисная архитектура обладает боль-

шей гибкостью и возможностью независимого масштабирования отдельных сервисов. Проще вносить локальные изменения в код без риска для всей системы, но взамен этого возрастает сложность взаимодействия между сервисами, а понимание законодательной базы оказывает значительное влияние на разработку приложения и его архитектурные решения.

**Второй раздел** «Практическое описание» посвящен рассмотрению архитектуры разрабатываемого приложения и обеспечение его информационной безопасности. Раздел включает в себя описания архитектурных решений и используемого программного обеспечения, а также какие технологические инструменты были выбраны для реализации проекта. Во второй части раздела разобраны аспекты информационной безопасности, которые являются необходимыми для защиты приложения и его пользователей, рассмотрено, какие меры были приняты для обеспечения безопасного и стабильного функционирования системы, а также выбор конкретных механизмов защиты.

В процессе разработки приложения была выбрана микросервисная архитектура, поскольку она предоставляет значительные преимущества по сравнению с монолитной. Проект включает несколько систем, которые могут функционировать независимо друг от друга, что требует обеспечения их автономной работы и взаимодействия.

Приложение занимается автоматизацией бухгалтерского и кадрового учета, что является главным аспектом управления любой организацией. Оно предназначено для упрощения и оптимизации бизнес-процессов, связанных с учетом рабочего времени, расчетами заработной платы и управлением информацией о персонале. Система принимает на себя функции, которые обычно выполняют бухгалтеры и кадровики, позволяя автоматизировать различные задачи, снижая вероятность ошибок и увеличивая производительность. Основными пользователями системы будут бухгалтеры, сотрудники кадровой службы и администраторы, которые непосредственно занимаются управлением данными о сотрудниках и ведением бухгалтерского учета.

Необходимость реализации мер информационной безопасности в разрабатываемом веб-приложении, обусловлена требованиями мер защиты информации. Программа позволяет реализовывать меры защиты персональных данных, описанные в 21 приказе ФСТЭК России.

Для достижения какого-то определенного УЗ ПДн необходимо реализо-

вать дополнительные меры. В комплекте с информационной системы поставляется документация, позволяющая обеспечить УЗ4.

— Акт определения уровня защищенности ПДн.
— Модель угроз безопасности информации.
— Согласие на обработку персональных данных.
— Ролевая модель разграничения прав.

**Третий раздел** «Демонстрация разработанного приложения и документации по безопасности» посвящен подробной демонстрации разработанного ПО, а так же документации, обеспечивающей многослойный подход к безопасности персональных данных.

Приложение построено на микросервисной архитектуре и включает в себя 8 микросервисов:

1. Сервис бухгалтерского учёта (Accounting-service): этот сервис отвечает за все аспекты бухгалтерского учета.
2. Кадровый сервис (Staff-service): отвечает за управление кадровыми данными сотрудников. Он реализует функциональность, позволяющую добавлять новых сотрудников, просматривать информацию о действующих работниках, а также отслеживать и контролировать рабочее время.
3. Пользовательский сервис (Users-service): является основой системы авторизации и аутентификации пользователей. Он использует JSON Web Tokens (JWT) для безопасной передачи и хранения информации о пользователях. Кроме того, реализовано хэширование паролей в базе данных, что обеспечивает дополнительный уровень безопасности. Users-service управляет ролями пользователей, определяя, какие права и доступ к определенным сервисам должен иметь каждый пользователь.
4. Административный сервис (Admin-service): предназначен для мониторинга и аудита работы всей системы.
5. Config-service: выполняет важную функцию централизованного управления конфигурациями для других сервисов. Он предоставляет общие настройки и конфигурационные параметры, которые могут быть запрашиваемы другими сервисами.
6. Eureka-server: является сервером обнаружения сервисов от Netflix, который позволяет различным компонентам системы автоматически регистрироваться и находить друг друга. Он управляет регистрацией и обнов-

лением информации о доступных сервисах, помогая избегать проблем с маршрутизацией и обеспечением доступности.

7. Show-service: представляет собой фронтенд приложения с пользовательским интерфейсом (UI). Оно отвечает за отображение информации для пользователей и взаимодействие с другими сервисами.
8. Gateway: служит центральной точкой доступа ко всем микросервисам. Он управляет маршрутизацией запросов от клиентов к соответствующим сервисам, обеспечивая контроль доступа, защиту и обработку запросов.

В ходе выполнения выпускной квалификационной работы была разра ботана документация, обеспечивающая многослойный подход к безопасности персональных данных:

1. Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных. Акт определения уровня защищенности персональных данных (ПДн), составляется после сбора и оценки характеристик и особенностей эксплуатации информационной системы, использующей персональную информацию.
2. Модель угроз безопасности информации: содержит список всех возможных угроз. Также включает описание вероятных сценариев реализации и выводы об актуальности угроз.
3. Согласие на обработку персональных данных (ПДн), разработано согласно федеральному закону от 27.07.2006 №152-ФЗ .
4. Ролевая модель разграничения прав содержит набор прав и разрешений для различных категорий пользователей (ролей) системы. Роли зависят от должностей, специфики отделов компании, типов рабочих задач. Количество полномочий, входящих в роли, не регламентируется строго — каждому сотруднику можно назначить как одно полномочие, так и несколько.

# ЗАКЛЮЧЕНИЕ

Микросервисная архитектура, как современный подход к разработке программного обеспечения, поражает своей гибкостью, надежностью и способностью к масштабированию. В условиях растущих требований к продуктивности и безопасности систем, данный метод позволяет преодолеть многие технические трудности. Введение в выпускную квалификационную работу показало актуальность использования микросервисов для создания сложных и хорошо управляемых приложений.

Цель работы заключалась в разработке программного обеспечения на основе микросервисной архитектуры, с учётом защищённого исполнения и использования передовых технологий, таких как Spring Boot, Spring Cloud и Docker. Мы исследовали разнообразные аспекты микросервисной архитектуры и проанализировали существующие решения для коммуникации и координации между микросервисами. Так же мы успешно внедрили комплексную политику безопасности, которая включает в себя идентификацию и оценку рисков, привлечение внимания к вопросу защиты данных на всех уровнях организации. Благодаря четкому распределению ролей и ответственностей, мы обеспечили должный контроль доступа к информации, минимизировав риски несанкционированного доступа и утечки данных.

В ходе выполнения работы были решены следующие задачи:

— Изучение и анализ подходов к реализации микросервисной архитектуры позволили глубже понять принципы, лежащие в основе данной методологии разработки.
— Исследование принципов и практик разделения приложения на микросервисы обеспечило основу для дальнейшей разработки.
— Анализ существующих решений и библиотек для обеспечения коммуникации между микросервисами дал возможность выбрать оптимальные инструменты для нашего проекта.
— Разработка микросервисного приложения с использованием Spring Boot и Spring Cloud позволили создать структурированную и легко масштабируемую систему.
— Проектирование и реализация нескольких микросервисов, отвечающих за разные функциональные задачи, привели к созданию модульного и гибкого приложения.

— Организация взаимодействия между микросервисами с использованием Spring Cloud гарантировала корректную и эффективную коммуникацию.
— Обеспечение защищенного исполнения микросервисного приложения с использованием Docker помогло создать надёжную среду выполнения.
— Создание и настройка Docker-контейнеров для каждого микросервиса способствовали улучшению портативности и управляемости приложения.
— Обеспечение безопасности микросервисного взаимодействия и защиты данных при их передаче между контейнерами повысило уровень доверия к системе.
— Внедрение журналирования, шифрования данных и защиты подключения.
— Разработка документации: Мы создали полное руководство по безопасности, которое включает все процессы и процедуры по защите данных.

Таким образом, достигнутые результаты не только соответствуют требованиям законодательства, но и соответствуют современным стандартам в области информационной безопасности. Результаты выпускной квалификационной работы обладают практической значимостью и могут быть полезны широкомукругу специалистов, занимающихся разработкой и поддержкой программного обеспечения. Они демонстрируют возможности и преимущества микросервисной архитектуры и позволяют лучше понять её место в современной разработке программных систем.

**Основные источники информации:**


1. Ньюмен, С. Создание микросервисов / С. Ньюмен.— СПб: Питер, 2023.— 624 с.
2. Митра, Р. Микросервисы. От архитектуры до релиза / Р. Митра.— СПб.:Питер, 2023.— 336 с.
3. Хоффман, А. Безопасность веб-приложений. Разведка, защита, нападение / А. Хоффман.— Астана: Спиннк Бук, 2025.— 432 с.
4. Методический документ ФСТЭК России .Методика оценки угроз безопасности информации..—М.: ФСТЭК России, 2015.
5. Приказ Федеральной службы по техническому и экспортному контролю. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. 8 февраля 2013 года №21 // —М.: ФСТЭК России, 2015.