Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Выпускная квалификационная работа бакалавра

Система авторизации инфраструктурных сервисов

Студент: Васильев А. И. ИУ7-82Б
Научный руководитель: Клорикьян П. В.

Цели и задачи работы

Цель: реализация программно-алгоритмического комплекса для авторизации запросов в инфраструктурные сервисы.

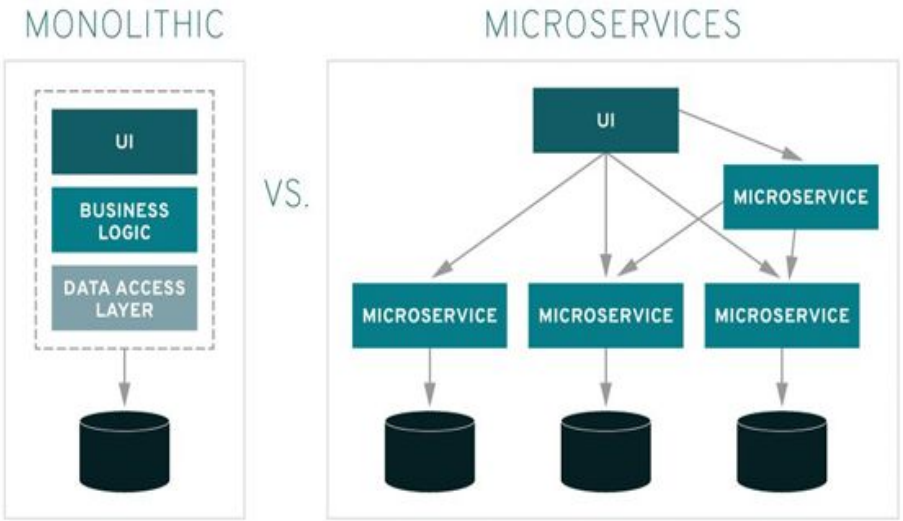
Задачи:

1. Провести обзор предметной области, существующих решений, подходов к аутентификации и авторизации в микросервисной архитектуре.
2. Разработать и описать ключевые алгоритмы работы программно-алгоритмического комплекса, реализующего аутентификацию и авторизацию запросов в инфраструктурные сервисы.
3. Провести исследование влияния работы авторизации на время выполнения запросов в инфраструктурные сервисы.

Обзор предметной области

Микросервисная архитектура – архитектурный подход к разработке программного обеспечения, при котором оно состоит из небольших слабо связанных сервисов.

Инфраструктурный сервис предоставляет базовый функционал для работы сервисов с бизнес-логикой. Пример – база данных.



<u>Решаемая проблема</u> – запросы из сервисов с бизнес-логикой в инфраструктурные должны быть авторизованы во избежании несанкционированного доступа.

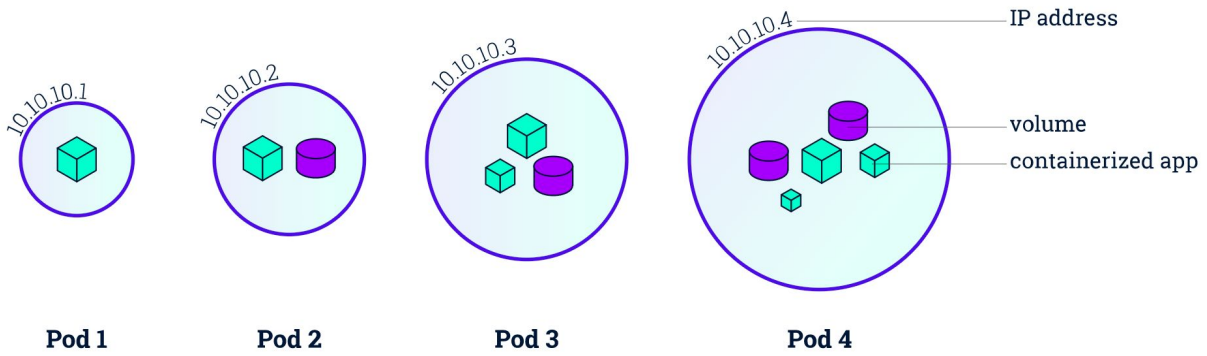
Kubernetes и сайдкар контейнер

Kubernetes (k8s) – система для управления приложениями в изолированных друг от друга контейнерах.

Под – представляет собой группу из одного или нескольких контейнеров приложения, совместно использующие ресурсы.

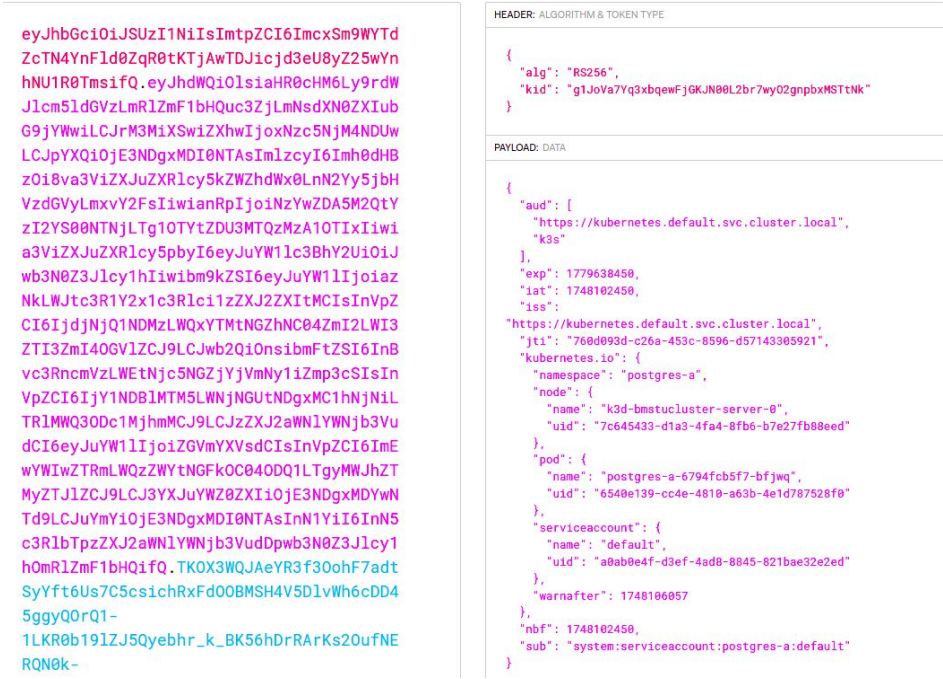
Кластер – содержит набор таких рабочих машин.

Сайдкар – дополнительный контейнер, выполняющий вспомогательные для основного функции.
В работе использован как прокси эндпоинт для внедрения авторизации входящих запросов.



Основные используемые понятия авторизации

Аутентификация – проверка личности сервиса.
Авторизация – проверка доступов сервиса.
OAuth 2.0 – открытый стандарт авторизации, позволяет приложению получать ограниченный доступ к ресурсам от сервиса.
OIDC – надстройка над OAuth 2.0 для аутентификации. Предоставляет стандартный способ аутентификации субъекта (ID Token в формате JWT).
JSON Web Token (JWT) – зашифрованный приватным ключом токен в формате json.
IdP (Identity Provider) – сервис, управляющий идентификацией и правами доступа, выпускающий токены с учетными данными.

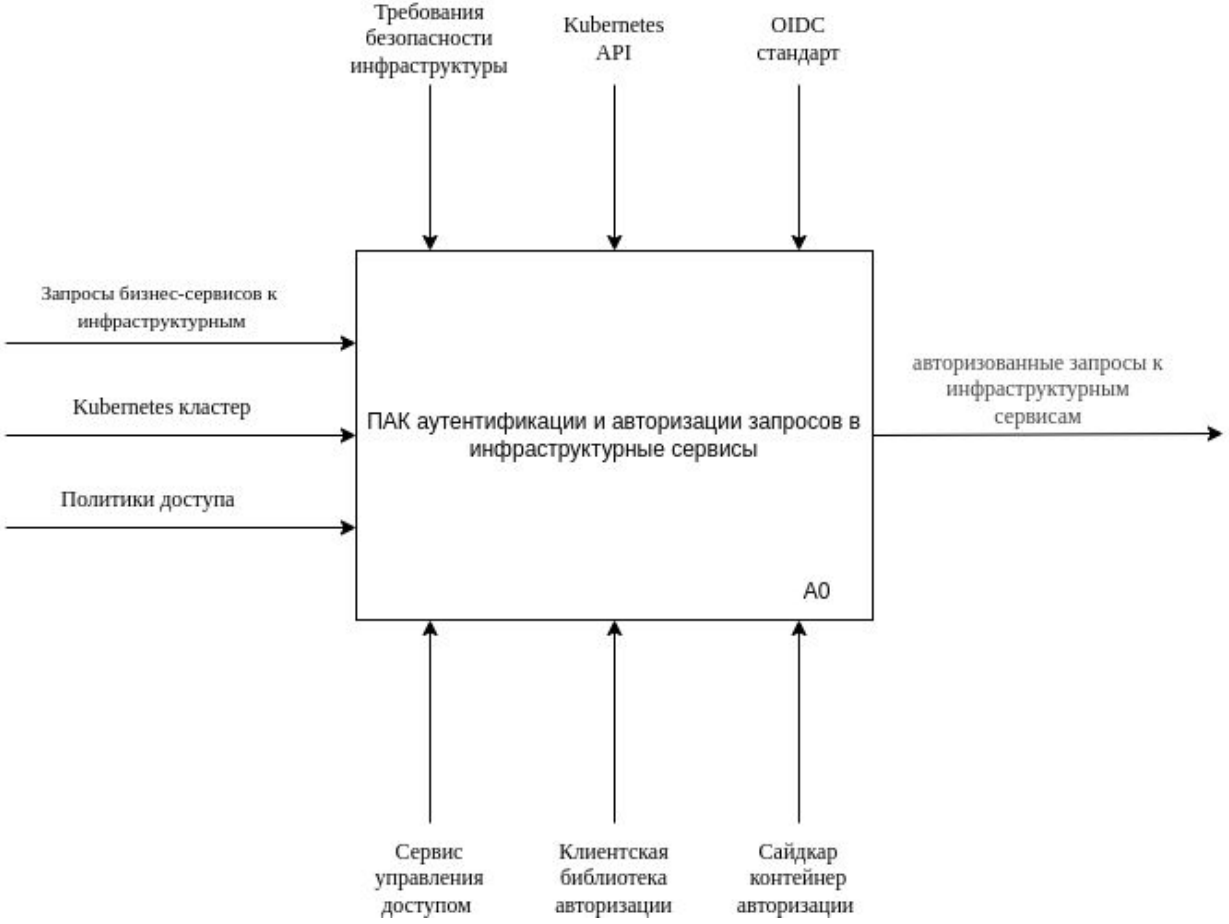


Пример k8s ID Token в формате JWT

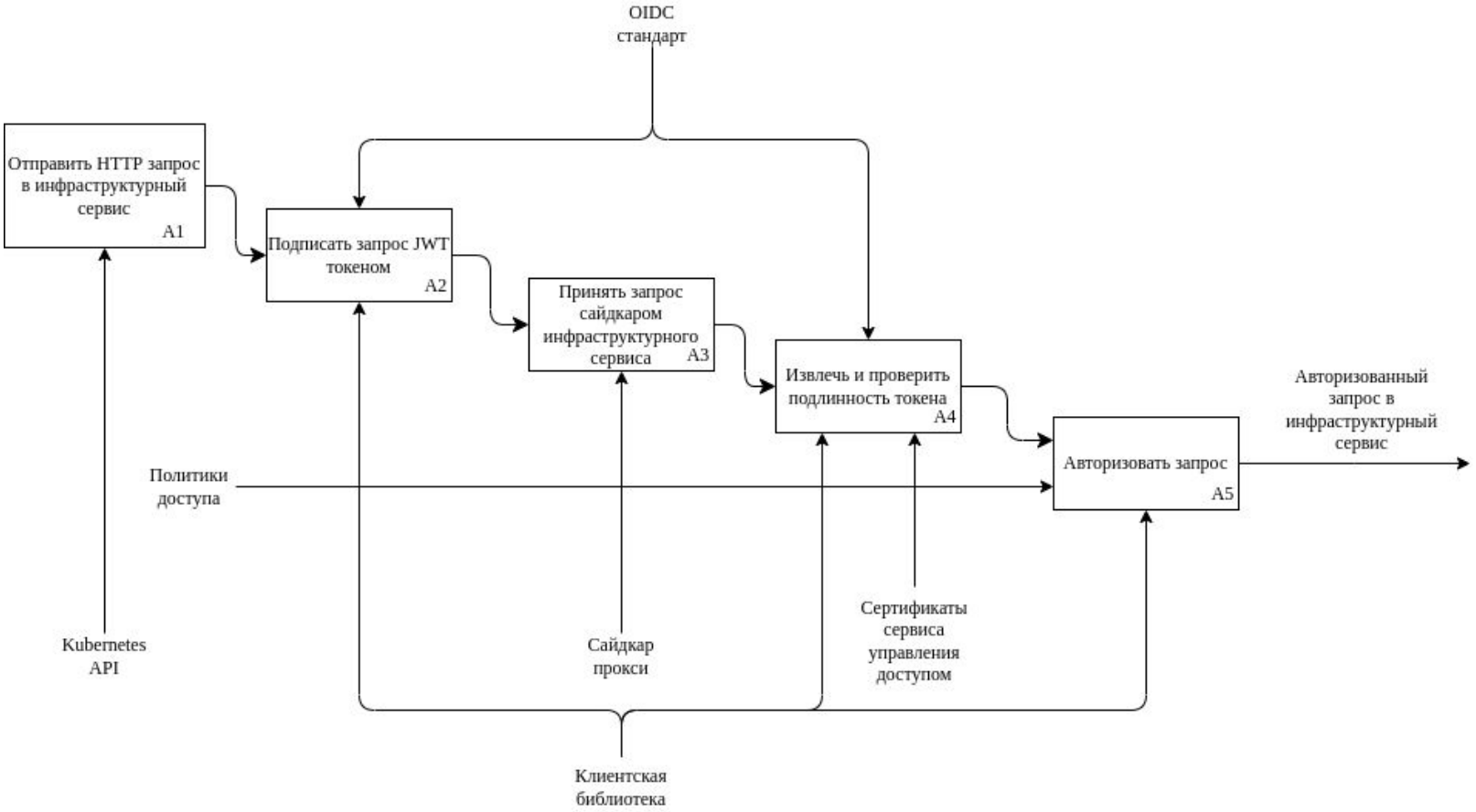
Обзор существующих подходов и решений

Подход	Аутентификация	Авторизация	Управление доступами
K8s политики сети	нет	нет	нет
Service Mesh (Istio, Linkerd)	да (mTLS)	да	нет
SPIFFE/SPIRE	да	нет	да
Предлагаемое решение	**да**	**да**	**да**

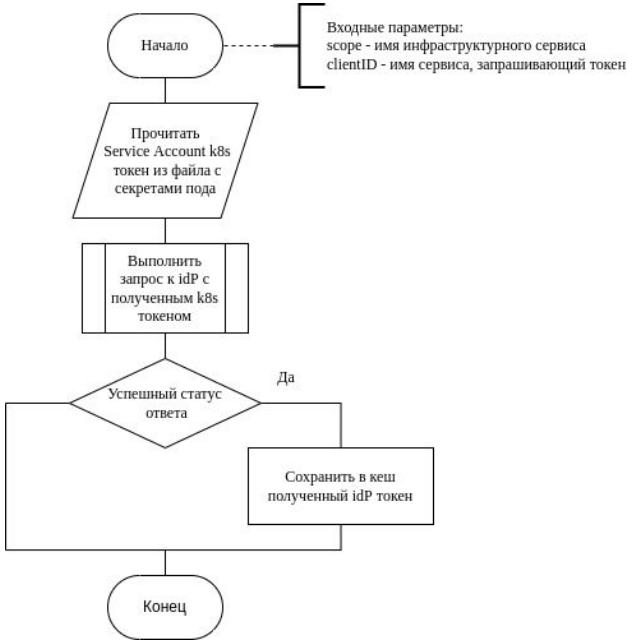
Формальная постановка задачи



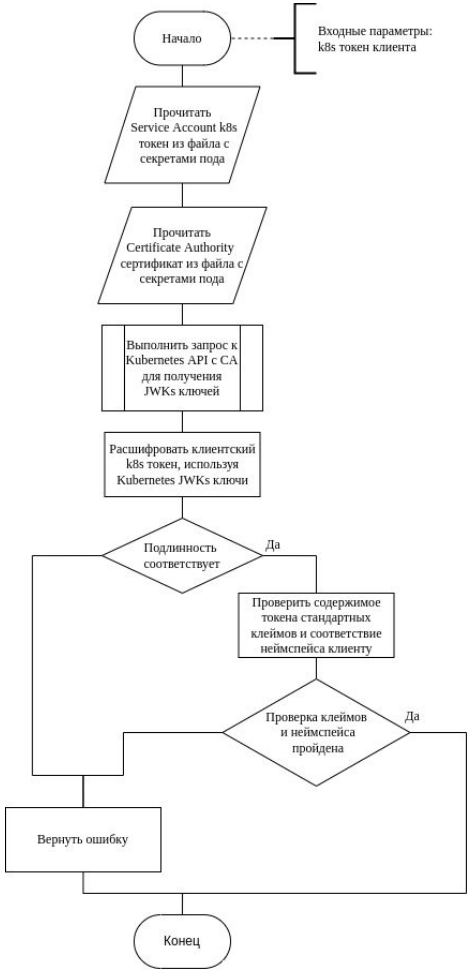
Функциональная модель метода авторизации запроса



Алгоритм выпуска IdP токена



Алгоритм проверки k8s токена



Алгоритм авторизации входящего запроса

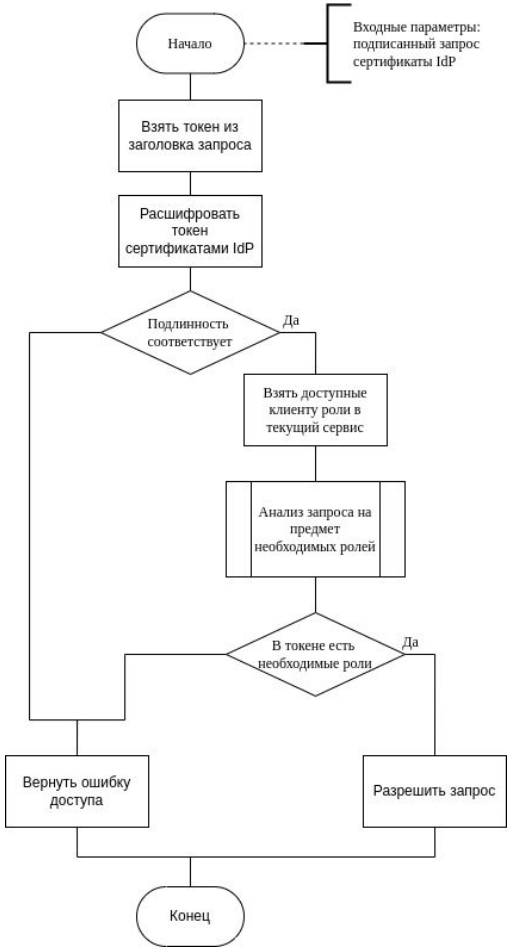
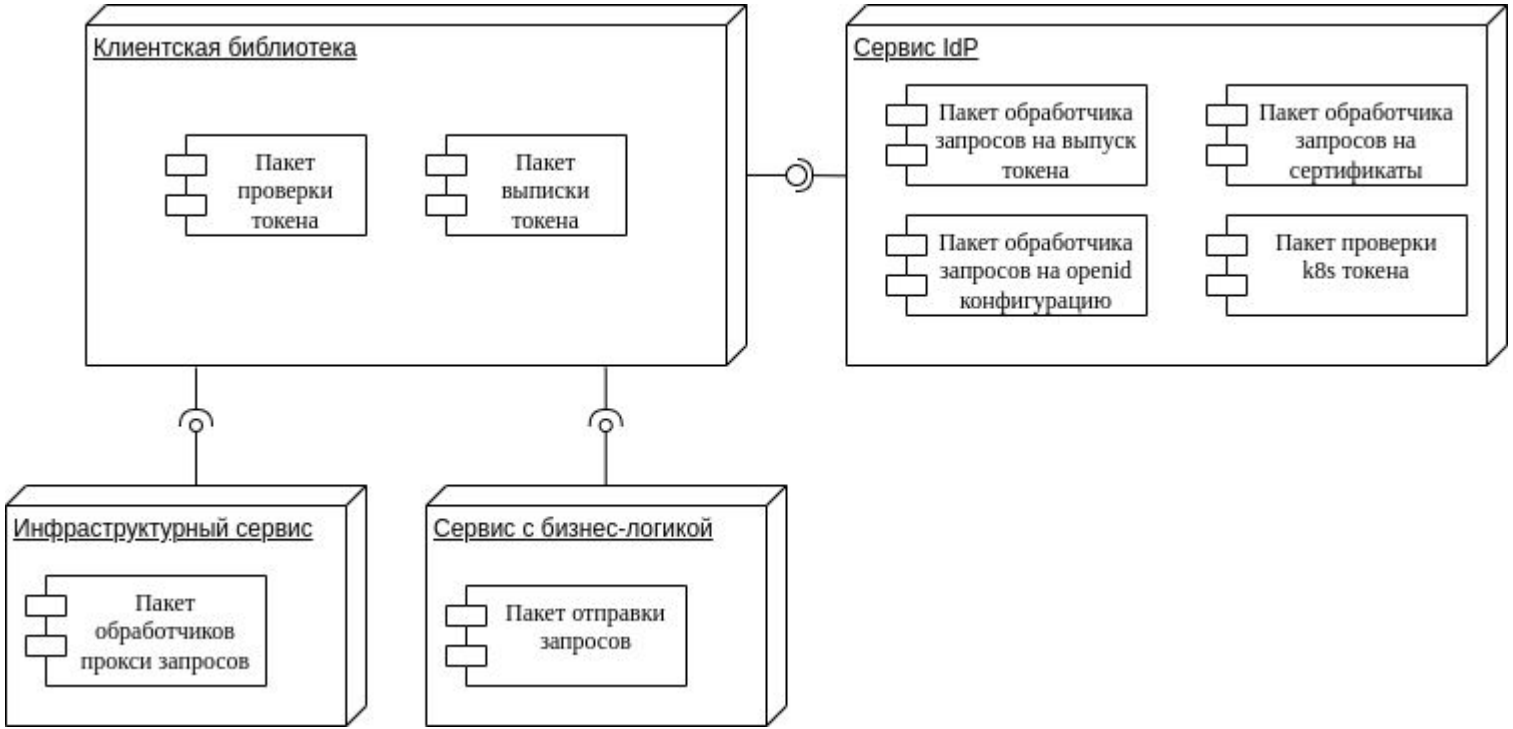
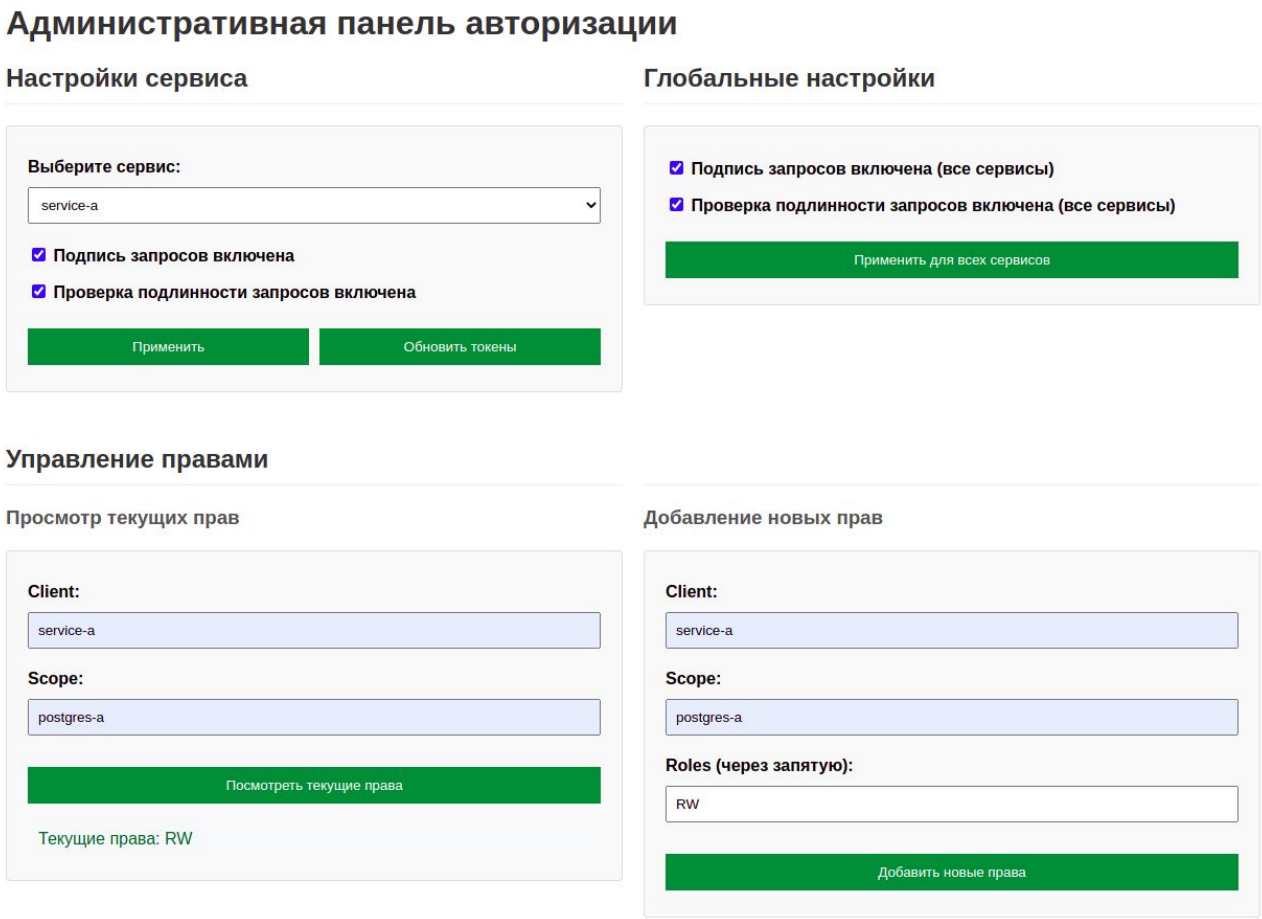


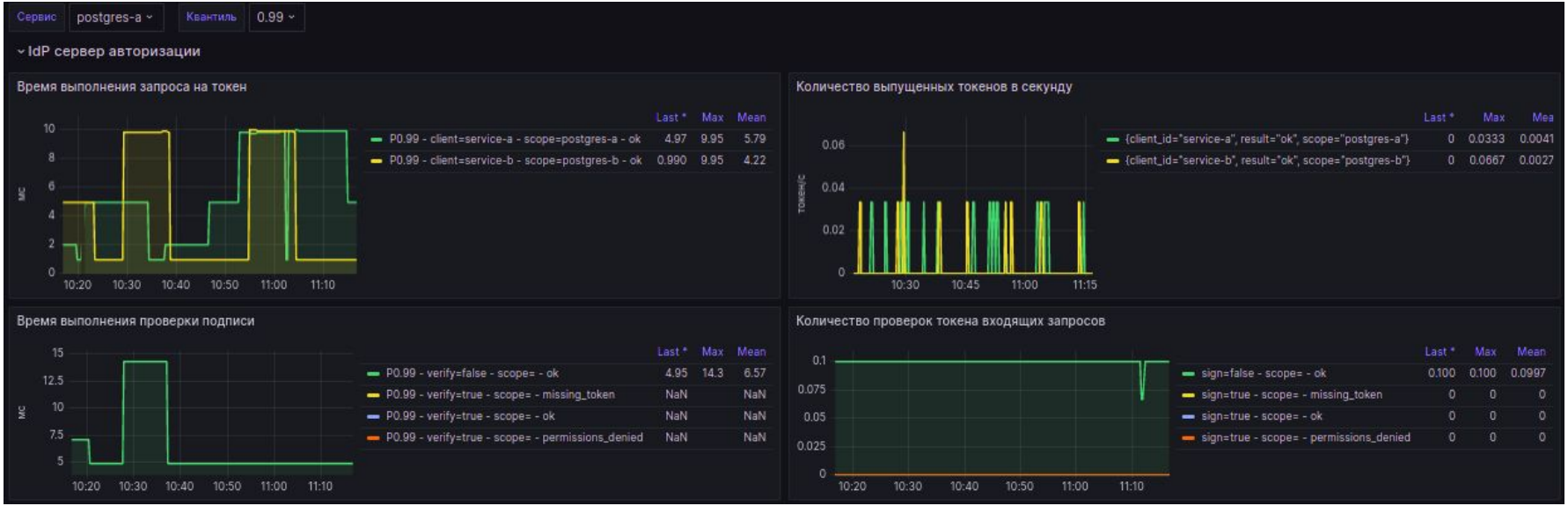
Диаграмма компонентов разработанного ПО



Пример интерфейса ПО

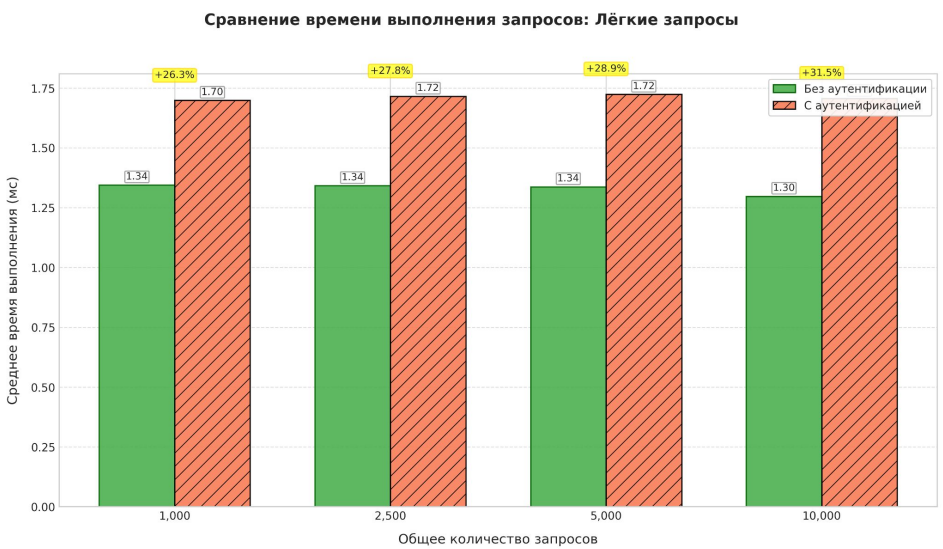


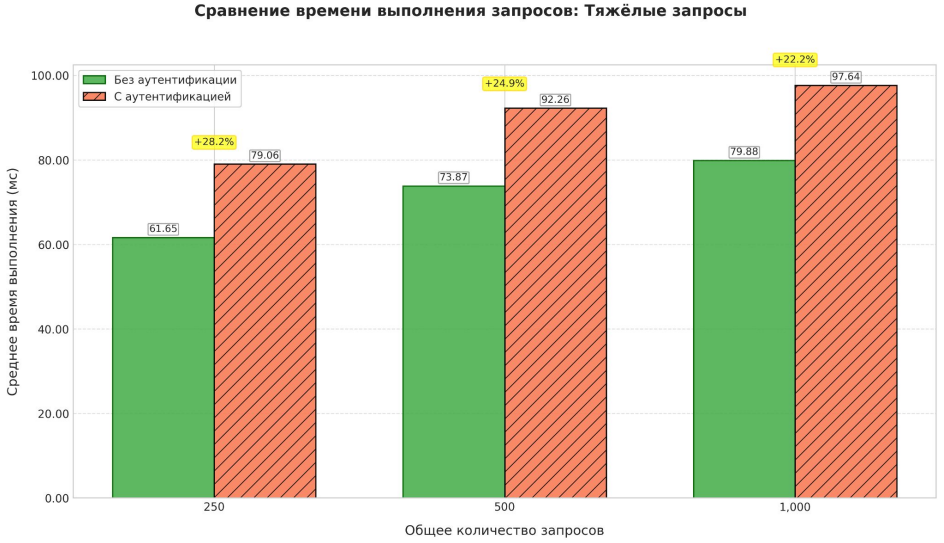
Мониторинг показателей сервисов



- **Prometheus** – инструмент для сбора данных (метрик) сервиса.
- **Grafana** – инструмент для визуализации собранных данных.
- Всего было задано **15 метрик**.

Исследование влияния работы авторизации





`INSERT INTO log (message) VALUES (Benchmark at %s", time.Now())`

`WITH heavy_cte AS (SELECT generate_series(1,1000000) AS data)
SELECT COUNT(*), AVG(data) FROM heavy_cte`

Заключение

Выполнена цель: реализован программно-алгоритмический комплекс для авторизации запросов в инфраструктурные сервисы.

Выполнены задачи:

1. Проведен обзор предметной области, существующих решений, подходов к аутентификации и авторизации в микросервисной архитектуре.
2. Разработаны и описаны ключевые алгоритмы работы программно-алгоритмического комплекса, реализующего аутентификацию и авторизацию запросов в инфраструктурные сервисы.
3. Проведено исследование влияния работы авторизации на время выполнения запросов в инфраструктурные сервисы.