Team A

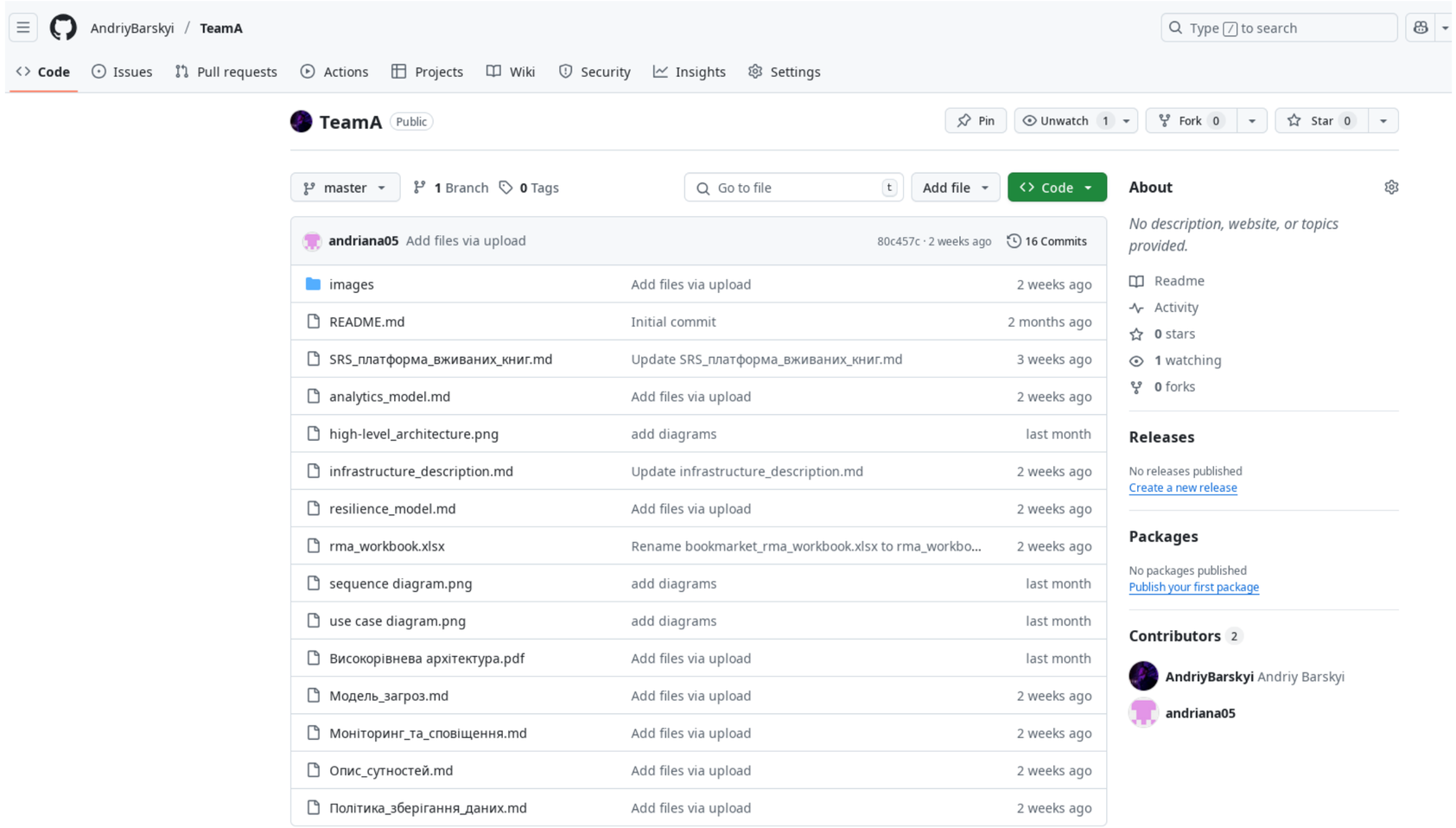
Платформа обміну та продажу вживаних книг

"БукМаркет"

Барський Андрій,
Сало Андріана
група ПМОм-11

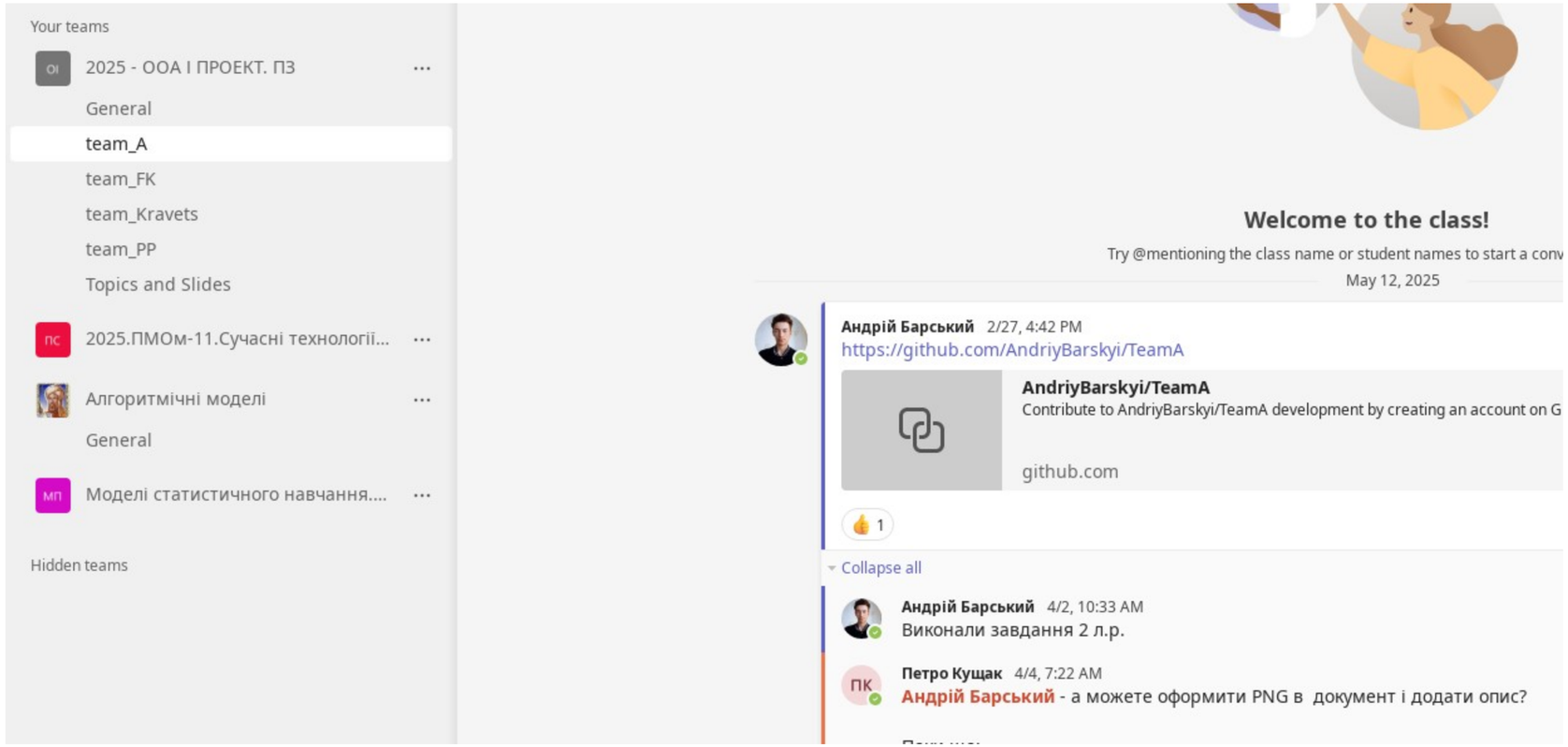
GitHub репозиторій

Документація проекту зберігається в GitHub репозиторії



Команда у MS Teams

Комунікація відбувалась у окремому каналі у MS Teams



Що таке БукМаркет?

"БукМаркет" - це веб-платформа, яка дозволяє користувачам продавати, купувати та обмінюватися вживаними книгами.

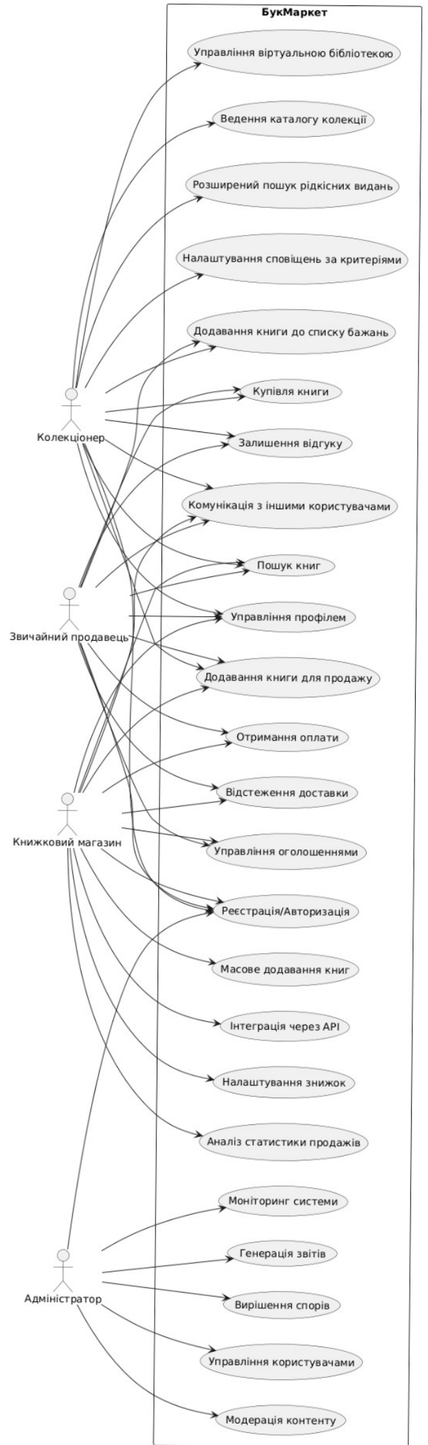
Система забезпечує зручний пошук книг за різними параметрами, комунікацію між користувачами, рейтингові системи для продавців та покупців, а також можливість створення особистої віртуальної бібліотеки.

Платформа спрямована на створення спільноти любителів книг, які цінують повторне використання ресурсів та доступ до рідкісних або бюджетних видань.

Описані функціональні вимоги продукту

- Реєстрація та управління профілем користувача
- Каталогізація книг та зручний пошук
- Додавання книг до каталогу з описом та фото
- Фільтрація і сортування книг за різними параметрами
- Вбудована система повідомлень між користувачами
- Відгуки та рейтинги продавців і покупців
- Безпечні транзакції та підтримка різних способів оплати
- Можливість обміну книгами без грошових операцій
- Відстеження статусу замовлення та доставки
- Інтеграція з поштовими та кур’єрськими службами
- Особиста віртуальна бібліотека і списки бажань
- Персоналізовані рекомендації та статистика активності
- Інтерфейс для адміністрування, модерації та вирішення спорів
- Підтримка багатомовності та адаптивний дизайн для різних пристроїв

Use-case діаграма



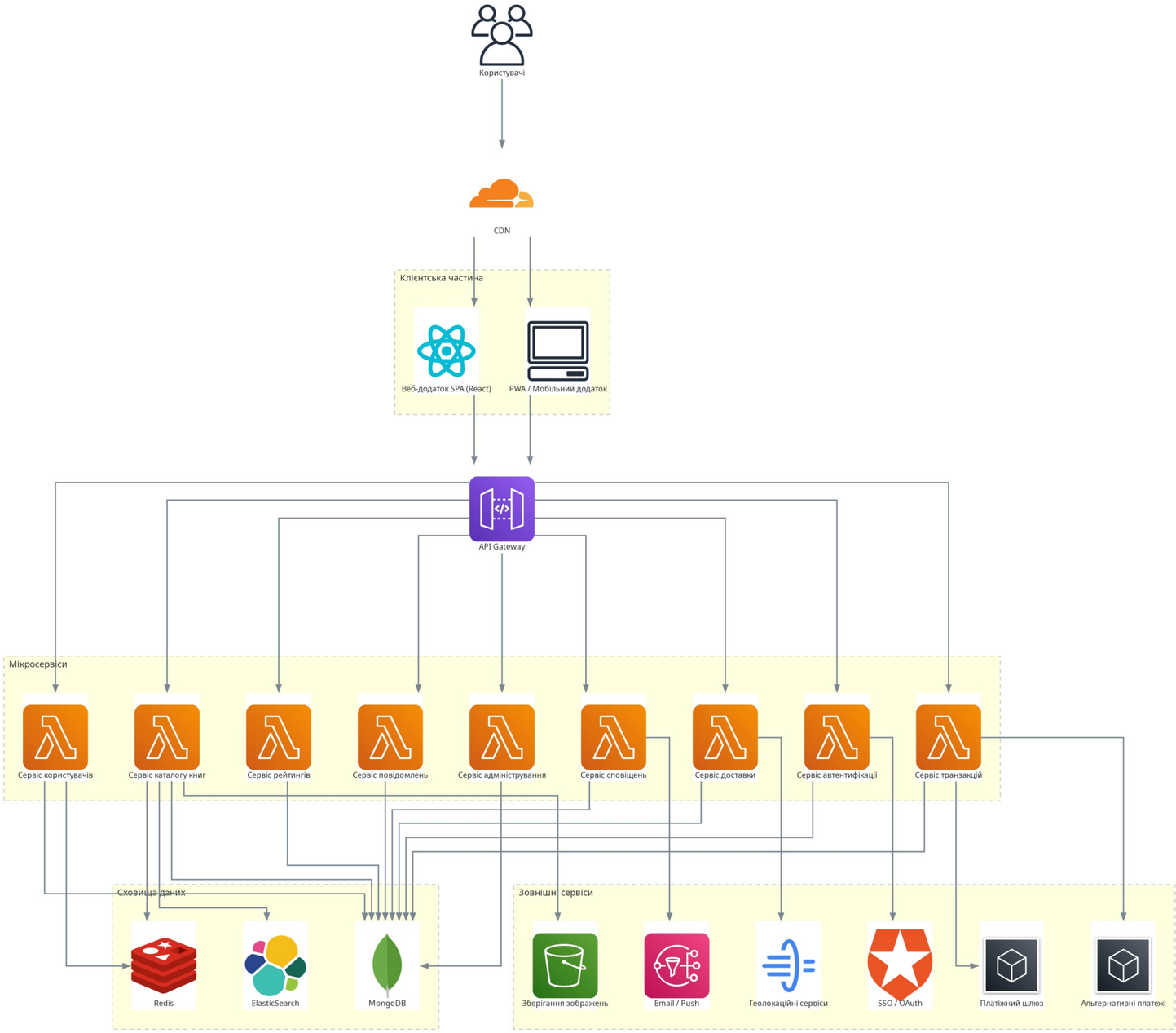
Архітектура

Платформа "БукМаркет" базується на мікросервісній архітектурі, що дозволяє забезпечити гнучкість, масштабованість та відмовостійкість системи.

Основні технологічні рішення включають:

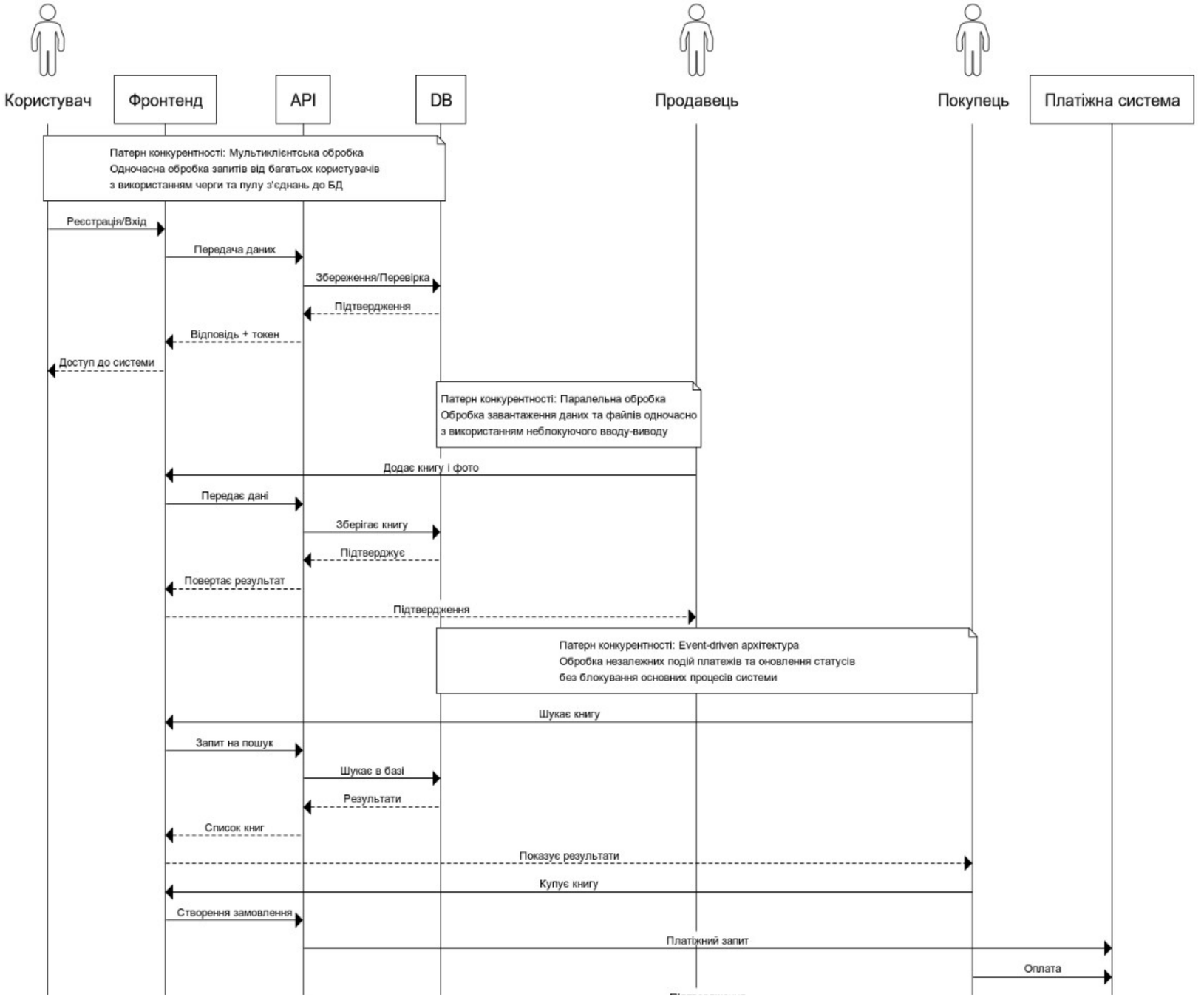
- Фронтенд: Single Page Application (SPA) з використанням React.js
- Бекенд: Мікросервісна архітектура з використанням Node.js
- Хмарне розгортання: Контейнеризація з Docker і оркестрація з Kubernetes
- Бази даних: MongoDB (основна БД), Redis (кешування), ElasticSearch (повнотекстовий пошук)
- Зовнішні інтеграції: RESTful API, WebSockets для повідомлень реального часу

Архітектура

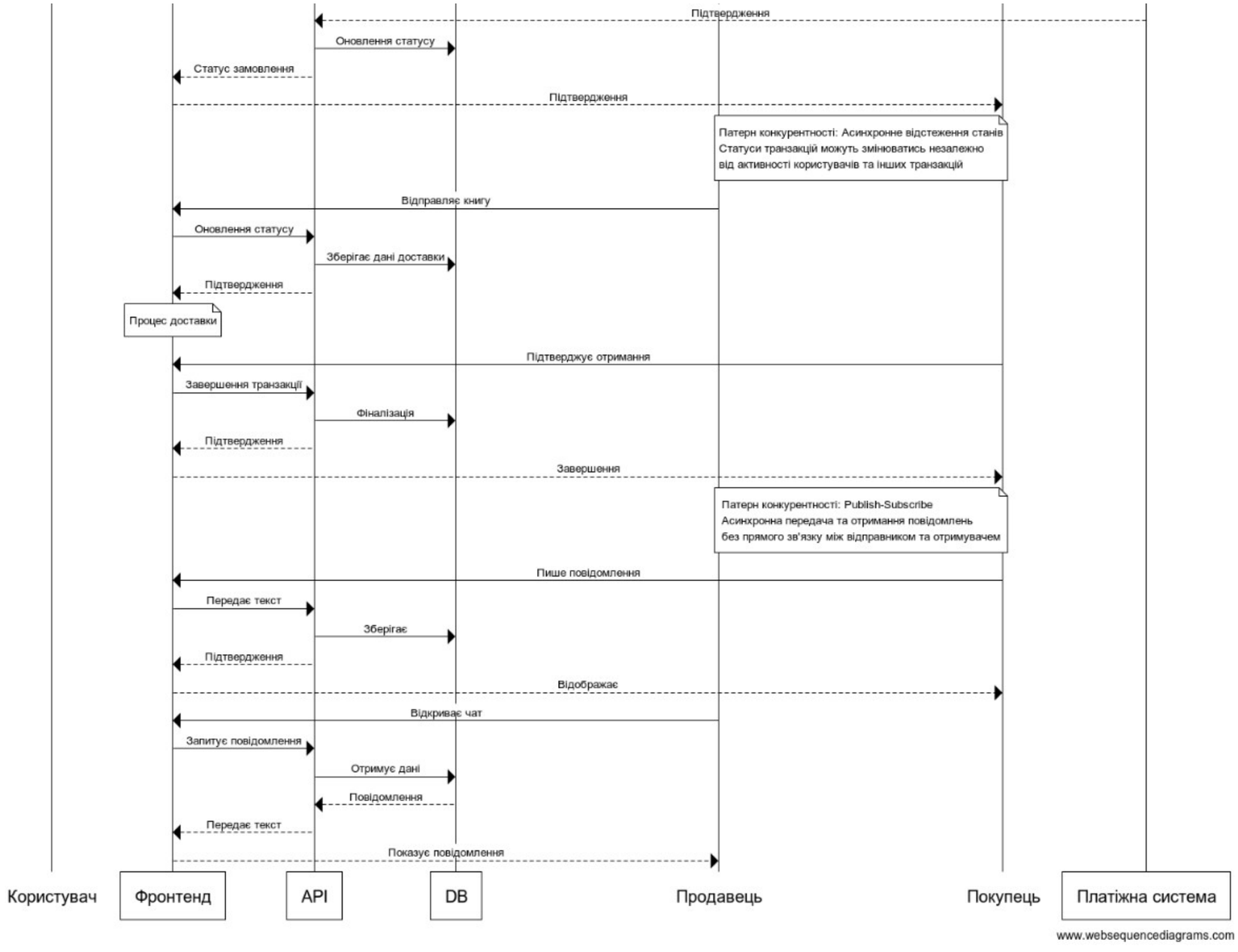


БукМаркет - Високорівнева архітектура

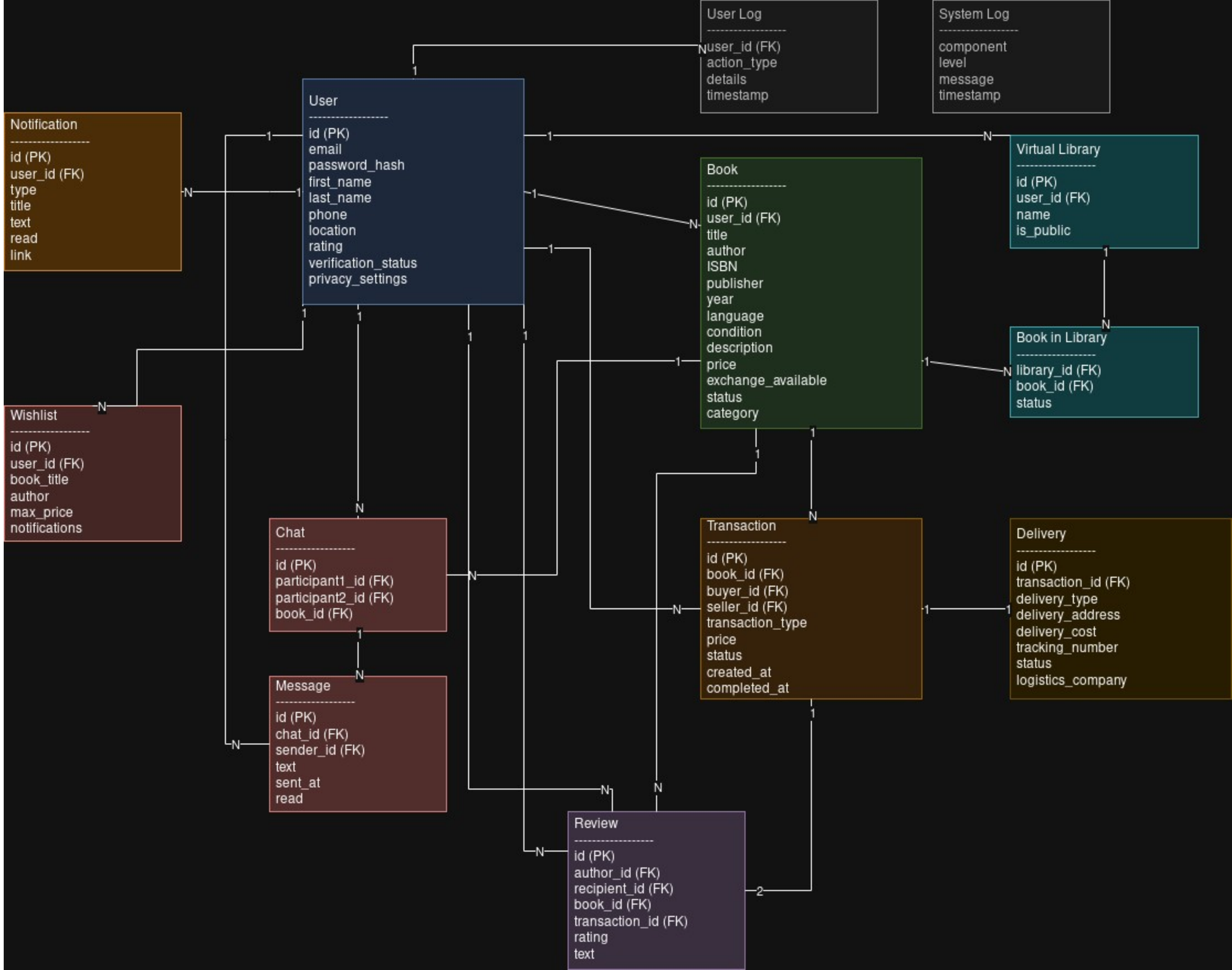
Діаграма послідовностей та патерни конкурентності



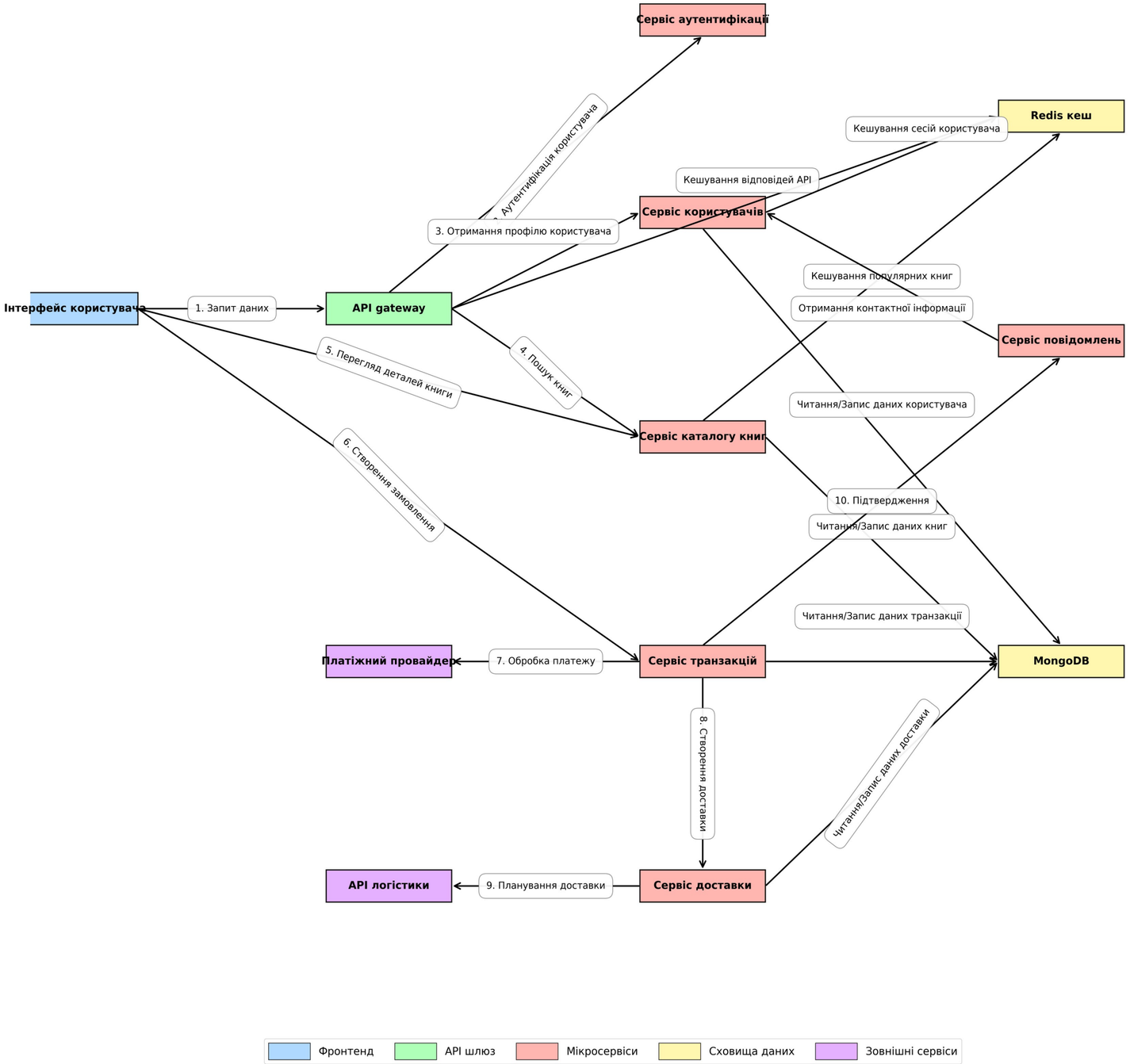
Діаграма послідовностей та патерни конкурентності



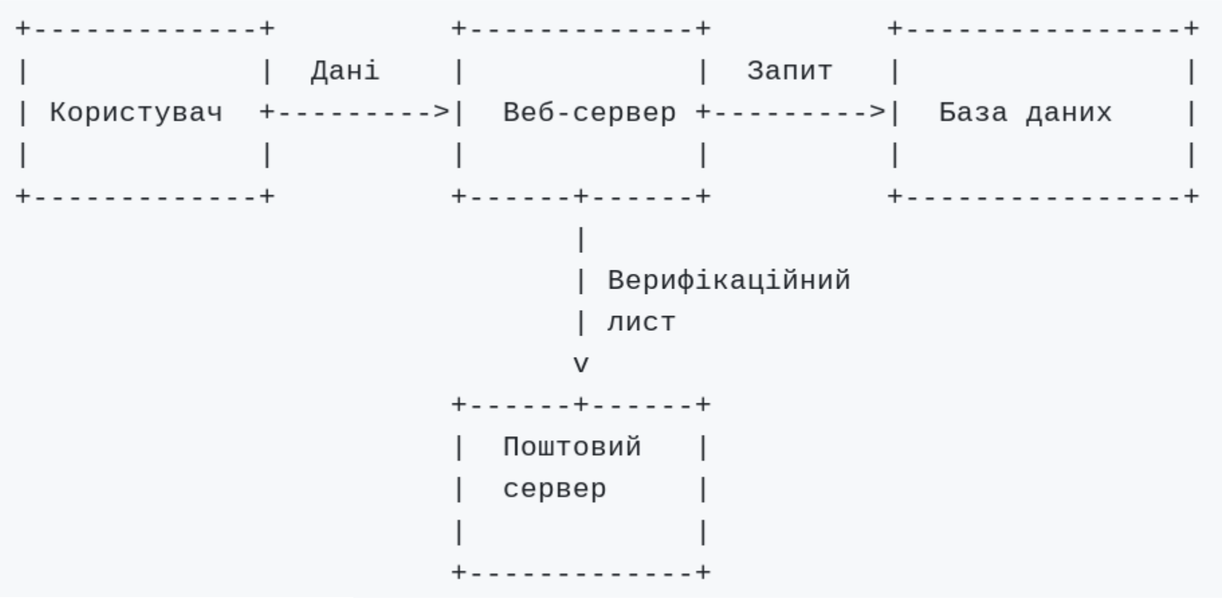
ER діаграма


User Log
user_id (FK)
action_type
details
timestamp
System Log
component
level
message
timestamp
User
id (PK)
email
password_hash
first_name
last_name
phone
location
rating
verification_status
privacy_settings
Notification
id (PK)
user_id (FK)
type
title
text
read
link
Book
id (PK)
user_id (FK)
title
author
ISBN
publisher
year
language
condition
description
price
exchange_available
status
category
Virtual Library
id (PK)
user_id (FK)
name
is_public
Book in Library
library_id (FK)
book_id (FK)
status
Wishlist
id (PK)
user_id (FK)
book_title
author
max_price
notifications
Chat
id (PK)
participant1_id (FK)
participant2_id (FK)
book_id (FK)
Message
id (PK)
chat_id (FK)
sender_id (FK)
text
sent_at
read
Transaction
id (PK)
book_id (FK)
buyer_id (FK)
seller_id (FK)
transaction_type
price
status
created_at
completed_at
Delivery
id (PK)
transaction_id (FK)
delivery_type
delivery_address
delivery_cost
tracking_number
status
logistics_company
Review
id (PK)
author_id (FK)
recipient_id (FK)
book_id (FK)
transaction_id (FK)
rating
text

Діаграма взаємодії компонентів



Security model



Ідентифіковані загрози

ID	Тип (STRIDE)	Опис загрози	Ризик	Вектор атаки
T1	S, I	Брутфорс атаки на облікові записи	Високий	Автоматизований підбір паролів
T2	I, D	Відмова в обслуговуванні через масову реєстрацію	Середній	Автоматизоване створення фейкових облікових записів
T3	S	Підміна верифікаційного посилання	Середній	Перехоплення або підробка верифікаційного листа
T4	I	Витік даних користувача	Критичний	Незашифроване зберігання персональних даних
T5	T	Ін'єкція шкідливого коду через поля реєстрації	Високий	XSS, SQL-ін'єкції через вхідні дані
T6	S	Зламування слабких парольних політик	Високий	Використання словників, соціальна інженерія
T7	I	Перехоплення даних при реєстрації	Високий	MITM-атаки при відсутності шифрування

Security model

Ідентифіковані загрози

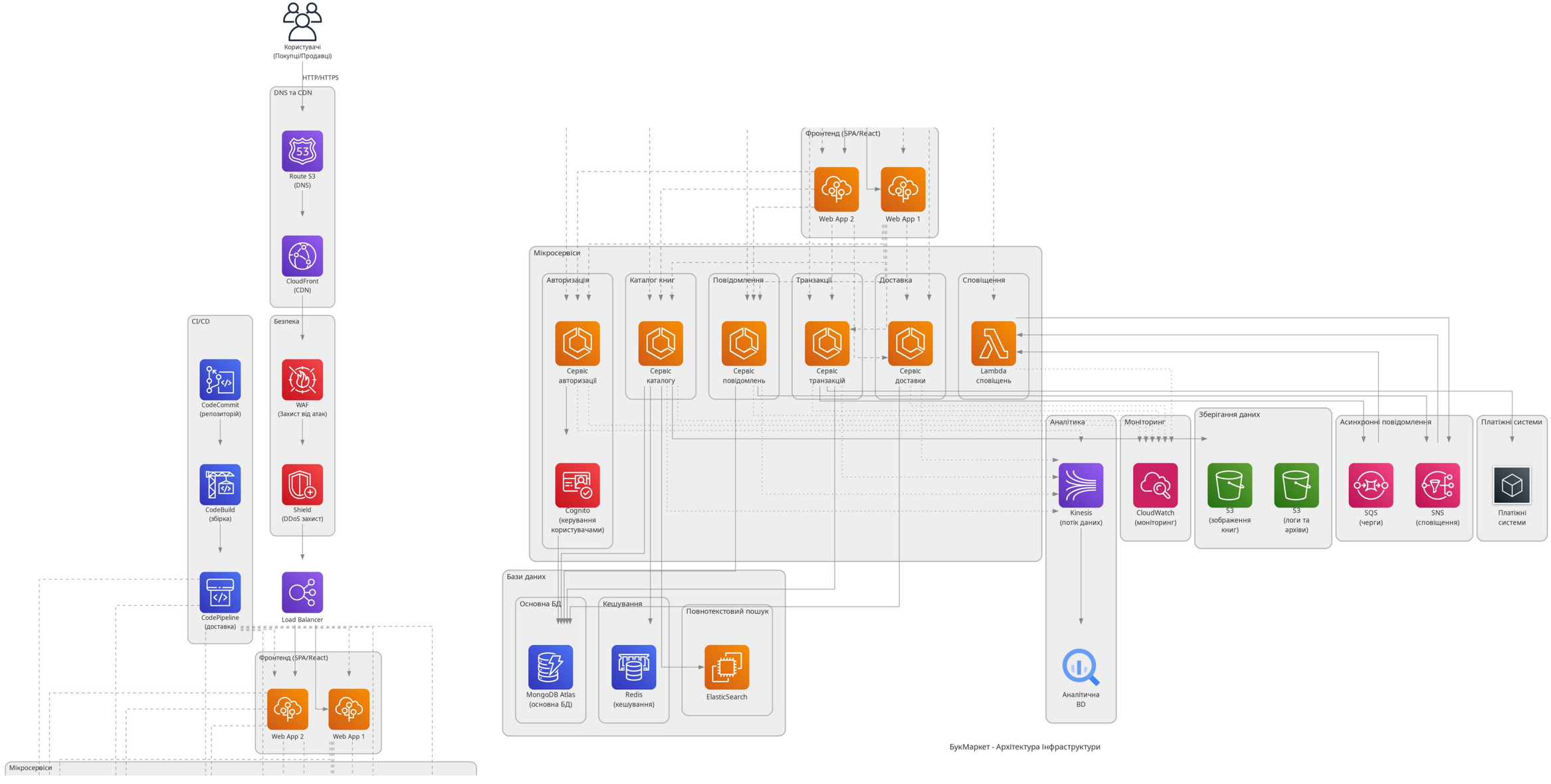
ID	Тип (STRIDE)	Опис загрози	Ризик	Вектор атаки
T8	I	Перехоплення платіжних даних	Критичний	MITM-атаки, кейлогери, фішинг
T9	T	Маніпуляція з ціною або деталями транзакції	Високий	Підміна параметрів запиту
T10	R	Відмова від здійснення транзакції	Середній	Недостатнє логування та аудит дій
T11	T, I	Підміна платіжних систем	Критичний	DNS-спуфінг, фішинг
T12	D	DoS атака на платіжну систему	Високий	Велика кількість фейкових транзакцій
T13	S	Використання вкрадених платіжних даних	Високий	Крадіжка номерів карток, даних авторизації
T14	I	Витік історії транзакцій користувача	Високий	Недостатня ізоляція даних, інсайдерські загрози

Security model

План для 10 найкритичніших загроз

ID	Загроза	План пом'якшення
T4	Витік даних користувача	1. Шифрування всіх персональних даних у базі даних 2. Впровадження принципу мінімізації даних 3. Регулярний аудит безпеки 4. Впровадження монітирингу аномального доступу до даних
T8	Перехоплення платіжних даних	1. Використання PCI DSS сертифікованих платіжних систем 2. Відмова від зберігання платіжних даних на серверах 3. Використання токенізації для платіжних операцій 4. Обов'язкове TLS 1.3 шифрування
T11	Підміна платіжних систем	1. Впровадження HSTS 2. Використання сертифікатів EV SSL 3. Впровадження Certificate Pinning 4. Використання мультифакторної автентифікації для транзакцій
T5	Ін'єкція шкідливого коду	1. Використання ORM для запитів до БД 2. Валідація всіх вхідних даних 3. Впровадження Content Security Policy 4. Використання parameterized queries
T7	Перехоплення даних при реєстрації	1. Використання TLS для всіх з'єднань 2. Впровадження HSTS 3. Моніторинг сертифікатів для виявлення підозрілих видач
T1	Брутфорс атаки	1. Обмеження кількості спроб входу 2. Впровадження CAPTCHA 3. Використання затримок при невдалих спробах 4. Сповіщення про підозрілі спроби входу
T6	Зламування слабких парольних політик	1. Впровадження вимог до складності паролів 2. Перевірка паролів проти баз скомпрометованих паролів 3. Заохочення використання парольних менеджерів 4. Реалізація двофакторної автентифікації
T9	Маніпуляція з деталями транзакції	1. Перевірка цілісності параметрів на сервері 2. Криптографічне підписання платіжних даних 3. Багаторівнева валідація транзакцій 4. Використання ідемпотентних API
T13	Використання вкрадених платіжних даних	1. Впровадження аналізу поведінки для виявлення аномалій 2. Використання Address Verification Service (AVS) 3. Використання 3D Secure протоколу 4. Впровадження геолокаційної перевірки
T14	Витік історії транзакцій	1. Шифрування історії транзакцій 2. Розділення даних користувача і транзакцій 3. Контроль доступу на основі ролей 4. Детальне логування доступу до транзакційних даних

Deployment model



БукМаркет - Архітектура Інфраструктури

Analytics model

Ключові функціональні метрики:
- Нові реєстрації, конверсія в користувача, активні користувачі (DAU/MAU)
- Кількість доданих/проданих книг, середній час додавання книги
- Кількість транзакцій, середня вартість і завершення транзакцій
- Кількість та рейтинг продавців, вчасність доставок, утримання користувачів

Основні конверсійні воронки:
1. Воронка придбання книги: Пошук → Перегляд → Транзакція → Оплата → Отримання
2. Воронка активації продавця: Реєстрація → Профіль → Додавання книги → Продаж

Стратегія аналітики:
- Збір даних через GA/Firebase, логування (ELK), сховища (Redshift/BigQuery), ETL (Airflow)
- Візуалізація: Tableau/Looker/PowerBI, щотижневі/щомісячні звіти
- Прогнозування попиту, сегментація користувачів, виявлення аномалій

Бізнес-показники (цілі):
- Приріст активних користувачів >15%/міс
- Утримання на 30 день >40%
- ARPU >50 грн/міс
- Витрати на маркетинг <25% доходу
- NPS >40

Інтеграції:
- CRM, email-маркетинг, платіжні та доставочні системи

Monitoring & Alerting model

Основні операційні метрики:
- Час відгуку API, доступність сервісів, утилізація CPU/пам’яті, кількість помилок авторизації, невдалих транзакцій, час обробки транзакцій, затримка БД, кількість запитів до API, використання диску, активні сесії, затримка між мікросервісами, розмір черги повідомлень.

Збір та зберігання метрик:
- AWS CloudWatch, Prometheus, ELK Stack, AWS X-Ray, CloudWatch RUM, Custom SDK.
- Зберігання: Amazon Timestream, архівування в S3.

Пороги для сповіщень:
- Доступність сервісів < 99.9% — критичне сповіщення (email, sms, дзвінок).
- Час відгуку API > 500 мс, помилки транзакцій > 5 за 15 хв, CPU > 80%, пам’ять > 85%, затримка БД > 100 мс, помилки авторизації > 10 за 5 хв — email/sms.

Реакція на інциденти:
- Автоматичне перемикання на резервні ресурси, аналіз логів, ізоляція проблемних компонентів, сповіщення користувачів.
- Превентивно: регулярний аудит, тестування disaster recovery, авто scaling, багаторівневий моніторинг безпеки.

Відповідальні:
- DevOps, CTO, Product, Security, Backend, Payment team.