КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем

Лабораторна робота №1

з дисципліни «Методи забезпечення якості програмних систем»
на тему «Специфікація програмних вимог для торгової платформи «Binance» та її API інтерфейсів»

Виконав:
Студент групи ПЗС-1
Лутай Артем Сергійович

КИЇВ 2025

ЗМІСТ

Вступ

Призначення документа (Purpose)

Цей документ містить специфікацію програмних вимог (SRS) до торгової платформи **Binance**. Він описує функціональні можливості веб-терміналу та публічного/приватного API для алгоритмічної торгівлі. Документ призначений для розробників ядра (Matching Engine), фронтенд-команди, QA-інженерів та API-клієнтів.

Сфера продукту (Product Scope)

Платформа Binance забезпечує доступ до спотової та ф'ючерсної торгівлі криптовалютними активами та опціонів на них. Ключові можливості:

1. Веб-інтерфейс для ручної торгівлі та аналізу графіків.
2. Високопродуктивний API (REST + WebSocket) для підключення торгових роботів.
3. Система керування гаманцями (введення/виведення коштів).
4. Механізм зведення ордерів (Matching Engine) з низькою затримкою.

Терміни та скорочення (Definitions, Acronyms)

1. **Order Book (Стакан)** — список активних ордерів на купівлю та продаж.
2. **Matching Engine** — ядро системи, що зводить ордери покупців та продавців.
3. **Maker/Taker** — ролі учасників ринку (Maker створює ліквідність, Taker забирає).
4. **API Key** — унікальний пара ключів для автентифікації програмних запитів. Складається з ключа та секрету (api key та secret key)
5. **KYC (Know Your Customer)** — процедура верифікації особистості.
6. **TPS (Transactions Per Second)** — кількість транзакцій на секунду.
7. **CEX (Centralized Exchange)** - централізована біржа
8. **DEX (Decentralized exchange)** - децентралізована біржа

Огляд продукту

Перспектива продукту

Система «Binance» є найбільшою за об’ємом торгівлі платформою для торгівлі цифровими активами (CEX), яка функціонує як високонавантажена розподілена система. Вона виступає посередником між покупцями та продавцями криптовалют, забезпечуючи ліквідність та безпеку угод. Система є незалежною, але тісно інтегрується з такими зовнішніми компонентами та сервісами:

1. **Блокчейн-мережі (Blockchain Nodes):** Взаємодія з мережами Bitcoin, Ethereum, BNB Chain, Tron та іншими для моніторингу депозитів та виконання транзакцій на виведення коштів.
2. **Платіжні шлюзи (Fiat Gateways):** Інтеграція з провайдерами (Banxa, Simplex, Advcash) та банківськими системами (SEPA, SWIFT) для обробки фіатних операцій.
3. **Сервіси автентифікації та безпеки:** Використання Google Authenticator, YubiKey (FIDO2) для двофакторної автентифікації (2FA).
4. **Системи KYC/AML:** Інтеграція із сервісами верифікації особистості (Sumsub або аналогами) для дотримання регуляторних норм.
5. **Клієнтські інтерфейси:** Веб-термінал, мобільні додатки (iOS/Android) та API-клієнти (торгові роботи).

Основні функції продукту

Функціональність системи поділяється на користувацький інтерфейс (UI) та програмний інтерфейс (API).

1. **Торгові операції (Matching & Execution):**
    a. **Спотова торгівля:** Обмін однієї валюти на іншу з миттєвим розрахунком.
    b. **Ф'ючерсна торгівля:** Торгівля деривативами з використанням кредитного плеча (leverage).
    c. **Торгівля опціонами** з фіксованою датою експірації.
    d. **Типи ордерів:** Підтримка Limit, Market, Stop-Limit, Trailing Stop, OCO (One Cancels the Other).

e. **Matching Engine:** Зведення ордерів на купівлю та продаж за пріоритетом ціни та часу (Price-Time Priority) з наднизькою затримкою.

2. **API Інтерфейси (для алгоритмічної торгівлі)**
   a. **Public REST API:** Надання доступу до ринкових даних (тікери, історичні свічки, глибина стакану, час сервера) без необхідності авторизації.
   b. **Private REST API:** Розміщення, скасування та запит статусу ордерів, отримання інформації про баланс. Вимагає підпису запитів за допомогою HMAC SHA256 та API-ключів.
   c. **WebSocket Market Streams:** Асинхронна трансляція змін у стакані (Diff. Depth), угод (Agg. Trades) та свічок у реальному часі (push-повідомлення).
   d. **WebSocket User Data Stream:** Отримання оновлень про виконання власних ордерів та зміну балансу без необхідності постійного опитування сервера.

3. **Управління акаунтом та активами:**
   a. **Гаманець:** Генерація депозитних адрес, історія транзакцій, внутрішні перекази між спотовим та ф'ючерсним балансами.
   b. **Керування API-ключами:** Створення ключів, налаштування дозволів (тільки читання, дозвіл торгівлі, дозвіл виведення), прив'язка до "білого списку" IP-адрес.
   c. **Субакаунти:** Створення та керування вкладеними акаунтами для розділення торгових стратегій.

Обмеження (Constraints)

1. **Ліміти навантаження (Rate Limits):** Система накладає суворі обмеження на кількість запитів до API (наприклад, 1200 ваги запитів на хвилину для IP), при перевищенні яких користувач отримує блокування (HTTP 429).
2. **Часові обмеження (Latency):** Критична вимога до мінімізації затримок (latency) у Matching Engine та API для забезпечення чесної торгівлі.
3. **Регуляторні обмеження:** Відсутність доступу для користувачів з санкційних країн або регіонів із забороною криптоактивів.

4. **Вимоги до синхронізації часу:** API-клієнт повинен мати синхронізований час із сервером біржі (допустиме відхилення < 1000 мс) для валідації підпису.

Характеристики користувачів (User Characteristics)

1. **Роздрібні трейдери (Retail):** Використовують переважно графічний веб-інтерфейс або мобільний додаток, здійснюють угоди вручну, мають базові технічні знання.
2. **Алгоритмічні трейдери та розробники (Algo/Devs):** Використовують API для створення торгових ботів, маркет-мейкінгу та арбітражу. Потребують детальної документації API та стабільності з’єднання.
3. **Інституційні клієнти:** Великі фонди, що потребують розширених лімітів, субакаунтів та звітності.
4. **Адміністратори платформи:** Здійснюють моніторинг підозрілої активності, керують лістингом активів та технічною підтримкою.

Припущення та залежності (Assumptions and Dependencies)

1. **Стабільність мережі Інтернет:** Користувач повинен мати стабільне з'єднання для підтримки WebSocket-сесій без розривів (reconnection issues).
2. **Працездатність блокчейнів:** Введення та виведення коштів залежить від швидкості та статусу відповідних блокчейн-мереж (наприклад, перевантаження мемпулу Bitcoin може затримати депозити).
3. **Хмарна інфраструктура:** Передбачається, що сервери (наприклад, AWS) забезпечують необхідний аптайм та масштабованість під час пікових навантажень ринку.

Вимоги (Requirements)

Зовнішні інтерфейси (External Interfaces)

Цей розділ описує зовнішні інтерфейси системи: користувацькі інтерфейси, апаратні та програмні інтеграції, необхідні для функціонування платформи Binance.

Користувацькі інтерфейси (User Interfaces)

ID	Сторінка / Елемент	Опис
UI-01	Головна сторінка	Огляд ринку (популярні пари), банери нових лістингів, кнопки входу/реєстрації, завантаження додатку.
UI-02	Торговий термінал (Spot)	Графік (TradingView), Книга ордерів (Order Book), список останніх угод, панель створення ордерів (Buy/Sell).
UI-03	Панель створення ордера	Форма вибору типу ордера (Limit, Market, Stop-Limit), введення ціни та кількості, слайдер відсотка балансу.
UI-04	Гаманець (Fiat and Spot)	Таблиця активів користувача, баланс у BTC/USDT еквіваленті, кнопки «Депозит», «Вивід», «Переказ».
UI-05	Історія ордерів	Списки відкритих ордерів, історія торгівлі, історія транзакцій (введення/виведення) з фільтрацією за датою та парою.
UI-06	Управління API	Генерація API Key / Secret Key, налаштування прав доступу (Read-only, Enable Spot Trading), білий список IP-адрес.
UI-07	Сторінка входу / 2FA	Введення email/пароля, перевірка капчі, введення коду 2FA (Google Auth / SMS / YubiKey).

UI-08	KYC Верифікація	Форма завантаження документів, селфі-перевірка (Liveness check), статус верифікації.
UI-09	P2P Платформа	Список оголошень купівлі/продажу криптоактивів за фіат, чат з контрагентом, механізм апеляцій.
UI-10	Налаштування безпеки	Зміна пароля, керування пристроями, налаштування анти-фішинг коду, активність акаунта.
UI-11	Мобільний інтерфейс	Адаптивна версія всіх вищезазначених сторінок для iOS/Android браузерів та WebView.

Апаратні інтерфейси (Hardware Interfaces)

ID	Пристрій	Опис
HW-01	Серверна інфраструктура	Кластери високопродуктивних серверів (Linux) для Matching Engine, розміщені в зоні доступності (AWS/GCP).
HW-02	Клієнтські пристрої	PC (Windows/macOS/Linux), смартфони (iOS/Android) з доступом до інтернету.
HW-03	Апаратні ключі безпеки	Підтримка YubiKey (FIDO2/U2F) для фізичної двофакторної автентифікації користувачів.

Програмні інтерфейси (Software Interfaces)

ID	Система / Сервіс	Опис
SW-01	Блокчейн-ноди	Інтеграція з нодами Bitcoin, Ethereum, BNB Chain, Tron та ін. для моніторингу депозитів та бродкастингу транзакцій.

SW-02	KYC Provider	Зовнішній API (наприклад, Sumsub/Jumio) для автоматизованої перевірки документів та біометрії.
SW-03	Платіжні шлюзи	API провайдерів (Simplex, Banxa) для обробки платежів банківськими картками Visa/Mastercard.
SW-04	Бази даних	In-memory DB (Redis) для кешування стакану, RDBMS (PostgreSQL/MySQL) для зберігання даних користувачів.
SW-05	Public API (REST)	Відкритий інтерфейс для отримання ринкових даних (GET запити).
SW-06	Private API (Signed)	Захищений інтерфейс для торгівлі, що вимагає підпису HMAC SHA256.
SW-07	WebSocket Server	Сервер для push-повідомлень про зміни ринку та виконання ордерів у реальному часі.

Функціональні вимоги (Functional Requirements)

ID	Вимога
FR-01	Система повинна підтримувати реєстрацію нових користувачів через Email або мобільний телефон.
FR-02	Система повинна забезпечувати вхід з обов'язковою перевіркою 2FA (якщо налаштовано).
FR-03	Система повинна відображати актуальні ціни (Ticker) для всіх торгових пар у реальному часі.
FR-04	Система повинна відображати глибину ринку (Order Book) з візуалізацією обсягів.
FR-05	Система повинна дозволяти розміщення лімітних ордерів (Limit Order) за вказаною ціною та кількістю.
FR-06	Система повинна дозволяти розміщення ринкових ордерів (Market Order) з миттєвим виконанням за найкращою ціною.

FR-07	Система повинна підтримувати ордери типу Stop-Loss та OCO (One Cancels the Other).
FR-08	Система повинна перевіряти наявність достатнього балансу перед прийняттям ордера ("Pre-trade validation").
FR-09	Matching Engine повинен зводити ордери відповідно до алгоритму Price-Time Priority.
FR-10	Система повинна дозволяти скасування відкритих ордерів через UI та API.
FR-11	Система повинна генерувати унікальні депозитні адреси для кожного користувача та підтримуваної мережі.
FR-12	Система повинна автоматично зараховувати депозити після досягнення необхідної кількості підтверджень мережі.
FR-13	Система повинна обробляти запити на виведення коштів (Withdrawal) з перевіркою лімітів та 2FA/Email підтвердженням.
FR-14	API повинен валідувати параметр timestamp та recvWindow для захисту від Replay-атак.
FR-15	API повинен повертати інформацію про комісію за кожну виконану угоду (Trade).
FR-16	Система повинна підтримувати створення API-ключів з правами "Тільки читання" та "Дозвіл торгівлі".
FR-17	Система повинна надсилати WebSocket-повідомлення executionReport при зміні статусу ордера (New, Partially Filled, Filled, Canceled).
FR-18	Система повинна дозволяти переказ коштів між Спотовим та Ф'ючерсним гаманцями (Internal Transfer).
FR-19	Система повинна блокувати виведення коштів на 24 години після зміни налаштувань безпеки (пароль, 2FA).
FR-20	Система повинна надавати історію торгів за період (до 3 місяців безпосередньо, архів — за запитом).
FR-21	Система повинна підтримувати конвертацію дрібних залишків активів ("пилу") у нативний токен біржі (BNB).

FR-22	Адміністративна панель повинна дозволяти блокування акаунтів при виявленні підозрілої активності.

Вимоги до якості (Quality of Service)

Продуктивність (Performance)

ID	Вимога
NFR-01	Час обробки ордера (Matching Latency) повинен бути менше 50 мікросекунд (внутрішня метрика).
NFR-02	Час відповіді REST API (Round-trip time) не повинен перевищувати 100 мс для 95% запитів.
NFR-03	Пропускна здатність системи повинна забезпечувати обробку не менше 100,000 ордерів за секунду (TPS).
NFR-04	Затримка оновлення WebSocket потоків (Market Data) не повинна перевищувати 200 мс від моменту події.

Надійність (Reliability)

ID	Вимога
NFR-05	Доступність системи (Uptime) повинна складати 99.9% (допускаються планові технічні роботи).
NFR-06	У випадку збою Matching Engine, система повинна гарантувати цілісність даних (ACID) без втрати ордерів.
NFR-07	Система повинна мати гаряче резервування (Hot Standby) для критичних вузлів.

Безпека (Security)

ID	Вимога
NFR-08	Усі з'єднання (Web та API) повинні використовувати шифрування TLS 1.2 або вище.

NFR-09	Приватні ключі гаманців (Cold Storage) повинні зберігатися на пристроях без прямого доступу до інтернету (Air-gapped).
NFR-10	Система повинна блокувати IP-адресу після 5 невдалих спроб входу.
NFR-11	Підпис API-запитів повинен здійснюватися алгоритмом HMAC SHA256.
NFR-12	Система повинна проходити регулярні зовнішні аудити безпеки та Penetration Testing.

Зручність (Usability)

ID	Вимога
NFR-13	Інтерфейс повинен підтримувати темну та світлу теми ("Dark Mode").
NFR-14	Повідомлення про помилки API повинні містити зрозумілий код помилки та опис (наприклад, "Code: -2010, Msg: Account has insufficient balance").

Підтримуваність (Maintainability)

ID	Вимога
NFR-15	Система повинна підтримувати версійність API (наприклад, /api/v1/, /api/v3/) для зворотної сумісності.
NFR-16	Логи транзакцій повинні зберігатися мінімум 5 років для аудиту.

Доступність (Availability & Scalability)

ID	Вимога
NFR-17	Система повинна автоматично масштабуватися (Auto-scaling) при різкому зростанні трафіку.
NFR-18	Rate Limits повинні застосовуватися на рівні шлюзу (Gateway) для захисту бекенду від перевантаження.

Відповідність стандартам (Compliance)

ID	Вимога
C-01	Система повинна відповідати вимогам GDPR при роботі з персональними даними користувачів ЄС.
C-02	Процедури KYC/AML повинні відповідати міжнародним стандартам (FATF recommendations).
C-03	Архітектура безпеки повинна відповідати стандарту ISO/IEC 27001.

Вимоги до проєктування та реалізації (Design and Implementation)

Встановлення (Installation)

Оскільки це веб-платформа (SaaS), встановлення на стороні клієнта не вимагається. Користувачам доступна опціональна установка настільних додатків (Electron-based) для Windows/macOS та мобільних додатків. Серверна частина розгортається у контейнеризованому середовищі (Docker/Kubernetes) або bare-metal для деяких компонентів.

Розповсюдження (Distribution)

Архітектура системи є розподіленою мікросервісною:

1. **Matching Engine:** Rust/C++ (для максимальної швидкодії).
2. **API Gateway:** C#/Go/Java (для обробки великої кількості з'єднань).
3. **Web Frontend:** React/Vue.js.
4. **Mobile Apps:** Native (Swift/Kotlin) або Flutter.

Повторне використання (Reusability)

Внутрішні бібліотеки для роботи з криптографією, підключенням до блокчейнів та валідацією ордерів повинні бути виділені в окремі модулі для використання різними сервісами (наприклад, Spot та Futures).

Вартість (Cost)

Основні витрати включають:

1. Комісії мереж блокчейн за консолідацію коштів.
2. Оплата хмарної інфраструктури та трафіку (AWS/Cloudflare).
3. Оплата послуг KYC-провайдерів (за кожну верифікацію).
4. Заробітна плата команди інженерів та служби підтримки.

Верифікація (Verification)

Цей розділ описує методи перевірки, що забезпечують підтвердження виконання вимог, наведених у розділі 3. Для кожної вимоги визначається спосіб перевірки: тестування (Testing), інспекція (Inspection), аналіз (Analysis) або демонстрація (Demonstration).

Верифікація функціональних вимог (Verification of Functional Requirements)

Ця таблиця визначає методи перевірки коректності бізнес-логіки та функцій системи, описаних у підрозділі 3.

ID	Вимога (FR)	Метод перевірки	Опис процедури
FR-01	Реєстрація та вхід з 2FA	Функціональне тестування	Проходження сценарію реєстрації (Happy path) та спроба входу з неправильним кодом 2FA (Negative test).
FR-04	Відображення Order Book	Інспекція + Тестування	Візуальна перевірка стакану в UI та порівняння даних з відповіддю REST API GET /depth.
FR-05	Розміщення Limit ордера	Автоматизоване тестування	Відправка signed POST-запиту до API; перевірка, що ордер з'явився у статусі NEW і відображається в стакані.

FR-09	Алгоритм Price-Time Priority	Аналіз + Unit-тестування	Перевірка логіки Matching Engine на наборі тестових даних: ордери з однаковою ціною мають виконуватися в порядку їх надходження.
FR-11	Генерація депозитних адрес	Функціональне тестування	Запит на генерацію адреси для різних мереж (BTC, ERC20) та валідація формату отриманої адреси.
FR-13	Виведення коштів (Withdrawal)	Тестування сценарію	Спроба виведення суми, що перевищує баланс (очікується помилка), та валідне виведення з підтвердженням по email.
FR-14	Захист від Replay-атак	Тестування безпеки	Відправка API-запиту зі старим timestamp (поза межами recvWindow). Очікується HTTP помилка.
FR-16	Права API-ключів	Тестування доступу	Спроба розмістити ордер, використовуючи API-ключ з правами "Read-only". Очікується помилка 401/403.
FR-17	WebSocket повідомлення	Інтеграційне тестування	Підключення до WS-стріму, розміщення ордера через REST та очікування події executionReport у сокеті.
FR-19	Блокування виводу після зміни пароля	Тестування бізнес-правил	Зміна пароля акаунта та миттєва спроба створення заявки на вивід (має бути заблоковано).

Верифікація нефункціональних вимог (Verification of Non-Functional Requirements)

Ця таблиця визначає методи перевірки якісних показників системи (швидкодія, надійність, безпека), описаних у підрозділі 3.

ID	Вимога (NFR)	Метод перевірки	Опис процедури
NFR-01	Matching Latency < 50 µs	Бенчмаркінг (Performance)	Внутрішній нагрузочний тест ядра Matching Engine із заміром часу між входом ордера в чергу та подією Match.
NFR-02	Час відповіді REST API < 100 ms	Навантажувальне тестування	Використання JMeter/Gatling для відправки серії запитів і вимірювання перцентилів (p95, p99) часу відповіді.
NFR-03	Пропускна здатність > 100k TPS	Стрес-тестування	Подача критичного навантаження на тестовому оточенні для визначення точки відмови системи.
NFR-04	Затримка WebSocket < 200 ms	Інструментальний моніторинг	Порівняння timestamp події на сервері та часу отримання пакету клієнтом у контрольованій мережі.
NFR-05	Доступність 99.9% (Uptime)	Аналіз логів / Моніторинг	Перевірка звітів системи моніторингу (Prometheus/Grafana) за звітний період (місяць).
NFR-08	Шифрування TLS ≥ 1.2	Інспекція (Security Audit)	Використання інструментів типу SSL Labs для перевірки конфігурації веб-сервера та сертифікатів.
NFR-10	Блокування IP (Rate Limiting)	Тестування безпеки	Скрипт, що надсилає запити з частотою, вищою за ліміт, і перевіряє отримання коду HTTP 429 (Too Many Requests).
NFR-11	Валідація HMAC SHA256	Криптографічний аналіз	Перевірка коректності реалізації алгоритму підпису; спроба зміни payload без зміни підпису.
C-01	Відповідність GDPR	Аудит (Compliance)	Юридичний та технічний аудит процедур зберігання персональних даних та механізмів їх видалення.