# Опис серверної частини.

Серверна частина нашого додатку побудована на Node.js. [Node.js®](https://nodejs.org/uk/) — це JavaScript–оточення побудоване на JavaScript–рушієві Chrome V8.

У документації до Node.js зазначено, що як асинхронне подієве JavaScript–оточення, Node.js спроектований для побудови масштабованих мережевих додатків. Для кожного з’єднання викликається функція зворотнього виклику, проте коли з’єднань немає Node.js засинає.

Це контрастує з більш загальною моделлю в якій використовуються паралельні OS потоки. Такий підхід є відносно неефективним та дуже важким у використанні. Більше того, користувачі Node.js можуть не турбуватись про блокування процесів, оскільки немає жодних блокувань. Майже жодна з функцій у Node.js не працює напряму з I/O, тому процес не блокується ніколи. Оскільки нічого не блокується на Node.js легко розробляти масштабовані системи.

Для забезпечення створення http-сервера і роботи додатка за протоколом http був використаний фреймворк [Express - Fast, unopinionated, minimalist web framework for Node.js](https://expressjs.com). Як стверджує сайт Express.js Express — це мінімальний і гнучкий фреймворк веб-додатків Node.js, який надає надійний набір функцій для веб- та мобільних додатків.

Для взаємодії з клієнтською частиною нашого додатку за протоколом Web Socket була використана бібліотека [Socket.IO](https://socket.io/docs/v4/). Socket.IO — це бібліотека, яка забезпечує двонаправлений зв'язок між клієнтом і сервером із низькими затримками та на основі подій. Вона побудована на основі протоколу WebSocket і надає додаткові гарантії, такі як повернення до тривалого опитування HTTP, якщо браузер не підтримує роботу за протоколом web socket або автоматичне повторне підключення.

Для зберігання даних додатку використовується система керування базою даних [PostgreSQL](https://www.postgresql.org). PostgreSQL – це потужна система об’єктно-реляційних баз даних з відкритим вихідним кодом, яка використовує та розширює мову SQL у поєднанні з багатьма функціями, які безпечно зберігають і масштабують найскладніші робочі навантаження даних.

Проаналізувавши предметну область нашого завдання прийшли до висновку, у нас існує три окремих сутності, а саме користувач, «кімната для переговорів» або чат, повідомлення.

Користувач має наступні властивості: логін, пароль, ім’я, що відображається, аватар – графічне зображення, яке пов’язане з цим користувачем. Для зберігання аватару будемо використовувати файлову систему, а в базі даних будемо зберігати тільки ім’я файлу.

«Кімната для переговорів» повинна мати такі властивості

Ідентифікатор, тип кімнати (коли програма буде розвиватися, з’явиться можливість створювати не тільки персональні чати, але і групи та інформаційні канали. Крім того в подальшому функціонал програми буде передбачати можливість блокування «кімнат» адміністратором або співрозмовником. Тому в базі даних такі можливості повинні бути передбачені. Назва кімнати є індивідуальною для кожного користувача і тому не повинна бути пов’язана з цією таблицею.

Повідомлення має такі властивості: автор повідомлення, кімната, в яку це повідомлення відправлено, та власне текст повідомлення.

Сутності мають наступні зв’язки;

Користувачі пов’язані з повідомленнями зв’язком «один до багатьох» через поле в таблиці повідомлень – «автор».

«Кімнати» пов’язані з повідомленнями зв’язком «один до багатьох» через поле в таблиці повідомлень «призначення».

«Кімнати» пов’язані з користувачами зв’язком «багато до багатьох». Для реалізації такого зв’язку необхідно ввести додаткову таблицю, що пов’язує кімнати та користувачів. Додатково в базі даних заведена таблиця для зберігання сесій фреймворка Express. ERD діаграма наведена нижче.



Для спрощення побудови SQL запитів, необхідних для роботи програми створено 2 представлення:

room\_members – встановлює зв'язок між членами однієї «кімнати»

CREATE OR REPLACE VIEW public.room\_members

    AS

     SELECT ro.member AS owner,

    o.user\_name AS owner\_name,

    ro.room\_id,

    ro.room\_name,

    rm.member,

    mb.user\_name AS member\_name,

    ro.id as owner\_ru\_id,

    rm.id as member\_ru\_id

   FROM room\_users ro

     JOIN room\_users rm ON ro.room\_id = rm.room\_id AND ro.member <> rm.member

     JOIN users o ON ro.member = o.id

     JOIN users mb ON rm.member = mb.id;

Contacts відображає для кожного користувача його список контактів, тобто перелік користувачів, з яким у даного користувача відсутні «переговорні кімнати»

CREATE OR REPLACE VIEW public.contacts

 AS

 SELECT u.id AS owner,

    u1.id,

    u1.login,

    u1.user\_name,

    u1.state,

    u1.avatar,

    u1.created\_at,

    u1.modified\_at

   FROM users u

     JOIN users u1 ON u.id <> u1.id

     LEFT JOIN room\_members rm ON u.id = rm.owner AND u1.id = rm.member

  WHERE rm.room\_id IS NULL

  ORDER BY u1.id;

Для забезпечення роботи нашої програми з базою даних використовується драйвер [node-postgres](https://github.com/brianc/node-postgres). Node-postgres це неблокуючий клієнт PostgreSQL для Node.js. Node-postgres має наступні властивості:

* чистий клієнт JavaScript і власні прив’язки бібліотеки libpq мають однаковий API;
* пул підключень;
* розширене приведення типу даних між PostgreSQL та JavaScript;
* підтримка властивостей PostgreSQL:
  + параметризовані запити;
  + іменовані оператори з кешуванням плану запитів;
  + асинхронні сповіщення за допомогою LISTEN/NOTIFY;
  + масовий імпорт та експорт за допомогою COPY TO/COPY FROM.

Для взаємодії з базою даних створений модуль db\index.js. При завантаженні цього модуля створюються пул з’єднань з базою даних, використовуючи рядок приєднання до бази даних зазначений в змінній оточення.

const connectionString = process.env.DATABASE\_URL;

pool = new Pool({

      connectionString,

      ssl: false,

    })

Чому використовується пул з’єднань?

Підключення нового клієнта до сервера PostgreSQL вимагає рукостискання, яке може тривати 20-30 мілісекунд. Протягом цього часу узгоджуються паролі, може бути встановлений SSL, а інформація про конфігурацію передається клієнту та серверу. Виникнення цих витрат кожного разу , коли ми хочемо виконати запит, істотно уповільнює роботу нашої програми.

Сервер PostgreSQL може обробляти лише обмежену кількість клієнтів одночасно . Залежно від доступної пам’яті вашого сервера PostgreSQL, ви можете навіть вийти з ладу сервера, якщо підключите необмежене число клієнтів.

PostgreSQL може обробляти лише один запит на одному підключеному клієнті за принципом «першим прийшов – першим вийшов». Якщо веб-додаток із багатьма клієнтами використовує лише один підключений клієнт, усі запити між усіма одночасними запитами будуть конвеєрними та виконуватися послідовно, один за одним. Не добре!

Виходячи з цих міркувань в програмі обрано механізм роботи через пул. Максимальна кількість одночасних клієнтів, які можуть бути підключеними через пул є 10. Якщо буде більше одночасних запитів, то вони будуть ставитись в чергу. Метод getClient() повертає нового клієнта з пула.

В цьому ж модулі реалізований метод який використовується для виконання всіх параметризованих запитів до бази даних:

  /\*\* виконує SQL запит з вказаним клієнтом

   \* @param { PoolClient } client

   \* @param { String } sql

   \* @param {Array} params

   \* @returns  { Promise<pg.Result> } повертає результат виконання sql

   \*/

  async clientQuery(client, sql, params) {

    try {

      console.dir({ sql, params });

      const result = await client.query(sql, params);

      return result;

    } catch (error) {

      if (!error.type) {

        error.type = 'db error';

      }

      if (!error.source) {

        error.source = 'db index clientQuery';

        console.log(error);

      }

      throw error;

    }

  },

};

В програмі використовуються виключно параметризовані запити до бази даних. Це дає можливість запобігти атакам на додаток, які називаються SQL Injection. SQL Injection – це техніка введення коду, яка може знищити базу даних. SQL Injection є однією з найпоширеніших методик веб-зламу. SQL Injection – це розміщення шкідливого коду в операторах SQL через введення веб-сторінки.

В модулі db/Model.js визначений клас Model, в якому реалізовані основні операції по роботі з таблицями в базі даних. В якості властивостей цей клас приймає назву таблиці та клієнта з пулу, під’єднаного до бази даних. В класі є наступні методи

find: Побудова та виконання звичайного select до таблиці this.table. Методу

в якості параметрів передається масив з переліком назв колонок таблиці, які будуть повертатися, як результат виконання SQL, перелік умов для виборки у вигляді об’єкту JavaScript в форматі {key: value}. Також передається масив колонок для побудови сортування. Результатом є масив об’єктів JavaScript;

findOne: Аналогічний попередньому, але повертає тільки перший рядок результату;

delete: Видалення записів з таблиці. Критерії відбору передаються в якості об’єкту JavaScript в форматі {key: value}. Результатом роботи методу є кількість рядків, які були видалені;

insert: Додавання запису в таблицю. Назви колонок та їх значення передаються в параметрі columns у вигляді об’єкту JavaScript в форматі {key: value}. В масиві returning передається перелік колонок запису в таблиці, що був доданий. Результатом є масив об’єктів JavaScript;

update: Внесенні змін в таблицю. Назви колонок та їх значення передаються в параметрі columns. Критерії відбору передаються в якості об’єкту JavaScript в форматі {key: value} в параметрі params. Повертається кількість змінених рядків.

Для роботи з конкретними таблицями визначені класи-нащадки класу Model, в яких реалізовані специфічні методи для цих сутностей.

Клас User визначений в модулі user/User.js. У зв’язку із тим, що дана сутність є важливою з точки зору безпеки (в таблиці зберігається хеш пароля) в даному класі визначено перелік колонок таблиці, які можуть повертатися з бази даних (пароль не передається). Визначено наступні методи:

findUser – пошук користувача за параметрами. Наприклад за його логіном.

У зв’язку із тим, що дуже часто використовується пошук користувача за його ідентифікатором, ця процедура винесена в окремий метод getUserById(userId), де ідентифікатор передається як параметр.