УДК 004.4:004.056

РОЗРОБКА ВЕБ-ДОДАТКУ ДЛЯ ЗБЕРІГАННЯ ТА КЕРУВАННЯ ПАРОЛЯМИ

Горішня К.О.
Науковий керівник – к.т.н., проф. Бондарєв В.М.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна
тел.: +38(066) 524-61-51, e-mail: kateryna.horishnia@nure.ua

Web development is an important field in today's world as an ever-increasing number of people use the internet in their daily lives. Websites are an integral part and continue to be relevant and useful tools for people and businesses. Various websites are created daily and used by billions of people.

The purpose of my development is to create a «Password Manager» web application that will help users store and manage their passwords in a safe and accessible place. Such services have become very relevant in recent years, as users use more and more websites and services that require entering passwords.

Мета роботи – створити веб-додаток, де користувачі можуть зберігати та керувати своїми паролями в безпечному та доступному місці. Такі сервіси стали дуже актуальними в останні роки, оскільки користувачі використовують все більше ресурсів, які вимагають введення паролів.

Однією з головних переваг веб-додатку «Менеджер паролів» є захист конфіденційної інформації. Користувачі, які застосовують один і той же пароль для різних вебсайтів, ризикують, що їхні дані можуть бути скомпрометовані у випадку, якщо один із сайтів, буде зламаний. «Менеджер паролів» дозволяє використовувати унікальні та складні паролі для кожного вебсайту, що зменшує ризик крадіжки їхніх даних.

Іншою важливою функцією веб-додатку є легкий доступ до паролів з будь-якого пристрою з доступом до Інтернету. Користувачам більше не потрібно запам'ятовувати або записувати свої паролі на папері, щоб мати до них доступ. Можна просто зайти на свій обліковий запис зі свого комп'ютера, планшета або смартфона та знайти необхідний пароль.

Для реалізації веб-додатку «Менеджер паролів» будемо використовувати наступні допоміжні технології.

Angular (TypeScript, HTML, CSS) – для розробки фронтенду веб-додатку «Менеджер паролів». Angular – для створення зручного та ефективного інтерфейсу, що дозволяє користувачам додавати, редагувати та видаляти свої паролі. TypeScript – для підвищення продуктивності розробки та полегшення підтримки коду. HTML використовується для створення розмітки вебсторінки «Менеджер паролів», тоді як CSS – для оформлення цієї розмітки та надання вигляду інтерфейсу користувача [1].

Express.js/Node.js – для розробки бекенду веб-додатку «Менеджер паролів». Node.js – для розробки серверної логіки, яка відповідає за

збереження та обробку даних користувачів. Express.js – для створення API, яке дозволяє звертатися до серверу та обробляти запити.

JavaScript – для створення API-маршрутів та реалізації бізнес-логіки на сервері, за допомогою Node.js та Express.js [2].

Postman – для тестування та перевірки API-маршрутів.

Дані користувачів та їх паролі зберігаються в базі даних MongoDB. Для забезпечення захисту даних користувачів застосуємо бібліотеку CryptoJS, яка підтримує симетричне шифрування з ключем. Коли користувач вводить свій пароль, він шифрується і зберігається в базі даних. Взаємодія веб-сторінки «Менеджер паролів», серверу та бази даних представлена на рисунку 1.

Перш ніж почати користуватися онлайн-сервісом, користувач повинен зареєструватися та увійти до свого особистого кабінету. Після цього він отримає можливість додавати, видаляти, редагувати паролі та логіни (інтерфейс сторінки користувача представлено на рисунку 2).

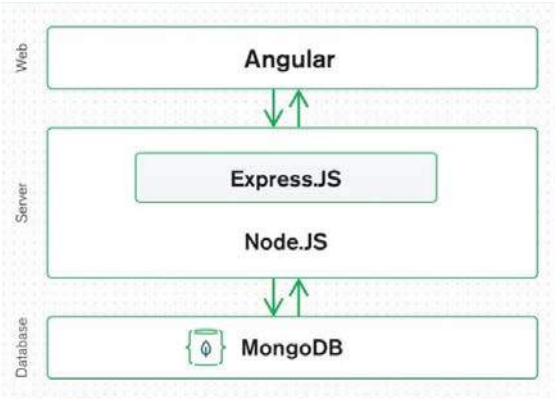

Рисунок 1 – Схема взаємодії технологій, що використовуються у веб-додатку «Менеджер паролів»

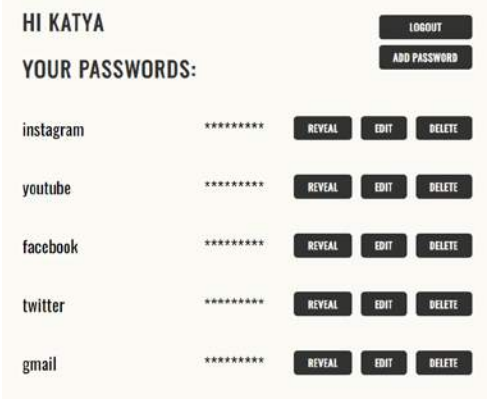

Рисунок 2 – Скріншот інтерфейсу сторінки користувача веб-додатку «Менеджер паролів»

Отже, веб-додаток «Менеджер паролів» є важливим та актуальним інструментом для збереження та керування паролями в безпечному та доступному місці. Він допоможе користувачам захистити свою конфіденційну інформацію, зменшить ризик втрати або забуття паролів, та забезпечить зручний доступ до них з будь-якого місця за умови наявності Інтернету. Надалі плануємо покращити безпеку даних користувачів додатковим шифруванням, щоб вся інформація зберігалася на сервері в зашифрованому форматі.

Список використаних джерел:

1. Duckett, D. (2011). HTML and CSS: Design and Build Websites. Wiley.

2. Haverbeke, M. (2018). Eloquent JavaScript: A Modern Introduction to Programming. No Starch Press.