Годлевський О.О., здобувач
Фант М.О., к.філол.н., доцент
Державний університет «Житомирська політехніка»

БЕЗПЕЧНА АУТЕНТИФІКАЦІЯ ТА УПРАВЛІННЯ КОРИСТУВАЧАМИ У ВЕБДОДАТКАХ НА ОСНОВІ NEST.JS ТА NEXT.JS

У сьогоденному онлайн-світі важливо переконатися, що лише потрібні люди можуть отримати доступ до веб-сайтів. Щорічно кібер -ризики можуть спричинити порушення даних, несанкціоноване введення ресурсів або вразливості системи. Основна мета розробки сучасних веб -додатків - це не лише гарантування простоти для клієнтів, а й максимальна безпеки. Nest.js і Next.js дозволяє створювати безпечні системи з контролем доступу та управлінням ролями користувачів. Це дослідження аналізує стратегії аутентифікації, їхні переваги та недоліки, та рекомендує найкращу практику.

Існує декілька основних підходів до аутентифікації користувачів у веб-додатках, кожен із яких має свої особливості та сфери застосування. Перший спосіб JWT. Є одним із найбільш поширених методів аутентифікації. У цьому підході сервер генерує цифровий токен, який містить зашифровану інформацію про користувача. Токен може бути збережений у localStorage, sessionStorage або у HTTP-only cookie. Його переваги це безстейтова автентифікація (сервер не зберігає інформацію про сесію) та простота інтеграції з API. Також наявні і недоліки, а саме це, якщо access-token скомпрометовано, зловмисник отримує доступ до акаунту. Другий спосіб це використання NextAuth.js. Це бібліотека, що забезпечує інтеграцію OAuth. До переваг можна віднести легкість інтеграції з популярними постачальниками OAuth та гнучкості налаштування провайдерів. Щодо недоліків, то це менший контроль над внутрішньою логікою у порівнянні з власною реалізацією. І третій спосіб це за допомогою OAuth 2.0 та OpenID Connect. OAuth 2.0 – це протокол авторизації, який дозволяє користувачам входити через сторонні сервіси (Google, Facebook, GitHub тощо). OpenID Connect є розширенням OAuth 2.0 для ідентифікації користувачів. Головна перевага це додатковий рівень безпеки, оскільки пароль не передається додатку. Недоліки це залежність від сторінніх сервісів.

У роботі реалізовано систему аутентифікації на основі Nest.js для бекенду та Next.js для фронтенду з використанням наступних підходів:

- Реєстрація та аутентифікація користувачів реалізована через JWT з access та refresh-токенами; OAuth 2.0 використовується для входу через Google;
- База даних – Postgresql у поєднанні з Prisma для управління користувачами;
- HTTP-only cookies використанно для збереження токенів, щоб зменшити ризики XSS-атак.

Коли йдеться про автентифікацію користувачів та управління їхніми обліковими записами, то забезпечення безпеки є головним ключем до розробки веб-додатків. Можливі загрози, з якими можуть зіштовхнутися веб-додатки: несанкціонований доступ, витік персональних даних, DDoS-атаки та надмірне навантаження. Щоб запобігти цим загрозам, слід використовувати заходи безпеки, а саме: шифрування паролей, використання refresh-token для оновлення сесії, використання CAPTCHA для захисту від ботів та валідацію вхідних даних

Даний аналіз аутентифікації дозволяє забезпечити рівень безпеки завдки використанню JWT, bcrypt тощо. Гнучко масштабувати систему та додавати нові можливості. Надавати зручний інтерфейс користувачам через Next.js. Підтримувати вхід через Google, що спрощує аутентифікацію.

Можливі напрямки подальшого розвитку: додавання двофакторної автентифікації через SMS або TOTP. Інтеграція з GoogleFit для персоналізованого досвіду. Розширення логування для моніторингу активності користувачів.

Запропонована система є ефективним рішенням для сучасних веб-додатків, що потребують безпечної та масштабної автентифікації.

Список використаних джерел:

1. Nest.js Documentation: Introduction. Nest.js Documentation. URL: https://docs.nestjs.com (дата звернення: 21.03.2025).
2. Nest.js Documentation: Prisma. Nest.js Documentation. URL: https://docs.nestjs.com/recipes/prisma (дата звернення: 21.03.2025).
3. Next.js Documentation: Authentication. Next.js Documentation. URL: https://nextjs.org/docs/app/building-your-application/authentication (дата звернення: 21.03.2025).