**Теоретичне завдання**

**1. В чому різниця між авторизацією і аутентифікацією?**

Аутентифікація − це процес перевірки того, що користувач, який намагається отримати доступ до ресурсів, є тим, за кого він себе видає. Це зазвичай здійснюється за допомогою введення ідентифікатора користувача та пароля. Після успішної аутентифікації користувача система надає йому токен доступу, який може використовуватися для подальшої авторизації.

Авторизація − це процес перевірки того, що користувач, який намагається отримати доступ до конкретних ресурсів, має дозвіл на їх використання. Дозвіл надається системою на основі токену доступу, отриманого під час аутентифікації. У процесі авторизації система перевіряє, чи має користувач право на доступ до запитуваного ресурсу, і, якщо так, то надає йому доступ.

Аутентифікація визначає, хто користувач, а авторизація − що він можете робити в системі.

**2. Що таке OAuth і для чого використовується?**

OAuth − це відкритий протокол авторизації, який використовується для забезпечення безпечного доступу до захищених ресурсів. OAuth дозволяє стороннім додаткам отримувати доступ до захищених ресурсів без необхідності передавати ім'я користувача та пароль сторонньому додатку.

За допомогою OAuth користувач може дозволити доступ до свого облікового запису сторонній службі. OAuth дозволяє користувачам контролювати, кому та який рівень доступу надається до їх облікового запису.

Основна ідея протоколу полягає в тому, що сторонній додаток отримує доступ до захищених ресурсів, надаючи власний токен доступу, який був виданий авторизаційним сервером після того, як власник ресурсу надав дозвіл на доступ до свого облікового запису.

**3. Які є типи авторизації користувачів?**

Basic Authentication − це простий метод авторизації, де клієнт надсилає свої ім’я користувача та пароль на сервер. Для цього використовується заголовок Authorization, який містить базовий кодувальний блок.

Form-based Authentication − це метод, який використовується для авторизації користувачів, що вимагає введення логіна та пароля на сторінці веб-додатка. Дані авторизації надсилаються на сервер у вигляді POST-запиту.

Social Authentication − це метод, який дозволяє користувачам авторизуватися за допомогою своїх облікових записів у соціальних мережах.

Certificate-based Authentication − це метод, який використовується для авторизації користувачів за допомогою сертифікатів. У цьому методі користувач має власний сертифікат, який використовується для підтвердження його особи.

Token-based Authentication − це метод, який дозволяє користувачам отримувати доступ до захищених ресурсів за допомогою токенів. Токен може бути згенерований під час аутентифікації користувача та використовуватися як ідентифікатор, що дозволяє доступ до ресурсів.

**4. Який тип авторизації було використано в поточній роботі?**

У поточній роботі було використано Token-based Authentication, а саме авторизацію за допомогою JWT токенів. Це механізм авторизації, що використовує JSON Web Tokens для передачі інформації про авторизованого користувача між сторонами. Після успішної аутентифікації JWT токен генерується на сервері, підписується та повертається клієнту. Клієнт може потім передавати цей токен у кожен запит до серверу для перевірки його валідності та авторизації на доступ до ресурсів сервера.