

JWA (JSON Web Algorithms) специфікації, виділяють групи алгоритмів шифрування з використання симетричних та асиметричних алгоритмів.

Інформаційна частина складається з наборів пар ключ-значення (JWT Claims Set), що в загальному випадку містять мінімально необхідні для аутентифікації та авторизації в системі дані про користувача, якому даний токен належить. Інформаційна частина з чотирьох полів, що містять певні значення, має наведений на прикладі вигляд:

```
{  
  "sub": "1234567890",  
  "name": "Honcharenko Kostiantyn",  
  "company": "VNTU",  
  "auth": 4,  
  "exp": 1492883341  
}
```

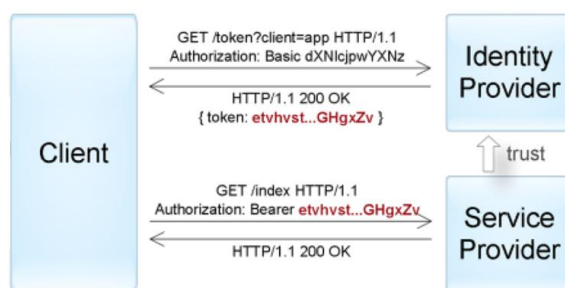


Рис.1 – Принцип роботи JWT

Недоліком використання токенів є необхідність обмеження довжини заголовка у запиті для деяких серверів. У таких випадках до інформаційної частини токена варто вводити лише необхідні дані. Крім цього, токен містить термін дії, який відповідно до вимог безпеки повинен бути не дуже тривалим, а після його закінчення необхідно формувати новий токен.

Визначено, що основною перевагою використання JWT-токенів є відсутність необхідності зберігання будь-яких даних про токени чи самі токени на сервері. Кожен токен містить всі необхідні дані для перевірки його достовірності, а також дає можливість передавати довільний набір даних. Серверна частина забезпечує формування, підпис та видачу JWT-токенів, перевірку дійсності токенів у вхідних запитах. Також при створенні токена задається параметр, який відповідає за час його дії та який неможливо знімати. Таким чином виникає проблема інвалідації токена.

Висновки

Розглянуто особливості існуючих методів автентифікації користувача у веб-сервісах. Обґрунтовано вибір технології JSON Web Token для подальшої розробки програмного модулю автентифікації користувача. Визначено проблему інвалідації токена, яка буде вирішена шляхом використання бази даних для збереження стану точена.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Річард Сміт, Аутентификация: от паролей до открытых ключей / Річард Сміт — М. Вільямс, 2002.
2. А. Еременко, А. Сулавко , Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку — М: Издательский дом Университета "Синергия", 2004. — 13 с.
3. Habrhabr [Электронный ресурс] – Режим доступа: habr.com/ru/company/dataart/blog/311376

Гончаренко Костянтин Олександрович — студент групи ІКН-17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: kostinadress@gmail.com

Науковий керівник: **Суприган Олена Іванівна** — канд. техн. наук, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Honcharenko Kostiantyn O. — student of Information Technologies and Computer Engineering Department, ІCS17m, Vinnytsia National Technical University, Vinnytsia, e-mail: kostinadress@gmail.com

Supervisor: **Supryhan Olen I.** — Ph.D., Assistant Professor of the computer science Chair, Vinnytsia National Technical University, Vinnytsia.