УДК 004.428.2

**В. О. Фоучек**[1]
**С. А. Лухверчик**[2]
**І. В. Богач**[1]

# БЕЗПЕКА ТА ІМПЛЕМЕНТАЦІЯ АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ В ВЕБ-ДОДАТКАХ ЗА ДОПОМОГОЮ JWT ТА HTTPS ПРОТОКОЛУ

[1] Вінницький національний технічний університет
[2] Донецький національний університет імені Василя Стуса

***Анотація***
*В роботі розглянуто принципи та проектування JWT, а саме підхід до вимог та методів реалізації системи авторизації та аутентифікації, на основі JSON Web Tokens (JWT).*
**Ключові слова:** безпека, аутентифікація, авторизація, JWT, HTTPS.

***Abstract***
*The paper discusses the principles and design of JWT, namely, the approach to the requirements and methods of implementing an authorization and authentication system based on JSON Web Tokens (JWT).*
**Keywords**: security, authentication, authorization, JWT, HTTPS.

## Вступ

В сучасному інформаційному середовищі, де забезпечення безпеки даних та захист приватності користувачів стають дедалі більшою проблемою, системи автентифікації та авторизації відіграють ключову роль у забезпеченні цих аспектів. У цьому контексті виникає необхідність розробки та впровадження ефективних та безпечних механізмів автентифікації та авторизації для веб-додатків. Одним з таких механізмів є використання JWT, які надають зручний та безпечний спосіб обміну інформацією між сторонами, та HTTPS, що є дотриманням захисту безпеки передачі даних.

## Результати дослідження

У роботі було проведено аналіз JWT, та його процесу роботи. Він надає безпечний спосіб відправлення інформації між двома сторонами. Нижче ми описали структурно його принцип створення, впровадження та роботи розподіливши це на чіткі послідовні етапи, наведені нижче:

Генерація JWT:

1. Імітер (iss): Ідентифікатор сервісу, який генерує токен.
2. Суб'єкт (sub): Ідентифікатор користувача.
3. Аудиторія (aud): Ідентифікатор сервісу, для якого призначений токен.
4. Час видачі (iat): Час створення токена.
5. Час закінчення дії (exp): Час, коли токен перестає бути дійсним.
6. Токен має бути підписаний використовуючи безпечний ключ.

Аутентифікація:

1. Користувач подає свої аутентифікаційні дані (наприклад, логін і пароль).
2. Система перевіряє ці дані та генерує JWT, якщо дані коректні.
3. JWT відправляється користувачу як доказ аутентифікації.

Авторизація:

1. При спробі доступу до захищеного ресурсу користувач відправляє JWT разом з запитом.
2. Система перевіряє JWT (валідність, час життя та інші претензії).
3. Якщо токен дійсний, система надає доступ до запитаного ресурсу.

Заходи безпеки:

1. Використання HTTPS для захисту даних при передачі.

2. Строге управління ключами для підпису JWT.
3. Обмеження часу життя токена для зменшення ризику використання вкрадених токенів.
4. Перевірка на наявність CSRF (Cross-Site Request Forgery) атак.
5. Опціонально, використання JWE (JSON Web Encryption) для шифрування токенів.

Реалізація:

При реалізації системи авторизації та аутентифікації на основі JWT важливо вибрати надійні бібліотеки та фреймворки, які підтримують стандарти безпеки та пропонують достатні можливості для контролю над процесом аутентифікації та авторизації.

Ця специфікація встановлює основні вимоги та керівні принципи для створення безпечної та ефективної системи авторизації та аутентифікації на основі JWT, але конкретні деталі реалізації можуть варіюватись в залежності від конкретних потреб і умов використання.

Використання HTTPS

Вимоги для використання HTTPS (рис. 1) включає в себе ретельне планування та врахування різноманітних аспектів безпеки, сумісності та виконання. HTTPS (Hypertext Transfer Protocol Secure) є розширеним варіантом HTTP, який захищає передачу даних між клієнтом і сервером за допомогою шифрування.

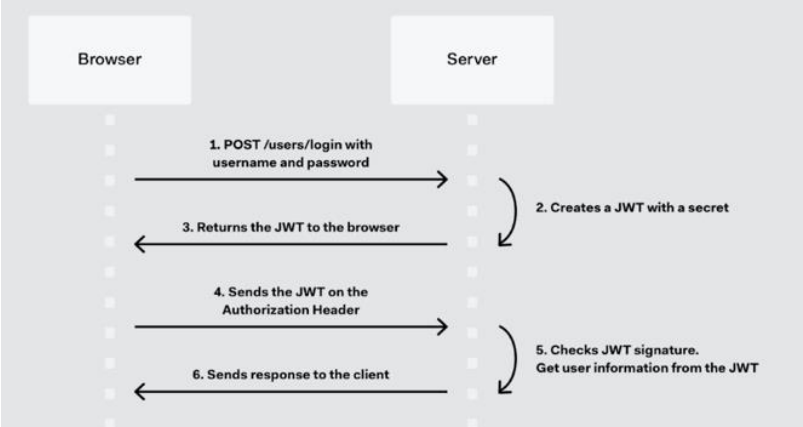


Рис. 1. Основні компоненти HTTPS

1. SSL/TLS Сертифікати: Використання SSL (Secure Sockets Layer) або TLS (Transport Layer Security) сертифікатів для шифрування з'єднань та верифікації ідентичності сервера. Сертифікати повинні бути видані надійним сертифікаційним органом (CA).
2. Ключові Параметри Шифрування:
   а) Сильне Шифрування: Використання сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard) з ключем щонайменше 256 біт.
   б) Версії Протоколу TLS: Рекомендується використовувати TLS версії 1.2 або вище для забезпечення найкращого рівня безпеки.
   в) Список Шифрів (Cipher Suite): Налаштування сервера для підтримки безпечного набору шифрів, що запобігає атакам, пов'язаним з вразливими шифрами.
3. HSTS (HTTP Strict Transport Security): Конфігурація сервера для використання HSTS, що примушує клієнтські браузери використовувати безпечні з'єднання при доступі до сайту.

## Висновки

Реалізація системи автентифікації та авторизації на основі JWT відіграє важливу роль у забезпеченні безпеки веб-додатків. Використання HTTPS та дотримання заходів безпеки є критичними для запобігання атак та забезпечення надійності системи. Однак, варто зауважити, що конкретні деталі реалізації можуть відрізнятися залежно від контексту та потреб конкретного веб-додатку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *"JSON Web Tokens Introduction". JWT Documentation.* [Електронний ресурс] - https://jwt.io/introduction/

2. *Dan Moore & Brian Pontarelli (2022). Breaking down JSON Web Tokens: From pros and cons to building and revoking* [Книга]

3. *"What Is HTTPS & How Does It Work?"* [Електронний ресурс] - https://www.semrush.com/blog/what-is-https/

***Фоучек Володимир Олексійович –*** *студент групи ЗАКІТ-20б, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: vinvova555333@gmail.com*

***Лухверчик Сергій Андрійович*** *– студент групи Б20_Д/122-Б, кафедра інформаційних технологій, факультет інформаційних і прикладних технологій, Донецький національний університет імені Василя Стуса, м.Вінниця, e-mail: serhiilukhverchyk@gmail.com*

***Богач Ілона Віталіївна*** *– к.т.н., доцент кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: lona.bogach@gmail.com*

***Fouchek Volodymyr Oleksiiovych –*** *student of 3ACIT-20B group, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: vinvova555333@gmail.com*

***Lukhverchyk Serhii Andriyovych****- student of group B20_D/122-B, Department of Information Technologies, Faculty of Information and Applied Technologies, Vasyl' Stus Donetsk National University, Vinnytsia, e-mail: serhiilukhverchyk@gmail.com*

***Bogach Ilona Vitaliivna*** *– Associate Professor of Automation and Intelligent Information Technologies, Faculty of Computer Systems and Automatics Vinnytsia National Technical University, Vinnytsia, e-mail: lona.bogach@gmail.com*