- звернення суб'єкта до електронного сервісу ініціює запит сервісу щодо отримання даних атрибутів;

- для безпечного надання атрибутів суб'єкт здійснює авторизований вхід до додатку підпису на основі атрибутів;

- додаток надає запит щодо сеансу обміну атрибутами сервісу служби контролю;

- сервіс здійснює повторну аутентифікацію користувача (дзвінком, надсиланням цифрового коду на телефон або QR коду тощо);

- після авторизації користувача сервіс перевіряє наявність GDPR-сертифікації електронного сервісу, визначає перелік атрибутів, які вимагає сервіс і передає інформацію-запит підписанту;

- підписант приймає рішення щодо передачі кожного атрибуту в електронному сервісу і підтверджує своє рішення позначенням атрибутів для передачі та наданням загального підтвердження;

- за згодою підписанта сервіс надає дозвіл додатку передати атрибути сервісу.

Для сервісів, якими підписант користується постійно, процедура може бути спрощена через створення в додатку шаблонів заздалегідь погоджених (в попередніх сеансах) наборів атрибутів для взаємодії з сервісом.

Застосування технології цифрового підпису з використанням атрибутів дозволяє спростити дії власника особистих даних при підписанні документів в системах електронного документообігу, збільшити захищеність конфіденційних (особистих) даних, реалізувати надання мінімально-необхідного набору даних у відповідності до вимог GDPR, а також убезпечити постачальників послуг від надання неправдивої інформації замовником-підписантом.

Список використаних джерел

1. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL:https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 09.11.2023).
2. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 09.11.2023).
3. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII, редакція від 19.11.2022. URL:https://zakon.rada.gov.ua/laws/show/675-19. (дата звернення: 09.11.2023).
4. Ke Gu, Keming Wang, Lulu Yang Traceable attribute-based signature. Journal of Information Security and Applications. Volume 49. 2019. Article ID 102400.
5. F2P-ABS: A Fast and Secure Attribute-Based Signature for Mobile Platforms. Security and Communication Networks. Volume 2019, Article ID 5380710. 12p.
6. 10 кращих програм для цифрового підпису. Apix-drive блог. URL:https://apix-drive.com/ua/blog/reviews/10-krashih-program-dlja-cifrovogo-pidpisu (дата звернення: 09.11.2023).
7. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 4.5.2016. 88 p.

РИЖКОВ А. К., ВОЙЦЕХОВСЬКА О. В., ГОРОДЕЦЬКА О. С.
Вінницький національний технічний університет

АНАЛІЗ МЕТОДІВ АВТОРИЗАЦІЇ ПРИ ПРОЕКТУВАННІ СЕРВЕРНОЇ ЧАСТИНИ ВЕБ-ЗАСТОСУНКУ

Анотація: В роботі проведено аналіз методів авторизації користувачів у веб-застосунку. Розглянуто основні аспекти використання JWT токенів для авторизації, зокрема їх структуру, генерацію та перевірку, а

також способи їх збереження на клієнтському боці через cookies.
Ключові слова: авторизація, аутентифікація, Jwt-токен, Cookie.
Abstract: The article analyzes user authorization methods in the web application. The main aspects of using JWT tokens for authentication are considered, in particular their structure, generation, and validation, as well as the methods of storing them on the client side through cookies.
Keywords: authorization, authentication, Jwt-token, Cookie.

Вступ

В сучасному контексті інформаційних технологій забезпечення безпеки та аутентифікації користувачів у веб-застосунках є актуальною і складною проблемою. Для збереження конфіденційності даних та контролю доступу до ресурсів необхідно впроваджувати ефективні методи авторизації. В роботі проведено аналіз методів аутентифікації користувачів у контексті проектування серверної частини веб-застосунків. Одним із ключових аспектів цього дослідження є використання JWT-токенів (JSON Web Tokens) [1] та механізму для їх збереження на стороні клієнта через cookies (куки) [2]. JWT-токени стали популярним інструментом для спрощення аутентифікації та контролю доступу у веб-застосунках завдяки їхній простоті та ефективності, тому тема роботи є актуальною.

Мета даної роботи полягає в аналізі методів для збереження JWT-токенів на стороні клієнта через куки, а також основних переваг та обмежень використання цих токенів для аутентифікації користувачів. Це дасть можливість визначити, як ці технології взаємодіють в контексті безпеки та ефективності, і надати практичні рекомендації для їх використання під час розробки веб-застосунків.

Результати досліджень

Результати дослідження вказують на різні аспекти використання JWT-токенів та механізму збереження токенів оновлення на стороні клієнта через куки.

Як перевагу, слід відмітити, що JWT-токени ефективні та зручні у використанні. Вони дозволяють здійснювати аутентифікацію користувачів з обмеженими витратами ресурсів. Крім того, JWT-токени мають зрозумілу структуру та містять корисну інформацію про користувача, що спрощує обробку даних при роботі з авторизацією та ідентифікацією (рисунок 1).

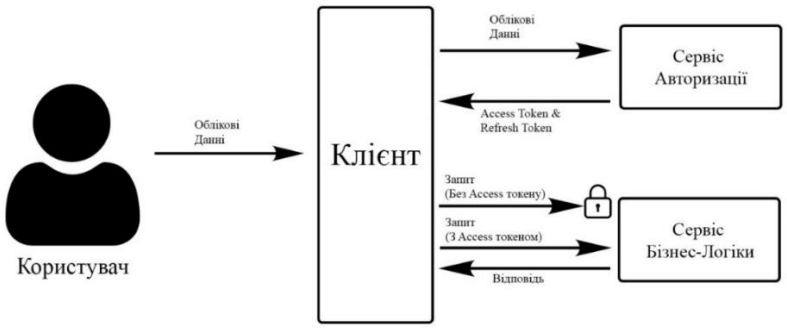

Рисунок 1 – Узагальнена схема механізму авторизації

З рисунка видно, що сервіс бізнес логіки захищений авторизацією за JWT-токеном. Коли неавторизований користувач відправить запит для отримання даних із сервісу бізнес-логіки, він отримає помилку 401 (Unauthorized) у відповідь. Тому спочатку користувач повинен ввести свої облікові данні і надіслати їх на сервіс авторизації. Якщо такий користувач зареєстрований, для нього створиться токен доступу, який містить в собі інформацію про роль користувача, залежно від якої користувачу будуть доступні на сайті різні функціональні можливості. Так, наприклад, модератор зможе писати статті, а читач зможе отримувати усі статті, але не буде мати можливості їх змінювати. Далі, після авторизації, у запит користувача буде додаватись унікальний токен, за яким користувач отримає доступ до сервісу бізнес-логіки.

JWT-токени можуть бути використані для авторизації в різних системах та службах, що забезпечує єдину точку входу для користувача.

З іншого боку, JWT-токени неможливо відкликати після їх видання, що може створити проблеми безпеки у випадку втрати токена. Збереження JWT-токенів на стороні клієнта через куки може бути вразливим, особливо при неналежному збереженні та відсутності відповідних заходів безпеки, що створює можливість для атак на перехоплення токенів.

Саме тому токен доступу (access-token) [3] не зберігається у куках на стороні клієнту, а видається користувачу на певну сесію та може бути протермінованим. У випадку, якщо токен доступу протермінований, але користувач продовжує працювати із додатком, завдяки токену оновлення (refresh-token) [4], який зберігається в куках, можна отримати новий токен доступу і продовжити активну сесію користувача.

Як недолік використання даного підходу можна виділити, що JWT-токени не надають механізму для автоматичного завершення сесій після виведення користувача, що може створити проблеми з безпекою та конфіденційністю протягом певного часу до його протермінування.

Отже, використання JWT-токенів та куків для авторизації має свої переваги та недоліки, і ефективність залежить від належного використання та застосування відповідних заходів безпеки. При використанні цих методів важливо дотримуватися найкращих практик та стандартів безпеки для забезпечення надійності авторизації та захисту користувачів у веб-додатку.

Висновки

JWT-токени та збереження певних даних через куки є ефективним і зручним механізмом авторизації користувачів у веб-застосунках, який дозволяє ефективно здійснювати аутентифікацію з меншими витратами ресурсів та забезпечує гнучку систему авторизації.

При використанні JWT-токенів важливим є забезпечення належного керування безпекою та конфіденційністю, оскільки переваги цього методу супроводжуються ризиками, такими як неможливість відкликання токенів та можливість їх втрати або зламу. Збереження секретних ключів та забезпечення належної безпеки стають важливими аспектами розглянутої системи авторизації.

Список використаних джерел

1. JSON Web Tokens [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/secure/tokens/json-web-tokens
2. Cookie Authentication [Електронний ресурс] – Режим доступу до ресурсу: https://swagger.io/docs/specification/authentication/cookie-authentication/
3. What is difference between Access-token and Refresh-token [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@greekykhs/springsecurity-what-is-the-difference-between-access-and-refresh-token-65296bcb13fc
4. What Are Refresh Tokens and How to Use Them Securely [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/blog/refresh-tokens-what-are-they-and-when-to-use-them/

УДК 004.92

РОМАНЮК О. Н., СТАНІСЛАВЕНКО Є. Г., МЕЛЬНИК А. В., РОМАНЮК С. О.
Вінницький національний технічний університет

ВИКОРИСТАННЯ ПРОГРАМНОГО ПАКЕТА SUBSTANCE PAINTER ДЛЯ РОЗРОБКИ 3Д МОДЕЛЕЙ

Анотація: Розглянуто використання програмного пакета Substance painter для розробці 3Д моделей
Ключові слова:ренденинг, Substance Painter, текстура

Substance Painter [1-3] - це програмний пакет для текстурування та розфарбовування 3D-моделей, що розробляється компанією Allegorithmic (зараз частина Adobe). Він широко