

УДК 004

Волов М.М.¹, Зайко Т.А.²

¹ студ. гр. КНТ-112сп НУ «Запорізька політехніка»

² канд. техн. наук, доц. НУ «Запорізька політехніка»

МЕТОДИ АВТОРИЗАЦІЇ В СУЧАСНИХ ВЕБ-ЗАСТОСУНКАХ ЗА ПРИНЦИПОМ ZERO TRUST

Сьогодні концепція Zero Trust стає все більш популярною у сфері кібербезпеки, зокрема в веб-застосунках. Основна ідея Zero Trust полягає в тому, щоб жодна частина системи не була автоматично довіреною. Це вимагає суворої перевірки всіх користувачів і пристроїв, незалежно від їхнього розташування, перш ніж надавати доступ до ресурсів. У цій роботі розглянемо сучасні методи авторизації, що відповідають принципу Zero Trust, такі як OAuth 2.0, JWT та багатофакторна авторизація (MFA).

Мета Zero Trust полягає в побудові архітектури, де доступ до даних або додатків дозволяється лише після перевірки особистості користувача та

авторизації на основі мінімально необхідних прав. Це зменшує ризик компрометації системи в разі витоку облікових даних або доступу з ненадійного пристрою.

Існує три основних методи авторизації в рамках концепції Zero Trust.

OAuth 2.0 та OpenID Connect. Протокол OAuth 2.0 є одним із сучасних стандартів авторизації для веб-додатків і API. Він дозволяє делегувати доступ до ресурсів користувача іншим сервісам без необхідності передачі облікових даних [2]. Основним принципом роботи є використання access tokenів, що видаються клієнтам після успішної автентифікації. Ці токени мають обмежений термін дії та надають доступ лише до визначених ресурсів. OpenID Connect (OIDC) є надбудовою над OAuth 2.0, що додає рівень автентифікації та дозволяє використовувати профілі користувачів для авторизації в різних сервісах. У рамках Zero Trust авторизація за допомогою OAuth 2.0 і OIDC дозволяє динамічно перевіряти запити та контролювати доступ до ресурсів на основі кожного окремого запиту, що відповідає принципам постійної перевірки і відсутності довіри до попередніх сесій [1].

Багатофакторна автентифікація (MFA). MFA є ключовим елементом Zero Trust, оскільки забезпечує додатковий рівень захисту через підтвердження особи користувача за допомогою кількох факторів: знання (пароль), володіння (телефон, апаратний токен) або біометричні дані. Це дозволяє мінімізувати ризики компрометації навіть у разі, якщо один із факторів автентифікації скомпрометовано. В Zero Trust MFA зазвичай застосовується на кожному рівні доступу до ресурсів, не обмежуючись лише початковою автентифікацією, забезпечуючи постійний контроль [1].

JSON Web Tokens (JWT). JWT є компактним і безпечним способом передачі інформації про користувача між сторонами. У моделі Zero Trust ці токени використовуються для передачі інформації про автентифікацію та авторизацію без необхідності зберігання сесій на стороні сервера [3]. JWT-токени зазвичай мають короткий термін дії і повинні постійно оновлюватись для мінімізації ризику компрометації. Завдяки тому, що кожен запит може бути перевірений за допомогою короткоживучого токена, цей метод ідеально підходить для реалізації принципів Zero Trust, де довіра не зберігається між запитами [3].

Однією з основних переваг Zero Trust є можливість його застосування в масштабованих хмарних середовищах. Наприклад, веб-додатки, розгорнуті на платформах AWS або Google Cloud, активно використовують принципи Zero Trust для захисту даних та забезпечення мінімального доступу до ресурсів.

Для захисту сучасних веб-додатків у відповідності до концепції Zero Trust важливо реалізувати стратегію мінімізації прав доступу (Least Privilege),

що передбачає надання прав лише для необхідних дій користувача. Це зменшує ймовірність компрометації системи в разі атаки.

У висновку можна сказати, що методи авторизації, що базуються на концепції Zero Trust, дозволяють підвищити рівень безпеки веб-застосунків, мінімізуючи ризики несанкціонованого доступу до даних. Використання OAuth 2.0, JWT та багатофакторної авторизації у поєднанні з іншими методами забезпечує надійний захист у хмарних середовищах та в традиційних веб-застосунках.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kohnfelder, L., and Garg, P. The Security Architecture of Zero Trust Networks / L. Kohnfelder, P. Garg. – Google Scholar, 2021.
2. Ward, P. OAuth 2.0: Security for Modern Web Applications / P. Ward. – Cybersecurity Journal, 2020.
3. Adams, J. JWT and Modern Token-Based Authentication / J. Adams, S. Wenzel. – IEEE, 2019.