

## **SINGLE SIGN-ON ДЛЯ ІНТЕРНЕТ МАГАЗИНУ ЗА ДОПОМОГОЮ ПРОТОКОЛУ OPENID CONNECT**

У сучасному світі, де кількість онлайн-сервісів росте з кожним днем, питання ефективної та безпечної аутентифікації стає все більш актуальним. Користувачам часто доводиться використовувати десятки різних сервісів, для кожного з яких потрібно запам'ятовувати унікальний набір облікових даних. Це не тільки створює додатковий тягар для користувачів, але й значно збільшує ризики безпеки. Рішенням цієї проблеми є впровадження системи Single Sign-On (SSO), що дозволяє використовувати єдиний набір облікових даних для доступу до різноманітних сервісів.

Метою цього дослідження є аналіз можливостей протоколу Open IDConnect (OIDC) для реалізації ефективної та безпечної системи SingleSign-On. Ми розглядаємо основні компоненти та механізми OIDC, їх вплив на безпеку аутентифікації та зручність використання сервісів. Особлива увага приділяється аналізу реалізації та тестуванню системи SSO на базі OIDC у вигляді кейс-стаді.

В рамках основної частини нашого дослідження, ми зосередили увагу на розробці та аналізі системи SingleSign-On (SSO) для інтернет-магазину, використовуючи протокол OpenIDConnect (OIDC). Цей протокол включає в себе функціонал ідентифікації користувачів, що дозволяє надійно ідентифікувати особу користувача та управляти доступом до різноманітних сервісів.

Особливість OIDC полягає в використанні ID Token, який діє як доказ того, що користувач був успішно аутентифікований у постачальника ідентифікаційних даних (IdP). Цей токен містить інформацію про користувача та його сесію, яка може бути перевірена системою інтернет-магазину для підтвердження аутентичності користувача і безпеки сесії. Завдяки цьому підходу магазин може уникнути необхідності зберігання паролів користувачів, знижуючи таким чином ризики безпеки та підвищуючи зручність використання своїх сервісів.

Процес створення демонстраційної версії SSO для інтернет-магазину на базі OIDC передбачав визначення вимог до системи, в тому числі з питань безпеки, масштабованості та користувацької зручності. Було обрано технологічний стек на базі .NET, що найкраще відповідає цим критеріям, з особливим акцентом на механізми шифрування даних і перевірку цифрових підписів токенів.

Ми інтегрували протокол OIDC до наявного процесу аутентифікації користувачів у середовищі інтернет-магазину. Система демонструє здатність безперервно ідентифікувати користувачів при переході між різними секціями магазину, уникаючи необхідності повторної аутентифікації. Ефективність і безпека розробленої системи були підтверджені за допомогою серії тестів, які продемонстрували високу швидкодію та надійність управління сесіями. Аналіз отриманих даних виявив, що використання OpenIDConnect для створення системи SSO в інтернет-магазині дозволяє не тільки спростити процес аутентифікації для кінцевих користувачів, але й значно підвищити рівень безпеки.

Також було розроблено інтерфейс для зручного входу та управління профілем користувача, що сприяє покращенню загального досвіду покупок.

Також, було доцільно додати підтримку декількох IdP, адже протокол один. Ми додали відповідну сторінку конфігурації. В результаті користувач має змогу обрати найбільш зручний для нього варіант. Ми в свою чергу отримали достатній рівень гнучкості, для заміни IdP в разі потреби.

Впровадження системи SingleSign-On на базі OpenIDConnect дозволяє значно спростити процес аутентифікації для користувачів, забезпечуючи їм доступ до різних сервісів за допомогою єдиного набору облікових даних. Крім того, використання OIDC сприяє підвищенню загального рівня безпеки системи, оскільки інформація про аутентифікацію передається у зашифрованому вигляді, а доступ до сервісів контролюється на основі токенів, які можуть бути швидко анульовані у випадку необхідності. Таким чином, OIDC є ефективним інструментом для реалізації SSO, що підтверджено результатами нашого дослідження.

### **Список використаних джерел**

1. Final: OpenIDConnectCore 1.0 incorporatingerrataset 2. Open ID – OpenIDFoundation. URL: [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)
2. Hardt D. (2012). The OAuth 2.0 Authorization Framework. RFC 6749.
3. Microsoft. ASP.NET Core. Authentication. OpenIdConnect Microsoft Learn: Builds kills that open doors in your career. URL: <https://learn.microsoft.com/ru-ru/dotnet/api/microsoft.aspnetcore.authentication.openidconnect?view=aspnetcore-8.0>
4. Add user authentication and Okta Resource Management to your ASP.NET Core app | Okta Developer. Home | Okta Developer. URL: <https://developer.okta.com/code/dotnet/aspnetcore/>.