

ДОЦІЛЬНІСТЬ ТА ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ПРОТОКОЛУ OPENID CONNECT ПРИ РОЗРОБЦІ ВІДКРИТИХ ОСВІТНІХ ПЛАТФОРМ

Тієвський І.О.

Інтеграція різноманітних систем управління навчанням (LMS) стає необхідною умовою для забезпечення академічної мобільності, обміну освітніми ресурсами та створення єдиних освітніх екосистем. Ключовим аспектом такої інтеграції є управління ідентифікацією користувачів, їх автентифікація та авторизація для доступу до ресурсів різних платформ.

OAuth 2.0 як протокол делегування доступу широко застосовується в освітніх платформах, проте демонструє ряд суттєвих обмежень при використанні в багатокомпонентних освітніх системах:

- **Відсутність стандартизованого механізму автентифікації.** OAuth 2.0 – це протокол авторизації, не автентифікації, що змушує розробників створювати власні рішення для перевірки особистості користувача.
- **Обмежена інформація про користувача.** Базовий OAuth 2.0 не специфікує стандартного способу отримання профілю користувача, що ускладнює синхронізацію даних між LMS.
- **Фрагментація реалізацій.** Різні LMS (Moodle, Canvas, Blackboard, Google Classroom) реалізують OAuth 2.0 по-своєму, створюючи складнощі при побудові уніфікованого підходу до інтеграції.
- **Проблеми безпеки.** При неправильній реалізації OAuth 2.0 виникають ризики CSRF-атак, витоку або підміни токенів, що особливо критично для систем з персональними даними студентів.

Протокол OpenID Connect (OIDC), побудований як розширення OAuth 2.0, вирішує ці проблеми, надаючи стандартизований механізм автентифікації та обміну інформацією про користувача, що робить його оптимальним рішенням для освітніх екосистем. Його важливість і актуальність зумовлені сучасними вимогами до безпеки, користувацького досвіду, інтеоперабельності та регуляторних стандартів. OIDC додає шар автентифікації, що дозволяє безпечно ідентифікувати користувачів і передавати їхні дані між системами [1].

Протокол визначає ролі Identity Provider (IdP) та Relying Party (RP), де IdP відповідає за автентифікацію, а RP – за надання доступу до ресурсів після успішного входу [1]. Серед ключових переваг використання OIDC можна виділити наступні:

- **Безпека.** OIDC використовує JSON Web Tokens (JWT), які підписуються та шифруються, що захищає від несанкціонованого доступу та підробки. Це критично в умовах зростання кіберзагроз, таких як фішинг чи перехоплення даних.
- **Єдиний вхід (SSO).** OIDC дозволяє користувачам автентифікуватися один раз і отримувати доступ до кількох систем без повторного введення логіна та пароля, що покращує зручність і зменшує ризик компрометації облікових даних.
- **Стандартизація.** Як відкритий стандарт, OIDC підтримується більшістю сучасних платформ (Google, Microsoft, AWS), що забезпечує сумісність і спрощує інтеграцію.
- **Гнучкість.** OIDC дозволяє передавати кастомні атрибути (наприклад, ролі, ідентифікатори курсів), що робить його універсальним для різних сценаріїв.

Згідно з EdTech Trends 2025, опублікованим Digital Learning Institute [2], підвищення рівня безпеки у сфері електронного навчання є одним із найбільш пріоритетних напрямів роботи у 2025 році. При цьому відкриті LMS часто розгортаються

в різних закладах із власними конфігураціями, що ускладнює уніфікацію безпеки. OIDC забезпечує стандартний протокол, який працює незалежно від локальних налаштувань. Крім цього, студенти, які переходять між закладами, потребують збереження доступу до навчальних ресурсів. OIDC дозволяє передавати ідентифікатори та атрибути (наприклад, кредити ECTS) між LMS. Наприклад, у рамках Erasmus+ європейські університети можуть використовувати OIDC для обміну даними про студентів.

Одна з особливостей LMS – різноманітність користувачів. Відкриті платформи обслуговують студентів, викладачів, адміністраторів і зовнішніх партнерів, кожен із яких має різні права доступу. OIDC дозволяє гнучко управляти ролями через атрибути в ID Token. Наприклад, студент може мати доступ лише до своїх курсів, тоді як викладач — до аналітики.

Відкриті LMS часто інтегруються з хмарними сервісами (Google Classroom, Microsoft Teams) або інструментами (Zoom, Turnitin). OIDC забезпечує безпечну автентифікацію для цих інтеграцій. Наприклад, LTI Advantage у Moodle використовує OIDC для підключення зовнішніх інструментів. При цьому спільнота розробників вищезгаданої LMS Moodle активно підтримує OIDC через плагіни, такі як `auth_oidc`, що сприяє його поширенню, а також спонукає великі корпорації до розробки власних рішень (схожий плагін розроблений та підтримується компанією Microsoft).

В якості практичного прикладу пропонується розглянути ймовірний сценарій побудови інтеграційної платформи, що об'єднує різні ЗВО в рамках проєкту забезпечення академічної мобільності в онлайн-навчанні. Вхідні умови:

- кожен заклад використовує власну LMS на базі Moodle;
- створюється центральна інтеграційна платформа на базі Moodle для координації мобільності;
- необхідно забезпечити безшовний досвід студентів при навчанні в різних закладах.

За умови структури, що складається із чотирьох основних компонентів: OIDC провайдера (IdP), інтеграційної платформи, інстансів Moodle окремих ЗВО та сервісу синхронізації даних – шлях автентифікації студента, що користується можливостями академічної мобільності може виглядати наступним чином:

1. Студент відкриває інтеграційну платформу та обирає курс іншого (не “свого”) ЗВО.
2. Інтеграційна платформа ініціює OIDC Auth Flow, перенаправляючи студента на IdP.
3. IdP визначає домашній заклад студента (на основі домену email або вибору користувача) і перенаправляє на відповідний локальний IdP.
4. Студент проходить автентифікацію у своєму домашньому закладі.
5. Після успішної автентифікації локальний IdP генерує assertion для IdP.
6. IdP створює OIDC ID-токен перенаправляє студента назад на інтеграційну платформу.
7. Інтеграційна платформа верифікує токен, створює або оновлює профіль студента.
8. Платформа використовує access-токен для отримання додаткової інформації через API домашнього закладу.
9. Система створює тимчасовий обліковий запис у LMS цільового закладу, використовуючи його API.
10. Інтеграційна платформа перенаправляє студента до відповідного курсу на LMS цільового закладу з автоматичним входом.

Цей процес забезпечує безшовний досвід для студента, який фактично працює у “віртуальному кампусі” консорціуму, не відчуючи переходів між різними системами.

При цьому слід мати на увазі ймовірні додаткові складнощі реалізації при використанні ЗВО різних LMS або різних їх версій. Втім сам механізм використання OIDC може значно спростити процес інтеграції та підвищити рівень безпеки при взаємодії освітніх платформ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OpenID Connect Core 1.0 incorporating errata set 2 [Електронний ресурс]: OpenID Foundation. – Режим доступу: https://openid.net/specs/openid-connect-core-1_0.html (Дата звернення: 16.04.2025).
2. Education Technology Trends to Watch in 2025 [Електронний ресурс]: Digital Learning Institute. – Режим доступу: <https://www.digitallearninginstitute.com/blog/education-technology-trends-to-watch-in-2025> (Дата звернення: 18.04.2025).

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів