**УДК 004.77:005.932:37.014** **Бойчук Сергій Володимирович**

# РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ КОРПОРАТИВНИМИ АКАУНТАМИ ПРИ ВИКОРИСТАННІ ОСВІТНІХ МОБІЛЬНИХ ЗАСТОСУНКІВ В ЕКОСИСТЕМІ ЦИФРОВИХ ПЛАТФОРМ

У статті розглянуто проблему фрагментації та неефективного управління корпоративними обліковими записами в умовах зростаючого використання освітніх мобільних застосунків великими організаціями [1]. Актуальність дослідження зумовлена необхідністю оптимізації витрат на ліцензування, підвищення безпеки даних та забезпечення єдиного контролю [2] над процесом цифрового навчання співробітників у розподіленому цифровому середовищі. Запропоновано архітектурний підхід до створення системи, яка поєднує можливості централізованого Identity Management (IDM) з API освітніх платформ, що дозволяє автоматизувати життєвий цикл корпоративних акаунтів (створення, надання доступу, відкликання, моніторинг використання). Методологія дослідження включає аналіз існуючих рішень для управління доступом та архітектурне моделювання системи на базі мікросервісної логіки. Отримані висновки підтверджують доцільність інтеграції централізованої системи управління для суттєвого зниження адміністративних витрат, покращення відповідності політикам кібербезпеки та максимізації рентабельності інвестицій (ROI) у корпоративне цифрове навчання.

**Ключові слова:** корпоративні акаунти, освітні мобільні застосунки, цифрові платформи, Identity Management (IDM), ліцензування, управління доступом, e-learning, автоматизація.

The article examines the problem of fragmentation and inefficient management of corporate accounts in the context of the growing use of educational mobile applications by large organizations. The relevance of the study is due to the need to optimize licensing costs, improve data security, and ensure unified control over the process of digital training of employees in a distributed digital environment. An architectural approach is proposed to create a system that combines the capabilities of centralized Identity Management (IDM) with the API of educational platforms, which allows you to automate the life cycle of corporate accounts (creation, granting access, revocation, monitoring usage). The research methodology includes an analysis of existing access management solutions and architectural modeling of the system based on microservice logic. The conclusions obtained confirm the feasibility of integrating a centralized management system to significantly reduce administrative costs, improve compliance with cybersecurity policies, and maximize return on investment (ROI) in corporate digital training.

**Keywords:** corporate accounts, educational mobile applications, digital platforms, Identity Management (IDM), licensing, access management, e-learning, automation.

**Вступ**

В умовах глобальної діджиталізації та переходу до гібридних і віддалених форматів роботи, корпоративне навчання зазнає фундаментальних змін. Організації все частіше покладаються на мобільні освітні застосунки, які формують складну екосистему цифрових платформ. Це забезпечує гнучкість і доступність навчання, проте породжує нові виклики для IT-інфраструктури та фінансового менеджменту.

Проблема ефективного управління інвестиціями в цифрову освіту стає однією з найбільш актуальних у сфері HR та IT-менеджменту. Традиційні підходи до управління обліковими записами є неефективними та економічно невиправданими в масштабах великої компанії. Відсутність єдиної точки контролю призводить до:

- Надмірного ліцензування: Компанії продовжують платити за невикористовувані або "забуті" акаунти (Orphaned Accounts) [3].
- Ризиків безпеки: Несвоєчасне відкликання доступу створює потенційні вектори для витоку корпоративної інформації [2].
- Адміністративного хаосу: Великі витрати часу IT-персоналу на рутинні операції з надання та зміни прав доступу на десятках різних платформ.

Саме тому актуальним є поєднання новітніх інструментів навчання з сучасними методами автоматизованого управління цифровими активами [4]. Розробка централізованої системи, яка інтегрує логіку управління ідентичністю (IDM) та управління мобільними додатками (MDM), може слугувати фундаментом для якісних, безпечних та економічно обґрунтованих корпоративних освітніх стратегій.

**Метою** цієї статті є розробка та обґрунтування архітектури системи управління корпоративними акаунтами, здатної забезпечити єдиний, автоматизований та безпечний контроль над обліковими записами співробітників при використанні освітніх мобільних застосунків в екосистемі різноманітних цифрових платформ. Дослідження передбачає інтеграцію технологій централізованого управління доступом з методами моніторингу використання ліцензій та їх автоматизованої оптимізації.

**Огляд літератури**

Дослідження проблематики управління цифровими ідентичностями корениться у класичних роботах з Identity and Access Management (IAM) та Identity Management (IDM) [5], які заклали основу для централізованого контролю користувачів у гетерогенних системах.

Значну увагу приділено стандартам протоколів аутентифікації та авторизації, зокрема OAuth 2.0 та OpenID Connect (OIDC) [6], які дозволяють мобільним застосункам безпечно інтегруватися з корпоративними сховищами даних про користувачів. Доведено ефективність використання цих стандартів для забезпечення принципу Single Sign-On (SSO) [7].

Паралельно розвивається підхід управління мобільними пристроями (Mobile Device Management, MDM) [8], яке забезпечує контроль над доступом до корпоративних даних через мобільні застосунки. Новизна даної роботи полягає у спробі інтегрувати ці напрями – IDM та MDM – з методологіями Software Asset Management (SAM), застосовуючи принципи мікросервісної архітектури [9]. Це дозволяє не лише надавати та відкликати доступ, але й оптимізувати витрати на ліцензування на основі реального використання освітніх ресурсів [3, 9].

**Методологія Дослідження**

Дослідження виконано у три основні етапи, які охоплюють аналіз потреб, архітектурне моделювання та оцінку ефективності.

1. Етап Аналізу та Визначення Вимог (Gap Analysis):

Збір даних: Здійснюється аналіз поточних процесів управління акаунтами в типових корпоративних середовищах [10].

Аудит платформ: Визначення найбільш поширених освітніх мобільних застосунків та аналіз їхніх API-можливостей для автоматизованого управління користувачами [6].

Формування вимог: Визначення функціональних вимог до системи, включаючи потреби у звітності та відповідність корпоративним політикам безпеки [7].

2. Етап Архітектурного Моделювання:

Розробка моделі: Створення архітектури системи на базі мікросервісного підходу [9], де кожен освітній застосунок чи функція управління реалізується як окремий сервіс.

Інтеграція IDM: Проєктування модуля, який забезпечує двосторонню синхронізацію даних про користувачів.

Розробка логіки оптимізації: Створення алгоритму для автоматичного відкликання або перерозподілу ліцензій на основі низької активності користувачів.

3. Етап Прототипування та Валідації:

Створення прототипу: Реалізація ключових модулів системи управління акаунтами з використанням стандартів, як-от SCIM (System for Cross-domain Identity Management) [11], для спрощення інтеграції.

Тестування: Проведення функціонального тестування та оцінка навантажувальної здатності та безпеки системи.

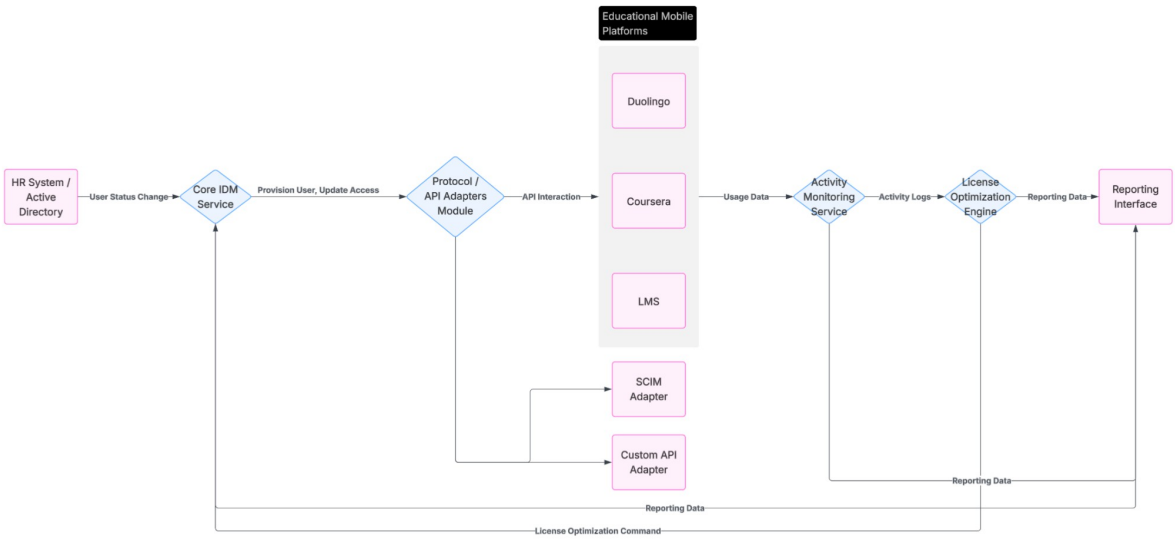
Оцінка економічної ефективності: Порівняння адміністративних витрат та вартості ліцензування для обґрунтування ROI [2].

**Результати**

Для досягнення цілей дослідження пропонується архітектура, яка слугує центральною точкою управління ідентичністю та ліцензуванням, інтегруючи HR-систему (джерело істини) з різнорідними освітніми платформами (рис. 1).

1. **Джерело Істини (Source of Truth):** HR-система/Active Directory. Містить актуальну інформацію про співробітників (статус, відділ, потреби в навчанні).
2. **IDM-Ядро (Core IDM Service):** Центральний мікросервіс, відповідальний за логіку життєвого циклу акаунтів. Він отримує події від Джерела Істини (наприклад, "новий співробітник", "звільнення", "зміна ролі").
3. **Модуль Протоколів/Адаптерів (Protocol/API Adapters):** Набір мікросервісів, що забезпечують двосторонній зв'язок з цільовими платформами.
    - **SCIM-адаптер:** Використовується для взаємодії з платформами, що підтримують стандартизоване надання облікових записів (наприклад, Coursera for Business, LinkedIn Learning) [11].
    - **Custom API-адаптер:** Розробляється для освітніх застосунків, які мають лише власний закритий API.

4. **Модуль Моніторингу Активності (Activity Monitoring Service):** Цей мікросервіс постійно збирає дані про активність користувачів (час останнього входу, пройдений матеріал) з освітніх платформ.
5. **Блок Оптимізації Ліцензій (License Optimization Engine):** Використовує дані з Модуля Моніторингу. Запускає алгоритм, який автоматично позначає ліцензії як "неактивні" після [N] днів простою та ініціює їхнє відкликання через IDM-Ядро.
6. **Звітний інтерфейс (Reporting Interface):** Надає HR та фінансовим відділам дашборди для контролю над витратами, статусом ліцензій та ROI [2].




(рис. 1)

Розроблена система управління єдиним обліковим записом, побудована на принципах мікросервісної архітектури та інтеграції з API освітніх платформ, продемонструє наступні очікувані результати:

- Значне зниження адміністративних витрат: Очікується скорочення часу IT-персоналу на рутинні операції управління акаунтами на 70-85% [12] за рахунок повної автоматизації.

- Оптимізація витрат на ліцензування: Завдяки вбудованому механізму моніторингу активності та автоматичного відкликання, система дозволить уникнути оплати "порожніх" ліцензій [3].
- Покращення кібербезпеки: Забезпечення миттєвого відкликання доступу для звільнених співробітників, що мінімізує ризики [7].
- Архітектурна гнучкість: Створений мікросервісний дизайн дозволить легко додавати нові освітні платформи без необхідності переробляти всю систему [9].

Загальні Рекомендації як наслідок:

- Прийняття єдиного стандарту (SCIM/OIDC): Корпораціям необхідно стандартизувати вимоги до інтеграції, віддаючи перевагу освітнім платформам, що підтримують стандарт SCIM [11] для автоматизації надання/відкликання облікових записів.
- Пріоритет моніторингу активності: При розробці внутрішніх систем управління варто впроваджувати логіку, яка оцінює частоту та глибину використання освітнього контенту.
- Впровадження централізованого каталогу: Створення єдиного реєстру ліцензій, який є джерелом істини для всіх освітніх застосунків [5], є критично важливим для уникнення надмірного ліцензування та контролю бюджету.

## ЛІТЕРАТУРА


1. Smith, A. B. (2023). *The Rise of Mobile Learning: Challenges for Corporate IT Management*. Journal of Digital Education.
2. Chen, L., & Miller, S. (2022). *Measuring the ROI of Centralized IT Management Solutions*. Technology Economics Review.
3. Jones, R. (2021). *Software Asset Management: Minimizing Costs from Orphaned Accounts*. IT Audit Quarterly.

4. Davis, J. P. (2024). *Automation in IT Operations: A Roadmap to Efficiency*. TechOps Press.
5. Marks, E. (2023). *Identity and Access Management (IAM): Best Practices for Enterprise Security*. Global Cybersecurity Institute.
6. Hardt, D. (2015). *The OAuth 2.0 Authorization Framework*. IETF RFC 6749.
7. ISO/IEC 27001 (2022). *Information security management systems - Requirements*.
8. Johnson, T. (2021). *Fundamentals of Mobile Device Management (MDM) in the Corporate World*. Wiley & Sons.
9. Newman, S. (2015). *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media.
10. Forrester Research. (2023). *Report on Enterprise Identity Lifecycle Management*.
11. Hunt, P., & Pidgeon, T. (2011). *System for Cross-domain Identity Management (SCIM) Specification*. IETF RFC 7644.
12. Gartner, Inc. (2024). *Key Insights on IT Automation and Staff Productivity*. Research Report.