УДК 004.738.5

Грищенко Д.С., здобувач,
Колощук М.С., ст. викладач,
Окунькова О.О., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ IAM-ПЛАТФОРМ ДЛЯ УПРАВЛІННЯ ДОСТУПОМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Зростання кількості корпоративних інформаційних систем, хмарних середовищ та розподілених користувачів ускладнює контроль доступу до ресурсів організацій, що підтверджується сучасними дослідженнями [1]. Традиційні підходи на основі локальних облікових записів і ручного адміністрування прав є недостатньо гнучкими та схильними до помилок, що зумовлює необхідність використання систем класу Identity and Access Management (IAM).

Метою дослідження є порівняльний аналіз функціональних можливостей та ефективності провідних IAM-платформ для управління доступом у корпоративних інформаційних системах з урахуванням сучасних вимог інформаційної безпеки.

Для досягнення поставленої мети застосовано метод порівняльного аналізу, узагальнення та систематизації функціональних характеристик трьох IAM-платформ – Microsoft Entra ID, Okta та Keycloak – за такими критеріями: підтримка протоколів автентифікації (OAuth 2.0, SAML 2.0, OpenID Connect), реалізація рольової моделі доступу (Role-Based Access Control, RBAC), наявність багатофакторної автентифікації (Multi-Factor Authentication, MFA), функції аудиту та моніторингу подій, а також можливості інтеграції з хмарними і гібридними середовищами.

Таблиця 1 – Порівняльна характеристика IAM-платформ

Платформа	MFA	RBAC	Протоколи	Інтеграція
Microsoft Entra ID	+	+	OAuth 2.0, SAML, OIDC	Висока
Okta	+	+	OAuth 2.0, SAML, OIDC	Висока
Keycloak	+	+	OAuth 2.0, SAML, OIDC	Гнучка

IAM-платформи є комплексними рішеннями, що забезпечують управління цифровими ідентичностями користувачів та контроль їх доступу до інформаційних ресурсів, включаючи автентифікацію, авторизацію, управління ролями, аудит та моніторинг. Централізація управління правами дозволяє адміністратору обслуговувати великі організації з тисячами користувачів з єдиного інтерфейсу, що мінімізує ймовірність помилок та знижує операційне навантаження. Застосування моделі RBAC забезпечує логічний розподіл прав відповідно до функціональної ролі: від базового доступу рядового співробітника до повноважень системного адміністратора [2].

У результаті порівняльного аналізу встановлено, що всі три платформи реалізують ключові функції IAM, однак відрізняються за

моделлю розгортання та гнучкістю налаштування. Microsoft Entra ID є оптимальним рішенням для організацій, що використовують екосистему Microsoft 365, завдяки нативній інтеграції з корпоративними сервісами. Okta вирізняється широкими можливостями підключення до хмарних застосунків через готові конектори та підтримкою складних сценаріїв федерації ідентичностей. Keycloak як рішення з відкритим кодом забезпечує максимальну гнучкість конфігурації за умови наявності достатніх ресурсів для самостійного розгортання та підтримки. Використання механізму MFA у поєднанні з RBAC суттєво знижує ризики несанкціонованого доступу: за даними галузевих досліджень, впровадження MFA дозволяє заблокувати понад 99,9 % автоматизованих атак на облікові записи [1].

Окрему увагу у дослідженні приділено механізмам аудиту та автоматизації. IAM-системи ведуть журнали подій, у яких фіксуються всі дії користувачів: автентифікаційні спроби, операції зміни прав, доступ до ресурсів. Це забезпечує оперативне виявлення підозрілої активності та відповідає вимогам регуляторних стандартів (ISO/IEC 27001, GDPR). Автоматизація циклу управління обліковими записами (provisioning/deprovisioning) скорочує час реакції на кадрові зміни та унеможливлює збереження надлишкових прав доступу після звільнення працівника.

Наукова новизна роботи полягає у формалізації критеріїв оцінювання IAM-платформ як компонентів корпоративної системи безпеки та встановленні залежності ефективності їх застосування від архітектурної моделі IT-інфраструктури.

За результатами дослідження встановлено, що ефективність IAM-платформи визначається не лише переліком підтримуваних функцій, а й відповідністю архітектурній моделі організації та рівнем зрілості її IT-інфраструктури. Застосування рольової моделі доступу та багатофакторної автентифікації у поєднанні з інструментами аудиту забезпечує комплексний контроль над інформаційними ресурсами. Вибір між комерційними хмарними рішеннями (Entra ID, Okta) та відкритими самостійно розгорнутими платформами (Keycloak) має здійснюватися з урахуванням масштабу організації, наявних технічних компетенцій та бюджетних обмежень. Впровадження IAM-рішень є доцільним для організацій будь-якого масштабу як ефективний інструмент підвищення рівня кібербезпеки та оптимізації процесів управління доступом.

Список використаних джерел

1. What is Identity and Access Management (IAM)? IBM. URL: https://www.ibm.com/topics/identity-access-management.

2. NIST Special Publication 800-63-3: Digital Identity Guidelines. National Institute of Standards and Technology. URL: https://pages.nist.gov/800-63-3/.