1. Zhihu. *How can Android apps detect system touch event interception (clickjacking)?* [Електронний ресурс]. – Режим доступу: https://www.zhihu.com/question/37378266 – Дата звернення: 29.04.2025.

2. Bai Qin. *Binder File Descriptor Usages*. Medium [Електронний ресурс]. – Режим доступу: https://baiqin-droid1001.medium.com/binder-file-descriptor-usages-b2b8a672873f – Дата звернення: 29.04.2025.

Огляд існуючих рішень в області управління доступом до хмарних середовищ

УДК 004.738.056

Володимир Бескровний[1], Олександр Сиропятов[2]

Національний університет «Одеська політехніка»,
[1]9560418@stud.op.edu.ua, [2]o.a.syropiatov@op.edu.ua

У сучасних умовах розвитку цифрових технологій та зростання обсягів обробки корпоративних даних у хмарних середовищах питання побудови безпечної та гнучкої системи управління доступом набуло особливої актуальності. Хмарна інфраструктура дозволяє підприємствам оптимізувати свої процеси, однак одночасно створює нові ризики, пов'язані з несанкціонованим доступом до ресурсів, витоком даних та інсайдерськими загрозами. Зокрема, важливо розглянути традиційні та сучасні підходи, що дозволяють гнучко адаптувати доступ відповідно до змін у бізнес-процесах, а також вивчити можливості реалізації цих моделей на найпопулярніших хмарних платформах.

Метою роботи є проведення аналізу моделі управління доступом у хмарних середовищах, а також провести порівняння можливостей найбільш поширених платформ IAM (AWS IAM, Azure AD, Google Cloud IAM) для побудови безпечної системи контролю доступу в умовах корпоративної хмарної інфраструктури.

Ефективне управління доступом у хмарних середовищах є ключовим аспектом безпеки корпоративних даних. Існує кілька базових моделей, які широко застосовуються у сучасних системах управління доступом.

Рольова модель доступу (RBAC) передбачає прив'язку прав доступу до певних ролей, які призначаються користувачам відповідно до їх посадових обов'язків [1]. Наприклад, розробник має доступ до репозиторіїв коду, а фінансовий аналітик — до фінансових звітів.

Атрибутна модель доступу (ABAC) дозволяє приймати рішення про надання доступу на основі атрибутів користувача (посада, місце роботи, час доступу, тип пристрою) та характеристик ресурсу [2].

Політично-орієнтована модель доступу (PBAC) формує доступ на основі динамічних політик та правил, що можуть змінюватися у реальному часі залежно від поведінки користувача або рівня ризику.

На практиці часто використовується комбінація моделей, де базова рольова модель доповнюється атрибутними правилами та політиками поведінки для підвищення гнучкості й безпеки.

У хмарному середовищі управління доступом реалізується за допомогою спеціалізованих платформ Identity and Access Management (IAM). Найпопулярнішими серед них є:

AWS IAM (Identity and Access Management) - сервіс в хмарі Amazon Web Services, який дозволяє організаціям безпечно керувати доступом до ресурсів AWS [3]. За допомогою IAM адміністратори можуть контролювати, хто має доступ до конкретних ресурсів у вашій інфраструктурі та що саме ці користувачі можуть робити з цими ресурсами.

Azure Active Directory (Azure AD) – рішення Microsoft для управління ідентифікацією в хмарних та гібридних середовищах. Він є базовим компонентом для багатьох корпоративних рішень Microsoft і часто використовується корпоративними системами, що робить його популярним серед великих компаній.

Google Cloud IAM – інструмент керування ідентичностями та доступом в хмарі Google, що дозволяє організаціям керувати тим, хто має доступ до ресурсів у Google Cloud Platform (GCP), і які саме права доступу ці користувачі мають.

Таблиця 1

Порівняння платформ

Платформа	**Підхід до управління доступом**	**Особливості**
AWS IAM	RBAC + умови доступу	Широкі можливості кастомізації через політики JSON
Azure AD	RBAC + умовні політики	Глибока інтеграція з Microsoft екосистемою
Google Cloud IAM	RBAC + ABAC	Деталізовані умови доступу на основі атрибутів

Всі розглянуті платформи підтримують гібридні підходи до управління доступом, поєднуючи RBAC з атрибутними та політико-орієнтованими механізмами.

Аналіз основних моделей управління доступом показав, що найкращі результати забезпечує комбіноване використання RBAC, ABAC та PBAC. Це дозволяє гнучко адаптувати політики під змінні бізнес-процеси та загрози. Розгляд платформ демонструє, що сучасні хмарні рішення підтримують складні механізми доступу, орієнтовані на мінімізацію ризиків. Таким чином, вибір платформи має базуватися на відповідності вимогам підприємства, інтеграційним можливостям і рівню захисту даних.

1. Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models. IEEE Computer, 1996, Vol. 29(2), pp. 38-47

2. Hu V.C., Ferraiolo D.F., Kuhn D.R. Attribute-Based Access Control (ABAC) Definition and Considerations. National Institute of Standards and Technology, 2014. 78 p

3. Amazon Web Services. AWS Identity and Access Management (IAM) User Guide. Amazon, 2023.

Кібератаки як загроза критичній інфраструктурі

УДК 004.56.5(043.2)

Павло Билень

Західноукраїнський національний університет,
pavlobulen@gmail.com

За 2024–2025 роки енергетична інфраструктура виявилася у центрі уваги хакерських атак, що стали частиною ширшого спектра гібридних загроз. Зі зростанням залежності енергосистем від цифрових технологій, підвищується і рівень їхньої вразливості до кібервтручань. У цьому дослідженні представлено аналіз найрезонансніших інцидентів останніх двох років, виявлено типові сценарії атак, ймовірні джерела загроз, а також надано огляд заходів, що вживаються для підвищення стійкості енергетичної інфраструктури до подібних втручань.

Протягом 2024 року в Україні було зафіксовано понад 4300 кібератак на об'єкти критичної інфраструктури, що свідчить про 70-відсоткове зростання порівняно з попереднім роком [1]. Основною мішенню залишаються енергетичні компанії, державні інформаційні платформи, зокрема Міністерство енергетики, операційні центри енергосистем та системи обліку. У грудні 2024 року відбулася масштабна атака, яка вивела з ладу цифрові реєстри Міністерства юстиції, а також тимчасово зупинила роботу сервісу “Дія”. Характерною особливістю цих атак є використання складних багаторівневих методів, включно з соціальною інженерією, фішингом, шкідливим ПЗ типу wiper та атакою через ланцюг постачання [2].

На початку 2025 року увагу світової спільноти привернув масштабний збій в енергосистемах Іспанії та Португалії. 28 квітня близько 60% енергоспоживання цих країн було раптово втрачено через зупинку десятків електростанцій [3]. Попри те, що офіційні оператори електромереж REE (Іспанія) та REN (Португалія) не підтвердили факт кібератаки, експерти не виключають можливість цілеспрямованого зовнішнього втручання у частотну стабільність мереж. Ситуація ускладнювалася синхронністю збоїв, що є нетиповим для звичайних технічних аварій.

Паралельно з європейськими інцидентами, протягом 2024–2025 років фіксувалися атаки на енергетичні об'єкти в інших регіонах. Зокрема, у США відома атака на комунальне підприємство в Айові призвела до порушень в електропостачанні та витоку персональних даних. У Німеччині постачальник Tibber повідомив про злом систем збереження даних близько 50 тисяч споживачів. У Румунії та Камеруні кібератаки спричинили тимчасову втрату доступу до електронних сервісів та енергетичних даних споживачів.

Джерела атак залишаються різноманітними за походженням і мотивацією. Частина інцидентів ідентифікована як операції, проведені державними