УДК 004.75; 004.8
DOI: 10.31673/2409-7292.2025.017186

Абібулаєв А.Р., Піскозуб А.З.

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ УПРАВЛІННЯ ДОСТУПОМ У ХМАРНОМУ СЕРЕДОВИЩІ

Зі зростанням використання хмарних технологій питання управління доступом стає одним із ключових аспектів забезпечення кібербезпеки. З огляду на глобальну цифрову трансформацію, організації дедалі частіше мігрують свої сервіси та дані до хмарних середовищ, що спричиняє нові виклики щодо безпеки, масштабованості та відповідності нормативним вимогам. Традиційні підходи до управління доступом, які використовувалися у локальних середовищах, не завжди ефективні у розподілених хмарних екосистемах, що вимагає розробки нових методів автентифікації, авторизації та моніторингу доступу. Сучасні тенденції у сфері інформаційної безпеки спрямовані на розширене використання Zero Trust моделі – моделі «нульової довіри», адаптивної багатофакторної автентифікації (Multi-Factor Authentication, MFA), а також систем управління доступом (Cloud Identity & Access Management, Cloud IAM), що забезпечують централізоване управління обліковими записами та контроль рівня довіри до кожного запиту на доступ. Зростання популярності гібридних і мультихмарних середовищ також додає складності у розгортанні ефективних систем контролю доступу.

Відсутність єдиного стандарту управління доступом між різними хмарними провайдерами змушує організації використовувати комплексні підходи, такі як політики найменших привілеїв (Principal of Least Privilege, PoLP), мікросегментацію мережі та поведінкову аналітику користувачів (User Behavior Analytics, UBA). Це означає, що компанії повинні не лише впроваджувати технологічні рішення для управління доступом, а й забезпечувати аудит доступу, моніторинг активності користувачів та застосування політик відповідності.

У цьому дослідженні проаналізовано сучасні підходи до контролю доступу, зокрема Identity and Access Management (IAM), Privileged Access Management (PAM), модель Zero Trust та принцип PoLP (найменших привілеїв). Наголошено на важливості інтеграції штучного інтелекту (Artificial Intelligence, AI), машинного навчання (Machine Learning, ML) та обробки природньої мови (Natural Language Processing, NLP) у процеси моніторингу й виявлення аномалій, що дозволяє підвищувати адаптивність політик безпеки. Розглянуто також перспективи переходу до автоматизованого аналізу ризиків, коли поведінкова аналітика допомагає своєчасно ідентифікувати загрози та знижувати кількість хибних сповіщень. Підкреслено роль відповідності міжнародним стандартам та регуляторним вимогам для уніфікованого керування безпекою у мультихмарних середовищах. Як результат, комбінований та адаптивний підхід до управління доступом, який опирається на AI/ML/NLP та ретельно налаштовані політики доступу, стає ключовим чинником захисту корпоративних активів у сучасній кіберпросторовій екосистемі.

Результати дослідження будуть корисними ІТ-відділам і фахівцям з безпеки, які впроваджують чи вдосконалюють системи управління доступом у динамічних хмарних середовищах, щоб забезпечити високий рівень захисту та відповідність нормативним вимогам, а також надає розуміння сучасних тенденцій розвитку систем управління доступом.

Ключові слова: управління доступом, хмарні технології, безпека даних, IAM, PAM, Zero Trust.

Вступ

Інтенсивний розвиток хмарних обчислень сприяє масовому переносу даних та сервісів до хмарних середовищ, що вимагає якісних механізмів управління доступом. Використання хмарних рішень дозволяє організаціям масштабувати свої обчислювальні ресурси, забезпечувати безперервність бізнес-процесів та оптимізувати витрати. Проте, разом із цими перевагами, зростають і ризики, пов’язані з витоками даних, несанкціонованим доступом та порушенням відповідності нормативним вимогам.

Традиційні моделі безпеки, що використовувалися для локальної інфраструктури, не завжди адаптуються до нових умов, що породжує необхідність у розширених методах автентифікації, адаптивного управління доступом та динамічного контролю привілеїв. Слід згадати підхід «замкненого периметру» (Perimeter-Based Security), який був ефективним у традиційних дата-центрах, більше не працює в розподілених системах, де співробітники, партнери та клієнти можуть отримувати доступ до корпоративних ресурсів з будь-якої точки світу. Окрім того, розвиток гібридних і мульти-хмарних середовищ вимагає гнучких та масштабованих підходів до управління доступом. Використання технологій автоматизації, штучного інтелекту (AI), машинного навчання (ML) та обробки природньої мови (NLP) дозволяє створювати ефективніші системи контролю доступу, які забезпечують швидке

реагування на загрози, можуть аналізувати поведінкові шаблони користувачів та виявляти аномальні дії, що можуть свідчити про злам облікового запису або інші загрози безпеці.

Можемо зробити однозначний висновок, що сучасне управління доступом у хмарних середовищах вимагає комплексного підходу, що включає використання адаптивних методів автентифікації, поведінкового аналізу, штучного інтелекту та автоматизації процесів. Подальше дослідження цих технологій допоможе підвищити рівень безпеки та ефективності управління доступом у хмарній інфраструктурі.

Аналіз літературних джерел та формулювання проблеми

За останнє десятиліття дослідження у сфері хмарної безпеки значно активізувалися. Було проведено численні дослідження з питань безпеки даних, ідентифікації та авторизації, динамічного управління доступом та впливу людського фактора на інформаційну безпеку, зокрема у джерелі [1]. На думку авторів, важливим аспектом також є зростання використання штучного інтелекту, машинного навчання та обробки природньої мови для автоматизації процесів контролю доступу, аналізу поведінки користувачів та запобігання кіберзагрозам.

У багатьох публікаціях розглянуто важливість інтеграції концепцій Zero Trust та «найменших привілеїв» (PoLP) у хмарних середовищах. Зокрема, автор Chava, A. (2024) [2] наголошує, що Zero Trust сприяє зменшенню ризиків, пов'язаних із несанкціонованим доступом, завдяки обов'язковій перевірці всіх запитів до мережевих ресурсів, а PoLP мінімізує обсяг прав кожного користувача. Такий підхід дає змогу унеможливити надмірні привілеї, які часто стають критичною вразливістю, що зазначає Mandru, S. (2022) [3].

Окрім загального розгляду безпеки в хмарі, у літературі виокремлюється роль керування доступом до привілейованих облікових записів (PAM). Авторами Garbis, J., Chapman, J.W. (2021) [4] досліджено, що розширені права адміністраторів і розробників створюють потенційно небезпечну «точку входу» для зловмисників. Тому низка дослідників пропонує поєднувати обов'язкову багатоетапну автентифікацію, аудит активності та обмеження тривалості привілеїв [3, 5].

Зокрема, авторами Taiwo Awoyinfa, James Greenwood, Varvara Semenova (2023) [6] описано механізм тимчасового підвищення привілеїв (temporary elevated access), за яким додаткові права користувачеві надаються лише на визначений проміжок часу, необхідний для виконання конкретного завдання. Після завершення цього часу система автоматично відкликає доступ, що зменшує імовірність зловживань і усуває потребу надавати працівникові постійну роль з найвищими повноваженнями. Вважаємо, що також важливим елементом комплексного підходу до безпеки є автентифікація (MFA), яка поєднує кілька факторів перевірки (пароль, одноразовий код, біометрію тощо). За даними [7], це значно ускладнює несанкціонований доступ до системи, навіть якщо окремий фактор (наприклад, пароль) стає відомий зловмисникам. У контексті хмарних сервісів, зокрема AWS, автори в [8] аналізують можливості AWS SSO (Single-Sign On, зараз IAM Identity Center), в якому реалізовано централізоване керування ролями та MFA для різних AWS-акаунтів і сторонніх застосунків. Така інтегрована модель допомагає дотримуватися принципу «найменших привілеїв» у масштабах усієї організації та дає змогу гнучко впроваджувати Zero Trust-архітектуру [9].

Таким чином, у літературі підкреслюється, що комплексне поєднання IAM, Zero Trust, PoLP, PAM-рішень та багатофакторної автентифікації, доповнене механізмами тимчасового підвищення привілеїв, відіграє ключову роль у захисті сучасних хмарних інфраструктур від внутрішніх та зовнішніх загроз.

Мета та завдання дослідження. Метою роботи є дослідження сучасних підходів до управління доступом у хмарному середовищі, аналіз їхньої достатності у контексті сучасних викликів безпеки та визначення перспектив подальшого розвитку, включно з можливостями ML, AI і NLP. Завдання дослідження:

- Розглянути традиційні та сучасні методи управління доступом (MFA, SSO, Zero Trust, PoLP).

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

- Аналізувати переваги та виклики впровадження IAM, PAM-рішень у хмарних сценаріях.
- Оцінити ефективність моделей типу Zero Trust і найменших привілеїв (PoLP) з погляду забезпечення захисту даних.
- Виявити напрями розвитку технологій управління доступом у мультихмарних середовищах та оцінити їхні обмеження.
- Сформулювати висновок, що узагальнить здобуті результати й визначить потенціал ML, AI та NLP для подальшого вдосконалення методів доступу.

Результати досліджень

Перші системи управління доступом були невіддільні від локальних мереж та серверів, де основний акцент робився на класичні механізми аутентифікації за допомогою статичних паролів чи вибіркового обліку активних сеансів. Зауважимо, що у невеликих (локальних) мережах цей підхід цілком задовольняв потреби організацій: ризики були відносно низькими, інфраструктура мала чіткі кордони, а користувачі працювали всередині корпоративного периметру. Проте, зі зростанням масштабів та ускладненням IT-середовищ, зокрема появою розподілених систем, модель «замкненого периметру» перестала ефективно функціонувати. Зрештою, збільшення кількості користувачів та додатків призвело до того, що традиційне управління доступом виявилося обтяжене дублюванням облікових даних, надмірною кількістю ролей і громіздкими процесами оновлення політик, що обґрунтовує автор Ghadge, N. (2024) [10].

Подальший перехід бізнесу в хмарні середовища підсилив проблему масштабованості та безпеки. Організації, що почали використовувати публічні або гібридні хмари, стикнулися з потребою інтегрувати нові методи аутентифікації та авторизації для великої кількості розподілених ресурсів. Зрозуміло, що умовах динамічного створення й видалення серверів, контейнеризації та мікросервісів, ручне управління обліковими записами й привілеями стало надто складним і ризикованим. Маємо підстави вважати, що саме це і підштовхнуло розвиток сучасних IAM-рішень, які передбачають ідентифікацію, контроль над привілейованими доступами до інформації і інфраструктури, багатофакторну автентифікацію, а також автоматизований моніторинг поведінки користувачів у хмарному середовищі. Такий підхід не лише підвищив безпеку, а й підготував ґрунт для впровадження методологій Zero Trust та «найменших привілеїв», а згодом і для інтеграції методів машинного навчання, штучного інтелекту та обробки природньої мови.

Використання IAM значно знижує ризик несанкціонованого доступу, особливо при впровадженні MFA та адаптивних механізмів аутентифікації. Аналізуючи статтю автора Chava, A. (2024) [2], можемо зробити висновок, що компанії, які впровадили централізоване IAM-рішення із принципом «найменших привілеїв» на початкових етапах розробки хмарної інфраструктури, змогли значно скоротити кількість інцидентів, пов’язаних із компрометацією облікових записів та їх несанкціонованим продажем. Зокрема, адаптивна автентифікація, що використовує аналіз поведінкових шаблонів, дозволяє ідентифікувати користувачів на основі їх звичної активності та виявляти підозрілі дії. Наведемо приклад - якщо користувач намагається отримати доступ до корпоративної мережі з незвичної локації або незнайомого пристрою, система може автоматично вимагати додаткову перевірку або блокувати запит.

Identity and Access Management (IAM). Узагальнений термін для технологій і процесів, що дозволяють контролювати, хто (або що) може отримувати доступ до ресурсів у певному середовищі, а також у яких випадках, на яких умовах і з якими привілеями. У традиційних (локальних) IT-середовищах під IAM мають на увазі системи управління обліковими записами користувачів, групами, політиками безпеки, наданням доступу до файлів, баз даних тощо. У хмарному ж контексті, наприклад в AWS, підхід стає більш багатовимірним через динамічну природу інфраструктури, розподілену модель доступу та необхідності централізованого контролю.

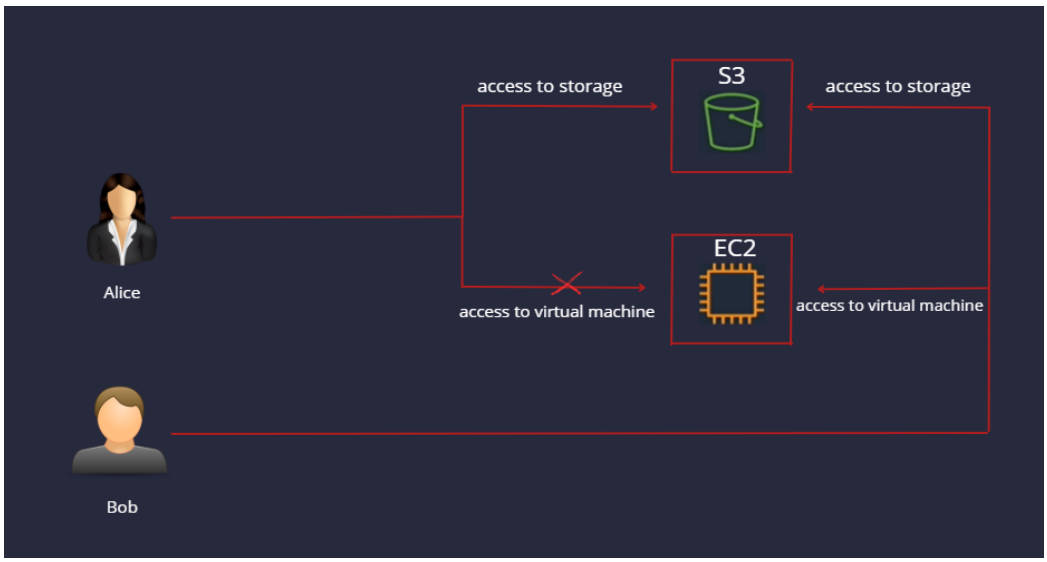

Рис. 1. Приклад контролю доступу засобами IAM. [1]

На рисунку (рис. 1) зображено ситуаційну модель, коли двоє користувачів в одній компанії мають мати гранульований доступ відповідно до їхніх робочих функцій. Причому, користувач Alice має мати доступ до сховища S3 (Simple Storage Service), але не має мати доступу до віртуальної машини EC2 (Elastic Compute Cloud), а системний адміністратор Bob має мати доступ до обох сервісів. Це типова ситуація для застосування IAM підходу, де IAM політики доступу для Alice та Bob будуть мати наступний вигляд:

Alice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3Read",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::example-bucket",
        "arn:aws:s3:::example-bucket/*"
      ]
    },
    {
      "Sid": "DenyEC2Access",
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*"
    }
  ]
}
```

Bob:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AllowS3AndEC2",
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "ec2:*"
      ],
      "Resource": "*"
    }
  ]
}
```

За таких політик доступу, Alice може виконувати лише операції читання об'єктів у сховищі S3 (діапазон дій обмежено до `GetObject` та `ListBucket`), а всі операції з EC2 для неї заборонено. Системний адміністратор Bob отримує повний доступ як до S3, так і до EC2 (усі операції `"s3:*"` та `"ec2:*"`).

Ключові принципи IAM. Наведемо наступні принципи IAM, що на думку авторів є ключовими:

●Найменші привілеї (Least Privilege) - полягає в тому, що кожному користувачеві, процесу чи сервісу виділяються лише ті права, які потрібні для виконання поточного завдання. Це унеможливлює ситуацію, коли, наприклад, розробник має доступ не лише до тестових, а й до виробничих середовищ без жодної потреби. На прикладі хмарного постачальника AWS, ми можемо налаштувати IAM-політику, що дозволяє лише «читати» об'єкти всередині конкретного сховища S3, без права створювати або видаляти їх.

●Розмежування обов'язків (Separation of duties) - завдяки цьому принципу важливі зміни не може вносити одна людина «від початку й до кінця». Наприклад, один спеціаліст ініціює створення привілейованої ролі, а інший — затверджує цю зміну в системі керування конфігурацією.

●Мультифакторна автентифікація (MFA) - для посиленої перевірки справжності користувачів чи сервісів рекомендується поєднувати декілька факторів (пароль, SMS/Push токен, біометрія тощо). У хмарному середовищі MFA часто є обов'язковою вимогою до адміністраторів або привілейованих акаунтів.

●Делегування доступу через ролі (Role-Based Access Control) - замість «жорстких» прив'язок до облікових записів (наприклад, користувацьких), AWS та інші провайдери пропонують використовувати ролі. Роль задає набір привілеїв, а користувач або сервіс «беруть на себе» (assume) цю роль на час виконання певних операцій.

●Аудит і моніторинг - безперервний запис подій (наприклад, AWS CloudTrail) дає змогу відстежувати, хто і які дії виконував, та вчасно реагувати на порушення.

●Сесійне підключення (session-based access) – дозволяє впроваджувати механізм отримання тимчасових (ефемерних) облікових даних користувачем або процесом, які автоматично втрачають чинність через певний час. Сесійне підключення дозволяє уникнути ситуацій, коли «назавжди дійсні» ключі зберігаються у відкритому вигляді та можуть бути скомпрометовані; натомість, користувач (чи процес) отримує лише короткочасні права доступу, що підсилює загальний рівень безпеки.

Причини і виклики щодо впровадження IAM у хмарі. Виділимо основні причини і виклики щодо впровадження IAM у хмарній інфраструктури:

● Зростання кількості користувачів і ролей - у великих мультихмарних середовищах необхідно уникати «хаосу» в правах, адже надмірні привілеї підвищують ризик атак та ускладнюють адміністрування;

● Високий ризик витоку даних - випадкове призначення критичних прав або відкриті паролі в репозиторії — серйозна загроза. IAM дає змогу упорядкувати доступ і унеможливити

надмірні привілеї через Permission Boundaries – спеціальні політики, які обмежують максимальний перелік доступів для користувача чи груп користувачів;

- Дотримання нормативних вимог - стандарти, на кшталт PCI DSS (Payment Card Industry Data Security Standard) [11] чи GDPR (General Data Protection Regulation) [12], зобов'язують відстежувати та логувати всі операції. Правильно налаштований IAM відповідає цим вимогам, гарантуючи аудит доступів.
- Масштабованість і гнучкість - у міру розширення компанії (нові середовища, сервіси) IAM спрощує додавання користувачів і забезпечує контроль безпеки.

Вважаємо, що надто складні політики IAM можуть призводити до помилок, а «сірий доступ» (застарілі ключі, тимчасові паролі) створює вразливості. Для зменшення цих ризиків, Josang, A. (2025) [13] у своєму дослідженні вказує на регулярну ротацію даних облікових даних та навчання персоналу принципам найменших привілеїв і роботи з IAM-ролями.

Можемо зробити висновок, що загальна мета IAM — надавати конкретному користувачеві достатній рівень доступу до правильних ресурсів у конкретний момент.

Privileged Access Management (PAM). У середовищі, де оновлення виконуються безперервно, наявність надійної системи для захисту привілейованих облікових записів стає критичною. PAM має на меті контролювати, відслідковувати й захищати найвищі рівні доступу в організації — наприклад, доступи супер-користувача чи системні облікові дані. Згідно з дослідженням W. Tirtadjaja, M. E. Rana та K. Shanmugam [14], якщо подібні ключі чи паролі випадково опиняються у відкритому доступі, це може призвести до витоку даних, блокування роботи застосунків чи ураження всієї інфраструктури (рис. 2).

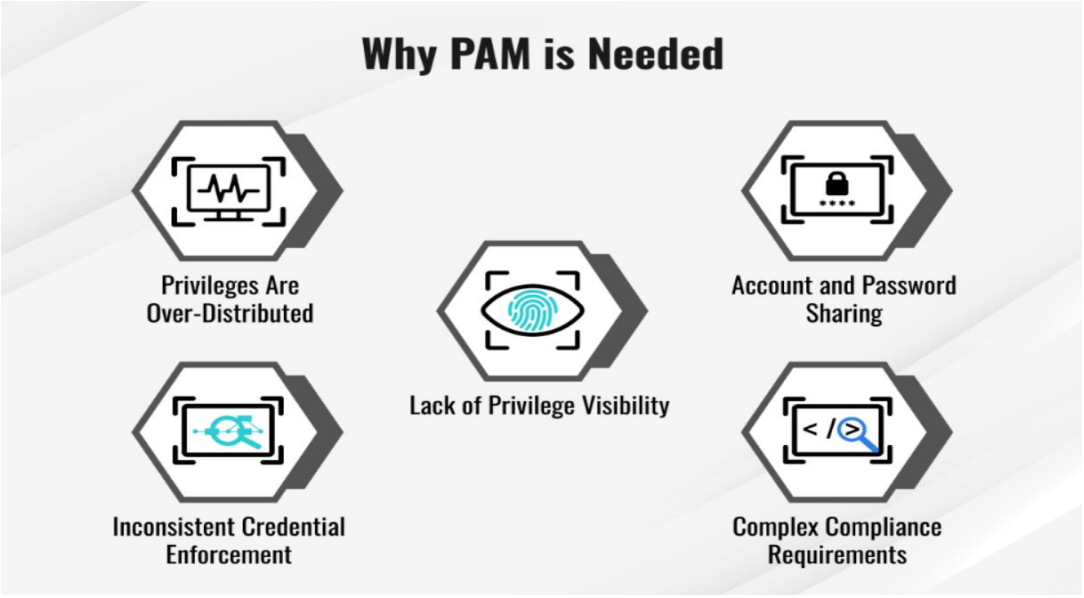

Рис. 2. Проблеми, що вирішує PAM. [15]

На думку авторів, відсутність механізмів PAM у розрізі DevOps (підхід, що базується на інтеграції та автоматизації процесів розробки програмного забезпечення й інформаційних технологій) підходів до автоматизації, часто призводить до:

- проблем із явним вказанням привілейованих облікових даних безпосередньо у конфігураційному файлі, що у разі витоку надає зловмиснику «прямий доступ» до критичної інфраструктури;
- унеможливлює аудит активності та прозорий контроль за тим, хто і в який момент користується привілейованими обліковими даними;
- відкриває доступ до ширших повноважень, що створює можливість для зловживань або помилок, що можуть паралізувати проєкт.

Основні принципи PAM. Охарактеризуємо основні принципи PAM:

- централізоване зберігання автентифікаційних даних - впровадження спеціалізованих сховищ (Vault-платформи, AWS Secrets Manager із AWS Key Management Service), які шифрують облікові дані, забезпечують ротацію паролів і надають доступ лише за чіткими політиками авторизації.
- контроль сесій і моніторинг активності - PAM надає можливість запису або трансляції привілейованих сесій (адміністраторських), що дає змогу швидко визначити відповідальну особу і причину ризикованих дій у випадку інциденту.
- автоматизація ротації ключів**.** Система PAM повинна регулярно змінювати пароль або ключ після кожного використання чи через певні інтервали, аби мінімізувати потенційну шкоду, якщо облікові дані потраплять «не в ті руки».
- тимчасове надання привілеїв за запитом (Just-in-Time Access) - у такій моделі користувачі або процеси отримують розширені права тільки на обмежений час і лише для виконання конкретних завдань. Після завершення цього періоду доступ автоматично скасовується, що додатково зменшує вірогідність зловживань та витоків.

У висновку, запровадження PAM-рішень є критично важливим для забезпечення безпеки й безперервного вдосконалення хмарних сервісів та контейнеризованих середовищ, де доступ до привілейованих облікових записів повинен бути ретельно контрольованим та прозорим

Single-Sign On (SSO). Дозволяє користувачеві (співробітнику, партнеру чи клієнту) автентифікуватися один раз і отримувати доступ до різних додатків чи сервісів без повторного введення логіну/паролю. За даними автора [4], такий механізм не лише покращує зручність користувачів, а й підвищує загальний рівень безпеки, оскільки єдиний «вхід» централізовано контролюється та відстежується. SSO інтенсивно використовує IAM як базовий рівень управління обліковими записами, групами, ролями. У хмарному середовищі (AWS, Azure, GCP) зазвичай передбачені нативні засоби SSO (наприклад, AWS SSO/AWS IAM Identity Center), що інтегруються з іншими сервісами і політиками безпеки (Service Control Policies, Managed Policies тощо).

Основні компоненти SSO. Наведено основні компоненти SSO:

- IdP (Identity Provider) - сторона (сервіс або сервер), яка «знає» користувача, зберігає його облікові дані та видає токени аутентифікації. Приклади: Okta, Azure AD (Entra ID), AWS IAM Identity Center (раніше AWS SSO), Keycloak тощо.
- SP (Service Provider) - додаток чи вебсервіс, який «дозволяє» доступ за умови, що користувач надав валідний токен від IdP.
- Сесійний/автентифікаційний токен - у SSO найчастіше використовують SAML (Security Assertion Markup Language), OAuth (Open Authorization) 2.0, OpenID Connect або інші протоколи, що дозволяють SP перевірити дійсність токена й отримати інформацію про користувача.

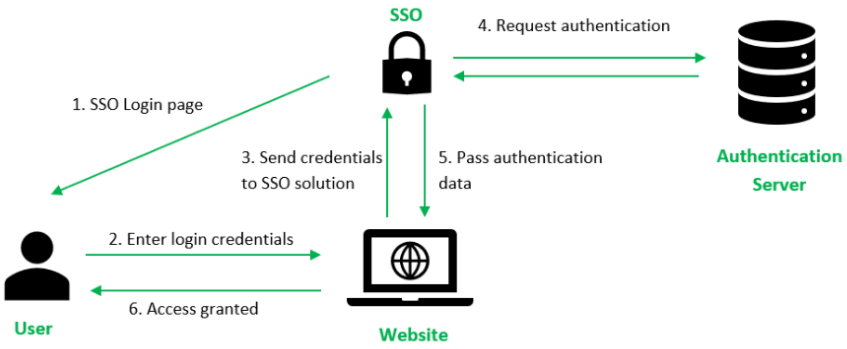

Рис. 3. Схема автентифікації по SSO. [16]

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

Процес автентифікації по SSO наступний (рис. 3):

1. Користувач переходить до програми (SP), але не автентифікований.
2. SP перенаправляє користувача до IdP (серверу автентифікації).
3. IdP перевіряє логін/пароль (або MFA) і, якщо все гаразд, видає токен.
4. Користувач повертається до SP з токеном. SP перевіряє його справжність (може звернутися до IdP або користуватися локальною перевіркою).
5. Доступ надано, і користувач отримує сесію, що діє певний час, та отримує доступ до додатка.

Якщо користувач згодом відкриває інший додаток, що теж довіряє цьому IdP, процедуру аутентифікації повторювати не потрібно — в рамках поточного сеансу він вже вважається перевіреним.

Переваги впровадження SSO. Серед переваг впровадження SSO, виділимо наступні:

- покращений користувацький досвід - менше полів для заповнення, зменшення кількості паролів.
- вища безпека - єдине місце автентифікації з MFA, централізованими політиками.
- прозорість - легше збирати та аналізувати журнали входів, у тому числі для відповідності стандартам PCI DSS, HIPAA (Health Insurance Portability and Accountability Act), GDPR.
- Масштабованість - легко додавати нові додатки (SP), передаючи їм лише параметри інтеграції з IdP.

Отже, Single Sign-On — фундаментальний механізм, що забезпечує автентифікацію «в один клік» до різних сервісів, покращуючи як зручність для користувачів, так і підвищуючи загальний рівень безпеки. Автор BasavaRaju, D. K. (2019) [8] у своєму дослідженні рекомендував поєднувати SSO з мультифакторною автентифікацією**,** IAM (керування ролями й політиками) та PAM (контроль привілейованих сесій) для побудови комплексної системи захисту в хмарних і гібридних середовищах.

Zero Trust – недовіра по замовчуванню

Zero Trust (у перекладі «нульова довіра») — це модель безпеки, у якій жодна мережа, користувач чи пристрій не вважається «довіреним» за замовчуванням. Кожен запит на доступ до даних чи сервісів вимагає повторної перевірки та авторизації. Відповідно до дослідження автора Johnny, R. (2019) [18], базові принципи Zero Trust можна сформулювати так:

1. Міжмережна сегментація - інфраструктуру розбивають на дрібніші «зони безпеки» (наприклад, мікросервіси, окремі облікові записи, VPC у хмарі), щоб ускладнити латеральний рух зловмисників у випадку компрометації одного вузла.
2. Постійна верифікація - навіть якщо користувач успішно пройшов аутентифікацію, кожний запит повинен перевірятися додатково: чи є у нього потрібний рівень привілеїв, чи відповідає його профіль нормам поведінки тощо.
3. Динамічний контроль доступу - рівень доступу може змінюватися залежно від контексту (геолокація, час доби, пристрій). Якщо система виявляє аномалії, їй варто посилити перевірки (MFA) або взагалі тимчасово заблокувати доступ.
4. Жорстка політика «ніколи не довіряй» - будь-яка частина системи повинна бути готова «не довіряти» іншій частині і вимагати додаткової авторизації або шифрування.

Інтеграція Zero Trust із IAM

У сучасному хмарному середовищі, наприклад, у AWS, реалізація Zero Trust неможлива без IAM [19]**,** оскільки саме IAM забезпечує:

- керування обліковими записами та ролями - кожен користувач чи сервіс отримує окрему ідентифікацію (користувацький обліковий запис, роль, група), що дає змогу відстежувати та контролювати операції дуже детально.

● мультифакторну автентифікацію (MFA), що допомагає у перевірці на різних рівнях: навіть якщо пароль став відомим зловмисникам, наявність другого фактора (апаратний токен чи мобільний додаток) значно ускладнює несанкціонований доступ.

● політики доступу «на вимогу» - IAM може надавати тимчасові облікові дані (ефемерні токени), які дійсні лише короткий час. Це відповідає ідеї Zero Trust: навіть якщо токен «скопроментований», зловмисник не зможе тривалий час ним скористатися.

● суворе журналювання (AWS CloudTrail), завдяки IAM можна ідентифікувати, хто саме виконав певну дію, в який час і з якої IP-адреси, що відповідає принципу «завжди перевіряй та моніторі».

Взаємодія Zero Trust із PAM

Зауважимо, що PAM зосереджений на привілейованих облікових записах, тобто таких, що дозволяють адмініструвати інфраструктуру, отримувати доступ до критичних баз даних, керувати мережею або CI/CD (Continuous Integration/Continuous Deployment) конвеєрами. У контексті Zero Trust:

1. Локальний адміністраторський доступ заміщується на користь централізованого контролю. Усі привілейовані доступи (SSH-ключі (Secure Shell), паролі root) передаються через PAM-інструменти, що забезпечують періодичну ротацію і відстежують, хто і коли використовував їх.

2. Динамічне надання привілеїв - Zero Trust вимагає, щоб кожен крок був обґрунтований. PAM реалізує те саме в контексті привілейованих акаунтів, дозволяючи Just-in-Time Access: доступ «на вимогу» з таймером автоматичного відкликання.

3. Моніторинг і журналювання сесій. PAM-продукти часто зберігають записи дій адміністраторів. Якщо аналіз журналів виявляє аномалію (зайвий запуск команд, звернення до конфіденційних директорій), система може заблокувати або запросити додаткове підтвердження.

З погляду Zero Trust, кожен привілейований запит має знову перевірятися: PAM якраз і виконує роль точкового «пропускного» механізму для облікових даних найвищого рівня.

Zero Trust і принцип найменших привілеїв (PoLP)

PoLP (Principle of Least Privilege) означає, що кожен користувач, процес або сервіс отримує лише той обсяг доступу, який вимагається для конкретної задачі. У контексті Zero Trust, IAM та PAM виділимо наступні:

1. Чіткі політики доступу - у IAM вказуються мінімально необхідні дії (наприклад, розробник Alice може переглядати деякі S3-дані, але не видаляти чи модифікувати).

2. Рольова модель - для взаємодії зі сховищем, сервісом чи базою даних користувач «бере на себе» (assume) конкретну роль на обмежений час; ролі виділяють лише потрібні дії (створення, видалення, читання).

3. Тимчасове надання привілеїв за запитом - при застосуванні PoLP з Zero Trust і PAM, надання привілейованих доступів відбувається через тимчасові автентифікаційні дані і токени, які швидко відкликаються. Якщо виявлено несанкціоновану активність — доступ одразу знешкоджується.

Автори [3, 4, 5] виділяють наступні особливості Zero Trust:

1. Поведінковий аналіз і аудит - Zero Trust посилює контроль із залученням моделей поведінкового аналізу (якщо користувач зазвичай лише має доступ до читання сховища S3, а зараз раптово намагається видаляти багато об’єктів — це сигнал тривоги) [4].

2. Автоматизація конфігурації - при інтеграції з DevOps практиками IaC (Infrastructure as Code), CI/CD, Zero Trust «вшивається» на рівні Pipelines, де PAM-інструменти видають ключі лише на конкретні стадії збірки. По завершенню — привілеї відкликаються, а IAM звітує в журнали CloudTrail [3].

3. Сегментація та політики SCP - AWS Organizations і Service Control Policies (SCP) часто згадуються як базовий інструмент для сегментації акаунтів. Це дає змогу на кожному рівні

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

заборонити певні дії (наприклад, будь-які операції з IAM у виробничому середовищі), що підтримує Zero Trust-архітектуру на організаційному рівні [5].

Zero Trust – це методологія «ніколи не довіряй за замовчуванням», яка базується на постійній перевірці користувачів/пристроїв і динамічному контролі. Разом Zero Trust, IAM, PAM і PoLP формують багаторівневу систему безпеки, яка знижує ризик несанкціонованого доступу та полегшує масштабування інфраструктури відповідно до сучасних вимог DevOps і хмарних застосунків (рис.4). Успішним кейсом впровадження Zero Trust є практика великих фінансових установ, які використовують цю модель для управління доступом до критично важливих систем [9]. Внаслідок цього значно зменшилася кількість внутрішніх порушень безпеки, спричинених неналежним використанням облікових записів.

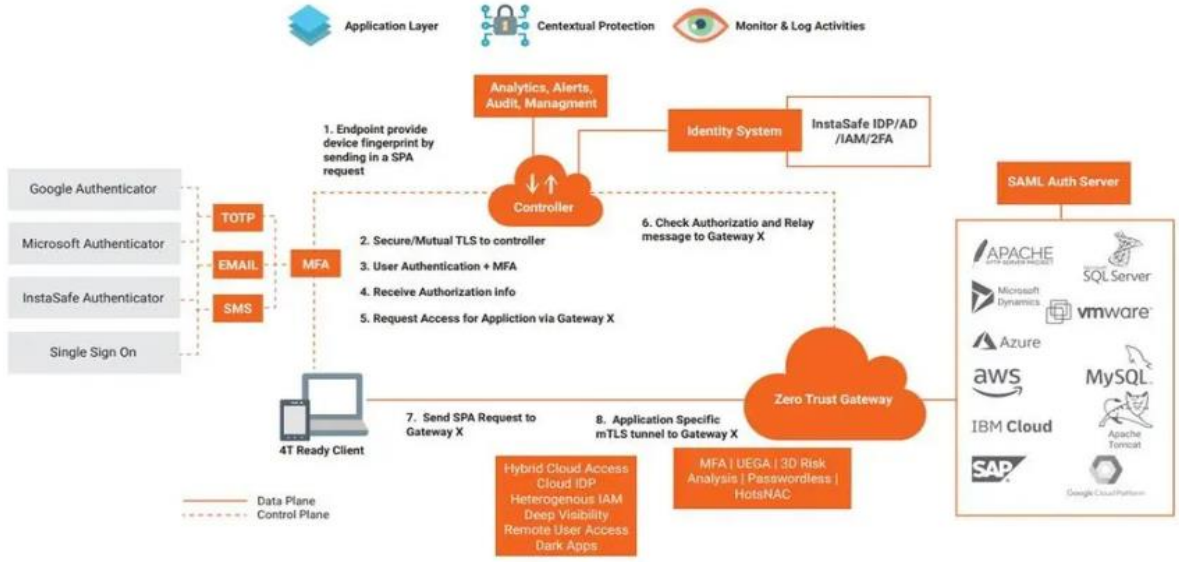

Рисунок 4. Схема архітектури Zero Trust. [17]

Виклики сучасному «золотому стандарту»

Окреслимо, що Zero Trust базується на принципі, що жоден компонент або користувач не повинен вважатися «безпечним за замовчуванням». Кожен запит на доступ має повторно автентифікуватися, а всі операції — перевірятися незалежно від того, «де» фізично чи логічно перебуває користувач. Цей підхід суттєво змінив парадигму корпоративної безпеки, оскільки:

1. Сувора сегментація - організація структурує свою інфраструктуру на відокремлені «зони безпеки». Завдяки цьому ускладнюється бічний рух зловмисника усередині мережі.
2. Безперервний моніторинг - кожен запит (до бази даних, до веб-додатку чи внутрішньої системи) аналізується з точки зору відповідності контексту (геолокація, час доби, історія дій користувача).
3. Мінімізація довіри (навіть усередині мережі) - користувач у межах «внутрішньої» мережі компанії не має автоматично отримувати більші привілеї. Кожна дія вимагає перевірки та авторизації.
4. Динамічний контроль доступу - рівень доступу формується на основі ризику (Risk-Based Access Management). Якщо активність здається ризикованою, запускається додаткова автентифікація чи обмежуються операції [20].

Zero Trust ефективно дає змогу зменшити ризик бічних атак і компрометації ключових систем. Проте досвід компаній, що працюють у мультихмарних середовищах (AWS, Azure, GCP, тощо), демонструє, що деякі аспекти безпеки та автоматизації в Zero Trust важко реалізувати засобами «класичних» інструментів [9]:

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

- Складність централізованого управління політиками - у мультихмарних середовищах з різнорідними IAM-моделями (AWS IAM, Google Cloud IAM, Azure AD) підтримувати єдиний набір Zero Trust-політик непросто. Потрібне зведення логів, подій та ролей «під один дах», що ускладнюється відсутністю уніфікованих стандартів.
- Надмірна кількість хибно-позитивних сповіщень - при активному контролі кожного запиту Zero Trust генерує величезний потік логів і тригерів. Це створює значне навантаження на безпекові команди, які змушені переглядати й фільтрувати гігабайти подій.
- Обмежені можливості прогнозування - Zero Trust орієнтований на поточні або вже відомі загрози. Однак сучасні атаки, зокрема варіанти зі зміною тактик, наприклад APT (Advanced Persistent Threats) та складні фішингові кампанії, що вимагають проактивної ідентифікації нетипової поведінки чи аномальних шаблонів, що не завжди легко виявити традиційними методами.
- Інцидент-орієнтований підхід - Zero Trust добре реагує на вже виявлені ризики. Проте повна автоматизація виявлення і класифікації інцидентів досі обмежена — особливо, коли потрібний аналіз змісту (наприклад, тексти листів, логів, повідомлень у внутрішніх чатах).

Прогалини у Zero Trust. Наведемо приклади аспектів, які Zero Trust самостійно не покриває:

1. Складні «соціотехнічні» атаки - соціальна інженерія, складні фішингові схеми, списи-фішинг (spear-phishing) — Zero Trust перевіряє доступи, однак не завжди здатний аналізувати текст повідомлень або визначати, що саме відбувається «поза контурами» традиційної авторизації.
2. Інтегровані мультихмарні сценарії - Zero Trust захищає ресурси, але в кожній хмарі свої політики IAM [21], свої механізми ліцензування та логування. Координація й уніфікація цих політик часто потребує ручної роботи або зовнішніх інструментів.
3. Вчасна диференціація рівня доступу - у багатьох випадках потрібно забезпечити миттєву зміну політики доступу. Zero Trust передбачає «перевірку» кожного запиту, проте без AI- та ML-аналізу складно оцінити контекст загрози у реальному часі (поведінку користувача, артефакти потенційної компрометації тощо).

Перспективи інтеграції управління доступом з AI (Artificial Intelligence), ML (Machine Learning) та NLP (Natural Language Processing). Сформулюємо наступні визначення вище перелічених технологій:

- AI — це широка галузь комп'ютерних наук, мета якої навчити системи виконувати завдання, що зазвичай вимагають людського інтелекту. Сюди належать розпізнавання образів, прийняття рішень, розуміння мови й інші когнітивні функції;
- ML — це піднапрямок AI, який зосереджується на розробці алгоритмів, що здатні самостійно «вчитися» на даних без чіткого програмування. ML-моделі визначають закономірності у великих масивах інформації та можуть робити прогнози або ухвалювати рішення (наприклад, класифікувати загрози за рівнем ризику);
- NLP — це технологія, яка дає змогу комп'ютерам розуміти, інтерпретувати й генерувати природну (людську) мову. У контексті безпеки завдяки NLP можна виявляти фішингові повідомлення, аналізувати тексти журналів подій чи листів, а також розуміти зміст і наміри зловмисників, сховані у текстових каналах.

AI, ML та NLP інтеграція із Zero Trust. Інтеграція Zero Trust із технологіями AI, ML та NLP може бути застосована у наступному вигляді:

1. AI для адаптивного (risk-based) доступу
   - Динамічна модель ризику. Машинний інтелект аналізує минулу поведінку користувача, контекст сеансів та виявляє підозрілі зміни, щоб у режимі реального часу підвищувати або знижувати рівень доступу.

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

- Контекстуальна оцінка. ML-алгоритми враховують геолокацію, годину доби, історію взаємодій, аномальні ознаки в запитах тощо, аби автоматично коригувати політики доступу (Zero Trust).

2. Автоматизація інцидент-менеджменту

- Зниження потоку хибних тривог. ML-моделі оперативно обробляють величезні журнали подій (logs), визначаючи аномалії та істотно скорочуючи кількість «false positives», характерних для суворих Zero Trust-налаштувань.
- Самонавчання на інцидентах. Нейронні мережі вчяться на попередніх загрозах, постійно вдосконалюючи точність прогнозів та рекомендацій щодо реагування.

3. NLP для аналізу змісту

- Виявлення фішингу. Фішингові кампанії часто будуються на текстових повідомленнях. NLP допомагає розпізнавати специфічні мовні шаблони, «сигнали обману» та визначати рівень небезпеки листа.
- Класифікація інцидентів. Методами NLP можна автоматично розподіляти репорти чи логи за типами інцидентів, визначати їх критичність і автоматично запускати відповідні сценарії (протоколи) Zero Trust.

4. Проактивне виявлення складних атак

- Прогнозування на основі шаблонів. AI здатний виявляти кореляції у поведінці користувача (наприклад, нестандартні години входу, нові пристрої, одночасний доступ до конфіденційних ресурсів). Це дає змогу попередити ріст ризику та вжити контрзаходів.
- Адаптивні тривоги. Зі збільшенням обсягу даних ML-алгоритми краще розрізняють нормальну поведінку й атаку, суттєво зменшуючи кількість фальшивих сповіщень.

Компенсація недоліків Zero Trust за допомогою AI, ML і NLP. Базуючись на аналізі недоліків Zero Trust, можемо сформулювати наступні покращення у разі інтеграції із AI, ML та NLP:

1. Глибинний поведінковий аналіз

- ML-моделі можуть відстежувати нетипову поведінку користувачів у різних сценаріях. Наприклад, якщо працівник ніколи не експортував великі обсяги даних із S3-бакета, а тепер робить це опівночі з чужого регіону, система автоматично блокує дію чи активує додаткову аутентифікацію (MFA, ручне підтвердження тощо).
- Такий адаптивний підхід дозволяє миттєво реагувати на нестандартні ситуації, випереджаючи розвиток потенційної атаки.

2. Зниження навантаження на SOC

- Система зі штучним інтелектом відсіює «псевдотригери» та очевидні фальшиві сповіщення, які часто виникають за умов суворого Zero Trust (коли кожен запит гіпотетично вважається ризиковим).
- У результаті аналітики у центрах безпеки (SOC) одержують відфільтровані інциденти, які дійсно заслуговують на увагу, що збільшує ефективність і економить час.

3. Семантичний аналіз

- NLP-алгоритми здатні розпізнавати шкідливий вміст листів, чатів, внутрішніх повідомлень: виявляти фішингові шаблони, потенційні маркери витоку інформації, ключові слова тощо [22].
- Zero Trust в базовому вигляді не «читає» самих повідомлень і не визначає їх зміст, тоді як NLP дає змогу «зрозуміти» текст і відстежити підступні схеми атаки.

4. Єдине «полотно» для всієї інфраструктури

- Централізований моніторинг та SIEM/UEBA у поєднанні з ML-алгоритмами формують єдину картину безпекових подій у всіх хмарних середовищах.
- Наприклад, якщо у GCP зафіксовано невластиву активність, а в AWS паралельно з’являються нетипові запити з підвищеними привілеями, система об’єднає ці факти й згенерує

спільне попередження [23]. Це дає змогу швидше реагувати на складні атакувальні ланцюжки, які інакше залишилися б «розділеними» між різними хмарами.

Можемо зробити висновок, що поєднання Zero Trust із можливостями AI, ML та NLP забезпечує багаторівневий підхід до безпеки, що охоплює поведінкові шаблони, аналіз тексту та зведену картину подій у мультихмарному середовищі, що дозволяє оперативно реагувати на складні загрози, зменшувати помилкові сповіщення та в цілому підвищувати рівень кіберстійкості організації.

Перспективи розвитку управління доступом із AI, ML і NLP. Підсумувавши результати аналізу сучасних підходів, можемо зробити наступні висновки щодо подальшого розвитку управління доступом у хмарному середовищі, що буде зосереджений на:

1. Динамічному аналізі доступу й прогнозування ризиків за допомогою AI/ML
   - Алгоритми штучного інтелекту розпізнають аномалії в реальному часі та автоматично коригують політики доступу відповідно до поточного рівня ризику.
   - Машинне навчання (ML) дає змогу вивчати поведінкові шаблони користувачів і пристроїв, проактивно виявляти загрози ще до того, як вони зможуть завдати шкоди.
2. Безпарольній автентифікації
   - Активний перехід від традиційних паролів до біометричних методів (розпізнавання обличчя, відбитків пальців, голосу) та криптографічних протоколів (FIDO2, Fast Identity Online 2).
   - Завдяки ML можливе вдосконалення точності біометрії: система вчиться розрізняти «шум» або спроби підробки, аналізуючи найменші відмінності у даних.
3. Автоматизований моніторинг та адаптивний контроль доступу
   - Використання SIEM (Security Information and Event Management) та аналітики великих даних для оперативного виявлення загроз.
   - NLP-технології можуть аналізувати журнали подій (logs) та мережеві повідомлення, виявляючи підозрілі шаблони комунікацій (наприклад, фішингові листи).
   - Зростає популярність XDR (Extended Detection and Response), що об’єднує різні джерела даних безпеки, допомагаючи AI швидше виявляти складні атаки.
4. Квантово-стійкі алгоритми шифрування
   - Розробка рішень, що витримають загрозу квантових обчислень, є пріоритетом для хмарних середовищ, де велика кількість даних перебуває у відкритій мережі.
   - AI/ML-алгоритми можуть підбирати й тестувати оптимальні криптографічні методи, аналізуючи надійність різних ключів та механізмів.
5. Єдине управління доступом у гібридних і мультихмарних середовищах
   - Зріла інтеграція з AI для централізованої координації політик: ML-моделі узгоджують правила між різними постачальниками (AWS, Azure, GCP), знижуючи фрагментацію.
   - Єдина автентифікація та моніторинг у «розподілених» середовищах зменшує ризик «прогалин», коли різні хмари керуються різними підходами до доступу.
6. Розвиток Zero Trust Network Access (ZTNA)
   - Модель Zero Trust дедалі більше покладається на AI, ML та NLP, щоб автоматично адаптувати привілеї, оцінюючи контекст: місцезнаходження, час, тип даних, текст листування тощо.
   - Підхід «найменших привілеїв» посилюється завдяки ML, що аналізує поведінку користувача і знижує ризик внутрішніх атак.
7. Блокчейн у керуванні ідентифікацією
   - Децентралізовані системи аутентифікації можуть інтегруватися з ML-обробкою транзакцій, відстежуючи нетипову поведінку в реєстрі й підвищуючи прозорість.
   - Цей підхід може стати ефективною альтернативою традиційним централізованим методам зберігання облікових даних.

Робимо висновок, що майбутнє управління доступом зосередиться на інтелектуальних, адаптивних і автоматизованих рішеннях, глибоко інтегрованих із AI, ML і NLP. Це дозволить значно підвищити безпеку та відповідати викликам сучасних загроз, водночас залишаючись зручними для кінцевих користувачів.

Висновки

Управління доступом у хмарному середовищі залишається критично важливим аспектом загальної стратегії кіберзахисту, адже від нього залежить цілісність та конфіденційність корпоративних ресурсів. Завдяки широкому використанню IAM (Identity and Access Management), PAM (Privileged Access Management), та Zero Trust принципово підвищується рівень безпеки, але ці рішення потребують комплексного й узгодженого впровадження. Крім того, організаціям слід систематично переглядати й адаптувати політики управління доступом із урахуванням динамічних загроз і розбудови технологій. Особливу увагу слід приділяти автоматизації процесів за допомогою штучного інтелекту та поведінкової аналітики. Саме інвестиції в AI-/ML-рішення (machine learning, deep learning) дозволяють проактивно виявляти й блокувати аномалії, прогнозувати загрози та гнучко коригувати політики доступу. При цьому NLP (Natural Language Processing) доповнює Zero Trust, «читаючи» вміст повідомлень та журналів, виявляючи приховані фішингові чи соціоінженерні атаки. Паралельно збільшується тенденція до безпарольної автентифікації з розширенням біометричних підходів (розпізнавання обличчя, голосу, відбитків пальців). Перехід до рішень на зразок FIDO2 знижує вразливість до крадіжки та підбору паролів. Також набирають обертів проєкти з інтеграції блокчейну задля децентралізації систем ідентифікації та підвищення прозорості. У висновку, майбутнє управління доступом у хмарних середовищах формується за рахунок:

- Комплексного та автоматизованого підходу, що поєднує Zero Trust, ML-, NLP- та AI-алгоритми для швидкого виявлення й блокування загроз.
- Безперервної адаптації політик, завдяки аналізу поведінкових шаблонів користувачів та динамічній зміні привілеїв у режимі реального часу.
- Синергії різних технологій (блокчейн, біометрія, SIEM/XDR, квантово-стійкі алгоритми) задля підсилення контролю доступу.
- Відповідності нормативним вимогам, що гарантує не лише безпеку, а й довгострокову надійність хмарної інфраструктури.

Запровадження таких рішень дасть змогу компаніям мінімізувати ризики витоку облікових даних і сформувати більш зрілу, ефективну та масштабовану модель контролю доступу в умовах стрімкого зростання кіберзагроз.

Перелік посилань

1. Volodymyr Khoma, Aziz Abibulaiev, Andrian Piskozub, and Taras Kret. (2024). Comprehensive Approach for Developing an Enterprise Cloud Infrastructure, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3654 (2024) pp. 201–215.

2. Chava, A. (2024). APPLICATION SECURITY AND LEAST PRIVILEGE ACCESS IN MODERN DEVOPS. *The American Journal of Engineering and Technology*, *6*(10), 75-85. DOI: https://doi.org/10.37547/tajet/Volume06Issue10-09

3. Mandru, S. (2022). PAM (Privileged Access Management) and DevOps: Secure Management of Privileged Accounts: Integrating PAM with DevOps Practices To Ensure Secure Development Processes. *J Artif Intell Mach Learn & Data Sci 2022*, *1*(1), 783-787. DOI: https://doi.org/10.51219/JAIMLD/sri-kanth-mandru/194

4. Garbis, J., Chapman, J.W. (2021). Privileged Access Management. In: Zero Trust Security. *Apress, Berkeley, CA*. DOI: https://doi.org/10.1007/978-1-4842-6702-8_12

5. Tuononen, H. (2023). Privileged access management model for a managed service provider. https://urn.fi/URN:NBN:fi:amk-2023052614542

6. Taiwo Awoyinfa, James Greenwood, and Varvara Semenova. (2023). Temporary elevated access management with IAM Identity Center, *AWS Security Blog © 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved,* (Apr.2023). URL: https://aws.amazon.com/blogs/security/temporary-elevated-access-management-with-iam-identity-center/ (дата звернення: 24.02.2025).

© Абібулаєв А.Р., Піскозуб А.З. (2025). Аналіз сучасних підходів управління доступом у хмарному середовищі. Сучасний захист інформації, 1(61), 174–188.
https://doi.org/10.31673/2409-7292.2025.017186.

7. Semko, D., & Gerasymchuk, T. V. (2023). Securing your aws workloads: best practices for Identity and Access Management. URL: https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/1563bd9d-56a8-4d47-99cc-da50c5db5a92/content (дата звернення: 12.02.2025).

8. BasavaRaju, D. K. (2019). Single Sign on Using Cloud Computing. *JETIR-International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN*, 2349-5162. ISSN: 2349-5162

9. National Security Agency (NSA). (2023). Zero Trust Guidance. URL: https://media.defense. gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF (дата звернення: 01.02.2025).

10. Ghadge, N. (2024). Enhancing threat detection in Identity and Access Management (IAM) systems. *International Journal of Science and Research Archive*, *11*(2), 2050-2057. DOI: https://doi.org/10.30574/ijsra.2024.11.2.0761

11. PCI Security Standards Council, LLC, Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 (2022) © 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved. URL: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf (дата звернення: 03.02.2025).

12. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата звернення: 13.02.2025).

13. Josang, A. (2025). IAM—Identity and Access Management. In: Cybersecurity. Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-68483-8_9

14. W. Tirtadjaja, M. E. Rana and K. Shanmugam, (2021). Managing High Privileged Accounts in IT Enterprise: Enhanced Security Infrastructure, *International Conference on Data Analytics for Business and Industry (ICDABI)*, Sakheer, Bahrain, pp. 655-660, DOI: https://doi.org/10.1109/ICDABI53623.2021.9655847

15. Fortinet, (2025). What Is Privileged Access Management (PAM)? Copyright © 2025 Fortinet, Inc. All Rights Reserved. URL: https://www.fortinet.com/resources/cyberglossary/privileged-access-management (дата звернення: 18.02.2025).

16. GeeksforGeeks, (2025). Introduction of Single-Sign On (SSO). (2024). @GeeksforGeeks, Sanchhaya Education Private Limited, All rights reserved. URL: https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso/ (дата звернення: 18.02.2025).

17. InstaSafe, (2025). Choosing the right Zero Trust architecture. Zero Trust Blog. URL: https://instasafe.com/blog/choosing-the-right-zero-trust-architecture/ (дата звернення: 20.02.2025).

18. Johnny, R. (2019). Identity and Access Management in Zero Trust Frameworks. URL: https://www.researchgate.net/profile/Ricky-Johnny/publication/388106052_Identity_and_Access_Management_in_Zero_Trust_Frameworks/links/678a377d98c4e967fa6712e2/Identity-and-Access-Management-in-Zero-Trust-Frameworks.pdf (дата звернення: 20.02.2025).

19. AWS Prescriptive Guidance: Embracing Zero Trust: A strategy for secure and agile business transformation Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved. URL: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/strategy-zero-trust-architecture/strategy-zero-trust-architecture.pdf (дата звернення: 21.02.2025).

20. Agorbia-Atta, C., Atalor, I., & andRichard Nachinaba, R. K. A. (2024). Leveraging AI and ML for Next-Generation Cloud Security: Innovations in Risk-Based Access Management. *World Journal of Advanced Research and Reviews*, *23*(3). DOI: https://doi.org/10.30574/wjarr.2024.23.3.2788

21. Singh, C., Thakkar, R. and Warraich, J. 2023. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*. 8, 4 (Aug. 2023), 30–38. DOI: https://doi.org/10.24018/ejeng.2023.8.4.307

22. Ismail, W. S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity. *J. Internet Serv. Inf. Secur.*, *14*(1), 195-205. DOI: https://doi.org/10.58346/JISIS.2024.I1.013

23. Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. *Authorization, and Access Control within Cloud-Based Systems (January 25, 2024)*. DOI: https://doi.org/10.9734/AJRCOS/2024/v17i3423

Надійшла 12.02.2025