

ПОРІВНЯЛЬНИЙ АНАЛІЗ РЕАЛІЗАЦІЇ МОДЕЛІ БЕЗПЕКИ ZERO TRUST У AWS ТА GOOGLE CLOUD PLATFORM

Вінницький національний технічний університет

Анотація

У роботі проведено порівняльний аналіз реалізації концепції Zero Trust («Нульова довіра») у хмарних середовищах AWS та Google Cloud Platform. Досліджено архітектурні відмінності IAM-систем: рольову модель доступу (RBAC) в AWS та контекстно-залежний доступ у GCP. Особливу увагу приділено інструментам AWS Identity Center та Google BeyondCorp, а також механізмам протидії латеральному переміщенню злоумисників. Визначено, що Google фокусується на проксі-орієнтованому підході, тоді як AWS надає перевагу гранулярним політикам на рівні ресурсів.

Ключові слова: IAM, Zero Trust, AWS, Google Cloud, BeyondCorp, найменші привілеї, хмарна безпека, Service Control Policies, Identity-Aware Proxy.

Abstract

The paper provides a comparative analysis of the Zero Trust concept implementation in AWS and Google Cloud Platform cloud environments. Architectural differences in IAM systems are investigated: Role-Based Access Control (RBAC) in AWS and context-aware access in GCP. Particular attention is paid to AWS Identity Center and Google BeyondCorp tools, as well as mechanisms for countering lateral movement of attackers. It is determined that Google focuses on a proxy-oriented approach, while AWS prioritizes granular resource-level policies.

Keywords: IAM, Zero Trust, AWS, Google Cloud, BeyondCorp, least privilege, cloud security, Service Control Policies, Identity-Aware Proxy.

Вступ

Поняття Zero Trust у контексті хмарних технологій набуло виняткового значення після розмиття традиційного мережевого периметра. Ця стратегія безпеки стала фундаментом для архітектури сучасних хмарних провайдерів, яка забезпечує безперервну верифікацію кожного запиту незалежно від походження трафіку. Її впровадження стало головним бар'єром проти атак на ланцюги постачання та витоків даних через скомпрометовані облікові записи. Функціонування IAM (Identity and Access Management) нині вийшло за межі простого адміністрування користувачів і набуло значення, як критична інфраструктура, що впливає на стійкість бізнесу. Тут важливо підкреслити не лише технічне, а й стратегічне значення вибору провайдера, адже логіка реалізації IAM у AWS та Google Cloud Platform кардинально відрізняється в підходах до ізоляції ресурсів [1].

Результати дослідження

Ера активного впровадження Zero Trust розпочалася після гучних кібератак 2010-х (зокрема, операція Aurora), коли довіра до внутрішньої корпоративної мережі перестала бути аксіомою. Інженери Google, реагуючи на загрози державного рівня, розробили архітектуру BeyondCorp, відмовившись від VPN на користь суворої перевірки пристроїв та користувачів на прикладному рівні [2]. Після цього підхід Identity as a Perimeter (Ідентичність, як периметр) став стратегічним стандартом, який AWS та Google розвивають паралельно до сьогодні [3].

Що таке Zero Trust у хмарі? Уперше цей термін був популяризований аналітиками Forrester, а згодом Національний інститут стандартів і технологій США (NIST) формалізував його концепцію у спеціальній публікації NIST SP 800-207, яка визначила базові принципи та компоненти цієї архітектури [4]. На практиці це повна відмова від поняття «довірена зона». Фактично, це система, у якій кожен запит до API розглядається, як потенційно ворожий, доки не доведено зворотне. В одному із звітів з

пентестингу, «білий хакер» намагався пояснити замовнику, чому не зміг просунутися вглиб інфраструктури AWS, хоча отримав доступ до одного сервера. «Просто лабіринт якийсь, а не мережа», – сказав він, коментуючи неможливість доступу через блокування на рівні IAM-політик.

Системи IAM діють у складних умовах: гібридні хмари, тисячі мікросервісів, BYOD (Bring Your Own Device). Попри це, AWS та GCP продовжують виконувати функції арбітра доступу, демонструючи різні шляхи до однієї мети.

Однією з найважливіших архітектурних відмінностей став підхід до структури дозволів. AWS зробив ставку на модель Implicit Deny (неявна заборона) та складну ієрархію політик. Рішення про доступ приймається на основі перетину identity-based policies, resource-based policies та permissions Boundaries. Це дозволяє досягти високої точності, але потребує глибокого розуміння JSON-структур [3].

Водночас ринок поставив перед адміністраторами вимогу: навчитися створювати політики найменших привілеїв або отримати критичну вразливість. Адміністратори AWS обрали шлях детальної гранулярності. Унаслідок неправильної конфігурації S3-бакетів постраждало багато компаній, але ті, хто опанував механізм Service Control Policies (SCP), отримали повний контроль над організацією.

Користувачі Google Cloud Platform пішли іншим шляхом – через адитивну модель, де права успадковуються за схемою «Організація → Папка → Проєкт». Це значно спрощує адміністрування, але створює ризик надмірних прав через надання доступу на верхньому рівні.

Наступний етап еволюції технологій відбувся з розвитком захисту сервісних акаунтів. В AWS ключовим механізмом стала служба AWS STS (Security Token Service), яка видає тимчасові токени на термін від 15 хвилин до 12 годин, усуваючи необхідність зберігання статичних ключів доступу. Google Cloud, навпаки, тривалий час покладался на завантажувані JSON-ключі для Service Accounts, що часто ставало вектором атак.

Однак із впровадженням Workload Identity Federation, GCP також перейшов на безключовий доступ, інтегруючи зовнішні ідентифікатори. До боротьби за периметр долучився інструмент VPC Service Controls у Google, який створює захищений контур навколо API-сервісів, запобігаючи витоку даних, навіть за наявності валідних облікових даних [5].

Вважається, що AWS IAM є більш складним для новачків через величезну кількість дозволів (actions), яких налічується понад 13 тисяч. Підхід Google Cloud часто називають більш «розробничо-орієнтованим» завдяки інтеграції з Google Workspace та інтуїтивному інтерфейсу Identity-Aware Proxy (IAP). Проте, чималий сектор Enterprise-клієнтів все ще тримається на AWS через можливість написати політику (Condition Keys), яка враховує, навіть час доби, наявність MFA та теги ресурсів. Зловмисники, коли стикаються з MFA Delete в AWS або апаратними ключами Titan у Google, нездатні обійти фізичну автентифікацію. У критичних ситуаціях, коли ключі доступу скомпрометовано, спрацьовує механізм автоматичної ремедіації (SOAR). Система моніторингу (AWS CloudTrail або Google Cloud Audit Logs) виявляє аномалію. Через виклики Lambda-функцій система може автоматично відкликати сесії, додати обмежувальні політики (DenyAll) та ізолювати скомпрометовану сутність, повертаючи контроль над периметром [6]. Відтоді стандарт NIST SP 800-207 вважають «біблією» архітекторів безпеки. Цей документ став символом переходу від захисту мереж до захисту даних і важливою сторінкою в історії хмарних обчислень [7].

Висновки

Модель Zero Trust у хмарах стала символом зрілості IT-індустрії. AWS, з його гранулярним механізмом IAM Policies, та Google Cloud із контекстно-орієнтованою архітектурою BeyondCorp, попри різні технічні реалізації, забезпечують єдиний стандарт безпеки. Це не просто налаштування прав доступу, а філософія, що забезпечила еволюцію від статичних ключів до тимчасових токенів і стала гарантом цілісності даних [7]. Порівняння цих платформ демонструє, що ідеальної системи не існує, однак баланс між автоматизованим реагуванням на інциденти та глибокою ізоляцією ресурсів формує надійний захист сучасного бізнесу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kodala V. A comparative study of zero trust security implementations across multi-cloud environments: aws and azure. *ResearchGate*. URL: https://www.researchgate.net/publication/394888333_ (дата звернення: 18.02.2026).
2. Walker K. Transparency in the shadowy world of cyberattacks. *Google*. URL: <https://blog.google/outreach-initiatives/public-policy/transparency-in-the-shadowy-world-of-cyberattacks/> (дата звернення: 18.02.2026).

3. Compare AWS and Azure services to Google Cloud | Get started | Google Cloud Documentation. *Google Cloud Documentation*. URL: <https://docs.cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison> (дата звернення: 19.02.2026).
4. *NIST Technical Series Publications*. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf> (дата звернення: 22.02.2026).
5. McNamara R. Complete Guide to AWS Security | Getting Started with AWS Security | Snyk. *Snyk*. URL: <https://snyk.io/articles/aws-security/> (дата звернення: 23.02.2026).
6. Automated Security Response on AWS. *Amazon Web Services, Inc.* URL: <https://aws.amazon.com/solutions/implementations/automated-security-response-on-aws/> (дата звернення: 23.02.2026).
7. SP 800-207A, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: <https://csrc.nist.gov/pubs/sp/800/207/a/final> (дата звернення: 25.02.2026).

Деркач Євгеній Юрійович – студент групи ЗКІТС-23б, Факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: derkaczena81@gmail.com

Науковий керівник: **Бондаренко Ірина Олексіївна** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Derkach Evgeniy Yuriyovich – student of group 3KITS-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, e-mail: derkaczena81@gmail.com

Supervisor: **Bondarenko Iryna O.** – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua