DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-20
УДК.004.7
Бідюк Олександр Володимирович, аспірант
https://orcid.org/0009-0009-8490-4552
Марценко Сергій Володимирович, PhD, доцент
https://orcid.org/0000-0003-2205-0204
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ ІТ СЕРЕДОВИЩ

Бідюк О.В., Марценко С.В. Дослідження методів та засобів інформаційної безпеки хмарних ІТ середовищ. У статті проведено аналіз основних засобів для побудови захисту хмарних ІТ середовищ, на основі загроз та вразливостей, характерних для хмарних технологій, таких як несанкціонований доступ, витік даних, атаки на рівні додатків та інфраструктури. До основних напрямків дослідження методів захисту хмарних ІТ інфраструктур відносяться: шифрування даних, багатофакторна аутентифікація, управління доступом, моніторинг та аудит безпеки, мережева безпека та безпека додатків. Враховуючи сучасні тенденції розвитку технологій інформаційної безпеки, в контексті зростаючої популярності хмарних рішень, розкрито питання ролі провайдерів хмарних послуг у забезпеченні безпеки та їх відповідальність. Наведено рекомендації щодо вибору та впровадження ефективних засобів захисту для різних типів хмарних середовищ, зокрема приватних, публічних та гібридних хмар. Окремим напрямком дослідження виділено використання підходів автоматизації до розгортання та керування хмарною інфраструктурою. Засоби автоматизації дають можливість з допомогою підходу Infrastructure as a code (IaC), сформувати опис інфраструктури у форматі коду, таким чином забезпечити збереження резервних копій елементів хмарної ІТ інфраструктури і швидкого її розгортання. Інтеграція елементів Continuous Integration/Continuous Delivery (CI/CD) до даного підходу дозволяє виконувати тестування елементів інфраструктури перед розгортанням чи внесення нової конфігурації, а також перевіряти відповідність їх політикам інформаційної безпеки.
Ключові слова: інформаційна безпека, хмара, аутентифікація, мережева безпека, управління доступом, багатофакторна аутентифікація.

Bidiuk O., Martsenko S. Methods and tools of the information security IT cloud infrastructure. The article analyses the main tools for building protection for cloud IT environments, based on threats and vulnerabilities typical for cloud technologies, such as unauthorized access, data leakage, attacks at the application and infrastructure levels. The main areas of research into methods for protecting cloud IT infrastructures include data encryption, multi-factor authentication, access management, security monitoring and auditing, network security and application security. Based on current trends in the development of information security technologies, in the context of the growing popularity of cloud solutions, the issue of the role of cloud service providers in ensuring security and their responsibility is revealed. Recommendations are given for the selection and implementation of effective protection tools for different types of cloud environments, in particular private, public and hybrid clouds. A separate area of research is the use of automation approaches to deploying and managing cloud infrastructure. Automation tools make it possible, using the Infrastructure as a code (IaC) approach, to form a description of the infrastructure in code format, thus ensuring the preservation of backup copies of cloud IT infrastructure elements and its rapid deployment. The integration of Continuous Integration/Continuous Delivery (CI/CD) elements into this approach allows testing of infrastructure elements before deployment or introduction of a new configuration, as well as checking their compliance with information security policies.
Keywords: information security, cloud, authentication, network security, access control, multi-factor authentication.

Постановка проблеми

У сучасному світі хмарні ІТ середовища стають все більш популярними завдяки своїй гнучкості, масштабованості та економічній ефективності. Однак, разом із зростанням використання хмарних технологій, виникає значна кількість проблем, пов'язаних із інформаційною безпекою. Основні загрози включають несанкціонований доступ до даних, витік конфіденційної інформації, атаки на рівні додатків та інфраструктури, а також внутрішні загрози від користувачів або адміністраторів [1]. Враховуючи критичність даних, що зберігаються у хмарі, та потенційні наслідки їх компрометації, питання інформаційної безпеки набуває особливої актуальності.

У роботі пропонується провести:

- дослідження сучасних методів та засобів інформаційної безпеки (ІБ) хмарних ІТ середовищ, в тому числі з використанням підходів автоматизації розгортання та керування хмарною ІТ інфраструктурою;
- аналіз ризиків ІБ та методи підвищення її рівня для додатків та компонентів хмарних технологій [2].

Розв'язання проблеми інформаційної безпеки хмарних ІТ середовищ має вагоме значення як для наукових досліджень, так і для практичної реалізації. Наукові завдання включають розробку нових алгоритмів шифрування, методів аутентифікації та авторизації, а також моделей

прогнозування загроз [3]. Практичні завдання зосереджені на впровадженні ефективних засобів захисту, таких як багатофакторна аутентифікація, управління доступом, моніторинг та аудит безпеки, мережева безпека. Крім того, важливою є роль провайдерів хмарних послуг у побудові комплексної безпеки, що вимагає від них постійного оновлення та вдосконалення захисних механізмів. Вирішення цих завдань сприятиме підвищенню довіри користувачів до хмарних технологій та забезпеченню їх безперебійної роботи, що є ключовим фактором для успішного розвитку цифрової економіки та зростання інноваційних технологій.

Аналіз останніх досліджень і публікацій

Хмарні провайдери надають сервіси для побудови IT інфраструктури, які складають собою комплексне рішення, що базується на вимогах інформаційної безпеки. Хмара працює на серверах у центрах обробки даних, які представлені для клієнта чи користувача платформою з набором підготовлених та налаштованих IT сервісів [4]. Здатність швидко надавати, налаштовувати та захищати ресурси за допомогою хмарних провайдерів стала ключем до надзвичайного успіху та складності сучасних підходів DevOps та Serverless.

Хмарна інфраструктура складається з одного або більше віртуальних приватних сегментів (Virtual Private Cloud), які представлені трьома основними архітектурними компонентами, що зображені на рисунку 1.:

1. Обчислювальний компонент (Compute).
2. Мережевий компонент (Networking).
3. Компонент зберігання даних Storage.

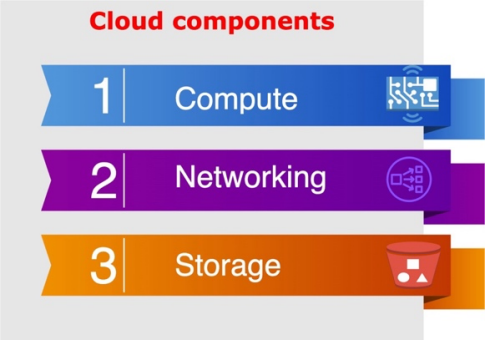

Рис. 1. Компоненти хмарної IT інфраструктури

Обчислювальний компонент являє собою набір ресурсів та сервісів, які забезпечують виконання програм і обробку даних. Віртуалізація є ключовою технологією, яка розділяє фізичні ресурси на кілька віртуальних екземплярів, забезпечуючи гнучкість і ефективність використання [5].

Контейнери, як гнучкі середовища виконання, забезпечують швидке розгортання та ізоляцію додатків, що є важливим для сучасних DevOps практик. Хмарні провайдери пропонують різноманітні Compute сервіси, від IaaS (інфраструктура як послуга) до PaaS (платформа як послуга), що дозволяє користувачам вибирати оптимальні рішення для своїх завдань. Автоматизація управління обчислювальними ресурсами є критичною для забезпечення безперебійної роботи та швидкого масштабування [6]. Балансування навантаження і оркестрація ресурсів допомагають оптимізувати використання Compute потужностей, забезпечуючи високу доступність і продуктивність.

Також Compute сервіси, дають можливість використання підходу побудови інфраструктури, який називається сервери без сервера (Serverless) [7]. Даний підхід дозволяє виконувати код без необхідності управління серверною інфраструктурою чи контейнерами. Compute сервіс відіграє одну з основних ролей у підтримці різноманітних бізнес-процесів і технологічних інновацій, забезпечуючи ефективне управління і обробку даних [8].

Мережевий компонент (Networking) забезпечує з'єднання і передачу даних між різними обчислювальними ресурсами та користувачами. Сервіс складається з віртуальних мереж, маршрутизації, балансування навантаження і управління трафіком та надає можливість організовувати комунікацію в хмарі. Віртуальні приватні мережі (VPN) надають безпечний доступ до хмарних ресурсів через зашифровані канали, що є критичним для захисту даних [9].

Балансування навантаження розподіляє вхідний трафік між кількома серверами, оптимізуючи продуктивність і забезпечуючи високу доступність додатків. Служби доменних імен (DNS) в хмарі управляють розв'язанням імен в IP-адреси, полегшуючи доступ до ресурсів.

Автоматизація мережевих процесів, включаючи конфігурацію і моніторинг, дозволяє швидко адаптуватися до змін у навантаженні та вимогах. Безпека мережі в хмарі охоплює захист від DDoS-атак, контроль доступу і шифрування даних, та є важливими для запобігання несанкціонованому доступу. Інтеграція мережевих сервісів з іншими компонентами хмарної інфраструктури, такими як Compute і Storage, забезпечує комплексне управління і взаємодію.

Отже, сервіс Networking, надає можливість швидкої і надійної передачі даних між різними інфраструктурними компонентами хмарної інфраструктури, що забезпечує їх безперебійну роботу [10,11].

Компонент зберігання даних Storage виконує функцію зберігання даних у різних форматах і обсягах, підтримуючи доступність і масштабованість, що включає об'єктне, блокове та файлове зберігання, кожне з яких має свої специфічні застосування і переваги. Об'єктне зберігання забезпечує розміщення великих обсягів даних у вигляді об'єктів. Блокове зберігання надає низьку затримку і високу продуктивність, що підходить для баз даних і додатків, які вимагають швидкого доступу до даних[12]. Файлове зберігання являє собою сервіс для організації спільного доступу до файлів через мережу, що робить його корисним для спільної роботи і зберігання даних додатків.

Хмарні провайдери також надають автоматизовані рішення для резервного копіювання та відновлення даних, забезпечуючи захист від втрат і пошкоджень. Масштабованість хмарного зберігання дозволяє легко збільшувати або зменшувати обсяги зберігання відповідно до потреб бізнесу, без необхідності інвестувати в фізичне обладнання. Безпека зберігання даних включає шифрування, контроль доступу і аудит, що є критичними для захисту конфіденційної інформації [13].

На рисунку 2, зображена загальна схема хмарної IT інфраструктури на прикладі Amazon Web Service (AWS).

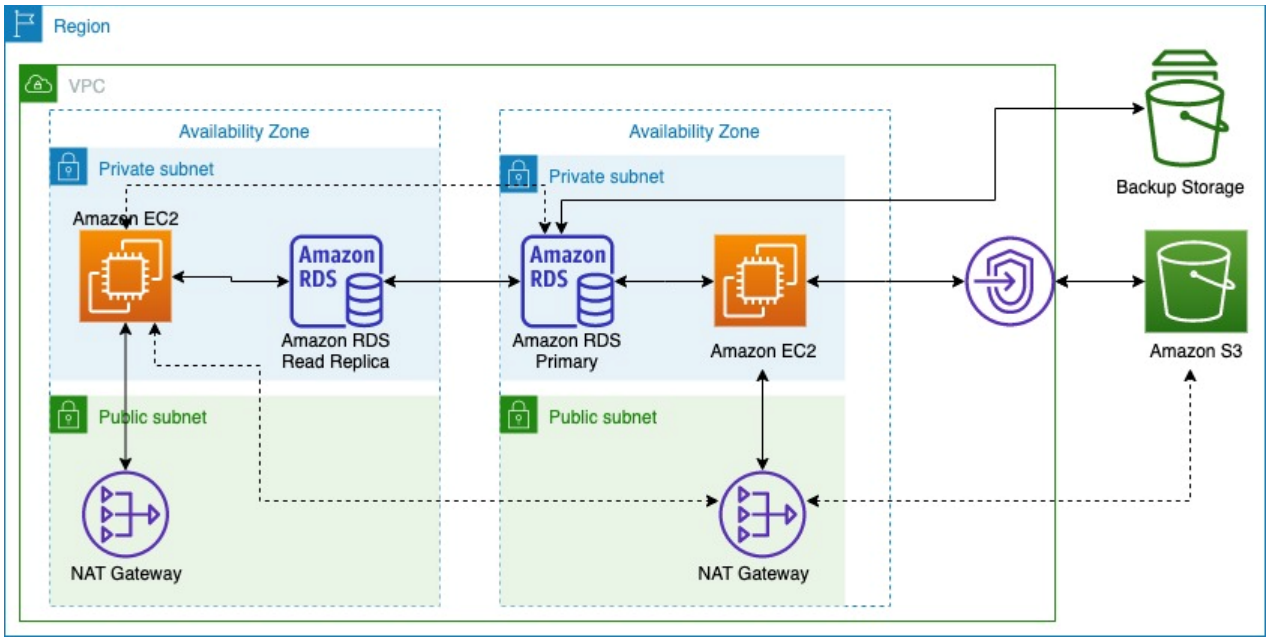

Рис. 2. Загальна схема хмарної IT інфраструктури [14]

До Compute компонентів належать Amazon EC2 та Amazon RDS, що являють собою відповідно, віртуальні сервери та бази даних. NAT Gateway відноситься до компоненту Networking. Storage компонент представлений у вигляді Amazon S3 та Backup Storage.

Проаналізувавши властивості та функції компонентів хмарної IT інфраструктури, можемо узагальнити, що активний розвиток і різноманітність хмарних технологій та компонентів забезпечує гнучкість, масштабованість і ефективне управління ресурсами, дозволяючи організаціям зосередитися на своїх бізнес-завданнях [15.16].

Використання підходів автоматизації до розгортання та керування хмарною IT інфраструктурою є важливим аспектом сучасних технологій, що дозволяє підвищити ефективність, гнучкість та надійність управління ресурсами. Дані підходи включають в себе використання засобів та методів, які автоматизують процеси розгортання, конфігурації, моніторингу та масштабування хмарних сервісів [17].

Проведено аналіз підходів до автоматизації хмарної IT інфраструктури [18]. Використання інструментів інфраструктури як коду (IaC) дозволяє описувати та керувати інфраструктурою через програмний код, забезпечуючи можливість автоматизованого розгортання та управління ресурсами в хмарі. Розглянемо застосування підходу IaC на прикладі інтеграції інструментів Terraform та Ansible, що зображені на рисунку 3.

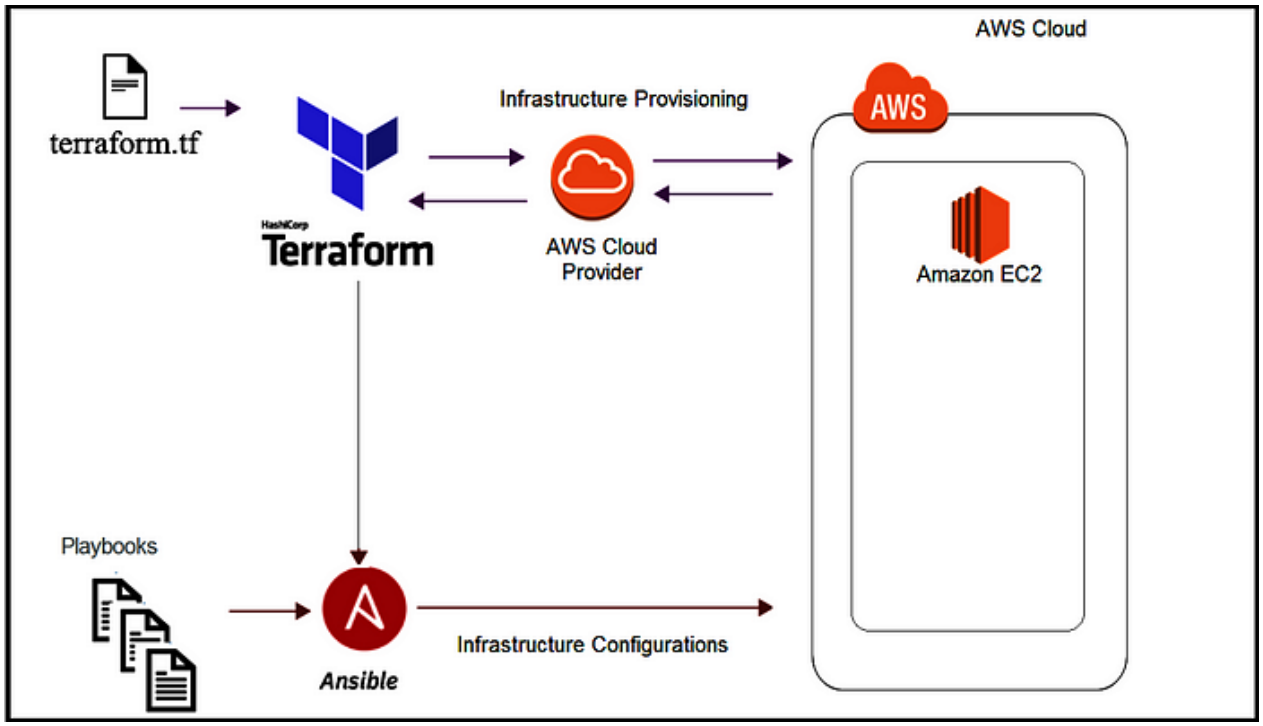

Рис. 3. Схема інтеграції інструментів IaC [19]

Terraform — це інструмент для управління інфраструктурою як кодом (IaC), розроблений компанією HashiCorp. Він дозволяє користувачам описувати компоненти IT інфраструктури у вигляді конфігураційних файлів, що робить процес розгортання, зміни та управління ресурсами автоматизованим та контрольованими [20].

Основною перевагою Terraform є його здатність працювати не тільки з хмарними провайдерами, а також з локальними рішеннями, що забезпечує універсальність і гнучкість. Конфігурації в Terraform пишуться на власній декларативній мові — HashiCorp Configuration Language (HCL), яка зрозуміла і легка для читання. Даний інструмент використовує концепцію планування та дає змогу користувачам переглядати зміни перед їх застосуванням, тим самим зменшуючи ризик помилок [21]. Terraform також підтримує стан (state) інфраструктури, зберігаючи інформацію про поточний стан ресурсів та відстежує зміни в IT інфраструктурі. Використання модулів в Terraform забезпечує повторне використання конфігурації, що спрощує управління великими проектами. Інтеграція з системами контролю версій, такими як Git, сприяє кращому управлінню змінами та співпраці в команді.

Ansible — це інструмент для автоматизації управління конфігураціями, розгортання додатків та оркестрації IT інфраструктури. Розроблений компанією Red Hat, Ansible відомий своєю простотою у використанні та відсутністю потреби в агентській архітектурі. Він використовує засоби віддаленого підключення для управління вузлами і не потребує встановлювати додаткове програмне забезпечення на віддалених машинах [22].

Конфігурації в Ansible описуються за допомогою YAML у вигляді плейбуків, які визначають необхідні стани системи. Плейбуки містять завдання, що виконуються послідовно, дозволяючи

адміністраторам описувати складні процеси налаштування в зрозумілому форматі. Ansible також використовує ролі, які забезпечують організацію плейбуків та інших ресурсів для повторного використання та кращої структури прожекту [23].

Ansible інтегрується з іншими DevOps інструментами, такими як Jenkins, Docker і Kubernetes, що робить його частиною комплексних рішень для автоматизації. Завдяки своїй простоті, потужності та гнучкості, Ansible є популярним вибором для організацій, які прагнуть швидко автоматизувати управління своєю IT-інфраструктурою без складнощів, пов'язаних з агентськими системами [24].

Використання цих інструментів Terraform та Ansible надає можливість створити, налаштувати компоненти хмарної IT інфраструктури з допомогою коду та налаштувати додатки та сервіси всередині цих компонентів з використанням елементів автоматизації та контролю конфігурації.

Автоматизація хмарної IT інфраструктури також включає оркестрацію контейнерів за допомогою платформ, таких як Kubernetes, та забезпечує управління життєвим циклом контейнерів та їх масштабування. Однією з основних властивостей даної платформи є створення Serverless архітектури, що в поєднанні з використанням хмарної інфраструктури робить її більш гнучкою і масштабованою. На рисунку 4 зображено схему інфраструктура на прикладі Kubernetes, яка дуже швидко адаптується відповідно до задач і цілей її застосування.

Використання CI/CD (безперервної інтеграції та безперервного розгортання) дозволяє автоматизувати процеси розробки, тестування та розгортання додатків, а також швидкого впровадження змін. Моніторинг та логування автоматизованих процесів допомагають виявляти проблеми та оптимізувати продуктивність.

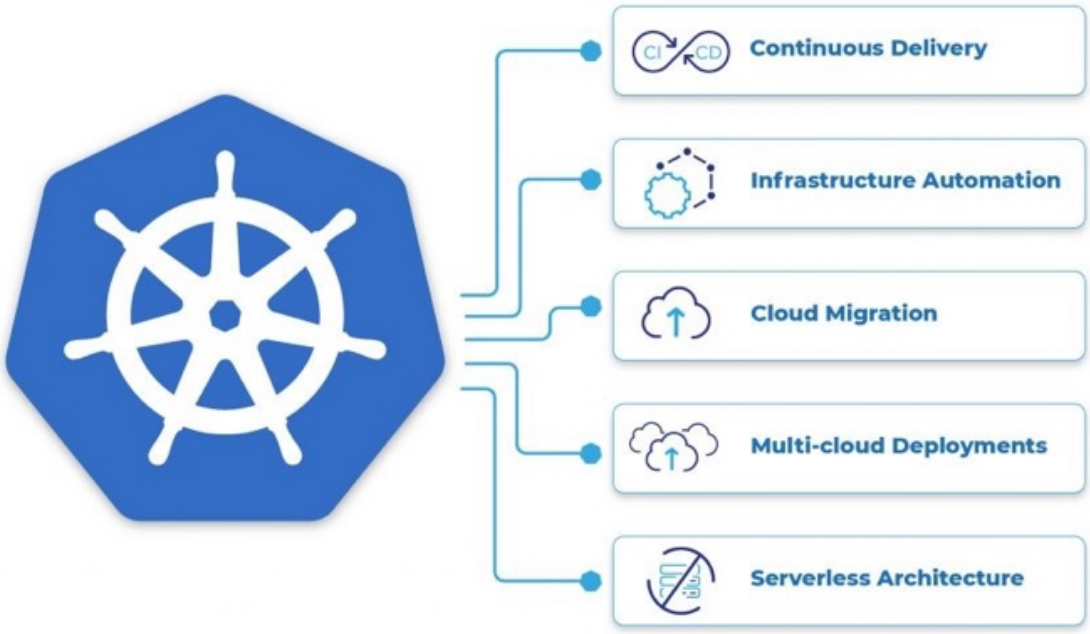

Рис. 4. Схема застосування Kubernetes [25]

Підхід автоматизації управління знижує ризики людських помилок, підвищує швидкість реагування на зміни та забезпечує високу доступність сервісів. Важливим аспектом є безпека автоматизованих процесів, включаючи контроль доступу, шифрування даних, виявлення вразливого коду і помилок в конфігурації [26,27].

Мета і завдання дослідження

Метою роботи є дослідження методів та засобів інформаційної безпеки, які використовуються в хмарних IT середовищах, з метою визначення їх ефективності та виявлення можливих шляхів вдосконалення. Це включає аналіз існуючих методів захисту даних, оцінку їх відповідності сучасним загрозам, а також розробку рекомендацій для оптимізації безпекових стратегій у хмарних системах. Додатково, робота спрямована на вивчення ролі провайдерів хмарних послуг у побудові інформаційної безпеки та визначення їх відповідальності. Зрештою, мета полягає

у сприянні підвищенню рівня безпеки хмарних технологій, що дозволить зміцнити довіру користувачів і забезпечити захист критичних даних у цифровій економіці.

Виклад основного матеріалу

Розміщення IT інфраструктури в хмарі та використання підходів автоматизації приносить значні переваги, проте також супроводжується ризиками інформаційної безпеки [28,29]. Одним з основних ризиків є несанкціонований доступ до даних, що стається через недостатньо захищені облікові записи або вразливості в системах аутентифікації. Витік даних також становить серйозну загрозу, особливо якщо конфіденційні дані не шифруються належним чином.

Крім того, внутрішні загрози, що походять від співробітників або адміністраторів, найчастіше спричинені ненавмисними помилками або зловмисними діями. Дотримання нормативних вимог, таких як General Data Protection Regulation (GDPR) або Health Insurance Portability and Accountability Act (HIPAA), є складним завданням, особливо якщо дані розміщуються в хмарах, що знаходяться в різних юрисдикціях [30]. Відсутність прозорості з боку провайдерів хмарних послуг ускладнює оцінку ризиків та впровадження адекватних заходів безпеки. Уразливість до DDoS-атак може призвести до недоступності сервісів, що негативно вплине на бізнес-операції [31].

Інциденти, пов'язані з безпекою, завдають шкоди репутації організації та призводять до фінансових втрат. Зрештою, важливо розробити комплексну стратегію управління ризиками, яка включає регулярний аудит безпеки, навчання персоналу та впровадження сучасних технологій захисту для мінімізації потенційних загроз [32,33]. Хмарні провайдери надають досить різноманітний перелік сервісів для керування та підвищення інформаційної безпеки. Основною перевагою є те, що в даному випадку клієнти використовують дані інструменти у вигляді безпека як сервіс (Security as a Service). Тобто керування, налаштування, оновлення компонентів, які забезпечують роботу даних сервісів є обов'язком хмарного провайдера, а користувач використовує лише наданий інтерфейс [34,35].

Провівши аналіз ризиків інформаційної безпеки у напрямку автоматизації хмарної IT інфраструктури, виділяєм один з ключових, а саме, можливість помилок у конфігураційних скриптах або шаблонах, які можуть призвести до вразливостей у системі [36]. Автоматизація спрощує процес розгортання, але якщо не забезпечити належний контроль доступу, це може відкрити шлях для несанкціонованих змін або доступу до критичних ресурсів [34,37].

Засоби автоматизації часто зберігають конфіденційні дані, такі як ключі доступу та паролі, що робить їх потенційними цілями для атак. Відсутність регулярного моніторингу та аудиту автоматизованих процесів може дозволити атакам залишатися непоміченими, збільшуючи ризик компрометації системи. Залежність від сторонніх бібліотек та модулів у автоматизаційних скриптах може призвести до впровадження вразливостей, якщо ці компоненти не оновлюються регулярно [38,39]. Інциденти безпеки виникають через недостатню перевірку змін, що вносяться в інфраструктуру, особливо в динамічних середовищах, де зміни відбуваються часто.

Важливою є проблема конфіденційності даних, особливо якщо автоматизація включає переміщення даних між різними середовищами або хмарами. Відсутність належного навчання персоналу щодо безпечного використання засобів автоматизації призводить до людських помилок, які створюють нові ризики. Зрештою, для мінімізації ризиків необхідно впроваджувати комплексні стратегії безпеки, що інтегруються в CI/CD процеси, які включають різні перевірки логіки програмного коду, розміщення чутливої інформації, а також відповідність встановленим нормам політикам інформаційної безпеки [40,41].

Для мінімізації ризиків потрібно використати комплексний підхід, який являє собою оптимальне використання сервісів інформаційної безпеки, що надають хмарні провайдери, а також інтеграції інформаційної безпеки в процеси CI/CD для перевірки та сканування коду, який використовується у IaC підході для побудови IT інфраструктури.

Актуальним підходом для побудови інформаційної безпеки хмарної IT інфраструктури є безпека як сервіс. Він включає в себе набір нативних (native) інструментів, що надає хмарний провайдер у вигляді готових рішень, а також систем які інтегруються і працюють на обчислюваних (Compute) ресурсах хмарної IT інфраструктури [42.43].

Проаналізувавши ризики ІБ хмарної інфраструктури, виділяємо основні, з найвищим пріоритетом. Мінімізація ризиків, наведених в таблиці 1, дозволить отримати базовий рівень інформаційної безпеки IT інфраструктури в хмарному середовищі:

Таблиця 1 – Ризики інформаційної безпеки хмарних IT інфраструктур

№	Ризик	Опис ризику	Імовірність	Пріоритет	Заходи пом'якшення
1	Несанкціонований доступ	Потенційний доступ зловмисників до хмарних ресурсів	Висока	Високий	Впровадження MFA, контроль доступу, аудит
2	Витік конфіденційних даних	Витік або крадіжка даних через неправильні налаштування	Висока	Високий	Шифрування даних, політики доступу, моніторинг
3	Відмова сервісу (DDoS атаки)	Перевантаження сервісів, що призводить до простою	Середня	Високий	Використання захисту від DDoS, масштабування
4	Помилки конфігурації	Неправильні налаштування безпеки або мережі	Висока	Високий	Автоматизовані перевірки

Провівши дослідження сервісів інструменти безпеки, що надаються хмарними провайдерами, можемо виділити три основні:

- Сервіси керування доступом (Identity Access Management, IAM) надають можливість використання і гнучкого налаштування процесів аутентифікації та авторизації [44]. Наприклад, використання сучасних протоколів аутентифікації, таких як SSO, SAML, oAuth, а також двухфакторної аутентифікації для користувачів. Процес авторизації побудований на основі підходу нульової довіри (Zero Trust), тобто по замовчуванні будь який доступ заблокований [45]. Політики доступу описують застосування лише дозволених операції, а правила заборони, по замовчувані, мають найвищий пріоритет. На рисунку 5 наведено приклад написання IAM політики в AWS хмарі, що описує права доступу на читання та записи об'єкту сервісу зберігання даних S3:

```
{
  "Version": "2025-02-17",
  "Statement": [
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::bucket-name"]
    },
    {
      "Sid": "AllObjectActions",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": ["arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Рис.5 Приклад IAM політики доступу до сервісу зберігання даних S3 [46]

- Сервіси мережевого доступу (Network Security Groups and Access Lists, SG and NACL) являють собою інструменти файєрволінгу, що надають можливість налаштування обмеження мережевого доступу на основі IP адрес та TCP/UDP портів [47]. Наприклад, AWS

провайдер надає можливість використання сервісів мережевої безпеки SG та NACL, з підтримкою stateless та stateful файєрволінгу, на рівні підмережі або мережевого інтерфейсу. На рисунку 6 представлено архітектурну схему застосування NACL та SG в AWS хмарі:

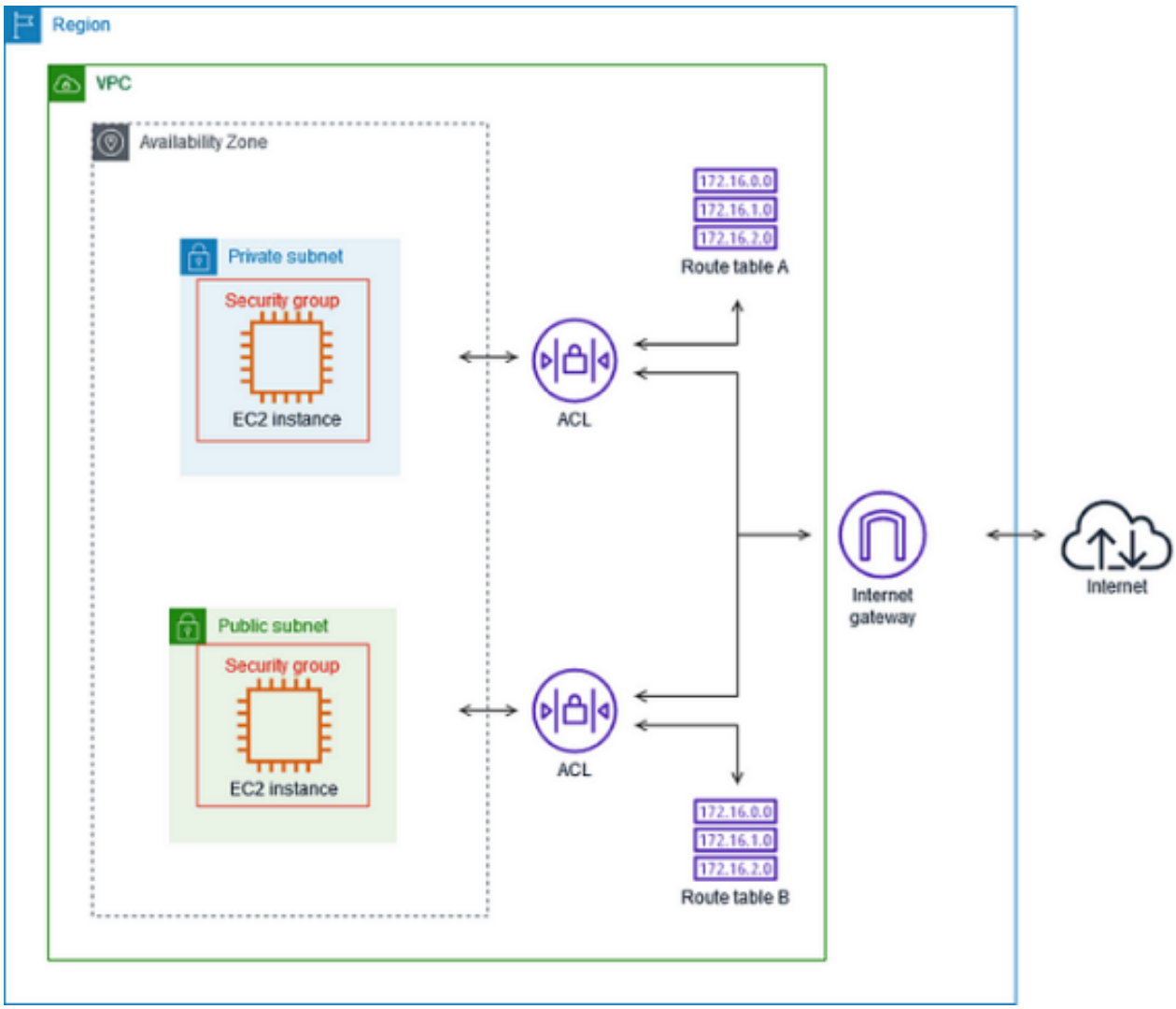

Рис 6. Архітектурна схема використання SG та NACL в AWS хмарі [48]

- Сервіс логування, аудиту і моніторингу змін (Cloud Trails and Logs) використовується для відстежування дії користувачів та сервісів в рамках віртуальної приватної інфраструктури. Також в конфігурації даного сервісу застосовуються метрики, які описують алгоритм створення ідентифікатора аномальної події [49]. На рисунку 7 зображені основні блоки, з яких складається сервіс AWS CloudTrail:

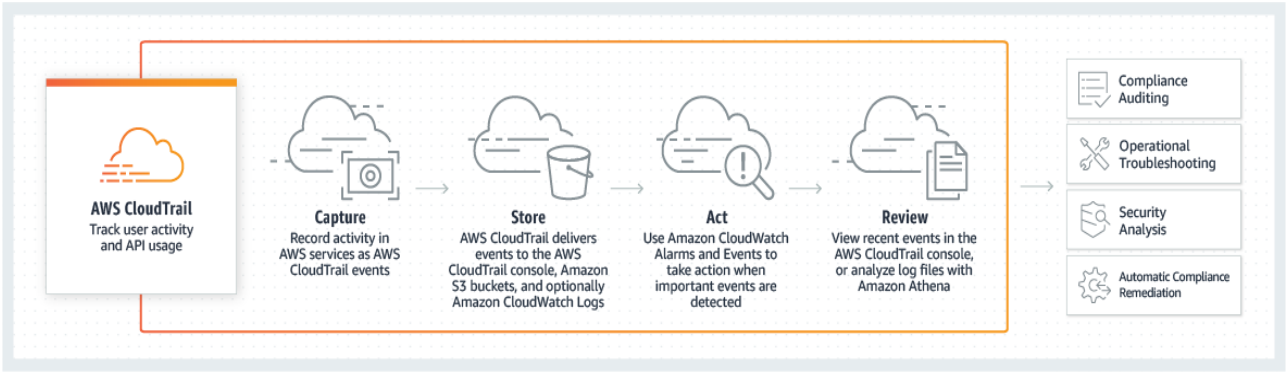

Рис 7. AWS CloudTrail архітектура [50]

Налаштувавши перелічені сервіси можна отримати базовий рівень інформаційної безпеки приватної віртуальної інфраструктури та мінімізувати ризики інформаційної безпеки, що характерні хмарним IT інфраструктурам. Тобто за допомогою політик IAM описати правила доступу до ресурсів і компонентів інфраструктури, а також безпечне підключення до консолі хмарного середовища [51]. Мережеві сервіси дозволять обмежити периметр інформаційної безпеки, а також мережеву взаємодію всередині віртуальної інфраструктури. А сервіси аудиту і моніторингу забезпечать видимість інфраструктури, для швидкої реакції на аномалії в конфігурації та інформаційній безпеці, що можуть призвести до інциденту інформаційної безпеки [52].

Ефективність проаналізованих сервісів інформаційної безпеки досягається через їхню багаторівневу інтеграцію один з одним, що повністю відповідає моделі ешелонованої оборони (Defense in Dept).

Застосувавши дану модель на практиці для організації захисту критичного ресурсу, що містить веб сервіс для шифрованої передачі конфіденційної інформації користувачів, ми отримаємо трьохрівневу архітектуру інформаційної безпеки хмарної інфраструктури, кожен рівень якої також складається з декількох підрівнів.

1. Рівень превентивного логічного захисту. Даний рівень побудований на основі хмарного сервісу інформаційної безпеки IAM. Доступ до об'єктів сховища та обчислювальних ресурсів реалізується з використанням моделі «нульової довіри» (Zero Trust). Надання прав доступу відбувається на основі IAM-ролі, а не для конкретного користувача:

- створюється політика, яка дозволяє лише операції читання та запису виключно для конкретного сервера додатків.
- всі інші дії кваліфікуються як несанкціонований доступ, оскільки будь-який інший елемент системи за замовчуванням не має прав на взаємодію з даними.

2. Рівень мережевої ізоляції. Мережевий трафік обмежується на рівні підмереж та конкретних елементів обчислювальних ресурсів. Це мінімізує «поверхню атаки» та запобігає розповсюдженню загрози всередині хмари у разі компрометації одного з елементів.. Тому якщо зловмисник отримає доступ до ідентифікатора IAM ролі він отримає обмеження, які передбачені мережевим захистом:

- на рівні підмережі (NACL) блокується весь трафік, крім портів, необхідних для роботи додатка.
- на рівні конкретного сервера, наприклад веб сервісу, встановлюється правило (SG), що дозволяє вхідні з'єднання (наприклад, порт 443) лише від IP-адреси сервера додатків.

3. Рівень детективного контролю та аудиту (CloudTrail). Останній етап, що забезпечує прозорість та можливість реагування на інциденти, пов'язані з внутрішніми загрозами або помилками автоматизації.

- кожен виклик API, що стосується зміни мережевих правил або доступу до даних, автоматично фіксується сервісом AWS CloudTrail.
- система виконує повний цикл, від фіксації події (Capture) до автоматичного сповіщення адміністраторів або активації сценаріїв блокування (Act). Це дозволяє також дотримуватися нормативних вимог, таких як GDPR або HIPAA, забезпечуючи доказову базу для аудиту.

На рисунку 8 зображена схема роботи базового сервісу веб додатків з використанням трьохрвіневої моделі компонентів захисту хмарної IT інфраструктури:

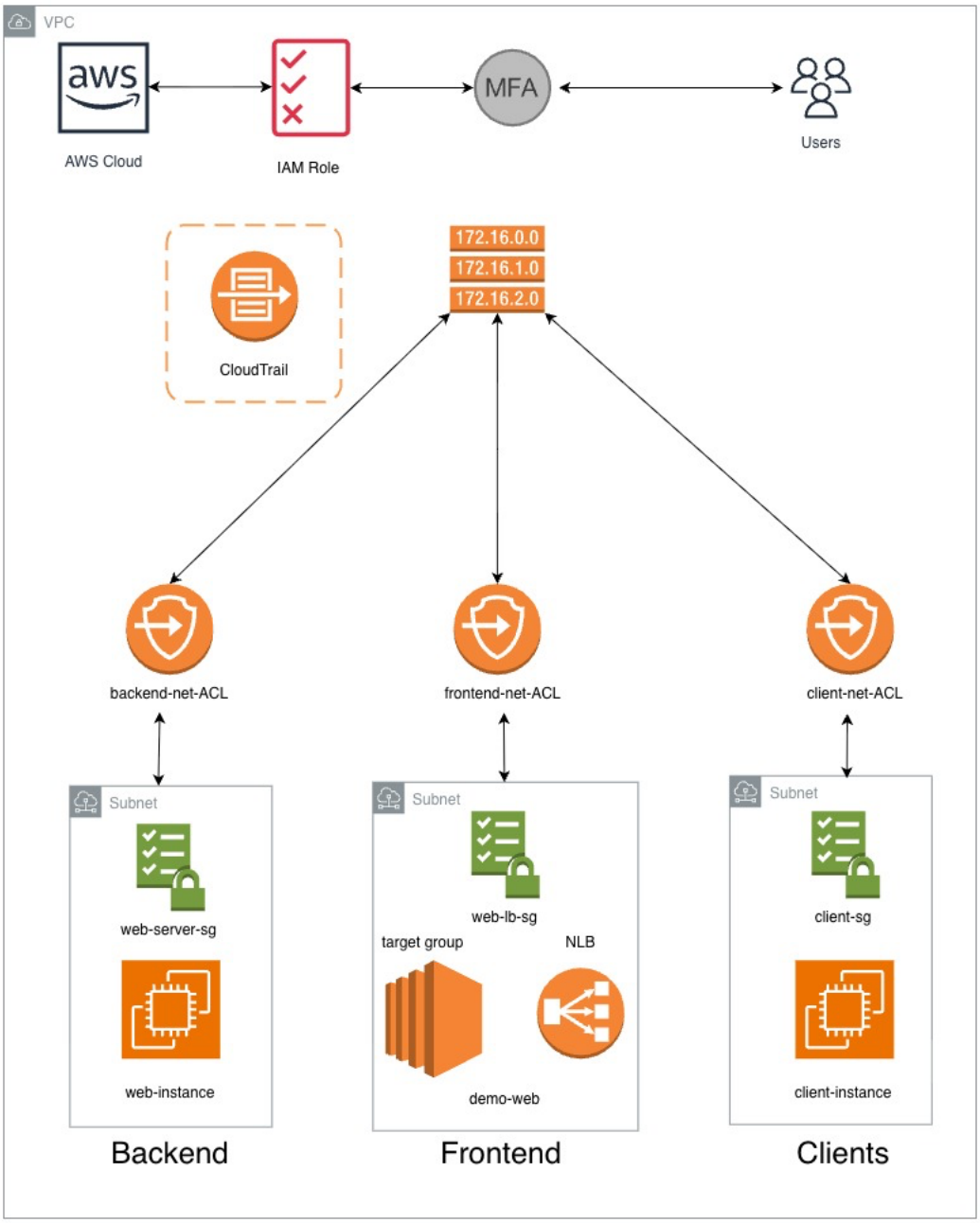

Рис 8. Схема роботи веб сервісу з використанням елементів захисту трьохрівневої архітектури інформаційної безпеки

Поєднання цих трьох сервісів у межах CI/CD процесів дозволяє створити динамічне середовище, де безпека є невід'ємною частиною інфраструктури, що автоматично перевіряється та масштабується разом із бізнес-завданнями. Інтеграція сервісів один з одним забезпечують комплексний підхід до інформаційної безпеки в хмарі AWS. [53].

Висновки та перспективи подальших досліджень. За результатами проведеного аналізу і дослідження можем зробити висновок, що хмарні технології, хоча й надають значні переваги в гнучкості та масштабованості, супроводжуються численними викликами в галузі безпеки. Основні загрози включають несанкціонований доступ, витік даних, атаки на рівні додатків та інфраструктури. Ефективне використання засобів безпеки, описаних в дослідженні, є критично важливим для захисту даних та хмарної IT інфраструктури. Важливою є роль провайдерів хмарних послуг, які повинні надавати високий рівень безпеки та прозорість своїх процесів.

Подальші дослідження можуть бути зосереджені на розробці нових методів виявлення та запобігання загрозам, використовуючи штучний інтелект та машинне навчання. Інтеграція засобів безпеки з платформами автоматизації, оркестрації та контейнеризації може підвищити ефективність

управління безпекою в хмарних середовищах. Детальне дослідження даних питань сприяють створенню екосистеми, де автоматизовані процеси стають нормою, що значно підвищує ефективність і інноваційність у сфері IT.

Список бібліографічного опису

1. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing Cloud Security Alliance. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ (дата звернення: 10.01.2026)
2. Turner, H.; Scott, P. Identity and Access Management in Cloud Computing. Computers & Security. 2022. P. 121. URL: https://doi.org/10.1016/j.cose.2022.102830 (дата звернення: 10.01.2026)
3. Bhardwaj, A.; Goundar, S.; Singh, A.K.; Sharma, S.K. Cloud computing: A study of emerging security issues and solutions. J. King Saud Univ. Computer and Information Sciences. 2022. 34. URL: https://doi.org/10.1016/j.jksuci.2021.07.008 (дата звернення: 10.01.2026)
4. NIST. Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/sp/800-144/final (дата звернення: 10.01.2026).
5. Cloud computing with AWS Amazon AWS. URL: https://aws.amazon.com/what-is-aws (дата звернення: 11.01.2026).
6. AWS Support Automation Workflows (SAW) Amazon AWS. URL: https://aws.amazon.com/premiumsupport/technology/saw/ (дата звернення: 11.01.2026).
7. Campbell, S.; Perez, L. Implementing Zero Trust Architecture in Cloud Systems. Computers & Security. 2023. 122. URL: https://doi.org/10.1016/j.cose.2022.102901(дата звернення: 11.01.2026)
8. CIS. CIS Benchmarks for Cloud Security Center for Internet Security. URL: https://www.cisecurity.org/cis-benchmarks/ (дата звернення:: 11.01.2026).
9. Cisco Cloud Security Solutions Cisco. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/cloud-security-solutions.html (дата звернення: 12.01.2026).
10. AWS Security Documentation Amazon AWS URL: https://docs.aws.amazon.com/security/ (дата звернення: 12.01.2026).
11. Azure Security Center Microsoft Azure. URL: https://azure.microsoft.com/en-us/services/security-center/ (дата звернення: 12.01.2026).
12. Liu, W.; Zhao, Y.; Zhang, X.; Chen, D. A Survey on Security Isolation of Cloud Computing. IEEE Access 2020. 8. URL: https://doi.org/10.1109/ACCESS.2020.2982823 дата звернення: 12.01.2026).
13. OWASP. Cloud-Native Application Security Top 10 OWASP Foundation. URL: https://owasp.org/www-project-cloud-native-application-security-top-10/ (дата звернення:: 12.01.2026).
14. Journey to Cloud-Native Architecture Series #6: Improve cost visibility and re-architect for cost optimization. Amazon AWS. URL: https://aws.amazon.com/blogs/architecture/journey-to-cloud-native-architecture-series-6-improve-cost-visibility-and-re-architect-for-cost-optimization/ (дата звернення: 12.01.2026).
15. AWS Security Overview Amazon AWS. URL: https://aws.amazon.com/security/overview/ (дата звернення: 12.01.2026).
16 Google Cloud Security Solutions Google Cloud. URL: https://cloud.google.com/security/solutions (дата звернення: 12.01.2026).
17. Carter, B.; Adams, R. Securing Cloud APIs: Methods and Best Practices. J. Inf. Secur. Appl. 2023, 65. URL: https://doi.org/10.1016/j.jisa.2022.103117 (дата звернення: 12.01.2026).
18. HashiCorp. Terraform Security Best Practices HashiCorp Developer. URL: https://developer.hashicorp.com/terraform/tutorials/security (дата звернення:: 12.01.2026).
19. The Most Simplified Integration of Ansible and Terraform Medium. URL: https://medium.com/geekculture/the-most-simplified-integration-of-ansible-and-terraform-49f130b9fc8 (дата звернення: 15.01.2026).
20. Infrastructure as code Wikipedia. URL: https://en.wikipedia.org/wiki/Infrastructure_as_code (дата звернення: 15.01.2026).
21. What is infrastructure as code? Microsoft. URL: https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code - (дата звернення: 17.01.2026).
22. Infrastructure as Code: базові принципи vs інструменти, що еволюціонують. DOU.UA URL: https://dou.ua/lenta/articles/infrastructure-as-code/ (дата звернення: 17.01.2026).
23. Calico service mesh. Tigera. URL: https://www.tigera.io/project-calico/ (дата звернення: 18.01.2026).
24. G. Budigiri, C. Baumann, J. T. Mühlberg, E. Truyen, and W. Joosen, "Network policies in kubernetes: Performance evaluation and security analysis," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit). 2021. 407–412. URL: https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482436 (дата звернення: 18.01.2026).
25. Why use Kubernetes for your enterprise? Nearsource. URL: https://nearsource.ca/why-use-kubernetes-for-your-enterprise/ (дата звернення: 18.01.2026).
26. Red Hat. Understanding Kubernetes Security Red Hat. URL: https://www.redhat.com/en/topics/containers/kubernetes-security (дата звернення:: 19.01.2026).
27. CNCF. Cloud Native Security Whitepaper Cloud Native Computing Foundation. URL: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/v2-whitepaper.md (дата звернення:: 19.01.2026).
28. Patel, R.; Singh, T. Access Control Mechanisms for Cloud Computing: A Survey. Journal of Information Security and Applications 2022. 64. URL: https://doi.org/10.1016/j.jisa.2021.103046 (дата звернення:: 19.01.2026).
29. Oracle. Oracle Cloud Infrastructure Security Guide Oracle Help Center. URL: https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm (дата звернення:: 21.01.2026).

30. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2021. 12. URL: https://doi.org/10.1186/2192-113X-2-5 (дата звернення:: 21.01.2026).
31. Liu, W.; Zhao, Y.; Zhang, X.; Chen, D. A Survey on Security Isolation of Cloud Computing. IEEE Access 2020. 8. URL: https://doi.org/10.1109/ACCESS.2020.2982823 (дата звернення:: 21.01.2026).
32. Docker. Docker Security Best Practices Docker Documentation. URL: https://docs.docker.com/develop/security-best-practices/ (дата звернення:: 21.01.2026).
33. Carter, B.; Adams, R. Securing Cloud APIs: Methods and Best Practices. Journal of Information Security and Applications. 2023. 65. URL: https://doi.org/10.1016/j.jisa.2022.103117 (дата звернення:: 21.01.2026).
34. Snyk. 10 Best Practices for Cloud Security Snyk Blog. URL: https://snyk.io/blog/cloud-security-best-practices/ (дата звернення:: 21.01.2026).
35. Palo Alto Networks. What is Cloud Security Posture Management (CSPM)? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-cspm (дата звернення:: 22.01.2026).
36. Check Point. Cloud Security Best Practices for 2026 Check Point Software. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/cloud-security-best-practices/ (дата звернення:: 23.01.2026).
37. Sharma, S.; Chen, X.; Sheth, P. Toward Privacy Preserving Data Sharing for Cloud Computing: A Survey. Computer Communications. 2021. 10–29. URL: https://doi.org/10.1016/j.comcom.2021.04.020 (дата звернення:: 23.01.2026).
38. Datadog. State of Cloud Security Report Datadog. URL: https://www.datadoghq.com/state-of-cloud-security/ (дата звернення:: 25.01.2026).
39. CrowdStrike. Comprehensive Guide to Cloud Security CrowdStrike. URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/ (дата звернення:: 25.01.2026).
40. Gartner. Top Strategic Technology Trends: Cloud Security Gartner. URL: https://www.gartner.com/en/information-technology/topics/cloud-security (дата звернення:: 27.01.2026).
41. GitLab. DevSecOps: Security at the speed of DevOps GitLab. URL: https://about.gitlab.com/topics/devsecops/ (дата звернення:: 27.01.2026).
42. AWS Security Best Practices Amazon AWS. URL: https://aws.amazon.com/security/best-practices/ (дата звернення: 28.01.2026).
43. Microsoft Azure Security Documentation Microsoft Azure. URL: https://docs.microsoft.com/en-us/azure/security/ (дата звернення: 28.01.2026).
44. Google Cloud Security Tools Google Cloud. URL: https://cloud.google.com/security/tools (дата звернення: 29.01.2026).
45. IBM Cloud Security Guide IBM Cloud. URL: https://www.ibm.com/cloud/security-guide (дата звернення: 29.01.2026).
46. Grant read and write access to Amazon S3 bucket objects. Amazon AWS. URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html (дата звернення: 30.01.2026).
47. Google Cloud Security Architecture Google Cloud. URL: https://cloud.google.com/security/architecture (дата звернення: 30.01.2026).
48. AWS — Difference between Security Groups and Network Access Control List (NACL) Medium. URL: https://medium.com/awesome-cloud/aws-difference-between-security-groups-and-network-acls-adc632ea29ae (дата звернення: 31.01.2026).
49. AWS Security Tools Amazon AWS. URL: https://aws.amazon.com/security/tools/ (дата звернення: 01.02.2026).
50. AWS Cloudtrail Roi4cio. URL: https://roi4cio.com/catalog/product/amazon-cloudtrail (дата звернення: 02.02.2026).
51. Trend Micro Cloud Security Architecture Trend Micro. URL: https://www.trendmicro.com/en_us/business/cloud-security/architecture.html (дата звернення: 28.10.2025).
52. Microsoft Azure Security Tools Microsoft Azure. URL: https://azure.microsoft.com/en-us/tools/security/ (дата звернення: 03.02.2026).
53. Google Cloud Security Best Practices Google Cloud. URL: https://cloud.google.com/security/best-practices (дата звернення: 03.02.2026).

References:

1. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing Cloud Security Alliance. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ (date of access: 10.01.2026).
2. Turner, H.; Scott, P. Identity and Access Management in Cloud Computing. Computers & Security. 2022. P. 121. URL: https://doi.org/10.1016/j.cose.2022.102830 (date of access: 10.01.2026).
3. Bhardwaj, A.; Goundar, S.; Singh, A.K.; Sharma, S.K. Cloud computing: A study of emerging security issues and solutions. J. King Saud Univ. Computer and Information Sciences. 2022. 34. URL: https://doi.org/10.1016/j.jksuci.2021.07.008 (date of access: 10.01.2026).
4. NIST. Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/sp/800-144/final (date of access: : 10.01.2026).
5. Cloud computing with AWS Amazon AWS. URL: https://aws.amazon.com/what-is-aws (date of access: 11.01.2026).
6. AWS Support Automation Workflows (SAW) Amazon AWS. URL: https://aws.amazon.com/premiumsupport/technology/saw/ (date of access: 11.01.2026).
7. Campbell, S.; Perez, L. Implementing Zero Trust Architecture in Cloud Systems. Computers & Security. 2023. 122. URL: https://doi.org/10.1016/j.cose.2022.102901 (date of access: 11.01.2026).

8. CIS. CIS Benchmarks for Cloud Security Center for Internet Security. URL: https://www.cisecurity.org/cis-benchmarks/ (date of access: : 11.01.2026).
9. Cisco Cloud Security Solutions Cisco. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/cloud-security-solutions.html (date of access: 12.01.2026).
10. AWS Security Documentation Amazon AWS URL: https://docs.aws.amazon.com/security/ (date of access: 12.01.2026).
11. Azure Security Center Microsoft Azure. URL: https://azure.microsoft.com/en-us/services/security-center/ (date of access: 12.01.2026).
12. Liu, W.; Zhao, Y.; Zhang, X.; Chen, D. A Survey on Security Isolation of Cloud Computing. IEEE Access 2020. 8. URL: https://doi.org/10.1109/ACCESS.2020.2982823 (date of access: 12.01.2026).
13. OWASP. Cloud-Native Application Security Top 10 OWASP Foundation. URL: https://owasp.org/www-project-cloud-native-application-security-top-10/ (date of access: : 12.01.2026).
14. Journey to Cloud-Native Architecture Series #6: Improve cost visibility and re-architect for cost optimization. Amazon AWS. URL: https://aws.amazon.com/blogs/architecture/journey-to-cloud-native-architecture-series-6-improve-cost-visibility-and-re-architect-for-cost-optimization/ (date of access: 12.01.2026).
15. AWS Security Overview Amazon AWS. URL: https://aws.amazon.com/security/overview/ (date of access: 12.01.2026).
16 Google Cloud Security Solutions Google Cloud. URL: https://cloud.google.com/security/solutions (date of access: 12.01.2026).
17. Carter, B.; Adams, R. Securing Cloud APIs: Methods and Best Practices. J. Inf. Secur. Appl. 2023, 65. URL: https://doi.org/10.1016/j.jisa.2022.103117 (date of access: 12.01.2026).
18. HashiCorp. Terraform Security Best Practices HashiCorp Developer. URL: https://developer.hashicorp.com/terraform/tutorials/security (date of access: : 12.01.2026).
19. The Most Simplified Integration of Ansible and Terraform Medium. URL: https://medium.com/geekculture/the-most-simplified-integration-of-ansible-and-terraform-49f130b9fc8 (date of access: 15.01.2026).
20. Infrastructure as code Wikipedia. URL: https://en.wikipedia.org/wiki/Infrastructure_as_code - (date of access: 15.01.2026).
21. What is infrastructure as code? Microsoft. URL: https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code - (date of access: 17.01.2026).
22. Infrastructure as Code: базові принципи vs інструменти, що еволюціонують. DOU.UA URL: https://dou.ua/lenta/articles/infrastructure-as-code/ (date of access: 17.01.2026).
23. Calico service mesh. Tigera. URL: https://www.tigera.io/project-calico/ (date of access: 18.01.2026).
24. G. Budigiri, C. Baumann, J. T. Mühlberg, E. Truyen, and W. Joosen, "Network policies in kubernetes: Performance evaluation and security analysis," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit). 2021. 407–412. URL: https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482436 (date of access: 18.01.2026).
25. Why use Kubernetes for your enterprise? Nearsource. URL: https://nearsource.ca/why-use-kubernetes-for-your-enterprise/ - (date of access: 18.01.2026).
26. Red Hat. Understanding Kubernetes Security Red Hat. URL: https://www.redhat.com/en/topics/containers/kubernetes-security (date of access: : 19.01.2026).
27. CNCF. Cloud Native Security Whitepaper Cloud Native Computing Foundation. URL: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/v2-whitepaper.md (date of access: : 19.01.2026).
28. Patel, R.; Singh, T. Access Control Mechanisms for Cloud Computing: A Survey. Journal of Information Security and Applications 2022. 64. URL: https://doi.org/10.1016/j.jisa.2021.103046 (date of access: : 19.01.2026).
29. Oracle. Oracle Cloud Infrastructure Security Guide Oracle Help Center. URL: https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm (date of access: : 21.01.2026).
30. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2021. 12. URL: https://doi.org/10.1186/2192-113X-2-5 (date of access: : 19.01.2026).
31. Liu, W.; Zhao, Y.; Zhang, X.; Chen, D. A Survey on Security Isolation of Cloud Computing. IEEE Access 2020. 8. URL: https://doi.org/10.1109/ACCESS.2020.2982823 (date of access: : 19.01.2026).
32. Docker. Docker Security Best Practices Docker Documentation. URL: https://docs.docker.com/develop/security-best-practices/ (date of access: 21.01.2026).
33. Carter, B.; Adams, R. Securing Cloud APIs: Methods and Best Practices. Journal of Information Security and Applications. 2023. 65. URL: https://doi.org/10.1016/j.jisa.2022.103117 (date of access: : 19.01.2026).
34. Snyk. 10 Best Practices for Cloud Security Snyk Blog. URL: https://snyk.io/blog/cloud-security-best-practices/ (date of access:: 21.01.2026).
35. Palo Alto Networks. What is Cloud Security Posture Management (CSPM)? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-cspm (date of access: 22.01.2026).
36. Check Point. Cloud Security Best Practices for 2026 Check Point Software. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/cloud-security-best-practices/ (date of access: 23.01.2026).
37. Sharma, S.; Chen, X.; Sheth, P. Toward Privacy Preserving Data Sharing for Cloud Computing: A Survey. Computer Communications. 2021. 10–29. URL: https://doi.org/10.1016/j.comcom.2021.04.020 (date of access: 23.01.2026).
38. Datadog. State of Cloud Security Report Datadog. URL: https://www.datadoghq.com/state-of-cloud-security/ (date of access: 25.01.2026).
39. CrowdStrike. Comprehensive Guide to Cloud Security CrowdStrike. URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/ (date of access: 25.01.2026).

40. Gartner. Top Strategic Technology Trends: Cloud Security Gartner. URL: https://www.gartner.com/en/information-technology/topics/cloud-security (date of access: 27.01.2026).
41. GitLab. DevSecOps: Security at the speed of DevOps GitLab. URL: https://about.gitlab.com/topics/devsecops/ (date of access: 27.01.2026).
42. AWS Security Best Practices Amazon AWS. URL: https://aws.amazon.com/security/best-practices/ - (date of access: 28.01.2026).
43. Microsoft Azure Security Documentation Microsoft Azure. URL: https://docs.microsoft.com/en-us/azure/security/ (date of access: 28.01.2026).
44. Google Cloud Security Tools Google Cloud. URL: https://cloud.google.com/security/tools (date of access: 29.01.2026).
45. IBM Cloud Security Guide IBM Cloud. URL: https://www.ibm.com/cloud/security-guide (date of access: 29.01.2026).
46. Grant read and write access to Amazon S3 bucket objects. Amazon AWS. URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html (date of access: 30.01.2026).
47. Google Cloud Security Architecture Google Cloud. URL: https://cloud.google.com/security/architecture (date of access: 30.01.2026).
48. AWS — Difference between Security Groups and Network Access Control List (NACL) Medium. URL: https://medium.com/awesome-cloud/aws-difference-between-security-groups-and-network-acls-adc632ea29ae (date of access: 31.01.2026).
49. AWS Security Tools Amazon AWS. URL: https://aws.amazon.com/security/tools/ (date of access: 01.02.2026).
50. AWS Cloudtrail Roi4cio. URL: https://roi4cio.com/catalog/product/amazon-cloudtrail - (date of access: 02.02.2026).
51. Trend Micro Cloud Security Architecture Trend Micro. URL: https://www.trendmicro.com/en_us/business/cloud-security/architecture.html (date of access: 28.10.2025).
52. Microsoft Azure Security Tools Microsoft Azure. URL: https://azure.microsoft.com/en-us/tools/security/ (date of access: 03.02.2026).
53. Google Cloud Security Best Practices Google Cloud. URL: https://cloud.google.com/security/best-practices (date of access: 03.02.2026).

Історія статті:
Отримано: 20.02.2026 Доопрацьовано: 13.03.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026