МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ: СУЧАСНІ ВЕКТОРИ АТАК ТА ЗАСОБИ ЗАХИСТУ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микита ЛУГІН
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач вищої освіти гр. УБД-41

Микита Лугін

Керівник: Володимир ШУЛЬГА
д-р істор. наук ,
професор

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лугіну Микиті Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Безпека хмарних технологій у корпоративному середовищі: сучасні вектори атак та засоби захисту”,
керівник кваліфікаційної роботи Легомінова Світлана, д-р екон. наук., професор,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління персоналом з інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Дослідити теоретичні основи безпеки корпоративних хмарних середовищ.
   4.2. Розглянути моделі хмарних сервісів і модель спільної відповідальності.
   4.3. Дослідити атаки, пов’язані з управлінням доступом, обліковими записами та надмірними привілеями.
   4.4 Запропонувати технічні та організаційні заходи захисту корпоративної хмари.
   4.5 Розробити комплексну модель захисту корпоративного хмарного середовища.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз сучасних векторів атак на корпоративні хмарні середовища.	08.04.2026	
4.	Дослідження особливостей захисту корпоративних хмарних середовищ та моделей управління доступом.	15.04.2026	
5.	Вивчення засобів захисту хмарної інфраструктури, зокрема IAM, Zero Trust, CSPM, SIEM/SOAR та механізмів моніторингу.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ДЕК.	__.06.2026	

Здобувач вищої освіти _____ Микита ЛУГІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Лугін М.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Безпека хмарних технологій у корпоративному середовищі: сучасні вектори атак та засоби захисту ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЛУГІН Микита у кваліфікаційній роботі проаналізував особливості забезпечення безпеки хмарних технологій у корпоративному середовищі, дослідив сучасні вектори атак на хмарну інфраструктуру, розглянув ризики, пов’язані з управлінням доступом, обліковими записами, надмірними привілеями, API-ключами та недостатнім журналюванням, а також запропонував практичні засоби підвищення рівня захищеності корпоративної хмари.

ЛУГІН Микита показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового аналізу, продемонстрував уміння систематизувати матеріал, робити обґрунтовані висновки та формулювати практичні рекомендації. Під час виконання кваліфікаційної роботи здобувач проявив себе як організований, відповідальний і самостійний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЛУГІНА Микити на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Лугін Микита допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувач вищої освіти ЛУГІНА Микити

на тему “Безпека хмарних технологій у корпоративному середовищі: сучасні вектори атак та засоби захисту ”

Актуальність. Корпоративні інформаційні системи дедалі активніше використовують хмарні технології для зберігання даних, організації віддаленої роботи, розгортання сервісів та забезпечення безперервності бізнес-процесів. Разом із цим зростає кількість кіберзагроз, пов’язаних із компрометацією облікових записів, помилками конфігурації, надмірними привілеями, вразливостями API, витоком даних та недостатнім контролем доступу. Особливої уваги потребує захист корпоративного хмарного середовища, оскільки порушення його безпеки може призвести до втрати конфіденційної інформації, фінансових збитків і порушення стабільної роботи організації.

Позитивні сторони.

1. У роботі досліджено теоретичні основи хмарних технологій, моделі їх розгортання та обслуговування, а також особливості забезпечення безпеки корпоративного хмарного середовища.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено послідовно, відповідно до структури дослідження, сформульовано логічні висновки. Основні положення роботи доповнено таблицями, рисунками та схемами, що підвищує наочність поданого матеріалу.
3. Автор опрацював достатню джерельну базу, зокрема наукові публікації, стандарти, аналітичні матеріали та джерела, пов’язані з питаннями хмарної безпеки, управління доступом, Zero Trust та захисту корпоративної інфраструктури.
4. У роботі проаналізовано актуальні вектори атак на корпоративні хмарні середовища, зокрема атаки, пов’язані з обліковими записами, надмірними привілеями, API-ключами, сервісними акаунтами, недостатнім журналюванням і помилками конфігурації.
5. За результатами дослідження запропоновано практичні рекомендації щодо підвищення рівня захищеності корпоративної хмари, зокрема через удосконалення управління доступом, застосування багатофакторної автентифікації, принципу найменших привілеїв, моніторингу подій безпеки та підходу Zero Trust.

Недоліки.

Доцільно було б приділити більше уваги порівнянню конкретних інструментів хмарної безпеки, зокрема рішень класу CSPM, SIEM, IAM та засобів моніторингу активності користувачів у різних хмарних платформах. Також роботу можна було б посилити ширшим аналізом практичних сценаріїв реагування на інциденти у хмарному середовищі.

Однак вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні, відповідає вимогам до бакалаврських кваліфікаційних робіт і заслуговує оцінки “відмінно”, а здобувач вищої освіти ЛУГІН Микита заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

Д-р.техн.наук, професор _____ *підпис* Олександр ТУРОВСЬКИЙ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню безпеки хмарних технологій у корпоративному середовищі, аналізу сучасних векторів атак на хмарну інфраструктуру та обґрунтуванню ефективних засобів захисту. Робота складається зі вступу, трьох розділів, що містять 23 рисунки, висновківі списку використаних джерел із 30 найменувань. Загальний обсяг роботи становить 84 сторінок, з яких 5 сторінок займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження сучасних векторів атак на хмарні технології у корпоративному середовищі та обґрунтування ефективних засобів їх захисту з урахуванням особливостей хмарної інфраструктури.

Об'єктом дослідження є процес забезпечення безпеки хмарних технологій у корпоративному середовищі.

Предметом дослідження є сучасні вектори атак на корпоративні хмарні середовища, а також підходи, методи, засоби до їх виявлення, запобігання та мінімізації наслідків.

Методи дослідження. Для досягнення поставленої мети в роботі використано системний підхід, методи аналізу та синтезу, порівняння, класифікації, узагальнення, а також методи оцінювання ризиків інформаційної безпеки. Застосування цих методів дозволило дослідити архітектурні особливості хмарних технологій, проаналізувати актуальні загрози для корпоративних хмарних середовищ і визначити доцільні технічні та організаційні механізми захисту.

У роботі досліджено теоретичні основи безпеки корпоративних хмарних середовищ, розглянуто моделі хмарних сервісів і модель спільної відповідальності між хмарним провайдером та організацією-користувачем. Проаналізовано сучасні вектори атак на корпоративну хмару, зокрема атаки, пов'язані з управлінням доступом, компрометацією облікових записів, API-ключами, сервісними ідентичностями, надмірними привілеями та помилками конфігурації хмарних ресурсів.

У практичній частині роботи обґрунтовано засоби захисту корпоративного хмарного середовища, зокрема IAM, MFA, RBAC, ABAC, принцип найменших привілеїв, моніторинг доступу, журналювання подій, аудит конфігурацій, CSPM-рішення, policy-as-code, реагування на інциденти та впровадження принципів Zero Trust. На основі проведеного аналізу запропоновано інтегровану модель захисту корпоративної хмари, яка поєднує превентивні, детекційні та реактивні заходи.

Галузь застосування. Результати роботи можуть бути використані під час планування, побудови та вдосконалення системи захисту корпоративної хмарної інфраструктури, розроблення політик інформаційної безпеки, управління доступом, оцінювання ризиків, контролю конфігурацій і впровадження організаційно-технічних заходів захисту у хмарному середовищі.

Ключові слова: ХМАРНІ ТЕХНОЛОГІЇ, КОРПОРАТИВНЕ СЕРЕДОВИЩЕ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ВЕКТОРИ АТАК, МОДЕЛЬ СПІЛЬНОЇ ВІДПОВІДАЛЬНОСТІ, ZERO TRUST, IAM, MFA, CSPM, УПРАВЛІННЯ ДОСТУПОМ, ПОМИЛКИ КОНФІГУРАЦІЇ, ХМАРНА ІНФРАСТРУКТУРА, ЗАСОБИ ЗАХИСТУ.

ABSTRACT

The qualification work is devoted to the study of cloud technology security in a corporate environment, the analysis of modern attack vectors targeting cloud infrastructure, and the substantiation of effective protection measures. The work consists of an introduction, three chapters containing 23 figures, conclusions and the list of references containing 30 items. The total volume of the work is 84 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the work is to study modern attack vectors on cloud technologies in the corporate environment and to substantiate effective means of their protection, taking into account the features of the cloud infrastructure.

The object of the study is the process of ensuring the security of cloud technologies in the corporate environment.

The subject of the study is modern attack vectors on corporate cloud environments, as well as approaches, methods, means for their detection, prevention and minimization of consequences.

Research methods. To achieve the set goal, the work used a systemic approach, methods of analysis and synthesis, comparison, classification, generalization, as well as methods for assessing information security risks. The application of these methods allowed to study the architectural features of cloud technologies, analyze current threats to corporate cloud environments and determine appropriate technical and organizational protection mechanisms.

As a result, the work examines the theoretical foundations of corporate cloud environment security, cloud service models and the shared responsibility model between a cloud provider and a client organization. The study analyzes modern attack vectors against corporate cloud environments, including attacks related to access management, account compromise, API keys, service identities, excessive privileges and cloud resource misconfigurations. The work also substantiates the use of protection measures such as IAM, MFA, RBAC, ABAC, the principle of least privilege, access monitoring, event logging, configuration auditing, CSPM solutions, policy-as-code, incident response and Zero Trust principles.

Field of application. The developed approaches can be used in the planning, implementation and improvement of corporate cloud infrastructure protection systems, as well as in the development of information security policies, access management, risk assessment, configuration control and the implementation of organizational and technical security measures in cloud environments.

Keywords: CLOUD TECHNOLOGIES, CORPORATE ENVIRONMENT, INFORMATION SECURITY, CYBERSECURITY, ATTACK VECTORS, SHARED RESPONSIBILITY MODEL, ZERO TRUST, IAM, MFA, CSPM, ACCESS MANAGEMENT, MISCONFIGURATION, CLOUD INFRASTRUCTURE, SECURITY MEASURES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ABAC — Attribute-Based Access Control, контроль доступу на основі атрибутів.

API — Application Programming Interface, інтерфейс програмування застосунків.

CIA — Confidentiality, Integrity, Availability; конфіденційність, цілісність і доступність інформації.

CSPM — Cloud Security Posture Management, управління станом безпеки хмарного середовища.

FaaS — Function as a Service, функція як сервіс.

IAM — Identity and Access Management, управління ідентичностями та доступом.

IaaS — Infrastructure as a Service, інфраструктура як сервіс.

MFA — Multi-Factor Authentication, багатофакторна автентифікація.

PaaS — Platform as a Service, платформа як сервіс.

RBAC — Role-Based Access Control, контроль доступу на основі ролей.

SaaS — Software as a Service, програмне забезпечення як сервіс.

SIEM — Security Information and Event Management, система управління інформацією та подіями безпеки.

SOAR — Security Orchestration, Automation and Response, оркестрація, автоматизація та реагування на інциденти безпеки.

Zero Trust — концепція безпеки, що передбачає відмову від автоматичної довіри та постійну перевірку кожного запиту доступу.

ІБ — інформаційна безпека.

ІТ — інформаційні технології.

ПЗ — програмне забезпечення.

ВСТУП

Актуальність теми. У сучасних умовах хмарні технології стали одним із ключових інструментів цифрової трансформації підприємств. Корпоративні організації активно використовують хмарні сервіси для зберігання даних, розгортання інформаційних систем, забезпечення віддаленої роботи працівників, резервного копіювання, обробки великих обсягів інформації та підтримки бізнес-процесів. Такий підхід дає змогу підвищити гнучкість IT-інфраструктури, зменшити витрати на її обслуговування та швидше масштабувати ресурси відповідно до потреб організації.

Водночас активне використання хмарних технологій супроводжується зростанням кількості ризиків і загроз інформаційній безпеці. Корпоративне хмарне середовище не має чітко визначеного фізичного периметра, а доступ до ресурсів може здійснюватися з різних пристроїв, мереж і географічних локацій. У таких умовах традиційні підходи до захисту, орієнтовані лише на внутрішню мережу або окремі технічні засоби, не забезпечують достатнього рівня безпеки.

Особливу небезпеку для корпоративної хмари становлять атаки, пов’язані з компрометацією облікових записів, надмірними привілеями, викраденням API-ключів, неконтрольованими сервісними акаунтами, помилками конфігурації ресурсів і недостатнім журналюванням подій. У багатьох випадках зловмиснику не потрібно атакувати інфраструктуру хмарного провайдера безпосередньо. Достатньо використати слабке місце на стороні самої організації: неправильно налаштоване сховище, відкритий службовий інтерфейс, відсутність багатофакторної автентифікації або активний обліковий запис, який уже не повинен використовуватися.

Актуальність теми також зумовлена особливостями моделі спільної відповідальності в хмарному середовищі. Хмарний провайдер забезпечує захист базової інфраструктури, фізичних дата-центрів і окремих вбудованих механізмів безпеки, однак організація-користувач залишається відповідальною за власні дані, облікові записи, ролі, політики доступу, конфігурації ресурсів і моніторинг подій. Неправильне розуміння цього розподілу може призвести до критичних

інцидентів, зокрема витоку даних, несанкціонованої зміни конфігурацій, втрати доступності сервісів або ускладнення розслідування інцидентів.

З огляду на це дослідження сучасних векторів атак на хмарні технології у корпоративному середовищі та засобів їх захисту є актуальним науково-практичним завданням. Воно має значення для організацій, які використовують хмарні сервіси, впроваджують гібридні або мультихмарні архітектури, працюють із великими обсягами корпоративних даних і потребують системного підходу до управління ризиками інформаційної безпеки.

Метою роботи є дослідження сучасних векторів атак на хмарні технології у корпоративному середовищі та обґрунтування ефективних засобів їх захисту з урахуванням особливостей хмарної інфраструктури.

Об'єктом дослідження є процес забезпечення безпеки хмарних технологій у корпоративному середовищі.

Предметом дослідження є сучасні вектори атак на корпоративні хмарні середовища, а також підходи, методи, засоби до їх виявлення, запобігання та мінімізації наслідків.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. дослідити сутність та особливості корпоративного хмарного середовища;
2. розглянути основні моделі хмарних сервісів і визначити їхній вплив на розподіл відповідальності за безпеку між хмарним провайдером і організацією-користувачем;
3. проаналізувати основні принципи захисту корпоративної хмари та концепцію Zero Trust;
4. дослідити сучасні загрози корпоративним хмарним середовищам;
5. проаналізувати атаки, пов'язані з управлінням доступом, обліковими записами, API-ключами, сервісними акаунтами та надмірними привілеями;
6. проаналізувати атаки, спричинені помилками конфігурації хмарних ресурсів;
7. обґрунтувати технічні та організаційні засоби захисту

корпоративного хмарного середовища;

8. розробити інтегровану модель захисту корпоративного хмарного середовища.

Методи дослідження. У роботі використано методи аналізу та синтезу, порівняння, класифікації, узагальнення, системного підходу, а також методи оцінювання ризиків інформаційної безпеки. Метод аналізу застосовано для дослідження хмарних моделей, загроз і засобів захисту. Метод порівняння використано для зіставлення моделей хмарних сервісів і розподілу відповідальності між провайдером та організацією. Метод класифікації дав змогу систематизувати вектори атак і засоби захисту. Системний підхід використано для побудови інтегрованої моделі захисту корпоративного хмарного середовища.

Практичне значення одержаних результатів. полягає в тому, що запропоновані підходи можуть бути використані під час розроблення та вдосконалення системи захисту корпоративної хмарної інфраструктури. Результати роботи можуть застосовуватися для формування політик управління доступом, впровадження багатофакторної автентифікації, контролю привілеїв, аудиту конфігурацій, моніторингу подій безпеки, використання CSPM-рішень і побудови захисту на основі принципів Zero Trust.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ КОРПОРАТИВНИХ ХМАРНИХ СЕРЕДОВИЩ

1.1 Поняття та особливості корпоративного хмарного середовища

Хмарні технології слід розглядати не лише як окремі сервіси для зберігання даних або запуску застосунків, а як комплексну систему обчислювальних ресурсів, моделей доступу, способів розгортання та засобів адміністрування, що забезпечують функціонування корпоративної IT-інфраструктури.

Хмарні обчислення доцільно розглядати як спосіб організації IT-ресурсів, за якого сервери, сховища, бази даних, програмні сервіси та інші компоненти надаються організації через мережу. У такій моделі компанія може використовувати необхідні обчислювальні потужності без повного розгортання й самостійного обслуговування власної фізичної інфраструктури [1]. У корпоративному середовищі така модель використовується для підтримки бізнес-процесів, організації віддаленої роботи, розміщення інформаційних систем, резервного копіювання та централізованого керування доступом.

Хмарні технології мають кілька характерних особливостей, серед яких:

- віддалений доступ до ресурсів через мережу;
- можливість швидкого масштабування обчислювальних потужностей;
- використання ресурсів хмарного провайдера;
- гнучке розгортання сервісів і застосунків;
- залежність безпеки від правильності налаштувань і політик доступу;
- розподіл відповідальності між провайдером і організацією-користувачем [1].

Основні поняття, пов’язані з корпоративними хмарними середовищами, можна класифікувати на кілька категорій:

1) Загальні поняття хмарних технологій.
2) Моделі розгортання хмарного середовища.
3) Поняття, пов’язані з управлінням доступом і безпекою.

Загальні поняття хмарних технологій. До цієї категорії належать базові терміни, які характеризують сутність хмарного середовища та його роль у корпоративній інфраструктурі.

Хмарне середовище — це організований набір обчислювальних ресурсів, сервісів, мережевих компонентів, облікових записів і політик доступу, які спільно забезпечують зберігання, обробку, передавання та захист даних у межах хмарної інфраструктури.

Корпоративне хмарне середовище — це частина IT-інфраструктури організації, у якій хмарні ресурси використовуються для роботи бізнес-сервісів, розміщення застосунків, зберігання службової інформації, керування користувачами та організації доступу до корпоративних систем.

Хмарний сервіс — це функціональна послуга, яку провайдер надає через мережу для виконання певних IT-завдань, зокрема зберігання даних, запуску застосунків, обробки інформації, резервного копіювання, моніторингу або адміністрування ресурсів.

Хмарний провайдер — це постачальник хмарних послуг, який забезпечує роботу дата-центрів, серверного обладнання, мережевої інфраструктури та базових сервісів, а також надає організаціям доступ до інфраструктурних, платформних або програмних ресурсів [1, 6].

Моделі розгортання хмарного середовища. Ця категорія відображає, яким способом організація може розміщувати та використовувати хмарні ресурси.

Публічна хмара — це модель розгортання, у якій інфраструктура належить зовнішньому провайдеру, а її ресурси надаються через Інтернет багатьом незалежним клієнтам.

Приватна хмара — модель, за якої хмарна інфраструктура призначена для потреб однієї організації та може розміщуватися як у власному середовищі компанії, так і на ресурсах зовнішнього постачальника.

Гібридна хмара — підхід, за якого локальна або приватна інфраструктура поєднується з публічними хмарними сервісами, що дає змогу розміщувати дані

й застосунки в різних середовищах залежно від вимог безпеки, продуктивності та доступності.

Мультихмарне середовище — це спосіб побудови хмарної інфраструктури, за якого організація використовує сервіси кількох провайдерів одночасно, щоб підвищити гнучкість, зменшити залежність від одного постачальника та оптимізувати розміщення ресурсів [1, 6].

Поняття, пов'язані з управлінням доступом і безпекою. Ця категорія є особливо важливою для теми дослідження, оскільки більшість сучасних загроз корпоративній хмарі пов'язана з обліковими записами, правами доступу, конфігураціями та моніторингом.

IAM — система керування цифровими ідентичностями та правами доступу, яка визначає, які користувачі, групи, застосунки або сервісні облікові записи можуть взаємодіяти з хмарними ресурсами та які операції їм дозволено виконувати.

MFA — це механізм посиленої автентифікації, за якого для підтвердження особи користувача використовується не лише пароль, а й додатковий фактор, наприклад одноразовий код, мобільний застосунок, апаратний ключ або біометрична перевірка.

API-ключ — це спеціальний ідентифікатор або токен доступу, за допомогою якого застосунок, сервіс чи автоматизований процес підтверджує право взаємодіяти з хмарним API або окремими ресурсами провайдера.

Сервісний обліковий запис — це технічна ідентичність, призначена не для звичайного користувача, а для застосунку, скрипта, інтеграції або автоматизованого процесу, який повинен виконувати дії в хмарному середовищі.

Zero Trust — це підхід до організації безпеки, за якого доступ до ресурсу не надається автоматично лише через факт перебування користувача або пристрою в корпоративному середовищі. Кожен запит має перевірятися окремо з урахуванням ідентичності, стану пристрою, місця підключення, ролі, типу ресурсу та рівня ризику [5, 6].

Наведені поняття формують термінологічну основу для подальшого аналізу моделей хмарних сервісів, розподілу відповідальності та принципів захисту корпоративної IT-інфраструктури.

1.2 Моделі хмарних сервісів та розподіл відповідальності за безпеку

Подальший аналіз потребує розгляду моделей хмарних сервісів, оскільки саме вони визначають, які компоненти середовища залишаються під контролем організації, а які переходять до зони відповідальності хмарного провайдера. Тому вибір моделі хмарного сервісу впливає не лише на спосіб використання ресурсів, а й на межі відповідальності за їх захист [3, 4].

У корпоративному середовищі хмарні сервіси рідко використовуються ізольовано. Організація може одночасно застосовувати інфраструктурні ресурси для розміщення серверів, платформні сервіси для розробки застосунків, готові SaaS-рішення для документообігу або електронної пошти, а також безсерверні функції для автоматизації окремих процесів. Така комбінація підвищує гнучкість IT-інфраструктури, проте ускладнює управління безпекою, оскільки кожна модель має власний рівень контролю та власні ризики [6].

Характер моделі хмарного сервісу визначає практичну логіку захисту. Чим більше рівнів інфраструктури залишається під контролем організації, тим ширшим є перелік завдань із безпеки, які вона має виконувати самостійно. Водночас перехід до моделей, де більшість технічних компонентів обслуговує провайдер, не означає повного усунення відповідальності організації. Навіть у готових хмарних сервісах компанія продовжує відповідати за власні дані, облікові записи, ролі, політики доступу та налаштування безпеки.

Найбільший рівень контролю організація зберігає під час використання інфраструктурних сервісів. У такому випадку провайдер забезпечує базову інфраструктуру, але значна частина операційного керування залишається на стороні користувача. Організація самостійно визначає параметри операційних систем, мережеві правила, засоби журналювання, резервне копіювання та політики доступу. Такий підхід дає можливість гнучко адаптувати середовище до власних потреб, однак одночасно підвищує залежність безпеки від якості

адміністрування. Саме тому для інфраструктурних сервісів характерними є ризики, пов’язані з відкритими мережевими портами, помилками налаштування віртуальних машин, несвоєчасним оновленням систем або надмірними правами користувачів [8].

У платформних сервісах акцент безпеки зміщується з адміністрування базової інфраструктури на захист застосунків, даних та інтеграцій. Провайдер бере на себе частину системних компонентів, однак організація продовжує відповідати за власний код, API, секрети, бази даних, сервісні облікові записи та логіку доступу до ресурсів. У цьому випадку основні ризики виникають не стільки на рівні серверів, скільки на рівні помилок у застосунках, некоректних інтеграцій, небезпечного зберігання ключів або неправильного розмежування доступу до даних [6, 8].

Під час використання готових програмних сервісів організація має найменший вплив на технічну інфраструктуру, але її відповідальність не зникає. Основний обсяг завдань переноситься на користувацький рівень: створення та блокування облікових записів, налаштування ролей, застосування багатофакторної автентифікації, контроль спільного доступу до файлів і захист корпоративної інформації. Тому для таких сервісів особливо небезпечними є компрометація акаунтів, збереження доступу після звільнення працівників, надмірні права користувачів або некоректні параметри спільного використання даних [4, 8].

Самостійне значення мають безсерверні обчислення, де організація не керує серверною інфраструктурою безпосередньо, але відповідає за безпеку функцій, їхні дозволи, секрети та зв’язки з іншими хмарними сервісами. Такий підхід зменшує обсяг класичного адміністрування, проте підвищує значення контролю за правами виконання, API-інтеграціями та обліковими даними, які використовуються автоматизованими процесами. Якщо функція має надмірні дозволи або використовує незахищені ключі доступу, її компрометація може стати шляхом до інших ресурсів корпоративної хмари.

Таким чином, відмінність між моделями хмарних сервісів полягає не лише в технічному способі їх надання, а й у розподілі безпекових обов'язків. Інфраструктурні сервіси потребують більшого контролю операційних систем, мережі та віртуальних ресурсів; платформні сервіси — посиленого захисту застосунків, API та даних; готові програмні сервіси — якісного управління користувачами, ролями та доступами; безсерверні рішення — контролю дозволів функцій, секретів і сервісних інтеграцій.

Таблиця 1.1

Порівняння основних моделей хмарних сервісів з погляду безпеки [1, 6]

Модель	**Рівень контролю організації**	**Основна зона відповідальності організації**	**Типові ризики**
IaaS	Високий	Операційні системи, застосунки, мережеві правила, права доступу, дані	Відкриті порти, помилки конфігурації ВМ, несвоєчасне оновлення ОС
PaaS	Середній	Код застосунків, API, бази даних, секрети, сервісні облікові записи	Вразливості застосунку, витік секретів, помилки інтеграції
SaaS	Обмежений	Користувачі, ролі, MFA, спільний доступ, корпоративні дані	Компрометація акаунтів, надмірні права, неправильні політики доступу
FaaS	Обмежений на рівні інфраструктури, але значний на рівні коду	Код функції, секрети, права доступу, інтеграції	Надмірні дозволи функцій, витік токенів, помилки логіки виконання

Одним із базових підходів до організації хмарної безпеки є розмежування відповідальності між провайдером і клієнтом. Постачальник хмарних послуг забезпечує захист базової інфраструктури, тоді як організація-користувач відповідає за власні дані, облікові записи, ролі, конфігурації та політики доступу [3, 4].

Таблиця 1.2

Розподіл відповідальності між організацією та хмарним провайдером [3, 4]

On-site	**IaaS**	**PaaS**	**SaaS**
Додатки	Додатки	Додатки	Додатки
Дані	Дані	Дані	Дані
Проміжне ПО	Проміжне ПО	Проміжне ПО	Проміжне ПО
ОС	ОС	ОС	ОС
Віртуалізація	Віртуалізація	Віртуалізація	Віртуалізація
Сервери	Сервери	Сервери	Сервери
Мережа	Мережа	Мережа	Мережа

Керуєте ви

Керує постачальник послуг

Розподіл обов'язків у різних моделях хмарних сервісів показує, що перехід до хмари не усуває відповідальність організації за безпеку, а лише змінює її межі. У локальній моделі компанія контролює всі рівні інфраструктури, тоді як в IaaS, PaaS і SaaS частина технічних компонентів переходить до провайдера, але дані, користувачі, ролі доступу та налаштування безпеки залишаються в зоні контролю організації.

Неправильне розуміння моделі спільної відповідальності є однією з поширених причин хмарних інцидентів. Організація може помилково вважати, що після переходу до хмари всі питання безпеки автоматично переходять до провайдера. Насправді відкритий доступ до сховища, надмірні права адміністратора, відсутність багатофакторної автентифікації, активні облікові записи звільнених працівників або вимкнене журналювання зазвичай належать до зони відповідальності самої організації.

Вибір моделі сервісу також визначає, на яких напрямах захисту потрібно зосередитися. Для інфраструктурних сервісів першочерговими є захист мережевих правил, операційних систем і віртуальних машин. Для платформних сервісів важливими стають безпека застосунків, API, секретів, баз даних і сервісних облікових записів. Для готових програмних сервісів основний акцент переноситься на керування користувачами, ролями, багатофакторною автентифікацією, політиками доступу та корпоративними даними.

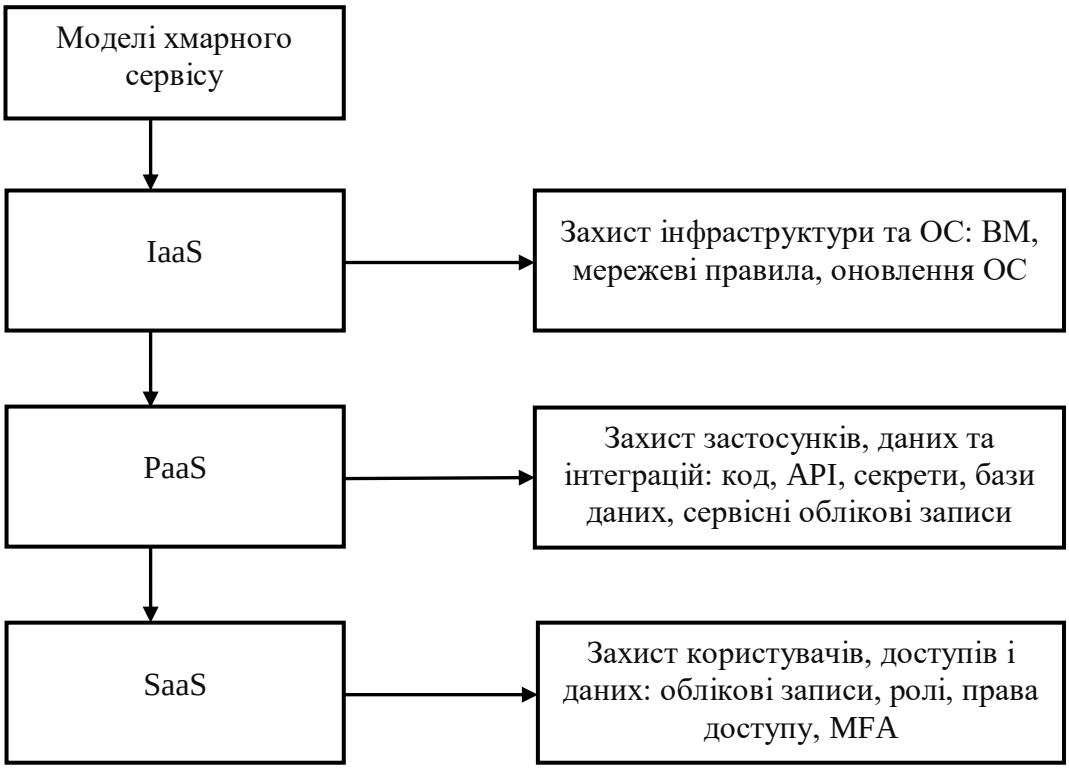

Рис. 1.1. Організація захисту залежно від моделі хмарного сервісу

У реальному корпоративному середовищі зазвичай поєднуються кілька моделей хмарних сервісів. Віртуальні сервери можуть працювати в IaaS, вебзастосунки — у PaaS, а електронна пошта або документообіг — у SaaS.

Отже, моделі хмарних сервісів безпосередньо впливають на побудову системи захисту корпоративного хмарного середовища. Чим більше контролю має організація, тим більше технічних і організаційних заходів вона повинна виконувати самостійно. Водночас навіть у моделях, де основну інфраструктуру підтримує провайдер, організація залишається відповідальною за власні дані, доступи, конфігурації та політики безпеки. Саме тому ефективний захист хмари потребує чіткого розуміння меж відповідальності, регулярного контролю налаштувань і застосування принципу найменших привілеїв.

1.3 Основні принципи захисту корпоративної хмари та концепція Zero Trust

Безпека корпоративної хмари має формуватися не як набір окремих інструментів, а як узгоджена система технічних, організаційних і контрольних заходів. Така потреба зумовлена розподіленим характером хмарної інфраструктури, відсутністю чітко визначеного фізичного периметра, різноманітністю користувачів і постійною зміною ресурсів, доступів та конфігурацій.

За таких умов захист корпоративної хмари не може ґрунтуватися лише на одному механізмі, зокрема паролі, міжмережевому екрані або шифруванні. Ефективна система безпеки має охоплювати декілька взаємопов'язаних рівнів: ідентифікацію користувачів, контроль доступу до ресурсів, захист даних, перевірку конфігурацій, моніторинг подій і реагування на інциденти [20, 28]. Саме поєднання цих рівнів дає змогу зменшити ймовірність атаки та обмежити її наслідки у випадку компрометації окремого елемента.

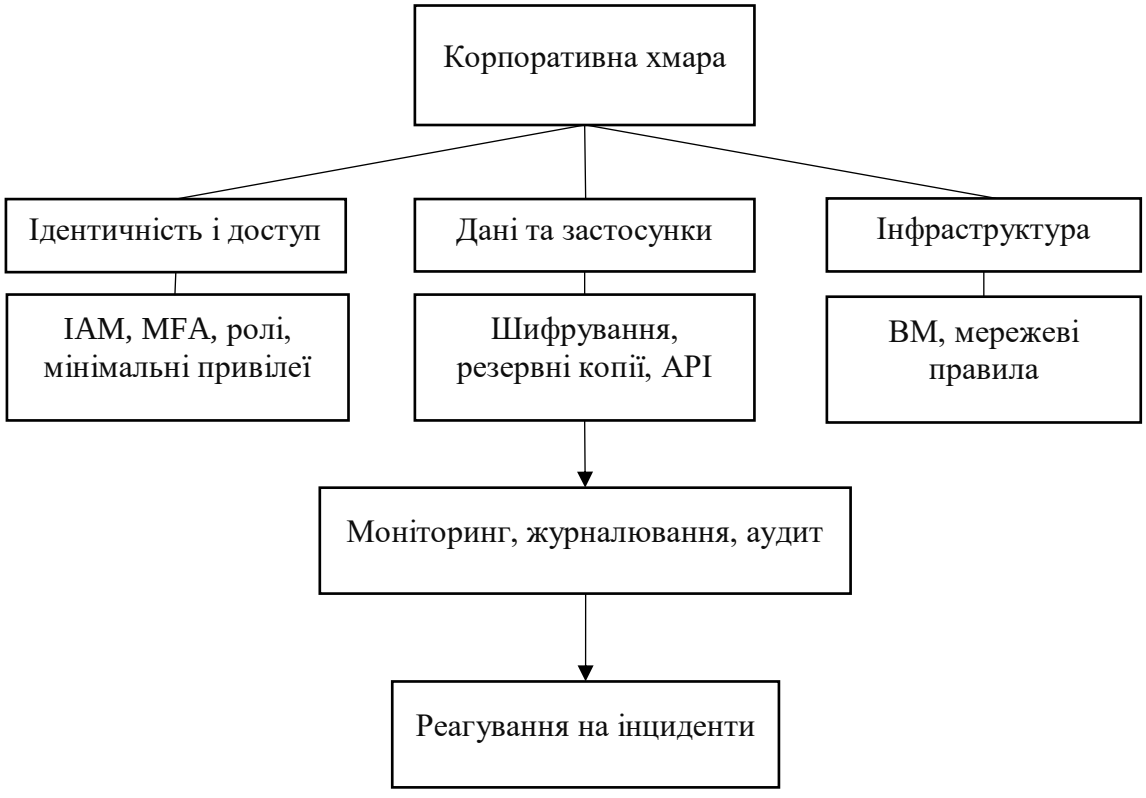

Рис. 1.2. Рівні захисту корпоративного хмарного середовища

Така структура захисту показує, що безпека корпоративної хмари не може обмежуватися лише контролем входу користувачів або налаштуванням окремих сервісів. Найбільш стійкою є модель, у якій доступи, дані, інфраструктура, журналювання та реагування працюють як взаємопов'язані рівні контролю.

Для більш повного розуміння підходів до захисту корпоративного хмарного середовища важливим є визначення основних принципів, на яких повинна будуватися система безпеки. У хмарній інфраструктурі такі принципи мають не лише запобігати несанкціонованому доступу, а й обмежувати наслідки можливого інциденту, забезпечувати контроль дій користувачів, захист даних і своєчасне виявлення небезпечних змін. Саме тому захист корпоративної хмари доцільно розглядати як поєднання управління привілеями, посиленої автентифікації, сегментації ресурсів, шифрування, моніторингу, журналювання та аудиту конфігурацій (Таблиця 1.3).

Таблиця 1.3

Основні принципи захисту корпоративного хмарного середовища

Принцип захисту	**Зміст принципу**	**Практичне значення**
Принцип найменших привілеїв	Надання користувачу або сервісу лише необхідних прав	Зменшення наслідків компрометації акаунта
Багатофакторна автентифікація	Підтвердження входу за допомогою кількох факторів	Підвищення захисту облікових записів
Сегментація ресурсів	Поділ середовища на окремі логічні зони	Обмеження поширення атаки
Шифрування даних	Захист інформації під час зберігання та передавання	Збереження конфіденційності даних
Моніторинг та журналювання	Фіксація подій, дій користувачів і змін конфігурацій	Своєчасне виявлення інцидентів
Аудит конфігурацій	Перевірка налаштувань ресурсів і політик безпеки	Виявлення помилок і вразливих налаштувань

Практична цінність наведених принципів полягає в тому, що вони перекривають різні етапи можливої атаки. MFA ускладнює початковий несанкціонований вхід, принцип найменших привілеїв обмежує дії скомпрометованого акаунта, а моніторинг і журналювання дозволяють виявити нетипову активність та відновити послідовність подій.

Серед сучасних підходів до хмарної безпеки одним із ключових підходів до посилення хмарної безпеки є концепція Zero Trust. Вона ґрунтується не на довірі до внутрішньої мережі або факту успішного входу, а на постійній перевірці кожного запиту до ресурсу з урахуванням контексту та рівня ризику [5, 29]. Для корпоративної хмари це особливо актуально, оскільки користувачі можуть працювати віддалено, ресурси можуть розміщуватися в різних сервісах, а доступ до даних часто здійснюється через облікові записи, API та сервісні інтеграції.

Логіку Zero Trust доцільно розглядати як процес послідовної перевірки запиту доступу.

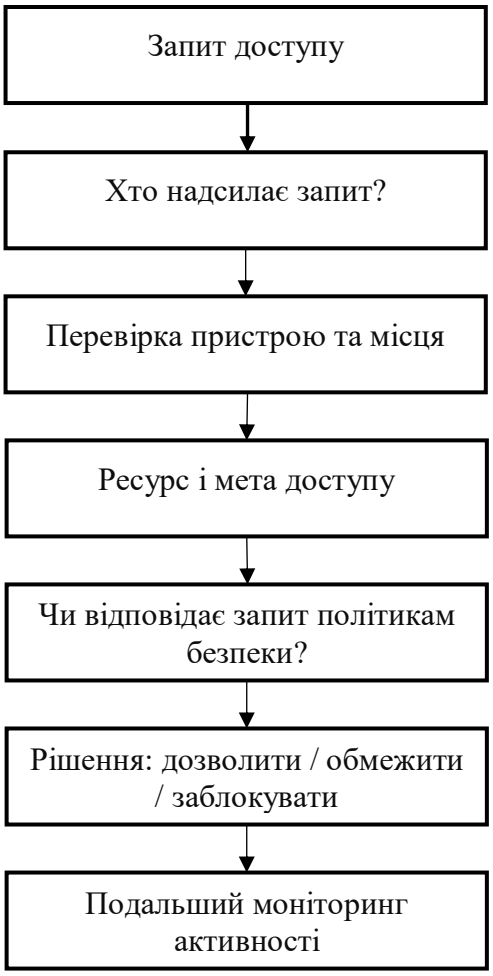

Рис. 1.3. Логіка прийняття рішення про доступ за концепцією Zero Trust

Концепція Zero Trust не обмежується перевіркою пароля або самим фактом входу користувача до системи. Рішення про надання доступу формується на основі ширшого контексту: ідентичності користувача, стану пристрою, місця підключення, ролі, типу ресурсу та рівня ризику. Навіть після успішного надання

доступу активність користувача повинна залишатися під контролем, оскільки нетипова або підозріла поведінка може свідчити про компрометацію облікового запису чи спробу виконання несанкціонованих дій [5, 8].

Висновки до розділу 1

У розділі 1 досліджено теоретичні основи безпеки корпоративних хмарних середовищ, їхню сутність, основні компоненти та особливості використання в сучасній IT-інфраструктурі організацій. Встановлено, що корпоративна хмара є складним і багаторівневим середовищем, яке охоплює облікові записи, ролі доступу, хмарні сховища, бази даних, віртуальні машини, API, сервісні облікові записи та засоби моніторингу. Таке середовище забезпечує гнучкість, масштабованість і зручність віддаленої роботи, однак водночас створює нові ризики для конфіденційності, цілісності та доступності корпоративних даних.

Аналіз моделей хмарних сервісів показав, що IaaS, PaaS, SaaS і FaaS відрізняються рівнем контролю з боку організації та хмарного провайдера. Чим більше компонентів середовища залишається під контролем організації, тим більший обсяг технічних і організаційних заходів безпеки вона повинна виконувати самостійно. Водночас навіть у моделях, де основну інфраструктуру підтримує провайдер, організація не звільняється від відповідальності за власні дані, облікові записи, права доступу, конфігурації та політики безпеки. Особливе значення має модель спільної відповідальності, неправильне розуміння якої може призвести до відкритих сховищ, надмірних привілеїв, неактивних облікових записів або відсутності належного журналювання.

Дослідження основних принципів захисту корпоративної хмари показало, що ефективна безпека не може базуватися лише на одному технічному засобі. Вона повинна поєднувати принцип найменших привілеїв, багатофакторну автентифікацію, сегментацію ресурсів, шифрування даних, моніторинг, журналювання та аудит конфігурацій. Використання цих принципів дозволяє не лише зменшити ймовірність успішної атаки, а й обмежити її наслідки у випадку компрометації окремого користувача, сервісу або ресурсу.

Окрему увагу приділено концепції Zero Trust, яка є особливо актуальною для корпоративних хмарних середовищ через відсутність чіткого мережевого периметра, віддалений доступ користувачів і використання різних хмарних сервісів. Визначено, що Zero Trust ґрунтується на відмові від автоматичної довіри та передбачає постійну перевірку кожного запиту доступу з урахуванням користувача, пристрою, місця підключення, ролі, типу ресурсу та рівня ризику.

Отже, корпоративне хмарне середовище можна охарактеризувати як динамічну, розподілену та залежну від правильності налаштувань інфраструктуру. Її захист потребує комплексного підходу, чіткого розуміння меж відповідальності між організацією та провайдером, контролю доступів, постійного моніторингу й застосування принципів Zero Trust.

Теоретичний аналіз корпоративного хмарного середовища, моделей сервісів, розподілу відповідальності та принципів Zero Trust створює основу для подальшого дослідження конкретних векторів атак, які виникають через помилки управління доступом, неправильні конфігурації ресурсів і недостатню видимість подій безпеки.

РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ ВЕКТОРІВ АТАК НА КОРПОРАТИВНІ ХМАРНІ СЕРЕДОВИЩА

2.1. Загальна характеристика загроз корпоративним хмарним середовищам

Корпоративні хмарні середовища стали привабливою ціллю для зловмисників, оскільки в них зосереджується значна частина критичних цифрових активів організації: службові документи, персональні дані, фінансова інформація, резервні копії, бази даних, облікові записи, API-ключі та конфігурації сервісів. Компрометація таких ресурсів може вплинути не лише на окремий сервіс, а й на безперервність роботи підрозділів або всієї організації. Тому аналіз загроз корпоративній хмарі має враховувати не тільки технічні вразливості, а й організаційні помилки, особливості управління доступом, конфігурації ресурсів та рівень моніторингу подій безпеки [6].

На відміну від локальної інфраструктури, де значна частина ресурсів розміщується в межах контрольованого периметра, хмарне середовище є більш розподіленим. Доступ до нього може здійснюватися з різних пристроїв, мереж і географічних локацій, що збільшує кількість можливих точок входу для атаки [5, 6].

Особливість загроз хмарним технологіям полягає в тому, що зловмиснику не завжди потрібно безпосередньо атакувати інфраструктуру хмарного провайдера.

У багатьох випадках достатньо використати слабке місце на стороні організації або користувача. До таких слабких місць належать:

- помилки конфігурації;
- надмірні права доступу;
- відсутність багатофакторної автентифікації;
- відкриті хмарні сховища;
- викрадені облікові дані;
- неактивні облікові записи;

- небезпечні API-ключі або недостатнє журналювання подій [6, 8].

Отже, безпека корпоративної хмари залежить не лише від надійності платформи провайдера, а й від того, наскільки коректно організація налаштовує та контролює власні ресурси. Провайдер забезпечує фізичну безпеку дата-центрів, доступність базової інфраструктури та окремі вбудовані механізми захисту, однак саме організація визначає, хто має доступ до даних, які ролі надаються користувачам, чи ведеться моніторинг активності та чи обмежено публічний доступ до ресурсів. Це підтверджує практичне значення моделі спільної відповідальності, розглянутої в першому розділі [4].

Аналіз сучасних кіберінцидентів показує, що атаки на хмарні середовища дедалі частіше зміщуються від класичного зламу окремих серверів до компрометації облікових записів, використання помилок конфігурації та атак на інтеграції між сервісами [14, 15, 16]. Це пов’язано з тим, що корпоративні хмарні сервіси часто доступні через мережу Інтернет, а облікові записи користувачів, сервісні ролі або API-ключі можуть мати доступ одразу до багатьох ресурсів.

За даними Verizon Data Breach Investigations Report 2025, експлуатація вразливостей як початковий вектор доступу до порушень зросла до 20%, а участь третіх сторін у порушеннях подвоїлася до 30% [12]. Для корпоративної хмари це має особливе значення, оскільки хмарне середовище часто інтегрується зі сторонніми платформами, підрядниками, SaaS-рішеннями та зовнішніми API. Отже, джерело загрози може перебувати не лише всередині організації, а й у пов’язаних сервісах або партнерських системах.

Загрози корпоративним хмарним середовищам доцільно розглядати через базові властивості інформаційної безпеки: конфіденційність, цілісність і доступність [6, 8].

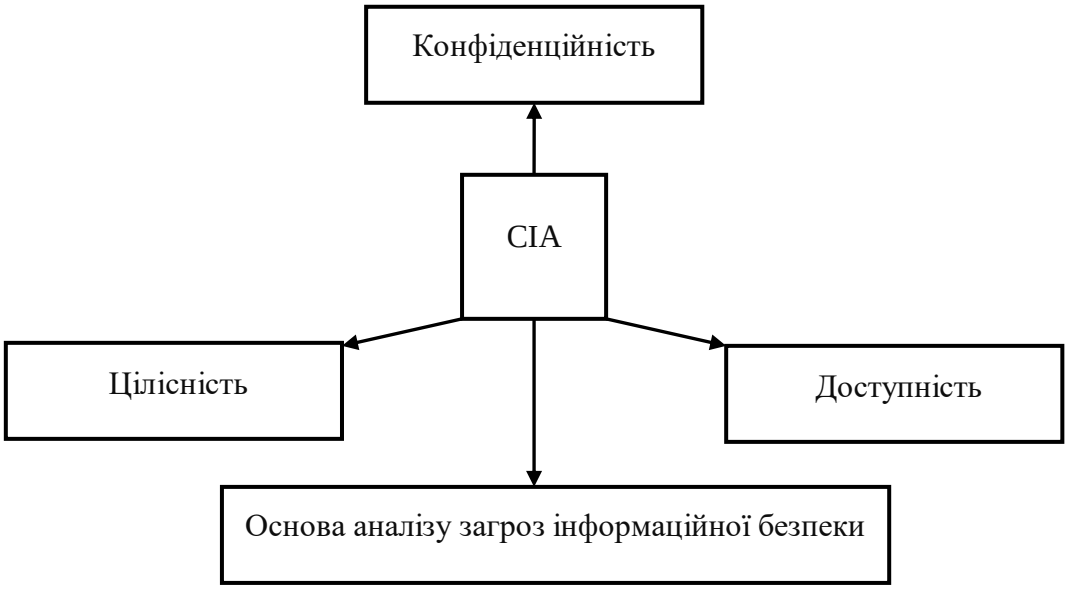

Рис. 2.1. Тріада CIA як основа аналізу загроз інформаційній безпеці

Використання тріади CIA дозволяє оцінити не лише сам факт реалізації атаки, а й характер її впливу на організацію. Для хмарного середовища доцільно також враховувати контрольованість, тобто здатність організації бачити події, відстежувати дії користувачів і своєчасно виявляти небезпечні зміни. Саме тому загрози корпоративній хмарі можна проаналізувати через вплив на конфіденційність, цілісність, доступність і контрольованість.

Таблиця 2.1

Вплив загроз корпоративній хмарі на властивості інформаційної безпеки [6, 8]

Властивість інформаційної безпеки	**Як може порушуватися в хмарі**	**Приклад загрози**
Конфіденційність	Несанкціонований доступ до даних, файлів, пошти або резервних копій	Викрадення облікових даних, відкритий доступ до сховища
Цілісність	Несанкціонована зміна даних, ролей, політик або конфігурацій	Зміна прав доступу, модифікація налаштувань сервісу
Доступність	Неможливість користувачів або систем працювати з хмарними ресурсами	Ransomware, DDoS, видалення ресурсів, блокування акаунтів
Контрольованість	Втрата видимості подій і неможливість відстежити дії користувачів	Вимкнене журналювання, відсутність моніторингу

Вплив хмарних загроз не обмежується лише витоком інформації. Один інцидент може одночасно порушувати конфіденційність, цілісність, доступність і контрольованість середовища: наприклад, скомпрометований обліковий запис може використовуватися для доступу до файлів, зміни політик, видалення ресурсів або вимкнення журналювання.

Окремо варто звернути увагу на те, що атаки на хмарні сервіси стосуються не лише IT-компаній. Хмарні технології активно використовуються державним сектором, сферою послуг, фінансовими організаціями, медичними установами, промисловістю, освітніми й науковими установами. Через це атаки на хмарну інфраструктуру мають міжгалузевий характер і можуть впливати як на комерційні організації, так і на соціально важливі або критичні сервіси.

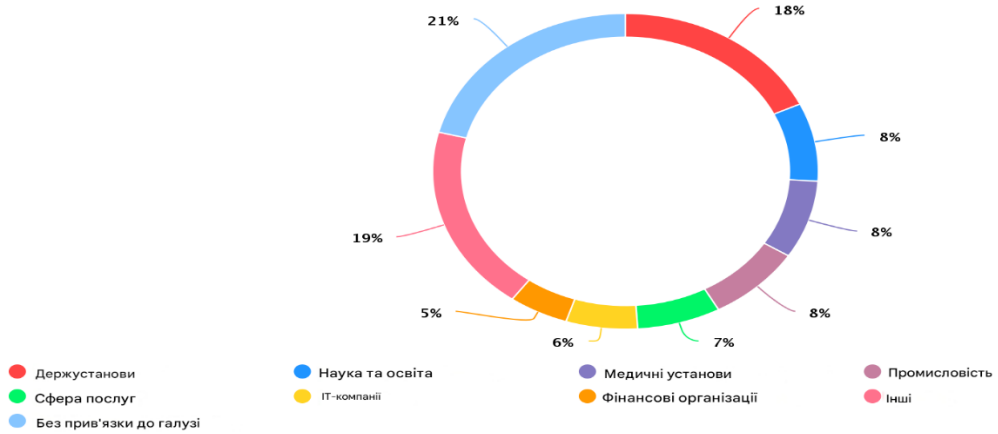

Рис. 2.2. Розподіл атак на хмарні сервіси за галузями

Джерело: складено автором.

За наведеним розподілом державний сектор має одну з найбільших часток атак — 18%. Це може пояснюватися тим, що такі організації обробляють значні обсяги персональних і службових даних, використовують цифрові сервіси, онлайн-кабінети, CRM-системи, хмарні сховища та платіжні інтеграції. У разі компрометації таких середовищ наслідки можуть бути не лише фінансовими, а й соціальними або репутаційними.

Медичні установи, промисловість, наука та освіта мають по 8% у наведеному розподілі. Для цих сфер основними ризиками є витік чутливих даних, порушення доступності інформаційних систем, вплив на виробничі

процеси або втручання в роботу навчальних і дослідницьких платформ. Фінансові організації та IT-компанії мають меншу частку — 6% і 5%, проте інциденти в цих секторах можуть бути особливо критичними через фінансові втрати, шахрайські операції або подальший вплив на клієнтів і партнерів.

Діаграма підтверджує той факт, що атаки на хмарні сервіси мають широкий галузевий розподіл. Тому захист корпоративної хмари повинен враховувати не лише технічну архітектуру, а й специфіку діяльності організації, типи даних, кількість користувачів і можливі наслідки інциденту.

Разом із галузевим розподілом атак важливо враховувати й основні джерела загроз усередині самого корпоративного хмарного середовища. У більшості випадків ризики виникають не в одному конкретному елементі, а на перетині кількох напрямів: користувацьких доступів, конфігурацій ресурсів, API та інтеграцій, сховищ даних, механізмів моніторингу, а також особливостей гібридної або мультихмарної інфраструктури.

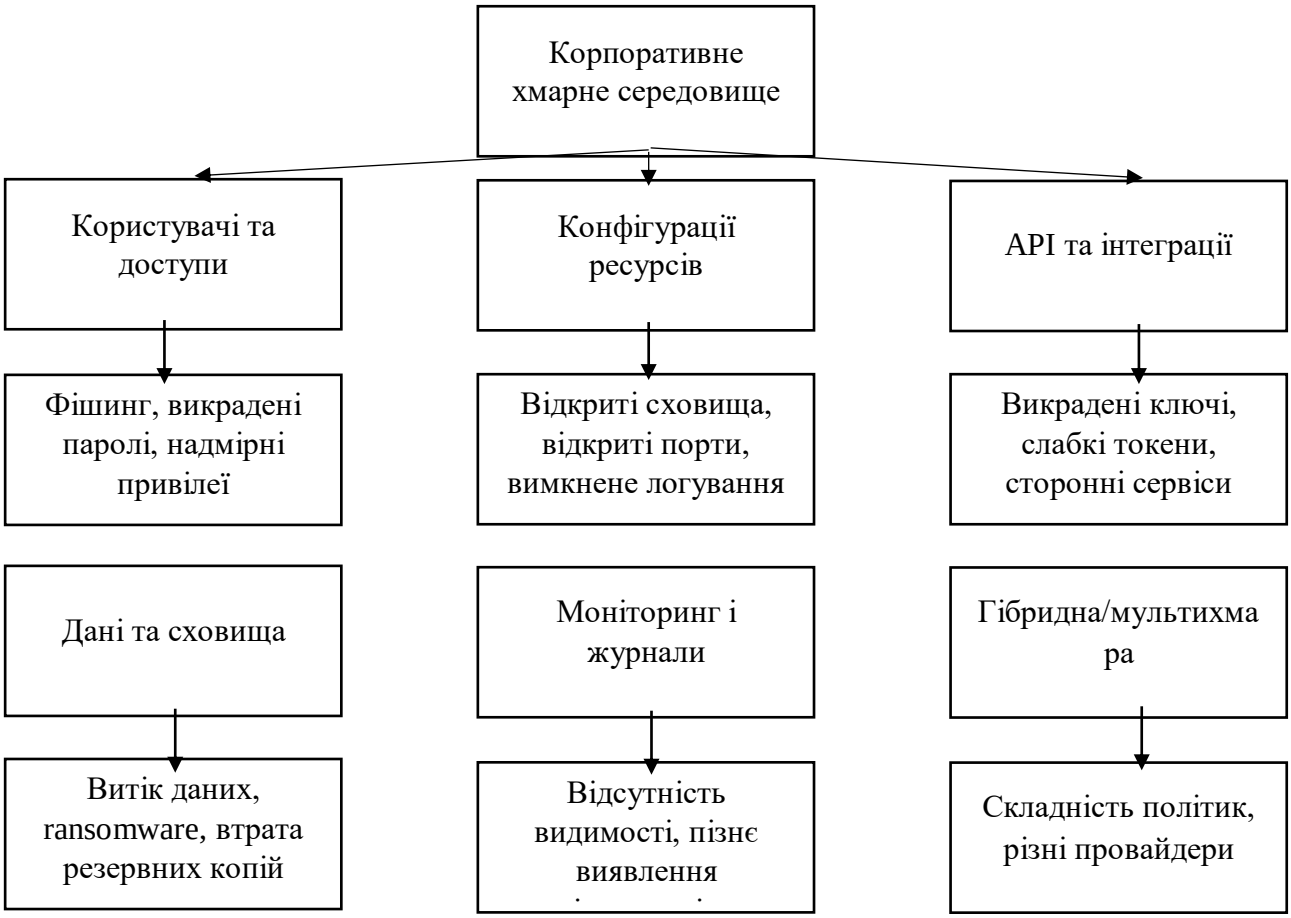

Рис. 2.3. Основні джерела загроз корпоративному хмарному середовищу [6, 8]

Загрози корпоративній хмарі варто оцінювати як взаємопов’язаний ланцюг ризиків. Компрометація користувача може посилюватися надмірними правами, помилка конфігурації — відкривати доступ до даних, а відсутність журналювання — ускладнювати виявлення інциденту та подальше розслідування.

Не менш важливим джерелом ризику є конфігурації ресурсів. Неправильно налаштовані сховища, відкриті мережеві порти, надмірно широкі дозволи або вимкнене журналювання можуть створювати вразливості навіть без прямого зламу системи. Такі помилки часто виникають через швидке розгортання сервісів, відсутність єдиних правил адміністрування або недостатній контроль змін.

Окрему групу становлять API та інтеграції. Корпоративні хмарні сервіси активно взаємодіють зі сторонніми платформами, застосунками та внутрішніми системами. У разі компрометації API-ключа, токена або небезпечної інтеграції зловмисник може отримати канал доступу до даних чи окремих функцій системи. У цьому контексті ризик посилюється тим, що такі доступи часто використовуються автоматизовано і можуть залишатися активними тривалий час без належного контролю [11, 24].

Критичним об’єктом захисту залишаються дані та хмарні сховища. Саме з ними пов’язані ризики витоку інформації, несанкціонованого копіювання, шифрування або втрати резервних копій. Для корпоративного середовища це має особливе значення, оскільки хмарні сервіси можуть містити великі обсяги фінансової, персональної, службової або комерційної інформації.

Важливу роль у зниженні рівня загроз відіграють моніторинг і журналювання. Якщо організація не має достатньої видимості подій, не відстежує входи користувачів, зміну ролей, створення ресурсів і зміну конфігурацій, атака може залишатися непоміченою протягом тривалого часу. У таких умовах навіть незначна помилка може перерости у повноцінний інцидент [7, 8, 18].

Додаткову складність створюють гібридні та мультихмарні середовища. Використання кількох провайдерів, поєднання локальної інфраструктури з хмарними сервісами та різні політики доступу ускладнюють централізоване управління безпекою. За таких умов організації важче забезпечити єдині правила контролю доступу, моніторингу, журналювання та реагування на інциденти [6, 30].

Окремим джерелом ризику є людський фактор. У корпоративній хмарі з ресурсами працюють адміністратори, розробники, DevOps-фахівці, працівники бізнес-підрозділів, зовнішні підрядники та автоматизовані сервіси. Кожен із цих суб’єктів може стати причиною інциденту як через навмисні дії, так і через помилку. Наприклад, адміністратор може випадково відкрити доступ до сховища, розробник — залишити секрет у репозиторії, підрядник — зберегти активний доступ після завершення робіт, а звичайний користувач — стати жертвою фішингової атаки [8, 12].

Отже, сучасна атака на хмарне середовище не обов’язково починається зі складного технічного злому. У багатьох випадках достатньо однієї помилки: слабкого пароля, неправильно наданого дозволу, активного застарілого токена, відкритого сховища або відсутності журналювання. Тому захист корпоративної хмари має включати не лише технічні засоби, а й організаційні процеси: регулярний перегляд доступів, інвентаризацію ресурсів, контроль конфігурацій, навчання користувачів і перевірку дій адміністраторів.

Ще однією проблемою є складність інвентаризації хмарних ресурсів. Хмарне середовище постійно змінюється: ресурси створюються, масштабуються, переміщуються, видаляються або інтегруються з іншими сервісами. Частина таких змін виконується вручну, частина — через автоматизовані сценарії. Якщо організація не має єдиного реєстру ресурсів і не контролює зміни, у середовищі можуть залишатися “забуті” об’єкти: тестові сервери, невикористовувані сховища, неактивні акаунти або токени, що продовжують мати доступ до даних.

На практиці саме такі елементи часто стають зручними точками входу для зловмисника. Наприклад, тестове середовище може мати слабші налаштування безпеки, але зберігати реальні дані. Старий API-ключ може залишатися активним після завершення проєкту, а сервісний обліковий запис може мати надмірні права через відсутність регулярного перегляду доступів. Усе це створює ризики, які складно виявити без системного моніторингу та аудиту.

Узагальнення наведених загроз дозволяє виділити основні чинники, які підвищують ризик реалізації атак у корпоративному хмарному середовищі:

1. розмиття традиційного мережевого периметра через віддалений доступ і використання SaaS-сервісів;
2. велика кількість користувачів, ролей, сервісних облікових записів і токенів;
3. швидке створення та зміна ресурсів без належного контролю конфігурацій;
4. активне використання API та інтеграцій між різними сервісами;
5. поєднання локальної, хмарної та мультихмарної інфраструктури;
6. залежність від сторонніх провайдерів і підрядників;
7. недостатня видимість подій безпеки та відсутність централізованого журналювання;
8. людський фактор, зокрема помилки адміністрування та фішинг.

З економічного погляду хмарні інциденти можуть бути особливо відчутними для організації. За даними IBM Cost of a Data Breach Report 2025, середня глобальна вартість витоку даних становить 4,4 млн доларів США [13]. Це підтверджує, що інциденти в хмарному середовищі слід розглядати не лише як технічну проблему, а й як загрозу для фінансової стабільності, репутації та безперервності бізнесу.

Таким чином, загрози корпоративній хмарі мають змішану природу: вони виникають як через технічні недоліки, так і через організаційні помилки. Найбільш небезпечним є те, що хмарне середовище може створювати ілюзію автоматичної захищеності. Організація користується сервісами великого провайдера і може помилково вважати, що більшість ризиків уже усунена. Насправді значна частина атак реалізується саме через ті налаштування, які залишаються відповідальністю самої організації.

Отже, актуальні загрози корпоративному хмарному середовищу формуються на перетині кількох чинників: доступності сервісів через Інтернет, великої кількості облікових записів, складності конфігурацій, активного використання API, залежності від сторонніх платформ і недостатнього моніторингу. Тому подальший аналіз доцільно зосередити на двох напрямах, які мають найбільший вплив на безпеку корпоративної хмари: атаках на управління доступом та атаках, спричинених помилками конфігурації ресурсів.

2.2. Аналіз атак, пов’язаних з управлінням доступом, обліковими записами та надмірними привілеями

У хмарній інфраструктурі управління доступом набуває особливого значення, оскільки саме через облікові записи, ролі, токени, сервісні акаунти й API-ключі користувачі та застосунки взаємодіють із ресурсами. Через це ідентичність стає не допоміжним, а центральним елементом захисту [20, 29].

Особливість атак на управління доступом полягає в тому, що зловмисник не завжди намагається зламати хмарну платформу технічно. Часто його мета полягає в отриманні можливості діяти в системі як легітимний користувач. У такому випадку атака може виглядати не як зовнішнє вторгнення, а як звичайний вхід до акаунта, перегляд файлів, створення ресурсу або зміна налаштувань. Це значно ускладнює виявлення інциденту, особливо якщо в організації недостатньо налаштовано моніторинг, журналювання та аналіз поведінки користувачів.

За даними Verizon Data Breach Investigations Report 2025, зловживання обліковими даними залишається одним із провідних початкових векторів атак і

становить 22%, тоді як експлуатація вразливостей становить 20% [12]. Для корпоративної хмари це має особливе значення, оскільки один скомпрометований обліковий запис може надати доступ не лише до окремого сервісу, а й до пов’язаних сховищ, застосунків, панелей адміністрування, API та резервних копій.

Основними причинами успішних атак на управління доступом у хмарному середовищі є використання слабких або повторно застосованих паролів, відсутність багатофакторної автентифікації, фішингові повідомлення, надмірні права користувачів, активні облікові записи колишніх працівників, неконтрольовані сервісні акаунти, відкриті API-ключі та відсутність регулярного перегляду ролей. У сукупності ці чинники створюють умови, за яких зловмисник може отримати доступ до хмарного середовища без складного технічного злому.

Для наочного відображення послідовності дій зловмисника доцільно подати типовий сценарій розвитку атаки через скомпрометований обліковий запис.

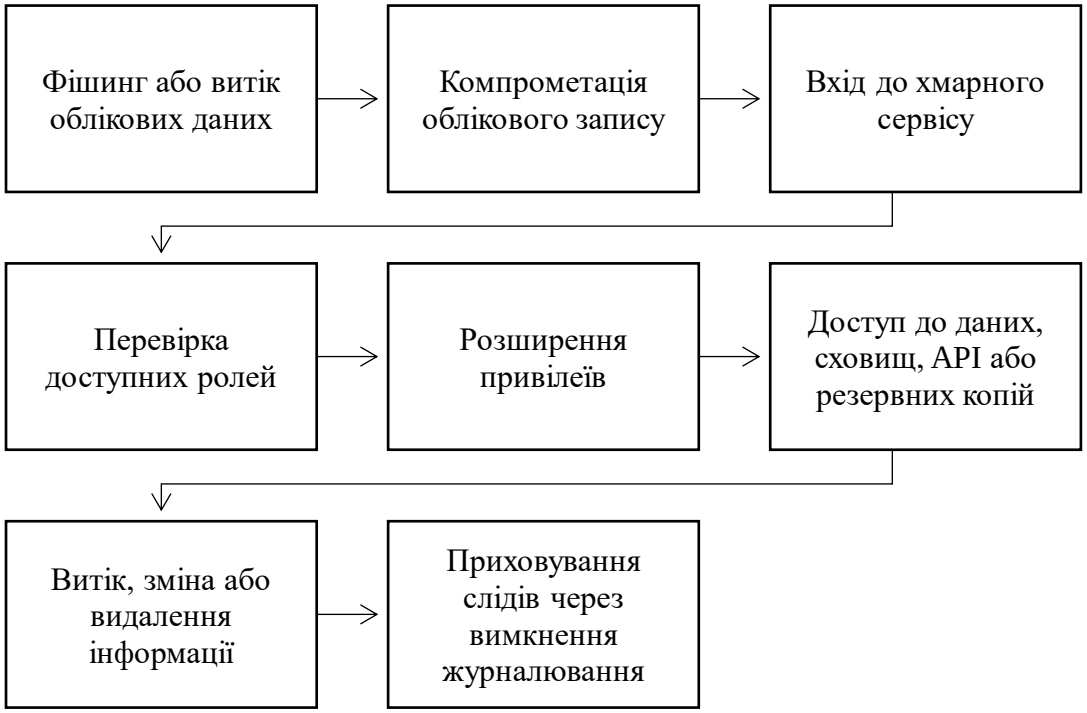

Рис. 2.4. Ланцюг розвитку атаки через скомпрометований обліковий запис

Найбільша небезпека такого сценарію полягає в тому, що початковий вхід може виглядати як звичайна активність користувача. Якщо обліковий запис має

надмірні привілеї, а події доступу не контролюються належним чином, атака швидко переходить від простого входу до зміни політик, доступу до даних або приховування слідів.

Важливим напрямом аналізу є атаки, пов’язані з надмірними привілеями. Надмірні привілеї виникають тоді, коли користувач, сервісний акаунт або застосунок має більше прав, ніж потрібно для виконання його функцій. Наприклад, працівник, якому потрібен лише перегляд документів, може мати можливість їх редагувати, видаляти або поширювати за межі організації. Аналогічно, сервісний обліковий запис може мати права адміністратора, хоча фактично потребує доступу лише до одного сховища або бази даних.

Надмірні права особливо небезпечні в хмарному середовищі через взаємозв’язок ресурсів. Один акаунт може мати доступ до кількох сервісів одночасно: сховищ, віртуальних машин, баз даних, журналів подій, систем резервного копіювання та інструментів адміністрування. У разі компрометації такого акаунта зловмисник отримує не лише початковий доступ, а й можливість переміщуватися між ресурсами, змінювати політики доступу, створювати нові ключі, вимикати моніторинг або видаляти резервні копії.

Особливу групу ризиків формують машинні ідентичності: сервісні облікові записи, API-ключі, токени доступу та ролі застосунків. На відміну від звичайних користувачів, вони часто працюють автоматизовано, мають тривалий строк дії й можуть залишатися поза регулярним контролем адміністраторів [16, 24].

Для більш системного аналізу атак, пов’язаних з управлінням доступом, доцільно розглянути їх за початковим вектором, механізмом реалізації, можливими наслідками та ознаками виявлення.

Таблиця 2.2

Аналіз атак, пов’язаних з управлінням доступом у корпоративній хмарі [6, 8, 12]

Вектор атаки	**Механізм реалізації**	**Можливі наслідки**	**Ознаки виявлення**
Фішинг облікових даних	Користувач вводить логін і пароль на підробленому ресурсі	Несанкціонований вхід, доступ до пошти, файлів або SaaS-сервісів	Вхід із незвичної локації, новий пристрій, підозріла активність після входу
Відсутність MFA	Зловмисник використовує викрадений пароль без додаткової перевірки	Швидка компрометація акаунта, доступ до корпоративних ресурсів	Успішні входи без другого фактора, масові спроби входу
Надмірні привілеї	Акаунт має ширші права, ніж потрібно для роботи	Зміна політик, видалення ресурсів, доступ до критичних даних	Використання адміністративних функцій звичайним користувачем
Активні акаунти колишніх працівників	Обліковий запис не заблоковано після звільнення	Несанкціонований доступ після завершення трудових відносин	Вхід неактивного користувача, активність після дати звільнення
Компрометація API-ключа	Ключ потрапляє до репозиторію, журналу або стороннього сервісу	Доступ до API, автоматизоване копіювання або зміна даних	Нетипові API-запити, різке збільшення кількості операцій
Неконтрольований сервісний акаунт	Сервісний обліковий запис має постійні або надмірні права	Переміщення між ресурсами, створення нових ключів, прихований доступ	Активність сервісного акаунта поза типовим сценарієм
Відсутність журналювання	Події доступу не фіксуються або зберігаються недостатньо довго	Складність розслідування інциденту, неможливість встановити джерело атаки	Відсутність логів, прогалини в історії подій, вимкнення аудиту

Атаки на управління доступом слід оцінювати не тільки за способом початкового входу, а й за умовами, які дозволяють зловмиснику розвивати атаку. Фішинг або викрадення пароля створюють лише перший етап ризику; подальші наслідки залежать від наявності MFA, обсягу привілеїв, контролю сервісних ідентичностей та якості журналювання.

Рівень небезпеки окремих векторів атак відрізняється, оскільки одні з них створюють лише початковий доступ, а інші дають змогу швидко розширити контроль над хмарним середовищем.

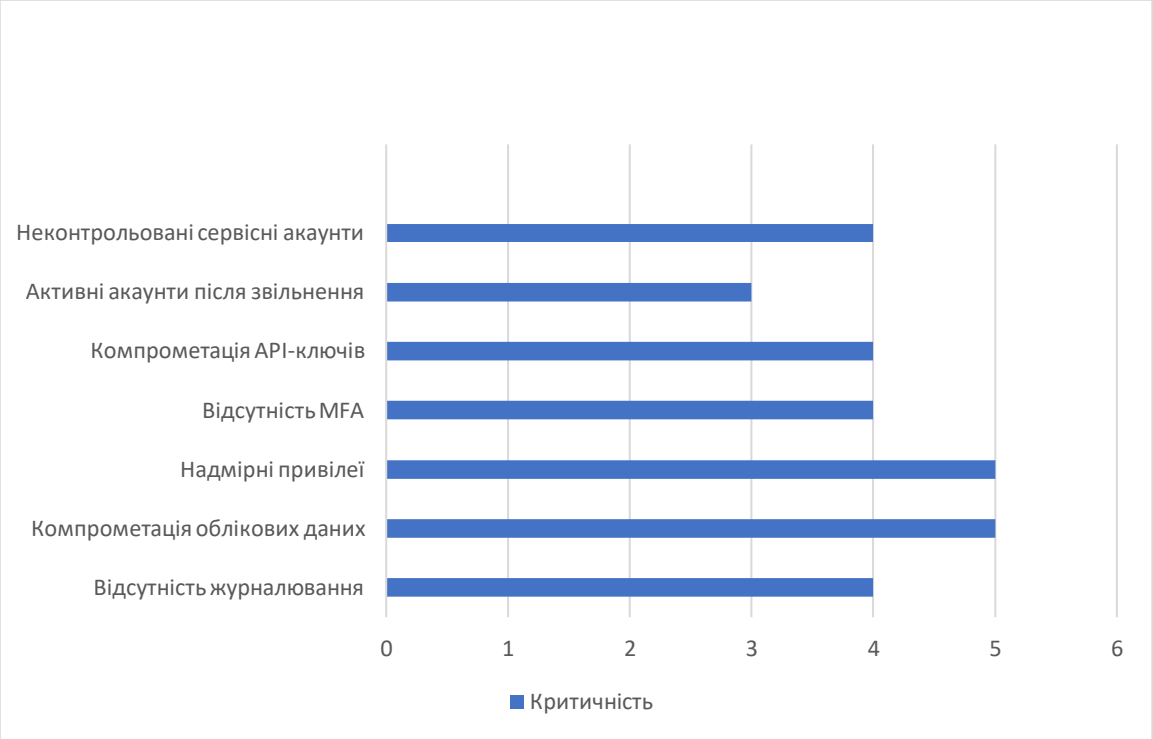

Рис. 2.5. Оцінка критичності основних векторів атак на управління доступом

Найвищу критичність отримують компрометація облікових даних і надмірні привілеї, оскільки саме їх поєднання створює умови для швидкого переходу від початкового доступу до контролю над даними або конфігураціями. Відсутність MFA, компрометація API-ключів і неконтрольовані сервісні акаунти мають дещо нижчу, але також високу критичність, оскільки часто залишаються непомітними без якісного журналювання.

З аналітичної точки зору найбільш небезпечними є не окремі слабкі місця, а їх поєднання. Наприклад, викрадений пароль сам по собі не завжди призводить до критичного інциденту, якщо в організації використовується багатофакторна автентифікація, обмежені ролі та контроль входів із нових пристроїв. Однак за відсутності MFA, наявності надмірних привілеїв і недостатнього журналювання атака може швидко перейти від початкового доступу до повної компрометації середовища. Саме тому аналіз атак на управління доступом повинен враховувати

не лише факт наявності вразливості, а й сукупність умов, які дозволяють зловмиснику розвивати атаку.

Особливої уваги потребує проблема життєвого циклу доступів. У корпоративній хмарі права користувачів і сервісів постійно змінюються: працівники переходять між підрозділами, підрядники завершують роботу, застосунки оновлюються, а автоматизовані процеси отримують нові дозволи. Якщо організація не проводить регулярний перегляд доступів, у середовищі накопичуються зайві ролі, неактивні акаунти, застарілі токени та сервісні облікові записи з невиправдано широкими правами. Такі елементи формують приховану поверхню атаки, яку складно виявити без централізованого аудиту [8, 18, 19].

Отже, атаки, пов’язані з управлінням доступом, обліковими записами та надмірними привілеями, є одним із найбільш небезпечних напрямів загроз для корпоративної хмари. Їхня небезпека полягає в тому, що зловмисник може діяти під виглядом легітимного користувача або сервісу, використовуючи наявні права доступу. Найбільш критичними чинниками є компрометація облікових даних, відсутність багатофакторної автентифікації, надмірні привілеї, неконтрольовані API-ключі, сервісні акаунти та недостатнє журналювання. Це підтверджує необхідність застосування принципу найменших привілеїв, регулярного аудиту доступів, моніторингу поведінки користувачів і посиленої автентифікації, що буде розглянуто в третьому розділі роботи.

2.3. Аналіз атак, спричинених помилками конфігурації хмарних ресурсів

Конфігураційні помилки є одним із найпоширеніших джерел ризику в хмарному середовищі, оскільки вони можуть створювати небезпечний стан ресурсу ще до початку активних дій зловмисника. Йдеться про ситуації, коли сховище, база даних, віртуальна машина, API, контейнер або службовий інтерфейс налаштовані ширше, ніж це потрібно для роботи організації [10, 18, 19].

У попередньому підрозділі основну увагу було приділено атакам, пов’язаним з управлінням доступом, обліковими записами та надмірними привілеями. У таких сценаріях зловмисник намагається отримати можливість діяти в системі від імені легітимного користувача або сервісу. Помилки конфігурації мають іншу природу: вони можуть створити небезпечний стан ресурсу ще до активних дій зловмисника. Тобто проблема виникає не тоді, коли захист уже подолано, а тоді, коли самі налаштування середовища не забезпечують належного рівня обмеження доступу, контролю змін або фіксації подій.

У корпоративній хмарі конфігураційні помилки виникають через поєднання технічних, організаційних і процедурних чинників. Найбільш характерними серед них є такі:

1) *Швидке створення ресурсів без повної перевірки параметрів безпеки.*

Хмарна інфраструктура дозволяє швидко розгортати нові сервіси, сховища, віртуальні машини, бази даних і контейнери. Це зручно для бізнесу та розробки, однак за відсутності контролю може призвести до запуску ресурсів зі стандартними або недостатньо захищеними налаштуваннями.

2) *Відсутність єдиного підходу до налаштування хмарних сервісів.*

Якщо адміністратори, розробники або DevOps-фахівці самостійно визначають параметри доступу без узгоджених правил, у середовищі можуть з’являтися суперечливі конфігурації. Один ресурс може мати суворо обмежений доступ, тоді як інший — залишатися відкритим для зовнішніх підключень.

3) *Недостатній контроль змін у хмарній інфраструктурі.*

Хмарне середовище постійно змінюється: ресурси створюються, масштабуються, переносяться, інтегруються з іншими сервісами або видаляються. Якщо організація не відстежує такі зміни, небезпечні параметри можуть залишатися активними тривалий час і не виявлятися під час щоденного адміністрування.

4) Помилкове трактування моделі спільної відповідальності.

Частина організацій може вважати, що після переходу до хмари більшість питань безпеки автоматично переходить до провайдера. Насправді провайдер відповідає за базову інфраструктуру та окремі вбудовані механізми захисту, але налаштування доступу, ролей, журналювання, шифрування, мережевих правил і політик безпеки залишаються зоною відповідальності організації.

5) Використання тестових, тимчасових і застарілих ресурсів.

У процесі розробки, тестування або міграції можуть створюватися тимчасові сервери, демонстраційні бази даних, тестові сховища або експериментальні середовища. Якщо після завершення робіт такі об’єкти не видаляються, не ізолюються і не перевіряються, вони можуть стати непомітним джерелом ризику.

6) Відсутність регулярного аудиту конфігурацій.

Навіть безпечне на момент створення налаштування з часом може втратити актуальність. Зміна ролей, інтеграцій, мережевих правил або бізнес-процесів може створити нові ризики. Без періодичної перевірки організація не завжди здатна своєчасно виявити відкриті порти, публічні сховища, вимкнене журналювання або надмірно широкі дозволи [18, 19].

На практиці конфігураційні помилки можуть проявлятися у різних формах, зокрема:

- публічний доступ до хмарних сховищ;
- відкриті бази даних або адміністративні інтерфейси;
- надмірно широкі мережеві правила;
- відкриті службові порти;
- вимкнене або неповне журналювання подій;
- відсутність шифрування даних;
- використання небезпечних стандартних налаштувань;
- активні тестові або застарілі ресурси;
- неправильні політики резервного копіювання;
- неконтрольовані інтеграції між хмарними сервісами.

Небезпека таких помилок полягає в тому, що вони можуть спростити дії зловмисника. Якщо сховище, база даних або службовий інтерфейс уже доступні ззовні, атака може початися не з подолання захисних механізмів, а з виявлення неправильно налаштованого ресурсу. У цьому випадку організація фактично сама створює умови для інциденту, оскільки ресурс перебуває у небезпечному стані ще до моменту активного втручання зловмисника.

Для системного аналізу конфігураційні помилки доцільно розглядати не як окремі технічні недоліки, а як сукупність ризиків, що впливають на різні компоненти корпоративної хмари: дані, мережеву інфраструктуру, облікові записи, журнали подій, резервні копії, тестові середовища та інтеграції. Такий підхід дозволяє оцінити не лише сам факт помилки, а й можливий сценарій її використання, наслідки для організації та складність своєчасного виявлення інциденту.

Таблиця 2.3

Аналіз ризиків, пов’язаних із помилками конфігурації хмарних ресурсів [6, 8, 10]

Категорія помилки конфігурації	**Ймовірний сценарій атаки**	**Потенційні наслідки**	**Рівень ризику**
Публічний доступ до хмарного сховища	Зловмисник виявляє відкритий ресурс і отримує доступ до його вмісту без належної автентифікації	Витік даних, копіювання службової інформації, розкриття резервних копій або технічних параметрів середовища	Критичний
Відкриті бази даних або адміністративні інтерфейси	Ресурс доступний з Інтернету через надмірно широкі мережеві правила або відсутність обмеження за джерелом підключення	Несанкціонований перегляд, зміна або видалення даних, порушення роботи сервісу	Критичний

Категорія помилки конфігурації	**Ймовірний сценарій атаки**	**Потенційні наслідки**	**Рівень ризику**
Надмірно широкі мережеві правила	Дозволено підключення з будь-яких IP-адрес або відкрито порти, які не потрібні для роботи сервісу	Сканування ресурсу, спроби підбору облікових даних, атаки на вразливі служби	Високий
Вимкнене або неповне журналювання	Дії користувачів, зміни конфігурацій або підозрілі операції не фіксуються повністю	Пізнє виявлення інциденту, ускладнення розслідування, неможливість відновити послідовність дій зловмисника	Високий
Відсутність шифрування даних	У разі доступу до ресурсу інформація може бути прочитана без додаткового подолання криптографічного захисту	Розкриття конфіденційної інформації, підвищення наслідків витоку	Високий
Неконтрольовані тестові середовища	Тимчасовий ресурс залишається активним після завершення робіт або має слабші правила безпеки, ніж основне середовище	Використання тестового середовища як точки входу, доступ до реальних даних або пов’язаних сервісів	Високий
Невикористовувані або “забуті” ресурси	Ресурс не оновлюється, не перевіряється та не контролюється відповідальними фахівцями	Компрометація застарілого компонента, доступ до залишкових даних, використання старих інтеграцій	Середній / високий
Небезпечні стандартні налаштування	Ресурс запускається зі стандартними параметрами без адаптації до вимог безпеки організації	Надмірні дозволи, відкритий доступ, слабкий контроль змін	Середній

Найбільш критичними є ті конфігураційні помилки, які безпосередньо відкривають доступ до даних або адміністративних функцій. Публічні сховища, відкриті бази даних, доступні з Інтернету службові інтерфейси та надмірно

широкі мережеві правила створюють умови, за яких зловмисник може почати атаку без подолання складних захисних механізмів [10, 18, 19].

Водночас частина конфігураційних помилок не завжди одразу призводить до несанкціонованого доступу, але значно посилює наслідки інциденту. Наприклад, вимкнене журналювання не відкриває ресурс напряму, проте ускладнює виявлення атаки та подальше розслідування. Відсутність шифрування збільшує шкоду у разі витоку даних, а неконтрольовані тестові середовища або застарілі ресурси створюють приховані точки входу, які можуть не враховуватися в основній системі захисту.

Найвищий рівень ризику виникає тоді, коли в одному середовищі одночасно присутні кілька конфігураційних недоліків. Наприклад, публічне сховище саме по собі створює загрозу витоку інформації. Якщо в ньому додатково зберігаються резервні копії, конфігураційні файли або службові журнали, зловмисник може отримати не лише доступ до даних, а й інформацію для подальшого розвитку атаки. Отже, критичність помилки визначається не тільки її типом, а й тим, з якими іншими недоліками вона поєднується.

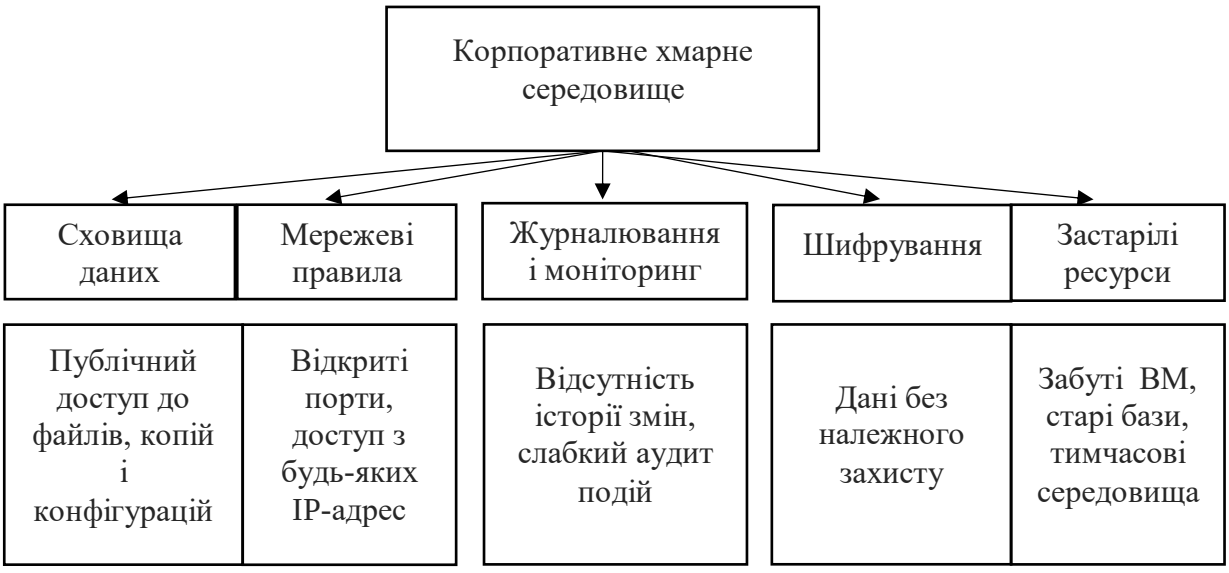

Рис. 2.6. Карта конфігураційних ризиків корпоративного хмарного середовища

Конфігураційні ризики доцільно оцінювати не за окремими ресурсами, а за їхнім зв’язком із даними, мережевими правилами, журналюванням, шифруванням і актуальністю середовища. Наприклад, відкритий ресурс становить значно вищу загрозу, якщо він містить чутливі дані, пов’язаний із

привілейованими ролями або не фіксується в журналах подій. Тому аналіз конфігураційних помилок має враховувати не лише сам факт неправильного налаштування, а й можливий ланцюг наслідків для всієї корпоративної хмари.

Особливо важливо враховувати взаємозв'язок між різними групами ризиків. Наприклад, відкритий доступ до сховища створює загрозу витоку даних, але за наявності неповного журналювання організація може не мати достатніх доказів для встановлення факту інциденту. Аналогічно, тестове середовище саме по собі може не містити критичних сервісів, однак за наявності реальних даних, старих ключів або підключення до основної інфраструктури воно перетворюється на небезпечний канал доступу.

Одним із найбільш критичних проявів конфігураційних помилок є публічний доступ до хмарних сховищ і баз даних. У корпоративному середовищі такі ресурси часто використовуються для зберігання документів, резервних копій, журналів подій, експортів баз даних, файлів конфігурації та службової інформації.

Небезпека відкритих сховищ полягає не лише у самому факті доступності файлів. У багатьох випадках у таких ресурсах можуть зберігатися дані, які допомагають розвинути атаку: резервні копії баз даних, службові журнали, токени, конфігураційні файли або внутрішня документація. Тому наслідки помилки можуть виходити за межі одного ресурсу й охоплювати інші елементи корпоративної хмари.

Відкриті бази даних або адміністративні інтерфейси створюють ще вищий рівень ризику, оскільки можуть впливати не тільки на конфіденційність, а й на цілісність та доступність інформації. У разі доступу до такої бази зловмисник може не лише переглянути дані, а й змінити записи, видалити інформацію або порушити роботу сервісу. Для організації це може означати втрату контролю над критичними бізнес-процесами, фінансові збитки та репутаційні наслідки.

Іншим поширеним джерелом ризику є надмірно широкі мережеві правила. У хмарному середовищі адміністратори самостійно визначають, які сервіси доступні з Інтернету, які порти відкриті та з яких IP-адрес дозволено

підключення. Якщо ці правила налаштовано занадто широко, ресурс стає доступним для значно більшої кількості суб’єктів, ніж це потрібно для його нормальної роботи.

Особливо небезпечними є випадки, коли з Інтернету доступні адміністративні панелі, бази даних, SSH/RDP-підключення, службові API або системи керування контейнерами. Навіть якщо такі сервіси захищені паролем, сам факт їхньої відкритості збільшує ризик сканування, підбору облікових даних або використання відомих вразливостей. У такій ситуації помилка конфігурації фактично розширює поверхню атаки та створює додаткове навантаження.

Початковий недолік у налаштуваннях може поступово перетворитися на повноцінний інцидент: від виявлення доступного ресурсу до отримання доступу, розвитку атаки, витоку даних або порушення роботи сервісів.

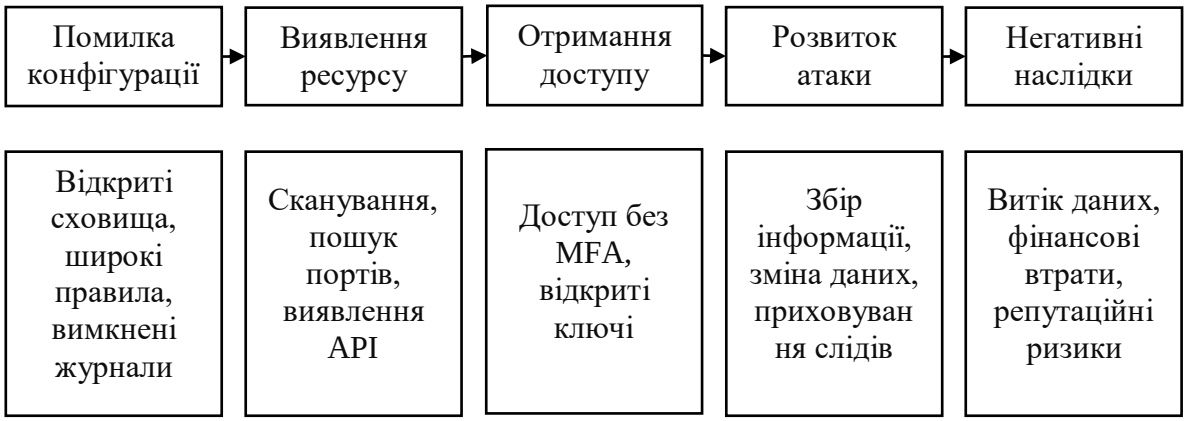

Рис. 2.7. Сценарій розвитку атаки через помилку конфігурації хмарного ресурсу

Початкова помилка конфігурації може перерости у повноцінний інцидент, якщо вона поєднується з відкритим доступом, слабким контролем привілеїв і недостатнім журналюванням. У такому випадку зловмисник отримує не лише доступ до окремого ресурсу, а й можливість розвивати атаку в напрямі витоку даних, порушення роботи сервісу або приховування слідів активності.

Найвищий рівень ризику мають комбіновані сценарії, у яких конфігураційна помилка поєднується з іншими недоліками безпеки. Наприклад, відкрите сховище становить загрозу конфіденційності, але за наявності надмірних прав сервісного акаунта воно може стати джерелом подальшого доступу до інших ресурсів. Вимкнене журналювання, у свою чергу, не створює прямого доступу

для зловмисника, але ускладнює встановлення факту атаки та її хронології. Тому конфігураційні помилки доцільно оцінювати не лише за самим фактом порушення налаштувань, а й за тим, які дані, ролі, мережеві доступи та журнали пов’язані з відповідним ресурсом.

Отже, атаки, спричинені помилками конфігурації, є одним із ключових напрямів ризику для корпоративної хмари. Вони можуть виникати без складного технічного злому та часто пов’язані з неправильним адмініструванням, відсутністю контролю змін, недостатнім аудитом і помилковим розумінням меж відповідальності організації. Проведений аналіз підтверджує необхідність системного контролю конфігурацій, інвентаризації ресурсів, моніторингу змін і застосування спеціалізованих засобів виявлення небезпечних налаштувань, що буде розглянуто в третьому розділі роботи.

Висновки до розділу 2

У другому розділі було проаналізовано сучасні вектори атак на корпоративні хмарні середовища. Встановлено, що загрози хмарній інфраструктурі мають комплексний характер і формуються на перетині технічних, організаційних та процедурних чинників. На відміну від традиційної локальної інфраструктури, корпоративна хмара не має чітко визначеного фізичного периметра, а доступ до ресурсів здійснюється через облікові записи, ролі, API, сервісні інтеграції та віддалені канали зв’язку.

Аналіз показав, що одним із найбільш небезпечних напрямів атак є компрометація ідентичностей та порушення процесів управління доступом. Викрадені облікові дані, відсутність багатофакторної автентифікації, надмірні привілеї, активні акаунти колишніх працівників, неконтрольовані сервісні облікові записи та API-ключі створюють умови для несанкціонованого доступу до хмарних ресурсів. Особливу небезпеку становить ситуація, коли зловмисник діє під виглядом легітимного користувача або сервісу, оскільки така активність може тривалий час не відрізнятися від звичайної роботи системи.

Окремо встановлено, що значна частина ризиків пов’язана з помилками конфігурації хмарних ресурсів. Відкриті сховища, надмірно широкі мережеві

правила, доступні з Інтернету адміністративні інтерфейси, вимкнене журналювання, відсутність шифрування, тестові середовища та застарілі ресурси можуть створювати умови для витоку даних, порушення цілісності інформації або ускладнення розслідування інцидентів. При цьому критичність конфігураційної помилки залежить не лише від її типу, а й від контексту: характеру даних, рівня привілеїв, доступності ресурсу з Інтернету та наявності журналів подій.

Проведений аналіз підтвердив, що захист корпоративної хмари не може обмежуватися окремим технічним засобом. Найбільш небезпечні сценарії виникають тоді, коли кілька слабких місць поєднуються між собою: викрадений пароль використовується без MFA, акаунт має надмірні права, ресурс налаштований небезпечно, а журналювання не сприяє своєчасному виявленню атак. Саме тому в третьому розділі доцільно перейти до розробки практичних заходів захисту, зокрема багаторівневого контролю доступу, застосування IAM, MFA, RBAC, ABAC, контролю сервісних акаунтів, моніторингу подій і виявлення конфігураційних помилок за допомогою CSPM-рішень.

РОЗДІЛ 3 ПРАКТИЧНІ ЗАХОДИ ЗАХИСТУ КОРПОРАТИВНОГО ХМАРНОГО СЕРЕДОВИЩА

3.1 Технічні засоби захисту хмарного середовища: IAM, MFA, RBAC, ABAC та моніторинг доступу

Результати аналізу другого розділу показали, що найбільш небезпечні атаки на корпоративні хмарні середовища часто пов’язані не з прямим зламом інфраструктури провайдера, а з використанням слабких місць на стороні самої організації. До таких слабких місць належать скомпрометовані облікові записи, надмірні привілеї, неактивні акаунти, неконтрольовані сервісні облікові записи, API-ключі без ротації та недостатнє журналювання подій [8]. Тому захист хмарного середовища доцільно будувати не навколо одного окремого інструмента, а як багаторівневу систему контролю доступу [5, 6].

У межах цього підрозділу запропоновано підхід, за якого доступ до хмарних ресурсів проходить кілька послідовних рівнів перевірки: ідентифікацію користувача або сервісу, автентифікацію, перевірку IAM-політик, оцінювання ролі, аналіз контексту запиту, обмеження привілеїв і журналювання виконаної дії. Така логіка відповідає принципам Zero Trust, оскільки жоден запит не вважається безпечним автоматично лише через факт входу до системи.

Для обґрунтування запропонованого рішення доцільно зіставити основні ризики, виявлені під час аналізу атак, із технічними механізмами, які можуть їх зменшити. Такий підхід дозволяє перейти від загального опису засобів захисту до прикладної моделі, у якій кожен елемент виконує конкретну функцію: запобігає початковій компрометації, обмежує наслідки атаки, підвищує контрольованість середовища або забезпечує розслідування інциденту.

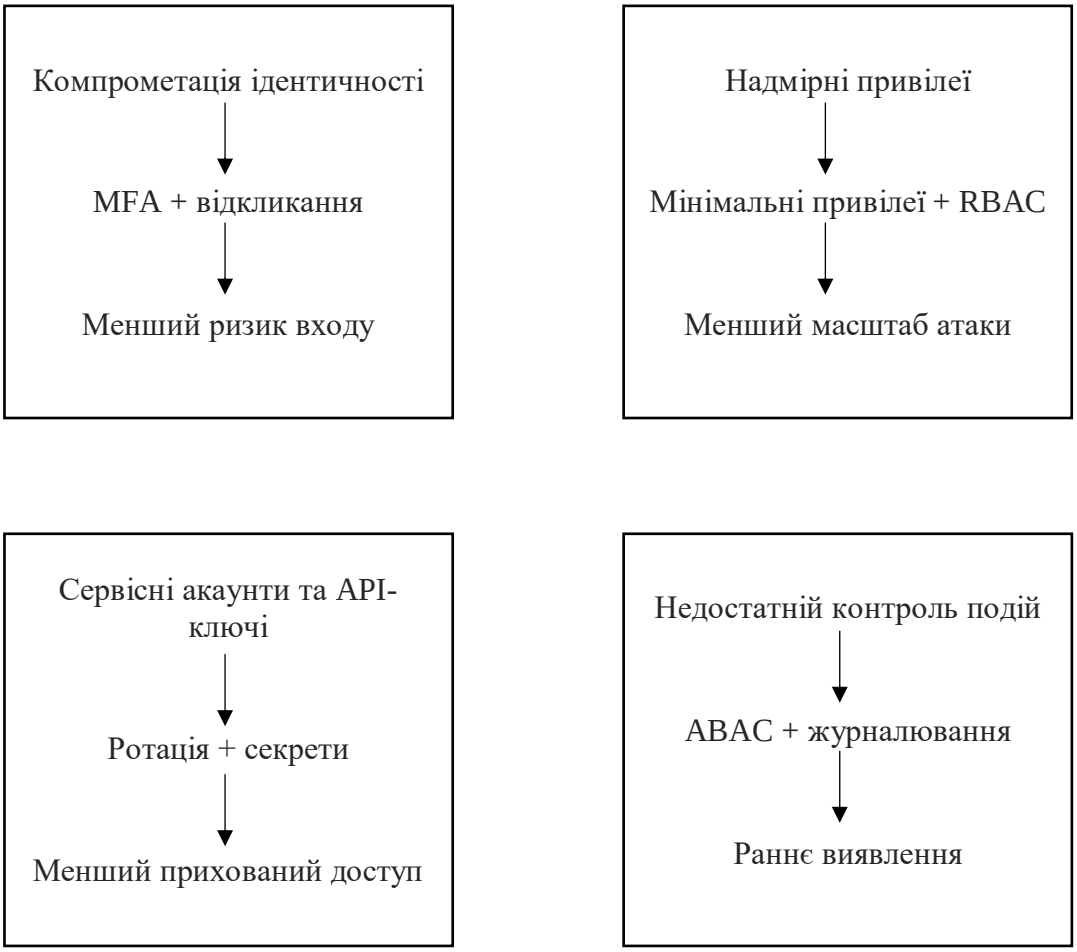

Рис. 3.1. Відповідність загроз, технічних рішень і результатів захисту доступу в корпоративній хмарі

Захист доступу в корпоративній хмарі має відповідати конкретним ризикам. Компрометація ідентичності потребує посиленої автентифікації та швидкого відкликання доступу, надмірні привілеї — принципу найменших прав і рольової моделі, а ризики сервісних акаунтів та API-ключів — ротації, обмеження дозволів і захищеного зберігання секретів [8, 11].

Для зниження ризиків компрометації облікових записів і надмірних привілеїв запропоновано багаторівневу модель контролю доступу. Кожен запит користувача, сервісного акаунта або застосунку проходить послідовну перевірку: ідентифікацію, автентифікацію, IAM-політики, роль, контекст, привілеї та журналювання дії [6, 8].

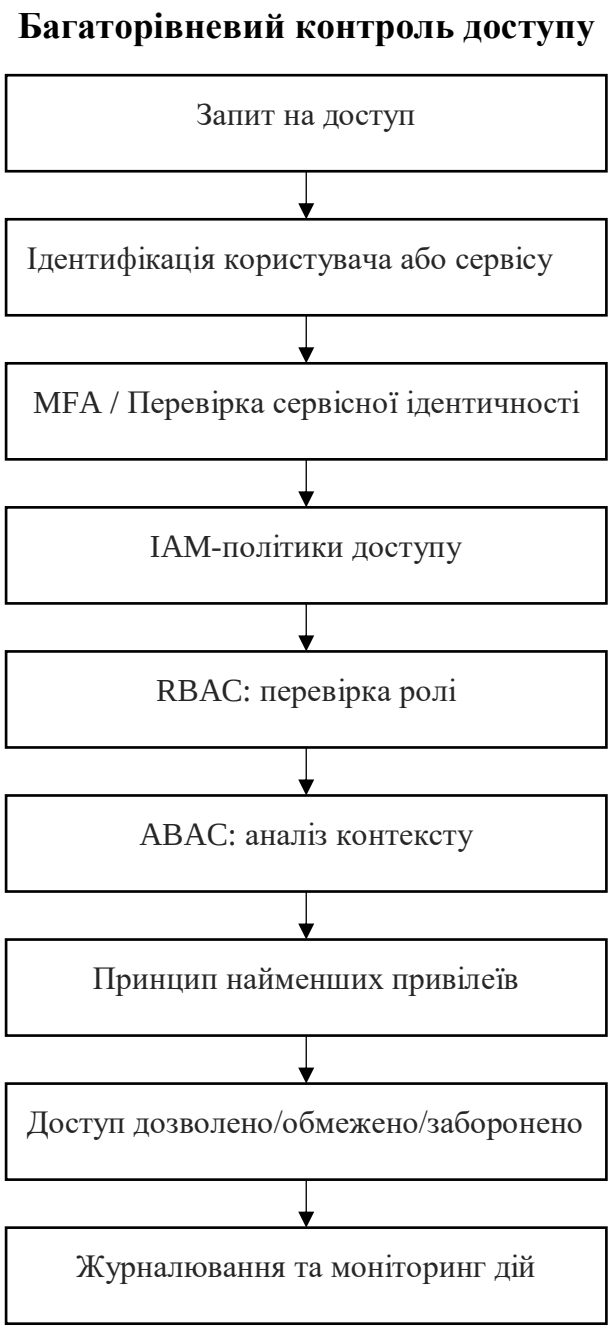

Рис. 3.2. Запропонована модель багаторівневого контролю доступу до хмарного ресурсу [8]

Доступ до хмарного ресурсу варто розглядати не як разову перевірку пароля, а як послідовний процес оцінювання запиту [20, 29]. Спочатку визначається суб’єкт доступу, далі перевіряються автентифікація, політики IAM, роль, контекст запиту та обсяг необхідних привілеїв. Спочатку визначається суб’єкт запиту — користувач, адміністратор, застосунок або сервісний обліковий запис, після чого перевіряються автентифікація, IAM-політики, роль і контекст доступу. Лише за результатами цих перевірок доступ може бути дозволений,

обмежений або заблокований, а виконана дія має фіксуватися в журналах для подальшого аналізу.

Практичне впровадження IAM має передбачати централізоване керування користувачами, використання груп і ролей замість індивідуального призначення прав, регулярний перегляд дозволів, контроль сервісних акаунтів, обмеження адміністративних функцій і видалення невикористаних доступів. Такий підхід дозволяє зменшити хаотичне призначення прав і створити зрозумілу структуру відповідальності за доступ до хмарних ресурсів.

Таблиця 3.1

Практичні правила застосування IAM у корпоративній хмарі

Напрям контролю	**Рекомендована дія**	**Очікуваний ефект**
Користувачі	Створювати облікові записи через централізований каталог і групи	Спрощення управління і зменшення випадкових доступів
Ролі	Формувати типові ролі для адміністраторів, аудиторів, розробників і користувачів	Зменшення хаотичного призначення дозволів
Привілеї	Надавати лише мінімально необхідні дозволи	Обмеження наслідків компрометації
Сервісні акаунти	Прив'язувати до конкретного процесу або застосунку	Уникнення невідомих або зайвих автоматизованих доступів
API-ключі	Застосовувати ротацію, обмеження за ресурсами та захищене зберігання	Зниження ризику використання викрадених секретів
Перегляд доступів	Проводити періодичний аудит ролей, ключів і невикористаних акаунтів	Виявлення застарілих і надмірних прав

Центральним правилом IAM у корпоративній хмарі має бути принцип найменших привілеїв. Його практичний зміст полягає в тому, що користувач, роль або сервісний обліковий запис отримує лише ті дозволи, які потрібні для конкретного завдання.

Окремого значення набуває управління життєвим циклом доступу. У корпоративній хмарі права користувачів, сервісних облікових записів і автоматизованих процесів не залишаються сталими, оскільки середовище

постійно змінюється. Найчастіше потреба в перегляді доступів виникає у таких випадках:

- працівник переходить до іншого підрозділу або змінює посаду;
- підрядник завершує виконання робіт за проєктом;
- застосунок оновлюється або отримує нові функції;
- автоматизований процес потребує тимчасового доступу до додаткових ресурсів;
- сервісний обліковий запис більше не використовується, але залишається активним.

Якщо ці зміни не контролюються, у хмарному середовищі поступово накопичуються неактивні акаунти, застарілі токени, невикористані ролі та надмірні привілеї. У результаті доступ, який спочатку був потрібний для виконання конкретного завдання, з часом може перетворитися на додаткову точку ризику для корпоративної хмари.

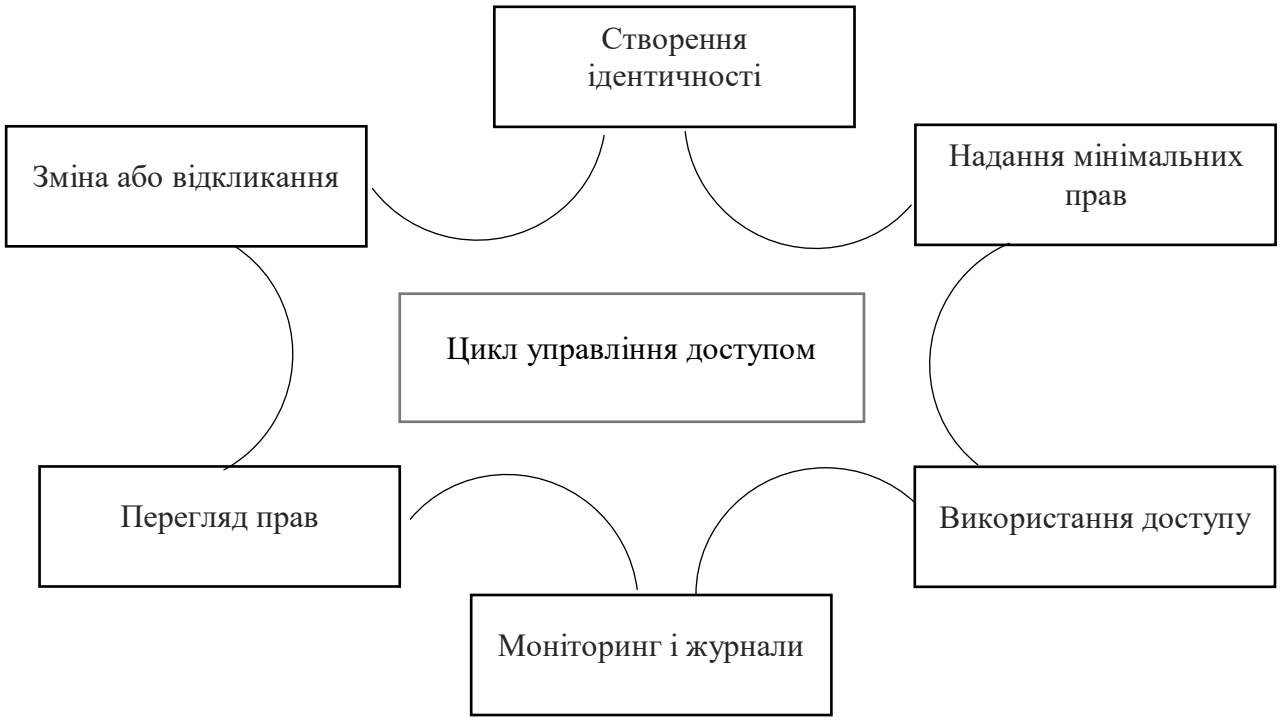

Рис. 3.3. Життєвий цикл управління доступом у корпоративній хмарі

Управління доступом доцільно розглядати як безперервний цикл, а не як одноразове створення облікового запису. На етапі створення ідентичності визначається, кому саме потрібен доступ і для якої мети. На етапі надання прав користувач або сервісний акаунт отримує лише мінімально необхідні дозволи. Під час використання доступу його дії мають фіксуватися в журналах, а на етапі перегляду — оцінюватися відповідність прав актуальним службовим потребам. Завершальним етапом є зміна або відкликання доступу після звільнення працівника, завершення проєкту чи виявлення ризикової активності.

Додатковим рівнем захисту є MFA. Її доцільно застосовувати насамперед для адміністраторів, користувачів із доступом до критичних даних, облікових записів фінансових і технічних підрозділів, а також для входу до панелей керування хмарною інфраструктурою. Проте MFA не повинна розглядатися як самодостатній засіб захисту. Вона зменшує ризик використання викраденого пароля, але не усуває проблему надмірних привілеїв, небезпечних API-ключів або слабкого журналювання.

Для розмежування прав доступу в корпоративній хмарі варто поєднувати RBAC і ABAC.

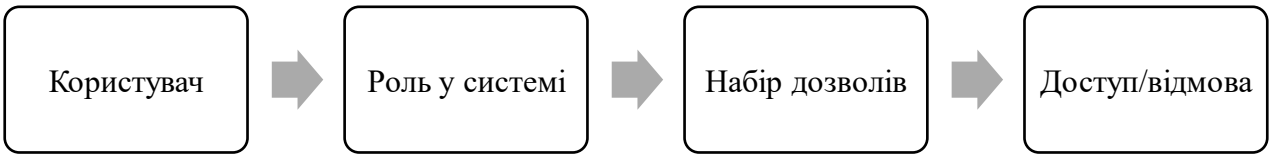

Рис. 3.4. Логіка RBAC у хмарному середовищі

RBAC забезпечує базовий розподіл прав за посадовими функціями, наприклад для адміністратора, аудитора, розробника або звичайного користувача.

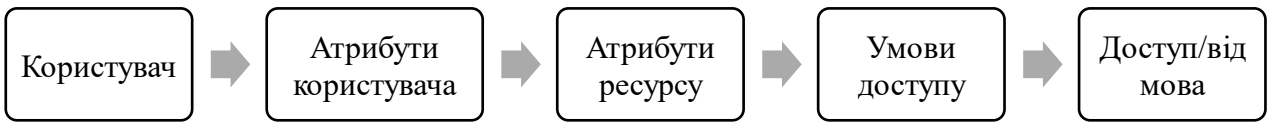

Рис. 3.5. Логіка ABAC у хмарному середовищі

ABAC доповнює цю модель контекстною перевіркою: враховує пристрій, локацію, час запиту, рівень ризику та тип ресурсу. У результаті доступ визначається не лише посадою користувача, а й умовами, за яких він намагається виконати дію.

Порівняння RBAC та ABAC показує, що статичної рольової моделі недостатньо для складного хмарного середовища. RBAC спрощує адміністрування, однак може призводити до надмірного укрупнення ролей. ABAC створює можливість точніше контролювати доступ у ризикових ситуаціях, наприклад під час входу з невідомого пристрою, незвичної локації або спроби отримати доступ до критичного ресурсу. Тому для корпоративної хмари доцільною є комбінована модель: RBAC визначає базові права, а ABAC уточнює рішення з урахуванням контексту.

Окремим рівнем запропонованої моделі є моніторинг і журналювання подій доступу. Їхнє завдання полягає не лише у збереженні інформації після інциденту, а й у ранньому виявленні підозрілої активності. У хмарному середовищі доцільно фіксувати успішні та невдалі входи, зміну ролей, створення нових ключів, зміну політик доступу, звернення до сховищ, видалення ресурсів, вимкнення журналювання та активність сервісних акаунтів.

Практичне значення журналювання полягає в тому, що воно дозволяє виявляти нетипові сценарії поведінки. Наприклад, вхід із незвичної країни, масове завантаження файлів, створення нового адміністративного акаунта або активність сервісного облікового запису поза типовим часом можуть свідчити про компрометацію. Без централізованого журналювання такі події залишаються розрізненими, а отже організація втрачає можливість швидко встановити джерело інциденту.

Таблиця 3.2

Події доступу, які доцільно контролювати в хмарному середовищі

Група подій	**Приклади подій**	**Безпекове значення**
Входи до системи	Успішні та невдалі входи, новий пристрій, незвична локація	Виявлення спроб компрометації облікового запису

Група подій	**Приклади подій**	**Безпекове значення**
Зміни прав	Призначення ролей, створення адміністративного акаунта, зміна IAM-політик	Контроль ескалації привілеїв
Ключі та токени	Створення, використання, ротація або видалення API-ключів	Виявлення небезпечних сервісних доступів
Доступ до даних	Масове завантаження, копіювання або видалення файлів	Раннє виявлення витоку або шифрування даних
Журнали	Вимкнення логування, зміна політик зберігання журналів	Виявлення спроб приховати сліди атаки

Особливу увагу в корпоративній хмарі потрібно приділяти сервісним обліковим записам, API-ключам і токенам доступу. На відміну від звичайних користувачів, такі ідентичності часто працюють автоматизовано і можуть залишатися активними тривалий час без перевірки. Це створює ризик прихованого доступу, оскільки зловмисник може використати скомпрометований ключ або токен без проходження звичайної процедури входу.

Зменшити цей ризик можна через окремі правила контролю сервісних ідентичностей: вести реєстр усіх сервісних акаунтів, обмежувати їхні права конкретними ресурсами, використовувати тимчасові облікові дані, проводити ротацію ключів, забороняти зберігання секретів у відкритих репозиторіях і фіксувати активність таких акаунтів у журналах подій. Це дозволяє зменшити ймовірність того, що автоматизований доступ стане неконтрольованим каналом проникнення до хмарного середовища. Запропоновану модель доцільно впроваджувати поетапно.

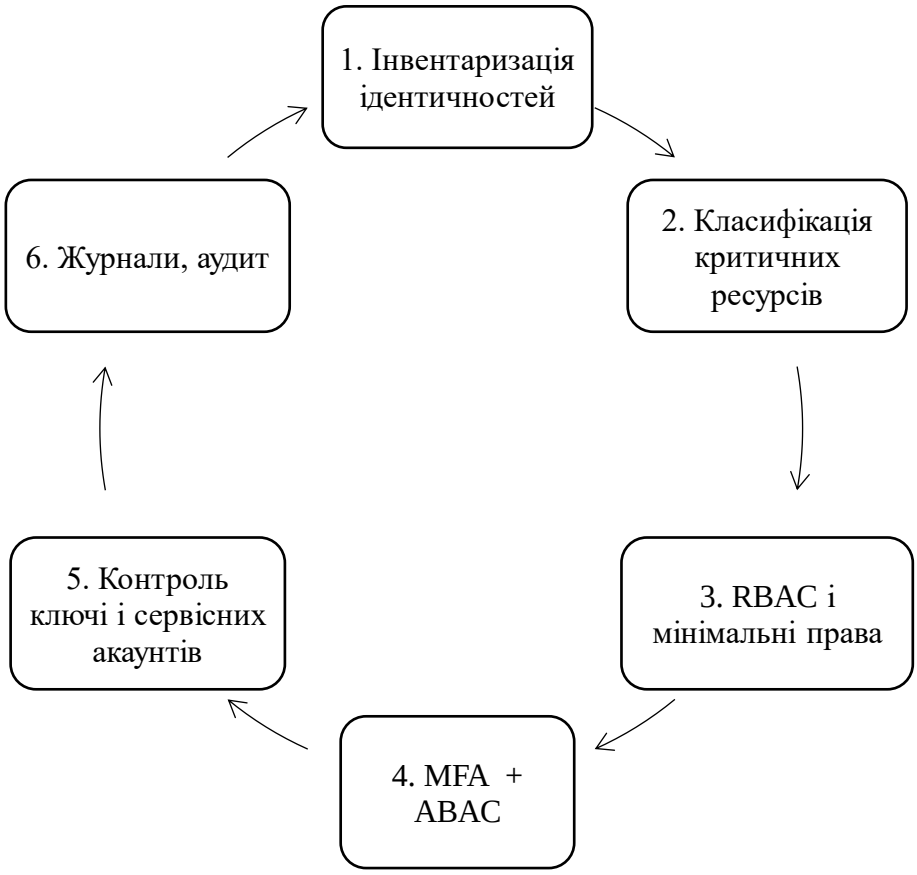

Рис. 3.6. Поетапне впровадження запропонованої моделі контролю доступу

Запропонована послідовність переводить управління доступом із реактивного режиму в превентивний. Зайві дозволи, неактивні акаунти, небезпечні ключі та ризикові підключення виявляються ще до того, як ними скористається зловмисник.

Для практичного застосування запропонованої моделі можна використовувати такий алгоритм впровадження:

1. провести інвентаризацію користувачів, ролей, сервісних акаунтів, API-ключів і токенів;

2. визначити критичні ресурси, зокрема бази даних, сховища, резервні копії, панелі адміністрування та журнали подій;

3. розподілити користувачів за типовими ролями на основі RBAC;

4. обмежити кожну роль мінімально необхідними дозволами;

5. застосувати MFA для адміністраторів і користувачів із доступом до критичних ресурсів;

6. для ризикових сценаріїв застосувати ABAC: перевірку пристрою, локації, часу доступу та типу ресурсу;

7. замінити постійні API-ключі тимчасовими обліковими даними там, де це можливо;

8. налаштувати централізоване журналювання входів, змін ролей, створення ключів і доступу до даних;

9. встановити періодичний перегляд прав доступу;

10. автоматизувати відкликання доступу після звільнення працівника або завершення проєкту.

Такий алгоритм дозволяє зробити контроль доступу не формальною процедурою, а постійним процесом управління ризиками. Його перевага полягає у тому, що кожен рівень захисту компенсує слабкі сторони іншого: MFA ускладнює початковий вхід, RBAC і найменші привілеї обмежують дозволи, ABAC враховує контекст, а журналювання забезпечує контроль подій і можливість подальшого аналізу.

Отже, у межах підрозділу запропоновано багаторівневу модель контролю доступу до корпоративного хмарного середовища. Вона поєднує IAM, MFA, RBAC, ABAC, принцип найменших привілеїв, управління життєвим циклом доступів, контроль сервісних ідентичностей і централізоване журналювання. На відміну від ізольованого використання окремих засобів, така модель створює можливіть одночасно зменшити ризик початкової компрометації, обмежити дії користувача після входу, врахувати контекст запиту та забезпечити виявлення підозрілої активності.

Розглянуте рішення безпосередньо відповідає загрозам, розглянутим у другому розділі: компрометації облікових записів, надмірним привілеям, неконтрольованим сервісним акаунтам, скомпрометованим API-ключам і слабкому журналюванню. Водночас контроль доступу не усуває всіх ризиків хмарного середовища, оскільки значна частина інцидентів виникає через помилки конфігурації ресурсів, відкриті сховища, неправильні мережеві правила або відсутність контролю змін. Тому наступним напрямом захисту є виявлення

й усунення конфігураційних помилок за допомогою CSPM-рішень і політик безпеки.

3.2 Засоби виявлення та усунення помилок конфігурації: CSPM та політики безпеки

Небезпечний сценарій може виникнути не через злам хмарного провайдера, а через помилкове налаштування ресурсу: публічне сховище, надто широке мережеве правило, вимкнене шифрування, неповне журналювання або тестовий сервіс, який залишився доступним після завершення робіт. Тому другим практичним напрямом захисту є системне виявлення і виправлення конфігураційних відхилень.

У цьому підрозділі запропоновано підхід, за якого контроль конфігурацій розглядається як постійний цикл, а не як разова перевірка перед аудитом. Основою такого підходу є CSPM, політики безпечних налаштувань і ризик-орієнтована пріоритизація. CSPM доцільно трактувати не як звичайний сканер, а як механізм, що підтримує актуальну видимість хмарних активів, порівнює їхній стан із політиками, визначає критичність відхилень і контролює виконання виправлень. У документації Microsoft CSPM описується як засіб постійної оцінки безпекової позиції хмарних активів і навантажень із рекомендаціями щодо її покращення в Azure, AWS та GCP [15].

Конфігураційні помилки мають специфічну природу: вони не завжди є вразливостями у класичному розумінні. Ресурс може працювати без технічного збою і не містити відомої CVE-вразливості, однак його параметри можуть створювати шлях для атаки. Наприклад, сховище може дозволяти зовнішнє читання файлів, віртуальна машина може мати надмірні дозволи, а Kubernetes-кластер може мати доступний API-сервер без достатніх обмежень. Через це оцінювати потрібно не тільки сам факт помилки, а й контекст: які дані містить ресурс, хто має до нього доступ, чи видно його з Інтернету і чи можна через нього перейти до інших сервісів.

Практична проблема полягає ще й у масштабі хмарного середовища. Ресурси створюються автоматизовано, змінюються через Infrastructure as Code,

підключаються до сторонніх сервісів і можуть існувати в кількох хмарах одночасно. Без єдиної моделі контролю організація бачить лише окремі попередження, але не завжди розуміє, які з них формують реальну загрозу. Тому CSPM у межах корпоративної хмари має виконувати не лише функцію виявлення помилок, а й функцію управління ризиком: формувати видимість ресурсів, перевіряти їх відповідність політикам, визначати критичність відхилень і контролювати процес усунення.

Рис. 3.7. Цикл виявлення та усунення помилок конфігурації у хмарному середовищі

Контроль конфігурацій у хмарному середовищі має бути безперервним процесом, оскільки стан ресурсів постійно змінюється через розгортання нових сервісів, автоматизовані сценарії та ручні дії адміністраторів. Після інвентаризації активів їхні налаштування порівнюються з політиками безпеки, оцінюються за рівнем ризику та передаються на виправлення відповідальним фахівцям.

Таблиця 3.3

Типові конфігураційні помилки та способи їх виявлення

Тип помилки	**Можливий ризик**	**Механізм перевірки**
Публічне хмарне сховище	Несанкціоноване читання або копіювання файлів, резервних копій чи службових даних	Перевірка bucket/container policy, ACL, умов спільного доступу та класифікації даних
Надмірно відкриті мережеві правила	Сканування сервісу з Інтернету, підбір паролів або експлуатація відкритого інтерфейсу	Аналіз security groups, firewall rules, відкритих портів і дозволів 0.0.0.0/0
Вимкнене шифрування	Зростання наслідків витоку або несанкціонованого копіювання даних	Контроль шифрування дисків, сховищ, баз даних і використання ключів KMS

Тип помилки	Можливий ризик	Механізм перевірки
Неповне журналювання	Складність встановлення джерела інциденту та відновлення хронології подій	Перевірка audit logs, строків зберігання журналів і передавання подій до централізованого сховища
Стандартні або дефолтні налаштування	Наявність неврахованих акаунтів, типових ролей або параметрів без hardening	Виявлення стандартних політик, дефолтних сервісних акаунтів і ресурсів без базового посилення
Надмірні права сервісних акаунтів	Прихована ескалація привілеїв або доступ до суміжних ресурсів	Аналіз permissions, невикористаних сервісних ідентичностей, ключів і пов'язаних ролей
Незахищені Kubernetes-кластери	Доступ до API-сервера, секретів, workload-ідентичностей або вузлів	Перевірка доступності API, RBAC, секретів, node role і мережевих політик

Одна й та сама помилка може мати різний рівень небезпеки залежно від контексту. Відкрите сховище з персональними даними потребує швидкого реагування, тоді як тестовий ресурс без чутливої інформації може бути виправлений у плановому режимі. Так само відкритий адміністративний порт на машині з привілейованою роллю є небезпечнішим, ніж відкритий службовий порт у відокремленому тестовому сегменті. Отже, простого переліку помилок недостатньо: CSPM має показувати, які відхилення можуть перетворитися на реальний шлях атаки.

Актуальність такого підходу підтверджується прикладними дослідженнями хмарної безпеки. У звіті Datadog State of Cloud Security 2025 зазначено, що ризикові дозволи мають 13% Amazon EKS-кластерів і 11% Google Cloud GKE-кластерів; крім того, 19,4% EC2-інстансів є надмірно привілейованими, а 23% Google Cloud VM мають ризикові дозволи [15]. Ці показники демонструють, що проблема стосується не одного типу ресурсу, а різних рівнів хмарної інфраструктури.

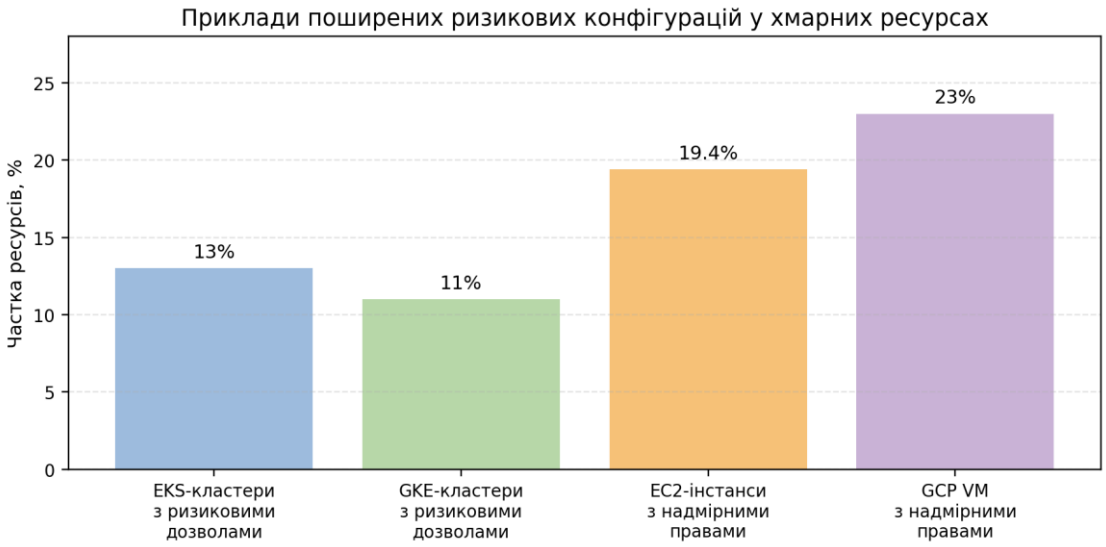

Рис. 3.8. Поширеність окремих ризикових конфігурацій у хмарних ресурсах за даними Datadog State of Cloud Security 2025

Ризикові конфігурації у хмарному середовищі не обмежуються відкритими портами або публічно доступними сервісами. Значну небезпеку створюють також надмірні дозволи, пов’язані з віртуальними машинами, обчислювальними ресурсами та Kubernetes-кластерами, оскільки такі привілеї можуть бути використані для подальшого переміщення між сервісами або доступу до критичних даних [25].

Подібний ризик простежується і в галузевих звітах щодо хмарної безпеки, де наголошується на проблемі занедбаних, публічно доступних або неправильно налаштованих хмарних активів [15, 16]. У цьому випадку небезпека полягає не лише у самому факті відкритого доступу, а в поєднанні кількох умов: ресурс доступний з Інтернету, може не мати відповідального власника, залишатися без оновлень і містити відомі вразливості. Тому CSPM-рішення мають оцінювати конфігурацію комплексно: враховувати не тільки відкриті порти, а й вік ресурсу, його призначення, наявність чутливих даних, пов’язані привілеї та стан журналювання.

Таблиця 3.4

Модель пріоритизації конфігураційних помилок

Пріоритет	**Рівень**	**Критерій**	**Приклад**	**Рекомендована реакція**
P1	Критичний	Публічна доступність поєднується з чутливими даними або адміністративними правами	Сховище з персональними даними відкрите назовні; ВМ має відкритий SSH доступ	Усунути протягом 24-72 годин
P2	Високий	Відхилення може бути використане для початкового доступу	Сервісний акаунт має зайві дозволи	Усунути до 14 днів
P3	Середній	Помилка підвищує ризик, але не створює прямого доступу до критичних даних	Неповне журналювання; вимкнене шифрування ресурсу	Усунути до 30 днів
P4	Низький	Порушення політики не має негайного впливу на критичні ресурси	Невідповідність тегів, застаріла назва, відхилення від стандарту	Планове усунення

Ризик-орієнтована пріоритизація зменшує перевантаження попередженнями та дає змогу зосередитися на найбільш небезпечних відхиленнях. Під час оцінювання важливо враховувати не лише кількість виявлених помилок, а й їхній можливий вплив: доступність ресурсу з Інтернету, чутливість даних, рівень привілеїв пов’язаних ідентичностей та ймовірність подальшого переміщення в середовищі.

Рис. 3.9. Матриця пріоритизації конфігураційних помилок

Матриця пріоритизації дає змогу відокремити критичні відхилення від тих, які можна усувати в межах планового циклу. Якщо ресурс є публічно доступним і пов’язаний із чутливими даними або привілейованою роллю, він має отримати найвищий пріоритет. Якщо ж помилка не відкриває прямого шляху до критичних ресурсів, її можна включити до плану контрольованого усунення. Такий підхід робить процес виправлення більш керованим і зменшує навантаження на адміністраторів.

Окреме місце у запропонованій моделі займають політики безпеки. CSPM виявляє відхилення, але саме політики визначають, який стан ресурсу вважається допустимим. Для корпоративної хмари політики мають охоплювати не тільки загальні вимоги, а й конкретні правила: заборону публічного доступу до сховищ, обов’язкове шифрування, обмеження адміністративних портів, увімкнене журналювання, використання тегів власника та середовища, контроль сервісних акаунтів і ротацію секретів.

Таблиця 3.5

Приклади політик безпеки для контролю конфігурацій

Об’єкт контролю	Правило політики	Що перевіряється
Сховища даних	Публічний доступ заборонено; шифрування обов’язкове; доступ	Bucket/container policy, ACL, encryption flag, data classification

Об’єкт контролю	Правило політики	Що перевіряється
	надається лише через затверджені ролі	
Мережеві правила	Адміністративні порти не відкриваються для 0.0.0.0/0 без погодженого винятку	Firewall/security group rules, port exposure, source ranges
Віртуальні машини	Дефолтні сервісні акаунти та надмірні ролі не використовуються без обґрунтування	Attached roles, service account scope, privilege escalation permissions
Бази даних	Публічні кінцеві точки доступу допускаються лише як виняток; шифрування, резервне копіювання й аудит є обов’язковими	Network exposure, encryption, backup policy, audit logging
Журналювання	Audit logs мають бути ввімкнені, зберігатися визначений строк і передаватися до централізованого сховища	Logging status, retention period, forwarding rules
Секрети та ключі	Секрети не зберігаються у відкритому коді; ключі мають проходити ротацію	Secret storage, key age, exposed credentials, repository scanning

Щоб політики не залишалися лише організаційним документом, їх необхідно переводити у формат policy-as-code. У такому випадку правило безпеки описується у формалізованому вигляді й перевіряється автоматично під час створення або зміни ресурсу. Наприклад, якщо шаблон Infrastructure as Code містить сховище з публічним доступом або базу даних без шифрування, перевірка має заблокувати таку зміну або створити обов’язкове завдання на виправлення. Це дає змогу змістити контроль конфігурацій ближче до етапу розгортання, а не чекати виявлення помилки вже в продуктивному середовищі [27].

Для формування таких політик можна використовувати кілька джерел контролів. CIS Benchmarks надають практичні рекомендації з безпечного налаштування платформ і сервісів [19]. CSA Cloud Controls Matrix може використовуватися як хмарна контрольна рамка [7], що охоплює конфігурації, IAM, журналювання, шифрування, управління вразливостями та розподіл відповідальності. NIST SP 800-53 Rev. 5 є корисним для побудови внутрішньої системи контролів, оскільки містить сімейства Configuration Management, Audit

and Accountability, Access Control, Risk Assessment та Security Assessment and Monitoring [18].

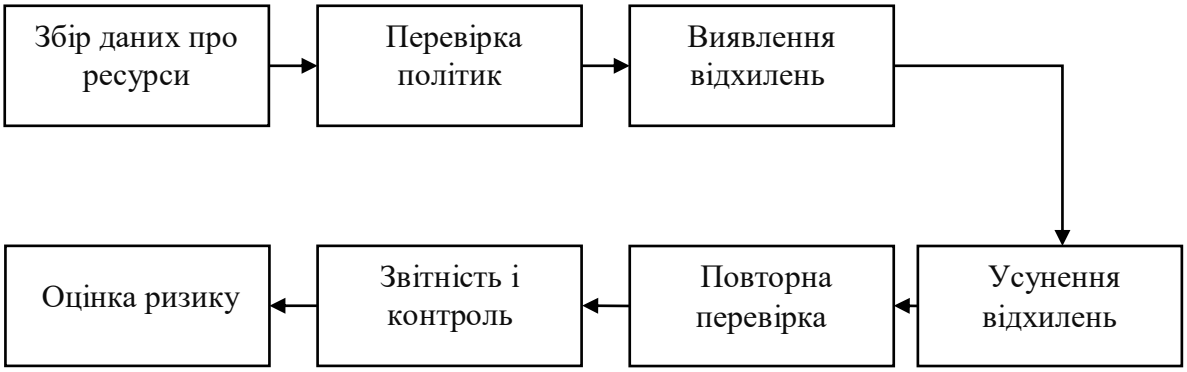

Рис. 3.10. Поетапне впровадження контролю конфігурацій у хмарному середовищі

Запропонована послідовність контролю конфігурацій поєднує технічну перевірку ресурсів із управлінською відповідальністю за їхній стан. Спочатку формується інвентар активів і визначаються власники ресурсів, після чого конфігурації перевіряються за політиками, оцінюються за рівнем ризику та виправляються відповідальними фахівцями.

Для практичного впровадження запропонованого підходу доцільно використовувати такий алгоритм:

1. сформувати інвентар хмарних ресурсів, включаючи сховища, бази даних, віртуальні машини, Kubernetes-кластери, мережеві правила, сервісні акаунти та журнали;

2. визначити критичні ресурси, які містять персональні, фінансові, службові або комерційно важливі дані;

3. розробити базові політики безпечної конфігурації для сховищ, мережі, обчислювальних ресурсів, баз даних, журналювання і секретів;

4. зіставити політики з CIS Benchmarks, CSA CCM, NIST SP 800-53 або внутрішніми вимогами організації;

5. увімкнути CSPM-перевірки для відкритих сховищ, надмірних мережевих правил, вимкненого шифрування, відсутніх журналів і небезпечних сервісних акаунтів;

6. пріоритизувати виявлені відхилення за зовнішньою доступністю, чутливістю даних, рівнем привілеїв і можливістю подальшого переміщення;

7. закріпити процес усунення: відповідальний власник, строк виправлення, контроль виконання та повторна перевірка;

8. дозволяти винятки лише за погодженням, із зазначенням причини, строку дії та компенсаційних заходів;

9. передавати критичні події CSPM до журналювання або SIEM/SOAR для сповіщення та подальшого реагування;

10. переглядати політики після появи нових сервісів, змін у бізнес-процесах або виявлення повторюваних помилок.

Усунення конфігураційних помилок не повинно завершуватися одноразовою правкою. Хмарне середовище є динамічним: ресурси створюються, масштабуються, видаляються або змінюються автоматизованими сценаріями. Через це після виправлення може виникнути конфігураційний дрейф. Наприклад, адміністратор може тимчасово відкрити порт для тестування і не закрити його, розробник може створити тестове сховище без шифрування, а шаблон розгортання може повторно створити ресурс зі стандартними дозволами. Саме тому CSPM має працювати постійно, а не лише перед перевіркою чи аудитом.

3.3 Розробка інтегрованої моделі захисту корпоративного хмарного середовища

Результати, отримані у підрозділах 3.1 та 3.2, показують, що ефективний захист корпоративної хмари не може будуватися лише на одному класі засобів. Контроль доступу зменшує ризик компрометації ідентичностей і надмірних привілеїв, тоді як CSPM та політики безпеки дозволяють виявляти небезпечні конфігураційні відхилення. Проте на практиці ці напрями тісно пов’язані: відкритий ресурс стає критичнішим за наявності чутливих даних, надмірні права посилюють наслідки компрометації акаунта, а відсутність журналювання ускладнює підтвердження факту атаки. Саме тому доцільно перейти від окремого опису засобів захисту до інтегрованої моделі, яка поєднує превентивні,

детекційні та реактивні механізми в єдиний процес управління хмарними ризиками.

З погляду MITRE ATT&CK Cloud Matrix такі ризики можуть відповідати різним етапам атаки, зокрема початковому доступу, закріпленню в середовищі, ескалації привілеїв, збору даних та впливу на хмарні ресурси [14].

Метою запропонованої моделі є не лише зменшення кількості окремих вразливих налаштувань, а формування керованого процесу безпеки. У такому процесі доступи, конфігурації, журнали, політики, події безпеки та реагування на інциденти розглядаються як взаємопов'язані елементи [20, 23, 30]. Це відповідає сучасній логіці хмарного захисту, де організація має не тільки встановити правила, а й постійно підтверджувати, що ці правила реально виконуються.

Для обґрунтування моделі використано підходи NIST SP 800-61 Revision 2, де реагування на інциденти розглядається як частина управління кіберризиками, а не як ізольована процедура після атаки [17]. Також враховано матрицю MITRE ATT&CK для хмарних середовищ, у якій дії зловмисника охоплюють початковий доступ, ескалацію привілеїв, ухилення від захисту, виявлення ресурсів, збір даних, ексфільтрацію та вплив на середовище [14].

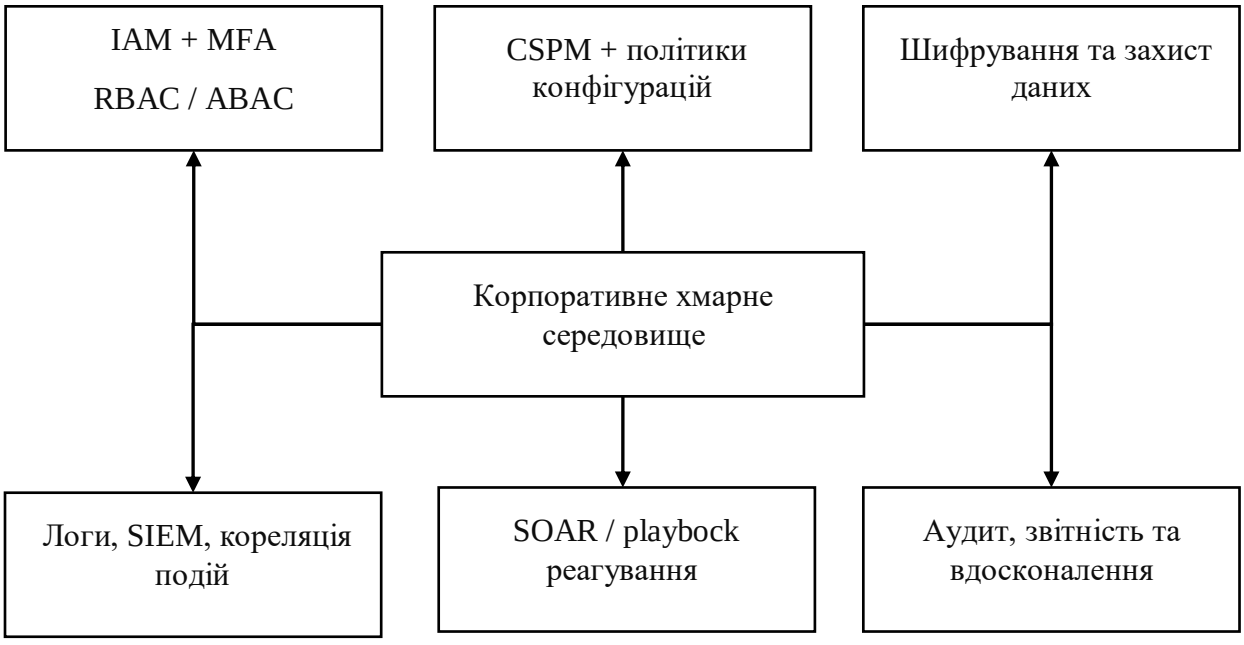

Рис. 3.11. Інтегрована модель захисту корпоративного хмарного середовища

Запропонована модель складається з шести взаємопов'язаних блоків. IAM, MFA, RBAC та ABAC обмежують доступ до ресурсів; CSPM і політики конфігурацій виявляють небезпечні відхилення; шифрування та захист даних зменшують наслідки можливого витоку; журнали, SIEM і кореляція подій забезпечують видимість; SOAR або сценарії реагування прискорюють обробку інцидентів; аудит і звітність дозволяють коригувати політики після інцидентів. Таким чином, модель поєднує контроль до інциденту, під час інциденту та після його завершення.

Таблиця 3.6

Відповідність елементів інтегрованої моделі основним ризикам корпоративної хмари

Елемент моделі	**Який ризик зменшує**	**Практичне застосування**	**Очікуваний результат**
IAM, MFA, RBAC, ABAC	Компрометація акаунтів, надмірні ролі, доступ без контексту	Мінімальні права, MFA для критичних акаунтів, контекстні правила доступу	Зменшення масштабу дій зловмисника після отримання доступу
CSPM та policy-as-code	Публічні сховища, відкриті порти, вимкнене шифрування, дефолтні параметри	Автоматична перевірка політик під час створення і зміни ресурсів	Виявлення помилок до їх використання в атаці
Шифрування та класифікація даних	Витік чутливих даних, копіювання резервних копій, доступ до службової інформації	KMS, класифікація даних, контроль доступу до ключів	Зменшення наслідків несанкціонованого доступу
Журналювання та SIEM	Пізнє виявлення атаки, неможливість відновити хронологію подій	Збір CloudTrail/Audit Logs, події IAM, мережеві й data access logs	Раннє виявлення аномалій і доказова база для розслідування
Аудит і вдосконалення	Повторення однакових помилок після виправлення	Періодичний перегляд політик, аналіз причин, звітність для власників ресурсів	Перехід від разового виправлення до постійного управління ризиком

Практична цінність інтегрованої моделі полягає в розподілі захисних функцій між окремими рівнями контролю. IAM, MFA, RBAC та ABAC зменшують ризики несанкціонованого доступу й надмірних привілеїв; CSPM та policy-as-code відповідають за контроль конфігурацій; шифрування знижує

наслідки витоку; SIEM і журнали забезпечують видимість подій; реагування на інциденти обмежує розвиток атаки.

Особливу увагу в моделі приділено машинним ідентичностям: сервісним акаунтам, токенам, ролям застосунків та автоматизованим процесам. У звіті Sysdig за 2025 рік підкреслюється, що машинні ідентичності у хмарних середовищах можуть суттєво переважати людські акаунти [16], що створює окрему проблему контролю доступів. Для корпоративної хмари це означає, що модель захисту має охоплювати не тільки користувачів, а й автоматизовані взаємодії між сервісами.

Практична модель застосування для умовного корпоративного середовища

Практичне застосування інтегрованої моделі доцільно розглянути на прикладі умовного корпоративного хмарного середовища, яке поєднує SaaS-сервіси для документообігу, віртуальні машини для внутрішніх застосунків, хмарне сховище для резервних копій, базу даних клієнтів, Kubernetes-кластер для мікросервісів і сервісні акаунти для автоматизованого розгортання.

У межах такого середовища модель має працювати не як набір окремих налаштувань, а як послідовність операційного контролю. Спочатку ресурси інвентаризуються і класифікуються за критичністю. Далі для кожного ресурсу визначаються допустимі ролі, мережеві параметри, вимоги до журналювання та правила зберігання даних. Після цього події доступу, зміни конфігурацій і спрацювання CSPM передаються до централізованого моніторингу, де зіставляються між собою.

Таблиця 3.7

Приклад практичного застосування моделі для типових сценаріїв хмарних інцидентів

Сценарій	**Ознака виявлення**	**Першочергова дія**	**Додаткова перевірка**	**Результат**
Компрометація користувача	Вхід із незвичної країни, масове	Призупинити сесію, вимагати повторну MFA, змінити пароль	Перевірити ролі, доступ до сховищ і створені токени	Обмеження доступу та збереження

Сценарій	Ознака виявлення	Першочергова дія	Додаткова перевірка	Результат
	завантаження файлів			журналів для розслідування
Витік API-ключа	Ключ використано з невідомої IP-адреси або з нетиповою частотою	Відкликати ключ, створити новий з обмеженими правами	Перевірити репозиторії, журнали CI/CD і секрети	Зменшення ризику повторного використання ключа
Публічне сховище	CSPM виявляє зовнішній доступ і чутливі дані	Закрити публічний доступ, зафіксувати стан політики	Перевірити історію завантажень і доступи сервісних акаунтів	Усунення відкритого каналу витоку
Підозрілий сервісний акаунт	Сервісний акаунт виконує дії поза типовим процесом	Тимчасово обмежити роль або вимкнути ключ	Перевірити власника, призначення, пов’язані ресурси	Виявлення прихованого автоматизованого доступу
Вимкнення журналювання	Зміна політики логування або строку зберігання	Відновити журналювання і заблокувати зміну без погодження	Перевірити, які дії відбулися до вимкнення журналів	Збереження доказової бази та контроль приховування слідів

Наведені сценарії демонструють практичну відмінність між ізольованою реакцією і комплексною моделлю. Наприклад, у разі витоку API-ключа недостатньо просто створити новий ключ. Потрібно також визначити, де саме ключ зберігався, які ресурси він міг читати або змінювати, чи не були створені нові облікові дані та чи збереглися журнали його використання. Такий підхід дозволяє не лише усунути симптом, а й встановити причину інциденту.

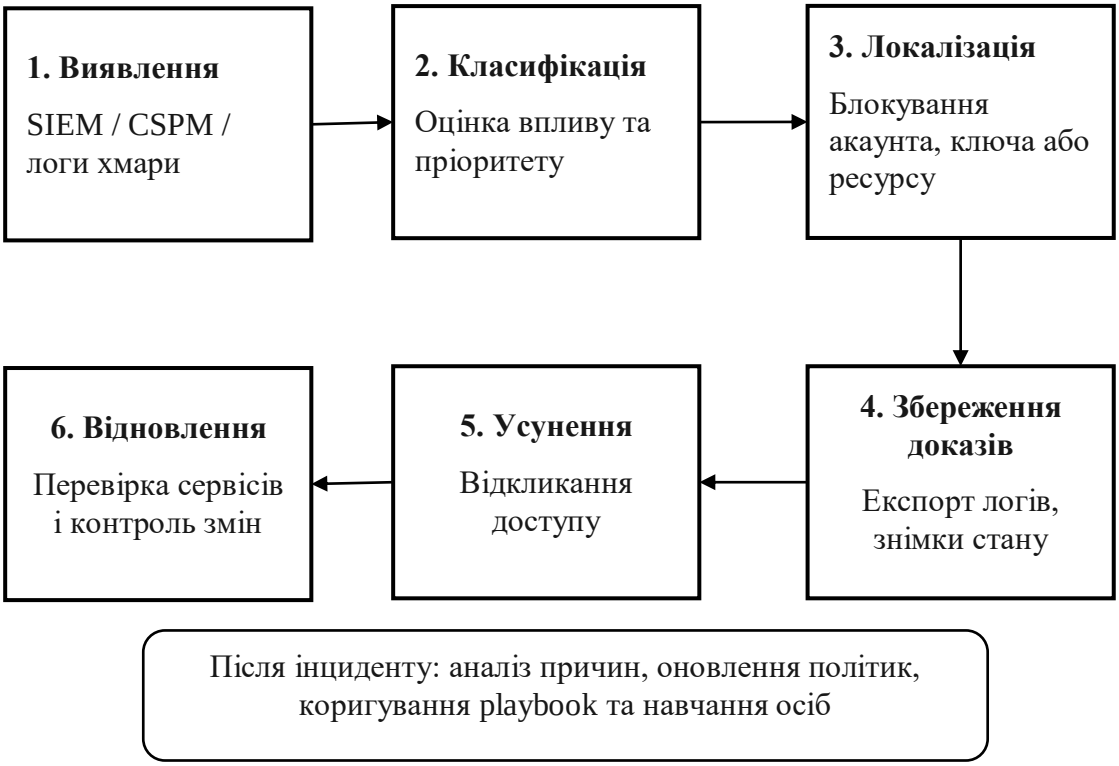

Рис. 3.12. Процес реагування на інцидент у корпоративній хмарі

Процес реагування у хмарному середовищі має враховувати особливості моделі спільної відповідальності. Організація не контролює фізичну інфраструктуру провайдера, однак відповідає за власні облікові записи, політики, дані, журнали, конфігурації та дії у межах хмарного середовища. Тому локалізація інциденту може передбачати не вимкнення сервера в класичному розумінні, а відкликання ключа, блокування ролі, ізоляцію ресурсу через security group, зміну політики сховища або створення незмінної копії журналів.

Ризик-орієнтована оцінка ефективності запропонованої моделі

Для оцінювання очікуваного ефекту від запропонованої моделі використано експертну шкалу залишкового ризику від 1 до 10. Оцінка не претендує на універсальне кількісне вимірювання, але дає змогу показати, як поєднання кількох рівнів захисту впливає на типові сценарії атаки. Початковий ризик визначався за припущенням, що організація має окремі засоби захисту, але не має єдиного процесу кореляції подій і реагування. Залишковий ризик після впровадження моделі враховує використання IAM, MFA, CSPM, централізованого журналювання, пріоритизації та playbook-реагування.

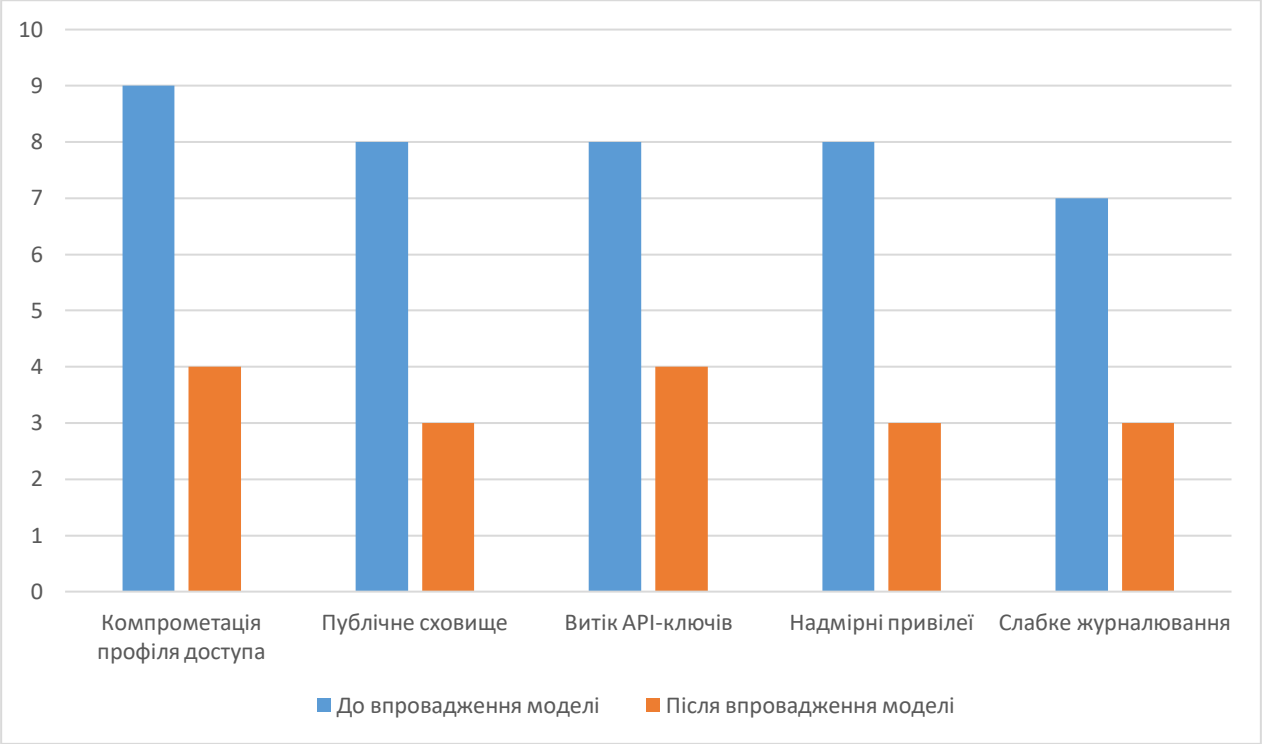

Рис. 3.13. Експертна оцінка зміни залишкового ризику після впровадження інтегрованої моделі

Найбільше зниження залишкового ризику очікується для тих сценаріїв, де ефективність захисту залежить від поєднання кількох контрольних заходів: контролю доступу, перевірки конфігурацій, журналювання та реагування. Це пояснюється тим, що окремий засіб захисту не усуває весь ланцюг атаки: MFA ускладнює початковий вхід, CSPM виявляє небезпечну конфігурацію, SIEM фіксує підозрілу активність, а playbook-реагування скорочує час локалізації інциденту.

Таблиця 3.8

Критерії оцінювання ефективності інтегрованої моделі захисту

Критерій	**Що оцінюється**	**Метод перевірки**	**Очікуване покращення**
Час виявлення	Скільки часу проходить від небезпечної дії до появи сповіщення	Перевірка логів, SIEM-правил, CSPM-спрацювань	Скорочення часу виявлення критичних подій
Час локалізації	Наскільки швидко блокується акаунт, ключ або ресурс	Тестові сценарії реагування і tabletop-вправи	Менша тривалість активності зловмисника

Критерій	Що оцінюється	Метод перевірки	Очікуване покращення
Повнота журналів	Чи достатньо подій для відновлення хронології інциденту	Перевірка збереження audit logs і data access logs	Краща доказова база для розслідування
Якість політик	Чи покривають політики критичні ресурси й типові помилки	Зіставлення з CIS, CSA CCM, NIST SP 800-53	Менше повторюваних відхилень
Залишковий ризик	Який ризик залишається після впровадження контролів	Оцінка за сценаріями атак і пріоритетами P1–P4	Кероване зниження ризику до прийнятного рівня

Важливим компонентом моделі є операційна сталість. Засоби захисту мають працювати не лише під час налаштування або аудиту, а постійно. Для цього необхідно організувати цикл роботи, у якому телеметрія збирається з хмарних сервісів, події корелюються між собою, ризикові сценарії отримують пріоритет, а реакція виконується за затвердженими правилами. У межах запропонованої моделі playbook-підхід і автоматизація реагування розглядаються як засоби скорочення часу між виявленням інциденту, його локалізацією та подальшим усуненням наслідків [17, 28].

Практична цінність інтегрованої моделі полягає в тому, що вона може бути використана як основа для побудови внутрішнього регламенту захисту корпоративної хмари. Її елементи дозволяють визначити відповідальних осіб за доступи, конфігурації, журнали подій і реагування на інциденти, а також встановити порядок регулярної перевірки хмарних ресурсів.

Алгоритм впровадження інтегрованої моделі

Для практичного впровадження запропонованої моделі доцільно використовувати поетапний алгоритм, який поєднує технічні та організаційні дії:

1. визначити межі корпоративного хмарного середовища: провайдери, облікові записи, підписки, проєкти, сховища, бази даних, обчислювальні ресурси, Kubernetes-кластери, SaaS-сервіси та інтеграції;

2. класифікувати ресурси за критичністю, типом даних, власником, рівнем зовнішньої доступності та залежністю від бізнес-процесів;

3. побудувати централізовану IAM-модель: типові ролі, MFA для привілейованих акаунтів, принцип найменших привілеїв, контроль сервісних ідентичностей і ротацію ключів;

4. налаштувати CSPM-перевірки для публічного доступу, відкритих портів, шифрування, журналювання, дефолтних параметрів, Kubernetes і надмірних прав сервісних акаунтів;

5. забезпечити передавання подій IAM, CSPM, мережевих змін, доступу до даних і дій адміністраторів до централізованого журналювання або SIEM;

6. розробити сценарії реагування для основних випадків: компрометація акаунта, витік API-ключа, публічне сховище, вимкнення журналювання, підозріла активність сервісного акаунта;

7. визначити правила локалізації інцидентів: блокування сесій, відкликання ключів, тимчасове обмеження ролей, ізоляція ресурсу, створення копії журналів і збереження доказів;

8. встановити метрики ефективності: час виявлення, час локалізації, частка критичних подій із повними журналами, кількість повторюваних конфігураційних помилок;

9. проводити регулярні тренування або настільні навчання з реагування на інциденти для перевірки ролей відповідальних осіб і працездатності сценаріїв реагування;

10. оновлювати політики, IAM-ролі, правила SIEM/SOAR і CSPM-перевірки після кожного значного інциденту, зміни архітектури або появи нового хмарного сервісу.

Запропонований алгоритм сприяє перетворити захист корпоративної хмари з набору окремих інструментів на керований процес. Його перевага полягає в тому, що кожен етап має практичний результат: інвентаризація дає видимість, IAM обмежує доступ, CSPM виявляє відхилення, SIEM формує картину подій, а SOAR або сценарії реагування пришвидшують реакцію, а аудит забезпечує коригування політик. У сукупності це зменшує не лише ймовірність інциденту, а й час, протягом якого зловмисник може залишатися непоміченим.

Висновки до розділу 3

У третьому розділі було сформовано практичний підхід до захисту корпоративного хмарного середовища з урахуванням загроз, проаналізованих у попередньому розділі. Основу цього підходу становить поєднання контролю доступу, перевірки конфігурацій, моніторингу подій, реагування на інциденти та подальшого вдосконалення політик безпеки [17, 28].

Розроблена модель контролю доступу поєднує IAM, MFA, RBAC, ABAC, принцип найменших привілеїв, управління життєвим циклом доступів і централізоване журналювання. Це дозволяє зменшити ризик компрометації облікових записів, обмежити наслідки надмірних привілеїв, контролювати сервісні акаунти й API-ключі та своєчасно виявляти підозрілу активність.

Окрему увагу приділено контролю конфігурацій хмарних ресурсів. CSPM-рішення запропоновано розглядати як постійний цикл, що включає інвентаризацію ресурсів, перевірку політик, оцінку ризику, пріоритизацію відхилень, усунення помилок і моніторинг змін конфігурацій [15, 19]. Додатково обґрунтовано доцільність використання policy-as-code, що дозволяє перевіряти вимоги безпеки ще на етапі створення або зміни хмарних ресурсів [26, 27].

Підсумком розділу є сформована модель захисту корпоративної хмари, у якій превентивні, детекційні та реактивні заходи працюють як єдиний цикл управління ризиками.

Отже, запропоновані заходи створюють практичну основу для підвищення стійкості корпоративної хмари. Їхнє значення полягає не лише в запобіганні окремим атакам, а й у формуванні постійного циклу безпеки: виявлення ризиків, обмеження доступів, контролю конфігурацій, моніторингу подій, реагування на інциденти та подальшого коригування політик.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено безпеку хмарних технологій у корпоративному середовищі, сучасні вектори атак на хмарну інфраструктуру та засоби їх захисту. Встановлено, що корпоративне хмарне середовище є складною та динамічною частиною IT-інфраструктури організації, яка забезпечує гнучкість, масштабованість і зручність використання ресурсів, але водночас створює нові ризики для конфіденційності, цілісності, доступності та контрольованості інформації.

У процесі дослідження розглянуто моделі хмарних сервісів IaaS, PaaS, SaaS і FaaS та визначено їхній вплив на розподіл відповідальності між хмарним провайдером і організацією-користувачем. Обґрунтовано, що перехід до хмари не усуває відповідальність організації за безпеку, а лише змінює її межі. Організація залишається відповідальною за власні дані, облікові записи, ролі доступу, конфігурації ресурсів, політики безпеки та моніторинг подій.

Проаналізовано основні принципи захисту корпоративної хмари, зокрема принцип найменших привілеїв, багатофакторну автентифікацію, сегментацію ресурсів, шифрування даних, журналювання, аудит конфігурацій і реагування на інциденти. Окрему увагу приділено концепції Zero Trust, яка передбачає постійну перевірку кожного запиту доступу з урахуванням ідентичності користувача, стану пристрою, місця підключення, ролі, типу ресурсу та рівня ризику.

У роботі встановлено, що найбільш небезпечними векторами атак на корпоративні хмарні середовища є компрометація облікових записів, відсутність MFA, надмірні привілеї, неконтрольовані сервісні акаунти, викрадені API-ключі, відкриті хмарні сховища, неправильні мережеві правила, вимкнене журналювання та помилки конфігурації ресурсів. Такі загрози часто реалізуються не через прямий злам інфраструктури провайдера, а через слабкі місця на стороні самої організації.

У практичній частині роботи обґрунтовано застосування технічних і організаційних засобів захисту корпоративного хмарного середовища. До них

належать IAM, MFA, RBAC, ABAC, регулярний перегляд доступів, контроль сервісних ідентичностей, моніторинг активності, журналювання подій, CSPM-рішення, policy-as-code, аудит конфігурацій і сценарії реагування на інциденти. Запропоновані заходи спрямовані на зменшення ймовірності успішної атаки, своєчасне виявлення небезпечних змін і обмеження наслідків можливого інциденту.

Підсумковим результатом роботи стало формування інтегрованої моделі захисту корпоративного хмарного середовища, яка поєднує превентивні, детекційні та реактивні заходи. Її практична цінність полягає в тому, що захист хмари розглядається як безперервний цикл управління ризиками: виявлення активів, обмеження доступів, контроль конфігурацій, моніторинг подій, реагування на інциденти та подальше коригування політик безпеки. Такий комплексний підхід дозволяє підвищити стійкість корпоративної хмарної інфраструктури та забезпечити більш надійний захист інформаційних ресурсів організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Електронні ресурси

1. Mell P., Grance T. The NIST Definition of Cloud Computing : NIST Special Publication 800-145. National Institute of Standards and Technology, 2011. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

2. Simmon E. Evaluation of Cloud Computing Services Based on NIST SP 800-145 : NIST Special Publication 500-322. National Institute of Standards and Technology, 2018. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

3. Shared Responsibility Model. Amazon Web Services. URL: https://aws.amazon.com/compliance/shared-responsibility-model/

4. Shared responsibility in the cloud. Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

5. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture : NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

6. Security Guidance for Critical Areas of Focus in Cloud Computing v5. Cloud Security Alliance, 2024. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v5

7. Cloud Controls Matrix. Cloud Security Alliance. URL: https://cloudsecurityalliance.org/research/cloud-controls-matrix

8. CIS Critical Security Controls v8.1. Center for Internet Security, 2024. URL: https://www.cisecurity.org/controls/v8

9. Secure Cloud Business Applications. Cybersecurity and Infrastructure Security Agency, 2024. URL: https://www.cisa.gov/sites/default/files/2024-03/Final-02262024-CSSO-SCUBA-508c.pdf

10. A05:2021 – Security Misconfiguration. OWASP Foundation, 2021. URL:

https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

11. OWASP Top 10 CI/CD Security Risks. OWASP Foundation. URL: https://owasp.org/www-project-top-10-ci-cd-security-risks/

12. 2025 Data Breach Investigations Report. Verizon, 2025. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

13. Cost of a Data Breach Report 2025. IBM, 2025. URL: https://www.ibm.com/reports/data-breach

14. MITRE ATT&CK Cloud Matrix. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/cloud/

15. State of Cloud Security 2025. Datadog, 2025. URL: https://www.datadoghq.com/state-of-cloud-security/

16. 2025 Cloud-Native Security and Usage Report. Sysdig, 2025. URL: https://www.sysdig.com/2025-cloud-native-security-and-usage-report

17. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Revision 2. National Institute of Standards and Technology, 2012. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final

18. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53 Revision 5. National Institute of Standards and Technology, 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

19. CIS Benchmarks. Center for Internet Security. URL: https://www.cisecurity.org/cis-benchmarks

20. AWS Well-Architected Framework. Security Pillar. Amazon Web Services. URL: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

21. Security – AWS Well-Architected Framework. Amazon Web Services. URL: https://docs.aws.amazon.com/wellarchitected/latest/framework/a-security.html

22. Microsoft Cloud Adoption Framework. Microsoft Learn. URL:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/overview

23. Google Cloud Architecture Framework: Security, Privacy and Compliance Pillar. Google Cloud. URL: https://docs.cloud.google.com/architecture/framework/security

24. OWASP API Security Top 10 – 2023. OWASP Foundation, 2023. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/

25. Security Checklist. Kubernetes Documentation. URL: https://kubernetes.io/docs/concepts/security/security-checklist/

26. Open Policy Agent Documentation. Open Policy Agent. URL: https://www.openpolicyagent.org/docs

27. Sentinel Documentation. HashiCorp Developer. URL: https://developer.hashicorp.com/sentinel/docs

28. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

29. Zero Trust Maturity Model Version 2.0. Cybersecurity and Infrastructure Security Agency, 2023. URL: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

30. Cloud Security Technical Reference Architecture. Cybersecurity and Infrastructure Security Agency, 2022. URL: https://www.cisa.gov/sites/default/files/2023-02/cisa_cloud_security_technical_reference_architecture_version_1_1.pdf