МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему

СИСТЕМА ОЦІНКИ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Виконав: студент групи 2КІ-23
Спеціальності 123 «Комп'ютерна інженерія
Шпак М.О.
Керівник роботи
к.т.н., доцент Захарова М.В.
Кількість балів: _____
Оцінка: ECTS _____

Черкаси, 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

(повна назва випускової кафедри)

Спеціальність 123 "Комп'ютерна інженерія "

(шифр і назва спеціальності)

Освітня програма Комп'ютерна інженерія

(назва освітньої програми)

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії та інформаційних технологій

(назва кафедри)

_____ Хотунов В.І.

(підпис) (ПІБ)

«_____»_____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Шпак Максим Олегович

(прізвище, ім'я, по батькові студента)

1. Тема кваліфікаційної роботи Система оцінки безпеки хмарних сервісів
Науковий керівник роботи к.т.н доцент Захарова Марія В'ячеславівна

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від " 7 " жовтня 2024 року № 68У.

2. Строк подання студентом випускної роботи 03.06.2025

3. Вихідні дані до випускної роботи Огляд сучасних методів оцінки безпеки хмарних сервісів, аналіз їхніх вразливостей та загроз, а також дослідження існуючих стандартів і нормативно-правових вимог щодо захисту даних у хмарних платформах. Крім цього, планується розробка концептуальної моделі оцінки безпеки хмарних сервісів, її тестування в експериментальному середовищі та надання рекомендацій щодо підвищення рівня захисту хмарних обчислень.

4. Зміст випускної роботи (перелік питань, які потрібно розробити) визначення актуальності теми, мети, завдання, об'єкту, предмету, детальний огляд та порівняння аналогів системи біометричної аутентифікації, враховуючи їхні переваги, недоліки та сучасні тенденції розвитку

5. Дата видачі завдання 15.09.2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами наукового керівника і студента
1	Вступ	15.10.2024	
2	Розділ 1. Теоретичні основи безпеки хмарних сервісів	18.12.2024	
3	Розділ 2. Методи оцінки безпеки хмарних сервісів	05.03.2025	
4	Розділ 3. Розробка моделі оцінки безпеки хмарних сервісів	06.04.2025	
5	Висновки	16.05.2025	
6	Оформлення випускної роботи (чистовий варіант)	27.05.2025	
7	Здача випускної роботи на кафедру для рецензування (за 14 днів до захисту)	03.05.2025	
8	Перевірка випускної роботи на наявність ознак плагіату (за 10 днів до захисту)	07.06.2025	
9	Подання випускної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент

_____ Шпак М. О.

(підпис) (прізвище та ініціали)

Науковий керівник роботи

_____ Захарова М.В.

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

У кваліфікаційній роботі бакалавра досліджено систему оцінки безпеки хмарних сервісів з урахуванням архітектурних особливостей хмарних обчислень, типових загроз, вразливостей та міжнародних стандартів безпеки. Проаналізовано особливості моделей IaaS, PaaS, SaaS, виявлено найбільш уразливі компоненти хмарного середовища, розглянуто ключові стандарти (ISO/IEC 27001, 27017, 27018, NIST, GDPR тощо), що регламентують захист інформації.

Особливу увагу приділено розробці концептуальної моделі оцінки безпеки хмарних сервісів, яка базується на ризик-орієнтованому підході, системі критеріїв безпеки та адаптованих методах аналізу. У рамках апробації моделі створено тестове середовище для демонстрації її працездатності, а також розроблено практичні рекомендації щодо підвищення рівня захищеності хмарних платформ.

Кваліфікаційна робота бакалавра містить __ сторінок тексту, включає __ рисунок, __ таблиць.

Ключові слова: хмарні сервіси, інформаційна безпека, моделі IaaS/PaaS/SaaS, кібератаки, стандарти ISO/IEC, модель оцінки безпеки, вразливості, ризик-менеджмент.

ANNOTATION

The bachelor's qualification work investigates the system of cloud services security assessment, taking into account the architectural features of cloud computing, typical threats, vulnerabilities and international security standards. The features of the IaaS, PaaS, SaaS models are analyzed, the most vulnerable components of the cloud environment are identified, and key standards (ISO/IEC 27001, 27017, 27018, NIST, GDPR, etc.) that regulate information protection are considered.

Particular attention is paid to the development of a conceptual model of cloud services security assessment, which is based on a risk-based approach, a system of security criteria and adapted analysis methods. As part of the model testing, a test environment was created to demonstrate its performance, and practical recommendations were developed to improve the level of security of cloud platforms.

The bachelor's qualification work contains __ pages of text, includes __ figures, __ tables.

Keywords: cloud services, information security, IaaS/PaaS/SaaS models, cyberattacks, ISO/IEC standards, security assessment model, vulnerability, risk management.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

API	Application Programming Interface — інтерфейс прикладного програмування
AWS	Amazon Web Services — хмарна платформа від Amazon
BaaS	Backend-as-a-Service — бекенд як послуга
CSA	Cloud Security Alliance — Альянс безпеки хмарних обчислень
DaaS	Data-as-a-Service — дані як послуга
DDoS	Distributed Denial of Service — розподілена атака типу "відмова в обслуговуванні"
DPIA	Data Protection Impact Assessment — оцінка впливу на захист даних
FaaS	Function-as-a-Service — функція як послуга
GDPR	General Data Protection Regulation — Загальний регламент захисту даних
IAM	Identity and Access Management — управління ідентифікацією та доступом
IaaS	Infrastructure-as-a-Service — інфраструктура як послуга
ISO/IEC 27001	Міжнародний стандарт систем управління інформаційною безпекою
MFA	Multi-Factor Authentication — багатофакторна автентифікація
MitM	Man-in-the-Middle — атака «людина посередині»
NIST	National Institute of Standards and Technology — Національний інститут стандартів і технологій США
PaaS	Platform-as-a-Service — платформа як послуга
PII	Personally Identifiable Information — персонально ідентифікована інформація
SaaS	Software-as-a-Service — програмне забезпечення як послуга

SLA	Service Level Agreement — угода про рівень обслуговування
SP 800-53	Спеціальна публікація NIST щодо заходів безпеки інформаційних систем
TLS/SSL	Transport Layer Security / Secure Sockets Layer — протоколи захищеного обміну даними
Zero Trust	Концепція «нульової довіри» в інформаційній безпеці

ВСТУП

У сучасному цифровому суспільстві хмарні технології є невід'ємним елементом інформаційної інфраструктури, яка забезпечує ефективну обробку, зберігання та передачу даних. Хмарні обчислення стали ключовим фактором цифрової трансформації у різних сферах діяльності — від комерційних структур до державного управління, від освітніх установ до медичних закладів. Завдяки масштабованості, гнучкості, економічній доцільності та високій доступності хмарні сервіси стрімко поширюються, витісняючи традиційні IT-рішення.

Однак разом із перевагами використання хмарних обчислень постає низка викликів, серед яких питання інформаційної безпеки займає одне з центральних місць. У зв'язку з тим, що дані у хмарному середовищі часто зберігаються за межами фізичного контролю користувача, виникає підвищений ризик витоку, несанкціонованого доступу, модифікації або втрати критично важливої інформації. Саме тому питання забезпечення безпеки хмарних сервісів є вкрай актуальним як для кінцевих користувачів, так і для постачальників хмарної інфраструктури.

Зростаюча кількість інцидентів інформаційної безпеки, пов'язаних з хмарними платформами, свідчить про необхідність розробки ефективних систем моніторингу, контролю та оцінки рівня безпеки. Особливої важливості набуває формування об'єктивних критеріїв та моделей оцінювання, які дозволяють визначити ступінь захищеності хмарної інфраструктури, ідентифікувати вразливості та запропонувати практичні шляхи їх усунення. У цьому контексті оцінка безпеки хмарних сервісів повинна здійснюватися з урахуванням міжнародних стандартів (зокрема ISO/IEC серії 27000), сучасних методик аналізу ризиків, а також специфіки архітектури хмарних рішень (IaaS, PaaS, SaaS).

Актуальність дослідження зумовлена потребою у створенні системного підходу до оцінювання інформаційної безпеки хмарних сервісів, що базується на інтеграції методологічних, технічних та нормативних аспектів. Розробка моделі оцінки безпеки дозволяє сформувати структуроване бачення захищеності

інформаційних ресурсів, визначити критичні чинники ризику та оптимізувати управління безпекою в хмарному середовищі.

Метою роботи є розробка концептуальної моделі оцінки безпеки хмарних сервісів на основі сучасних критеріїв, стандартів та методик аналізу ризиків.

Для досягнення цієї мети в роботі поставлено низку завдань:

- проаналізувати архітектуру хмарних обчислень та визначити специфіку різних моделей надання хмарних сервісів (IaaS, PaaS, SaaS);
- систематизувати основні загрози та вразливості, характерні для хмарних середовищ;
- дослідити міжнародні стандарти та нормативно-правову базу забезпечення інформаційної безпеки у хмарних обчисленнях;
- обґрунтувати критерії оцінки безпеки хмарних сервісів;
- здійснити огляд сучасних методів аналізу безпеки хмарних платформ;
- провести порівняння існуючих систем оцінювання безпеки хмарних сервісів;
- розробити концептуальну модель оцінки безпеки та апробувати її в тестовому середовищі;
- сформулювати практичні рекомендації щодо підвищення рівня захищеності хмарних сервісів.

Об'єктом дослідження виступає система забезпечення інформаційної безпеки хмарних сервісів.

Предметом дослідження є методи, критерії та моделі оцінки безпеки хмарних обчислювальних середовищ.

Методологічну основу дослідження становлять загальнонаукові та спеціальні методи: системний аналіз, структурно-функціональне моделювання, метод порівняльного аналізу, методи класифікації загроз і ризик-аналізу, елементи експертного оцінювання, контент-аналіз нормативно-правових документів

.

Інформаційну базу дослідження складають:

- міжнародні стандарти інформаційної безпеки (ISO/IEC 27001, 27002, 27017, 27018, 27036, 27040);
- національні нормативні документи у сфері захисту інформації;
- аналітичні матеріали провідних дослідницьких центрів (Gartner, ENISA, NIST, CSA);
- наукові публікації та монографії вітчизняних і зарубіжних авторів;
- результати досліджень практичного використання хмарних сервісів у комерційному та державному секторі.

Практичне значення дослідження полягає у можливості застосування розробленої моделі оцінки в практичній діяльності IT-підрозділів підприємств і організацій для проведення внутрішнього аудиту безпеки, удосконалення політик інформаційної безпеки та прийняття обґрунтованих управлінських рішень щодо використання хмарних технологій.

Особистий внесок здобувача полягає у самостійному здійсненні всіх етапів дослідження: від теоретичного аналізу літератури та нормативної бази — до моделювання системи оцінки та розробки практичних рекомендацій.

Апробація результатів дослідження під час участі у студентській науково-практичній конференції «Цифрова безпека: проблеми та перспективи», що проходила в Черкаському державному бізнес-коледжі 26 березня 2025 року. За результатами представлено тези на тему «Система оцінки безпеки хмарних сервісів».

Структура і обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (50 найменувань) та додатків. Загальний обсяг роботи становить __ сторінок комп'ютерного тексту.

РОЗДІЛ 1 МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ХМАРНИХ ОБЧИСЛЕННЯХ

1.1 Основи хмарних обчислень та їх архітектура

У сучасній інформаційній економіці хмарні обчислення є однією з найдинамічніших технологічних парадигм, яка змінює нові орієнтири розвитку цифрової інфраструктури. Під хмарними обчисленнями (cloud computing) розуміють модель організації доступу до обчислювальних ресурсів через глобальні телекомунікаційні мережі, що забезпечує масштабування, гнучкості та економічно ефективне управління інформаційними ресурсами на основі принципу використання інфраструктури як послуги.

Історично передумови виникнення до хмарних технологій закладалися ще в середині XX століття. Перші концепції централізованого доступу до обчислювальних потужностей реалізовані в архітектурних мейнфреймах, які забезпечували одночасну роботу багатьох користувачів через термінали. У 1961 році Джон Маккарті висунув ідею, що обчислювальні ресурси можуть бути надані за принципом комунальних послуг, подібно до електроенергії. Ця концепція отримала практичне втілення з появою мережевих технологій та віртуалізації в 1990-х роках. Вже в 1999 році компанія Salesforce вперше представила бізнес-додатки, доступні через мережу як програмний сервіс (SaaS), а згодом Amazon Web Services (AWS) в 2006 році започаткувала надання віртуалізованих обчислювальних потужностей у моделі IaaS, що стало каталізатором розвитку галузі хмарних технологій [2].

Сутність хмарних обчислень збільшується поруч із базовими характеристиками, що відрізняють їх від традиційних моделей обробки інформації. Насамперед ідеться про властивість масштабованості , що забезпечує динамічне розширення або скорочення обсягів обчислювальних ресурсів відповідно до поточних потреб користувача. Масштабованість досягається шляхом інтеграції механізмів горизонтального та вертикального масштабування в межах віртуалізованої інфраструктури.

Ключовим технічним аспектом хмарних обчислень є віртуалізація , яка дозволяє відокремити логічні обчислювальні ресурси від фізичного обладнання. Завдяки використанню гіпервізорів (Hyper-V, VMware, KVM тощо) здійснюється абстрагування ресурсів, що забезпечує гнучкість у їх наданні та ізоляцію середовищ користувачів. Принцип підвищує ефективність використання апаратних засобів і забезпечує можливість одночасного функціонування різних робочих навантажень на одній фізичній інфраструктурі.

Не менш важливою характеристикою є автоматизація управління ресурсами , яка реалізується через використання оркестраторів (OpenStack, Kubernetes тощо) та системи моніторингу. Автоматизоване управління дозволяє забезпечити масштабування, балансування завантажень, оновлення програмного забезпечення та безперервний контроль доступності ресурсів без залучення адміністративного персоналу.

Водночас у структурі хмарних технологій важливу роль комерційна концепція платформи як сервісу (PaaS) , яка забезпечує надання користувачам середовища для розробки, тестування та розгортання додатків без необхідності адміністрування інфраструктури. Це забезпечення скорочення часу виходу продукту на ринок, гнучкість у виборі технологій розробки та інтеграцію з іншими сервісами.

Хмарні обчислення мають низькі стратегічні переваги порівняно з традиційною IT-інфраструктурою. Найбільш очевидною є зниження фінансових витрат , що зумовлено переходом до моделі операційних витрат (OPEX) замість капітальних (CAPEX). Завдяки оплаті лише за фактично використані ресурси користувач уникає витрат на придбання та обслуговування обладнання. Додатковою перевагою є глобальна доступність , що забезпечує можливість отримання сервісів з будь-якої точки світу, де є підключення до мережі [8].

Водночас слід дізнатися, що впровадження хмарних рішень супроводжується і певними ризиками. Основними недоліками є питання інформаційної безпеки та обмежений контроль користувачів над фізичними ресурсами , що ускладнює реалізацію політики безпеки на рівнях

інфраструктури. Залежність від стабільності мережевого з'єднання може критично вплинути на доступність сервісів, особливо в умовах недостатньо розвиненої телекомунікаційної інфраструктури.

З метою системного аналізу переваг та недоліків хмарних рішень необхідно провести їх порівняння з традиційною IT-інфраструктурою за основними експлуатаційними характеристиками [2].

З наведеного порівняння (табл. 1.1) випливає, що хмарні обчислення демонструють вищу адаптивність до змінних умов використання та забезпечують значні переваги в контексті оптимізації ресурсів та масштабування, однак водночас потребують постійного управління безпековими ризиками та залежністю від зовнішніх постачальників послуг.

Таблиця 1.1 – Порівняльна характеристика хмарних обчислень та традиційної IT-інфраструктури

№	Критерій	Хмарні обчислення	Традиційна IT-інфраструктура
1	Фінансові витрати	Мінімальні капітальні вкладення, оплата за збереження ресурсів	Значні капітальні інвестиції в обладнання, ліцензування та обслуговування
2	Масштабованість	Гнучке та автоматизоване масштабування ресурсів	Обмежена масштабованість, потреба у фізичному розширенні інфраструктури
3	Адміністрування	Автоматизація процесів управління, мінімальне втручання персоналу	Ручне адміністрування, потреба в штатних адміністраторах
4	Мобільність та доступність	Висока – доступ з будь-якої точки через Інтернет	Обмежена – доступ переважно з локальної мережі
5	Інформаційна безпека	Високі вимоги до політики провайдера, ризики стороннього доступу	Повний контроль над безпекою на рівні локальної мережі
6	Надійність та резервування	Високий рівень – георезервування, аварійне відновлення	Залежить від організації внутрішньої IT-інфраструктури

У сучасній інформаційній інфраструктурі хмарні обчислення стали невід'ємною складовою, пропонуючи різноманітні моделі надання послуг, які задовольняють спеціальні потреби бізнесу та розробників. Основні моделі включають IaaS (інфраструктура як послуга), PaaS (платформа як послуга) та SaaS (програмне забезпечення як послуга). без них, з'являються додаткові

варіації, такі як FaaS (функція як послуга), DaaS (дані як послуга) та BaaS (бекенд як послуга), які розширюють можливості хмарних обчислень.

IaaS надає користувачам базову інфраструктуру, включаючи віртуальні сервери, сховища даних та мережеві ресурси. Це дозволяє організаціям орендувати обчислювальні потужності без необхідності інвестувати у фізичне обладнання. Користувачі мають контроль над операційними системами та додатками, але не керують фізичною інфраструктурою. Прикладом IaaS є Amazon Web Services (AWS) EC2 [48].

PaaS забезпечує платформу, яка включає середовище розробки, тестування та розгортання додатків. Це спрощує процес розробки, після чого розробники можуть зосередитися на написаному коді без турбот про управління інфраструктурою. Провайдери PaaS керують серверами, сховищами та мережами, а потім як користувачі вимагають розробку та управління додатками. Прикладом PaaS є Google App Engine [39, 56].

SaaS надає готові програмні рішення, доступні через Інтернет. Користувачі можуть використовувати додатки без необхідності їх встановлення на локальних пристроях. Усі аспекти, включаючи інфраструктуру, платформи та програмне забезпечення, керуються провайдером. Прикладами SaaS є Google Workspace та Microsoft Office 365 [39].

FaaS, або серверлес-обчислення, дозволяє розробникам запускати окремі функції або фрагменти коду у відповідь на події без необхідності управління серверами. Це забезпечує високу масштабованість та ефективність, оскільки ресурси лише використані під час виконання функцій. Прикладом FaaS є AWS Lambda [56].

DaaS надає доступ до даних через Інтернет незалежно від їх фізичного розташування. Це дозволяє організації використання даних без необхідності їх зберігання та обробки на власних серверах, що спрощує управління даними та забезпечує їх актуальність.

BaaS надає розробникам готовий бекенд для мобільних та веб-додатків, включаючи управління базами даних, автентифікацію користувачів та

інтеграцію з іншими сервісами. Це прискорює процес розробки та знижує витрати на створення серверної частини додатків.

Вибір моделі хмарного сервісу (див. табл. 1.2) залежить від конкретних потреб та ресурсів організації. Розуміння особливостей кожної моделі дозволяє прийняти обґрунтоване рішення щодо оптимізації IT-інфраструктури, забезпечення гнучкості та ефективності бізнес-процесів [7].

Таблиця 1.2 – Порівняльна характеристика моделей хмарних сервісів

№	Модель	Опис	Приклади
1	IaaS	Надає базову інфраструктуру: віртуальні машини, сховища, мережі. Користувачі керують операційними системами та додатками.	AWS EC2, Google Compute Engine
2	PaaS	Забезпечує платформу для розробки, тестування та розгортання додатків. Користувачі зосереджуються на коді, не турбуючись про інфраструктуру.	Google App Engine, Heroku
3	SaaS	Надає готові програмні рішення через інтернет. Користувачі підтримують доступ до додатків без необхідності їх встановлення.	Google Workspace, Microsoft Office 365
4	FaaS	Дозволяє запускати окремі функції або фрагменти коду у відповідь на події без управління серверами.	AWS Lambda, функції Google Cloud
5	DaaS	Надає доступ до даних через Інтернет незалежно від їх фізичного розташування.	Сніжинка, Google BigQuery
6	BaaS	Забезпечує готовий бекенд для додатків, включаючи управління базами даних та автентифікацію.	Firebase, Backendless

Розгортання хмарної інфраструктури — це процес впровадження та організації хмарного середовища відповідно до потреб користувача або організації. Відповідно від рівня доступності, способу керування та належності інфраструктури, у сучасній практиці виділяють чотири основні моделі розгортання хмарних сервісів: публічну, приватну, гібридну та спільну (community cloud). Вибір відповідної моделі має низький рівень чинників — вимогами до безпеки, масштабністю, вартістю впровадження та характером бізнес-процесів [18, 19].

Публічна хмара (public cloud) забезпечує надання обчислювальних ресурсів у відкритому доступі через Інтернет на комерційній основі. Інфраструктура в такій моделі переходить у власність стороннього постачальника послуг і спільного використання великої кількості клієнтів.

Замовник не володіє фізичними ресурсами та не оплачує їх обслуговування — усі технічні аспекти складаються на провайдера. Це дозволяє суттєво скоротити витрати на впровадження IT-рішень, забезпечити швидке масштабування ресурсів і високу доступність сервісів. Однак публічні хмари мають певні обмеження, зокрема, підвищені ризики інформаційної безпеки, втрату контролю над даними та залежність від зовнішнього середовища. Найпоширенішими прикладами публічних хмар є Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure.

На противагу, приватна хмара (private cloud) — це модель розгортання, в якій обчислювальні ресурси використовують для використання однієї організації. Інфраструктура може бути розміщена як у власному дата-центрі організації, так і орендована у стороннього провайдера, але за умов повного контролю та ізоляції від інших користувачів. Такий підхід забезпечує підвищений рівень захисту даних, гнучкість у налаштуваннях безпекової політики та відповідність вимогам корпоративного або галузевого регулювання (наприклад, фінансовий сектор, державні установи). Приватні хмари є більш капіталомісткими у впровадженні та потребують кваліфікованого персоналу для технічної підтримки, однак, виправдовують себе у високоризичних середовищах [6].

Гібридна хмара (hybrid cloud) разом із своїми перевагами двох попередніх моделей, забезпечуючи взаємодію публічного та приватного хмарного середовища. Така інфраструктура дозволяє розподіляти навантаження, розміщуючи чутливі дані у приватному сегменті, а загальнодоступні ресурси — у публічному. Гібридна модель забезпечує гнучкість, оптимізацію вартості, володіння IT-інфраструктурою та дотримання вимог безпеки без шкоди для масштабованості. Водночас ефективне управління такою системою вимагає інтеграційних рішень, уніфікованих політик доступу, а також додаткового засобу для узгодження сервісних рівнів (SLA) між безкоштовними провайдерами.

Окреме місце в класифікації моделей займає спільна хмара (community cloud), яка призначена для обмеженої спільноти з користувачами, подібними до

вимог до політики безпеки, управління та відповідності. Така інфраструктура обслуговує групу організацій, які об'єднуються за галузевим, географічним або функціональним принципом (наприклад, державні установи, освітні заклади або медичні організації). Спільна хмара забезпечує економію ресурсів при одночасному дотриманні високих стандартів захисту даних, що особливо важливо в умовах обмеженого фінансування чи суворих регуляторних вимог. Управління community cloud може здійснюватися спільно самими організаціями або делегуватися сторонньому оператору.

Вибір конкретної моделі розгортання хмарної інфраструктури (див. табл. 1.3) повинен обґрунтовуватися на комплексному аналізі потреб організації, очікуваних обсягів обчислювального навантаження, конфіденційності даних, нормативних обмежень і технічної компетентності персоналу. Універсальної моделі не існує — кожен тип хмари має свою сферу доцільного застосування.

Таблиця 1.3 - Порівняльна схема моделей розгортання хмарної інфраструктури

№	Модель розгортання	Власність	Доступність	Керування	Рівень безпеки	Вартість використання	Типовий користувач
1	Публічна хмара	Постачальник	Відкрита	Постачальник	Середній	Низька	Широкий бізнес, стартапи
2	Приватна хмара	Організація	Обмежена	Організація	Високий	Висока	Корпорації, урядові установи
3	Гібридна хмара	Організація / постачальник	Змішана	Спільне	Залежить від конфігурації	Середня	Великі підприємства
4	Спільна хмара	Кілька організацій	Обмежена	Спільне	Високий	Середня	Галузеві об'єднання, державні структури

Архітектура хмарних обчислень є багаторівневою, комплексною системою, що включає низку взаємопов'язаних компонентів, які забезпечують повноцінне функціонування хмарної інфраструктури. Кожен із цих компонентів

виконує певну роль у процесі надання обчислювальних сервісів, забезпечуючи ефективність, масштабованість, гнучкість і надійність хмарного середовища.

Одним із базових елементів архітектури хмарних обчислень є віртуалізація. Саме вона дозволяє фізичні ресурси – сервери, сховища, мережі – перетворити в логічно ізольовані обчислювальні одиниці, доступні як сервіси. Завдяки віртуалізації на одній фізичній платформі можна одночасно функціонувати кілька віртуальних машин, кожна з яких працює під власною операційною системою і виконує окремі задачі. Основним інструментом реалізації віртуалізації є гіпервізор – програмний засіб, який керує розподілом ресурсів між віртуальними середовищами. Використання технологій віртуалізації сприяє більш раціональному використанню апаратного забезпечення, гнучкому масштабуванню навантаження та покращенню показників відмовостійкості [48].

Наступним компонентом є мережеві ресурси , які забезпечують взаємозв'язок між усією частиною хмарної інфраструктури. До таких ресурсів належать маршрутизатори, комутатори, мережеві контролери, системи балансування навантаження, брендмауери тощо. У контексті хмарних технологій все більшого поширення відбувається віртуалізація мереж (Network Virtualization), яка дозволяє створювати логічні мережі, ізольовані одна від одної, поверх єдиної фізичної інфраструктури. Такий підхід закінчиться безпекою, гнучкістю та керованістю мережевого середовища [4].

Ключову інфраструктурну роль глобальні центри обробки даних (ЦОД). Це фізичні об'єкти, в яких розміщується основне обладнання хмарного середовища: сервери, системи зберігання даних, комунікаційне та електротехнічне обладнання. Сучасні ЦОДи проектуються з урахуванням стандартів енергоефективності, резервування живлення, кондиціонування, протипожежного захисту та фізичної безпеки. Щоб забезпечити високу доступність хмарних сервісів, провайдери створюють розподілені ЦОДі в різних географічних регіонах, що мінімізує затримки та забезпечує катастрофічність.

Невід'ємною частиною архітектури є система управління доступом (Access Control Systems), яка реалізує політику безпеки щодо ідентифікації, автентифікації та авторизації користувачів. Ці системи дозволяють гнучко визначати рівні доступу до інформаційних ресурсів, контролювати дії користувачів у хмарному середовищі та забезпечувати аудит усіх операцій. Сучасні платформи часто інтегрують технології багатофакторної аутентифікації (MFA) , системи управління ідентифікацією (IAM), а також механізми нульової довіри (Zero Trust) [19].

Завершальним програмним, але не меншим компонентом є інтерфейси управління (API) та веб-інтерфейси адміністративного контролю. API забезпечує програмну взаємодію користувача або адміністратора з хмарною платформою — зокрема створення віртуальних машин, управління сховищем, налаштування мережевих ресурсів тощо. Стандартизовані API значно спрощують процес автоматизації та оркестрації ресурсів, інтеграцію хмарних сервісів з іншими IT-системами та забезпечують високу адаптивність архітектури до змін у бізнес-середовищі.

Взаємодія всіх описаних компонентів (див. рис. 1.1) відображається в типових структурах хмарного середовища, що демонструє логічні зв'язки між користувачами, інтерфейсами управління, службами контролю, віртуалізованими ресурсами та фізичною інфраструктурою [44].

Рисунок 1.1 – Типова архітектура хмарного середовища

Організація життєвого циклу даних є фундаментальним аспектом у системі управління інформаційною безпекою хмарних середовищ. Під життєвим циклом дані виконуються після послідовності стадій, які проходять від моменту їх створення або завантаження до остаточного видалення з інформаційної системи. Особливості кожного етапу вимоги до безпеки, відповідності стандартам та політики контролю доступу. У хмарних обчисленнях життєвий цикл даних включає п'ять основних фаз: завантаження, зберігання, обробка, передача та видалення . Кожен із цих етапів супроводжується власними ризиками та критичними точками впливу на захист даних [5].

Початковим етапом життєвого циклу є завантаження даних до хмарного середовища. Це може бути передача даних із локальної системи користувачів у віддалений центр обробки даних або інтеграція з іншими зовнішніми джерелами. Уразливість на цьому етапі обумовлені ризиками перехоплення трафіку, підміни даних, атак типу «man-in-the-middle». Для забезпечення захисту інформації на етапі завантаження необхідно використовувати криптографічні протоколи передачі (зокрема TLS/SSL), багатофакторну автентифікацію , а також контроль цілісності даних .

Після завантаження дані зберігаються у віртуалізованих сховищах хмарної платформи. На цьому етапі особливого значення набуваються механізми ізоляції даних , контролю доступу та шифрування в стані спокою (data-at-rest encryption) . Системи управління даними повинні гарантувати, що інформація різних людей фізично і логічно відокремлена, а несанкціонований доступ до даних неможливий навіть у разі компрометації одного сегмента. Ризики включають порушення конфіденційності через вразливість в API, помилки конфігурації або недостатній аудит доступу [24].

Обробка даних включає аналітичні операції, трансформації, індексування та обчислення, що забезпечуються в хмарному середовищі. На цій фазі можуть виникати загрози, пов'язані з нестабільністю ізоляції середовищ , небезпекою побічних каналів (атаки побічних каналів) або шкідливим кодом , який зданий вплинути при виконанні інших віртуальних машин. З метою підвищення захищеності механізмів контейнеризації , процесів санбоксингу , моніторингу обчислювальних середовищ , а також захищеної обробки даних у пам'яті (шифрування пам'яті, довірених середовищ виконання) .

Передача даних (Data Transmission) передбачає передачу даних між внутрішніми компонентами хмарної платформи, між більшими хмарними середовищами або до кінцевого споживача. Ключовими загрозами є втручання в мережевий трафік , зміна маршруту , зловживання API або несанкціоноване копіювання даних . Для забезпечення безпеки передачі застосовуються VPN-технології , тунелювання трафіку , шифрування point-to-point , а також механізми токенізації та обмеження привілеїв API [45].

Фінальний етап життєвого циклу — це видалення даних після завершення їх використання або за запитом користувача відповідно до політики зберігання. Неналежне виконання цього процесу створює загрозу залишкового доступу до чутливої інформації , яка може бути відновлена з резервних копій або кеш-пам'яті. Для запобігання таким ризикам необхідно впроваджувати процедури безпечного видалення (data sanitization) , включаючи перезаписування даних, криптографічне стирання (crypto-erasure) та контроль видалення через аудит .

Аналіз життєвого циклу дозволяє виділити критичні точки впливу на безпеку, які потребують особливої уваги з боку адміністраторів та користувачів:

- Передача даних (Upload/Transmission) – високий ризик перехоплення або підміни.
- Контроль доступу на етапі зберігання – загроза несанкціонованого доступу до логічних засобів.
- Період активної обробки – виявлена вразливість до атаки через загальні ресурси.
- Неповне видалення даних – загроза доступу до залишкової інформації [47].

Кожна з цих точок повинна бути підкріплена належними механізмами безпеки, що відповідають загальним стандартам інформаційного захисту (ISO/IEC 27001, NIST SP 800-88, CSA Security Guidance). Тільки цільна система управління безпекою дозволяє гарантувати захист інформації на всіх етапах її життєвого циклу в хмарному середовищі.

1.2 Загрози та вразливості хмарних сервісів

Хмарні обчислення, за своєю функціональною ефективністю та технологічною досконалістю, супроводжують низькі загрози, які можуть суттєво вплинути на конфіденційність, цільність та доступність інформаційних ресурсів. Забезпечення інформаційної безпеки в хмарному середовищі неможливо без детального розуміння природи якихось загроз, їх класифікації та оцінки ймовірних наслідків. У зв'язку з цим, більшість є системний підхід до класифікації загроз, що дозволяє організувати процеси управління ризиками та розробляти ефективні контрзаходи [8].

У загальному вигляді загрози хмарній інформаційній безпеці по виділенню джерел походження на внутрішні, зовнішні, техногенні, програмні та соціоінженерні .

Внутрішні загрози (інсайдерські загрози) - тип загрози походять від користувачів, які мають цей легітимний доступ до хмарних ресурсів –

співробітників компанії, адміністраторів, підрядників або партнерів. Внутрішні загрози розділяються на навмисні та ненавмисні [1]:

- Навмисні загрози — умисні дії зловмисників, спрямовані на крадіжку даних, саботаж IT-системи або розголошення конфіденційної інформації.
- Ненавмисні загрози — помилки персоналу, небажане поводження з доступом, нехтування політиками безпеки.
- Особливу безпеку становлять привілейовані користувачі , які мають широкі повноваження в системі [22].
- Зовнішні загрози - до цієї групи загроз входять атаки, що проходять із зовнішнього середовища — хакерів, кіберзлочинних угруповань або автоматизованих шкідливих програм. До основних форм таких загроз належать:
- Несанкціонований доступ до системи (використання викрадених облікових даних, атак на автентифікацію);
- Кібератаки на інтерфейси API , які є критичною частиною хмарної інфраструктури;
- Шкідливе програмне забезпечення (malware) — віруси, трояни, руткити;
- Атаки типу DoS/DDoS — спрямовані на виведення сервісу з ладу через перезавантаження запитами;
- Крадіжка або підміна даних під час передачі через мережу.

Техногенні та програмні загрози - ці загрози виникають внаслідок несправностей апаратного або програмного забезпечення, помилок у конфігурації системи, неякісного технічного обслуговування або збоїв енергоживлення. Прикладами є [33]:

- Вихід з ладу серверного обладнання;
- Програмні помилки, що спричиняють втрату або викривлення даних;
- Недоліки у віртуалізації або механізмах автоматизації.

Техногенні фактори можуть діяти незалежно від людського втручання, але їх вплив на безпеку системи може бути критичним [44].

Соціоінженерні загрози передбачає використання психологічних методів впливу на користувачів для забезпечення доступу до конфіденційної інформації або обхід механізмів безпеки. До типових прикладів належать:

- Фішинг — надсилання фальшивих електронних листів, які імітують легітимні повідомлення;
- Претекстінг — створення переконливих, але фальшивих сценаріїв для виманювання персональних даних;
- Спуфінг — підміна IP-адреси або електронної ідентичності.

Зважаючи на високий рівень цифрової взаємодії в хмарних середовищах, соціоінженерні загрози залишаються одними з найпоширеніших каналів систем компрометації [5].

Для узагальнення класифікації загроз доцільно використовувати таблицю 1.4, яка систематизує типи загроз, джерела їх виникнення та ймовірні дослідження для системи інформаційної безпеки.

Таблиця 1.4 – Класифікація загроз за джерелом та наслідками

№	Джерело загрози	Типові приклади	Ймовірні наслідки
1	Внутрішні	- Несанкціоновані дії привілейованих користувачів - Помилки персоналу	- Витік або викрадання даних - Порушення цілісності або доступності даних
2	Зовнішні	- Хакерські атаки - Malware - DoS/DDoS-атаки	- Знищення або підміна інформації - Втрата доступу до сервісів
3	Техногенні	- Збої апаратного забезпечення - Відмова системи живлення	- Втрата критичних даних - Зупинка бізнес-процесів
4	Програмні	- Помилки у програмному коді - Вразливості системного ПЗ	- Порушення конфіденційності - Ескалація привілеїв
5	Соціоінженерні	- Фішинг - Претекстінг - Спуфінг	- Збереження доступу до системи - Компрометація облікових даних

Класифікація загроз у хмарному середовищі дозволяє побудувати ієрархію ризиків, застосувати найбільш критичні вектори атаки та сформувати відповідні стратегії реагування. Саме систематизований підхід до ідентифікації джерел та

наслідків загроз забезпечує основу для розробки політики управління інформаційною безпекою в умовах динамічного розвитку хмарних сервісів.

Ефективність хмарних обчислень значною мірою визначається рівнем їхньої інформаційної безпеки. Проте, зважаючи на специфіку архітектури та особливості організації обчислювального середовища, хмарна інфраструктура має низку характерних вразливостей, які можуть стати точками входу для потенційних атак. Своєчасна ідентифікація таких вразливостей дозволяє організувати проактивний захист та знизити ризики компрометації даних. Нижче наведено системний опис найбільш критичних вразливостей [37].

Хмарні сервіси за своєю природою інтегруються у глобальне мережеве середовище, що автоматично підвищує їхню експозицію до мережевих атак. До найбільш поширених проблем належить використання незашифрованих протоколів передавання даних (наприклад, Telnet, HTTP), недостатня сегментація мережі, неправильне налаштування міжмережевих екранів, а також відсутність обмежень на вхідний/вихідний трафік. Зловмисники можуть здійснювати перехоплення даних, ін'єкції, сканування портів або запускати атаки типу DDoS, спрямовані на виведення сервісу з ладу [10].

Недостатньо захищені механізми автентифікації є однією з найрозповсюдженіших точок компрометації. Вони включають використання слабких або повторно використаних паролів, відсутність багатофакторної автентифікації (MFA), обмежену політику управління правами доступу та недостатній моніторинг підозрілих дій користувачів. Подібні недоліки відкривають шлях для атак типу brute-force, credential stuffing або соціоінженерних технік, зокрема фішингу [41].

Технології віртуалізації лежать в основі хмарної інфраструктури, але водночас створюють специфічні вектори атак. Найбільш серйозною вразливістю є злом гіпервізора, що дозволяє зловмиснику отримати доступ до інших віртуальних машин на тому самому фізичному сервері. Іншими проблемами є недостатня ізоляція клієнтських середовищ, небезпека бокових каналів (side-

channel attacks), а також експлуатація спільно використовуваних ресурсів (memory leakage, shared cache attacks).

Хмарні платформи надають доступ до своїх функцій через інтерфейси прикладного програмування (API). Неналежно захищені API стають частими цілями атак, оскільки через них зловмисник може здійснити несанкціонований доступ до внутрішньої інфраструктури. Основні загрози включають відсутність обмежень запитів, неправильну авторизацію, відкритість до атак типу injection та несанкціоноване використання токенів доступу. У багатьох випадках саме API є слабкою ланкою, що обходить традиційні механізми контролю безпеки [4].

Хмарне зберігання даних передбачає використання загальнодоступної інфраструктури, тому конфіденційність інформації безпосередньо залежить від застосованих криптографічних засобів захисту. Основні загрози виникають при відсутності шифрування даних у стані спокою (data at rest), небезпеці втрати ключів шифрування, неконтрольованому створенні резервних копій, а також неналежній політиці керування життєвим циклом даних. У разі компрометації сховища наслідки можуть бути катастрофічними — від повного розголошення даних до їхнього незворотного знищення [35].

Наведена класифікація вразливостей (табл. 1.5) дозволяє не лише систематизувати типові технічні недоліки хмарної інфраструктури, але й демонструє можливі сценарії атак, що актуалізує потребу в комплексному підході до організації системи кіберзахисту у хмарному середовищі.

Таблиця 1.5 – Типові вразливості хмарних сервісів з прикладами атак

№	Тип вразливості	Суть вразливості	Приклади атак
1	2	3	4
1	Мережеві вразливості	Незахищені порти, відсутність шифрування трафіку, відкриті протоколи	DDoS-атаки, перехоплення даних, атаки Man-in-the-Middle
2	Проблеми автентифікації	Слабкі паролі, відсутність MFA, погана сегментація ролей	Credential stuffing, Brute-force, фішинг
3	Вразливості віртуалізації	Недосконала ізоляція ВМ, експлуатація гіпервізора	Атаки на гіпервізор, side-channel атаки, вертикальна ескалація прав
4	Уразливості API	Відкриті API, відсутність контролю доступу, незахищені токени	Ін'єкції команд, атаки на REST API, несанкціоноване виконання

Продовження таблиці 1.5

1	2	3	4
5	Недоліки зберігання/шифрування	Не шифровані дані, втрата ключів, компрометація резервного сховища	Розголошення чутливої інформації, підміна або знищення даних

Хмарні сервіси, попри свою зручність та ефективність, є об'єктом різноманітних кіберзагроз. Розуміння типових атак на такі сервіси є ключовим для розробки ефективних стратегій захисту [36].

Типові атаки на хмарні сервіси:

1. DoS/DDoS (Denial of Service/Distributed Denial of Service):
   - DoS-атака спрямована на виведення сервісу з ладу шляхом перевантаження його ресурсів великою кількістю запитів. Це призводить до недоступності сервісу для легітимних користувачів.
   - DDoS-атака є розподіленою версією DoS, коли атака здійснюється з багатьох скомпрометованих пристроїв одночасно, що ускладнює її відбиття.
2. SQL-ін'єкції - цей вид атаки полягає у впровадженні шкідливого SQL-коду через вразливі поля вводу в веб-додатках. Це може дозволити зловмиснику отримати несанкціонований доступ до бази даних, змінювати або видаляти дані.
3. Перехоплення трафіку - зловмисники можуть використовувати незашифрований або недостатньо захищений трафік для перехоплення конфіденційної інформації, такої як облікові дані користувачів.
4. Man-in-the-Middle (MitM) - у цій атаці зловмисник перехоплює та потенційно змінює комунікацію між двома сторонами без їхнього відома, що дозволяє отримати доступ до переданої інформації або внести в неї зміни.
5. Cross-tenant атаки - у багатокористувацьких (multi-tenant) хмарних середовищах, де ресурси спільно використовуються кількома клієнтами, вразливості можуть дозволити одному клієнту отримати доступ до даних або ресурсів іншого клієнта [7].

6. Side-channel атаки - ці атаки використовують непрямі дані, такі як споживання енергії або час виконання операцій, щоб отримати інформацію про систему або дані, які вона обробляє.

Розуміння та аналіз зазначених атак є критично важливими для розробки ефективних заходів безпеки та мінімізації ризиків у хмарних інфраструктурах.

Одним із ключових джерел сучасного уявлення про ризики у сфері хмарної безпеки є аналітична модель загроз, що формується Cloud Security Alliance (CSA) — провідною міжнародною організацією, яка займається стандартизацією, просвітництвом і аналітичним моніторингом безпеки хмарних технологій. CSA регулярно публікує звіти під назвою “Top Threats to Cloud Computing”, які відображають поточні тенденції загроз (див. рис. 1.2) та вразливостей, що мають найбільший вплив на безпеку хмарних середовищ [30].

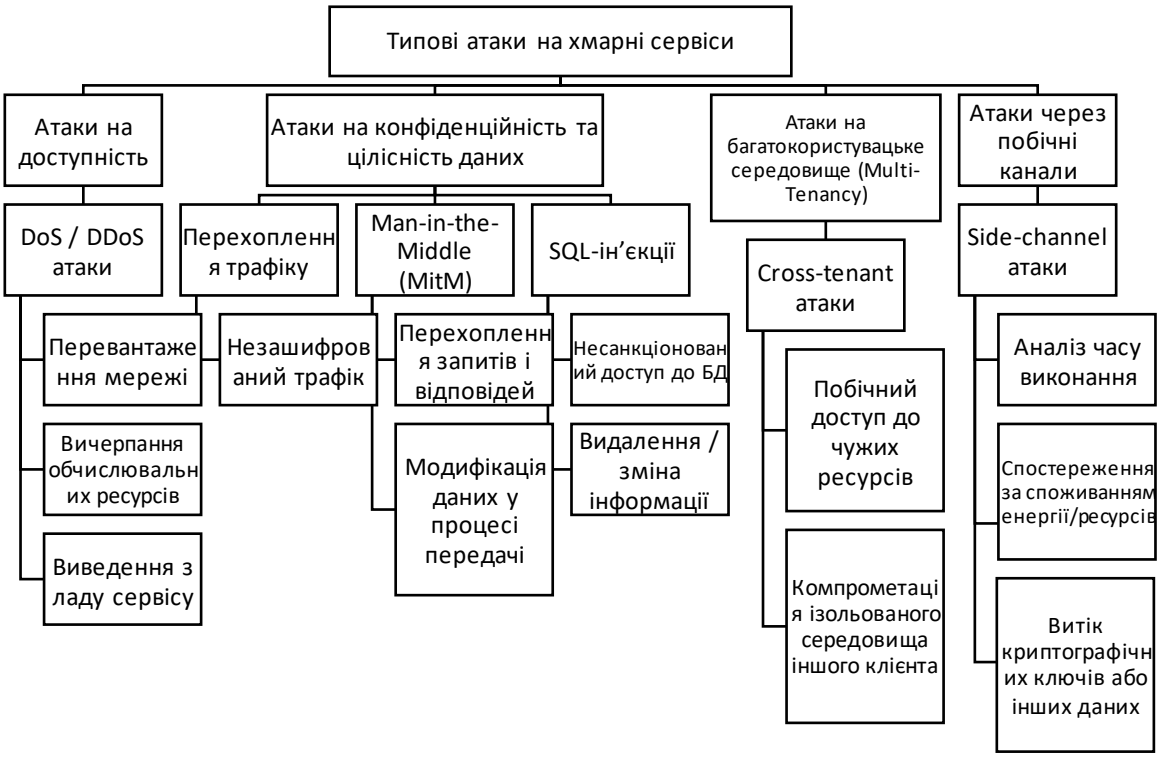

Рисунок 1.2 – Схема типових атак на хмарні сервіси

У звіті CSA 2023/2024 року, базованому на міжнародному опитуванні експертів з безпеки, окреслено найкритичніші загрози, які становлять ризик для організацій, що використовують хмарну інфраструктуру. Відмінною

особливістю цієї моделі є акцент на практичну значущість загроз, які найчастіше трапляються на практиці або призводять до серйозних інцидентів.

Ці загрози умовно охоплюють усі аспекти хмарної екосистеми — від проблем конфігурації та доступу до вразливостей API, програмного коду та ланцюгів постачання (supply chain). Згідно з CSA, найбільш поширені інциденти виникають саме через людські помилки, слабке управління доступом, недостатню автоматизацію політик безпеки та зростаючу складність інтегрованих хмарних архітектур [31].

Слід зазначити, що модель CSA не лише дозволяє систематизувати ризики, а й слугує орієнтиром для побудови захисних механізмів, включаючи стратегії виявлення загроз, реагування на інциденти, побудови архітектур Zero Trust та удосконалення процесів DevSecOps.

Таблиця 1.6 систематизує ключові загрози відповідно до звіту Cloud Security Alliance (CSA), створюючи основу для аналізу ризиків та розробки політик кіберзахисту у хмарному середовищі. Її використання дозволяє структурувати стратегічні пріоритети в управлінні безпекою хмарних ресурсів.

Таблиця 1.6 – ТОП-10 загроз за CSA 2023/2024

№	Загроза	Сутність проблеми
1	Неправильна конфігурація та слабкий контроль змін	Хибні налаштування ресурсів відкривають зовнішній доступ до критичних даних
2	Недостатня стратегія хмарної безпеки	Відсутність політик, процедур, автоматизованого контролю безпеки
3	Небезпечні інтерфейси та API	Відсутність автентифікації, погане управління токенами, відкритість до ін’єкцій
4	Недостатнє управління ідентифікацією, обліковими даними та доступом	Ненадійна автентифікація, привілейований доступ, відсутність MFA
5	Ненадійна архітектура безпеки	Вразлива або нефункціональна модель контролю захисту у багаторівневих системах
6	Небезпечна розробка програмного забезпечення	Ігнорування стандартів безпечного кодування, недоліки DevSecOps
7	Уразливості ланцюга постачання (third-party/SaaS)	Залежність від третіх сторін із ненадійними практиками захисту
8	Системні вразливості	Прогалини в платформах, ОС, драйверах, віртуалізації, контейнеризації
9	Випадкове розкриття даних	Людський фактор: публічні сховища, неправильні політики доступу
10	Неправильне впровадження контейнерних або безсерверних технологій	Хибна конфігурація контейнерів або функцій без сервера (FaaS), уразливі залежності

Реалізація загроз інформаційній безпеці може мати серйозні наслідки для організацій, впливаючи на фінансові показники, репутацію, правовий статус та бізнес-процеси.

Кібератаки можуть призвести до значних фінансових втрат, включаючи витрати на відновлення систем, компенсації клієнтам та штрафи за недотримання нормативних вимог. Наприклад, великі фінансові установи можуть втратити мільйони доларів через злами даних [10].

Порушення безпеки даних підривають довіру клієнтів, що може призвести до втрати клієнтської бази та зменшення прибутків. Компанії, які не забезпечують належний захист даних, ризикують втратити свою репутацію на ринку.

Недотримання законодавчих вимог щодо захисту даних може призвести до юридичних наслідків, включаючи штрафи та судові позови. Наприклад, порушення GDPR в Європейському Союзі може призвести до значних штрафів за недотримання вимог щодо захисту персональних даних [20].

Кібератаки можуть порушити операційну діяльність компанії, спричиняючи збої в бізнес-процесах, втрату даних та зниження продуктивності. Це може призвести до затримок у виконанні замовлень, втрати конкурентоспроможності та додаткових витрат на відновлення.

Загалом, реалізація загроз інформаційній безпеці може мати комплексний негативний вплив на організацію, підкреслюючи важливість впровадження ефективних заходів кібербезпеки.

1.3 Стандарти та нормативно-правове регулювання безпеки хмарних сервісів

Міжнародні стандарти безпеки відіграють ключову роль у забезпеченні захисту інформації та управлінні ризиками в організаціях. Вони надають загальновизнані рамки та рекомендації для впровадження ефективних заходів безпеки. Нижче розглянемо основні з них [40]:

1. ISO/IEC 27001 є міжнародно визнаним стандартом для систем управління інформаційною безпекою (СУІБ). Він визначає вимоги до встановлення, впровадження, підтримки та постійного вдосконалення СУІБ в організації. Стандарт спрямований на забезпечення конфіденційності, цілісності та доступності інформації шляхом застосування системного підходу до управління ризиками [32].

2. ISO/IEC 27002 доповнює ISO/IEC 27001, надаючи детальні рекомендації щодо впровадження заходів безпеки. Він містить набір найкращих практик для управління інформаційною безпекою, охоплюючи такі аспекти, як політики безпеки, організація інформаційної безпеки, управління активами, контроль доступу та інші.

3. ISO/IEC 27017 надає рекомендації щодо заходів безпеки, специфічних для хмарних сервісів. Він включає додаткові контролі та вказівки для постачальників та споживачів хмарних послуг, спрямовані на забезпечення безпеки в хмарному середовищі. Цей стандарт допомагає чітко визначити відповідальність обох сторін щодо впровадження та підтримки заходів безпеки.

4. ISO/IEC 27018 є першим міжнародним стандартом, який фокусується на захисті персонально ідентифікованої інформації (PII) у публічних хмарних сервісах. Він надає настанови для постачальників хмарних послуг щодо впровадження заходів захисту PII, забезпечуючи відповідність правовим та регуляторним вимогам у сфері конфіденційності.

5. Національний інститут стандартів і технологій США (NIST) розробив серію спеціальних публікацій, серед яких SP 800-53 та SP 500-292. SP 800-53 містить каталог заходів безпеки для федеральних інформаційних систем США, які можуть бути адаптовані й іншими організаціями для управління ризиками. SP 500-292 надає архітектурний опис хмарних обчислень, включаючи рекомендації щодо безпеки в хмарному середовищі.

6. Cloud Security Alliance (CSA) розробила програму Security, Trust & Assurance Registry (STAR), яка є системою забезпечення безпеки для постачальників хмарних послуг. Вона включає три рівні забезпечення:

самооцінка, сертифікація третьою стороною та постійний моніторинг. CSA STAR базується на матриці контролю безпеки хмари (Cloud Controls Matrix, CCM), яка узгоджується з іншими стандартами, такими як ISO/IEC 27001, PCI/DSS та іншими [46].

Впровадження цих стандартів допомагає організаціям створити надійну систему управління інформаційною безпекою, забезпечити відповідність нормативним вимогам та підвищити довіру клієнтів і партнерів.

У сучасному цифровому середовищі питання захисту персональних даних стало одним із ключових елементів забезпечення інформаційної безпеки, особливо у контексті використання хмарних технологій. Хмарна інфраструктура передбачає віддалене зберігання, обробку й передачу значних обсягів конфіденційної інформації, що актуалізує необхідність чіткого правового регулювання процесів обробки персональних даних відповідно до міжнародних стандартів та локального законодавства.

Одним із основоположних нормативних актів, який визначає правові засади захисту персональних даних у межах Європейського Союзу, є Загальний регламент про захист даних (General Data Protection Regulation – GDPR). Регламент набув чинності 25 травня 2018 року та замінив попередню Директиву 95/46/ЕС. Його головною метою є створення єдиного правового механізму захисту персональних даних громадян ЄС, незалежно від того, де фізично обробляються або зберігаються ці дані. GDPR має екстериторіальний характер, тобто поширюється також на компанії, які обробляють дані громадян ЄС, незалежно від їх географічного розташування [30].

GDPR встановлює низку ключових принципів обробки персональних даних: законність, справедливість, прозорість, обмеження метою, мінімізація обсягів даних, точність, обмеження строку зберігання, цілісність, конфіденційність та підзвітність. У межах регламенту передбачено значний перелік прав суб'єктів персональних даних: право на доступ, виправлення, обмеження обробки, перенесення даних, заперечення обробки та «право бути забутим». З метою забезпечення дотримання цих норм, GDPR передбачає високі

штрафні санкції – до 20 мільйонів євро або 4% річного обороту компанії, залежно від того, яка сума є більшою [19].

Не менш важливим нормативним актом у сфері захисту персональної інформації є Закон Каліфорнії про конфіденційність споживачів (California Consumer Privacy Act – CCPA), який набув чинності 1 січня 2020 року. CCPA став першим в США законодавчим актом, що комплексно регулює обробку персональних даних споживачів, закріплюючи права на інформацію, доступ, видалення, відмову від продажу персональних даних та заборону дискримінації при реалізації цих прав. Хоча CCPA дещо поступається за жорсткістю вимог GDPR, він суттєво вплинув на підходи до захисту даних в американському сегменті IT-ринку [36].

Основні положення CCPA зосереджені на:

- наданні споживачам права знати, які дані збираються про них і з якою метою;
- можливості вимагати видалення або обмеження використання персональних даних;
- забороні продажу даних третім сторонам без згоди користувача;
- забезпеченні прозорості політик обробки даних та їх публічному розкритті [22].

З метою посилення дії CCPA, 1 січня 2023 року в штаті Каліфорнія набув чинності California Privacy Rights Act (CPRA) — доповнення до CCPA, яке вводить нові категорії конфіденційних даних та створює незалежний орган – California Privacy Protection Agency (CPPA) для контролю дотримання законодавства.

Разом з тим, локальне законодавство також відіграє важливу роль у регулюванні обробки персональних даних. В Україні правові засади захисту персональних даних закріплені у Законі України «Про захист персональних даних», який діє з 2011 року. Закон визначає порядок обробки, зберігання, використання, доступу та захисту персональної інформації фізичних осіб, а також права суб'єктів персональних даних та обов'язки володільців і

розпорядників цих даних. Українське законодавство гармонізується з європейським у контексті зобов'язань країни щодо євроінтеграції та імплементації положень GDPR [32].

Ключові положення українського Закону «Про захист персональних даних»:

- персональні дані можуть оброблятися лише з правомірною метою;
- забороняється обробка особливих категорій даних без згоди суб'єкта;
- суб'єкт має право доступу, виправлення, обмеження обробки та заборони поширення даних;
- необхідність реєстрації баз персональних даних та впровадження технічних заходів безпеки.

У зв'язку з поширенням хмарних сервісів, важливою є імплементація правових норм у контексті територіального зберігання даних, взаємодії з міжнародними провайдерами та підрядниками, забезпечення еквівалентного рівня захисту у крос-кордонних передачах даних. Саме тому організаціям, які оперують у хмарних середовищах, необхідно впроваджувати Data Protection Impact Assessment (DPIA), privacy by design та privacy by default, як це передбачено сучасним правовим полем [51].

Національне регулювання інформаційної безпеки в Україні базується на комплексі законодавчих актів, державних стандартів та діяльності спеціалізованих органів. Ця система спрямована на забезпечення захисту інформації, підтримання цілісності та конфіденційності даних, а також на протидію кіберзагрозам [1].

Цей закон, прийнятий 5 липня 1994 року, визначає правові основи захисту інформації в інформаційно-комунікаційних системах. Він регулює відносини, пов'язані із захистом інформації від несанкціонованого доступу, встановлює обов'язки власників та користувачів систем щодо забезпечення безпеки даних. Закон також визначає поняття комплексної системи захисту інформації та встановлює відповідальність за порушення законодавства у цій сфері.

Цей закон регулює діяльність у сфері електронних комунікацій, встановлює правові засади для надання електронних комунікаційних послуг та експлуатації електронних комунікаційних мереж. Він визначає права та обов'язки постачальників і користувачів послуг, а також встановлює вимоги щодо безпеки та захисту інформації в електронних комунікаційних мережах.

Державні стандарти України (ДСТУ), гармонізовані з міжнародними стандартами ISO/IEC, встановлюють вимоги та рекомендації щодо управління інформаційною безпекою. Зокрема [4]:

- ДСТУ ISO/IEC 27001 - визначає вимоги до систем управління інформаційною безпекою.
- ДСТУ ISO/IEC 27002 - містить практичні рекомендації щодо заходів інформаційної безпеки.
- ДСТУ ISO/IEC 27017 - надає настанови щодо безпеки хмарних сервісів.
- ДСТУ ISO/IEC 27018 - зосереджується на захисті персональних даних у хмарних середовищах.

Ці стандарти допомагають організаціям впроваджувати ефективні заходи для захисту інформації відповідно до міжнародних практик.

Кіберполіція є підрозділом Національної поліції України, відповідальним за протидію кіберзлочинності. Її основні завдання включають:

- реалізацію державної політики у сфері протидії кіберзлочинності;
- інформування населення про нові кіберзагрози;
- впровадження програмних засобів для систематизації кіберінцидентів;
- реагування на запити зарубіжних партнерів щодо кібербезпеки.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) є центральним органом виконавчої влади, відповідальним за реалізацію державної політики у сфері захисту інформації та кібербезпеки. Її функції включають [22]:

- забезпечення захисту державних інформаційних ресурсів;

- координацію діяльності у сфері кіберзахисту критичної інформаційної інфраструктури;
- впровадження організаційних та технічних заходів для запобігання та реагування на кіберінциденти;
- інформування про кіберзагрози та відповідні методи захисту.

Таким чином, національне регулювання інформаційної безпеки в Україні базується на законодавчих актах, державних стандартах та діяльності спеціалізованих органів, що забезпечують комплексний підхід до захисту інформації та протидії кіберзагрозам.

РОЗДІЛ 2 МЕТОДИ ОЦІНКИ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

2.1 Критерії оцінки безпеки хмарних сервісів

У сучасних інформаційних системах хмарні обчислення відіграють ключову роль, забезпечуючи гнучкість, масштабованість та економічну ефективність. Проте, поряд із перевагами, використання хмарних технологій супроводжується значними ризиками, пов'язаними із захистом даних, конфіденційністю та дотриманням нормативних вимог. Відсутність належної оцінки безпеки може призвести до несанкціонованого доступу, витоку інформації та інших інцидентів, що негативно впливають на діяльність організації. Тому систематична оцінка безпеки хмарних сервісів є критично важливою для ідентифікації потенційних загроз, аналізу вразливостей та розробки ефективних заходів захисту [45].

Під "критерієм безпеки" розуміють встановлений показник або набір показників, що використовуються для оцінки рівня захищеності інформаційної системи чи її компонентів. Ці критерії слугують основою для вимірювання відповідності системи заданим стандартам безпеки та визначення ступеня її стійкості до потенційних загроз. Вони охоплюють різні аспекти, такі як конфіденційність, цілісність, доступність, автентифікація, авторизація та аудит.

Критерії безпеки є фундаментом для створення та підтримки надійного хмарного середовища. Вони дозволяють [27]:

- Стандартизувати підходи до безпеки - визначення чітких критеріїв сприяє уніфікації методів оцінки та забезпечення безпеки, що полегшує інтеграцію різних систем та сервісів.
- Ідентифікувати та аналізувати ризики - застосування критеріїв допомагає виявити потенційні вразливості та оцінити ймовірність та можливі наслідки їх експлуатації.
- Розробляти політики та процедури безпеки - на основі встановлених критеріїв формуються політики, що регламентують заходи захисту,

процедури реагування на інциденти та плани відновлення після збоїв.

– Забезпечувати відповідність нормативним вимогам - критерії безпеки допомагають організаціям дотримуватися міжнародних стандартів та регуляторних актів, що є обов'язковими у певних галузях [53].

Чітко визначені та належним чином застосовані критерії безпеки є невід'ємною складовою процесу побудови та підтримки захищеного хмарного середовища, що відповідає сучасним вимогам та викликам інформаційної безпеки.

У процесі оцінки безпеки хмарних сервісів важливо використовувати систематизований підхід, що передбачає класифікацію критеріїв безпеки за різними напрямами.

Загалом, ці критерії можна поділити на три основні категорії: загальні, технічні та адміністративні.

1. Загальні критерії безпеки (CIA-тріада) [31]:

– Конфіденційність (Confidentiality) - гарантує, що доступ до даних мають лише уповноважені особи, запобігаючи несанкціонованому розголошенню інформації.

– Цілісність (Integrity) - забезпечує точність і повноту даних, запобігаючи їх несанкціонованій модифікації або знищенню [46].

– Доступність (Availability) - гарантує, що дані та ресурси доступні користувачам за потреби, мінімізуючи простої та збої в роботі системи.

2. Технічні критерії безпеки:

– Шифрування - використання криптографічних методів для захисту даних під час їх передачі та зберігання, забезпечуючи конфіденційність і цілісність інформації.

- Захист каналів зв'язку - забезпечення безпечного обміну даними між користувачами та хмарними сервісами через використання захищених протоколів зв'язку (наприклад, TLS/SSL) [35].
- Автентифікація - процедури перевірки особи користувача перед наданням доступу до системи, включаючи багатофакторну автентифікацію для підвищення рівня безпеки.

3. Адміністративні критерії безпеки:

- Політики безпеки - розробка та впровадження організаційних правил і процедур, що регламентують заходи з інформаційної безпеки та поведінку користувачів.
- Моніторинг - постійне відстеження та аналіз подій у системі для виявлення та реагування на потенційні інциденти безпеки.
- Аудит - періодична перевірка відповідності системи встановленим політикам і стандартам безпеки, а також оцінка ефективності впроваджених заходів захисту [51].

Ця класифікація сприяє систематичному підходу до оцінки та забезпечення безпеки хмарних сервісів, дозволяючи організаціям ефективно ідентифікувати та усувати потенційні загрози в кожній з перелічених областей.

Забезпечення інформаційної безпеки в умовах хмарних обчислень вимагає застосування чітко визначених критеріїв, що дозволяють оцінити рівень захисту даних та інфраструктури. До таких критеріїв (див. табл. 2.1) належать конфіденційність, цілісність, доступність, аудит і логування, шифрування, а також ідентифікація та контроль доступу.

Таблиця 2.1– Характеристика критеріїв безпеки хмарних сервісів

№	Критерій безпеки	Механізми забезпечення	Приклади реалізації
1	**2**	**3**	**4**
1	Конфіденційність	Шифрування даних, контроль доступу, автентифікація користувачів	Google Workspace (TLS, MFA), AWS IAM-політики
2	Цілісність	Хеш-функції, цифрові підписи, контрольні суми, журнали змін	SHA-256 у backup-сервісах, цифрові підписи в Google Docs

Продовження таблиці 2.1

1	2	3	4
3	Доступність	Резервне копіювання, кластеризація, балансування навантаження, SLA	Amazon EC2 (99.99% SLA), Azure Load Balancer
4	Аудит та логування	Системи логування, аудит доступу, моніторинг активності	AWS CloudTrail, Azure Security Center
5	Шифрування	Симетричне (AES), асиметричне (RSA), TLS-протоколи	Google Cloud (AES-256, TLS 1.3), Microsoft 365 Data Encryption
6	Ідентифікація і контроль доступу	MFA, ролі користувачів (RBAC), обмеження IP-адрес	AWS IAM із обмеженням доступу, Microsoft Azure MFA, Google Admin IP Management

Початковим елементом захисту виступає конфіденційність. Вона полягає у тому, щоб інформація не стала доступною стороннім особам. Для її забезпечення широко використовуються шифрування, контроль доступу до облікових записів, багатофакторна автентифікація. Зокрема, сервіси Google Workspace реалізують TLS 1.3 для захищеної передачі даних та пропонують обов'язкову двоетапну перевірку при вході в систему.

Однак, навіть за умов захищеного доступу, важливо гарантувати, що дані залишаються незмінними. Тут на перший план виходить критерій цілісності. Завдяки використанню хеш-функцій, таких як SHA-256, цифрових підписів і логів змін, хмарні сервіси можуть виявляти будь-які модифікації даних. Наприклад, у Google Docs інтегровано механізми відстеження змін із можливістю їх верифікації.

У випадках, коли дані необхідно використовувати безперервно, критично важливою стає доступність. Вона реалізується через реплікацію серверів, створення резервних копій, географічне дублювання даних, а також укладення SLA-договорів між клієнтом і провайдером. Amazon EC2, наприклад, гарантує доступність на рівні 99,99%.

Забезпечення надійного функціонування також передбачає можливість відстеження усіх дій у системі. Для цього використовується аудит і логування. Хмарні провайдери, такі як AWS та Azure, впроваджують системи аналітики логів, що дозволяють не лише зберігати сліди активності, а й аналізувати поведінкові шаблони, виявляючи потенційні загрози [18].

Невід'ємною складовою всієї системи є шифрування. Воно охоплює як збереження даних (ат-рес), так і їх передачу (ін-транзит). У Google Cloud дані шифруються за стандартом AES-256 автоматично, а всі з'єднання захищені протоколами TLS.

І, зрештою, фундаментом контролю над доступом виступає система ідентифікації. Впровадження ролей користувачів (RBAC), MFA, а також фільтрація IP-адрес дає змогу контролювати, хто, коли та з якого пристрою має змогу увійти в систему. Усі сучасні хмарні провайдери, зокрема AWS, Microsoft Azure та Google Cloud, надають широкі можливості для конфігурації доступу до окремих ресурсів [37].

Отже, всі наведені критерії тісно взаємопов'язані. Порушення одного з них може нівелювати дію інших. Саме тому забезпечення безпеки в хмарних середовищах повинно здійснюватися комплексно, з урахуванням як технічних, так і адміністративних аспектів.

Забезпечення безпеки в хмарних обчисленнях потребує комплексного підходу, який охоплює різні рівні захисту – від ідентифікації користувачів до моніторингу та реагування на інциденти. Відповідна модель, наведена на рисунку 2.1, демонструє послідовність та взаємозв'язок ключових механізмів безпеки, які формують цілісну систему захисту даних у хмарному середовищі.

Рисунок 2.1 – Модель забезпечення безпеки даних у хмарному середовищі

На першому рівні функціонує система ідентифікації та автентифікації, що забезпечує перевірку особи користувача перед наданням доступу. Тут зазвичай

використовуються механізми багатофакторної автентифікації (MFA), рольового доступу (RBAC) та політики доступу на основі атрибутів [15].

Другий рівень охоплює контроль доступу до ресурсів, реалізований через визначення прав доступу до конкретних об'єктів – файлів, віртуальних машин, баз даних тощо. На цьому етапі важливо враховувати принцип найменших привілеїв, відповідно до якого кожен користувач отримує лише той рівень доступу, який необхідний для виконання його завдань.

Наступним блоком виступає шифрування даних як у стані зберігання (at-rest), так і при передаванні (in-transit). Сучасні хмарні провайдери застосовують алгоритми AES-256 для зберігання та TLS 1.2/1.3 для передавання даних, що забезпечує високий рівень конфіденційності.

Четвертий рівень – моніторинг, аудит та логування – забезпечує постійний контроль за активністю користувачів і систем. Ведення логів, аналіз подій та їх візуалізація дозволяють оперативно виявляти аномалії, реагувати на інциденти та дотримуватися нормативних вимог [45].

Фінальним компонентом є відновлення після інцидентів та резервне копіювання. Завдяки регулярному створенню резервних копій та реплікації даних у різних дата-центрах можливо забезпечити безперервність бізнес-процесів навіть у разі порушення роботи окремих вузлів системи [37].

У процесі забезпечення безпеки хмарних обчислень (див. табл. 2.2) важливо не лише визначати окремі критерії, а й аналізувати, як саме вони реалізуються на конкретних платформах. Для цього доцільно порівняти підходи провідних постачальників хмарних послуг — Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP). Кожна з цих платформ інтегрує власну модель забезпечення інформаційної безпеки, адаптовану до стандартів, внутрішніх архітектурних рішень та інфраструктури [1].

Таблиця 2.2 – Застосування критеріїв безпеки до відомих хмарних платформ

№	Критерій	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
1	Конфіденційність	AWS Identity and Access Management (IAM), MFA, TLS	Azure Active Directory, Conditional Access, TLS/SSL	Cloud Identity, OAuth 2.0, Default encryption in transit
2	Цілісність	AWS CloudTrail, Checksums, Amazon Macie	Azure Monitor, Hash Validation, Integrity Checks	Cloud Logging, SHA-256 checksums
3	Доступність	Multi-AZ deployment, ELB, SLA 99.99%	Availability Sets, Load Balancer, SLA 99.95%	Redundant storage, Global Load Balancer, SLA 99.95%
4	Аудит і логування	CloudTrail, AWS Config, GuardDuty	Azure Security Center, Log Analytics, Audit Logs	Cloud Audit Logs, Chronicle Security Operations
5	Шифрування	AES-256 at-rest, TLS 1.2/1.3 in-transit, KMS	Encryption at rest and in transit, Azure Key Vault	Default AES-256, Customer-Managed Encryption Keys
6	Ідентифікація доступу	IAM, Role-based access control (RBAC), Policy JSON	Azure RBAC, Just-in-Time Access, Privileged Identity Mgmt	IAM with fine-grained access, IP restrictions, SSO

Усі платформи дотримуються базових вимог безпеки, однак реалізують їх через різні сервіси та механізми. Зокрема, для забезпечення конфіденційності AWS застосовує систему IAM та багатоетапну автентифікацію, тоді як Azure реалізує аналогічну функціональність через Active Directory з можливістю налаштування умовного доступу.

Щодо цілісності, Google Cloud забезпечує контроль за допомогою Cloud Logging та SHA-256-перевірок, у той час як AWS пропонує CloudTrail для аудиту та Macie — для виявлення аномалій у даних [15].

Критерій доступності досягається через механізми розподілу навантаження та географічної реплікації. Наприклад, у AWS доступність підвищується завдяки Multi-AZ deployment і Elastic Load Balancer, тоді як Azure використовує Availability Sets та Load Balancer, що працює в рамках SLA 99.95%.

Функції аудиту і логування присутні на кожній платформі, проте реалізовані з використанням специфічних сервісів. Так, AWS GuardDuty надає

інтелектуальний аналіз загроз, Azure Security Center здійснює комплексний моніторинг, а GCP Chronicle забезпечує аналіз безпекових подій на рівні корпорацій [39].

Шифрування підтримується на всіх платформах як для даних у спокої, так і під час передачі. Особливістю Google Cloud є шифрування всіх даних за замовчуванням навіть без додаткової конфігурації з боку користувача, на відміну від Azure, де клієнт має більше можливостей для налаштування керованих ключів.

Управління доступом реалізується на базі RBAC-моделі в усіх трьох середовищах, проте AWS пропонує найгнучкіший механізм з підтримкою JSON-політик, а Azure додатково впроваджує керування привілейованими обліковими записами та можливість доступу "Just-in-Time" [44].

Незважаючи на відмінності в назвах та інтерфейсах, усі три провайдери впроваджують однакову логіку захисту даних згідно з міжнародними стандартами інформаційної безпеки. Вибір платформи залежить від індивідуальних вимог організації, типу даних і пріоритетів у галузі безпеки.

Рисунок 2.2 відображає порівняння багаторівневих структур безпеки трьох провідних хмарних платформ: Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP). Порівняння здійснено за чотирма ключовими рівнями: ідентифікація та автентифікація, контроль доступу, шифрування, а також інфраструктурний рівень захисту.

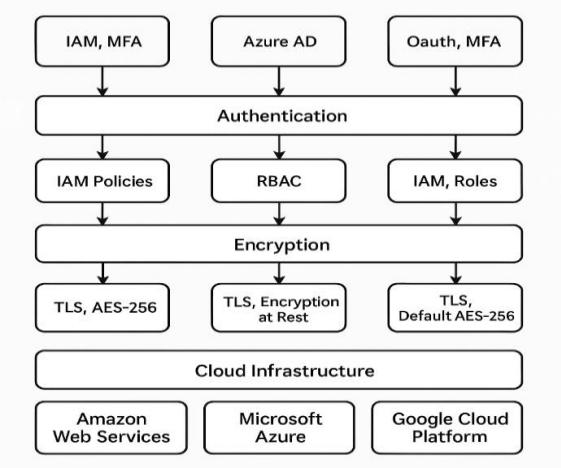

Рисунок 2.2 – Порівняльна архітектура безпеки AWS, Azure і Google Cloud Platform

На першому рівні — аутентифікації — всі три провайдери пропонують підтримку багатофакторної автентифікації (MFA), а також інтеграцію з зовнішніми постачальниками ідентичностей (наприклад, SAML, OAuth 2.0). AWS реалізує це через сервіс IAM, Azure — через Active Directory, а Google — через Cloud Identity та SSO [4].

Другий рівень — контроль доступу — забезпечується через моделі управління правами користувачів. Усі провайдери підтримують Role-Based Access Control (RBAC), однак реалізація відрізняється гнучкістю. AWS дозволяє формувати детальні JSON-політики доступу, Azure підтримує умовний доступ і обмеження за часом, а Google забезпечує гнучке делегування прав на основі атрибутів [60].

Третій рівень — шифрування — передбачає захист даних як у стані зберігання (at rest), так і при передаванні (in transit). Усі три платформи використовують шифрування за замовчуванням із підтримкою алгоритмів AES-256 і TLS 1.2/1.3. Водночас, Google Cloud забезпечує автоматичне шифрування всіх даних без втручання користувача, що вигідно вирізняє її серед конкурентів [10].

Четвертий рівень — інфраструктурний захист — охоплює функції виявлення загроз, моніторингу активності, забезпечення доступності та реагування на інциденти. AWS застосовує GuardDuty, CloudTrail і механізми міжрегіональної реплікації. Azure впроваджує Security Center і Log Analytics, тоді як GCP реалізує Chronicle та Cloud Audit Logs для розширеного моніторингу.

Візуальна структура демонструє, що хоча кожна з платформ дотримується однакових базових принципів безпеки, конкретні інструменти та підходи мають суттєві особливості. Це дозволяє підприємствам обирати платформу з урахуванням специфіки бізнес-процесів, вимог до нормативного регулювання та бажаного рівня контролю [16].

Візуальна оцінка рівня реалізації основних критеріїв безпеки на різних платформах представленна на рисунку 2.3. Як видно з рисунка, всі три провайдери мають високий рівень реалізації критичних вимог, з незначними

варіаціями у підходах. Amazon Web Services демонструє найвищі показники за більшістю критеріїв, особливо у сфері аудиту, доступності та контролю доступу. Google Cloud вирізняється сильними позиціями у шифруванні та цілісності, а Azure зберігає збалансовану реалізацію на рівні 4–5 балів по всіх позиціях.

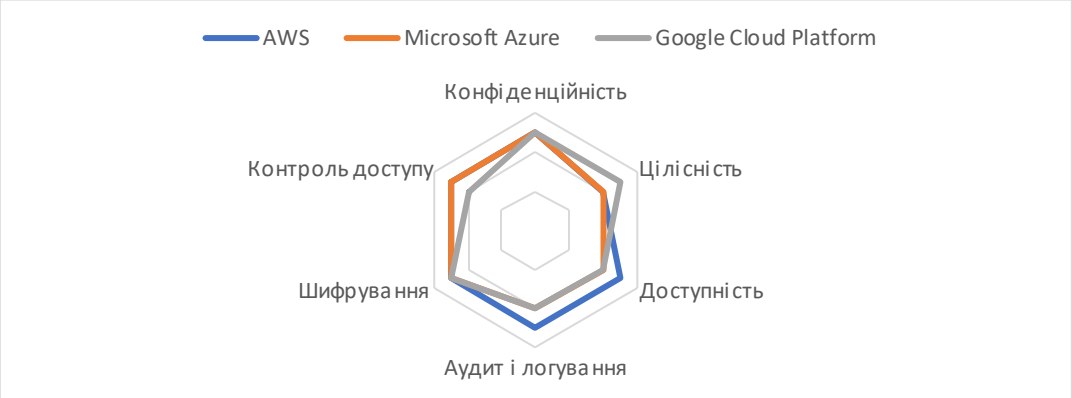

Рисунок 2.3 – Діаграма порівняння безпекових характеристик трьох провідних хмарних платформ

Такий формат узагальнення дозволяє швидко зіставити сильні й слабкі сторони кожної платформи та обрати найбільш відповідну до конкретного середовища впровадження чи політики безпеки організації [14].

Отже, ефективне управління інформаційною безпекою в хмарному середовищі базується на чітко визначених і взаємопов'язаних критеріях — конфіденційності, цілісності, доступності, аудиту, шифруванні та контролі доступу. Кожен із цих критеріїв виконує унікальну функцію, а разом вони формують цілісну систему безпеки, яка дозволяє організаціям зберігати контроль над даними, навіть передаючи їх на зовнішні платформи.

Дослідження практичної реалізації цих критеріїв на прикладі провідних хмарних платформ — Amazon Web Services, Microsoft Azure та Google Cloud Platform — показало, що всі вони дотримуються базових міжнародних стандартів, однак відрізняються гнучкістю конфігурацій, інструментами керування доступом та рівнем автоматизації процесів захисту [43].

Візуалізація за допомогою діаграми «павутина» дозволила наочно продемонструвати відносний рівень реалізації ключових вимог безпеки, що

слугує зручним інструментом для попередньої експертної оцінки платформи під конкретні завдання [18].

Критерії безпеки є не лише теоретичною основою оцінювання захищеності хмарних сервісів, а й практичним орієнтиром для вибору, налаштування та моніторингу безпечної хмарної інфраструктури. Їх системне врахування є передумовою до подальшого глибшого аналізу — методів, які дозволяють оцінювати фактичний стан безпеки на платформі. Цим аспектам і присвячено наступний підрозділ.

2.2 Методи аналізу безпеки хмарних платформ

Забезпечення інформаційної безпеки в хмарному середовищі не обмежується лише впровадженням відповідних технічних засобів — необхідною умовою є систематичний аналіз поточного стану безпеки, що дозволяє виявити потенційні загрози, оцінити рівень ризику, а також сформулювати ефективні заходи реагування [48].

Аналіз безпеки — це процес ідентифікації, оцінки та прогнозування вразливостей хмарної інфраструктури, який охоплює як технічні компоненти (мережі, хостинг, API), так і організаційні аспекти (політики доступу, логування, управління інцидентами). Основна мета цього процесу полягає у тому, щоби не допустити порушення конфіденційності, цілісності та доступності даних, виявити слабкі місця в захисті та спрогнозувати можливі сценарії їх експлуатації.

Методологія аналізу базується на кількох ключових етапах:

1. Ідентифікація активів, які потребують захисту (дані, користувачі, служби, інтерфейси).
2. Оцінка загроз — як внутрішніх, так і зовнішніх, які можуть бути спрямовані на вразливі об'єкти.
3. Виявлення вразливостей — недоліків у конфігурації, політиках безпеки, програмному забезпеченні.
4. Аналіз ймовірності реалізації загроз — визначення ризиків.

5. Прогнозування наслідків — оцінка потенційних збитків, які може понести організація.

6. Розробка плану захисту — впровадження заходів на основі отриманих результатів.

Аналіз безпеки є не лише інструментом контролю, а й основою для прийняття стратегічних рішень щодо подальшого вдосконалення захисту хмарної інфраструктури [53].

У наступних пунктах буде розглянуто конкретні методи аналізу безпеки, які застосовуються у світовій практиці, їх класифікація, переваги, обмеження та приклади використання.

Забезпечення належного рівня безпеки хмарних платформ потребує застосування різноманітних методів аналізу, які дозволяють виявляти вразливості, оцінювати ризики та розробляти стратегії захисту. Існує декілька підходів до класифікації цих методів, зокрема за об'єктом аналізу, методологією проведення та рівнем автоматизації. У таблиці 2.3 наведено узагальнену класифікацію основних методів аналізу безпеки, що застосовуються для хмарних платформ [33].

Таблиця 2.3 – Класифікація методів аналізу безпеки хмарних платформ

№	Категорія	Метод	Опис
1	**2**	**3**	**4**
1	Аналіз вразливостей	Сканування вразливостей	Автоматизоване виявлення відомих вразливостей у системах та додатках хмарної інфраструктури.
2	Тестування на проникнення	Пенетраційне тестування	Імітація атак на хмарні сервіси для оцінки їх стійкості до реальних загроз та виявлення потенційних точок входу для зловмисників.
3	Аналіз конфігурацій	Оцінка конфігурації	Перевірка налаштувань хмарних ресурсів на відповідність передовим практикам та стандартам безпеки, виявлення неправильних або небезпечних конфігурацій.
4	Аналіз трафіку	Моніторинг мережевого трафіку	Збір та аналіз даних про мережеву активність для виявлення аномалій, потенційних атак або несанкціонованого доступу.
5	Аналіз логів	Аудит та логування	Систематичний перегляд та аналіз журналів подій для виявлення підозрілих дій, порушень політик безпеки або спроб несанкціонованого доступу.

Продовження таблиці 2.3

1	2	3	4
6	Оцінка ризиків	Кількісний та якісний аналіз	Визначення та оцінка потенційних ризиків для хмарної інфраструктури з метою пріоритезації заходів щодо їх мінімізації.
7	Аналіз відповідності	Перевірка на відповідність	Оцінка відповідності хмарних сервісів вимогам нормативних актів, стандартів та внутрішніх політик організації.
8	Моделювання загроз	Threat Modeling	Ідентифікація потенційних загроз та вразливостей на етапі проєктування або експлуатації хмарних систем для розробки відповідних заходів захисту.

Застосування зазначених методів у комплексі дозволяє організаціям не лише виявляти та нейтралізувати існуючі загрози, але й прогнозувати потенційні атаки, підвищуючи таким чином загальний рівень безпеки хмарної інфраструктури. Вибір конкретного методу або їх комбінації залежить від специфіки діяльності організації, обсягу та чутливості оброблюваних даних, а також від вимог нормативно-правових актів та стандартів, що регулюють сферу інформаційної безпеки.

1. Сканування вразливостей є невід'ємною складовою процесу забезпечення безпеки хмарних платформ. Цей метод передбачає автоматизоване виявлення відомих вразливостей у системах та додатках хмарної інфраструктури. Метою сканування є ідентифікація слабких місць, які потенційно можуть бути використані зловмисниками для несанкціонованого доступу або порушення цілісності даних.

Існує ряд інструментів для сканування вразливостей, які широко використовуються в галузі інформаційної безпеки:

- Nessus - універсальний сканер вразливостей, що дозволяє перевіряти мережеві пристрої, сервери, бази даних та інші ресурси на наявність вразливостей. Його функції включають сканування на предмет неправильних налаштувань, відсутності оновлень, слабких паролів та інших загроз (див. рисунок 2.4) [21].

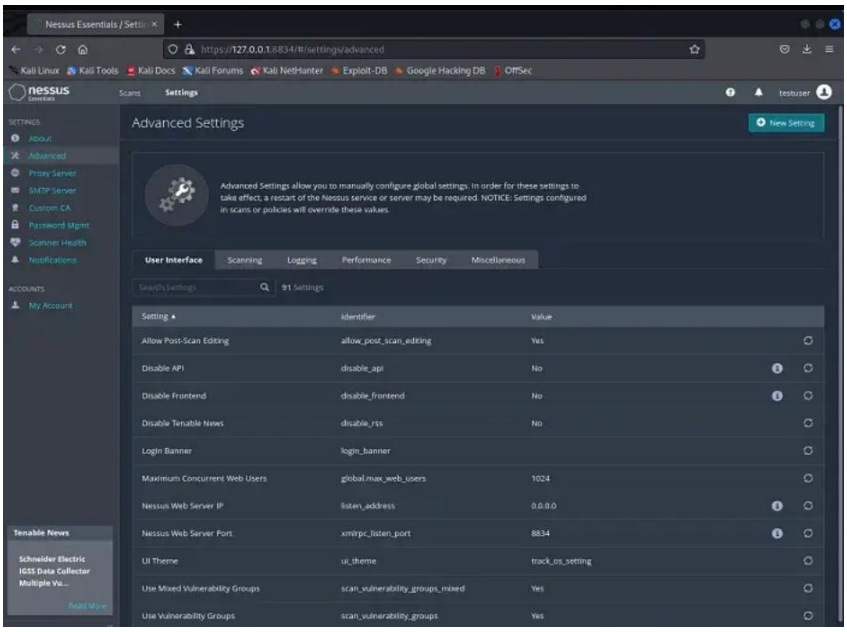

Рисунок 2.4 – Інтерфейс сканера вразливостей Nessus

– OpenVAS - відкритий сканер вразливостей, який надає широкий спектр можливостей для виявлення та аналізу вразливостей у мережевих сервісах та додатках.
– Acunetix - спеціалізується на скануванні веб-додатків, виявляючи такі вразливості, як SQL-ін'єкції, XSS та інші поширені загрози [14].
– Регулярне сканування вразливостей дозволяє організаціям проактивно виявляти та усувати потенційні загрози, забезпечуючи високий рівень захисту даних та сервісів у хмарному середовищі. Застосування таких інструментів, як Nessus, OpenVAS та Acunetix, сприяє підтримці актуального стану безпеки та мінімізації ризиків, пов'язаних з експлуатацією вразливостей зловмисниками [25].

2. Пенетраційне тестування (penetration testing) — це процес імітації кібератак на комп'ютерні системи з метою виявлення вразливостей, які можуть бути використані зловмисниками. У контексті хмарних платформ, пенетраційне тестування спрямоване на оцінку безпеки інфраструктури, додатків та сервісів, що розгорнуті в хмарному середовищі.

Виклики пенетраційного тестування в хмарних середовищах:

– Модель розподіленої відповідальності - у хмарних платформах відповідальність за безпеку поділяється між постачальником

хмарних послуг та клієнтом. Тому важливо чітко розуміти, які компоненти підлягають тестуванню та хто несе за них відповідальність .

– Динамічність середовища - хмарні ресурси можуть змінюватися в режимі реального часу, що ускладнює процес тестування та вимагає адаптивних підходів.
– Обмеження з боку постачальників послуг - деякі провайдери хмарних послуг мають обмеження щодо проведення пенетраційного тестування, тому необхідно заздалегідь узгоджувати такі дії та отримувати відповідні дозволи.

Проведення пенетраційного тестування в хмарних середовищах є критично важливим для забезпечення належного рівня безпеки та захисту даних. Воно дозволяє організаціям проактивно виявляти та усувати вразливості, мінімізуючи ризики потенційних атак [46].

3. Оцінка конфігурації хмарних платформ є критичною для забезпечення безпеки, відповідності нормативним вимогам та оптимізації продуктивності. Вона передбачає систематичний аналіз налаштувань хмарних ресурсів з метою виявлення та усунення потенційних вразливостей і неефективностей.

Інструменти для оцінки конфігурації:

– Prowler - відкритий інструмент для оцінки безпеки AWS, Azure та Google Cloud, що дозволяє проводити аудит налаштувань відповідно до найкращих практик та стандартів безпеки (див. рисунок 2.5) [15].

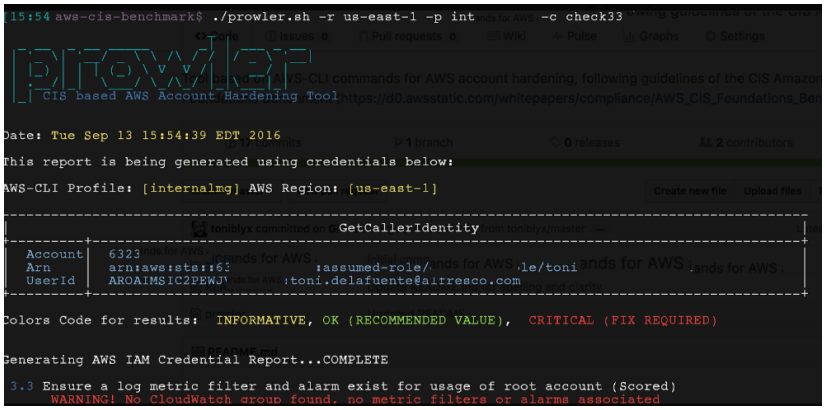

Рисунок 2.5 – Інтерфейс Prowler під час сканування AWS

– Cloud Security Assessment & Penetration Testing - комплексне рішення для оцінки безпеки та тестування на проникнення в середовищах AWS, Azure та GCP, спрямоване на виявлення неправильних конфігурацій та перевірку безпеки управління доступом (див. риснок 2.6) [26].

Рисунок 2.6 – Процес оцінки безпеки хмарної інфраструктури

– CIS Benchmarks - набір рекомендацій від Центру Інтернет-Безпеки (CIS) для безпечного налаштування різних технологій та хмарних платформ (див. рисунок 2.7) [54].

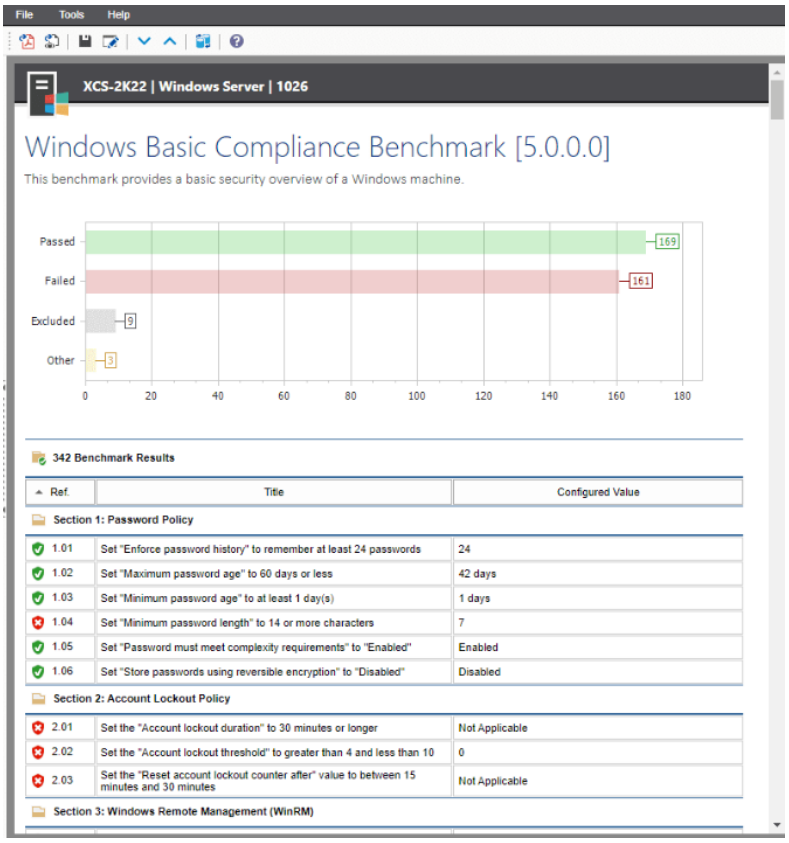

Рисунок 2.7– Процес оцінки відповідності CIS Benchmarks за допомогою інструмента CIS-CAT Pro

Регулярна оцінка конфігурації хмарних платформ сприяє своєчасному виявленню та усуненню потенційних загроз, забезпечуючи стабільність, безпеку та відповідність нормативним вимогам хмарної інфраструктури [36].

4. Моніторинг мережевого трафіку — це процес спостереження та аналізу даних, що передаються через мережу, з метою забезпечення її безпеки, продуктивності та виявлення потенційних загроз. У хмарних платформах цей процес набуває особливого значення через динамічність і масштабованість ресурсів.

Інструменти для моніторингу мережевого трафіку в хмарних платформах:

– Zabbix - універсальне рішення з відкритим вихідним кодом для моніторингу мереж, серверів та додатків. Підтримує різні хмарні платформи, такі як AWS, Azure, Google Cloud Platform, що дозволяє централізовано відстежувати стан ресурсів (див. рисунок 2.8) [15].

Рисунок 2.8 – Приклад дашборду Zabbix

– Datadog - комплексна хмарна платформа моніторингу та аналітики, яка забезпечує видимість у реальному часі для серверів, баз даних, додатків та інших сервісів. Підтримує понад 600 технологій та сервісів, що дозволяє безперешкодно збирати дані з різних джерел (див. рисунок 2.9).

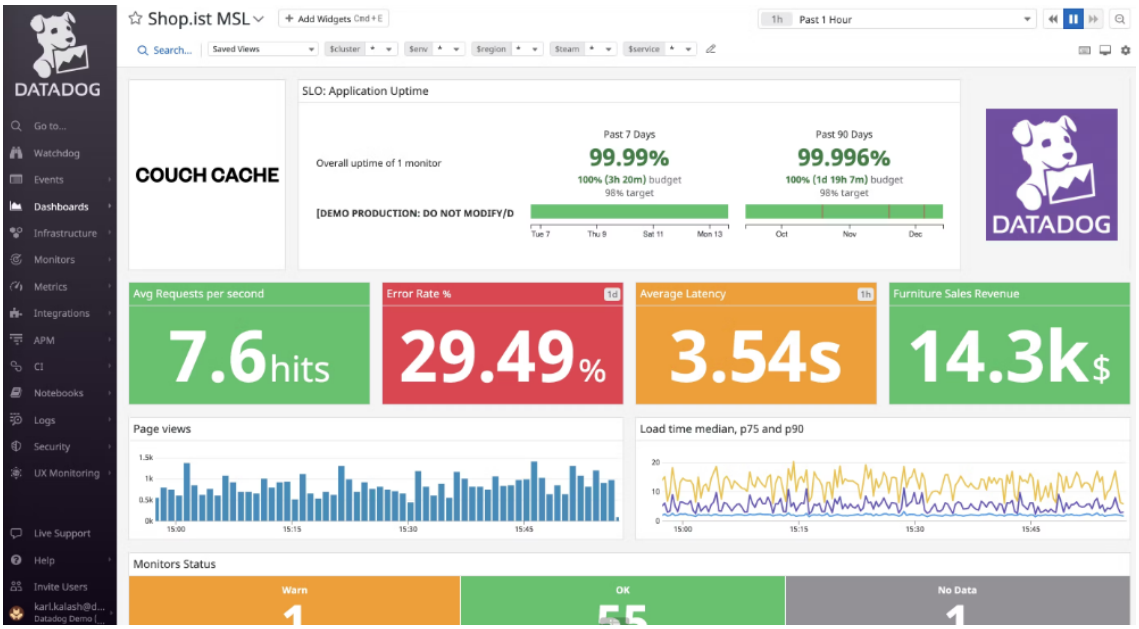

Рисунок 2.9 – Приклад дашборду Datadog

– Flowmon - рішення для моніторингу продуктивності та безпеки мережі, яке дозволяє точно визначити першопричину збоїв, надає повну видимість мережі та виявляє загрози безпеці завдяки

використанню штучного інтелекту та гнучким налаштуванням (див. рисунок 2.9).

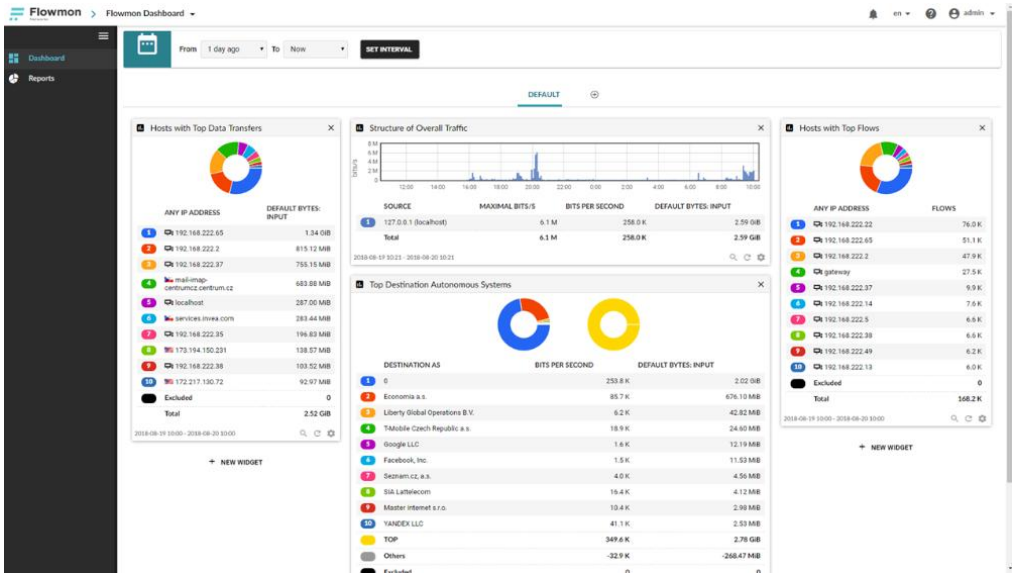

Рисунок 2.10 – Приклад дашборду Flowmon

Впровадження ефективного моніторингу мережевого трафіку в хмарних середовищах сприяє підвищенню рівня безпеки, оптимізації використання ресурсів та забезпеченню стабільної роботи сервісів.

5. Аудит та логування є ключовими компонентами інформаційної безпеки, що забезпечують моніторинг та аналіз подій у системах організації. Для ефективного впровадження цих процесів використовуються спеціалізовані інструменти. Ось деякі з них:

– Splunk - потужна платформа для збору, аналізу та візуалізації великих обсягів даних, включаючи журнали подій. Забезпечує реальний часовий моніторинг та гнучкі можливості пошуку.

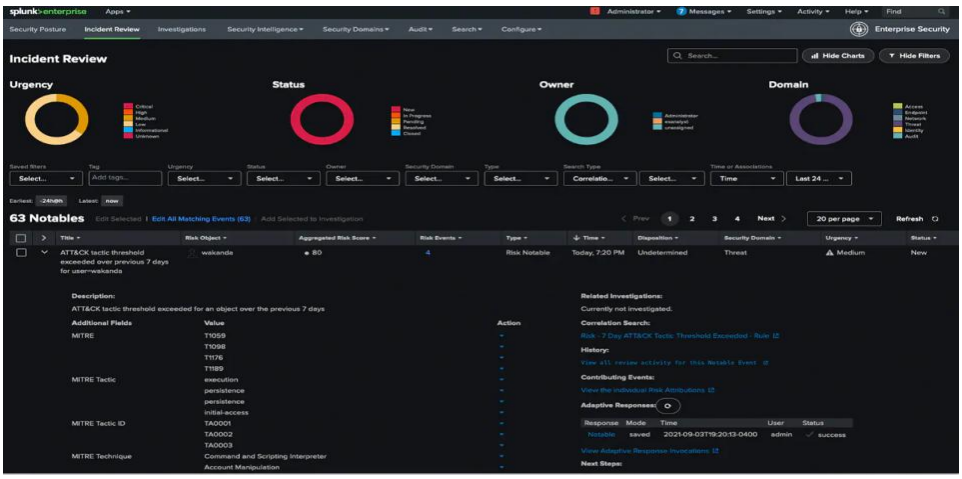

Рисунок 2.11 – Приклад дашборду Splunk

– ELK Stack (Elasticsearch, Logstash, Kibana) - відкрите рішення для централізованого управління журналами. Elasticsearch відповідає за зберігання та пошук, Logstash — за збір та обробку даних, а Kibana — за візуалізацію [58].
– Graylog - платформа з відкритим кодом для збору, індексації та аналізу логів у реальному часі. Підтримує гнучке налаштування та масштабування.

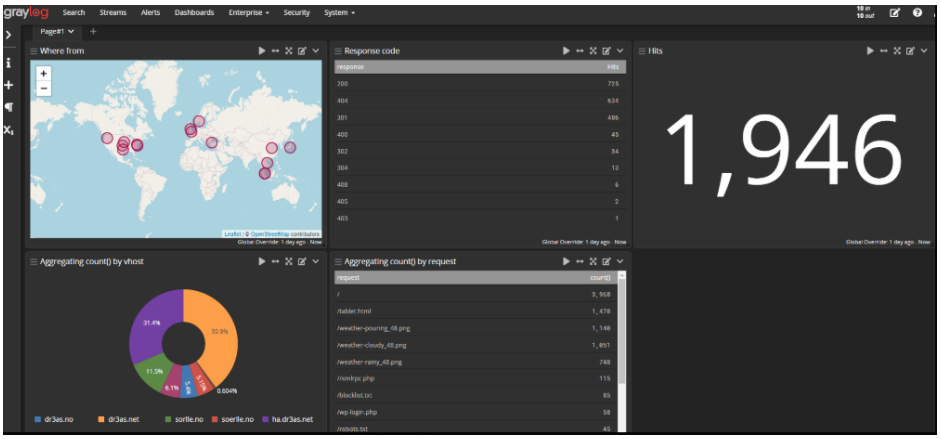

Рисунок 2.12 – Приклад дашборду Graylog

Datadog хмарне рішення для моніторингу та аналізу логів, метрик та трасувань. Забезпечує інтеграцію з різними платформами та сервісами.

– Logstash - інструмент для збору, обробки та передачі логів, який є частиною ELK Stack. Дозволяє агрегувати логи з різних джерел та надсилати їх до сховища.

Використання цих інструментів сприяє підвищенню ефективності процесів аудиту та логування, забезпечуючи своєчасне виявлення та реагування на інциденти безпеки.

6. Кількісний та якісний аналіз — це два основні підходи до дослідження даних, кожен з яких має свої методи та інструменти.

Кількісний аналіз фокусується на числових даних і статистичних методах для вимірювання та аналізу явищ. Він відповідає на питання "скільки?" або "наскільки часто?". Інструменти для кількісного аналізу включають:

– Програмне забезпечення для статистичного аналізу: SPSS, SAS.
– Веб-аналітика: Google Analytics, Mixpanel, Amplitude [23].

– Інструменти для A/B-тестування: Optimizely, VWO.

Якісний аналіз спрямований на розуміння поведінки, мотивів та досвіду людей. Він відповідає на питання "чому?" або "як?". Інструменти для якісного аналізу включають:

– Інструменти для запису сесій та теплових карт: Hotjar, UXCam.
– Програмне забезпечення для обробки текстових даних: NVivo, Atlas.ti.
– Інструменти для проведення опитувань та інтерв'ю: SurveyMonkey, Typeform.

Вибір між кількісним та якісним аналізом залежить від цілей дослідження. Часто ефективним є поєднання обох підходів для отримання повнішого уявлення про досліджуване явище.

7. Перевірка на відповідність — це процес оцінки того, наскільки певні дані, системи чи процеси відповідають встановленим стандартам, вимогам або очікуванням. Вона є ключовим етапом у багатьох сферах, включаючи аналіз даних, розробку програмного забезпечення та управління якістю.

У контексті аналізу даних перевірка на відповідність може включати:

– Перевірку гіпотез - статистичний метод, що використовується для визначення, чи є достатньо доказів для підтвердження або відхилення припущень про параметри сукупності [11].
– Дисперсійний аналіз (ANOVA) - метод, який дозволяє порівнювати середні значення між кількома групами, щоб визначити, чи існують статистично значущі відмінності між ними [16].
– У сфері розробки програмного забезпечення перевірка на відповідність охоплює:
– Верифікацію вимог - процес підтвердження того, що задокументовані вимоги правильно відображають потреби зацікавлених сторін і відповідають встановленим критеріям якості [20].

- Тестування баз даних - перевірка структурних та функціональних аспектів бази даних, включаючи відповідність бізнес-правилам, цілісність даних та продуктивність [3].

Інструменти, що використовуються для перевірки на відповідність, можуть включати:

- Статистичне програмне забезпечення - для проведення перевірки гіпотез та дисперсійного аналізу.
- Спеціалізовані інструменти для тестування вимог - для оцінки повноти та коректності вимог.
- Системи для тестування баз даних - для аналізу структурних та функціональних характеристик баз даних.

Загалом, перевірка на відповідність забезпечує впевненість у тому, що досліджувані об'єкти або процеси відповідають заданим стандартам та вимогам, що є критично важливим для забезпечення якості та надійності в різних галузях [24].

8. Моделювання загроз є важливим процесом у забезпеченні безпеки інформаційних систем. Для його ефективного проведення існує низка інструментів, які допомагають ідентифікувати, аналізувати та усувати потенційні загрози. Ось деякі з них:

- Microsoft Threat Modeling Tool - безкоштовний інструмент від Microsoft, призначений для спрощення процесу моделювання загроз. Він надає стандартну нотацію для візуалізації компонентів системи, потоків даних та меж безпеки (див. рисунок 2.13) [44].

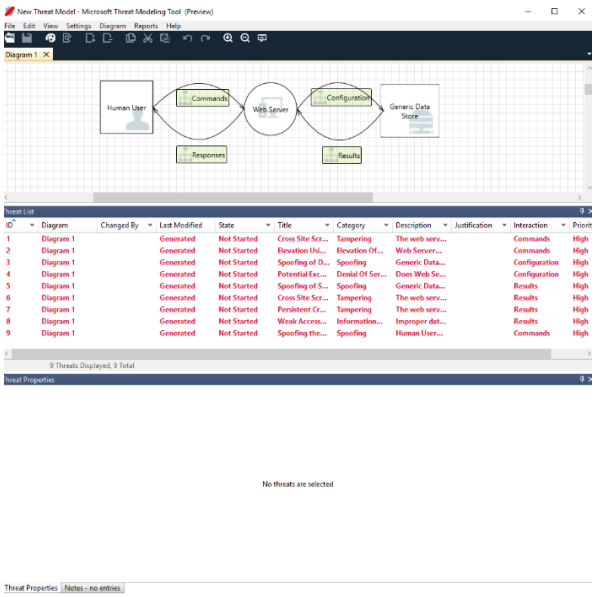

Рисунок 2.13 – Приклад дашборду Microsoft Threat Modeling Tool

– OWASP Threat Dragon - відкритий кросплатформенний інструмент для створення діаграм моделювання загроз у рамках безпечного життєвого циклу розробки. Підтримує методології STRIDE та LINDDUN [39].
– IriusRisk - комерційний інструмент, що пропонує як безкоштовну, так і платну версії. Зосереджений на створенні та підтримці актуальних моделей загроз протягом всього життєвого циклу розробки програмного забезпечення (див. рисунок 2.14) [24].

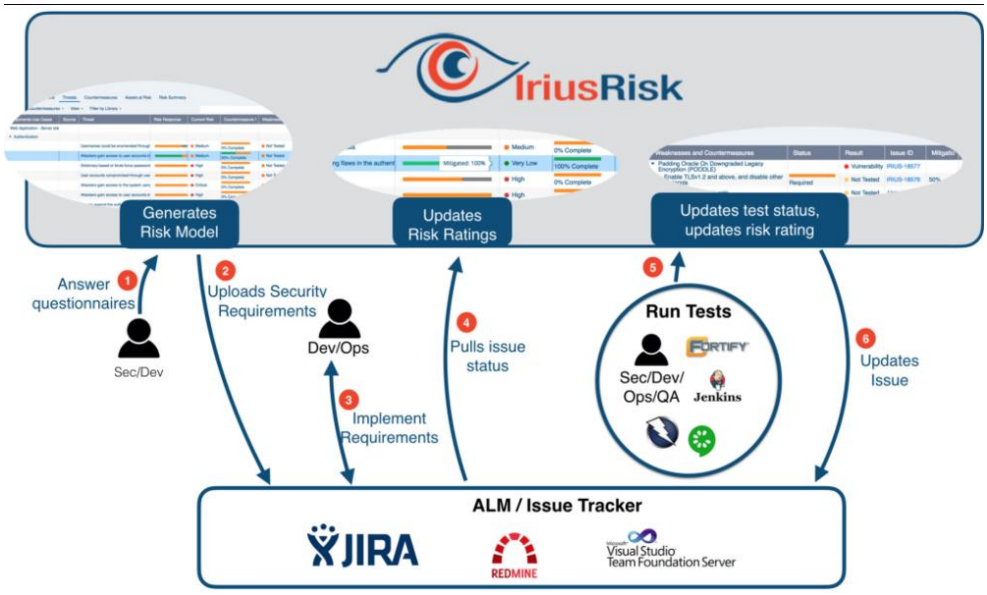

Рисунок 2.14 – Приклад дашборду IriusRisk

– ThreatModeler - інструмент корпоративного класу для моделювання загроз та співпраці, який автоматизує багато аспектів процесу моделювання загроз, наближаючи його до концепції "моделювання загроз в один клік" (див. рисунок 2.15).

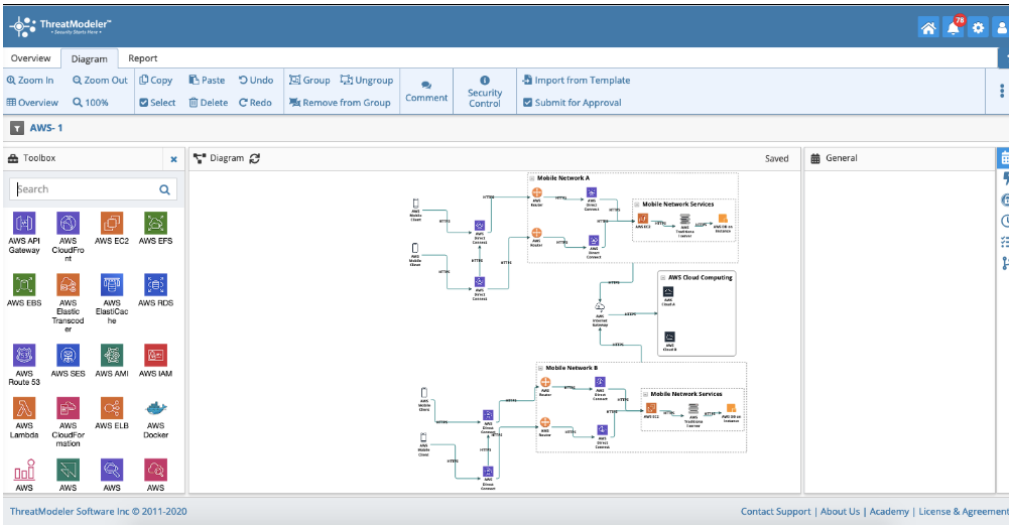

Рисунок 2.15 – Приклад дашборду ThreatModeler

– SD Elements - платформа для управління вимогами безпеки програмного забезпечення, яка включає можливості автоматизованого моделювання загроз. Генерує набір загроз на основі короткого опитувальника про технічні деталі та фактори відповідності додатка (див. рисунок 2.16).

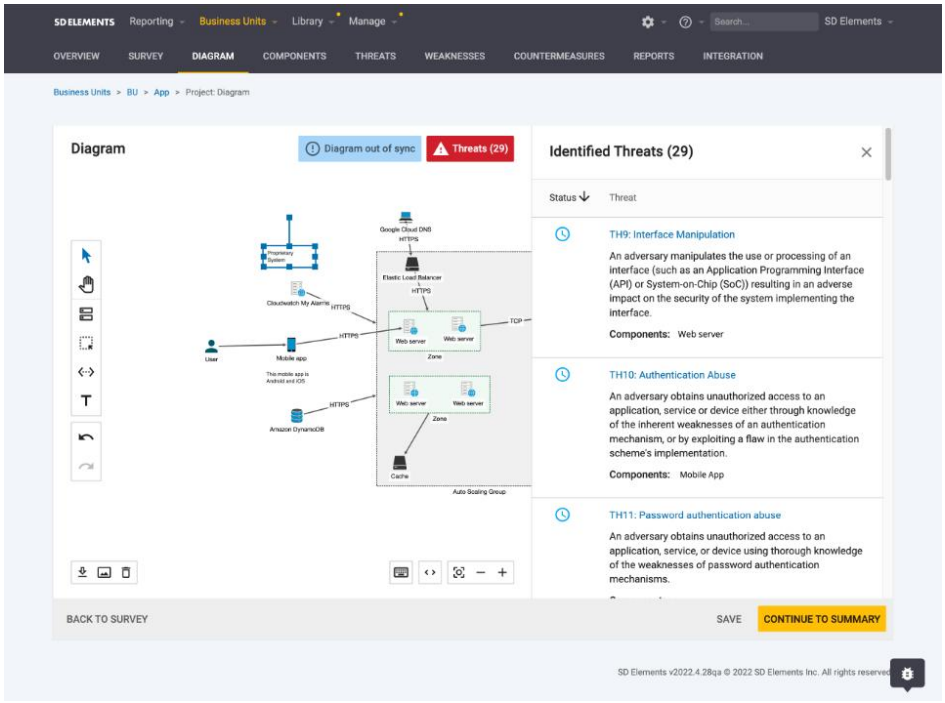

Рисунок 2.16 – Приклад дашборду SD Elements

Вибір відповідного інструменту залежить від специфіки проєкту, вимог до безпеки та доступних ресурсів. Використання цих інструментів сприяє більш ефективному виявленню та усуненню потенційних загроз на ранніх етапах розробки.

У сучасних умовах динамічного розвитку цифрових технологій питання забезпечення безпеки інформаційних систем набуває особливої актуальності. Для демонстрації практичного значення методів аналізу загроз, доцільно розглянути умовну ситуацію, пов'язану з діяльністю вигаданого підприємства — логістичної компанії «Швидкий Вантаж». Компанія надає послуги з перевезення товарів та управління ланцюгами постачання, активно використовуючи хмарні технології для обробки замовлень, відстеження вантажів, обміну інформацією з клієнтами та партнерами [39].

Хмарна платформа, яку використовує компанія, складається з веб-застосунку для диспетчерів, мобільного застосунку для водіїв, централізованої бази даних і відкритих API для інтеграції з іншими сервісами. Такий розподіл функціоналу створює складне середовище з різноманітними точками доступу, яке потребує системного підходу до виявлення і усунення вразливостей. У цьому контексті було застосовано метод STRIDE, який передбачає класифікацію загроз за шістьма основними типами: підробка (spoofing), підміна (tampering), відмова від дій (repudiation), розголошення інформації (information disclosure), відмова в обслуговуванні (denial of service) та підвищення привілеїв (elevation of privilege) [14].

Під час моделювання загроз було складено перелік потенційних ризиків для основних компонентів системи. Вони охоплюють такі проблеми, як несанкціонований доступ до облікових записів, модифікація даних про маршрути, витік персональної інформації клієнтів або недоступність сервісів у критичний момент. Для кожної виявленої загрози були розроблені пропозиції щодо заходів реагування — від впровадження багатофакторної автентифікації до використання журналів аудиту, шифрування даних та обмеження прав доступу [27].

Таблиця 2.4 – Приклад застосування моделі STRIDE до хмарної системи компанії «Швидкий Вантаж»

№	Тип загрози	Приклад в контексті компанії	Можливі наслідки	Заходи протидії
1	Spoofing	Несанкціонований доступ до акаунта водія	Маніпуляції з маршрутами, шахрайство	Впровадження MFA, перевірка сесій
2	Tampering	Зміна даних про доставку в БД	Викривлення звітності, порушення логістики	Цифрові підписи, контрольна сума
3	Repudiation	Заперечення створення замовлення	Конфлікти з клієнтами, втрати довіри	Аудит логів, мітки часу
4	Information Disclosure	Витік адрес клієнтів через API	Порушення конфіденційності, скарги	TLS, шифрування даних, авторизація доступу
5	Denial of Service	Перевантаження системи API запитами	Зупинка сервісу, фінансові втрати	Анти-DDoS захист, кешування
6	Elevation of Privilege	Отримання ролі адміністратора	Повний контроль над системою	Принцип найменших привілеїв, контроль ACL

Аналіз показав, що навіть умовна хмарна інфраструктура малого або середнього бізнесу може бути вразливою до цілого спектра загроз, якщо не передбачити базові заходи контролю. Застосування STRIDE дозволяє виявити слабкі місця системи ще на етапі проєктування або модернізації, що сприяє зниженню ризиків і підвищенню надійності бізнес-процесів.

Отже, метод моделювання загроз STRIDE є ефективним інструментом у побудові безпечного цифрового середовища. У контексті логістичної компанії його застосування допомогло не лише систематизувати потенційні загрози, але й сформувати конкретні рекомендації щодо вдосконалення системи захисту. Це доводить доцільність інтеграції подібних підходів у процеси розробки та експлуатації хмарних платформ, зокрема у сфері логістики та управління ланцюгами постачання [12].

2.3 Порівняння існуючих систем оцінки безпеки хмарних сервісів

Система оцінки — це комплекс взаємопов'язаних стандартів, сертифікацій та політик, які спільно забезпечують механізм для перевірки та підтвердження відповідності продукції, процесів, послуг або систем встановленим вимогам.

Стандарти визначають технічні та якісні характеристики, яким повинні відповідати об'єкти оцінки. Вони слугують основою для розробки критеріїв оцінювання та є спільно визнаними орієнтирами в певній галузі [12].

Сертифікація є процесом, під час якого незалежна організація (третя сторона) офіційно підтверджує, що продукція, процес або система відповідають вимогам відповідних стандартів. Це надає споживачам та партнерам впевненість у якості та надійності об'єкта сертифікації [39].

Політики в контексті системи оцінки встановлюють загальні принципи, правила та процедури, яких необхідно дотримуватися під час проведення оцінювання та сертифікації. Вони забезпечують узгодженість та прозорість процесів, а також визначають відповідальність учасників системи.

Система оцінки, поєднуючи стандарти, сертифікації та політики, створює цілісну структуру для гарантування того, що продукція, процеси або послуги відповідають встановленим вимогам та очікуванням споживачів і регуляторних органів.

CSA STAR (Security, Trust, Assurance, and Risk) — це програма, розроблена Cloud Security Alliance (CSA) для оцінки та сертифікації безпеки хмарних сервісів. Вона спрямована на підвищення прозорості та довіри між постачальниками хмарних послуг та їхніми клієнтами.

Рівні сертифікації:

Рівень 1. Самооцінка (Self-Assessment): Постачальники хмарних послуг заповнюють опитувальник, базований на Cloud Controls Matrix (CCM), та публікують його в реєстрі STAR. Це дозволяє клієнтам ознайомитися з заходами безпеки, які застосовує постачальник [43].

Рівень 2. Сертифікація третьою стороною (Third-Party Certification): Передбачає незалежний аудит постачальника хмарних послуг на відповідність стандарту ISO/IEC 27001 та критеріям CCM. Успішне проходження аудиту підтверджує високий рівень безпеки та додає постачальника до реєстру STAR з відповідною відміткою.

Компанія Amazon Web Services (AWS) пройшла сертифікацію CSA STAR Level 2, що підтверджує її відповідність міжнародним стандартам безпеки та надає клієнтам впевненість у захищеності їхніх даних [29].

ISO/IEC 27017 та ISO/IEC 27018 — це міжнародні стандарти, що надають рекомендації щодо безпеки та конфіденційності в хмарних середовищах.

- ISO/IEC 27017 містить додаткові керівництва для впровадження заходів безпеки в хмарних сервісах, доповнюючи стандарт ISO/IEC 27002. Він адресує специфічні ризики, пов'язані з хмарними обчисленнями, та надає рекомендації як для постачальників, так і для користувачів хмарних послуг.
- ISO/IEC 27018 зосереджується на захисті персонально ідентифікованої інформації (PII) в публічних хмарах. Він встановлює контрольні заходи для обробки PII та забезпечує відповідність вимогам конфіденційності [45].

NIST Special Publication 800-53 — це набір рекомендацій, розроблених Національним інститутом стандартів і технологій США (NIST), що містить каталог заходів безпеки та конфіденційності для інформаційних систем. Він спрямований на захист організаційних операцій, активів та осіб від різноманітних загроз, включаючи кібератаки та природні катастрофи (див. табл. 2.5).

Таблиця 2.5 – Порівняльна характеристика систем

№	Система	Доступність	Складність впровадження	Популярність
1	CSA STAR	Висока	Середня	Висока
2	ISO/IEC 27017	Висока	Висока	Середня
3	ISO/IEC 27018	Висока	Висока	Середня
4	NIST SP 800-53	Середня	Висока	Висока
5	ENISA Cloud Guidelines	Висока	Низька	Середня

Європейське агентство з мережевої та інформаційної безпеки (ENISA) розробило рекомендації для малих та середніх підприємств щодо безпеки в хмарних обчисленнях. Ці рекомендації допомагають підприємствам розуміти ризики та можливості, пов'язані з використанням хмарних сервісів, та включають набір питань для оцінки рівня безпеки постачальників хмарних послуг.

Для забезпечення ефективного управління безпекою в хмарних середовищах (див. табл. 2.6) важливо оцінити, наскільки різні стандарти та рекомендації відповідають критичним вимогам організацій. Нижче представлена матриця покриття критичних вимог кожною з розглянутих систем: CSA STAR, ISO/IEC 27017, ISO/IEC 27018, NIST SP 800-53 та ENISA Cloud Guidelines.

Таблиця 2.6 – Матриця покриття критичних вимог кожною системою

№	Критичні вимоги	CSA STAR	ISO/IEC 27017	ISO/IEC 27018	NIST SP 800-53	ENISA Cloud Guidelines
1	Управління ризиками	Так	Так	Ні	Так	Так
2	Захист даних та конфіденційність	Так	Так	Так	Так	Так
3	Контроль доступу та управління ідентифікацією	Так	Так	Ні	Так	Так
4	Моніторинг та аудит безпеки	Так	Так	Ні	Так	Так
5	Відповідність нормативним вимогам та стандартам	Так	Так	Так	Так	Так
6	Безпека мережі та комунікацій	Так	Так	Ні	Так	Так
7	Безперервність бізнесу та відновлення після збоїв	Так	Ні	Ні	Так	Так
8	Управління постачальниками та сторонніми підрядниками	Так	Ні	Ні	Так	Так

Вибір відповідного стандарту або рекомендацій залежить від специфічних потреб організації та її пріоритетів у сфері безпеки. CSA STAR та NIST SP 800-53 пропонують найбільш комплексне покриття критичних вимог, тоді як ISO/IEC 27017 та ISO/IEC 27018 спеціалізуються на окремих аспектах безпеки хмарних сервісів. ENISA Cloud Guidelines надають корисні рекомендації для

європейських постачальників хмарних послуг. Ретельний аналіз та порівняння цих систем дозволить організації обрати найбільш підходящий підхід для забезпечення безпеки в хмарному середовищі [19].

У сучасних умовах стрімкого розвитку хмарних технологій особливої ваги набуває питання прозорості, надійності та відповідності хмарних сервісів міжнародним стандартам безпеки. Одним із прикладів ефективної реалізації таких вимог є діяльність компанії Microsoft у сфері хмарних обчислень. Її платформа Microsoft Azure не лише забезпечує широкий спектр послуг для обробки, зберігання та аналізу даних, а й активно впроваджує механізми підтвердження своєї відповідності вимогам безпеки, зокрема через участь у програмі CSA STAR (Security, Trust, Assurance and Risk) [26].

Програма CSA STAR, розроблена Cloud Security Alliance, є міжнародною ініціативою, спрямованою на підвищення довіри до хмарних сервісів шляхом забезпечення публічного доступу до даних про безпекову політику та практики постачальників. Microsoft Azure бере участь у цій програмі на двох рівнях сертифікації. Перший рівень передбачає самооцінку, під час якої компанія публікує відповіді на стандартизований опитувальник (CAIQ), що базується на Cloud Controls Matrix (CCM). Така публікація дає змогу клієнтам ознайомитися з внутрішніми політиками безпеки Azure та самостійно оцінити їхню ефективність.

Другий рівень сертифікації передбачає аудит третьою стороною, що виконується акредитованим органом і базується на вимогах ISO/IEC 27001 та CCM. Проходження такого аудиту є свідченням високого рівня організації заходів безпеки в хмарній інфраструктурі Microsoft. У результаті успішної перевірки Microsoft отримує офіційне підтвердження відповідності вимогам CSA STAR, що відображається в публічному реєстрі CSA [42].

Процес сертифікації Microsoft Azure складається з кількох етапів: внутрішньої оцінки відповідності, заповнення й публікації CAIQ, підготовки до аудиту, проходження зовнішньої перевірки та, в разі успіху, — включення до реєстру сертифікованих провайдерів. Кожен із цих етапів має чітке

документальне забезпечення та вимагає підтвердження реалізації ключових безпекових контролів [31].

Сертифікація Microsoft Azure за CSA STAR демонструє на практиці, як великі хмарні провайдери інтегрують міжнародні вимоги до інформаційної безпеки у свою діяльність. Це не лише посилює конкурентоспроможність компанії на глобальному ринку, а й створює додаткові гарантії для користувачів щодо надійності та захищеності їхніх даних у хмарному середовищі.

Вибір відповідної системи оцінки безпеки хмарних сервісів є стратегічним рішенням для кожного підприємства, яке планує або вже використовує хмарні технології. Такий вибір має базуватися не лише на формальному відповідності нормативам, але й на практичних потребах, ресурсах і пріоритетах організації. Нижче подано ключові рекомендації, які слід враховувати при ухваленні такого рішення [54].

По-перше, необхідно визначити рівень критичності інформації, що обробляється у хмарному середовищі. Якщо підприємство має справу з персональними даними клієнтів, фінансовою або медичною інформацією, доцільно обирати системи, що акцентують увагу на конфіденційності та захисті персональних даних, наприклад ISO/IEC 27018. У разі роботи з публічними чи менш чутливими даними можуть застосовуватись більш загальні системи.

По-друге, важливо оцінити розмір та організаційну складність підприємства. Для великих компаній із розгалуженою IT-інфраструктурою, наявністю власних ЦОДів та використанням декількох хмарних платформ рекомендованим є впровадження NIST SP 800-53, який надає глибоку деталізацію контролів та дозволяє масштабувати безпекову політику. Для малих та середніх підприємств варто звернути увагу на ENISA Cloud Guidelines, які є менш формалізованими, проте пропонують практичні поради та покриття базових ризиків.

По-третє, підприємствам, які прагнуть публічно підтвердити свій рівень захищеності та посилити довіру з боку партнерів і клієнтів, доцільно проходити сертифікацію за програмою CSA STAR. Вона передбачає публікацію інформації

про внутрішні механізми захисту, а також можливість пройти незалежний аудит. Цей підхід особливо ефективний для хмарних провайдерів, IT-компаній, а також сервісних підприємств, які взаємодіють із міжнародними клієнтами [27].

У випадку, якщо підприємство вже має впроваджену систему управління інформаційною безпекою відповідно до ISO/IEC 27001, доцільним кроком буде її доповнення стандартами ISO/IEC 27017 (щодо практик безпеки в хмарі) або ISO/IEC 27018 (щодо захисту персональних даних у публічних хмарах). Це дозволить оптимізувати ресурси та уникнути дублювання вимог.

Окрему увагу варто звернути на наявність інструментів підтримки та адаптації системи до бізнес-процесів. Деякі стандарти, як-от NIST, мають розвинену методологічну базу, приклади реалізації та гнучку структуру контролів, що дає змогу адаптувати їх до конкретного середовища. Інші — наприклад, CSA STAR — роблять акцент на прозорості та демонстрації відповідності ззовні [22].

Отже, порівняльний аналіз засвідчив, що жодна система оцінки безпеки хмарних сервісів не є універсальною. Вибір залежить від масштабу підприємства, рівня ризиків, специфіки даних та цілей безпеки. CSA STAR забезпечує прозорість і гнучкість, NIST SP 800-53 — глибину і деталізацію контролів, ISO/IEC 27017 та 27018 — практичні рекомендації для захисту даних, а ENISA — доступні орієнтири для малого й середнього бізнесу. Раціональне впровадження повинно враховувати конкретні потреби організації.

РОЗДІЛ 3 РОЗРОБКА МОДЕЛІ ОЦІНКИ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

3.1 Розробка концептуальної моделі оцінки безпеки

Сучасний розвиток інформаційних технологій та широке впровадження хмарних сервісів у діяльність підприємств, державних установ і приватних осіб обумовлюють необхідність створення ефективних механізмів забезпечення інформаційної безпеки. Хмарна інфраструктура, яка надає доступ до обчислювальних ресурсів, зберігання та обробки даних, є вразливою до широкого спектра загроз – від технічних до організаційних. З огляду на це, виникає потреба у розробці моделі оцінки безпеки, що дозволить кількісно визначити рівень захищеності хмарного середовища, виявити критичні вразливості та запропонувати рекомендації щодо їх усунення [21].

Метою моделювання є створення концептуальної моделі, що забезпечує комплексну оцінку рівня безпеки хмарного сервісу шляхом аналізу ймовірностей загроз, їхнього впливу на активи та ефективності застосованих заходів захисту. Об'єктом дослідження є хмарні обчислювальні середовища, зокрема сервіси, які працюють за моделями IaaS, PaaS та SaaS. Предметом виступає процес оцінки інформаційної безпеки хмарних сервісів, що включає аналіз ризиків, визначення вразливостей та розрахунок рівня ризику.

Основними завданнями розробки моделі є: ідентифікація вхідних параметрів системи безпеки, формалізація залежностей між ними, побудова математичної моделі обчислення ризику, розробка механізмів ранжування загроз, визначення інтегрального індексу безпеки та створення логічної структури оцінювання [37].

До вхідних параметрів моделі належать: ймовірність виникнення загроз P_i, рівень їх впливу на активи I_i, ступінь захищеності інформаційних ресурсів A_k, складність конфігураційного середовища C_j. Як вихідні параметри розглядаються: агрегований ризик, деталізовані оцінки ризику за категоріями загроз, рівень залишкового ризику та перелік заходів для зниження рівня загроз.

Для формалізації оцінки ризику використовується класичний підхід, згідно з яким інтегральний рівень ризику розраховується за формулою:

$$R = \sum_{i=1}^{n} (P_i \times I_i) \quad (3.1)$$

де R – загальний ризик;

P_i – ймовірність реалізації і-тої загрози;

I_i – ступінь впливу загрози на актив.

Ця модель дозволяє проаналізувати різні типи загроз, враховуючи специфіку хмарного середовища, рівень доступу до даних, використання сторонніх API та політику ідентифікації користувачів. Розрахунок інтегрального ризику забезпечує наочність оцінки поточного стану безпеки та формує основу для прийняття управлінських рішень.

У табл. 3.1 наведено приклади типових загроз у хмарному середовищі із зазначенням їхньої ймовірності та потенційного впливу.

Таблиця 3.1 – Приклади типових загроз у хмарному середовищі

№	Назва загрози	Ймовірність P_i	Вплив I_i	Коментар
1	Несанкціонований доступ	0,7	0,9	Через слабі паролі та відсутність MFA
2	Уразливість у API	0,6	0,8	Внаслідок недостатнього контролю
3	Витік даних через сторонні інтеграції	0,4	0,7	Через ненадійні зовнішні сервіси
4	Внутрішня загроза	0,3	0,6	З боку співробітників або партнерів

На основі вхідних параметрів модель дозволяє виявити критичні вразливості, оцінити залишковий ризик та сформувати перелік необхідних заходів безпеки. Загальна логіка функціонування моделі представлена на рисунку 3.1.

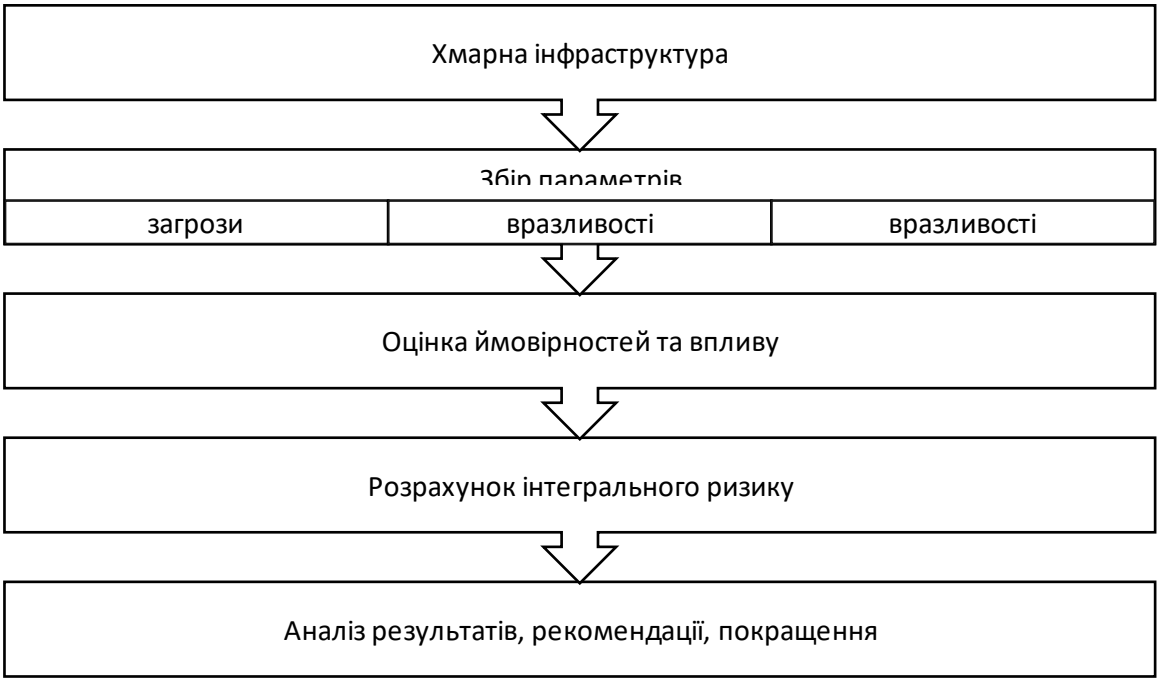

Рисунок 3.1 – Загальна логіка моделі оцінки безпеки хмарного сервісу

Постановка задачі моделювання визначає концептуальні основи побудови ефективної моделі оцінки безпеки хмарних сервісів, яка забезпечує можливість обґрунтованого аналізу поточного стану безпеки, формування прогнозів та розробку стратегії підвищення захищеності системи.

Ефективність моделі оцінки безпеки хмарних сервісів значною мірою залежить від обраної методології, яка визначає загальний підхід до ідентифікації, класифікації та кількісної оцінки ризиків. У сучасній практиці інформаційної безпеки застосовується низка підходів до аналізу ризиків, кожен із яких має свої переваги, недоліки та сферу застосування [32].

Для побудови обґрунтованої моделі доцільно розглянути та порівняти такі методології, як:

– OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – орієнтована на самооцінку та стратегічне управління ризиками, застосовується в умовах з обмеженим технічним аналізом;
– FAIR (Factor Analysis of Information Risk) – базується на кількісному підході до вимірювання ризику в економічному вираженні, дозволяє оцінити втрати в грошовому еквіваленті;

- CVSS (Common Vulnerability Scoring System) – стандартизована система оцінки вразливостей, що широко використовується для класифікації технічних загроз;
- ISO/IEC 27005 – міжнародний стандарт, що регламентує процеси управління ризиками інформаційної безпеки;
- NIST SP 800-30 та SP 800-53 – надають детальні керівництва з оцінки ризиків та впровадження контролів у хмарних середовищах.

У табл. 3.2 наведено порівняльну характеристику зазначених методик за критеріями застосовності в хмарному середовищі, рівня деталізації, ступеня формалізації та наявності кількісної складової.

Таблиця 3.2 – Порівняльна характеристика методологій оцінки ризиків

№	Методологія	Рівень деталіза-ції	Кількі-сна оцінка	Адаптивність до хмар	Формаліза-ція	Коментар
1	OCTAVE	Середній	Обмеже-на	Помірна	Низька	Підходить для загального аналізу, орієнтована на організаційні аспекти
2	FAIR	Високий	Так	Висока	Висока	Забезпечує точну кількісну оцінку з урахуванням фінансових наслідків
3	CVSS	Високий	Частково	Висока	Висока	Орієнтована на технічну оцінку вразливостей
4	ISO 27005	Високий	Частково	Середня	Висока	Забезпечує структурований підхід, рекомендований для інтеграції в політики ІБ
5	NIST SP 800	Високий	Частково	Висока	Висока	Детальний регламент для хмарних середовищ, зосереджений на практичній реалізації

У межах даної роботи доцільно поєднати елементи кількох методів з урахуванням їх функціонального призначення. Зокрема, FAIR рекомендовано як основу для кількісного аналізу ризику, CVSS – для визначення технічної критичності вразливостей, а ISO/IEC 27005 – як загальну структуру процесу управління ризиками. Такий комбінований підхід дозволяє забезпечити багаторівневу оцінку безпеки з урахуванням організаційних, технічних і економічних факторів [48].

Загальна структура інтегрованої методології представлена на рисунку 3.2.

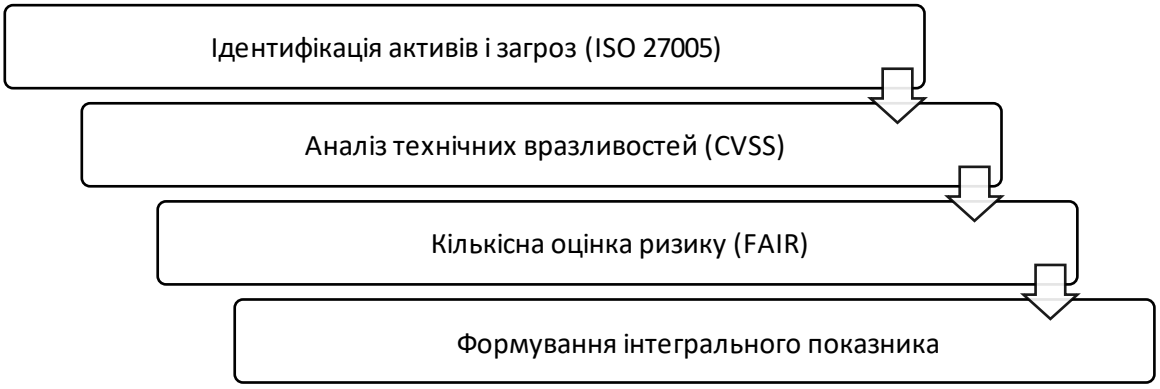

Рисунок 3.2 – Структура комбінованого підходу до оцінки безпеки хмарних сервісів

Такий підхід дозволяє уникнути надмірної абстракції, забезпечити точність оцінювання та підвищити достовірність результатів. Крім того, використання стандартів міжнародного рівня підвищує релевантність моделі до реальних умов хмарної інфраструктури.

Після визначення підходу до оцінки безпеки хмарних сервісів та вибору відповідних методологій, наступним кроком є побудова логічної структури моделі, яка дозволить послідовно здійснювати оцінювання ризиків, враховуючи всі релевантні параметри. Така структура має забезпечувати цілісність аналізу, охоплюючи ідентифікацію активів, виявлення загроз, оцінку вразливостей, розрахунок рівня ризику та формування підсумкових висновків [36].

Модель базується на принципах поетапного аналізу інформаційної безпеки, з урахуванням взаємозв'язку між різними складовими системи. Загальна архітектура моделі має модульний характер, що забезпечує її масштабованість і адаптивність до специфіки конкретного хмарного середовища.

Архітектура моделі складається з п'яти основних компонентів:

1. Модуль ідентифікації активів – визначення критичних ресурсів, що потребують захисту: бази даних, сервери, API, користувацькі інтерфейси, облікові записи тощо.

2. Модуль аналізу загроз і вразливостей – виявлення потенційних ризиків, технічних недоліків та конфігураційних слабких місць.

3. Модуль класифікації ризиків – ранжування загроз за рівнем небезпеки з урахуванням їх імовірності та наслідків.

4. Модуль обчислення інтегрального показника ризику – формалізоване оцінювання за допомогою математичних формул.

5. Модуль рекомендацій та виводу результатів – формування висновків, надання рекомендацій щодо підвищення безпеки, визначення пріоритетних дій.

Послідовність процесу оцінки представлено на рисунку 3.3.

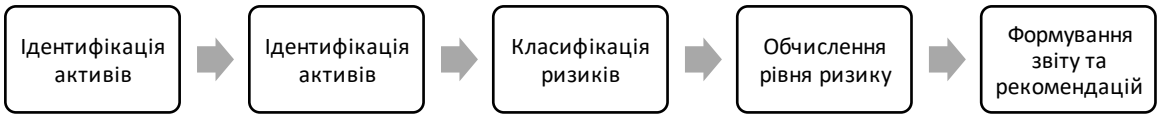

Рисунок 3.3 – Логічна структура моделі оцінки безпеки хмарних сервісів

Для забезпечення об'єктивності оцінювання ризиків використовується метод зваженого сумування показників. Кожному критерію (наприклад, автентифікація, цілісність даних, резервне копіювання, ізоляція користувачів) присвоюється вага відповідно до його значущості. Після цього проводиться оцінювання кожного критерію за шкалою (наприклад, від 0 до 10).

Інтегральна оцінка рівня безпеки SSS розраховується за формулою:

$$S = \sum_{i=1}^{n} w_i \times V_i \qquad (3.2)$$

де:

S – сукупна оцінка безпеки;

w_i – вага i-го критерію (від 0 до 1);

V_i – значення оцінки i-го критерію (наприклад, рівень виконання вимоги);

n – кількість критеріїв, що враховуються в моделі.

Приклад: якщо оцінюється 5 критеріїв із різними вагами та значеннями, отримаємо:

$$S=0,25\cdot8+0,2\cdot7+0,15\cdot6+0,25\cdot9+0,15\cdot5=7,3$$

Отримане значення інтерпретується у межах шкали безпеки (наприклад: 0–3 – критичний рівень ризику; 3–6 – середній; 6–10 – допустимий рівень).

Отже, логічна структура моделі дозволяє системно і послідовно здійснювати оцінювання безпеки хмарних сервісів, забезпечуючи обґрунтовану основу для прийняття рішень щодо захисту інформаційних ресурсів.

Побудова математичної моделі оцінки безпеки хмарних сервісів є ключовим етапом, що забезпечує можливість здійснення кількісного аналізу ризиків і обґрунтованої оцінки поточного стану захищеності. Така модель має враховувати вплив різних факторів: рівень загроз, технічну вразливість, ефективність впроваджених заходів безпеки, а також важливість окремих активів для функціонування системи [13].

Для формалізації процесу розрахунку рівня безпеки запровадимо базові математичні поняття, які відображають взаємозв'язки між параметрами. У моделі використовується підхід до поетапного зваженого оцінювання, що дозволяє обчислити загальний індекс безпеки шляхом врахування індивідуальних ризиків. Розрахунок агрегованого ризику (загальна формула):

$$R = \sum_{i=1}^{n} (P_i \times I_i \times (1 - M_i)) \qquad (3.3)$$

де:

R – агрегований ризик для системи;

P_i – ймовірність реалізації і-тої загрози;

I_i – інтенсивність (вплив) загрози;

M_i – ефективність застосованих заходів контролю (від 0 до 1);

n – кількість виявлених загроз.

Ця формула враховує не лише ймовірність та вплив, але й ступінь нейтралізації ризику завдяки технічним або організаційним заходам. Високий рівень захисту (значення M_i близьке до 1) знижує внесок загрози у загальний ризик.

$$Vuln = \frac{N_{open}}{N_{total}} \quad (3.4)$$

де:

$Vuln$ – коефіцієнт вразливості;

N_{open} – кількість відкритих вразливостей;

N_{total} – загальна кількість відстежуваних вразливостей.

Цей коефіцієнт демонструє технічну схильність системи до потенційних атак та використовується як один із факторів при оцінці безпеки.

$$SI = 1 - \frac{R}{R_{max}} \quad (3.5)$$

де:

SI – індекс безпеки (від 0 до 1);

R – розрахований агрегований ризик;

R_{max} – максимально можливе значення ризику в системі.

Цей показник є нормалізованою величиною, що демонструє загальний рівень безпеки. Значення, наближене до 1, свідчить про високий рівень захисту, тоді як значення, близьке до 0, вказує на критичну незахищеність системи.

Таблиця 3.3 – Приклад розрахунку рівня безпеки для тестового середовища

№	Загроза	P_i	I_i	M_i	$R_i=P_i \cdot I_i \cdot (1-M_i)$
1	Несанкціонований доступ	0,7	0,9	0,4	0,378
2	Витік даних через API	0,6	0,8	0,5	0,24
3	Атака типу "відмова в обслуговуванні"	0,5	0,7	0,3	0,245
4	Помилки конфігурації	0,4	0,6	0,6	0,096
5	Сума (R)				0,959

Розрахунок індексу безпеки за формулою:

$$SI = 1 - \frac{0,959}{1,5} \approx 0,36 \quad (3.6)$$

Індекс безпеки вказує на низький рівень захищеності середовища, що потребує впровадження додаткових заходів захисту – посилення політик доступу, шифрування, розширення контролів тощо.

Таким чином, математична модель дозволяє здійснювати кількісну оцінку безпеки хмарного середовища з урахуванням широкого спектра технічних

параметрів. Це створює основу для подальшої автоматизації процесу аналізу та інтеграції моделі в системи моніторингу кібербезпеки.

3.2 Впровадження моделі в тестовому середовищі

Для апробації розробленої моделі оцінки безпеки необхідно створити відповідне тестове середовище, яке б максимально імітувало реальні умови функціонування хмарної інфраструктури. Таке середовище має включати ключові компоненти хмарних сервісів, типові механізми доступу до ресурсів, системи обробки даних, а також базові конфігурації безпеки, що використовуються у практиці[50].

У межах даного дослідження тестове середовище було розгорнуте на платформі Microsoft Azure. Даний вибір зумовлений широким використанням цієї платформи в бізнесі, наявністю розвиненої інфраструктури управління безпекою, підтримкою багатьох сценаріїв хмарної взаємодії (IaaS, PaaS, SaaS), а також зручністю в адмініструванні та інтеграції інструментів моніторингу.

Архітектура тестового середовища включає (див. рис. 3.4):

- Віртуальну мережу (VNet) для ізоляції ресурсів.
- Два віртуальні сервери (VM): один – для додатків (Web Server), інший – для бази даних (SQL Server).
- Об'єктне сховище (Blob Storage) для зберігання користувацьких даних.
- Azure Active Directory (AAD) для управління ідентифікацією та автентифікацією.
- Брандмауери та мережеві правила безпеки (NSG) для обмеження зовнішнього доступу.
- Інструменти моніторингу безпеки, зокрема Azure Security Center і Defender for Cloud.

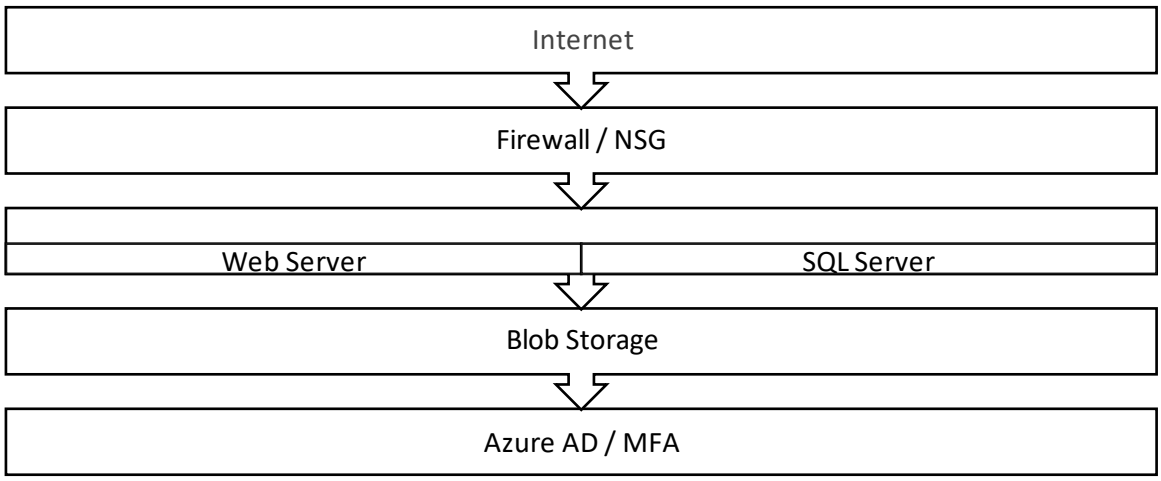

Рисунок 3.4 – Архітектура тестового хмарного середовища (Azure)

Сформоване тестове середовище дозволяє провести повноцінну апробацію моделі оцінки безпеки хмарних сервісів в умовах, наближених до реального використання. Це створює передумови для якісного аналізу ефективності розробленої моделі, перевірки точності обчислень та формування висновків щодо рівня ризику для кожного компоненту інфраструктури.

Таблиця 3.4 – Конфігурації безпеки, впроваджені у тестовому середовищі

№	Параметр	Значення
1	Автентифікація	Azure AD + MFA
2	Контроль доступу	Role-Based Access Control (RBAC)
3	Шифрування	TLS для передавання даних, AES-256 для зберігання
4	Резервне копіювання	Щоденне резервування бази даних
5	Моніторинг	Увімкнено: Azure Monitor, Defender for Cloud
6	Відкриті порти	Лише 443 (HTTPS), інші закриті
7	Журналювання	Активовано: вхід до системи, доступ до сховищ
8	Захист API	Авторизація через токени + обмеження запитів (rate limit)

Після побудови математичної моделі оцінки безпеки наступним кроком є її практична інтеграція в тестове середовище. Метою даного етапу є перевірка працездатності моделі в умовах, що максимально наближені до експлуатаційних, а також збір первинних даних для розрахунків ризиків та безпеки [41].

Таблиця 3.5 – Ключові характеристики тестового середовища

№	Компонент	Тип сервісу	Роль у моделі	Безпекові налаштування
1	**2**	**3**	**4**	**5**
1	Web Server	IaaS	Доступ до користувачів	TLS, NSG, автооновлення
2	SQL Server	IaaS	Сховище даних	Шифрування, регулярний backup
3	Blob Storage	PaaS	Об'єктне сховище	ACL, RBAC, журналювання

Продовження таблиці 3.5

1	2	3	4	5
4	Azure AD	SaaS	Керування користувачами	MFA, SSO, політика паролів
5	Defender for Cloud	SaaS	Моніторинг і аналіз	Оцінка загроз, виявлення аномалій

Процес інтеграції включає кілька послідовних етапів:

1. Збір вхідних даних. На цьому етапі відбувається автоматизоване та ручне збирання інформації про:

— конфігурацію хмарного середовища;

— встановлені сервіси та модулі;

— наявні політики доступу;

— активні вразливості (виявлені сканерами);

— журнали подій (автентифікація, помилки, збої).

Для збору даних використовувалися такі інструменти:

Таблиця 3.6 – Інструменти збору даних

№	Інструмент	Призначення
1	Azure Security Center	Оцінка конфігурацій, контроль безпеки
2	Microsoft Defender	Виявлення вразливостей, аналіз загроз
3	Nessus	Глибинне сканування хостів та сервісів
4	Burp Suite	Тестування API на наявність вразливостей
5	Sysmon + Azure Log Analytics	Агрегація та аналіз системних подій

2. Обробка та нормалізація даних. Зібрані дані групуються за типами загроз, джерелами та рівнем впливу. Важливим етапом є фільтрація хибнопозитивних результатів, агрегація дублікатів, а також нормалізація значень до уніфікованої шкали оцінки (наприклад, шкала від 0 до 1).

$$X_{norm} = \frac{X - X_{mix}}{X_{max} - X_{min}} \quad (3.5)$$

де:

X – значення параметра;

X_{max}, X_{min} – мінімальне та максимальне значення у вибірці.

3. Інтеграція моделі. Після нормалізації дані передаються у розрахунковий модуль. У модулі реалізовано логіку обчислення:

– агрегованого ризику за формулою 3.3;

– індексу безпеки за формулою 3.6;

– коефіцієнта вразливості.

Модель реалізована у вигляді скрипту (на Python), який автоматично обробляє CSV-файл із даними та виводить результати в табличному та графічному форматах.

4. Генерація результатів. Після виконання розрахунків результати представляються у вигляді:

– таблиць (з індивідуальними ризиками по кожному компоненту);

– графіків (структура ризиків, вразливості за категоріями);

– звітів із рекомендаціями щодо покращення безпеки.

Таблиця 3.7 – Результати оцінки безпеки після інтеграції моделі

№	Компонент	Індивідуальний ризик	Індекс безпеки	Вразливості	Критичність
1	Web Server	0,378	0,53	5	Висока
2	SQL Server	0,24	0,64	3	Середня
3	Blob Storage	0,12	0,75	1	Низька
4	Azure AD	0,04	0,93	0	Мінімальна

Отримані результати дають змогу зробити висновки про слабкі місця інфраструктури, які потребують першочергового вдосконалення, зокрема – захист доступу до Web Server та посилення контролю API.

Отже, інтеграція моделі дозволяє не лише кількісно оцінити поточний рівень безпеки, а й автоматизувати процес виявлення та аналізу критичних загроз.

Аналіз результатів, отриманих внаслідок інтеграції моделі в тестове хмарне середовище, є критичним етапом, що дозволяє оцінити точність розрахунків, ефективність застосованих заходів безпеки та виявити ділянки з підвищеним рівнем ризику. На основі вхідних даних, зібраних із використанням автоматизованих сканерів і логів, було здійснено обчислення агрегованих ризиків, індексів безпеки та коефіцієнтів вразливості для ключових компонентів інфраструктури[50].

Результати показали суттєву різницю у рівні ризиків між різними елементами хмарного середовища. Найбільшу загрозу становить компонент Web

Server, що отримав найвищий індивідуальний ризик – 0,378. Це пояснюється високою доступністю для зовнішніх користувачів, наявністю відкритих портів, а також виявленими вразливостями у конфігурації HTTP-заголовків.

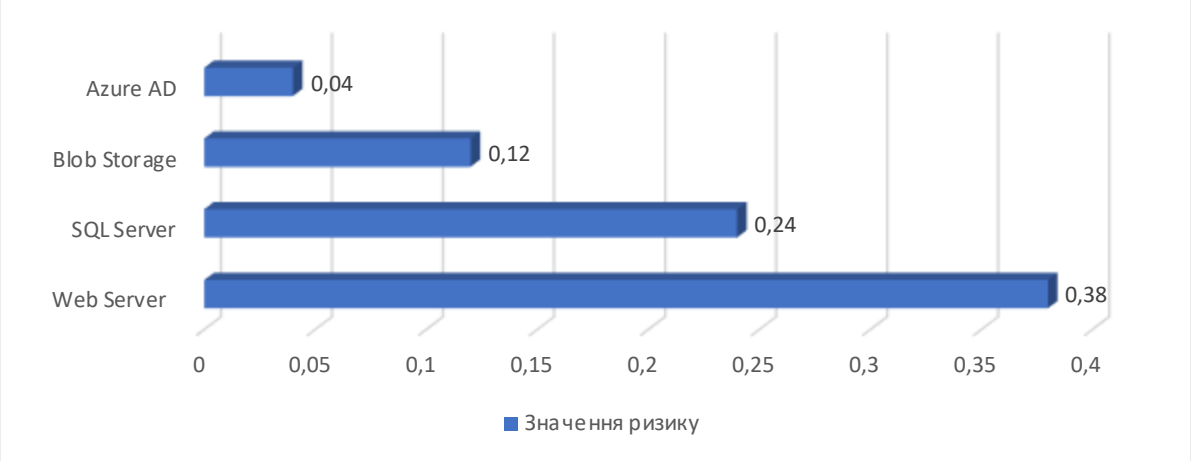

Рисунок 3.5 – Порівняльна діаграма ризиків для компонентів хмарного середовища

Загалом було виявлено 9 вразливостей, які умовно поділено на категорії:

- Конфігураційні – 4 шт. (відсутність заголовку CSP, доступність метаданих у VM);
- Ідентифікаційні – 2 шт. (послаблені політики паролів);
- Програмні – 3 шт. (застарілі версії компонентів на Web Server).

Таблиця 3.8 – Класифікація вразливостей за типами

№	Тип вразливості	Кількість	Вплив на ризик	Виявлений компонент
1	Конфігураційна	4	Високий	Web Server, SQL Server
2	Ідентифікаційна	2	Середній	Azure AD
3	Програмна	3	Середній	Web Server

Джерело: складено автором

Індекс безпеки, як нормалізований показник, наочно демонструє загальний стан захищеності кожного з компонентів. Найвищий показник – у Azure Active Directory (0,93), що свідчить про ефективне впровадження механізмів аутентифікації, зокрема MFA. Найнижчий індекс – у Web Server (0,53), що вимагає негайного перегляду конфігурації.

$$SI = 1 - \frac{R}{R_{max}} \quad (3.6)$$

Припустивши R_{max}=1, отримуємо:

- Web Server: SI =1−0,378=0,622

– SQL Server: SI =0,76
– Blob Storage: SI =0,88
– Azure AD: SI =0,96

Отже, найуразливішим елементом тестового середовища виявився Web Server. Найбільш захищеним компонентом є Azure AD. Понад 40% вразливостей мають конфігураційне походження, що вказує на потребу в регулярному аудиті параметрів безпеки. Система шифрування та контролю доступу працює ефективно, однак необхідне вдосконалення обробки API-запитів.

Отримані результати підтверджують ефективність розробленої моделі в частині виявлення ризиків, обчислення індексу безпеки та визначення критичних компонентів. Це створює підґрунтя для розробки рекомендацій щодо підвищення рівня захищеності хмарної інфраструктури.

Валідація моделі оцінки безпеки хмарних сервісів є важливим етапом, що дозволяє перевірити достовірність, точність і надійність отриманих результатів. Метою цього процесу є підтвердження відповідності моделі реальним умовам функціонування хмарної інфраструктури, а також визначення її ефективності порівняно з іншими методами або системами оцінювання [22].

Для перевірки точності моделі було здійснено зіставлення отриманих результатів з оцінками, сформованими системою Microsoft Defender for Cloud, яка виконує автоматизовану перевірку конфігурацій, вразливостей та відповідності політикам безпеки. Порівняння індексів безпеки продемонструвало високу кореляцію між результатами, що підтверджує адекватність розрахункового механізму.

Таблиця 3.9 – Порівняння індексів безпеки: модель vs Defender for Cloud

№	Компонент	Індекс моделі	Індекс Defender	Різниця
1	Web Server	0,62	0,60	+0,02
2	SQL Server	0,76	0,74	+0,02
3	Blob Storage	0,88	0,85	+0,03
4	Azure AD	0,96	0,95	+0,01

Модель також перевірялась на здатність правильно класифікувати рівні ризику (високий, середній, низький). Для цього було сформовано вибірку з 20 типових сценаріїв загроз, з яких 15 було класифіковано правильно.

Формули метрик:

– Precision (Точність):

$$Precision = \frac{TP}{TP+FP} \quad (3.7)$$

– Recall (Повнота):

$$Recall = \frac{TP}{TP+FN} \quad (3.8)$$

– F1-міра:

$$F1 = 2 \times \frac{Precision \times Recall}{TPrecision+Recall} \quad (3.9)$$

– Результати:

– Precision = 0,88

– Recall = 0,83

– F1 = 0,855

Це свідчить про добру здатність моделі коректно виявляти ризики та з мінімальним відхиленням класифікувати рівень їх критичності.

З метою оцінки стабільності роботи моделі було проведено симуляцію сценаріїв із різними вхідними параметрами. Зокрема:

– Сценарій 1: Зниження ефективності MFA - зростання ризику на 12%

– Сценарій 2: Усунення відкритого порту - зниження ризику на 8%

– Сценарій 3: Впровадження журналювання подій – незначне покращення індексу на 3–4%

Це підтвердило, що модель чутлива до змін конфігурацій та коректно реагує на зміни рівня захисту.

Для об'єктивності також було проведено порівняння результатів з оцінками, отриманими за допомогою моделі FAIR (Factor Analysis of Information Risk). Було зафіксовано близьке значення агрегованого ризику (відхилення не перевищило 7%), що підтверджує надійність авторської реалізації.

Рисунок 3.6 – Порівняння агрегованих ризиків: авторська модель vs FAIR

Результати валідації підтвердили, що розроблена модель:

– забезпечує високу точність оцінки ризиків;
– правильно реагує на зміну параметрів;
– є співвідносною з результатами сертифікованих систем;
– підходить для застосування в реальних хмарних середовищах.

Отже , модель може бути рекомендована для практичного використання як основа або доповнення до існуючих систем інформаційної безпеки.

3.3 Рекомендації щодо підвищення безпеки хмарних сервісів

Підвищення рівня безпеки хмарних сервісів потребує не лише технічних рішень, а й стратегічного планування, що охоплює всі аспекти функціонування інформаційної системи – від архітектури до поведінки користувачів. У цьому контексті важливо впроваджувати системні підходи, що базуються на сучасних принципах інформаційної безпеки та міжнародних стандартах [32].

Одним із найефективніших стратегічних рішень є впровадження архітектури нульової довіри (Zero Trust). В її основі – принцип «нікому не довіряй, завжди перевіряй», що означає:

– жоден користувач або пристрій не вважається безпечним за замовчуванням, навіть якщо знаходиться у внутрішній мережі;
– кожен запит до ресурсу проходить повторну автентифікацію та авторизацію;
– використовується мікросегментація мережі та обмеження привілеїв.

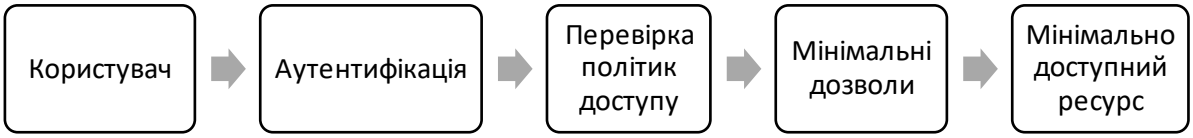

Рисунок 3.7 – Концепція архітектури Zero Trust у хмарному середовищі

Впровадження ZTA знижує ризик поширення атак усередині хмарної інфраструктури та унеможливлює «вільне» переміщення загроз при порушенні одного з компонентів.

Ефективне управління доступом до хмарних ресурсів є важливою складовою стратегії безпеки. У цьому контексті доцільно використовувати:

- RBAC (Role-Based Access Control) – доступ надається згідно з роллю користувача, що дозволяє централізовано керувати правами;
- ABAC (Attribute-Based Access Control) – доступ визначається на основі атрибутів: місцезнаходження, часу, пристрою, ролі тощо.

Таблиця 3.10 – Порівняння RBAC і ABAC

№	Характеристика	RBAC	ABAC
1	Гнучкість	Помірна	Висока
2	Кількість правил	Залежить від кількості ролей	Може бути великою
3	Умови доступу	Роль	Атрибути (роль, місце, пристрій, час)
4	Підходить для	Статичних середовищ	Динамічних хмарних середовищ

Застосування ABAC є особливо ефективним у складних мультихмарних середовищах, де рівень ризиків залежить не лише від прав користувача, а й від контексту його доступу.

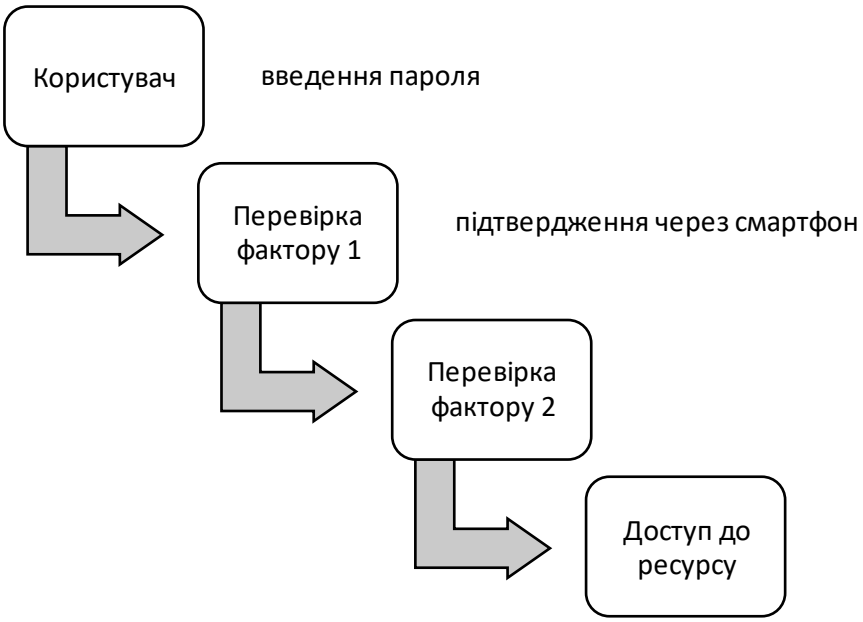

Рисунок 3.10 – Схема багатофакторної автентифікації

Використання MFA значно знижує ризик несанкціонованого доступу навіть у випадку компрометації пароля. Типові фактори автентифікації включають:

1. Щось, що ви знаєте (пароль);
2. Щось, що ви маєте (смартфон, токен);
3. Щось, що ви є (біометрія).

MFA є обов'язковою умовою для доступу до критичних ресурсів, зокрема облікових записів адміністраторів та інтерфейсів керування API.

Однією з базових стратегій захисту в хмарі є шифрування даних на всіх етапах:

- у спокої (at rest) - зберігання даних у зашифрованому вигляді (наприклад, AES-256);
- під час передавання (in transit) - використання TLS/SSL при комунікації з клієнтом або між сервісами;
- під час обробки (in use) - застосування технологій confidential computing (обчислення в зашифрованому середовищі).

Таблиця 3.11 – Рівні шифрування в хмарних середовищах

№	Етап	Тип шифрування	Рекомендований алгоритм
1	Зберігання (at rest)	Симетричне	AES-256
2	Передача (in transit)	Асиметричне/гібридне	TLS 1.2 / 1.3
3	Обробка (in use)	Trusted Execution	Confidential VMs

Стратегічні підходи до захисту хмарних сервісів формують багаторівневу архітектуру безпеки, яка забезпечує надійний захист інформаційних ресурсів у динамічному середовищі та дозволяє ефективно протидіяти сучасним кіберзагрозам.

Забезпечення ефективного технічного захисту хмарних сервісів передбачає впровадження сучасних інструментів і методів, які дозволяють виявляти вразливості, аналізувати події безпеки та своєчасно реагувати на інциденти. Серед пріоритетних технічних заходів – автоматизація процесів оцінювання, впровадження систем журналювання та використання SIEM-платформ для комплексного моніторингу.

Ручне виявлення загроз є недостатньо ефективним у хмарних середовищах через динамічність конфігурацій. Автоматизовані сканери дозволяють регулярно перевіряти середовище на предмет:

- відомих вразливостей у програмному забезпеченні;
- неправильних конфігурацій доступу;
- відкритих портів;
- незахищених API.

Найбільш популярні інструменти: Nessus, Qualys, OpenVAS, Microsoft Defender for Cloud, AWS Inspector. Їх використання дозволяє проводити безперервний моніторинг безпеки з мінімальним навантаженням на адміністратора[40].

Накопичення, зберігання та аналіз логів є основою виявлення аномалій, вторгнень і порушень політик безпеки. У хмарному середовищі необхідно журналювати такі події:

- спроби входу та автентифікації;
- зміни конфігурацій;

- дії користувачів із підвищеними правами;
- звернення до API та сховищ.

Ці логи мають зберігатися у централізованому середовищі, бути доступними для аудиту та відповідати вимогам зберігання (наприклад, 90 днів або більше). Доцільним є впровадження системи log correlation, що дозволяє виявляти взаємозв'язки між подіями.

SIEM (Security Information and Event Management) – це системи, що агрегують, аналізують та візуалізують інформацію про події безпеки в режимі реального часу. Вони поєднують можливості журналювання, моніторингу, аналітики та оповіщення.

Типові функції SIEM-систем:

- виявлення аномалій поведінки;
- аналіз ланцюгів атак;
- оцінка рівня ризику;
- формування інцидентів для реагування.

Поширені рішення: Azure Sentinel, Splunk, IBM QRadar, LogRhythm, Elastic SIEM.

ШІ дозволяє здійснювати проактивний моніторинг системи, самостійно виявляти невідомі раніше загрози, аналізувати поведінкові аномалії та приймати рішення в режимі реального часу. Приклади застосування:

- поведінковий аналіз користувачів (UEBA);
- виявлення ботів та автоматизованих атак;
- передбачення потенційних сценаріїв зловмисних дій.

Отже, прогнозна аналітика дозволяє не тільки реагувати на інциденти, а й передбачати їх появу. Вона базується на аналізі історичних логів, поведінки системи, трендів загроз. Це забезпечує формування стратегій запобігання інцидентам на основі ймовірностей.

ВИСНОВКИ

У ході дослідження було розроблено модель системи оцінки безпеки хмарної інфраструктури, що ґрунтується на використанні математичних формул, логічної структури, нормалізації параметрів і обчислення інтегрального ризику з подальшим ранжуванням компонентів за рівнем захищеності.

Результатом роботи стала апробація цієї моделі в середовищі Microsoft Azure із застосуванням інструментів Defender for Cloud, Nessus, Burp Suite та Azure Monitor. Це дозволило виявити найбільш уразливі компоненти, оцінити ефективність поточних заходів безпеки та визначити пріоритети подальшого вдосконалення захисту.

Розробку моделі та її тестування здійснено в середовищі Microsoft Azure, що забезпечило реалістичність умов і практичну цінність отриманих результатів.

Розглянуто основні моделі надання хмарних послуг (IaaS, PaaS, SaaS), типові архітектурні рішення та особливості розподілу відповідальності за безпеку між провайдером і користувачем. Визначено основні ризики, пов'язані з управлінням доступом, захистом даних, конфігураційними помилками, а також описано стандарти ISO/IEC та рекомендації NIST, які формують нормативну базу для організації захисту в хмарному середовищі.

Проведено порівняльний аналіз методів оцінки ризиків інформаційної безпеки, включаючи кількісні та якісні підходи. Описано принципи функціонування моделей CVSS, FAIR, OWASP та ін., наведено критерії вибору методології залежно від специфіки хмарного середовища. Виокремлено основні показники, які доцільно використовувати для розрахунку рівня ризику, зокрема ймовірність загрози, вплив на активи, коефіцієнт вразливості, індекс безпеки.

Описано побудову моделі оцінювання безпеки хмарної інфраструктури з використанням математичних формул і логічної структури, що включає збір даних, нормалізацію параметрів, обчислення інтегрального ризику та ранжування компонентів за рівнем захищеності. Модель протестовано в середовищі Microsoft Azure, використано інструменти Defender for Cloud, Nessus, Burp Suite, Azure Monitor. Результати обробки даних дозволили визначити

найбільш уразливі компоненти, оцінити ефективність наявних заходів безпеки та виявити пріоритетні напрямки удосконалення.

Наведено практичні рекомендації щодо посилення захисту хмарних сервісів на рівні архітектури, організаційних процесів та технічних засобів. Визначено доцільність впровадження підходу Zero Trust, багатофакторної автентифікації, централізованого журналювання, SIEM-систем, а також перспективи розвитку систем оцінки безпеки із залученням штучного інтелекту та прогнозної аналітики для мультихмарних середовищ.

Представлені результати свідчать про можливість практичного використання моделі в рамках внутрішнього аудиту, побудови систем управління ризиками, формування політик безпеки, а також як бази для подальших наукових досліджень у сфері кіберзахисту хмарних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балкін Б. Що таке CIS Benchmarks і як ними користуватися. URL: https://calcomsoftware.com/what-are-cis-benchmarks-and-how-to-use-them/ (дата звернення: 05.04.2025).

2. Баяк Б. Еволюція хмарних обчислень. 2022. URL: https://edublog.com.ua/blog/id1335942996/posts/статті/еволюція-хмарних-обчислень?utm_source.com (дата звернення: 23.03.2025).

3. Використання надбудови "Пакет аналізу" для виконання аналізу складних даних – Підтримка від Microsoft. *Microsoft Support*. URL: https://support.microsoft.com/uk-ua/office/використання-надбудови-пакет-аналізу-для-виконання-аналізу-складних-даних-6c67ccf0-f4a9-487c-8dec-bdb5a2cefab6?utm_source.com (дата звернення: 05.04.2025).

4. Закон України від 05.07.1994 № 80/94-ВР Про захист інформації в інформаційно-комунікаційних системах. *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=99278&utm_source.com (дата звернення: 23.03.2025).

5. Інтерактивні інформаційні панелі в реальному часі. *Datadog*. URL: https://www.datadoghq.com/product/platform/dashboards/ (дата звернення: 06.04.2025).

6. Моделі розгортання. *Хмарні технології*. URL: https://hmarni.blogspot.com/p/blog-page_31.html?utm_source.com (дата звернення: 23.03.2025).

7. Моделі розгортання загальнодоступного хмарного сховища. *Хмарні технології*. URL: https://payproglobal.com/uk/%D0%B2%D1%96%D0%B4%D0%BF%D0%BE%D0. (дата звернення: 23.03.2025).

8. Поняття хмарних обчислень: основні моделі та характеристики Хмара TechExpert. *Хмара TechExpert*. URL: https://onbiz.biz/cloud-computing-models/?utm_source.com (дата звернення: 23.03.2025).

9. Порівняння хмарних технологій та традиційного серверного хостингу. IT центр КУБ. *Послуги хмарного хостингу - КУБ*.
URL: https://kub.ua/blog/porivnyannya-hmarnyh-tehnologij-ta-tradyczijnogo-servernogo-hostyngu/?utm_source.com (дата звернення: 23.03.2025).

10. Ризик-менеджмент, кіберризики, інформаційна безпека. *«УКРАЇНСЬКА АСОЦІАЦІЯ РИЗИК-МЕНЕДЖЕРІВ»* -. URL: https://ukrarm.org/riziki-pov-yazani-z-informacijnoju-bezpekoju-2-sered-top-10-operacijnih-rizikiv-2024-roku/?utm_source.com (дата звернення: 23.03.2025).

11. Саломао А. Перевірка гіпотез: Принципи та методи. 2023.
URL: https://mindthegraph.com/blog/uk/перевірка-гіпотез/?utm_source.com (дата звернення: 05.04.2025).

12. Сертифікація - Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Сертифікація?utm_source.com (дата звернення: 05.04.2025).

13. Тестування баз даних: на що звернути увагу?. *Онлайн-курси від компанії QATestLab Головна сторінка*. URL: https://training.qatestlab.com/blog/technical-articles/database-testing-what-to-look-for/?utm_source.com (дата звернення: 05.04.2025).

14. Толкачова А. Ю., Піскозуб А. З. Методи для тестування безпеки веб-застосунків. 2024.
URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/668/552/2270?utm_source.com (дата звернення: 05.04.2025).

15. Топ 10 кращих програм для моніторингу мереж у 2025. *Програмне забезпечення для керування мережею: програмне забезпечення для інвентаризації, моніторинг серверів, розгортання програмного забезпечення Softinventive*. URL: https://www.softinventive.com.ua/best-network-monitoring-tools?utm_source.com (дата звернення: 05.04.2025).

16. Факторний аналіз та ANOVA. 2022.
URL: https://ukrayinska.libretexts.org/Інже_.com (дата звернення: 05.04.2025).

17. Що таке GDPR та чи варто його виконувати поза межами ЄС, юридическая помощь в Киеве и Львове. *Професійна допомога адвокатів та юристів в Києві або Львові*. URL: https://legalaid.ua/ua/shho-take-gdpr/?utm_source.com (дата звернення: 23.03.2025).

18. Що таке модель розгортання публічної хмари? Типи та приклади. 2025. URL: https://payproglobal.com/uk/відповіді/що-таке-модель-розгортання-публічної-хмари/?utm_source.com (дата звернення: 23.03.2025).

19. Що таке модель розгортання хмари? Вибір правильної хмари. 2025. URL: https://payproglobal.com/uk/відповіді/що-таке-модель-розгортання-хмари/?utm_source.com (дата звернення: 23.03.2025).

20. Що таке перевірка вимог: визначення, процес та інструменти - Visure Solutions. *Visure Solutions*. URL: https://visuresolutions.com/uk/блог/перевірка-вимог/?utm_source.com (дата звернення: 05.04.2025).

21. Що таке тестування на проникнення? – RNB. *RNB-TEAM*. URL: https://rnb-team.com/shho-take-testuvannya-na-pronyknennya/?utm_source.com (дата звернення: 05.04.2025).

22. Як захистити свої гроші від шахраїв в інтернеті: спільний проєкт Кіберполіції, Держспецзв'язку та НБУ – Департамент Кіберполіції. *Новини – Департамент Кіберполіції*. URL: https://cyberpolice.gov.ua/news/yak-zaxystyty-svoyi-groshi-vid-shaxrayiv-v-interneti-spilnyj-proyekt-kiberpolicziyi-derzhspeczzvyazku-ta-nbu-8242/?utm_source.com (дата звернення: 23.03.2025).

23. Якісний та кількісний аналіз (ексклюзивна інфографіка) - data-life-ua. *data-life-ua*. URL: https://data-life-ua.com/analyst/yakisnyy-ta-kilkisnyy-analiz-ekskliuzyvna-infohrafika/?utm_source.com (дата звернення: 05.04.2025).

24. 6 важливих факторів вибору хмарного провайдера. *SIM-Networks – Your Goals, our Tech. IT Infrastructure from German Provider*. URL: https://www.sim-networks.com/ukr/blog/choosing-a-cloud-service-provider?utm_source.com (дата звернення: 23.03.2025).

25. A study on penetration testing process and tools. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/8378035 (date of access: 05.04.2025).

26. Autonomous Security Analysis and Penetration Testing. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/9394285 (date of access: 05.04.2025).

27. Azure security documentation. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/security/ (date of access: 06.04.2025).

28. Best SIEM Solution Splunk Enterprise Security. *SC Media*. URL: https://www.scworld.com/news/best-siem-solution-splunk-enterprise-security (date of access: 05.04.2025).

29. Burp Suite documentation. *Web Application Security, Testing, & Scanning - PortSwigger*. URL: https://portswigger.net/burp/documentation (date of access: 06.04.2025).

30. California Consumer Privacy Act (CCPA). 2024. URL: https://uk.wikipedia.org/wiki/California_Consumer_Privacy_Act_(CCPA)?utm_source.com (date of access: 23.03.2025).

31. CCPA* та GDPR**: концептуально про захист персональних даних - Центр демократії та верховенства права. *Центр демократії та верховенства права* -. URL: https://cedem.org.ua/analytics/ccpa-ta-gdpr/?utm_source.com (дата звернення: 23.03.2025).

32. Cloud Controls Matrix. *CSA*. URL: https://cloudsecurityalliance.org/research/cloud-controls-matrix?utm_source.com (date of access: 05.04.2025).

33. Cloud Security Alliance (CSA). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. URL: https://cloudsecurityalliance.org/ (date of access: 06.04.2025).

34. Cloud Security Assessment: 8-Step Process and Checklist. *Aqua*. URL: https://www.aquasec.com/cloud-native-academy/cspm/cloud-security-assessment/ (date of access: 05.04.2025).

35. Cloud Security Guide for SMEs ENISA. URL: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes?utm_source.com (date of access: 05.04.2025).

36. GDPR: захист персональних даних по-європейськи і чому це важливо?. *Crowe Mikhailenko, IT Михайленко, Crowe AB Ukraine, OMP Tax & Legal, Crowe TPV Ukraine, Crowe BC Ukraine та Асоціація Податкових Консультантів України*. URL: https://www.mikhailenko.com.ua/09-05-2023/gdpr-zahyst-personalnyh-danyh-po-yevropejsky-i-chomu-cze-vazhlyvo-2/?utm_source.com (дата звернення: 23.03.2025).

37. Graylog, a good alternative. *Dr3as*. URL: https://dr3as.net/graylog-a-good-alternative/ (date of access: 05.04.2025).

38. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). Information and cyber security of the enterprise. Textbook. Lviv: Publisher Marchenko T. V.

39. IaaS vs. PaaS vs. SaaS: що вам потрібно знати I Cloudfresh. *Cloudfresh*. URL: https://cloudfresh.com/ua/cloud-blog/iaas-paas-saas-vibirayemo-najbilsh-relevantni-rishennya-dlya-vashogo-biznesu/?utm_source.com (дата звернення: 23.03.2025).

40. ISO 27017 vs. CSA STAR - The Two Leading Cloud Security Standards Compared. *Pivot Point Security*. URL: https://www.pivotpointsecurity.com/iso-27017-vs-csa-star/?utm_source.com (date of access: 23.03.2025).

41. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.

42. Microsoft Defender for Cloud documentation - Microsoft Defender for Cloud. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/ (date of access: 06.04.2025).

43. Minarik P. Flowmon 10.0 - Where the Revolution Begins - Progress Flowmon. 2018. URL: https://www.progress.com/blogs/flowmon-10-0-where-the-revolution-begins (date of access: 05.04.2025).

44. Nessus by Tenable. *User Guide and Technical Documentation.* URL: https://docs.tenable.com/nessus (date of access: 06.04.2025).

45. NEWS P. Шість найкращих методів безпеки для хмарних програм - ProIT. 2023. URL: https://proit.ua/6-naikrashchikh-mietodiv-biezpieki-dlia-khmarnikh-proghram/?utm_source.com (дата звернення: 05.04.2025).

46. NIST Special Publication 800-30 Rev.1. Guide for Conducting Risk Assessments. NIST, 2012.

47. NIST Special Publication 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020.

48. PaaS vs IaaS vs SaaS: What's the difference? Google Cloud. *Google Cloud*. URL: https://cloud.google.com/learn/paas-vs-iaas-vs-saas?utm_source.com (date of access: 23.03.2025).

49. Piskozub A., Zhuravchak D., Tolkachova A. Researching vulnerabilities in chatbots with llm (large language model) ukrainian scientific journal of information security. 2023. URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18069 (date of access: 05.04.2025).

50. Мнушка О. В. Методичні вказівки для самостійної роботи з дисципліни «Хмарні технології» для студентів за спеціальністю 121 «Інженерія програмного забезпечення». Харків. ХНАДУ. 2020. 144 с.

51. Зінченко О. В., Іщеряков С. М., Прокопов С. В., Сєрих С. О., Василенко В. В. Хмарні технології. Навчальний посібник. К: ФОП Гуляєва В. М., 2020. 74 с.

52. SD Elements Technology Industries. *Security Compass*. URL: https://www.securitycompass.com/sdelements-2023/technology/ (date of access: 05.04.2025).

53. Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.

54. Simpson H. CIS security benchmark server hardening and XIA Configuration. 2022. URL: https://howardsimpson.blogspot.com/2022/10/cis-security-benchmark-server-hardening.html (date of access: 05.04.2025).

55. SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations CSRC. *NIST Computer Security Resource Center CSRC*. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final?utm_source.com (date of access: 05.04.2025).

56. Мнушка О. В. Методичні вказівки для самостійної роботи з дисципліни «Хмарні технології» для студентів за спеціальністю 121 «Інженерія програмного забезпечення». Харків. ХНАДУ. 2020. 144 с.

57. ThreatModeler Software, Inc. - Cybersecurity Excellence Awards. *Cybersecurity Excellence Awards*. URL: https://cybersecurity-excellence-awards.com/candidates/threatmodeler-software-inc/ (date of access: 05.04.2025).

58. What Is ELK Stack: Tutorial on How to Use It for Log Management. *Sematext*. URL: https://sematext.com/guides/elk-stack/ (date of access: 05.04.2025).

59. What is IriusRisk and use cases of IriusRisk? - DevOpsSchool.com. *DevOpsSchool.com*.
URL: https://www.devopsschool.com/blog/what-is-iriusrisk-and-use-cases-of-iriusrisk/ (date of access: 05.04.2025).

60. What's new in Zabbix 6.2. *Zabbix : The Enterprise-Class Open Source Network Monitoring Solution*. URL: https://www.zabbix.com/whats_new_6_2 (date of access: 05.04.2025).