

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

Навчально-науковий інститут
“Інститут інформаційних технологій в економіці”
Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

Галузь знань 12 «Інформаційні технології»

Спеціальність 124 «Системний аналіз»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА
на тему “Аналіз ефективності та безпеки хмарної інфраструктури
корпоративних інформаційних систем”

Здобувача вищої освіти

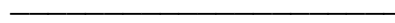
Кисельова Євгенія



(підпис)

Науковий керівник:

д.е.н., професор Камінський О. Є.



(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів
вищої освіти (ЕК)

Завідувач кафедри: доктор фізико-математичних наук, професор

Джалладова Ірада Агаверді-кизи _____

(науковий ступінь, учене звання, ПІБ, підпис)

Київ – 2026

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА: Системний аналіз

ГАЛУЗЬ ЗНАНЬ: 12 Інформаційні технології

СПЕЦІАЛЬНІСТЬ: 124 Системний аналіз

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

_____ І.А. Джалладова
(підпис) (ініціали, прізвище)
_____ 20__ р.

ЗАТВЕРДЖУЮ

Завідувач кафедри системного аналізу
та кібербезпеки

_____ І.А. Джалладова
(підпис) (ініціали, прізвище)
_____ 20__ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Кисельову Євгенію Олександровичу

(прізвище, ім'я, по батькові)

_____ очної (денної) _____ форми навчання

очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

на тему «Аналіз ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем»

Тему затверджено наказом ректора Університету від «___» _____ 20__ р.
№ _____

Кваліфікаційна бакалаврська робота виконується на матеріалах:
узагальненого розрахункового профілю корпоративної інформаційної системи,
сформованого за відкритими та галузевими даними реальних компаній за період не
менше двох років.

План кваліфікаційної бакалаврської роботи

Розділ 1. Теоретико-методичні засади оцінювання ефективності та безпеки хмарної інфраструктури.

Розділ 2. Апробація методики комплексного оцінювання ефективності та безпеки хмарної інфраструктури.

Розділ 3. Рекомендації щодо вибору, оптимізації та захисту хмарної інфраструктури.

Об'єкт дослідження: процеси функціонування хмарної інфраструктури корпоративних інформаційних систем.

Предмет дослідження: методи, моделі та показники оцінювання ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем.

Мета кваліфікаційної бакалаврської роботи: підвищення ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем на основі розроблення комплексної методики їх оцінювання та обґрунтування рекомендацій щодо вибору й конфігурації хмарного рішення.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1:

- 1) Дослідити сутність хмарної інфраструктури корпоративних інформаційних систем, її сервісні та розгортальні моделі.
- 2) Систематизувати показники ефективності хмарної інфраструктури та підходи до її оцінювання.
- 3) Проаналізувати моделі загроз, ризики та стандарти безпеки хмарних систем.
- 4) Обґрунтувати методичний апарат комплексного оцінювання ефективності та безпеки.

У розділі 2:

- 1) Провести системний аналіз об'єкта дослідження та апробувати обрані методики на узагальненому розрахунковому профілі, сформованому за відкритими й галузевими даними реальних компаній.
- 2) Виконати кількісне оцінювання ефективності й безпеки та інтегральне ранжування варіантів хмарних рішень.

У розділі 3:

- 1) Розробити рекомендації щодо вибору й конфігурації хмарної інфраструктури та оптимізаційну модель витрат із прогнозом.
- 2) Обґрунтувати заходи підвищення безпеки і спостережуваності та оцінити їх ефективність.

**Завдання підготував
науковий керівник.**

(підпис) О. Є. Камінський
(ініціали, прізвище)

« ____ » _____ 20__ р.

Завдання одержав здобувач

(підпис) Є. О. Кисельов
(ініціали, прізвище)

« ____ » _____ 20__ р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 56 сторінок основного тексту, 11 рисунків, 17 таблиць (з них 4 у додатках), список використаних джерел із 39 найменувань та 6 додатків.

АНАЛІЗ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Об'єкт дослідження: процеси функціонування хмарної інфраструктури корпоративних інформаційних систем.

Предмет дослідження: методи, моделі та показники оцінювання ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем.

Мета роботи: підвищення ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем на основі розроблення комплексної методики їх оцінювання та обґрунтування рекомендацій щодо вибору й конфігурації хмарного рішення.

Завдання:

1. Дослідити сутність хмарної інфраструктури корпоративних інформаційних систем, її сервісні та розгортальні моделі.
2. Систематизувати показники ефективності хмарної інфраструктури та підходи до її оцінювання.
3. Проаналізувати моделі загроз, ризики та стандарти безпеки хмарних систем.
4. Обґрунтувати методичний апарат комплексного оцінювання ефективності та безпеки.
5. Провести системний аналіз об'єкта дослідження та апробувати обрані методики на узагальненому розрахунковому профілі, сформованому за відкритими й галузевими даними реальних компаній за період не менше двох років.

6. Виконати кількісне оцінювання ефективності й безпеки та інтегральне ранжування варіантів хмарних рішень.
7. Розробити рекомендації щодо вибору й конфігурації хмарної інфраструктури та оптимізаційну модель витрат із прогнозом.
8. Обґрунтувати заходи підвищення безпеки і спостережуваності та оцінити їх ефективність.

Методи дослідження: системний аналіз, аналіз і синтез, багатокритеріальні методи прийняття рішень (TOPSIS, АНР), теорія масового обслуговування (модель М/М/с), методи кількісної оцінки ризику (CVSS, модель «ймовірність × збиток», імітаційне моделювання Монте-Карло), методи прогнозування (трендовий аналіз), ТСО-аналіз.

Структура роботи: робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Апробацію методик виконано на узагальненому розрахунковому профілі корпоративної КІС, параметри якого сформовано за відкритими й галузевими даними реальних компаній за період не менше двох років.

Результати роботи. За результатами апробації методики встановлено, що за прийнятих у моделі ваг і коефіцієнтів та збалансованого співвідношення ефективності й безпеки найстійкішою альтернативою для розглянутого корпоративного профілю є гібридна модель хмарної інфраструктури ($C_i = 0,71$ за TOPSIS); за інших пріоритетів або входних припущень порядок альтернатив може змінюватися, що показав аналіз чутливості. Метод аналізу ієрархій дав узгоджений ваговий вектор ($CR = 0,002$) з домінуванням безпеки та доступності. Кількісна оцінка ризиків методом Монте-Карло показала очікувані річні втрати близько 15,5 млн доларів за вираженого правого хвоста розподілу ($VaR(95\%) = 27,1$ млн), що обґрунтовує врахування не лише середнього ризику, а й хвостових мір. Запропонована оптимізаційна модель сукупної вартості володіння забезпечує економію до 58 % на обчислювальних ресурсах, а програма заходів безпеки знижує очікувані втрати приблизно на 51 %.

Рік виконання роботи - 2026. Рік захисту роботи - 2026.

Ключові слова: хмарна інфраструктура, корпоративні інформаційні системи, системний аналіз, ефективність, інформаційна безпека, оцінювання ризиків, багатокритеріальний аналіз.

Відгук

про кваліфікаційну бакалаврську роботу
здобувача навчально-наукового інституту Інформаційних технологій в економіці
освітньо-професійної програми «Системний аналіз»

Кисельова Євгенія Олександровича

на тему «Аналіз ефективності та безпеки хмарної інфраструктури корпоративних
інформаційних систем»

Актуальність теми: дипломна робота є самостійним дослідженням, яке присвячено важливій темі — аналізу ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем. У сучасних умовах перенесення корпоративних сервісів та даних у хмарне середовище створює нові виклики у сфері кібербезпеки, тому особливого значення набуває комплексний аналіз ефективності функціонування хмарної інфраструктури та оцінювання рівня її захищеності, тобто тема роботи Кисельова Євгенія Олександровича є актуальною.

Позитивні риси кваліфікаційної бакалаврської роботи: у роботі було застосовано комплексний підхід: проаналізовано моделі загроз, ризики та стандарти безпеки хмарних систем. Для оцінки ваг критеріїв обрано метод аналізу ієрархій (АНР), для аналізу продуктивності - модель масового обслуговування, для оцінки ризиків - підхід з імітаційним моделюванням Монте-Карло. Сформовано практичні рекомендації та запропоновано алгоритм вибору конфігурації за класом компанії та балансом пріоритетів. Робота має чітку структуру, логічно побудовані розділи та послідовне викладення матеріалу.

Наявність самостійних розробок автора: Розроблено алгоритм вибору конфігурації за класом компанії та балансом пріоритетів, та програму заходів безпеки.

Цінність теоретичних висновків та практичних рекомендацій. Результати дослідження обумовлюють практичну значущість роботи, у ході дослідження було підтверджено, що запропоновані рекомендації та алгоритм придатні для застосування підприємствами для підвищення захищеності хмарної інфраструктури. Практична цінність роботи полягає у можливості впровадження розроблених рекомендацій в реальні українські підприємства.

Наявність недоліків. Дипломна робота містить певну кількість недоліків, які не впливають на загальну якість виконаної роботи.

Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК: тема роботи розкрита, основні положення та висновки достатньо обґрунтовані. Робота Кисельова Євгенія Олександровича на тему «Аналіз ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем» може бути допущена до захисту перед ЕК і заслуговує на позитивну оцінку, а її автору може бути присвоєна ступінь бакалавра зі спеціальності «Системний аналіз».

Науковий керівник

д.е.н., професор кафедри системного аналізу та кібербезпеки,

Камінський О.Є.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу
здобувача вищої освіти

Кисельова Євгенія Олександровича

**Тема: «Аналіз ефективності та безпеки хмарної інфраструктури
корпоративних інформаційних систем»**

Актуальність теми кваліфікаційної бакалаврської роботи і доцільність її розроблення. Тема є актуальною та практично значущою. Сучасні компанії, зокрема у B2B-сегменті, переносять корпоративні інформаційні системи у хмарне й гібридне середовище, тому питання одночасного забезпечення ефективності та безпеки такої інфраструктури постає в щоденній експлуатації. Здобувач обрав проблему, яка має пряме прикладне значення для бізнесу: як обґрунтовано оцінити та порівняти варіанти хмарних рішень за вартістю, продуктивністю й рівнем захищеності. Розроблення теми доцільне, оскільки його результатом є придатний до використання інструмент підтримки рішень щодо вибору та конфігурації інфраструктури.

Якість проведеного дослідження. Дослідження виконане ґрунтовно й логічно. Автор поєднав у цілісну методику кілька методів: багатокритеріальний аналіз (TOPSIS і АНР), теорію масового обслуговування, кількісну оцінку ризиків методом Монте-Карло та аналіз сукупної вартості володіння. Методику апробовано на узагальненому корпоративному профілі, параметри якого сформовано за відкритими й галузевими даними. Структура роботи послідовна: від теоретико-методичних засад до практичних розрахунків і обґрунтованих рекомендацій. Отримані результати є кількісно підкріпленими та відтворюваними, що особливо цінно для практичного застосування.

Позитивні риси кваліфікаційної бакалаврської роботи.

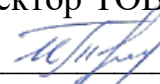
- комплексність методики, яка поєднує оцінювання ефективності та безпеки в єдиному підході;
- наявність конкретних кількісних результатів: інтегральне ранжування варіантів хмарних рішень, оптимізація сукупної вартості володіння з економією витрат, відчутне зниження очікуваних втрат завдяки запропонованим заходам безпеки;
- увага до спостережуваності (моніторинг, централізоване логування, алертинг) як складника надійної експлуатації, що повністю відповідає реальним потребам компаній;
- практична спрямованість: результати роботи можуть бути безпосередньо використані ІТ-підрозділами для обґрунтування вибору й конфігурації хмарної інфраструктури.

Зауваження. Робота містить значний обсяг розрахунків; у подальшому її доцільно доповнити апробацією методики на даних кількох реальних підприємств різних галузей для ширшої перевірки запропонованих рекомендацій. Зазначене зауваження має рекомендаційний характер і не впливає на загальну позитивну оцінку роботи.

Практична значимість висновків і рекомендацій. Висновки та рекомендації мають реальну прикладну цінність. Запропонована методика й оптимізаційна модель витрат можуть застосовуватися компаніями для обґрунтованого вибору та конфігурації хмарної інфраструктури, планування витрат і підвищення рівня інформаційної безпеки. Розглянуті підходи до моніторингу, логування й алертингу узгоджуються з практикою експлуатації корпоративних ІТ-систем і є придатними до впровадження у виробниче середовище.

Місце роботи та посада рецензента: Директор ТОВ «АГРОЗБУТ»

Таратінова Ірина Олексіївна
(ПІБ)


(підпис)

Місце печатки організації, де працює рецензент



ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	3
ВСТУП.....	4
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ.....	9
1.1. Сутність хмарної інфраструктури корпоративних інформаційних систем та її моделі.....	9
1.2. Показники ефективності хмарної інфраструктури та підходи до її оцінювання	11
1.3. Безпека хмарної інфраструктури: моделі загроз, ризики та стандарти	14
1.4. Методичний апарат комплексного оцінювання ефективності та безпеки хмарної інфраструктури.....	17
РОЗДІЛ 2 АПРОБАЦІЯ МЕТОДИКИ КОМПЛЕКСНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ.....	22
2.1. Постановка проблеми та системний аналіз об'єкта дослідження	22
2.2. Аналіз ефективності хмарної інфраструктури на основі фактичних і модельних даних	26
2.3. Кількісна оцінка ризиків безпеки хмарної інфраструктури.....	32
2.4. Інтегральне оцінювання «ефективність-безпека» і підтвердження проблеми	37
РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ, ОПТИМІЗАЦІЇ ТА ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ	43
3.1. Рекомендації щодо вибору й конфігурації хмарної інфраструктури	43
3.2. Оптимізаційна модель сукупної вартості володіння	44
3.3. Заходи підвищення безпеки та спостережуваності й оцінка їх ефективності	47
ВИСНОВКИ	50
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	53

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення	Розшифрування
KIC	корпоративна інформаційна система
AHP	Analytic Hierarchy Process (метод аналізу ієрархій)
API	Application Programming Interface (програмний інтерфейс застосунку)
APT	Advanced Persistent Threat (складна постійна загроза)
AWS	Amazon Web Services
CSA	Cloud Security Alliance
CVSS	Common Vulnerability Scoring System (система оцінювання вразливостей)
DNS	Domain Name System (система доменних імен)
ENISA	European Union Agency for Cybersecurity (Агентство ЄС з кібербезпеки)
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation (Загальний регламент захисту даних)
IaaS	Infrastructure as a Service (інфраструктура як послуга)
IAM	Identity and Access Management (управління ідентифікацією та доступом)
IOPS	Input/Output Operations Per Second (операцій введення-виведення за секунду)
ISMS	Information Security Management System (система управління інформаційною безпекою)
MTBF	Mean Time Between Failures (середнє напрацювання на відмову)
MTTR	Mean Time To Repair (середній час відновлення)
PaaS	Platform as a Service (платформа як послуга)
PII	Personally Identifiable Information (персональні дані)
SaaS	Software as a Service (програмне забезпечення як послуга)
SLA	Service Level Agreement (угода про рівень послуг)
SLO	Service Level Objective (ціль рівня послуг)
SQO	Service Qualitative Objective (якісна ціль послуги)
TCO	Total Cost of Ownership (сукупна вартість володіння)
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution

ВСТУП

Актуальність теми. Перенесення корпоративних інформаційних систем у хмару перестало бути технологічним експериментом і стало щоденною практикою бізнесу. Компанії відмовляються від утримання власних серверних на користь оренди обчислювальних потужностей: це скорочує капітальні витрати, прискорює запуск сервісів і дозволяє масштабувати ресурси під фактичне навантаження. Разом із цими перевагами хмара приносить і нові залежності. Відмова провайдера, помилки в налаштуванні прав доступу, витоки даних, втрата контролю над тим, де фізично зберігається інформація: усе це стає частиною операційних ризиків компанії.

Для України питання має додатковий вимір. Через загрозу фізичного знищення обладнання багато підприємств перенесли критичні дані та сервіси до зовнішніх дата-центрів, і хмара тут працює як інструмент стійкості бізнесу. Але та сама міграція створює нову залежність від іноземних провайдерів, ускладнює транскордонний захист персональних даних і розширює поверхню атаки. Тому для вітчизняних компаній ефективність і безпека хмарної інфраструктури - це не абстрактна технічна тема, а умова безперервності діяльності.

Звідси постає суперечність, що визначає проблему дослідження. Ефективність і безпека часто тягнуть рішення в протилежні боки: дешевша конфігурація буває менш захищеною, а посилення безпеки збільшує витрати й іноді знижує швидкодію. На практиці ці два аспекти оцінюють окремо - різними інструментами та різними фахівцями. Через це рішення про вибір і конфігурацію хмарного середовища нерідко ухвалюють без єдиної кількісної бази, спираючись на інтуїцію або маркетингові матеріали постачальників.

Подолати цю суперечність дозволяє системний аналіз. Він розглядає хмарну інфраструктуру як єдину систему, у якій показники продуктивності, вартості, доступності та захищеності пов'язані між собою, і дає математичний апарат для зведення цих показників у єдину оцінку. Розроблення такого комплексного підходу

до оцінювання ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем і визначає актуальність обраної теми.

Аналіз останніх досліджень і публікацій. Теоретичну основу оцінювання хмарної інфраструктури закладено в базових документах і стандартах: визначення та моделі хмарних обчислень систематизовано в NIST SP 800-145 і серії ISO/IEC 22123, питання захисту й управління ризиками опрацьовано в стандартах ISO/IEC 27001, 27017, 27018 та в NIST SP 800-30. Методичний апарат багатокритеріального оцінювання спирається на класичні праці Т. Сааті (метод аналізу ієрархій) і Ч.-Л. Хванга та К. Юна (метод TOPSIS), а оцінювання продуктивності систем масового обслуговування - на роботах Л. Клейнрока. Прикладну та галузеву картину доповнюють аналітичні звіти провідних організацій: переліки актуальних загроз Cloud Security Alliance і ENISA, оцінки вартості інцидентів IBM Security, а також звіти Flexera та практиків FinOps щодо оптимізації хмарних витрат. Водночас більшість наявних праць розглядає ефективність і безпеку хмарної інфраструктури окремо - як самостійні предмети з власним інструментарієм, - тоді як їх кількісне поєднання в межах єдиної оцінки висвітлено фрагментарно. Саме цю прогалину - відсутність інтегрованого підходу, що зводить різномірні показники ефективності та безпеки в спільну систему координат для обґрунтування вибору конфігурації, - і покликана заповнити ця робота.

Мета дослідження. Мета роботи полягає в тому, щоб підвищити ефективність і безпеку хмарної інфраструктури корпоративних інформаційних систем. Досягається вона розробленням єдиної методики, яка дозволяє кількісно оцінити обидва аспекти в спільній системі координат, та обґрунтуванням практичних рекомендацій щодо вибору й налаштування хмарного середовища під потреби підприємства.

Завдання дослідження. Для досягнення поставленої мети визначено такі завдання:

1. Дослідити сутність хмарної інфраструктури корпоративних інформаційних систем, розмежувати її сервісні (IaaS, PaaS, SaaS) та

розгортальні (публічна, приватна, гібридна) моделі й з'ясувати їхні особливості.

2. Систематизувати показники ефективності хмарної інфраструктури - продуктивність, доступність, вартість, рівень використання ресурсів - та підходи до їх вимірювання.
3. Проаналізувати моделі загроз і ризики хмарних систем, а також стандарти й практики забезпечення їх безпеки.
4. Обґрунтувати методичний апарат комплексного оцінювання, що поєднує показники ефективності та безпеки в межах єдиного підходу.
5. Провести системний аналіз об'єкта дослідження й апробувати обрані методики на узагальненому розрахунковому профілі, сформованому за відкритими й галузевими даними реальних компаній за період не менше двох років.
6. Виконати кількісне оцінювання ефективності та безпеки і на його основі побудувати інтегральне ранжування варіантів хмарних рішень.
7. Розробити рекомендації щодо вибору й конфігурації хмарної інфраструктури, а також оптимізаційну модель витрат із прогнозом на перспективу.
8. Обґрунтувати заходи підвищення безпеки і спостережуваності інфраструктури та оцінити очікувану ефективність їх упровадження.

Об'єкт дослідження. Об'єктом дослідження є процеси функціонування хмарної інфраструктури корпоративних інформаційних систем. У межах роботи ці процеси розглядаються як взаємопов'язана сукупність розгортання й експлуатації обчислювальних ресурсів, моніторингу їх стану, управління доступами та захисту даних. Саме в межах цих процесів виникають проблеми, на вирішення яких спрямовано роботу.

Предмет дослідження. Предметом дослідження є сукупність методів, моделей і показників, за допомогою яких оцінюють ефективність та безпеку хмарної інфраструктури корпоративних інформаційних систем. Предмет

конкретизує проблемну ситуацію в межах об'єкта й відповідає темі роботи; об'єкт і предмет співвідносяться між собою як загальне й часткове.

Методи дослідження. Теоретичну основу склали методи аналізу та синтезу, за допомогою яких узагальнено наукові підходи до оцінювання хмарної інфраструктури. Системний аналіз застосовано для декомпозиції інфраструктури на підсистеми та виявлення зв'язків між показниками ефективності й безпеки. Методи багатокритеріального прийняття рішень (TOPSIS, АНР) використано для зведення різнорідних показників в інтегральну оцінку та ранжування варіантів. Теорію масового обслуговування (модель М/М/с) застосовано для оцінювання продуктивності та обґрунтування параметрів масштабування. Методи кількісної оцінки ризику (CVSS, модель «ймовірність × збиток», імітаційне моделювання Монте-Карло) використано для розрахунку рівня захищеності та очікуваних втрат. Методи прогнозування (трендовий аналіз) і ТСО-аналіз застосовано для оцінювання та прогнозування витрат. Оброблення й візуалізацію даних виконано графічними та статистичними засобами.

Теоретична, методична та практична значущість одержаних результатів. Теоретична значущість полягає в систематизації показників ефективності та безпеки хмарної інфраструктури й у поєднанні цих двох аспектів у межах єдиного системного погляду. Методична значущість виявляється в розробленні комплексної методики, яка зводить різнорідні показники в інтегральну оцінку та дозволяє порівнювати й ранжувати варіанти хмарних рішень. Практична значущість полягає в тому, що запропоновані методика та рекомендації можуть бути використані підприємствами для обґрунтованого вибору й конфігурації хмарної інфраструктури з урахуванням балансу між вартістю, продуктивністю та захищеністю.

Інформаційна база дослідження. Інформаційною базою стали наукові праці з системного аналізу та інформаційної безпеки, міжнародні стандарти, аналітичні звіти провідних організацій галузі, офіційна технічна документація та цінові пропозиції хмарних провайдерів (Amazon Web Services, Microsoft Azure,

Google Cloud Platform), а також матеріали, зібрані автором під час переддипломної практики у ТОВ «АГРОЗБУТ».

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ

1.1. Сутність хмарної інфраструктури корпоративних інформаційних систем та її моделі

Сучасні корпоративні інформаційні системи (КІС) дедалі рідше працюють на власному обладнанні компанії й дедалі частіше спираються на орендовані обчислювальні ресурси. Щоб коректно оцінювати їх ефективність і безпеку, спершу потрібно чітко визначити, що саме розуміють під хмарними обчисленнями та хмарною інфраструктурою, оскільки на практиці ці терміни нерідко вживають як синоніми, хоча вони описують різні рівні системи.

Найавторитетнішим джерелом термінології залишається спеціальна публікація NIST SP 800-145. Згідно з нею, хмарні обчислення - це модель, що забезпечує зручний мережевий доступ на вимогу до спільного пулу налаштовуваних обчислювальних ресурсів, які можна швидко виділяти та вивільняти з мінімальними управлінськими зусиллями. Ця модель складається з п'яти суттєвих характеристик, трьох сервісних моделей і чотирьох моделей розгортання [1]. Близьке за змістом визначення дає міжнародний стандарт: хмарні обчислення трактують як парадигму мережевого доступу до масштабованого й еластичного пулу спільних фізичних або віртуальних ресурсів із самообслуговуванням на вимогу [2]. Базовий міжнародний стандарт-словник ISO/IEC 17788:2014 наприкінці 2023 року було скасовано: його замінено стандартами ISO/IEC 22123-1:2023 та ISO/IEC 22123-2:2023 [2, 3]. Друге видання ISO/IEC 22123-1 скасовує й замінює ISO/IEC 17788:2014 як технічно переглянуте [4], тому в роботі за основу взято чинну редакцію, а NIST SP 800-145 використано як усталене й широко цитоване визначення.

Окремо розмежуємо поняття «хмарна інфраструктура». У NIST SP 800-145 її визначають як сукупність апаратних і програмних засобів, що забезпечують суттєві характеристики хмари. У ній виділяють фізичний рівень - обладнання

(сервери, сховища, мережеві компоненти), і рівень абстракції - програмне забезпечення, розгорнуте поверх фізичного рівня [1]. Подібну логіку, через фізичні та логічні сутності, використовує і ISO/IEC 22123-2:2023 [3]. Саме хмарна інфраструктура, а не послуга як така, є об'єктом цього дослідження: від її конфігурації залежать і продуктивність, і вартість, і захищеність KIC.

Хмарну модель характеризують п'ять суттєвих ознак за NIST. Самообслуговування на вимогу дозволяє споживачеві виділяти ресурси самостійно, без втручання персоналу провайдера; широкий мережевий доступ забезпечує роботу з різних типів пристроїв; об'єднання ресурсів означає їх спільне використання багатьма споживачами за моделлю мультиоренди; швидка еластичність дає змогу масштабувати потужності відповідно до попиту; вимірюваність послуги передбачає автоматичний облік і контроль спожитих ресурсів [1]. Міжнародний стандарт додатково розглядає мультиоренду як окрему ключову характеристику: у ISO/IEC 22123-2:2023 ключові характеристики хмарних обчислень описано в підпунктах 5.2.2–5.2.7 [3], через що їх перелік іноді подають як шість. Для строгості викладу в роботі за канонічний прийнято перелік із п'яти ознак NIST, а мультиоренду розглянуто як істотну додаткову характеристику.

За способом надання послуг розрізняють три сервісні моделі, які відрізняються тим, ким контролюється кожен рівень інфраструктури. У моделі «інфраструктура як послуга» (IaaS) споживач отримує обчислювальні потужності, сховища та мережі й самостійно керує операційними системами та застосунками, не контролюючи базову інфраструктуру; у моделі «платформа як послуга» (PaaS) провайдер надає середовище для розгортання застосунків, а споживач керує лише застосунками та частиною налаштувань; у моделі «програмне забезпечення як послуга» (SaaS) користувач працює з готовим застосунком провайдера й не керує ні інфраструктурою, ні самим застосунком [1]. Ключовий практичний наслідок цього поділу - зміщення межі відповідальності: що ближче до SaaS, то більшу частину відповідальності за інфраструктуру й безпеку бере на себе провайдер, і навпаки. При цьому навіть у моделі SaaS за споживачем завжди лишається

відповідальність за дані, управління доступами та організаційні заходи безпеки. Детальний розподіл зон відповідальності за моделями наведено в Додатку А.

За способом організації виділяють чотири моделі розгортання. Приватна хмара призначена для одноосібного використання однією організацією; громадська (community) - для спільноти організацій зі спільними вимогами; публічна хмара відкрита для широкого загалу й існує на потужностях провайдера; гібридна хмара поєднує дві або більше окремих інфраструктур, пов'язаних технологіями перенесення даних і застосунків [1]. Для корпоративних інформаційних систем найбільш практично значущими є публічна, приватна та гібридна моделі.

У цьому й проявляється проблема, що проходить через усю роботу. Вибір сервісної та розгортальної моделі є водночас технічним і управлінським рішенням, у якому ефективність і безпека часто конкурують. Публічна хмара та модель SaaS зменшують витрати й навантаження на власний персонал, але передають значну частину контролю над даними зовнішньому провайдеру. Приватна хмара та IaaS повертають контроль, проте підвищують вартість і вимоги до кваліфікації команди. З огляду на цей баланс, для більшості корпоративних систем найбільш виправданою є гібридна модель: вона дозволяє утримувати критичні дані та сервіси під власним контролем, а менш чутливі або змінні за навантаженням завдання виносити в публічну хмару заради масштабованості й економії. Відкритим залишається питання, за якими саме показниками порівнювати ці варіанти, щоб рішення спиралося не на інтуїцію, а на кількісну оцінку. Відповідь на нього потребує системи показників ефективності та безпеки, яку розглянуто в наступних підрозділах.

1.2. Показники ефективності хмарної інфраструктури та підходи до її оцінювання

Ефективність хмарної інфраструктури не зводиться до одного числа. Вона багатовимірна: одна й та сама конфігурація може бути дешевою, але повільною, або швидкою, але з низьким коефіцієнтом використання ресурсів. Тому для оцінювання потрібна не окрема метрика, а система показників, що охоплюють різні

сторони роботи інфраструктури. У роботі їх згруповано за чотирма напрямками: доступність, продуктивність, використання ресурсів і вартість.

Доступність (availability) показує частку часу, протягом якого сервіс працездатний, і обчислюється за формулою

$$A = (T - D) / T \times 100 \% \quad (1.1)$$

де T - загальний час, D - час простою. Доступність традиційно описують через «дев'ятки»: 99,9 % - це «три дев'ятки», 99,99 % - «чотири». Різниця між ними здається малою, але в перерахунку на час простою вона суттєва (табл. 1.1). Поряд із доступністю використовують показники середнього напрацювання на відмову (MTBF) і середнього часу відновлення (MTTR). За експоненційного наближення доступність пов'язана з ними співвідношенням

$$A \approx \text{MTBF} / (\text{MTBF} + \text{MTTR}) \quad (1.2)$$

тобто висока доступність досягається або рідшими відмовами, або швидшим відновленням. Формально вимоги до доступності закріплюють в угоді про рівень послуг (SLA). Структуру таких угод унормовує серія стандартів ISO/IEC 19086, яка вводить поняття цілей рівня послуг (SLO) - кількісно вимірюваних, та якісних цілей (SQO), і пропонує модель опису метрик (частина 2) та компоненти безпеки й захисту персональних даних (частина 4) [5].

Таблиця 1.1 - Відповідність рівня доступності допустимому часу простою

Рівень доступності	Назва	Простій на рік	Простій на місяць
99 %	дві дев'ятки	$\approx 3,65$ дня	$\approx 7,3$ год
99,9 %	три дев'ятки	$\approx 8,76$ год	$\approx 43,8$ хв
99,95 %	-	$\approx 4,38$ год	$\approx 21,9$ хв
99,99 %	чотири дев'ятки	$\approx 52,6$ хв	$\approx 4,4$ хв
99,999 %	п'ять дев'яток	$\approx 5,26$ хв	≈ 26 с

Джерело: розраховано автором (525 600 хв на рік)

На практиці провайдери гарантують різні рівні доступності залежно від конфігурації. Для Amazon EC2 регіональний SLA становить 99,99 % за умови розгортання щонайменше у двох зонах доступності, тоді як для окремого інстансу - лише 99,5 % [6]. Microsoft Azure для віртуальних машин декларує 99,9 % для

одиночної VM, 99,95 % за наявності групи доступності та 99,99 % для розгортання в кількох зонах; Google Compute Engine - 99,9 % для одиночного інстансу та 99,99 % для багатозонного [7]. Закономірність спільна: високу доступність забезпечує не сам провайдер, а надлишковість конфігурації, за яку платить замовник.

Тут проявляється чинник негативного впливу, який треба враховувати. SLA вимірює те, що провайдер визначив як доступність, а не те, що відчуває користувач: планове обслуговування часто виключають із розрахунку, а реальна доступність застосунку нижча за паспортну, бо складається з послідовно з'єднаних сервісів - за правилом добутку ймовірностей три сервіси по 99,9 % дають уже близько 99,7 %. Жоден із гарантованих рівнів не убезпечує від масштабних збоїв. Лише за 2025 рік усі три найбільші провайдери пережили серйозні відмови: 12 червня - Google Cloud Platform через перевантаження служби Service Control; 20 жовтня - AWS у регіоні us-east-1, де відмова DNS, пов'язана з DynamoDB, каскадно вивела з ладу понад сотню сервісів більш ніж на 15 годин; 29 жовтня - Microsoft Azure через помилкову зміну конфігурації Azure Front Door, що спричинила близько 8–9 годин недоступності Microsoft 365, Teams й Outlook [8]. Тому задеклароване значення SLA - необхідний, але недостатній орієнтир, який слід доповнювати незалежним моніторингом і резервуванням на рівні архітектури.

Продуктивність описує, наскільки швидко інфраструктура обробляє навантаження. Основні показники - затримка (latency, час обробки однієї операції введення-виведення), час відгуку (response time), пропускна здатність (throughput, обсяг даних за одиницю часу) та кількість операцій введення-виведення за секунду (IOPS). Ці показники пов'язані між собою: за фіксованого розміру блоку пропускна здатність приблизно дорівнює добутку IOPS на розмір блоку. Вони безпосередньо впливають на досвід користувача й на здатність системи витримувати пікове навантаження.

Використання ресурсів (utilization) показує, наскільки повно задіяні оплачені потужності. Низький коефіцієнт використання означає переплату: інстанс, завантажений на 10 %, у більшості моделей тарифікації коштує стільки ж, скільки повністю завантажений [9]. Завелике резервування (over-provisioning)

призводить до зайвих витрат, а замале (under-provisioning) - до деградації продуктивності та порушень SLA. Простоювальні ресурси (idle resources) - невикористані диски, «висячі» IP-адреси, недовантажені інстанси - за галузевими оцінками є одним із найбільших джерел втрат у хмарі.

Вартість завершує систему показників і часто стає вирішальною. Хмара переводить витрати з капітальних в операційні, пропонуючи кілька моделей тарифікації: оплату за фактичне споживання (pay-as-you-go), зарезервовані потужності зі знижкою до 70 % за зобов'язання на 1–3 роки (reserved), переривані ресурси зі знижкою до 80–90 % (spot, preemptible) та автоматичні знижки за тривалість використання у Google Cloud (до ≈ 30 %) [9]. Для коректного порівняння варіантів використовують показник сукупної вартості володіння (TCO), який враховує не лише ціну обчислень, а й витрати на перенесення даних, підтримку, навчання персоналу, трафік назовні та вартість простоїв.

Зведені разом, ці показники мають різну природу й різні одиниці виміру: доступність - у відсотках, продуктивність - у мілісекундах, вартість - у грошах. Порівнювати варіанти хмарних рішень безпосередньо за такою різномірною сукупністю неможливо без приведення до спільної шкали. Тому далі в роботі застосовано методи багатокритеріального оцінювання, які зводять ці показники в єдину інтегральну оцінку. Досвід переддипломної практики підтверджує практичну значущість цих метрик: контроль доступності та продуктивності інфраструктури там реалізовано через систему моніторингу на базі Prometheus і Grafana, а швидкість реакції на збої - через налаштовані алерти.

1.3. Безпека хмарної інфраструктури: моделі загроз, ризики та стандарти

Якщо ефективність відповідає на питання «наскільки добре працює інфраструктура», то безпека - на питання «наскільки їй можна довіряти». У хмарі безпека має принципову особливість: вона не належить комусь одному. Відповідальність розподілена між провайдером і замовником за моделлю, яку прямо продовжує поділ із підрозділу 1.1 (табл. 1.2). Провайдер відповідає за безпеку самої хмари - фізичні центри обробки даних, обладнання, гіпервізор;

замовник - за безпеку в хмарі: дані, конфігурацію, управління доступами. Cloud Security Alliance наголошує, що цю модель спільної відповідальності потрібно не лише декларувати і водночас забезпечувати виконання, і що кінцева відповідальність за комплаєнс і безперервність діяльності залишається за замовником навіть тоді, коли окремі функції виконує провайдер [10].

Таблиця 1.2 - Розподіл відповідальності за безпеку за сервісними моделями

Рівень інфраструктури	IaaS	PaaS	SaaS
Дані	Замовник	Замовник	Замовник
Застосунки	Замовник	Замовник	Провайдер
Середовище виконання	Замовник	Провайдер	Провайдер
Операційна система	Замовник	Провайдер	Провайдер
Віртуалізація / гіпервізор	Провайдер	Провайдер	Провайдер
Сервери	Провайдер	Провайдер	Провайдер
Сховище	Провайдер	Провайдер	Провайдер
Мережа	Провайдер	Провайдер	Провайдер
Фізичний ЦОД	Провайдер	Провайдер	Провайдер

Джерело: складено автором за [10]

Підтверджує це й структура актуальних загроз. У звіті CSA «Top Threats to Cloud Computing 2024» перше місце вперше посіли не дії провайдера, а помилки конфігурації та неналежний контроль змін, які потіснили управління доступами (IAM). Помилки конфігурації стабільно входять до головних чинників хмарних інцидентів, хоча єдиного глобального відсоткового значення провідні звіти не фіксують [10]. Повний перелік провідних загроз наведено в табл. 1.3.

Таблиця 1.3 - Провідні загрози хмарним обчисленням за CSA (2024)

№ (2024)	Загроза	Ранг 2022
1	Помилки конфігурації та неналежний контроль змін	3
2	Управління ідентифікацією та доступом (IAM)	1
3	Незахищені інтерфейси та API	2
4	Неналежний вибір/реалізація стратегії безпеки	4
5	Незахищені сторонні ресурси	6
6	Незахищена розробка програмного забезпечення	5
7	Випадкове розкриття хмарних даних	8
8	Системні вразливості	7

№ (2024)	Загроза	Ранг 2022
9	Обмежена видимість і спостережуваність	-
10	Неавтентифікований обмін ресурсами	-
11	Складні постійні загрози (APT)	10

Джерело: складено автором за [10]

Характерно, що верхні позиції рейтингу - це здебільшого помилки на боці замовника: неправильні налаштування, надмірні права доступу, незахищені інтерфейси. Це підтверджує, що в сучасній хмарі основний центр ризику змістився від інфраструктури провайдера до того, як її конфігурує й експлуатує організація. Дев'ята позиція, обмежена видимість і спостережуваність, заслуговує окремої уваги: брак моніторингу сам собою визнано загрозою, оскільки без нього інциденти виявляють надто пізно. ENISA у звіті Threat Landscape 2024 також відзначає, що недостатні моніторинг і телеметрія посилюють загрози доступності та даних, особливо в гібридних і розподілених середовищах [11]. Це безпосередньо пов'язано з практичною частиною дослідження, де спостережуваність інфраструктури вибудовувалася саме для того, щоб скоротити час виявлення проблем.

Ризики, що впливають із цих загроз, доцільно групувати за природою: технічні (вразливості, збої, помилки конфігурації), організаційні (брак стратегії, кваліфікації, контролю), правові та комплаєнс-ризики (захист персональних даних, транскордонне зберігання) і ризики, пов'язані з даними (витоки, втрата, несанкціонований доступ). Така класифікація потрібна, щоб не лише перелічити загрози, а й зіставити їх із заходами протидії.

Заходи протидії впорядковують міжнародні стандарти. Базовим є ISO/IEC 27001, що задає систему управління інформаційною безпекою (ISMS); у редакції 2022 року до його Додатка А введено окремий контроль A.5.23 щодо інформаційної безпеки під час використання хмарних послуг [12]. Хмарну специфіку деталізують два кодекси усталеної практики: ISO/IEC 27017, який доповнює контролі ISO/IEC 27002 хмарною настановою та додає сім специфічних хмарних (CLD) контролів [13], та ISO/IEC 27018, що регулює захист персональних даних (PII) у публічних хмарах і узгоджений із вимогами захисту приватності на кшталт GDPR [14].

Зауважимо, що ISO/IEC 27017 і 27018 не є самостійними сертифікованими стандартами - їх упроваджують у межах ISMS за ISO/IEC 27001.

Щоб безпеку можна і описувати, і вимірювати, застосовують кількісні шкали оцінювання вразливостей. Найпоширеніша - Common Vulnerability Scoring System (CVSS). У версії 4.0 вона складається з чотирьох груп метрик (базової, загрозової, середовищної та додаткової) і дає числову оцінку серйозності вразливості в діапазоні від 0 до 10 [15]. При цьому сам CVSS не є мірою ризику: він оцінює серйозність вразливості, тоді як повна оцінка ризику потребує врахування ймовірності експлуатації та розміру збитку. Тому CVSS використовують як вхідні дані для моделі «ймовірність × збиток», яку застосовано далі в роботі.

Нарешті, ціна безпеки вимірюється і технічно, і фінансово. За звітом IBM «Cost of a Data Breach 2025», середня глобальна вартість витоку даних становила 4,44 млн доларів, а у США сягнула рекордних 10,22 млн; при цьому організаціям у середньому потрібен 241 день, щоб виявити й локалізувати порушення [16]. Ці цифри й закладають фактичне підтвердження проблеми: безпеку неможливо забезпечити «на сто відсотків», тому її розглядають як керування ризиком до прийняттого рівня, а рішення мають спиратися на вимірювані показники, а не на припущення. Звести показники безпеки разом із показниками ефективності в єдину оцінку дозволяє математичний апарат, описаний у підрозділі 1.4.

1.4. Методичний апарат комплексного оцінювання ефективності та безпеки хмарної інфраструктури

Попередні підрозділи окреслили дві системи показників - ефективності й безпеки - і зафіксували їхню різноманітність: доступність вимірюють у відсотках, продуктивність - у мілісекундах, вартість - у грошових одиницях, ризик - у грошових втратах або умовних балах. Безпосередньо порівнювати варіанти хмарних рішень за такою сукупністю неможливо. Для цього потрібен методичний апарат, здатний звести різноманітні показники до єдиної шкали, врахувати їхню відносну важливість і отримати кількісно обґрунтований результат. У цьому

підрозділі описано чотири групи методів - багатокритеріального аналізу, масового обслуговування, кількісної оцінки ризику та прогнозування, а також інтегральний показник, що об'єднує перші дві.

Метод TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) запропонували Hwang і Yoon для ранжування альтернатив за множиною критеріїв [17]. Ідея методу: кращою є альтернатива, що найближча до гіпотетичного ідеального розв'язку і найвіддаленіша від антиідеального. На першому кроці вихідну матрицю рішень нормалізують за кожним критерієм j :

$$r_{ij} = x_{ij} / \sqrt{\sum_i x_{ij}^2} \quad (1.3)$$

де x_{ij} - значення j -го критерію для i -ї альтернативи. Після зважування нормалізованих значень $v_{ij} = w_j \cdot r_{ij}$ визначають ідеальний розв'язок A^+ (найкращі значення за кожним критерієм) і антиідеальний A^- (найгірші), а потім обчислюють евклідові відстані S_i^+ і S_i^- від кожної альтернативи до A^+ та A^- відповідно. Підсумковий показник близькості до ідеалу:

$$C_i = S_i^- / (S_i^+ + S_i^-) \quad (1.4)$$

приймає значення від 0 до 1; альтернативи ранжують за спаданням C_i . Метод обрано тому, що він не вимагає монотонності функції корисності, стійкий до масштабних відмінностей між критеріями і підходить для порівняння обмеженого числа конфігурацій хмарної інфраструктури.

Ваговий вектор w для TOPSIS визначають методом аналізу ієрархій (АНП), запропонованим Saaty [18]. Відносну важливість критеріїв задають матрицею попарних порівнянь за шкалою 1–9, де 1 означає рівну важливість, а 9 - абсолютне переважання. Ваговий вектор апроксимується через нормоване геометричне середнє рядків матриці. Для перевірки узгодженості суджень обчислюють:

$$CI = (\lambda_{\max} - n) / (n - 1), \quad CR = CI / RI \quad (1.5)$$

де $\lambda_{\max}$ - найбільше власне значення матриці, n - її розмірність, RI - табличне значення випадкового індексу (табл. 1.4). Матрицю вважають достатньо узгодженою за умови $CR \leq 0,10$ [18].

Таблиця 1.4 - Значення випадкового індексу RI (Saaty, 1980)

п	3	4	5	6	7	8
RI	0,58	0,90	1,12	1,24	1,32	1,41

Джерело: [18]

Для оцінювання продуктивності хмарної інфраструктури та обґрунтування параметрів масштабування застосовано модель M/M/c [19]. У ній потік запитів моделюється як пуасонівський з інтенсивністю λ , час обслуговування - як експоненційно розподілений з параметром μ , а c - кількість паралельних вузлів. Коефіцієнт завантаження системи:

$$\rho = \lambda / (c \cdot \mu) \quad (1.6)$$

Умова стійкості - $\rho < 1$. Ймовірність очікування заявки в черзі визначають через функцію Ерланга $C(c, a)$, де $a = \lambda/\mu$ - пропоноване навантаження. Середній час очікування в черзі:

$$Wq = C(c, a) / (c \cdot \mu - \lambda) \quad (1.7)$$

У роботі модель використовують для розрахунку мінімально необхідної кількості інстансів c , за якої Wq задовольняє умовам SLA при прогнозованому навантаженні λ .

Відповідно до NIST SP 800-30 Rev. 1 ризик розглядають як функцію ймовірності реалізації загрози та величини можливого збитку [20]:

$$R = P \times I \quad (1.8)$$

де P - оцінювана ймовірність успішної реалізації загрози (визначається з урахуванням базового балу CVSS як характеристики вразливості та наявних засобів захисту), I - очікуваний збиток у грошовому вираженні (базується на галузевих даних [16]). Для сукупності загроз очікувані річні втрати:

$$E[L] = \sum_i P_i \cdot I_i \quad (1.9)$$

Для врахування невизначеності у значеннях P_i та I_i застосовують метод Монте-Карло: на кожній з $S \geq 10\,000$ ітерацій ймовірність кожної загрози вибирають із трикутного розподілу навколо оцінки CVSS, збиток - із логнормального розподілу

навколо галузевого значення, а сам факт реалізації інциденту розігрують випробуванням Бернуллі; сукупні втрати ітерації дорівнюють сумі збитків за загрозами, що справдилися. Результатом є емпіричний розподіл випадкової величини сукупних річних втрат L , на підставі якого оцінюють математичне сподівання $E[L]$, квантильні міри ризику (VaR , $CVaR$) та ймовірність перевищення критичного порогу втрат. Результати наведено в Додатку Г.

Оскільки методи TOPSIS і кількісної оцінки ризику дають результати на різних шкалах, для порівняння варіантів за обома аспектами одночасно введено інтегральний показник:

$$\hat{I}_i = \alpha \cdot \hat{E}_i + \beta \cdot \hat{S}_i, \quad \alpha + \beta = 1 \quad (1.10)$$

де $\hat{E}_i$ - нормалізована оцінка ефективності i -ї альтернативи (C_i за TOPSIS), $\hat{S}_i = 1 - \tilde{E}[L]_i$ - нормалізована оцінка безпеки (одиниця мінус нормалізовані очікувані втрати), α і β - вагові коефіцієнти, визначені через матрицю АНР.

Для порівняння варіантів за вартістю на горизонті 3–5 років використовують показник сукупної вартості володіння:

$$TCO = \sum_t \sum_j C_j(t) \quad (1.11)$$

де $j \in \{\text{обч, схов, мер, ліц, упр, без, компл, прост, прост.рес}\}$ - дев'ять категорій витрат (обчислення, зберігання, мережа, ліцензії, адміністрування, безпека, комплаєнс, вартість простоїв та надлишкових ресурсів), t - рік горизонту T . Прогноз витрат будується методом найменших квадратів за публічними даними цін провайдерів (2023–2025 рр.):

$$b = \Sigma(x_i - \bar{x})(y_i - \bar{y}) / \Sigma(x_i - \bar{x})^2, \quad \hat{C}(t) = a + b \cdot t \quad (1.12)$$

де b - нахил тренду, $a = \bar{y} - b \cdot \bar{x}$ - вільний член, x - рік спостереження, y - вартість у відповідний рік.

Відтак, методичний апарат складається з ланцюжка взаємопов'язаних методів: АНР визначає ваги $\rightarrow$ TOPSIS ранжує альтернативи за ефективністю $\rightarrow$ CVSS + NIST SP 800-30 + Монте-Карло кількісно оцінюють ризик $\rightarrow$ інтегральний показник (1.10) поєднує обидва виміри $\rightarrow$ М/М/с обґрунтовує параметри

масштабування $\rightarrow$ ТСО-модель оцінює повну вартість. Апробацію цього апарату на фактичних даних виконано в Розділі 2.

РОЗДІЛ 2

АПРОБАЦІЯ МЕТОДИКИ КОМПЛЕКСНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ

2.1. Постановка проблеми та системний аналіз об'єкта дослідження

Об'єктом дослідження є хмарна інфраструктура корпоративних інформаційних систем, тому аналіз починається не з окремої компанії, а з самого класу таких систем. Системний підхід вимагає розглянути хмарну інфраструктуру як взаємопов'язану сукупність підсистем, у межах яких і виникає проблема балансу між ефективністю та безпекою. Будь-яку корпоративну хмарну інфраструктуру можна декомпонувати на шість функціональних підсистем: обчислення, сховища даних, мережу, бізнес-сервіси, спостережуваність і інформаційну безпеку. Кожна підсистема має власні показники ефективності та власний профіль ризиків, а збій або недооцінка будь-якої з них впливає на систему загалом. Узагальнену декомпозицію наведено в табл. 2.1.

Таблиця 2.1 - Системна декомпозиція хмарної інфраструктури КІС

Підсистема	Показники ефективності	Основні ризики
Обчислення	Продуктивність, час відгуку, утилізація	Перевантаження, єдина точка відмови
Сховища даних	Пропускна здатність, латентність I/O	Втрата даних, відсутність реплікації
Мережа	Затримка, доступність каналів	DDoS, перехоплення трафіку
Бізнес-сервіси	Час відгуку застосунків, SLA	Простій сервісу, каскадні відмови
Спостережуваність	Повнота метрик, час виявлення	Пропущені інциденти, сліпі зони
Інформаційна безпека	Рівень захищеності, час реакції	Витік даних, помилки конфігурації, IAM

Джерело: складено автором за [1, 10]

Корпоративні інформаційні системи неоднаково залежать від хмарної інфраструктури, і ця залежність визначає, наскільки гостро для конкретної компанії стоїть проблема вибору. За рівнем хмарозалежності корпоративні КІС доцільно поділити на два класи. До класу А належать компанії, які фактично не можуть

працювати без хмари (cloud-native): їхня бізнес-модель побудована на еластичному масштабуванні та глобальній доступності, які власне обладнання забезпечити не здатне. До класу Б належать компанії з великим власним ІТ-сегментом, які технічно могли б працювати на власних дата-центрах (cloud-optional) і свідомо обирають гібридну або власну модель. Типологію з прикладами наведено на рис. 2.1.



Рисунок 2.1 - Типологія корпоративних КІС за рівнем хмарозалежності

Джерело: складено автором за [21–24]

Клас А ілюструє Netflix. Компанія завершила міграцію власних дата-центрів у хмару Amazon Web Services у 2016 році і відтоді працює повністю на ній. За оцінками галузевих аналітиків, у 2019 році рахунок Netflix за AWS становив близько 9,6 млн доларів на місяць, а сьогодні витрати на хмарні послуги сягають порядку 1 млрд доларів на рік, що при річному доході близько 39 млрд доларів (2024) відповідає приблизно 2,5 % доходу; офіційно компанія суму не розкриває [21]. До цього ж класу належать стримінгові, рекламні та SaaS-сервіси (Spotify, Snap, Shopify, Datadog), а також постачальники штучного інтелекту, чий обчислення фізично прив'язані до масштабних хмарних потужностей.

Постачальники штучного інтелекту - крайній випадок класу А, де хмарозалежність абсолютна. За оцінкою аналітичної групи Epoch AI, OpenAI у 2024 році витратила близько 7 млрд доларів на обчислення в Microsoft Azure: приблизно 5 млрд на тренування моделей і 2 млрд на inference [22]. Anthropic, за

умовами публічно відомих угод, отримала зобов'язання інвестицій і хмарних кредитів до 4 млрд доларів від Amazon, а також угоду з Google Cloud. Ці цифри засновані на непрямих оцінках і не підтверджені офіційною фінансовою звітністю, тому їх слід розглядати як орієнтовний порядок величини, а не точні дані. Втім, навіть на рівні порядку вони показують, що для таких компаній власна інфраструктура економічно й технічно неможлива - потрібні потужності існують лише у hyperscaler-ів.

Клас Б ілюструють два протилежні приклади. Walmart свідомо уникає AWS і тримає чутливі дані на власних серверах та в інфраструктурі конкурентів Amazon, оскільки сам конкурує з Amazon у роздрібній торгівлі; компанія розвиває власну мережу з понад 10 000 edge-вузлів у магазинах і складах, доповнюючи її хмарами Microsoft Azure та Google для окремих задач [23]. JPMorgan Chase, навпаки, активно мігрує в хмару, але в межах гібридної multi-cloud стратегії: технологічний бюджет банку у 2024 році сягнув близько 17 млрд доларів (проти $\approx 15,5$ млрд роком раніше), компанія скорочує мережу з 32 власних дата-центрів до приблизно 20 високоавтоматизованих і вже перевела близько 50 % застосунків і 70 % даних у приватну й публічну хмару, зберігаючи власні потужності для критичних навантажень [24]. Обидві компанії мають масштабний IT і фінансову спроможність утримувати власну інфраструктуру, тому хмара для них - вибір, а не необхідність. До цього ж класу належать й інші організації з великим власним IT-сегментом і значними технологічними бюджетами - Bank of America, AT&T, Volkswagen, - які з міркувань контролю над даними, регуляторних вимог або стратегічної незалежності зберігають критичну інфраструктуру у власних дата-центрах, виносячи в хмару лише окремі навантаження (рис. 2.1).

Малий бізнес становить третій, найменш дослідницьки цікавий полюс цього спектра, але він корисний як контрастний приклад реальної інфраструктури. Під час переддипломної практики у ТОВ «АГРОЗБУТ», B2B-компанії аграрного сектору, що надає в оренду нерухомість і техніку, IT-контур побудований за моделлю власних серверів (on-premise): корпоративні сервіси CRM, електронного документообігу та service desk GLPI працюють на Linux-хостах з PostgreSQL як

основною СУБД. У ході практики над цією інфраструктурою було розгорнуто повноцінний стек спостережуваності: Prometheus збирає метрики віртуальних машин, бази даних і резервного копіювання, Loki та Alloy агрегують логи, Grafana візуалізує стан через чотири дашборди (VM Health, PostgreSQL, Backup Health, GLPI Health), а Alertmanager надсилає сповіщення. Архітектуру цього контуру наведено на рис. 2.2, а фрагменти конфігурацій компонентів стека - у Додатку Д [25].



Рисунок 2.2 - Архітектура ІТ-контурів малого підприємства на прикладі ТОВ «АГРОЗБУТ»

Джерело: складено автором за матеріалами практики [25]

Цей приклад показує на малому масштабі те, що для компаній класів А і Б проявляється у кратно більших обсягах. Інфраструктура «АГРОЗБУТ» побудована на власних серверах, типова конфігурація для невеликого підприємства, де хмарна міграція ще тільки розглядається. Практика підтвердила закономірність, яка не залежить від масштабу: відсутність моніторингу прямо збільшує час простоїв і ймовірність пропущених інцидентів, а вибір між власними серверами та хмарою не має однозначно правильної відповіді без кількісного обґрунтування. Після впровадження observability-стека команда почала помічати проблеми до того, як

вони набували критичного характеру, що й поставило ширше питання про оптимальну модель інфраструктури.

Незалежно від класу, кожна компанія фактично обирає між шістьма варіантами інфраструктури: власні сервери (on-premise), публічна хмара на базі AWS, Microsoft Azure або Google Cloud Platform, приватна хмара та гібридна модель. Власні сервери дають максимальний контроль над даними і відсутність прив'язки до провайдера, але вимагають значних капітальних витрат і позбавляють еластичного масштабування. Публічна хмара знімає операційне навантаження і дає гнучкість, але створює залежність від провайдера, транскордонні ризики для даних і потенційно непередбачувані витрати. Приватна хмара поєднує ізоляцію з хмарною автоматизацією ціною високих початкових інвестицій. Гібридна модель є компромісом, але ускладнює архітектуру й управління безпекою.

Проблема полягає в тому, що жоден варіант не є очевидно кращим за всіма критеріями одночасно, і для різних класів компаній оптимум буде різним. Критерії до того ж конфліктують: виграш у вартості зазвичай супроводжується поступками в захищеності, а посилення контролю над даними коштує грошей і гнучкості. Прийняти обґрунтоване рішення без єдиної кількісної методики неможливо. Це підтверджує проблему, сформульовану у Вступі: відсутність інтегрованого підходу до оцінювання ефективності та безпеки хмарної інфраструктури КІС. Подальші підрозділи апробують такий підхід на фактичних даних реальних компаній обох класів.

2.2. Аналіз ефективності хмарної інфраструктури на основі фактичних і модельних даних

Поставивши проблему в підрозділі 2.1, переходимо до кількісної оцінки ефективності. Її виконано на узагальненому профілі великої корпоративної КІС за ланцюжком методів із підрозділу 1.4: метод аналізу ієрархій (АНР) визначає ваги критеріїв, модель масового обслуговування М/М/с обґрунтовує параметри масштабування, а ТСО-аналіз із трендовим прогнозом оцінює витрати на перспективу. Параметри профілю калібровано за фактичними даними реальних

компаній, насамперед Netflix і великих банків, наведеними в підрозділі 2.1, щоб розрахунки відображали реальний корпоративний масштаб, а не умовні величини.

Окремо варто пояснити природу вихідних даних. Детальні експлуатаційні та фінансові показники великих корпоративних хмарних інфраструктур здебільшого не є відкритими, тому в роботі використано узагальнений розрахунковий профіль корпоративної KIC. Його параметри сформовано на основі відкритих SLA та цінових даних хмарних провайдерів, галузевих аналітичних звітів за 2023-2025 роки й матеріалів переддипломної практики. Тому подальші розрахунки слід розглядати як апробацію методики на репрезентативному сценарії, а не як аудит внутрішньої інфраструктури конкретної компанії; за інших вихідних припущень числові значення можуть змінюватися, проте загальна логіка порівняння альтернатив залишається сталою.

Порівнюються шість альтернатив із підрозділу 2.1: власні сервери (on-premise), публічна хмара AWS, Azure та GCP, приватна хмара і гібридна модель. Ефективність оцінюють за п'ятьма критеріями: доступністю, затримкою (latency), сукупною вартістю володіння, масштабованістю та зрілістю вбудованих засобів безпеки. Перші чотири описують власне ефективність, п'ятий пов'язує цей підрозділ з аналізом ризиків у 2.3.

Перш ніж переходити до розрахунків, варто пояснити технічну природу різниці між альтернативами, бо саме архітектурні рішення визначають, які значення набувають показники ефективності. Доступність корпоративного сервісу залежить не від окремого сервера, а від схеми розгортання. Розгортання в одній зоні доступності (single availability zone) дає за SLA провайдерів близько 99,5-99,9 %, тоді як дублювання навантаження у двох і більше зонах (multi-AZ) піднімає гарантію до 99,99 % [6, 26, 27]. Механізм простий: за правилом добутку ймовірностей відмов незалежне резервування різко зменшує сумарний ризик одночасного збою. Платою за це є приблизно подвоєння витрат на обчислення, оскільки інстанси доводиться тримати в кількох зонах [6]. Власні сервери такого резервування без значних капітальних вкладень забезпечити не можуть, що й закладає їхнє відставання за доступністю.

Затримку для глобальних сервісів знижують мережі доставки контенту (CDN) та периферійні (edge) вузли: кешування ближче до користувача скорочує мережеву затримку з сотень мілісекунд до десятків, особливо для міжконтинентальних запитів (орієнтовно з понад 200 мс до менш як 50 мс), хоча конкретний вигаш залежить від географії й операторів. Масштабованість забезпечує автоматичне масштабування (auto-scaling): сервіси на кшталт AWS Auto Scaling, Azure VMSS і GCP MIG додають інстанси при зростанні навантаження й вимикають їх при спаді. За оцінками FinOps-практиків, перехід від статичного провіженінгу під піковий рівень до еластичного масштабування дає економію 30-50 % на обчисленнях для добово-варіативних навантажень, тоді як надмірне резервування породжує 20-50 % непродуктивних витрат [28, 29]. Саме auto-scaling робить кількість обчислювальних вузлів динамічною величиною, що далі моделюється в М/М/с як параметр s .

Критерії мають різну важливість, тому їхні ваги визначено методом аналізу ієрархій. Для великої корпорації, яка працює з регульованими даними й несе репутаційні ризики, безпека й безперебійність важать найбільше, масштабованість і вартість - помірно, а чиста швидкодія - найменше. Матрицю попарних порівнянь за шкалою Saaty наведено в табл. 2.2.

Таблиця 2.2 - Матриця попарних порівнянь критеріїв ефективності (АНР)

Критерій	Дост.	Latency	Варт.	Масшт.	Безп.
Доступність	1	3	2	2	1
Latency	1/3	1	1/2	1/2	1/4
Вартість (TCO)	1/2	2	1	1	1/2
Масштабованість	1/2	2	1	1	1/2
Безпека	1	4	2	2	1

Джерело: складено автором

Ваговий вектор обчислено через нормоване геометричне середнє рядків матриці (підрозділ 1.4). Отримано такі ваги: безпека - 0,312, доступність - 0,294, вартість і масштабованість - по 0,156, latency - 0,083. Узгодженість перевірено за формулою (1.5): найбільше власне значення $\lambda_{\max} = 5,010$, індекс узгодженості $CI = 0,0025$, а за $RI = 1,12$ коефіцієнт узгодженості $CR = 0,002$. Оскільки $CR \leq 0,10$,

матриця узгоджена, і ваги придатні для ранжування альтернатив у підрозділі 2.4. Розподіл ваг кількісно підтверджує, що для корпоративного профілю безпека й доступність разом визначають майже дві третини інтегральної оцінки ефективності. Повну матрицю попарних порівнянь і проміжні розрахунки вагового вектора наведено в Додатку Б.

Наступний крок - перевірка продуктивності за моделлю масового обслуговування. Параметри взято на рівні корпоративного масштабу: інтенсивність потоку $\lambda = 20\,000$ запитів за секунду, що за порядком величини відповідає піковому навантаженню продакшн-API Netflix, який ще у 2011 році обробляв понад мільярд запитів на добу [30], тож для сучасних систем це консервативна нижня оцінка; продуктивність одного обчислювального вузла прийнято на рівні $\mu = 2500$ запитів за секунду як типове значення для API-інстанса середнього класу (параметр моделі, що калібрується під конкретну систему). Пропоноване навантаження становить $a = \lambda/\mu = 8$ Ерлангів, тобто для стійкої роботи потрібно щонайменше дев'ять вузлів. Розрахунок коефіцієнта завантаження ρ за формулою (1.6) та середнього часу очікування W_q за формулою (1.7) для діапазону c наведено на рис. 2.3.

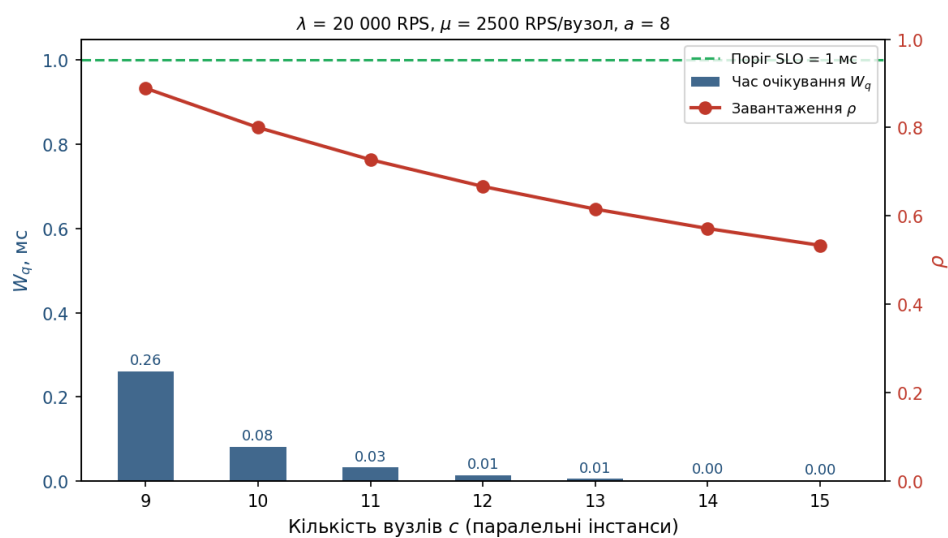


Рисунок 2.3 - Залежність часу очікування W_q і завантаження ρ від кількості вузлів

c

Джерело: розраховано автором за моделлю $M/M/c$

За дев'яти вузлів система стійка, але працює на межі: завантаження $\rho = 0,89$ і будь-який сплеск трафіку швидко вичерпує резерв. Додавання вузлів різко покращує показники - вже за одинадцяти вузлів завантаження падає до 0,73, а час очікування не перевищує сотих часток мілісекунди. Для критичних інтерактивних сервісів раціональним є діапазон 11-12 вузлів, що дає одночасно низьку затримку й запас потужності на пікові сплески. Принципова перевага хмарних альтернатив тут у тому, що завдяки auto-scaling кількість вузлів змінюється автоматично під фактичний попит: у години спаду система тримає мінімум, у пік - нарощує потужність. Для власних серверів з фіксованою й закладається із запасом наперед, тому вони або простоюють, або не витримують піків.

Третій складник аналізу - вартість. Вхідні цінові дані зібрано за публічними прайс-листами провайдерів за 2024-2025 роки для зіставних віртуальних машин конфігурації 4 vCPU та 16 ГБ оперативної пам'яті (Linux, регіон US-East), а також за офіційними угодами про рівень послуг. Враховано й доступні моделі знижок: зарезервовані потужності на 1-3 роки дають до 72 % економії, переривані інстанси - до 90 %. Зведені фактичні характеристики альтернатив подано в табл. 2.3, а повні вихідні дані щодо цін і SLA провайдерів за 2023-2025 роки - у Додатку Е.

Таблиця 2.3 - Порівняння варіантів інфраструктури за фактичними даними (2024-2025)

Параметр	AWS	Azure	GCP	Власні / приватна
Тип VM (4 vCPU / 16 ГБ)	m6a.xlarge	D4as v5	e2-standard-4	власне обладн.
Ціна on-demand, USD/год	0,17-0,20	$\approx 0,17$	0,13-0,14	CAPEX
SLA (одиначний)	99,5 %	99,9 %	99,9 %	немає гарантій
SLA (кілька зон)	99,99 %	99,99 %	99,99 %	залежить від резерв.
Знижка reserved (1-3 р.)	до 72 %	до 72 %	до 70 %	-
Частка ринку (кін. 2024)	≈ 30 %	≈ 21 %	≈ 12 %	-

Джерело: складено автором за [6, 9, 26, 27, 31]

Важливо розділяти два різні явища: питому ціну обчислень і сукупну вартість володіння. Питома ціна за період майже не змінилася - за індексом цін BCG у 2023 році середня вартість хмарних послуг трьох провайдерів зросла лише приблизно на 0,3 % з окремими підвищеннями до 2 % у певних регіонах, а базові віртуальні машини залишалися стабільними [32]. Натомість сукупна вартість володіння корпоративною інфраструктурою зростає значно швидше, бо складається не лише з compute: до неї входять сховища, мережевий трафік, керовані сервіси баз даних, ліцензії, засоби безпеки та оплата персоналу. У реальних кейсах структура витрат показова - за даними, оприлюдненими Capital One на AWS re:Invent 2023, близько 40 % хмарного рахунку компанії припадає на платформу даних і аналітики, а не на транзакційні обчислення [29]. Зростання обсягу даних і кількості сервісів і є головним драйвером збільшення TCO.

Щоб оцінити цю динаміку, застосовано трендову модель (1.12) до річних витрат узагальненого корпоративного профілю за 2023-2025 роки, відкаліброваних за фактичними ціновими даними провайдерів та оприлюдненими витратами компаній з підрозділу 2.1. Результат і прогноз на 2026-2028 роки наведено на рис. 2.4.

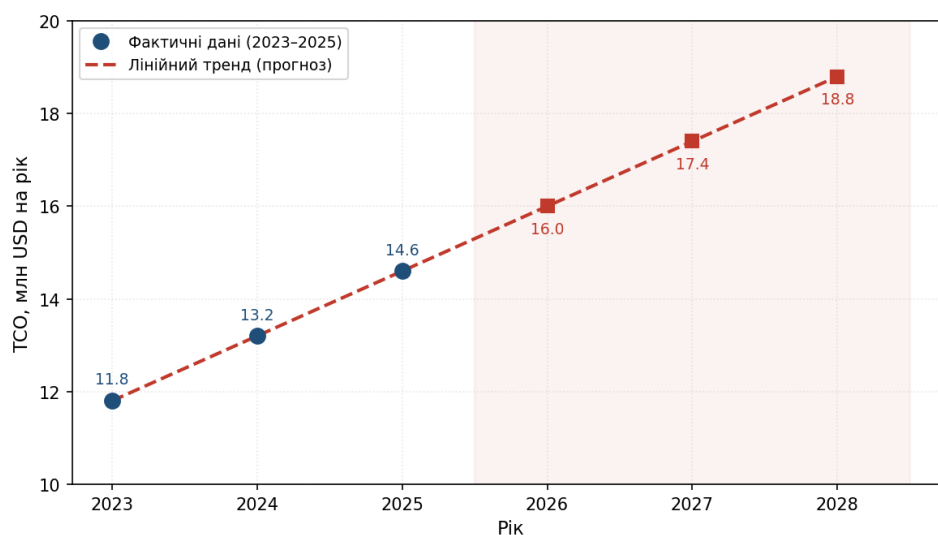


Рисунок 2.4 - Динаміка та прогноз сукупної вартості володіння (TCO)

Джерело: розраховано автором методом найменших квадратів

Лінійний тренд має нахил близько 1,4 млн доларів на рік, що відповідає зростанню витрат приблизно на 10-11 % щороку. За такої динаміки сукупна

вартість володіння зростає з 14,6 млн доларів у 2025 році до близько 18,8 млн у 2028-му. Прогноз показує, що навіть за стабільних питомих цін витрати корпорації на хмарну інфраструктуру помітно збільшуватимуться через зростання обсягів, тому вибір конфігурації має враховувати як поточну, так і перспективну вартість, а також потенціал оптимізації через auto-scaling і зарезервовані потужності. Водночас слід пам'ятати про обмеження прогнозу: тренд побудовано лише за трьома річними спостереженнями, тому отримані значення характеризують напрям і порядок величини, а не точні майбутні витрати.

Зведені результати дають проміжний висновок щодо ефективності. За питоמוю ціною обчислень найвигіднішим є Google Cloud Platform, за зрілістю екосистеми та часткою ринку - Amazon Web Services, за можливостями масштабування - публічні хмари загалом, тоді як власні сервери програють за гарантіями доступності та еластичністю. Проте жоден варіант не є найкращим за всіма критеріями одночасно, а отриманих оцінок ефективності недостатньо для остаточного рішення: вони не враховують захищеності. Тому порівняння доповнено кількісною оцінкою ризиків безпеки (підрозділ 2.3).

2.3. Кількісна оцінка ризиків безпеки хмарної інфраструктури

Вигідніші за вартістю й продуктивністю альтернативи ще не означають найкращі: оцінка ефективності навмисно лишила осторонь захищеність. Цей підрозділ доповнює картину кількісною оцінкою ризиків безпеки за апаратом із підрозділу 1.4: ймовірність реалізації загрози визначається на основі оцінок CVSS, збиток - на базі галузевих даних, добуток ризику обчислюється за формулою (1.8), а невизначеність моделюється методом Монте-Карло. Результат - очікувані річні втрати та їх розподіл, який далі інтегрується з ефективністю в підрозділі 2.4.

Для оцінки відібрано шість загроз із переліку CSA «Top Threats to Cloud Computing 2024» (табл. 1.3), найрелевантніших для хмарної KIC: помилки конфігурації, слабке управління доступами (IAM), незахищені інтерфейси та API, витік і незахищеність даних, обмежена спостережуваність, захоплення акаунтів. Перш ніж присвоювати їм числові оцінки, варто розібрати технічний механізм цих

загроз, бо саме він визначає, наскільки висока ймовірність реалізації і наскільки серйозний потенційний збиток.

Найпоказовіший приклад - ланцюг із помилки конфігурації, надмірних прав IAM і незахищеного інтерфейсу, який реалізувався у витоку даних Capital One 2019 року. Технічно атака відбулася так: зловмисник використав уразливість типу підробки запиту на боці сервера (Server-Side Request Forgery, SSRF) проти неправильно налаштованого міжмережевого екрана веб-застосунків (WAF), розгорнутого на інстансі AWS EC2. SSRF дозволила надіслати запит до сервісу метаданих інстансу (Instance Metadata Service, версія IMDSv1), який без автентифікації повернув тимчасові облікові дані IAM-ролі, прив'язаної до WAF. Ця роль мала надмірні права, тому отриманих облікових даних вистачило для доступу приблизно до 700 сегментів сховища S3 і викачування персональних даних близько 106 мільйонів клієнтів [33]. Інцидент коштував банку 80 мільйонів доларів штрафу від регулятора OCC у 2020 році, 190 мільйонів урегулювання колективних позовів у 2022 році та сукупно понад 300 мільйонів доларів прямих витрат [33].

Цей випадок ілюструє ключову тезу підрозділу 1.3: основний центр ризику в хмарі змістився на бік замовника. Жодна з ланок не була вразливістю самого AWS - усі вони були помилками конфігурації та управління доступами. Технічні контрзаходи теж відомі: версія IMDSv2 вимагає сесійних токенів і блокує SSRF-доступ до метаданих, принцип найменших привілеїв обмежив би права ролі, а шифрування й сегментація S3 зменшили б збиток. Що цей клас атак залишається актуальним, підтверджує статистика: за звітом SonicWall, у 2024 році кількість SSRF-атак зросла на 452 % порівняно з 2023 роком [34]. У 2025 році в Azure OpenAI було виявлено критичну SSRF-вразливість (CVE-2025-53767, CWE-918) з ескалацією привілеїв, хоча офіційний бал CVSS у базі NVD на момент аналізу ще не зафіксовано [15].

Для кількісної оцінки ймовірності використано систему CVSS (Common Vulnerability Scoring System) - відкритий стандарт оцінювання серйозності вразливостей, яким керує організація FIRST [35]. У версії 3.1 базова оцінка формується з двох наборів метрик: експлуатованості (вектор атаки AV, складність

АС, потрібні привілеї PR, взаємодія користувача UI, область дії S) та впливу на конфіденційність, цілісність і доступність (C, I, A). Комбінація цих метрик дає вектор і числовий бал від 0 до 10, що інтерпретується за п'ятьма рівнями: None (0), Low (0,1-3,9), Medium (4,0-6,9), High (7,0-8,9), Critical (9,0-10,0) [35]. Версія 4.0, опублікована у 2023 році, уточнює модель: групу Temporal замінено на Threat, додано групу Supplemental, область дії S замінено на роздільний вплив на вразливу й суміжні системи (VC/VI/VA та SC/SI/SA), а замість єдиної формули введено модель MacroVector [15]. Для цього дослідження за основу взято поширенішу версію 3.1, оскільки переважна частина записів у базі NVD оцінена саме нею.

Тут важливе розмежування: CVSS оцінює серйозність вразливості, а не ризик у конкретному середовищі, тому базовий бал не можна напрямку прирівнювати до ймовірності. Для переходу до ймовірності Р бал нормалізовано до діапазону [0, 1] діленням на 10 і скориговано на коефіцієнт наявних засобів захисту: що зріліші контролі (моніторинг, MFA, шифрування), то нижча фактична ймовірність реалізації. Збиток I оцінено на основі звіту IBM «Cost of a Data Breach 2025», за яким середня глобальна вартість витоку даних становить 4,44 мільйона доларів, а для фінансового сектору - близько 6-7 мільйонів [16]. Структура цього збитку показова: виявлення та ескалація - 1,47 мільйона (33 %), втрата бізнесу - 1,38 мільйона (31 %), реагування після інциденту - близько 1,2 мільйона (27 %), сповіщення - 0,39 мільйона (9 %) [16]. Підставивши оцінки Р та I у формулу (1.8), отримуємо ризик кожної загрози; сума за всіма загрозами за формулою (1.9) дає очікувані річні втрати. Результати наведено в табл. 2.4.

Таблиця 2.4 - Матриця ризиків безпеки хмарної інфраструктури

Загроза (CSA 2024)	CVSS	Р	I, млн USD	$R = P \times I$, млн
Помилки конфігурації	9,1	0,77	4,9	3,79
Слабкий IAM / надмірні права	8,2	0,62	4,4	2,71
Незахищені інтерфейси та API	8,6	0,69	3,8	2,61
Витік / незахищеність даних	7,5	0,53	5,2	2,73

Загроза (CSA 2024)	CVSS	P	I, млн USD	$R = P \times I$, млн
Обмежена спостережуваність	6,5	0,59	2,6	1,52
Захоплення акаунтів	8,0	0,52	4,1	2,13
Очікувані річні втрати $E[L] = \Sigma R$				15,49

Джерело: розраховано автором за [10, 16, 35]. Значення R обчислено за точними (незаокругленими) P та I ; у стовпцях P , I , R наведено заокруглені до двох знаків величини, тому добуток заокруглених P і I може незначно відрізнятися від показаного R .

Детермінований розрахунок дає очікувані річні втрати $E[L] = 15,49$ мільйона доларів, причому найбільший внесок робить найперша загроза рейтингу CSA - помилки конфігурації (3,79 мільйона), що повністю узгоджується з висновком підрозділу 1.3. Проте точкова оцінка приховує розкид: і ймовірність, і збиток є випадковими величинами. Щоб оцінити невизначеність, проведено імітаційне моделювання методом Монте-Карло на 10 000 ітерацій. Ймовірність кожної загрози моделювалася трикутним розподілом навколо оцінки CVSS, збиток - логнормальним розподілом навколо галузевого значення, а факт реалізації інциденту - випробуванням Бернуллі. Розподіл сукупних річних втрат наведено на рис. 2.5; код і повні результати симуляції винесено в Додаток Г.

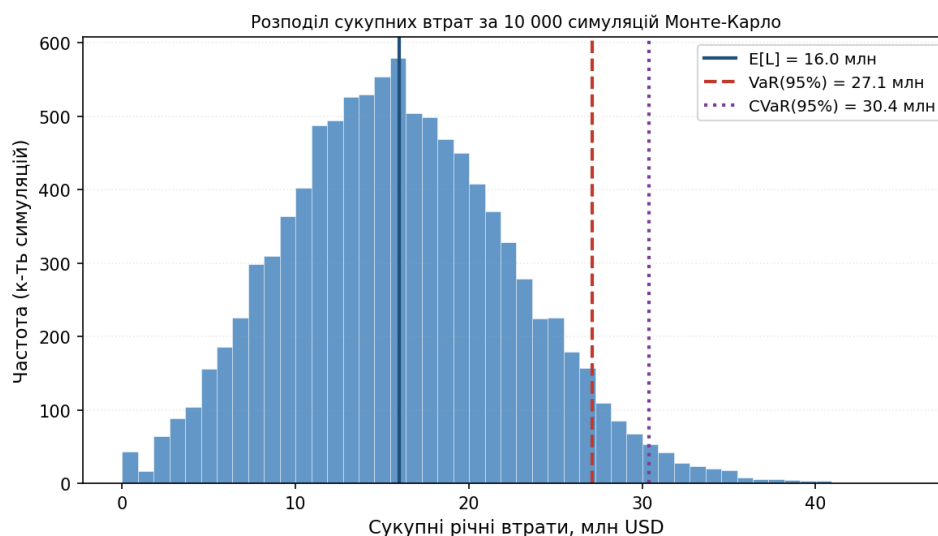


Рисунок 2.5 - Розподіл сукупних річних втрат за результатами моделювання Монте-Карло

Джерело: розраховано автором, 10 000 ітерацій

Симуляція дала середні очікувані втрати близько 16,0 мільйона доларів, що підтверджує детермінований розрахунок. Водночас розподіл має виражений правий хвіст: вартісна міра ризику VaR на рівні довіри 95 % становить 27,1 мільйона, а умовна VaR (CVaR, середнє у хвості за межею VaR) - 30,4 мільйона доларів. Це означає, що у найгірших 5 % сценаріїв річні втрати перевищать 27 мільйонів, а в середньому по цих сценаріях сягнуть 30 мільйонів. Імовірність того, що сукупні втрати перевищать 10 мільйонів доларів, становить близько 81 %. Такий хвіст принципово важливий для рішення: орієнтація лише на середнє занижує реальний ризик, тоді як саме хвостові сценарії визначають вимоги до резервування й страхування. Підкреслимо, що отримані ймовірності описують консервативний профіль, у якому ключові заходи захисту ще не впроваджені або незрілі; ефект від їх упровадження кількісно оцінено в підрозділі 3.3.

З аналізу впливають конкретні технічні пріоритети. Оскільки найбільші ризики формують помилки конфігурації, слабкий IAM і незахищені API, найбільший ефект дають заходи саме на цих напрямках: інструменти управління станом безпеки конфігурацій (CSPM) для автоматичного виявлення відхилень, примусове застосування принципу найменших привілеїв та багатофакторної автентифікації, шлюзи API з обмеженням частоти запитів і контролем автентифікації, а також наскрізне шифрування даних. Особливе місце посідає загроза обмеженої спостережуваності: хоча її прямий ризик найнижчий (1,52 мільйона), брак моніторингу збільшує час виявлення інших інцидентів, а отже, опосередковано підвищує їхній збиток - що підтверджує доцільність впровадження observability-стека, описаного в підрозділі 2.1.

Отримані оцінки ризику дають другий вимір для порівняння альтернатив - захищеність, виражену кількісно через очікувані втрати та хвостові міри ризику. Отже, у дослідженні з'явилися обидва виміри - ефективність (підрозділ 2.2) і безпека (підрозділ 2.3); їх інтегрування в єдиний показник та остаточне ранжування шести альтернатив завершують апробацію методики.

2.4. Інтегральне оцінювання «ефективність-безпека» і підтвердження проблеми

Підрозділи 2.2 і 2.3 оцінили альтернативи окремо за ефективністю та безпекою. Проте ці оцінки виражені в різних одиницях - відсотках доступності, мілісекундах, мільйонах доларів витрат і ризику - і безпосередньо не порівнювані. Щоб обрати найкращий варіант, потрібно звести різнорідні показники в єдину систему. Для цього застосовано метод TOPSIS (формули 1.3-1.4), а підсумкове рішення сформовано через інтегральний показник (формула 1.10). Розрахунок нижче показує, що оцінка лише за одним аспектом дає нестійке рішення і що суперечність, сформульовану у Вступі, знімає лише інтегральний підхід.

Для порівняння сформовано матрицю рішень із шести альтернатив і п'яти критеріїв: чотири характеризують ефективність (доступність, затримка, сукупна вартість володіння, масштабованість), а п'ятий - безпеку через очікувані річні втрати $E[L]$ з підрозділу 2.3. Значення критеріїв узяті з фактичних даних підрозділів 2.2-2.3: доступність - за SLA провайдерів, затримка й масштабованість - за архітектурними можливостями, TCO - за прогнозом, ризик - за матрицею загроз. Матрицю наведено в табл. 2.5.

Таблиця 2.5 - Зведена матриця рішень для порівняння альтернатив

Альтернатива	Дост.,%	Lat.,мс	TCO,млн	Масшт.	Ризик,млн
AWS	99,99	35	14,6	9,5	15,5
Azure	99,99	38	14,2	9,0	16,0
GCP	99,99	33	13,0	9,0	16,5
Приватна хмара	99,95	28	16,0	6,5	12,0
Гібридна	99,99	30	15,0	8,0	13,5
Власні сервери	99,50	25	13,5	4,0	18,0

Джерело: складено автором за даними підрозділів 2.2-2.3

Пояснимо походження значень матриці. Доступність відповідає офіційним SLA для багатозонного розгортання, а для власних серверів - типовій оцінці конфігурації без георезервування. Затримку взято за архітектурними характеристиками варіантів з підрозділу 2.2: публічні хмари виграють завдяки CDN і периферійним вузлам, власні сервери - завдяки фізичній близькості до

основної аудиторії. ТСО відповідає прогнозу з рис. 2.4 з поправкою на модель розгортання. Масштабованість оцінено експертно за десятибальною шкалою: 9-9,5 бала відповідає зрілому автоматичному масштабуванню публічних хмар, 8 - гібридній моделі, 6,5 - обмеженій еластичності приватної хмари, 4 - фіксованій потужності власних серверів. Значення ризику для кожної альтернативи отримано перерахунком очікуваних втрат за методикою підрозділу 2.3 зі скоригованими коефіцієнтами захищеності: для приватної хмари та гібридної моделі нижчими є ймовірності загроз, пов'язаних з мультиорендою та публічними інтерфейсами, тоді як для власних серверів вищу вагу мають обмежена спостережуваність і брак зрілих вбудованих засобів захисту. Прийняті коефіцієнти захищеності та похідні значення ризику наведено в табл. Г.1 Додатку Г. Отже, матриця поєднує фактичні дані (SLA, ціни) з експертно-модельними оцінками, що є звичайною практикою багатокритеріального аналізу.

Критерії різноспрямовані, і це принциповий момент для коректного застосування TOPSIS. Доступність і масштабованість є критеріями вигоди (benefit): що більше значення, то краще. Натомість затримка, вартість і ризик є критеріями витрат (cost): що менше значення, то краще. Якщо не врахувати цю різницю, метод дасть хибний результат, бо він шукає альтернативу, найближчу до ідеалу. Тому на етапі визначення ідеального розв'язку A^+ для критеріїв вигоди беруть максимум, а для критеріїв витрат - мінімум; для антиідеального A^- - навпаки. Вихідну матрицю спочатку нормалізують векторно за формулою (1.3), що зводить усі критерії до безрозмірного вигляду в діапазоні від 0 до 1 і робить їх порівнюваними попри різні одиниці виміру.

Після нормалізації кожен критерій зважують за його вагомістю. Ваги взято безпосередньо з вагового вектора методу аналізу ієрархій (підрозділ 2.2, Додаток Б): доступність - 0,294, безпека (ризик) - 0,312, вартість - 0,156, масштабованість - 0,156, затримка - 0,083. Безпека й доступність разом дають близько 60 % ваги, що відповідає профілю корпоративної КІС. Далі за формулою (1.4) обчислюють евклідові відстані кожної альтернативи до ідеального та антиідеального розв'язків

і коефіцієнт близькості C_i . Результати наведено в табл. 2.6, а покрокові проміжні розрахунки - у Додатку В.

Таблиця 2.6 - Результати ранжування альтернатив методом TOPSIS

Альтернатива	S^+	S^-	C_i	Ранг
Гібридна	0,0202	0,0502	0,713	1
Приватна хмара	0,0278	0,0547	0,663	2
AWS	0,0317	0,0494	0,609	3
Azure	0,0365	0,0443	0,548	4
GCP	0,0384	0,0445	0,537	5
Власні сервери	0,0666	0,0177	0,210	6

Джерело: розраховано автором

За базових ваг найкращою альтернативою є гібридна модель ($C_i = 0,713$), за нею - приватна хмара (0,663). Власні сервери посідають останнє місце (0,210), що очікувано: вони програють і за доступністю, і за масштабованістю, і за ризиком. Проте цей рейтинг отримано за конкретного балансу ваг, і постає питання, наскільки він стійкий до зміни пріоритетів. Щоб це перевірити, проведено аналіз чутливості за інтегральним показником (1.10): $\hat{I}_i = \alpha \cdot \hat{E}_i + \beta \cdot \hat{S}_i$, де $\hat{E}_i$ - нормалізована оцінка ефективності, $\hat{S}_i$ - нормалізована оцінка безпеки, а ваги α і β ($\alpha + \beta = 1$) задають баланс між аспектами. Варіюючи α від 0 (пріоритет лише безпеки) до 1 (пріоритет лише ефективності), отримуємо, як змінюється інтегральна оцінка кожної альтернативи. Результат наведено на рис. 2.6.

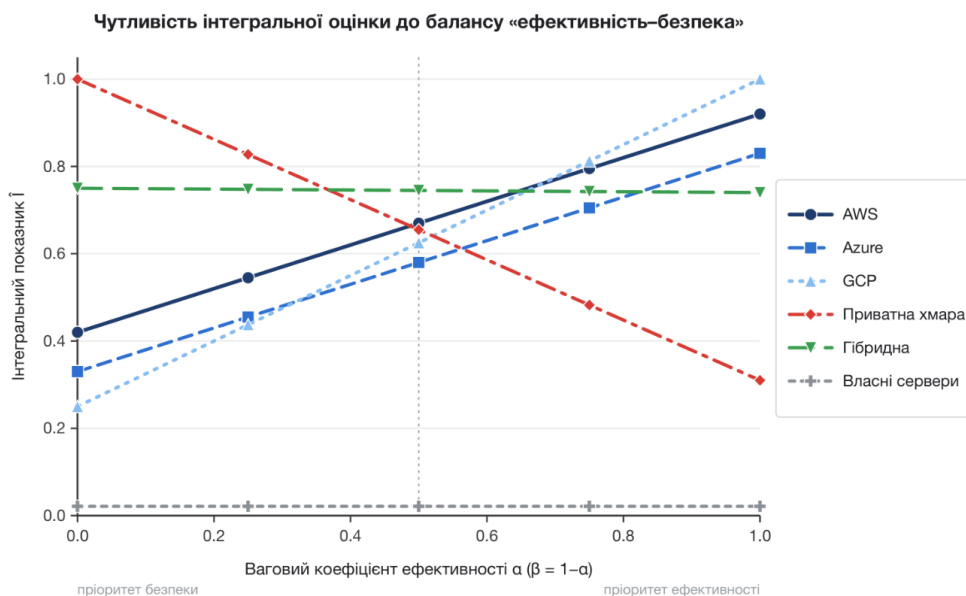


Рисунок 2.6 - Чутливість інтегральної оцінки до балансу «ефективність-безпека»

Джерело: розраховано автором

Графік чутливості наочно демонструє головний висновок дослідження. При пріоритеті ефективності ($\alpha \rightarrow 1$) лідирує Google Cloud Platform як найдешевший і найшвидший варіант. При пріоритеті безпеки ($\alpha \rightarrow 0$) перше місце посідає приватна хмара з найнижчим ризиком. Тобто залежно від того, який аспект вважати важливішим, оптимальна альтернатива змінюється - і це саме та суперечність, яку неможливо розв'язати, оцінюючи аспекти окремо. Натомість гібридна модель не виграє в жодній крайній точці, але стабільно тримає високу оцінку в центральному діапазоні приблизно $0,37 \leq \alpha \leq 0,64$, де обидва аспекти збалансовані; за межами цього діапазону лідерство переходить до приватної хмари (за пріоритету безпеки) або до GCP та AWS (за пріоритету ефективності). Тому за інтегрального підходу з рівними або близькими вагами найкращим рішенням стає саме гібридна модель. Нульова лінія власних серверів на рис. 2.6 - наслідок min-max-нормалізації інтегрального показника: ця альтернатива найгірша за обома нормалізованими вимірами, тому її оцінка дорівнює нулю за побудовою, що означає останнє місце в ранжуванні, а не нульову корисність. Підсумкове ранжування за єдиним методом TOPSIS, у якому безпеку враховано як п'ятий критерій з вагою 0,312 (а не як окремий доданок інтегрального показника), наведено на рис. 2.7.

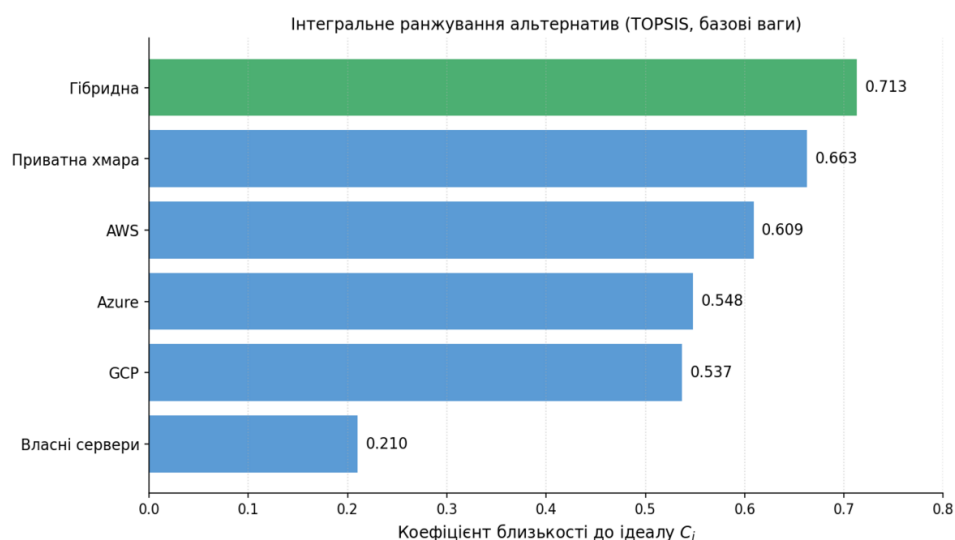


Рисунок 2.7 - Інтегральне ранжування альтернатив за методом TOPSIS

Джерело: розраховано автором

Зіставлення трьох підходів до ранжування фактологічно підтверджує проблему дослідження. Якщо оцінювати альтернативи лише за ефективністю, перше місце посідає GCP; якщо лише за безпекою - приватна хмара; а за інтегрального підходу - гібридна модель. Три різні методи дають три різні оптимуми. Це означає, що однобічна оцінка є неповною і здатна призвести до протилежних рішень, кожне з яких формально обґрунтоване. Лише інтегральний показник, що поєднує обидва аспекти із заданими вагами, дає стійкий і відтворюваний результат. Це прямо підтверджує тезу, сформульовану у Вступі: за відсутності інтегрованого підходу до оцінювання ефективності та безпеки вибір конфігурації хмарної інфраструктури КІС лишається необґрунтованим.

При цьому отриманий рейтинг не є універсальним рейтингом хмарних провайдерів чи моделей розгортання: він відображає результат для заданого профілю корпоративної КІС, обраного набору критеріїв і вагових коефіцієнтів. За зміни ваг або пріоритетів підприємства порядок альтернатив може змінюватися, що й показав аналіз чутливості. Невелика різниця між гібридною ($C_i = 0,713$) та приватною (0,663) моделями додатково свідчить, що в центральному діапазоні ваг ці варіанти близькі, а остаточний вибір залежить від конкретних пріоритетів організації.

Практичний висновок залежить від класу компанії: для класу А (cloud-native) виправдане збільшення ваги ефективності, що піднімає в рейтингу публічні хмари з їх зрілою еластичністю, а для класу Б (cloud-optional) - збільшення ваги безпеки, що підносить приватну та гібридну моделі. Компромісом, стійким до зміни пріоритетів, залишається гібридна модель. Перетворення цього висновку на конкретний алгоритм вибору й налаштування конфігурації під профіль компанії виконано в Розділі 3.

РОЗДІЛ 3

РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ, ОПТИМІЗАЦІЇ ТА ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ

3.1. Рекомендації щодо вибору й конфігурації хмарної інфраструктури

Розділ 2 довів проблему й дав інструмент її розв'язання - інтегральну методику оцінювання. Цей розділ перетворює результати оцінювання на практичні рекомендації: алгоритм вибору конфігурації, оптимізаційну модель витрат і програму заходів безпеки з кількісною оцінкою їх ефективності. Усі рекомендації спираються на розрахунки підрозділів 2.2-2.4 і не вводять припущень поза ними.

Вибір конфігурації хмарної інфраструктури доцільно будувати як послідовність рішень, що залежать від класу компанії та її пріоритетів. Аналіз чутливості в підрозділі 2.4 показав, що оптимальна альтернатива зміщується разом із балансом «ефективність-безпека», тому єдиної універсальної відповіді немає - є алгоритм, який веде до обґрунтованого рішення для конкретного профілю. Цей алгоритм подано на рис. 3.1.

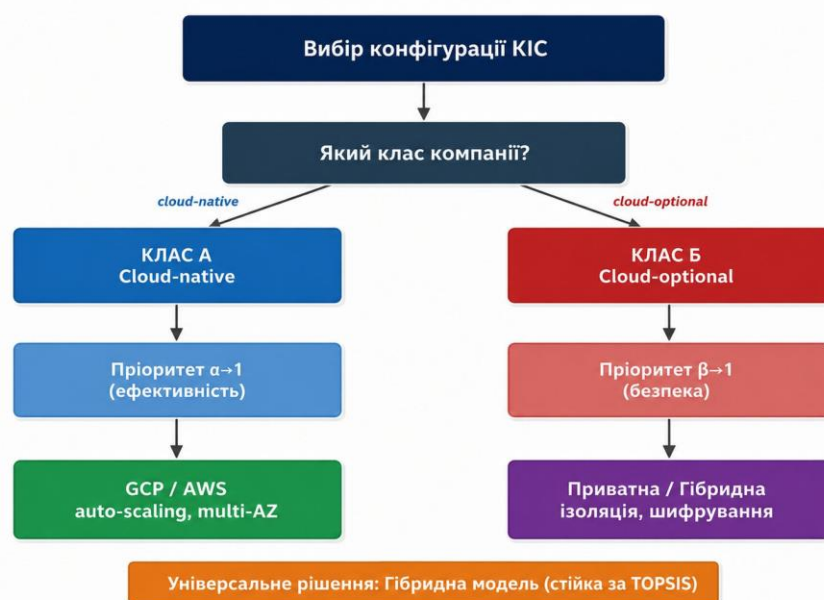


Рисунок 3.1 - Алгоритм вибору конфігурації хмарної інфраструктури

Джерело: складено автором

Алгоритм починається з визначення класу компанії за типологією підрозділу 2.1. Для класу А (cloud-native), де бізнес критично залежить від

еластичності та глобальної доступності, пріоритет зміщується до ефективності ($\alpha \rightarrow 1$), і алгоритм веде до публічних хмар - насамперед GCP і AWS з їх зрілим автоматичним масштабуванням і розгортанням multi-AZ. Для класу Б (cloud-optional) з підвищеними вимогами до контролю даних і регуляторними обмеженнями пріоритет зміщується до безпеки ($\beta \rightarrow 1$), що підносить приватну та гібридну моделі. За збалансованих пріоритетів універсальним рішенням, стійким до зміни ваг, залишається гібридна модель, що посіла перше місце в інтегральному ранжуванні (підрозділ 2.4).

Вибір моделі розгортання - лише перший рівень рішення. На другому рівні конфігурують окремі підсистеми згідно з системною декомпозицією (табл. 2.1), причому конкретні налаштування залежать від класу компанії. Зведені рекомендації наведено в табл. 3.1.

Таблиця 3.1 - Рекомендації щодо конфігурації підсистем за класами компаній

Підсистема	Клас А (cloud-native)	Клас Б (cloud-optional)
Обчислення	Auto-scaling, multi-AZ, контейнери	Гібрид: критичне on-premise, піки в хмарі
Сховища даних	Об'єктне сховище, авто-реплікація	Приватне сховище для чутливих даних
Мережа	CDN, глобальні точки присутності	Приватні канали, контроль трафіку
Безпека / IAM	Хмарний IAM, MFA, least privilege	Гібридний IAM, посилений контроль
Спостережуваність	Хмарний моніторинг + трасування	Власний стек (Prometheus, Loki, Grafana)

Джерело: складено автором за результатами підрозділів 2.1-2.4

3.2. Оптимізаційна модель сукупної вартості володіння

Прогноз у підрозділі 2.2 показав, що сукупна вартість володіння зростатиме навіть за стабільних питомих цін. Тому окрім вибору моделі важлива оптимізація витрат. Базовий принцип оптимізації в хмарі полягає в тому, щоб узгодити модель оплати з характером навантаження: стабільне базове навантаження вигідно

покривати зарезервованими потужностями, змінні піки - оплатою за фактом, а стійкі до переривань задачі - переривними інстансами. За даними FinOps-практики, зарезервовані потужності дають 30-72 % економії відносно on-demand, переривні (spot) інстанси - 70-90 %, а оптимізація розміру ресурсів і вимикання непродуктивних середовищ - ще десятки відсотків [36, 37]. При цьому, за звітом Flexera 2025, близько 27 % витрат на IaaS і PaaS у середньому марнується через надлишкове резервування й простій ресурсів [38].

Формалізуємо задачу оптимізації. Нехай загальне обчислювальне навантаження розподілено на три частини: baseline (стабільна частка b_s), пікова (b_p) і стійка до переривань (b_β), причому $b_s + b_p + b_\beta = 1$. Тоді оптимальна сукупна вартість обчислень мінімізується вибором моделі оплати для кожної частини:

$$C_{\text{opt}} = C_0 \cdot [b_s(1 - d_r) + b_p + b_\beta(1 - d_s)] \rightarrow \min, \quad (3.1)$$

де C_0 - вартість за повної оплати on-demand, d_r - знижка зарезервованих потужностей, d_s - знижка переривних інстансів. Обмеженнями виступають вимоги до доступності (частку критичних сервісів не можна переносити на spot) і до ризику (рівень захищеності не повинен падати нижче прийнятного за підрозділом 2.3). Для типового корпоративного профілю з розподілом $b_s = 0,60$, $b_p = 0,25$, $b_\beta = 0,15$ і консервативними знижками $d_r = 0,60$, $d_s = 0,75$ модель дає економію близько 47 % лише за рахунок міксу моделей оплати, а з урахуванням оптимізації розміру ресурсів - до 58 %. Декомпозицію цієї економії наведено на рис. 3.2.

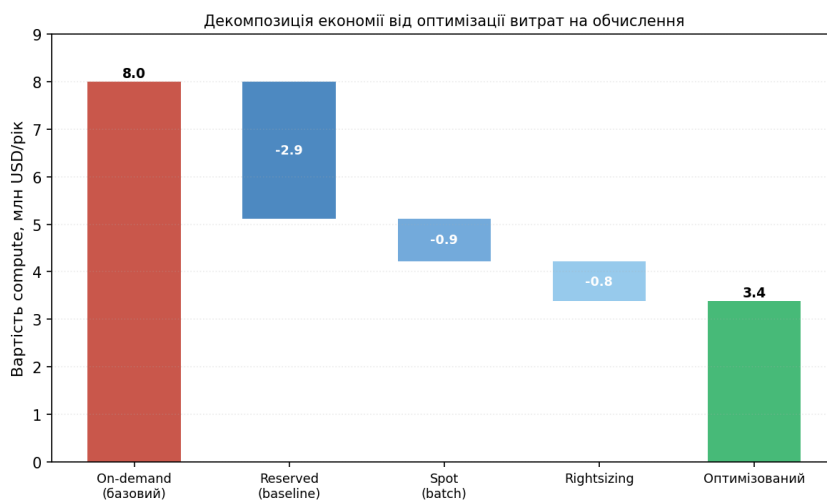


Рисунок 3.2 - Декомпозиція економії від оптимізації витрат на обчислення

Джерело: розраховано автором за моделлю (3.1)

Найбільший внесок дає перенесення базового навантаження на зарезервовані потужності (економія близько 2,9 мільйона доларів на рік для розглянутого профілю), далі - переривні інстанси для batch-задач і оптимізація розміру ресурсів. Застосувавши цю оптимізацію до прогнозу ТСО з підрозділу 2.2, отримуємо два сценарії розвитку витрат, наведені на рис. 3.3.

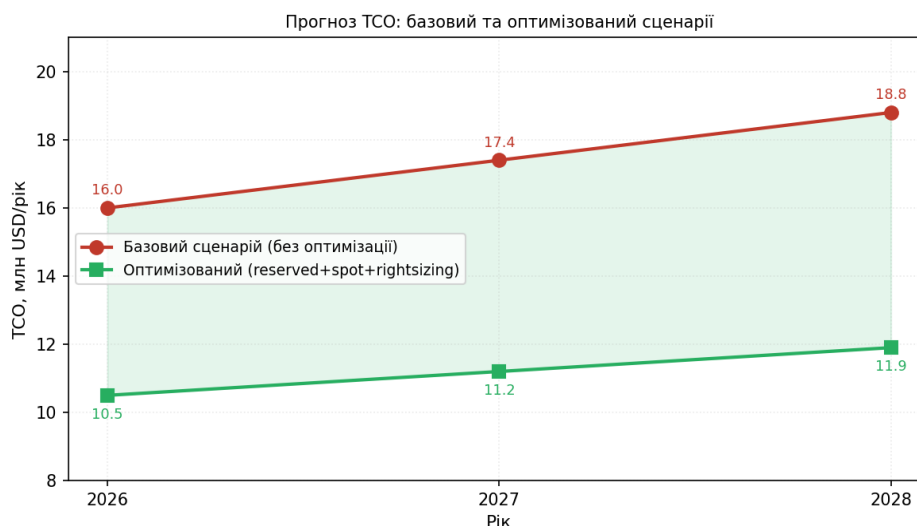


Рисунок 3.3 - Прогноз ТСО: базовий та оптимізований сценарії

Джерело: розраховано автором

Без оптимізації сукупна вартість володіння зростає до 18,8 мільйона доларів у 2028 році, тоді як оптимізований сценарій утримує її на рівні близько 11,9 мільйона. Різниця у майже 7 мільйонів доларів на рік є прямим економічним ефектом запропонованої моделі. Ця економія досягається без зниження доступності чи безпеки: критичні сервіси залишаються на надійних потужностях, а оптимізації підлягають лише ті навантаження, для яких це безпечно. Слід зауважити, що зниження ТСО перевищує економію лише на обчисленнях із рис. 3.2, оскільки оптимізація охоплює не тільки compute, а й суміжні статті витрат - зберігання, мережевий трафік і керовані сервіси, до яких застосовано аналогічний принцип узгодження тарифікації з характером навантаження. Конкретний розподіл моделей оплати для розглянутого профілю наведено в табл. 3.2.

Таблиця 3.2 - Оптимальний розподіл моделей оплати за типами навантаження

Тип навантаження	Частка	Модель оплати	Знижка
Базове (стабільне)	60 %	Reserved (1-3 р.)	до 72 %
Пікове (змінне)	25 %	On-demand + auto-scaling	-
Batch (стійке до перерв.)	15 %	Spot / preemptible	до 90 %

Джерело: складено автором за [36, 37]

3.3. Заходи підвищення безпеки та спостережуваності й оцінка їх ефективності

Кількісна оцінка ризиків у підрозділі 2.3 показала, що очікувані річні втрати від загроз безпеки становлять близько 15,5 мільйона доларів, а найбільший внесок дають помилки конфігурації, слабе управління доступами та незахищені API. Цей підрозділ пропонує програму заходів проти цих загроз і кількісно оцінює її ефективність через перерахунок очікуваних втрат.

Кожна загроза адресується конкретним технічним контролем. Помилки конфігурації усуваються інструментами управління станом безпеки (CSPM), які переводять виявлення відхилень із періодичних ручних аудитів у режим безперервного контролю й перевіряють конфігурації проти бенчмарків CIS та стандартів ISO/IEC 27017. Слабе управління доступами адресується примусовим застосуванням принципу найменших привілеїв і багатофакторної автентифікації (MFA). Тут варто бути обережним з оцінкою ефективності: за телеметрією Microsoft, увімкнення MFA блокує до 99,9 % автоматизованих атак на акаунти [39], проте незалежні експерти зазначають, що проти таргетованого фішингу й атак типу MFA-fatigue реальне зниження ризику ближче до 30-50 %, особливо при слабких каналах на кшталт SMS. Тому в розрахунках узято консервативні оцінки ефективності. Незахищені API захищаються шлюзами з обмеженням частоти запитів і контролем автентифікації, витік даних - наскрізним шифруванням, а обмежена спостережуваність - власне впровадженням observability-стека.

Ефективність програми оцінено кількісно. Кожен захід знижує ймовірність реалізації відповідної загрози на консервативно оцінений відсоток, після чого перераховано ризик $R = P \times I$ та сумарні очікувані втрати $E[L]$. Внесок кожного заходу у зниження ризику наведено на рис. 3.4.

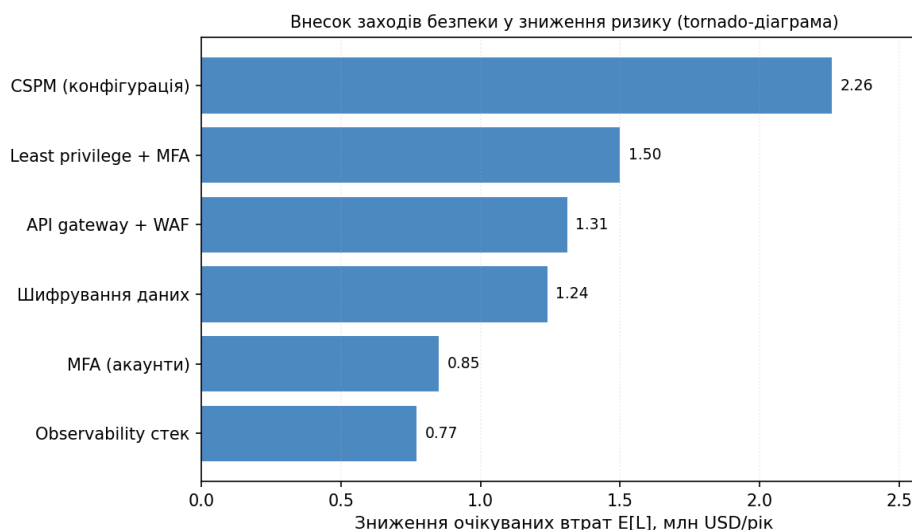


Рисунок 3.4 - Внесок заходів безпеки у зниження очікуваних втрат

Джерело: розраховано автором

Найбільший ефект дають інструменти CSPM проти помилок конфігурації (зниження очікуваних втрат на 2,26 мільйона доларів на рік), що логічно, адже саме ця загроза має найвищий ризик за підрозділом 2.3. Сукупно програма заходів знижує очікувані річні втрати з 15,5 до 7,6 мільйона доларів, тобто приблизно на 51 %. Зведену оцінку ефективності наведено в табл. 3.3.

Таблиця 3.3 - Оцінка ефективності заходів безпеки

Захід	Загроза	Зниження Р	$\Delta E[L]$, млн
CSPM	Конфігурація	60 %	2,26
Least privilege + MFA	IAM	55 %	1,50
API gateway + WAF	API	50 %	1,31
Наскрізне шифрування	Дані	45 %	1,24
MFA (акаунти)	Акаунти	40 %	0,85
Observability стек	Спостережув	50 %	0,77

Захід	Загроза	Зниження Р	$\Delta E[L]$, млн
Разом ($E[L]$: 15,5 → 7,6)			7,94

Джерело: розраховано автором за [10, 16, 39]. Підсумкове $\Delta E[L]$ обчислено за точними (незаокругленими) значеннями, тому може незначно відрізнятися від суми заокруглених величин у стовпці.

Сумарне зниження очікуваних втрат становить близько 7,9 мільйона доларів на рік (з 15,5 до 7,6 мільйона залишкового ризику) і є кількісним обґрунтуванням доцільності інвестицій у безпеку: навіть з урахуванням вартості впровадження й підтримки перелічених інструментів економічний ефект від запобігання інцидентам значно перевищує витрати. Окремо слід наголосити на ролі спостережуваності. Хоча прямий внесок observability-стека у зниження ризику найменший (0,77 мільйона), його справжня цінність опосередкована: моніторинг скорочує час виявлення інших інцидентів, а отже, зменшує їхній збиток. Це підтвердив і досвід практики у ТОВ «АГРОЗБУТ» (підрозділ 2.1), де впровадження стека Prometheus, Loki та Grafana дозволило виявляти проблеми до набуття ними критичного характеру. Конфігурації цього стека, придатні для відтворення в реальному середовищі, наведено в Додатку Д.

Підсумуємо. Розділ 1 дав теоретичну базу й методичний апарат, Розділ 2 апробував його й кількісно довів проблему, а Розділ 3 перетворив результати на практичні рекомендації: алгоритм вибору конфігурації, оптимізаційну модель витрат з економічним ефектом до 58 % на обчислювальних ресурсах (близько 37 % сукупної вартості володіння) та програму заходів безпеки, що знижує очікувані втрати на 51 %. Розроблена методика й рекомендації разом утворюють інтегрований інструмент обґрунтування рішень щодо хмарної інфраструктури корпоративних інформаційних систем, що відповідає меті роботи.

ВИСНОВКИ

У кваліфікаційній роботі розв'язано актуальне завдання - розроблено інтегровану методику оцінювання ефективності та безпеки хмарної інфраструктури корпоративних інформаційних систем, яка дозволяє обґрунтовано обирати конфігурацію під конкретний профіль компанії. Мету роботи досягнуто, а за результатами дослідження сформульовано такі висновки.

1. Досліджено сутність хмарної інфраструктури корпоративних інформаційних систем. Систематизовано три сервісні моделі (IaaS, PaaS, SaaS) та чотири моделі розгортання за NIST (публічна, приватна, громадська, гібридна); власні сервери (on-premise) розглянуто як окрему альтернативу порівняння, що не є хмарною моделлю розгортання. Описано також модель спільної відповідальності, яка визначає, що відповідальність за дані та управління доступами завжди залишається за замовником незалежно від сервісної моделі. Це формує теоретичну основу для подальшого аналізу ризиків.

2. Систематизовано показники ефективності хмарної інфраструктури та підходи до її оцінювання. Виокремлено ключові критерії - доступність, затримку, сукупну вартість володіння та масштабованість - і обґрунтовано доцільність їх кількісного зіставлення методами багатокритеріального аналізу, оскільки жоден окремий показник не дає повної картини.

3. Проаналізовано моделі загроз, ризики та стандарти безпеки хмарних систем. На основі переліку загроз CSA «Top Threats to Cloud Computing 2024» та стандартів серії ISO/IEC 27017, 27018 і NIST встановлено, що основний центр ризику в хмарі змістився на бік замовника, а провідними загрозами є помилки конфігурації, слабе управління доступами та незахищені інтерфейси.

4. Обґрунтовано методичний апарат комплексного оцінювання. Для оцінки ваг критеріїв обрано метод аналізу ієрархій (АНР), для аналізу продуктивності - модель масового обслуговування М/М/с, для оцінки ризиків - підхід $R = P \times I$ з імітаційним моделюванням Монте-Карло на основі балів CVSS, для інтегрального ранжування - метод TOPSIS, а для прогнозу витрат - модель сукупної вартості володіння з трендовим аналізом.

5. Проведено системний аналіз об'єкта дослідження й апробовано методики на фактичних і відкаліброваних за ними модельних даних за 2023-2025 роки. Запропоновано типологію корпоративних KIC за рівнем хмарозалежності з поділом на класи А (cloud-native) та Б (cloud-optional), підтверджену прикладами Netflix, OpenAI, Walmart і JPMorgan. Апробація АНР дала узгоджений ваговий вектор ($CR = 0,002$) з домінуванням безпеки (0,31) та доступності (0,29); модель М/М/с для навантаження 20 000 запитів за секунду показала потребу щонайменше в дев'яти обчислювальних вузлах; трендовий аналіз спрогнозував зростання сукупної вартості володіння до 18,8 мільйона доларів у 2028 році.

6. Виконано кількісне оцінювання ефективності й безпеки та інтегральне ранжування. Кількісна оцінка ризиків дала очікувані річні втрати $E[L] = 15,5$ мільйона доларів за вартісної міри ризику $VaR(95\%) = 27,1$ мільйона, причому найбільший внесок робить загроза помилок конфігурації, що підтверджено технічним розбором інциденту Capital One. Інтегральне ранжування методом TOPSIS показало ключовий результат дослідження: оцінювання лише за ефективністю визначає лідером GCP, лише за безпекою - приватну хмару, а інтегральний підхід - гібридну модель. Три підходи дають три різні оптимуми, що фактологічно підтверджує проблему: без інтегрованого оцінювання вибір конфігурації лишається необґрунтованим.

7. Розроблено практичні рекомендації та оптимізаційну модель. Запропоновано алгоритм вибору конфігурації за класом компанії та балансом пріоритетів, оптимізаційну модель сукупної вартості володіння, що за рахунок узгодження моделей оплати з характером навантаження дає економію до 58 % на обчислювальних ресурсах (близько 37 % сукупної вартості володіння), та програму заходів безпеки, яка знижує очікувані річні втрати з 15,5 до 7,6 мільйона доларів, тобто приблизно на 51 %.

Сукупність отриманих результатів становить інтегрований інструмент обґрунтування рішень щодо хмарної інфраструктури корпоративних інформаційних систем. Практична значущість роботи полягає в тому, що запропонована методика придатна для застосування підприємствами будь-якого

масштабу - від великих cloud-native компаній до малих підприємств на кшталт об'єкта практики ТОВ «АГРОЗБУТ» - для кількісного обґрунтування вибору, оптимізації витрат і підвищення захищеності хмарної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mell P., Grance T. The NIST Definition of Cloud Computing : NIST Special Publication 800-145. Gaithersburg : National Institute of Standards and Technology, 2011. 7 p. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>.
2. ISO/IEC 22123-1:2023. Information technology - Cloud computing - Part 1: Vocabulary. Geneva : ISO/IEC, 2023.
3. ISO/IEC 22123-2:2023. Information technology - Cloud computing - Part 2: Concepts. Geneva : ISO/IEC, 2023.
4. ISO/IEC 17788:2014. Information technology - Cloud computing - Overview and vocabulary. Geneva : ISO/IEC, 2014. (скасовано 2023, замінено ISO/IEC 22123-1:2023, ISO/IEC 22123-2:2023).
5. ISO/IEC 19086-1:2016. Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts. Geneva : ISO/IEC, 2016.
6. Amazon Compute Service Level Agreement. Amazon Web Services, 2024. URL: <https://aws.amazon.com/compute/sla/>.
7. Top Public Cloud Service Providers: How They Compare. TechTarget, 2025. URL: <https://www.techtarget.com/searchcloudcomputing/tip/Top-public-cloud-providers-A-brief-comparison>.
8. Major Cloud Outages of 2025. IncidentHub, 2025. URL: <https://blog.incidenthub.cloud/major-cloud-outages-2025>.
9. Understanding the Real Cost of Cloud VMs: AWS EC2 vs. Azure VMs vs. GCE. CloudZero, 2026. URL: <https://www.cloudzero.com/blog/aws-ec2-vs-azure/>.
10. Top Threats to Cloud Computing 2024. Cloud Security Alliance, 2024. URL: <https://cloudsecurityalliance.org/research/topics/top-threats>.
11. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. URL: <https://www.enisa.europa.eu/publications>.

12. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva : ISO/IEC, 2022.
13. ISO/IEC 27017:2015. Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Geneva : ISO/IEC, 2015.
14. ISO/IEC 27018:2019. Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Geneva : ISO/IEC, 2019.
15. Common Vulnerability Scoring System v4.0: Specification Document. FIRST.org, 2023. URL: <https://www.first.org/cvss/v4-0/specification-document>.
16. Cost of a Data Breach Report 2025. IBM Security, Ponemon Institute, 2025. URL: <https://www.ibm.com/reports/data-breach>.
17. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. New York : Springer-Verlag, 1981. 259 p. (Lecture Notes in Economics and Mathematical Systems; Vol. 186).
18. Saaty T.L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York : McGraw-Hill, 1980. 287 p.
19. Kleinrock L. Queueing Systems, Vol. 1: Theory. New York : Wiley, 1975. 417 p.
20. Ross R. Guide for Conducting Risk Assessments : NIST Special Publication 800-30 Rev. 1. Gaithersburg : NIST, 2012. URL: <https://doi.org/10.6028/NIST.SP.800-30r1>.
21. Inside Netflix's AWS Strategy: Cost Efficiency At Scale. CloudZero, 2026. URL: <https://www.cloudzero.com/blog/netflix-aws/>.
22. Most of OpenAI's 2024 Compute Went to Experiments. Epoch AI, 2025. URL: <https://epoch.ai/data-insights/openai-compute-spend>.
23. Walmart's Hybrid Data Storage Strategy De-emphasizes Public Cloud. DirectLTX, 2022. URL: <https://www.directltx.com/direct-ltx-news/walmarts-hybrid-strategy-deemphasizes-public-cloud>.

24. JPMorgan Chase to Host 75% of its Data in the Cloud in 2024. Data Center Dynamics, 2024. URL: <https://www.datacenterdynamics.com/en/news/jpmorgan-chase-to-host-75-of-its-data-in-the-cloud-in-2024/>.
25. Щоденник переддипломної практики у ТОВ «АГРОЗБУТ», лютий - березень 2026 р.
26. Compute Engine Service Level Agreement (SLA). Google Cloud, 2025. URL: <https://cloud.google.com/compute/sla>.
27. Service Level Agreements (SLA) for Online Services. Microsoft, 2026. URL: <https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services>.
28. The State of FinOps 2025 Report. FinOps Foundation, 2025. URL: <https://data.finops.org/2025-report/>.
29. AWS re:Invent 2023 - FinOps Tips for Optimizing Your Cloud Infrastructure and Data Costs (COP224). Amazon Web Services, 2023. URL: https://www.youtube.com/watch?v=u_tHthuyQ-Q.
30. Making the Netflix API More Resilient. Netflix Technology Blog, 2011. URL: <https://netflixtechblog.com/making-the-netflix-api-more-resilient-a8ec62159c2d>.
31. Cloud Market Jumped to \$330 Billion in 2024 - GenAI is Now Driving Half of the Growth. Synergy Research Group, 2025. URL: <https://www.srgresearch.com/articles/cloud-market-jumped-to-330-billion-in-2024-genai-is-now-driving-half-of-the-growth>.
32. Cloud Cover: Cloud Prices Rise as the Era of Generative AI Dawns. Boston Consulting Group, 2023. URL: <https://www.bcg.com/publications/2023/cloud-prices-surge-with-rise-of-genai>.
33. Capital One Breach 2019: 106M Records. CloudSkope, 2024. URL: <https://www.cloudskope.com/breaches/capital-one-breach-2019>.
34. SonicWall 2025 Annual Cyber Threat Report. SonicWall, 2025. URL: <https://www.sonicwall.com/threat-report>.

35. CVSS v3.1 Specification Document. Forum of Incident Response and Security Teams (FIRST), 2019. URL: <https://www.first.org/cvss/v3-1/specification-document>.
36. EC2 Reserved Instances Pricing. Amazon Web Services, 2025. URL: <https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>.
37. Cloud Cost Optimization Strategies for Modern FinOps Teams. ProsperOps, 2025. URL: <https://www.prosperops.com/blog/cloud-cost-optimization-strategies/>.
38. Flexera 2025 State of the Cloud Report. Flexera, 2025. URL: <https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-state-of-the-cloud-report/>.
39. Microsoft: 99.9% of Compromised Accounts Did Not Use Multi-Factor Authentication. ZDNet, 2020. URL: <https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/>.

Таблиця А.1 - Матриця розподілу відповідальності за моделями IaaS / PaaS / SaaS

Модель спільної відповідальності (shared responsibility) визначає, хто - провайдер чи замовник - відповідає за кожен рівень хмарної інфраструктури залежно від сервісної моделі. Знак «П» означає зону відповідальності провайдера, «З» - замовника, «П/З» - спільну відповідальність. Таблиця доповнює виклад підрозділу 1.1.

Рівень / Сервісна модель	IaaS	PaaS	SaaS
Дані та контент	З	З	З
Управління доступами (IAM)	З	З	З
Застосунки	З	З/П	П
Середовище виконання	З	П	П
Операційна система	З	П	П
Віртуалізація / гіпервізор	П	П	П
Сервери та сховища	П	П	П
Мережа та ЦОД	П	П	П

Джерело: складено автором за [1, 10]

Закономірність очевидна: що ближче модель до SaaS, то більше рівнів переходить до зони провайдера, проте відповідальність за дані та управління доступами завжди залишається за замовником. Саме на цих двох рівнях зосереджена більшість інцидентів, проаналізованих у підрозділі 2.3.

Таблиця Б.1 - Зведена система показників з ваговими коефіцієнтами та розрахунок АНР

Наведено зведену систему критеріїв багатокритеріального аналізу з ваговими коефіцієнтами та повний розрахунок вагового вектора за матрицею попарних порівнянь (табл. 2.2) методом аналізу ієрархій.

Критерій	Тип	Вага (ефект.)	Вага (інтегр.)
Доступність	вигода	0,294	0,294
Затримка (latency)	витрати	0,083	0,083
Вартість (ТСО)	витрати	0,156	0,156
Масштабованість	вигода	0,156	0,156
Безпека / ризик	витрати	0,312	0,312

Джерело: складено автором

Крок 1. Геометричне середнє кожного рядка матриці А розміром 5×5 . Крок 2. Нормалізація вагів. Крок 3. Перевірка узгодженості через $\lambda_{\max}$, $CI = (\lambda_{\max} - n) / (n - 1)$ та $CR = CI / RI$, де $RI = 1,12$ для $n = 5$.

```
import numpy as np
A = np.array([
    [1, 3, 2, 2, 1 ], # Доступність
    [1/3, 1, 1/2, 1/2, 1/4], # Latency
    [1/2, 2, 1, 1, 1/2], # Вартість
    [1/2, 2, 1, 1, 1/2], # Масштабованість
    [1, 4, 2, 2, 1 ], # Безпека
])
n = 5
gm = np.prod(A, axis=1) ** (1/n)
w = gm / gm.sum()
lmax = ((A @ w) / w).mean()
CI = (lmax - n) / (n - 1)
CR = CI / 1.12
print(np.round(w, 3)) # [0.294 0.083 0.156 0.156 0.312]
print(round(CR, 3)) # 0.002
```

Результат: $\lambda_{\max} = 5,010$, $CI = 0,0025$, $CR = 0,002 \leq 0,10$, отже матриця суджень узгоджена.

Покрокові розрахунки ранжування методом TOPSIS

Проміжні етапи розрахунку, результати якого узагальнено в табл. 2.6. Вихідні дані - матриця рішень (табл. 2.5) і вектор ваг $w = (0,294; 0,083; 0,156; 0,156; 0,312)$.

Крок 1. Векторна нормалізація за формулою (1.3). Крок 2. Зважування на ваги критеріїв. Крок 3. Визначення ідеалу A^+ (максимум для критеріїв вигоди, мінімум для критеріїв витрат) та антиідеалу A^- . Крок 4. Евклідові відстані S^+ і S^- . Крок 5. Коефіцієнт близькості $C_i = S^- / (S^+ + S^-)$.

```
import numpy as np
X = np.array([
    [99.99, 35, 14.6, 9.5, 15.5], # AWS
    [99.99, 38, 14.2, 9.0, 16.0], # Azure
    [99.99, 33, 13.0, 9.0, 16.5], # GCP
    [99.95, 28, 16.0, 6.5, 12.0], # Приватна хмара
    [99.99, 30, 15.0, 8.0, 13.5], # Гібридна
    [99.50, 25, 13.5, 4.0, 18.0], # Власні сервери
])
w = np.array([0.294, 0.083, 0.156, 0.156, 0.312])
types = ['benefit', 'cost', 'cost', 'benefit', 'cost']
norm = X / np.sqrt((X**2).sum(axis=0))
V = norm * w
Aplus = np.where([t=='benefit' for t in types], V.max(0), V.min(0))
Aminus = np.where([t=='benefit' for t in types], V.min(0), V.max(0))
Sp = np.sqrt(((V - Aplus)**2).sum(1))
Sm = np.sqrt(((V - Aminus)**2).sum(1))
C = Sm / (Sp + Sm)
print(np.round(C, 3)) # [0.609 0.548 0.537 0.663 0.713 0.210]
```

Підсумкові коефіцієнти близькості: гібридна модель - 0,713; приватна хмара - 0,663; AWS - 0,609; Azure - 0,548; GCP - 0,537; власні сервери - 0,210.

Код і результати імітаційного моделювання ризиків (Монте-Карло)

Моделювання виконано мовою Python із бібліотекою NumPy. Ймовірність кожної загрози задано трикутним розподілом навколо нормалізованої оцінки CVSS, збиток - логнормальним розподілом навколо галузевого значення IBM, факт реалізації інциденту - випробуванням Бернуллі. Обсяг вибірки - 10 000 ітерацій. Зауважимо, що параметр логнормального розподілу задано так, що галузеве значення IBM відповідає медіані збитку; через асиметрію логнормального закону математичне сподівання збитку приблизно на 8 % перевищує медіану, тому імітаційна оцінка $E[L]$ (близько 16,0 млн) дещо вища за детерміновану (15,49 млн) - ця різниця є очікуваною й закладеною в модель свідомо як консервативніша.

```
import numpy as np
np.random.seed(42)
threats = [
    (9.1, 0.85, 4.9), # помилки конфігурації
    (8.2, 0.75, 4.4), # слабкий IAM
    (8.6, 0.80, 3.8), # незахищені API
    (7.5, 0.70, 5.2), # витік даних
    (6.5, 0.90, 2.6), # обмежена спостережуваність
    (8.0, 0.65, 4.1), # захоплення акаунтів
]
N = 10000
total = np.zeros(N)
for cvss, cf, I in threats:
    Pm = cvss / 10 * cf
    Psim = np.random.triangular(max(0, Pm*0.7), Pm, min(1, Pm*1.15), N)
    Isim = np.random.lognormal(np.log(I), 0.4, N)
    occur = (np.random.random(N) < Psim).astype(float)
    total += occur * Isim
var95 = np.percentile(total, 95)
print(total.mean(), var95, total[total>=var95].mean())
```

Результати (10 000 ітерацій): $E[L] = 16,0$ млн USD; $VaR(95\%) = 27,1$ млн USD; $CVaR(95\%) = 30,4$ млн USD; $VaR(99\%) = 32,5$ млн USD; імовірність перевищення 10 млн USD - близько 81 %. Гістограму наведено на рис. 2.5.

Перерахунок очікуваних втрат за альтернативами (стовпець «Ризик» у табл. 2.5) виконано множенням базового рівня $E[L]$ консервативного публічно-хмарного профілю (15,49 млн USD, прийнятого за еталон AWS) на коефіцієнт захищеності k , що відображає зрілість вбудованих засобів контролю та ступінь публічної експозиції відповідної моделі розгортання. Значення k нижчі за одиницю для приватної та гібридної моделей (менша мультиоренда й експозиція публічних

інтерфейсів) і вищі для власних серверів (слабша спостережуваність і брак зрілих вбудованих контролів). Прийняті коефіцієнти та похідні значення ризику наведено в табл. Г.1.

Таблиця Г.1 - Коефіцієнти захищеності та похідний ризик за альтернативами

Альтернатива	Базовий E[L], млн	Коефіцієнт k	Ризик, млн
AWS (еталон)	15,49	1,00	15,5
Azure	15,49	1,03	16,0
GCP	15,49	1,06	16,5
Приватна хмара	15,49	0,78	12,0
Гібридна	15,49	0,87	13,5
Власні сервери	15,49	1,16	18,0

Джерело: розраховано автором. Коефіцієнти k - експертно-модельні оцінки за зрілістю вбудованих засобів захисту та рівнем публічної експозиції моделі розгортання.

Фрагменти конфігурацій спостережуваності (Prometheus + Loki + Grafana)

Ключові фрагменти конфігурацій стека спостережуваності, розгорнутого на інфраструктурі ТОВ «АГРОЗБУТ» під час практики (рис. 2.2). Подано у скороченому вигляді.

Д.1. Збір метрик Prometheus (prometheus.yml).

```
global:
  scrape_interval: 15s
  evaluation_interval: 15s
alerting:
  alertmanagers:
    - static_configs:
      - targets: ['localhost:9093']
scrape_configs:
  - job_name: 'node'
    static_configs:
      - targets: ['localhost:9100']
  - job_name: 'postgres'
    static_configs:
      - targets: ['localhost:9187']
  - job_name: 'backup'
    static_configs:
      - targets: ['localhost:9101']
```

Д.2. Правило сповіщення Alertmanager (alert_rules.yml).

```
groups:
  - name: instance_health
    rules:
      - alert: InstanceDown
        expr: up == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: 'Вузол {{ $labels.instance }} недоступний'
```

Д.3. Агент збору логів Alloy (пересилання журналу до Loki).

```
loki.source.journal "system" {
  forward_to = [loki.write.default.receiver]
  labels = { job = "systemd-journal" }
}
loki.write "default" {
  endpoint {
    url = "http://localhost:3100/loki/api/v1/push"
  }
}
```

Таблиця Е.1 - Вихідні дані щодо цін і SLA провайдерів за 2023-2025 роки

Зведені вихідні дані, що лягли в основу порівняння (табл. 2.3) та ТСО-розрахунків (рис. 2.4). Ціни наведено для віртуальних машин конфігурації 4 vCPU / 16 ГБ (Linux, регіон US-East) за публічними прайс-листами провайдерів.

Параметр	AWS	Azure	GCP	Джерело
Тип VM	m6a.xlarge	D4as v5	e2-standard-4	[9]
Ціна on-demand, USD/год	0,17-0,20	≈ 0,17	0,13-0,14	[9]
SLA одиночний, %	99,5	99,9	99,9	[6, 26, 27]
SLA multi-AZ, %	99,99	99,99	99,99	[6, 26, 27]
Reserved (1-3 р.), %	до 72	до 72	до 70	[9]
Spot / preemptible, %	до 90	до 90	до 80	[9]
Частка ринку 2024, %	≈ 30	≈ 21	≈ 12	[31]
Зростання цін 2023 (NPI), %	≈ 0,3	≈ 0,3	≈ 0,3	[32]

Джерело: складено автором за [6, 9, 26, 27, 31, 32]

Динаміка цін підтверджує висновок підрозділу 2.2: питома вартість обчислень за період майже не змінилася (індекс NPI зріс на 0,3 % у 2023 році), тоді як сукупна вартість володіння зростає переважно за рахунок збільшення обсягів даних і кількості сервісів.

КОРОТКИЙ ЗВІТ ПОДІБНОСТІ



Метадані

ДОКУМЕНТ

Заголовок

КБР_Кисельов_Євгеній

Автор

Кисельов Євгеній

Науковий керівник / Експерт

Камінський О.Є.

ІД документу

334362886

ОРГАНІЗАЦІЯ

Назва організації

Kyiv National Economic University named after Vadym Hetman
KNEU

підрозділ

кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту

2026-06-18

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

25

Довжина фрази для коефіцієнта подібності 2



КП 2

11257

Кількість слів



КЦ

84096

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		23
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		4

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Копію тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Копію тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://derainark.org/en/download/article-file/199503	14 0 (0 12 %)

2	ПІДГОТОВКА МАЙСТРА ВИРОБНИЧОГО НАВЧАННЯ, ВИКЛАДАЧА ПРОФЕСІЙНОГО НАВЧАННЯ ДО ВПРОВАДЖЕННЯ В ОСВІТНІЙ ПРОЦЕС ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ 11/22/2024 Hlukhiv National Pedagogical University of Oleksandr Dovzhenko (Hlukhiv National Pedagogical University of Oleksandr Dovzhenko)	13 0 (0.12 %)
3	SHA512 and MD5 Algorithm Vulnerability Testing Using Common Vulnerability Scoring System (CVSS) Ikbal Permana Putra, Mardi Hardjanto,Basya Fahmi;	12 0 (0.11 %)
4	Дослідження віртуалізації в хмарних системах для надання мережних сервісів 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	11 0 (0.1 %)
5	РОЗРОБКА АРХІТЕКТУРИ ХМАРНОЇ ПЛАТФОРМИ ДЛЯ ЗБЕРІГАННЯ ТА АНАЛІЗУ BIG DATA 2/11/2026 International University of Economics and Humanities named after Academician Stepan Demianchuk (International University of Economics and Humanities named after Academician Stepan Demianchuk)	10 0 (0.09 %)
6	Дослідження віртуалізації в хмарних системах для надання мережних сервісів 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	8 0 (0.07 %)
7	Дослідження віртуалізації в хмарних системах для надання мережних сервісів 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	8 0 (0.07 %)
8	https://antibotan.com/file.html?work_id=523645	8 0 (0.07 %)
9	Модель системи захисту інформації для хмарної СКБД 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	7 0 (0.06 %)
10	Дослідження віртуалізації в хмарних системах для надання мережних сервісів 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	7 0 (0.06 %)

База даних RefBooks (0.11 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

джерело: Paperity

1	SHA512 and MD5 Algorithm Vulnerability Testing Using Common Vulnerability Scoring System (CVSS) Ikbal Permana Putra, Mardi Hardjanto,Basya Fahmi;	12 (1) (0.11 %)
---	--	-----------------

Домашня база даних



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

Програма обміну базами даних (0.63 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

2	Дослідження віртуалізації в хмарних системах для надання мережних сервісів 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	41 (5) (0.36 %)
3	ПІДГОТОВКА МАЙСТРА ВИРОБНИЧОГО НАВЧАННЯ, ВИКЛАДАЧА ПРОФЕСІЙНОГО НАВЧАННЯ ДО ВПРОВАДЖЕННЯ В ОСВІТНІЙ ПРОЦЕС ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ 11/22/2024 Hlukhiv National Pedagogical University of Oleksandr Dovzhenko (Hlukhiv National Pedagogical University of Oleksandr Dovzhenko)	13 (1) (0.12 %)
4	РОЗРОБКА АРХІТЕКТУРИ ХМАРНОЇ ПЛАТФОРМИ ДЛЯ ЗБЕРІГАННЯ ТА АНАЛІЗУ BIG DATA 2/11/2026 International University of Economics and Humanities named after Academician Stepan Demianchuk (International University of Economics and Humanities named after Academician Stepan Demianchuk)	10 (1) (0.09 %)
5	Модель системи захисту інформації для хмарної СКБД 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	7 (1) (0.06 %)

Інтернет (0.25 %)



#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
6	https://antibotan.com/file.html?work_id=523645	14 (2) (0.12 %)
7	https://dergipark.org.tr/en/download/article-file/199503	14 (1) (0.12 %)

Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
---	-------	---------------------------------------