

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС–КОЛЕДЖ

Циклова комісія (кафедра) комп'ютерної інженерії та інформаційних технологій

**КВАЛІФІКАЦІЙНА РОБОТА**

на тему

**АНАЛІЗ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПОТРЕБ  
ОРГАНІЗАЦІЇ**

Виконала студентка групи 2К–21

Спеціальності 123 Комп'ютерна інженерія

Вікторія МАЗУРОК

Керівник:

Маргарита МЕДОЛИЗ

Черкаси 2025

## АНОТАЦІЯ

У кваліфікаційній роботі здійснено комплексний аналіз сучасних хмарних технологій та можливостей їх впровадження у діяльність середніх підприємств різних галузей. Особлива увага приділяється визначенню поняття хмарних технологій, етапам їх еволюції, а також класифікації основних моделей надання послуг: Інфраструктура як послуга (IaaS), Платформа як послуга (PaaS) та Програмне забезпечення як послуга (SaaS).

Робота висвітлює ключові аспекти забезпечення інформаційної безпеки в умовах використання хмарних рішень, питання конфіденційності даних та відповідності міжнародним стандартам захисту інформації. Проведено аналіз існуючих хмарних рішень, що дозволяють автоматизувати бізнес-процеси середніх підприємств, підвищувати ефективність управління, покращувати комунікацію всередині колективу та взаємодію з клієнтами. Значна увага приділяється питанням інфраструктурних рішень, що забезпечують гнучкість масштабування та стійкість до збоїв у роботі систем. У роботі обґрунтовано доцільність впровадження хмарних технологій для середніх підприємств як важливого етапу цифрової трансформації бізнесу.

Розроблено рекомендації щодо вибору оптимальної моделі хмарних послуг з урахуванням специфіки діяльності середнього бізнесу, запропоновано стратегії поступового переходу на хмарну інфраструктуру, враховуючи ризики та переваги такого переходу. Результати дослідження можуть бути використані власниками менеджерами середніх підприємств для конкурентоспроможності, зниження витрат на ІТ-інфраструктуру, забезпечення безперервного доступу до даних та швидкого реагування на потреби ринку.

## ABSTRACT

This qualification paper provides a comprehensive analysis of modern cloud technologies and their implementation potential in the operations of medium-sized enterprises across various industries. Special emphasis is placed on defining the concept of cloud computing, tracing its evolution, and classifying the main service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The paper explores the key aspects of ensuring information security, data privacy, and compliance with international data protection standards in cloud environments. It reviews existing cloud solutions that enable medium-sized businesses to automate their business processes, enhance management efficiency, and improve both internal communication and customer interactions. Considerable attention is given to infrastructure solutions that provide scalability, flexibility, and resilience against system failures. The study substantiates the relevance and feasibility of adopting cloud technologies as a crucial step toward the digital transformation of medium-sized businesses.

It develops practical recommendations for selecting the most suitable cloud service model according to the specific needs of a medium enterprise and outlines strategies for a gradual transition to a cloud-based infrastructure, considering potential risks and benefits. The results of this research can be used by owners and managers of medium-sized companies to strengthen their competitive advantages, reduce IT infrastructure costs, ensure continuous data access, and respond promptly to market demands.

## ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ .....	5
ВСТУП .....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ХМАРНИХ ТЕХНОЛОГІЙ .....	8
1.1 Поняття та еволюція хмарних технологій .....	8
1.2 Типи хмарних послуг: IaaS, PaaS, SaaS .....	11
1.3 Безпека та правові аспекти хмарних технологій .....	15
РОЗДІЛ 2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ .....	20
2.1 Хмарні рішення для автоматизації бізнес–процесів.....	20
2.2 Інфраструктурні рішення та хмарні обчислення .....	25
2.3 Хмарні технології для підвищення продуктивності та колаборації .....	29
РОЗДІЛ 3 ПРОПОЗИЦІЇ ЩОДО ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ХМАРНИМИ ТЕХНОЛОГІЯМИ.....	34
3.1 Стратегія впровадження хмарних технологій для організації .....	34
3.2 Оптимізація управління ресурсами в хмарі .....	37
3.3 Моделі кібербезпеки та захист даних в хмарних середовищах .....	42
ВИСНОВКИ.....	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	51
ДОДАТОК А – ПЕРЕВАГИ ХМАР .....	58

## ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IFTTT (від If This Then That) – це онлайн-платформа, яка дозволяє автоматизувати різноманітні дії між різними веб-сервісами та пристроями.

IT – інформаційні технології.

AWS (Amazon Web Services) - це широко відома хмарна платформа, що надає різноманітні послуги для інфраструктури IT, розробки програмного забезпечення, зберігання даних, та інших потреб бізнесу.

GDPR (General Data Protection Regulation) - регламент Європейського Союзу, який встановлює правила щодо захисту персональних даних фізичних осіб в межах Європейського Союзу та Європейської економічної зони.

DNS (Domain Name System) - це система, яка перетворює імена доменів (наприклад, google.com) на IP-адреси, що використовуються комп'ютерами для зв'язку в Інтернеті.

GCP (Google Cloud Platform) - запропонований компанією Google набір хмарних служб, які виконуються на тій же самій інфраструктурі, яку Google використовує для своїх продуктів призначених для кінцевих споживачів.

HIPAA (Health Insurance Portability and Accountability Act) - це федеральний закон США, прийнятий у 1996 році, який встановлює стандарти захисту конфіденційності та безпеки медичної інформації пацієнтів.

CRM (Customer Relationship Management) - система управління взаємовідносинами з клієнтами.

POS (Point of Sale) - система для точки продажу.

ERP (Enterprise Resource Planning) - система планування ресурсів підприємства.

IaaS (Infrastructure as a Service), це модель хмарних обчислень, яка надає компаніям віртуальні обчислювальні ресурси, такі як сервери, сховища даних, мережі та інше, через інтернет.

HRM-система (Human Resource Management) - приклад програмного забезпечення для HR-фахівців, система, яка об'єднує в одній платформі

різноманітні функції для управління та розвитку талантами в компанії, управління рекрутингом, аналітикою тощо.

PaaS (Platform as a Service) - це модель хмарних обчислень, що надає розробникам платформу для створення, розгортання та керування програмним забезпеченням.

SaaS (Software as a Service), це модель розповсюдження програмного забезпечення, де програмне забезпечення надається користувачам через інтернет як послуга, а не купується та встановлюється на їхні пристрої.

## ВСТУП

В умовах сучасного розвитку інформаційних технологій, хмарні технології відіграють важливу роль у забезпеченні ефективної роботи організацій різних галузей. З їх допомогою компанії можуть скоротити витрати на інфраструктуру, забезпечити гнучкість бізнес-процесів, підвищити продуктивність співробітників та оптимізувати управління даними.

Актуальність даного дослідження зумовлена зростаючою необхідністю організацій в оптимізації своїх бізнес-процесів за допомогою хмарних технологій. Сьогодні все більше компаній прагнуть інтегрувати хмарні рішення в свою діяльність, щоб забезпечити гнучкість, масштабованість та безпеку своїх операцій. Однак успішне впровадження хмарних технологій потребує детального аналізу існуючих рішень, їхньої безпеки та правових аспектів.

Об'єкт дослідження – сучасні рішення хмарних технологій, що використовуються для автоматизації бізнес-процесів та забезпечення кібербезпеки в організаціях.

Предмет дослідження – хмарні технології та їх застосування для забезпечення потреб організацій.

Мета дослідження – проаналізувати хмарні технології для забезпечення потреб організації та розробити пропозиції щодо вдосконалення управління ними.

Завдання дослідження:

1. Розглянути теоретичні аспекти хмарних технологій, еволюцію та типи послуг.
2. Проаналізувати існуючі рішення для автоматизації бізнес-процесів та інфраструктури організацій за допомогою хмарних технологій.
3. Оцінити можливості хмарних технологій для підвищення продуктивності та колаборації в організаціях.
4. Розробити пропозиції щодо вдосконалення управління ресурсами в хмарних середовищах та забезпечення кібербезпеки.

## РОЗДІЛ 1

### ТЕОРЕТИЧНІ АСПЕКТИ ХМАРНИХ ТЕХНОЛОГІЙ

#### 1.1 Поняття та еволюція хмарних технологій

Хмарні технології стали ключовим інструментом для багатьох організацій, які прагнуть підвищити ефективність бізнесу, зменшити витрати та забезпечити гнучкість у роботі. Вони дозволяють компаніям використовувати обчислювальні ресурси за моделлю "плати за використання" без необхідності інвестувати у власні сервери та інфраструктуру. Завдяки цьому організації можуть швидко масштабувати свої ІТ-потужності, забезпечуючи при цьому безпеку та доступність даних для співробітників у будь-якій точці світу [4].

Хмарні технології визначаються як модель надання ресурсів, що дозволяє отримувати доступ до обчислювальних потужностей через Інтернет на запит. За даними NIST, ця модель має п'ять ключових характеристик: самостійне обслуговування на вимогу, широка доступність через мережу, ресурсний пул, еластичність і вимірюваність послуг. IBM також підкреслює, що однією з основних переваг хмарних обчислень є їхня здатність допомагати організаціям скоротити витрати на ІТ та масштабувати ресурси в міру необхідності. AWS додає, що хмарні обчислення дозволяють компаніям глобально розгортати свої додатки за лічені хвилини, що значно покращує швидкість реагування на зміни ринку.

Хмарні технології також пропонують кілька моделей надання послуг (на рис. 1.2): Інфраструктура як Послуга (IaaS), Платформа як Послуга (PaaS) та Програмне Забезпечення як Послуга (SaaS). Кожна з цих моделей дозволяє організаціям отримувати необхідні ресурси, від серверів і зберігання даних до інструментів для розробки додатків та готових бізнес-рішень [10].

Хмарні технології дозволяють користувачам працювати з файлами та додатками з будь-якого пристрою, оскільки всі дані зберігаються і обробляються не на локальному комп'ютері, а на віддалених серверах у дата-центрах

(на рис.1.1). Наприклад, коли людина змінює телефон, вона все одно може зайти у свій обліковий запис Instagram з новим пристроєм і знайти всі свої фотографії, відео та повідомлення збереженими, оскільки ці дані зберігаються у хмарі. Це ж стосується хмарних сервісів електронної пошти, таких як Gmail або Microsoft 365, та сервісів зберігання файлів, таких як Google Drive або Dropbox. Завдяки хмарі всі зміни синхронізуються в режимі реального часу, і користувачі можуть отримати доступ до своїх даних з будь-якого місця, де є доступ до Інтернету [6].

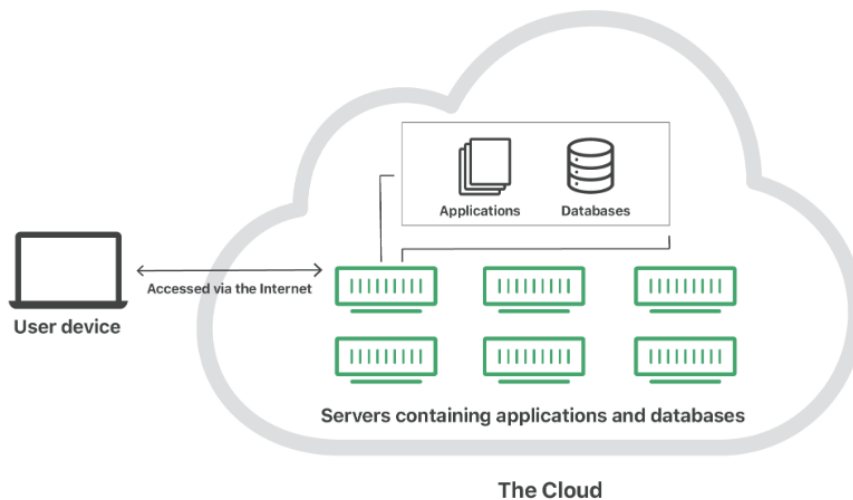


Рисунок 1.1 – Хмарні технології [8]

Хмарні рішення забезпечують високий рівень доступності та безперервності роботи сервісів, що дає можливість не лише зберігати важливі дані, але й відновлювати їх у разі втрати пристрою або інших технічних проблем. Це особливо корисно для бізнесу, де важливо забезпечити постійний доступ до робочих інструментів та інформації незалежно від місця перебування співробітників [18].

Перехід на хмарні обчислення дозволяє компаніям знизити витрати на управління власною ІТ-інфраструктурою, оскільки постачальники хмарних сервісів беруть на себе відповідальність за обслуговування та оновлення серверів. Це особливо корисно для малого бізнесу, який часто не має ресурсів для розгортання та підтримки власних серверів, але може орендувати хмарні

рішення за вигідною ціною. Хмарні технології також сприяють міжнародним операціям компаній, забезпечуючи доступ до даних і додатків для співробітників та клієнтів з будь-якої точки світу, що дозволяє легко керувати бізнесом незалежно від географічного розташування.

Хмарні обчислення функціонують завдяки технології віртуалізації, яка створює цифрові копії комп'ютерів, що імітують роботу фізичних пристроїв. Ці цифрові копії, відомі як віртуальні машини, поведуться так, ніби вони мають власне обладнання, хоча насправді функціонують на одному фізичному сервері. Основною перевагою віртуальних машин є те, що вони повністю ізольовані одна від одної, тобто вони працюють незалежно, і їхні дані не перетинаються з іншими віртуальними машинами на тому ж сервері. Завдяки цьому користувачі можуть безпечно зберігати свої файли та програми, не турбуючись про втручання інших систем, навіть якщо всі вони використовують одну фізичну інфраструктуру [5].

Віртуальні машини дозволяють значно підвищити ефективність використання серверних ресурсів. За допомогою віртуалізації можна одночасно запускати кілька віртуальних середовищ на одному фізичному сервері, що фактично перетворює його на багатофункціональний обчислювальний центр. Це дозволяє дата-центрам працювати з набагато більшою кількістю організацій та користувачів, ніж якби кожен використовував окреме фізичне обладнання. Завдяки такій архітектурі хмарні провайдери можуть обслуговувати сотні або навіть тисячі клієнтів одночасно, пропонуючи їм доступ до ресурсів за значно нижчою ціною. До того ж, ця модель допомагає знизити витрати на обслуговування фізичного обладнання та забезпечити безперервність послуг навіть у разі відмови окремих серверів, оскільки інші можуть взяти на себе навантаження [3].

Така оптимізація ресурсів робить хмарні рішення привабливими для широкого спектра підприємств – від малих компаній до великих корпорацій, які потребують масштабованих і доступних обчислювальних потужностей для своїх бізнес-процесів.

Навіть якщо один або декілька серверів вийдуть з ладу, хмарні системи зазвичай залишаються доступними і працюють безперебійно. Це досягається завдяки тому, що постачальники хмарних послуг розміщують резервні копії своїх даних та сервісів на різних серверах і навіть у різних регіонах. Така розподілена архітектура забезпечує надійність і високу доступність хмарних сервісів, дозволяючи мінімізувати ризик втрати даних або переривання в роботі.

Доступ до цих хмарних сервісів користувачі отримують через веб-браузер або спеціальний додаток, підключаючись до хмарної інфраструктури через Інтернет. Незалежно від пристрою – чи то смартфон, планшет, чи комп'ютер – користувачі можуть взаємодіяти з хмарою через глобальні мережі, що складаються з багатьох взаємопов'язаних інтернет-систем. Це дозволяє працювати з хмарними сервісами в будь-якій точці світу, де є доступ до Інтернету, забезпечуючи гнучкість і зручність у використанні хмарних технологій для як бізнесу, так і індивідуальних користувачів [20].

## **1.2 Типи хмарних послуг: IaaS, PaaS, SaaS**

Усі ресурси, що надаються через хмарні сервіси, отримали назву «послуги», оскільки вони активно підтримуються і керуються хмарними провайдерами. Ці ресурси можуть охоплювати різні аспекти, такі як інфраструктурні компоненти, додатки для користувачів, інструменти для розробки, а також сервіси для зберігання даних. Залежно від конкретних потреб, хмарні послуги класифікуються за різними моделями обслуговування, кожна з яких відповідає певному набору функцій та завдань.

Програмне забезпечення як послуга (SaaS) дозволяє користувачам отримувати доступ до програм без необхідності встановлення їх на свої пристрої. Замість цього всі програми розміщуються на хмарних серверах, а користувачі підключаються до них через Інтернет. SaaS можна порівняти з орендою квартири: орендодавець піклується про технічне обслуговування та оновлення, а орендар користується приміщенням, як своїм власним, маючи можливість

виконувати свої завдання. Основною перевагою цієї моделі є відсутність необхідності в управлінні інфраструктурою та регулярних оновленнях з боку користувачів, що робить цей варіант дуже зручним [15].

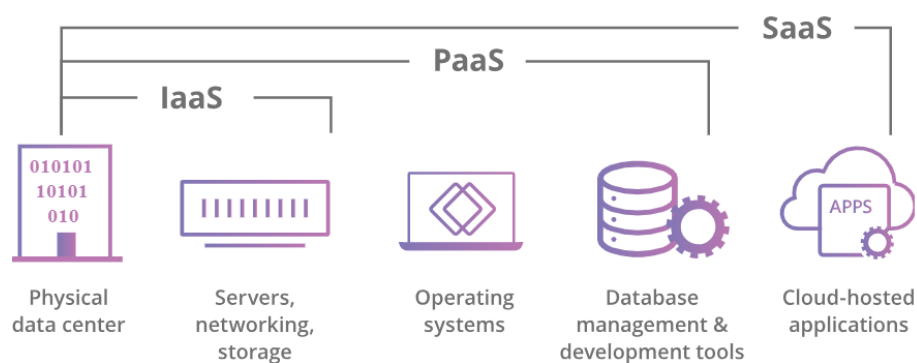


Рисунок 1.2 – Типи хмарних послуг [18]

SaaS–послуги охоплюють різноманітні інструменти для бізнесу і особистого користування. Приклади популярних SaaS–додатків включають Salesforce для управління взаємовідносинами з клієнтами, MailChimp для маркетингових розсилок, і Slack для командної комунікації. Завдяки SaaS, компанії можуть швидко впроваджувати нові технології та масштабувати свої послуги без значних витрат на локальну інфраструктуру.

Платформа як послуга (PaaS) – це хмарна модель, у якій компанії отримують доступ до інструментів для створення, тестування та запуску власних додатків, без необхідності керувати базовою інфраструктурою. На відміну від моделі SaaS, де користувачі отримують готові програми, в PaaS організації мають все необхідне для самостійного створення своїх додатків: сервери, мережі, бази даних, операційні системи та середовища розробки. Клієнти сплачують лише за використання цих ресурсів і не турбуються про фізичне обладнання або оновлення систем.

Порівнюючи це з будівництвом, PaaS можна уявити як оренду всіх інструментів та матеріалів, необхідних для зведення будинку, але без необхідності купувати саму землю чи обладнання для підтримки процесу будівництва. Постачальники PaaS забезпечують готову інфраструктуру для

розробки, а клієнти можуть зосередитися виключно на створенні власних продуктів [19].

Ця модель є ідеальною для компаній, які бажають розробляти нові додатки або сервіси, але не хочуть вкладати великі кошти в налаштування серверів або управління системами. Прикладами платформних сервісів є Heroku, яка забезпечує просте середовище для швидкої розробки, та Microsoft Azure, яка пропонує широкий спектр інструментів для різних типів проєктів, від баз даних до штучного інтелекту.

Завдяки PaaS, компанії отримують гнучкість, швидкість розробки та можливість зосередитися на основному бізнесі, не відволікаючись на технічну інфраструктуру.

Інфраструктура як послуга (IaaS) – це модель хмарних обчислень, яка надає компаніям можливість орендувати обчислювальні ресурси, такі як сервери, сховища даних та мережеві потужності, у хмарного провайдера. Це дозволяє організаціям уникнути значних капіталовкладень у фізичну інфраструктуру та зосередитися на розробці своїх програм і сервісів. Вони можуть масштабувати свої ресурси за потреби, не турбуючись про управління або технічне обслуговування обладнання [13].

IaaS можна порівняти з орендою ділянки землі, на якій компанія може будувати що завгодно, але їй потрібно самостійно забезпечити інструменти та матеріали для будівництва. Хмарний провайдер надає лише основні ресурси – сервери, зберігання даних та мережеві потужності. У цій моделі компанія самостійно керує операційними системами, програмним забезпеченням і додатками, які запускаються на орендованій інфраструктурі (на рис. 1.3).

Приклади постачальників IaaS включають DigitalOcean, яка пропонує прості та доступні серверні ресурси для стартапів і розробників; Google Compute Engine, яка надає потужні обчислювальні ресурси для масштабних проєктів; та OpenStack, яка є платформою для створення приватних і публічних хмарних рішень.

Завдяки IaaS компанії отримують повну свободу у виборі та налаштуванні програмних і апаратних ресурсів, що дозволяє ефективно масштабувати свої проекти в залежності від змін у попиту та бізнес-потребах [4].

Раніше моделі хмарних обчислень переважно зводилися до трьох основних категорій: SaaS, PaaS і IaaS, і більшість хмарних сервісів відповідали одній із цих категорій. Проте з розвитком технологій з'явилася нова, четверта модель – Функція як послуга (FaaS).

FaaS, або так зване безсерверне обчислення, полягає в тому, що хмарні додатки поділяються на невеликі частини, які запускаються лише за необхідністю. Ця модель дає змогу використовувати ресурси максимально ефективно: компанія платить тільки за фактичне використання обчислювальних потужностей у певний момент. Якщо провести аналогію з орендою будинку, то FaaS дозволяє платити лише за ті частини будинку, які використовуються: наприклад, за їдальню під час обіду, спальню на час сну, або вітальню, коли потрібен доступ до неї, а коли ці кімнати не використовуються – немає потреби за них платити [16].

Хоча FaaS називається "безсерверним", насправді ці програми все одно працюють на серверах, як і інші моделі хмарних обчислень. Однак компаніям, які створюють додатки на основі FaaS, не потрібно самостійно управляти серверами, що значно знижує операційні витрати. Платформа автоматично керує всіма процесами, необхідними для виконання програм, що робить модель особливо привабливою для розробників, яким важлива швидкість та ефективність [21].

Ця модель стає дедалі популярнішою завдяки своїй гнучкості та економічності, особливо для короткострокових або нестабільних робочих навантажень, коли традиційні моделі хмарних обчислень можуть бути менш ефективними.

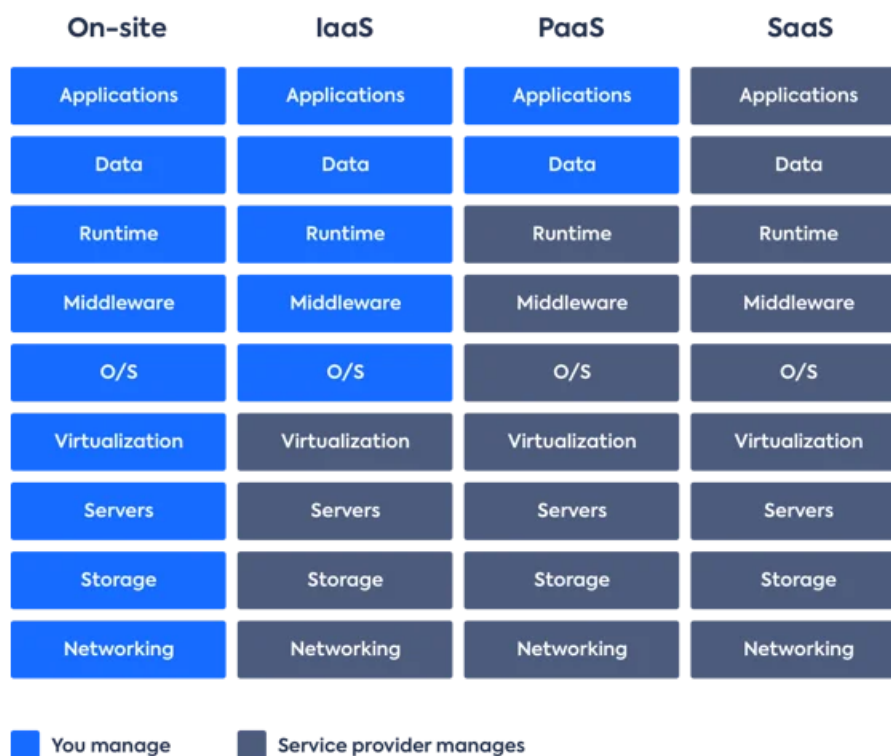


Рисунок 1.3 – Відмінності між IaaS і PaaS проти SaaS і рівень керування постачальником [39]

### 1.3 Безпека та правові аспекти хмарних технологій

Основні виклики безпеки у хмарних технологіях охоплюють серйозні загрози, пов'язані з конфіденційністю, захистом даних та забезпеченням доступності. Однією з головних проблем є витік даних, коли конфіденційна інформація користувачів стає доступною через недоліки у захисті або вразливості хмарної інфраструктури. Наприклад, у 2019 році стався витік 540 мільйонів записів користувачів Facebook, які зберігалися на відкритих серверах Amazon Web Services, що продемонструвало ризики неправильного налаштування захисту [38].

Другий критичний виклик – це несанкціонований доступ до даних. Якщо користувачі використовують слабкі паролі або їх облікові записи зламані, зловмисники можуть отримати доступ до конфіденційної інформації. Яскравим

прикладом є інцидент з iCloud у 2014 році, коли особисті фотографії знаменитостей були викрадені через слабкі паролі та фішингові атаки.

Ще однією важливою загрозою є недостатня захищеність конфіденційної інформації (на рис. 1.4). Відсутність належних засобів шифрування або неправильне налаштування хмарної інфраструктури може призвести до масштабних витоків. Випадок з Equifax у 2017 році, де було зламано особисті дані 143 мільйонів користувачів, є прикладом того, як недоліки у хмарних платформах можуть стати причиною серйозних наслідків [16].

Також варто відзначити DDoS-атаки, які можуть вивести з ладу хмарні сервіси шляхом перевантаження системи. У 2016 році відома атака на DNS-провайдера Dyn призвела до тимчасового відключення сервісів, таких як Amazon та Twitter, через перевантаження хмарної інфраструктури.

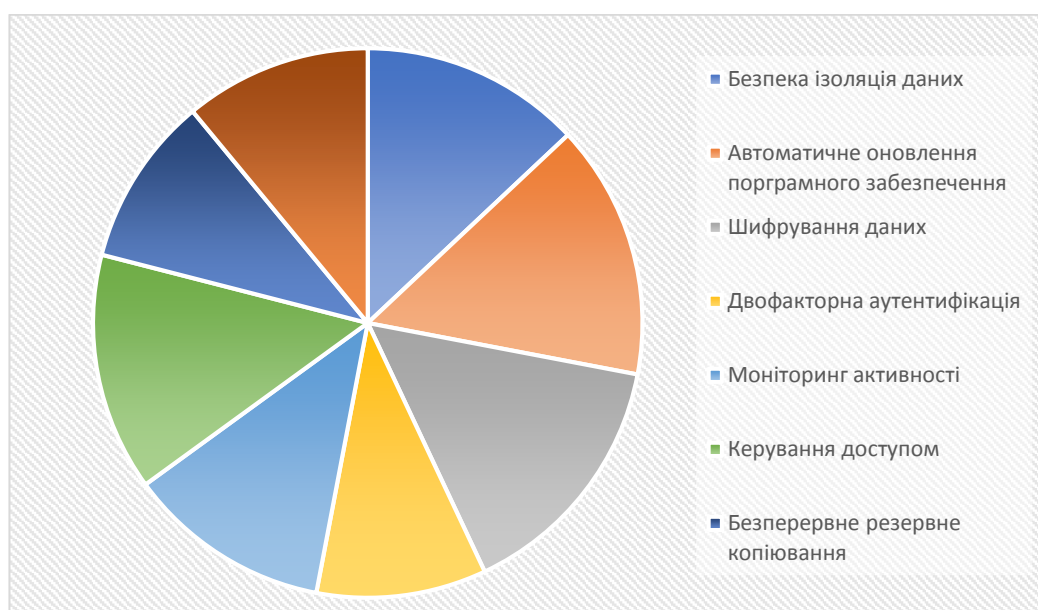


Рисунок 1.4 – Розподіл основних методів забезпечення безпеки в хмарних технологіях [4]

Зловмисне програмне забезпечення є постійною загрозою для хмарних сервісів. Напади із використанням вірусів та троянів можуть призвести до витоку інформації або руйнування даних. У 2020 році були виявлені кампанії, що

використовували хмарні сервіси для поширення зловмисного програмного забезпечення через скомпрометовані облікові записи [38].

Таблиця 1.1 – Методи забезпечення безпеки даних у хмарних технологіях

Security Method	Опис
Шифрування даних (Data Encryption)	Шифрування даних на рівні зберігання і передачі, що унеможлиблює доступ до інформації без ключа дешифрування.
Двофакторна аутентифікація (Two-Factor Authentication)	Додавання другого рівня перевірки при вході в систему, наприклад, код через SMS або додаток.
Моніторинг активності (Activity Monitoring)	Регулярне відстеження активності користувачів і систем для виявлення підозрілих дій або порушень.
Брандмауери (Firewalls)	Захищає мережі від несанкціонованого доступу через фільтрування трафіку та блокування небезпечних запитів.
Регулярне резервне копіювання (Regular Backups)	Автоматичне створення копій даних для їх відновлення у разі втрати або пошкодження.
Сегментація мережі (Network Segmentation)	Розподіл мережі на сегменти для зменшення ризику поширення атак між різними частинами системи.
Контроль доступу (Access Control)	Надання доступу до даних тільки авторизованим користувачам з різними рівнями привілеїв.
Інструменти управління вразливістю (Vulnerability Management Tools)	Інструменти для виявлення та усунення вразливостей в системі перед тим, як вони можуть бути використані зловмисниками.
Управління оновленнями (Patch Management)	Забезпечує своєчасне оновлення програмного забезпечення для усунення відомих вразливостей.
Шифрування під час передачі (Encryption in Transit)	Забезпечення безпеки даних під час їх передачі по мережі через шифрування.

Правові аспекти хмарних технологій регулюються як на міжнародному, так і на національному рівнях, зосереджуючись на захисті конфіденційності, безпеки даних та управлінні інформацією в хмарних середовищах. (див. табл.1.1)більш детальний розгляд основних регуляцій [16]:

#### 1. GDPR (General Data Protection Regulation).

Це основний нормативний акт Європейського Союзу, спрямований на захист персональних даних громадян. GDPR вимагає від хмарних провайдерів суворого дотримання правил обробки даних, зокрема щодо доступу, шифрування і збереження даних. Однією з ключових вимог є право на забуття, що дозволяє користувачам вимагати видалення своїх даних, а також право на доступ до інформації. Крім того, дані, що передаються між різними країнами, повинні бути належним чином захищені. Провайдери хмарних послуг зобов'язані

забезпечити належний захист персональних даних під час їх обробки та зберігання.

### 2. HIPAA (Health Insurance Portability and Accountability Act).

HIPAA регулює збереження та обробку електронної медичної інформації (ePHI) у США. Хмарні провайдери, які працюють з ePHI, повинні відповідати вимогам щодо безпеки, включаючи шифрування даних, забезпечення конфіденційності інформації та укладення угод про бізнес-асоціацію (BAA) з медичними установами. Провайдери не можуть уникати відповідальності навіть у випадках, коли вони не мають доступу до розшифрування даних, адже все одно залишаються відповідальними за безпеку систем, де зберігаються ці дані.

### 3. CCPA (California Consumer Privacy Act).

Регулює захист персональних даних у Каліфорнії, США. Закон надає громадянам право вимагати видалення своїх даних, інформувати їх про збір даних, а також обмежувати продаж даних третім особам. Це забезпечує прозорість та підвищує контроль споживачів над їх персональною інформацією.

Вибір хмарного провайдера для відповідності вимогам HIPAA є важливим процесом, який вимагає ретельної оцінки безпекових можливостей провайдера. Одним із ключових факторів є дотримання стандартів безпеки HIPAA. Провайдер повинен забезпечити шифрування даних як під час їх передачі, так і під час зберігання, а також впровадити контроль доступу та багатофакторну аутентифікацію для захисту конфіденційної медичної інформації (ePHI) [20].

Критично важливим є укладення угоди про бізнес-асоціацію (Business Associate Agreement, BAA) між медичною установою та хмарним провайдером. Ця угода чітко визначає обов'язки обох сторін щодо захисту даних і регламентує відповідальність у разі порушення вимог HIPAA. Провайдер, навіть якщо не має доступу до розшифрування даних, все одно відповідає за безпеку інфраструктури, де зберігаються дані.

Також важливо, щоб провайдер надавав рішення для планування відновлення після катастроф (Disaster Recovery Plan). Це забезпечить безперервність роботи систем у випадку збою або стихійного лиха, дозволяючи

зберегти доступ до критичних медичних даних і забезпечити їх відновлення. Наявність такого плану є обов'язковою вимогою для відповідності стандартам HIPAA [21].

При виборі провайдера важливо врахувати міжнародні регуляції, такі як GDPR, особливо якщо організація має міжнародні операції. Деякі з провайдерів, які пропонують сервіси, сумісні з HIPAA, включають Amazon Web Services (AWS), Microsoft Azure, і Google Cloud, кожен з яких має відповідні інструменти для забезпечення безпеки медичних даних.

## РОЗДІЛ 2

### АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ

#### 2.1 Хмарні рішення для автоматизації бізнес–процесів

Хмарні рішення для автоматизації бізнес–процесів відіграють ключову роль у сучасних організаціях, забезпечуючи ефективність і зручність управління щоденними операціями. Вони дозволяють підприємствам автоматизувати рутинні завдання, інтегрувати різні процеси та використовувати переваги хмарної інфраструктури, зменшуючи при цьому витрати на ІТ. Однією з найбільш популярних категорій хмарних рішень є CRM-системи (Customer Relationship Management), які автоматизують управління взаємовідносинами з клієнтами. (див. табл. 2.1) Наприклад, Salesforce дозволяє компаніям відслідковувати продажі, взаємодії з клієнтами, організовувати маркетингові кампанії в хмарному середовищі, що значно підвищує їхню ефективність [33].

Іншою важливою категорією є ERP-системи (Enterprise Resource Planning), які об'єднують управління ключовими процесами організації, такими як фінанси, логістика, виробництво та інші операції. Системи, як-от Oracle NetSuite або SAP S/4HANA, надають можливість автоматизувати ці процеси через хмару, дозволяючи компаніям отримувати доступ до ресурсів і даних з будь-якої точки світу без необхідності утримання локальної інфраструктури.

Маркетингова автоматизація є ще одним прикладом хмарних рішень, що дозволяють бізнесам ефективно керувати маркетинговими кампаніями. Такі інструменти, як HubSpot і MailChimp, забезпечують автоматизоване надсилання електронних листів, відстеження клієнтської активності та аналіз результатів кампаній, що допомагає оптимізувати взаємодію з клієнтами та підвищити рентабельність [7].

Для автоматизації управління персоналом існують хмарні HRM–системи (Human Resource Management). Платформи на кшталт Workday та BambooHR

допомагають оптимізувати процеси найму, управління персоналом і нарахування зарплат. Такі системи знижують необхідність у ручній роботі й мінімізують можливі помилки у роботі з персональними даними співробітників.

Роботизована автоматизація процесів (RPA) у хмарі також стала ефективним рішенням для автоматизації рутинних завдань. Платформи, такі як UiPath, дозволяють автоматизувати складні та повторювані бізнес-процеси, як-от обробку документів або управління клієнтськими запитами, що економить час та ресурси.

Хмарні рішення для автоматизації надають компаніям гнучкість у масштабуванні, зменшують витрати на ІТ, а також дозволяють швидко впроваджувати нові технології без необхідності значних інвестицій у локальну інфраструктуру.

Таблиця 2.1 – Хмарні провайдери для автоматизації бізнес – процесів [7, 11]

Провайдер	Категорія	Опис
Salesforce	Автоматизація CRM	Автоматизує управління взаємовідносинами з клієнтами, відстеження продажів, маркетингові кампанії
Oracle NetSuite	Автоматизація ERP	Хмарне ERP-рішення для автоматизації фінансів, операцій, ланцюгів постачання та взаємовідносин з клієнтами
HubSpot	Автоматизація маркетингу	Забезпечує автоматизацію маркетингу, продажів та обслуговування клієнтів, вбудовані можливості CRM
Workday	Автоматизація HRM	Автоматизує HR-процеси, включаючи набір персоналу, зарплату, управління персоналом та аналітику
UiPath	Автоматизація RPA (роботизація)	Автоматизує рутинні завдання через роботів, обробку даних, взаємодію з клієнтами та документообіг

Microsoft Power Automate – це потужний інструмент для автоматизації, який дозволяє створювати робочі процеси між різними додатками та службами. Він дозволяє налаштовувати автоматизовані робочі процеси без необхідності програмування, спрощуючи інтеграцію продуктів Microsoft 365. Наприклад, ви можете налаштувати Power Automate так, щоб нові електронні листи автоматично зберігалися у OneDrive або щоб форми з Microsoft Forms автоматично передавалися в Excel для обробки. Це ідеальний інструмент для

компаній, які використовують екосистему Microsoft і прагнуть оптимізувати свої робочі процеси [17].

Zapier – популярний сервіс для автоматизації, що працює з тисячами додатків і дозволяє з'єднувати їх між собою. Zapier дозволяє створювати автоматизовані процеси, такі як передача даних між CRM і маркетинговими платформами, оновлення таблиць у Google Sheets на основі нових подій у додатках або інтеграція даних з електронної пошти з іншими системами. Його простий інтерфейс дозволяє швидко налаштовувати робочі процеси без необхідності в знанні програмування [22].

Integromat (Make) – сервіс для створення більш складних інтеграцій та автоматизацій, що підтримує логічні умови, цикли й багатоступеневі сценарії. Наприклад, Integromat може автоматизувати процес збору інформації з форм, обробку цієї інформації в Google Sheets, а потім передачу результатів у CRM–систему для подальшого аналізу. Сервіс також підтримує автоматизацію за розкладом, що робить його корисним для складних бізнес–процесів.

IFTTT (If This Then That) – це хмарний сервіс, що спеціалізується на простих інтеграціях між додатками за принципом "якщо то". Наприклад, він може автоматично зберігати нові фотографії з Instagram у хмарне сховище або надіслати повідомлення в Telegram, коли з'являється новий вхідний лист. IFTTT ідеально підходить для автоматизації простих дій між соціальними мережами, смарт–пристроями та іншими хмарними сервісами [4].

Automate.io дозволяє створювати автоматизовані процеси для інтеграції популярних додатків, таких як Salesforce, Slack, Google Drive, і Trello. Він допомагає автоматизувати маркетингові кампанії, управління клієнтами та інші рутинні процеси. Наприклад, Automate.io може автоматично додавати нові контакти в CRM після отримання запиту на сайті або синхронізувати дані між різними інструментами для ефективнішого управління проектами.

Кожен з цих хмарних сервісів допомагає автоматизувати рутинні процеси та інтегрувати різні додатки, що дозволяє суттєво скоротити час і ресурси, необхідні для виконання ручних завдань (див. табл. 2.2).

Таблиця 2.2 – Порівняння хмарних сервісів для автоматизації бізнес – процесів [14]

Критерій	Microsoft Power Automate	Zapier	Integromat (Make)
Інтеграція з додатками	Широка інтеграція з продуктами Microsoft 365 (Outlook, SharePoint, Teams) та сторонніми сервісами	Інтеграція з більш ніж 3000 додатками, включаючи Google, Slack, Dropbox	Широка підтримка інтеграцій, включаючи Google Sheets, Shopify, Slack
Простота налаштування	Дружній інтерфейс, але потребує розуміння основ логіки автоматизації	Дуже простий у використанні інтерфейс, підходить для початківців	Складніший інтерфейс, вимагає більше часу на освоєння
Гнучкість	Висока гнучкість, особливо для користувачів екосистеми Microsoft	Обмежена гнучкість у порівнянні з іншими сервісами, підходить для простих процесів	Висока гнучкість для створення складних сценаріїв
Можливості для автоматизації складних процесів	Підтримка складних багатоступеневих робочих процесів, доступ до API	Підтримує базові автоматизації, але складні процеси можуть бути обмежені	Підтримує дуже складні автоматизації з умовами, циклами і логікою

Впровадження хмарних технологій значно допомагає підприємствам досягати своїх бізнес-цілей завдяки кільком ключовим перевагам.

Автоматизація скорочує кількість ручних операцій, дозволяючи знизити навантаження на співробітників та усунути рутинні завдання. За допомогою хмарних інструментів, таких як Microsoft Azure Automation або Zapier, підприємства можуть автоматизувати управління інфраструктурою та виконання операцій. Це звільняє ресурси для виконання стратегічно важливих завдань та підвищує ефективність роботи співробітників [7].

Ще однією вагомою перевагою є мінімізація людських помилок. Використання хмарних автоматизованих рішень знижує ризик помилок, пов'язаних з людським фактором, наприклад, при управлінні великими обсягами даних або конфігурації систем. Сервіси автоматизують виявлення проблем та підтримку безпеки в реальному часі, що підвищує точність процесів і дозволяє швидко реагувати на можливі загрози.

Хмарні технології сприяють швидшій реакції бізнесу на зміни ринку. Оскільки автоматизація дозволяє масштабувати ресурси на вимогу та аналізувати дані в реальному часі, компанії можуть швидше приймати рішення та адаптуватися до нових умов. (див. рис. 2.1) Це особливо важливо для динамічних ринків, де швидкість реагування може стати вирішальною конкурентною перевагою.

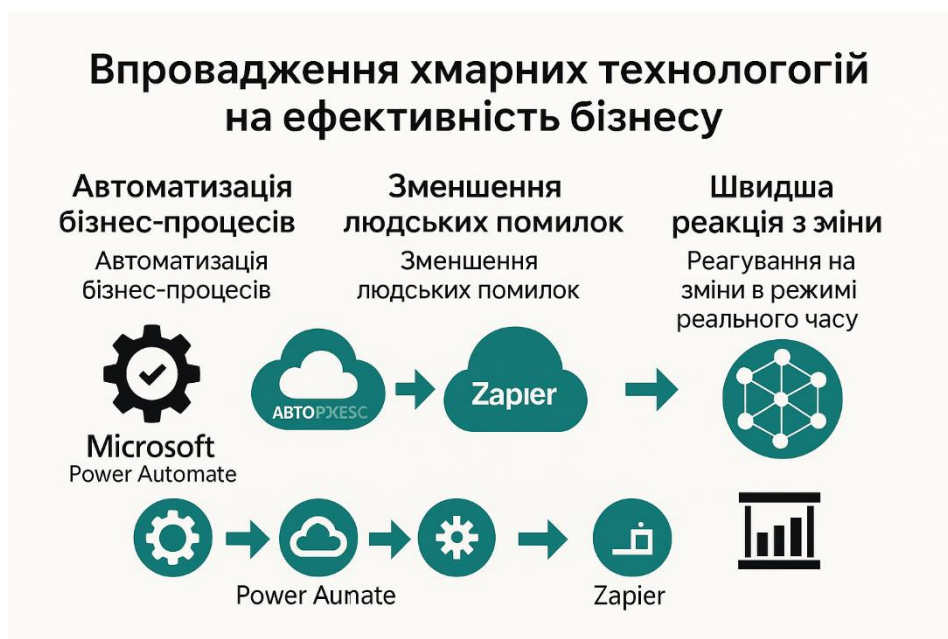


Рисунок 2.1 – Вплив впровадження хмарних технологій на ефективність бізнесу

Схема демонструє, як впровадження хмарних технологій може покращити ефективність бізнесу через три ключові аспекти: автоматизацію ручних процесів, зменшення кількості людських помилок і швидшу реакцію на ринкові зміни. Автоматизація таких рутинних завдань, як обробка документів та управління даними, дозволяє знизити витрати та підвищити продуктивність. Зменшення людських помилок відбувається завдяки автоматизованим перевіркам і моніторингу, що підвищує точність даних та ефективність безпеки. Завдяки аналізу даних у реальному часі бізнес може швидше адаптуватися до нових викликів і приймати обґрунтовані рішення [19].

## 2.2 Інфраструктурні рішення та хмарні обчислення

Основною моделлю є IaaS (Infrastructure as a Service) – це хмарний сервіс, який дозволяє компаніям орендувати обчислювальні потужності без необхідності інвестувати в фізичні сервери та інші компоненти інфраструктури. Компанії отримують доступ до необхідної інфраструктури, такої як віртуальні машини, дисковий простір, мережі та сервери, через інтернет.

Модель IaaS дозволяє підприємствам використовувати хмарні ресурси на основі оплати за фактичне використання, що знижує витрати на управління інфраструктурою. Наприклад, такі провайдери, як Amazon Web Services (AWS), Google Cloud, і Microsoft Azure, пропонують масштабовані інфраструктурні рішення, які дозволяють бізнесам швидко розширювати або скорочувати свої потужності в залежності від потреб. Це особливо корисно для компаній, які працюють у динамічних галузях, де попит на ресурси може швидко змінюватися.

Однією з основних переваг хмарної інфраструктури є її масштабованість. Наприклад, якщо компанії потрібні додаткові ресурси під час пікових навантажень, таких як Чорна П'ятниця для ритейлерів, хмарні провайдери дозволяють додати серверні потужності без затримок. Це особливо важливо для компаній електронної комерції або потокових сервісів, як-от Netflix, які використовують потужності хмарних обчислень для обробки великого обсягу даних і забезпечення безперервного доступу до своїх послуг у будь-який час [15].

У сучасних хмарних інфраструктурних рішеннях часто використовуються контейнери та віртуалізація. Контейнеризація (наприклад, з використанням Docker або Kubernetes) дозволяє запускати додатки у легких, ізольованих середовищах, що спрощує їх розгортання та управління. Це дає змогу компаніям швидко адаптуватися до змін і збільшувати кількість додатків, не турбуючись про конфлікти між різними частинами інфраструктури.

Віртуалізація ж дозволяє запускати кілька віртуальних машин на одному фізичному сервері, що підвищує ефективність використання обладнання. За

допомогою віртуалізації компанії можуть зменшити витрати на фізичні сервери та забезпечити безперерйну роботу своїх додатків, навіть якщо одне з обладнань виходить з ладу [22].

Одним із найважливіших аспектів використання хмарних інфраструктур є безпека. Хмарні провайдери забезпечують захист даних через шифрування, контроль доступу та моніторинг у режимі реального часу. Наприклад, провайдери, такі як AWS і Microsoft Azure, використовують передові методи шифрування для захисту даних як під час їх зберігання, так і під час передачі. Це дозволяє компаніям дотримуватися міжнародних стандартів безпеки, таких як GDPR у ЄС або HIPAA в США для захисту медичних даних.

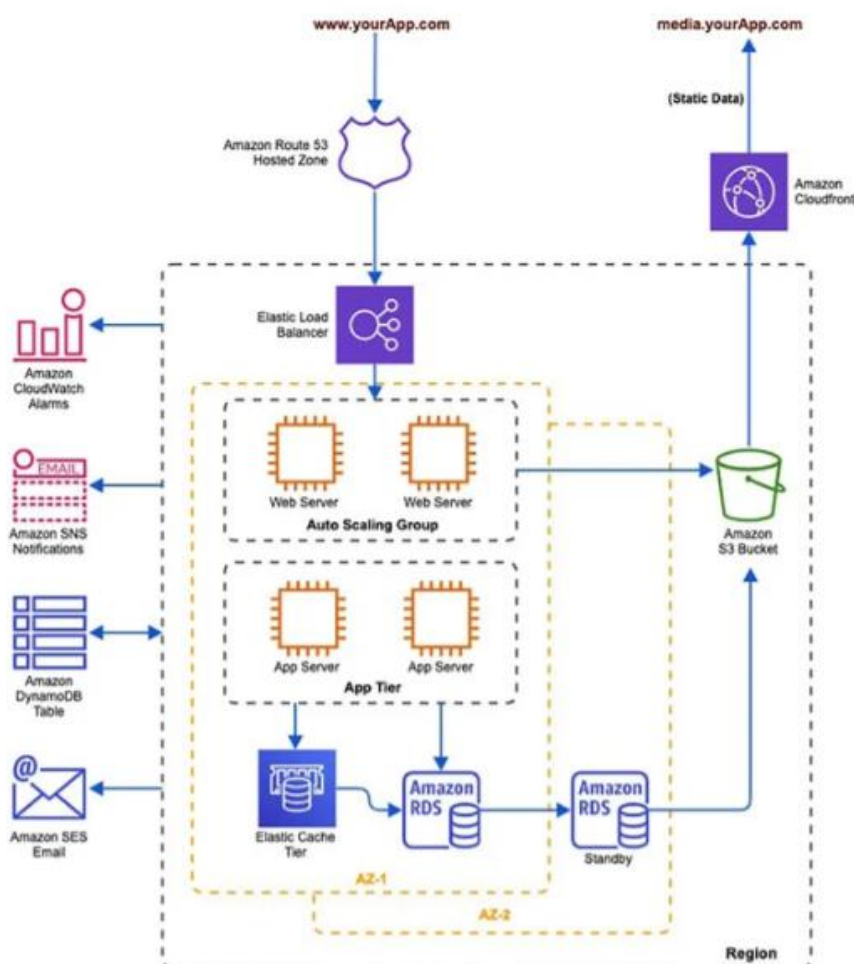


Рисунок 2.3 – AWS-архітекстура [13]

Успішні кейси впровадження хмарної інфраструктури демонструють, як бізнеси отримують конкурентні переваги завдяки хмарним технологіям. Наприклад, Uber використовує інфраструктуру Google Cloud для обробки даних у реальному часі, що допомагає оптимізувати маршрути та зменшити час очікування для клієнтів. Інший приклад – Coca-Cola, яка використовує AWS для аналітики та управління ланцюгом постачання, що допомагає компанії ефективніше керувати своїми операціями [13] (див рис. 2.3).

Google Cloud Platform (GCP) спочатку була створена, щоб підтримувати інфраструктурні потреби для власних сервісів компанії Google, таких як пошукова система Google, Gmail, і відеоплатформа YouTube. Ця платформа стала основою для надання масштабованих, надійних і безпечних хмарних послуг. Завдяки власній інфраструктурі Google змогла забезпечити безперебійну роботу мільярдів користувачів по всьому світу, і згодом відкрила доступ до своїх обчислювальних ресурсів іншим компаніям через GCP.

На сьогодні GCP є одним із найбільших провайдерів хмарних обчислень у світі, посідаючи третє місце за розміром ринку серед інших IaaS-постачальників. Платформа надає широкий спектр послуг – від обчислень, зберігання даних, машинного навчання до інструментів для розробки та обробки великих обсягів інформації в реальному часі. Одним з ключових факторів успіху GCP є його масштабованість і інфраструктура, здатна підтримувати навіть найбільш ресурсоємні процеси [18].

Gartner, відомий дослідник ринків, відзначає GCP як одного з провідних гравців на ринку хмарних послуг завдяки високій надійності, інноваціям і можливості масштабувати рішення відповідно до потреб бізнесу. Google також активно впроваджує нові технології, такі як штучний інтелект і машинне навчання, що робить GCP однією з найінноваційніших платформ на ринку.

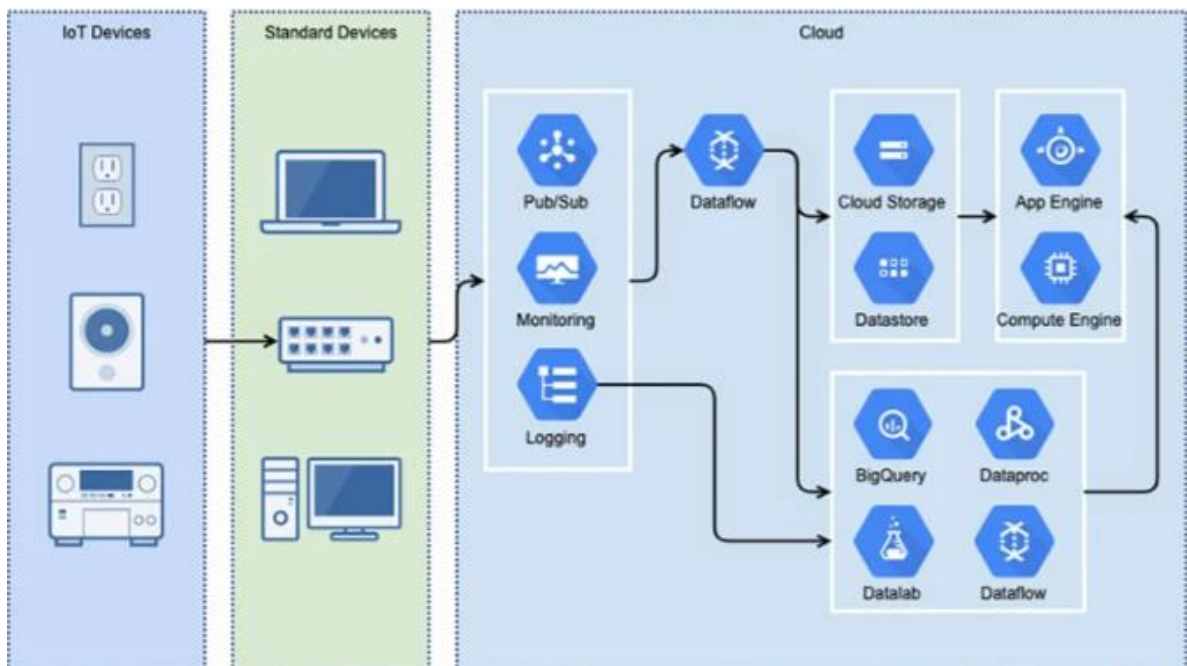


Рисунок 2.4 – GCP – архітектура [16]

Продуктом Microsoft для інфраструктури як послуги (IaaS) є платформа Microsoft Azure, яка займає друге місце за популярністю серед хмарних рішень після Amazon Web Services (AWS). Azure надає потужну хмарну інфраструктуру, що включає обчислювальні потужності, сховище даних, мережеві можливості та сервіси штучного інтелекту (на рис. 2.4). Особливістю Azure є його тісна інтеграція з іншими продуктами Microsoft, такими як Windows Server, SQL Server, Active Directory, і Microsoft 365, що робить його ідеальним вибором для підприємств, які вже використовують рішення Microsoft [21].

Завдяки такій інтеграції, організації можуть легко перенести свої існуючі локальні системи в хмару, зберігаючи знайомі інструменти та процеси. Це дозволяє компаніям мінімізувати витрати на перенавчання персоналу та спрощує процес міграції. Крім того, Microsoft Azure забезпечує підтримку різних операційних систем та програм, що робить його універсальним рішенням для компаній з різними інфраструктурними потребами (на рис. 2.5).

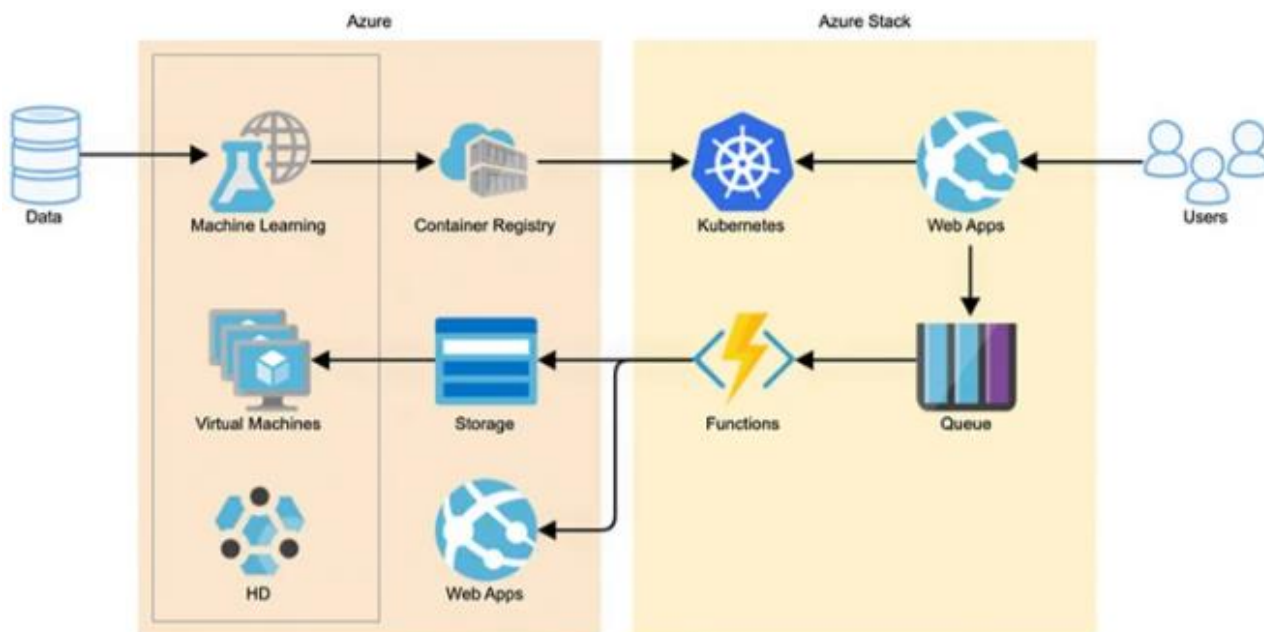


Рисунок 2.5 – Microsoft Azure – архітектура [39]

Azure також відзначається своїми можливостями для створення гібридних хмарних середовищ, що дозволяє компаніям поєднувати локальні ресурси з хмарними, забезпечуючи більшу гнучкість у використанні ресурсів. Це особливо важливо для організацій, які прагнуть поступово переходити на хмарні технології без втрати контролю над своїми даними та процесами.

Ці переваги роблять Microsoft Azure провідним вибором серед підприємств на ринку, особливо тих, які використовують інші продукти Microsoft, що значно спрощує інтеграцію та управління всією ІТ-інфраструктурою.

### 2.3 Хмарні технології для підвищення продуктивності та колаборації

Хмарні технології відіграють ключову роль у підвищенні продуктивності компаній, забезпечуючи такі можливості, як інтеграція хмарної телефонії для обробки дзвінків та організація онлайн-тренінгів для співробітників кол-центрів. Крім того, хмарні рішення для відеоконференцій значно спрощують проведення зустрічей незалежно від місця перебування учасників. Через це багато організацій планують перевести більше половини своєї інфраструктури та

додатків у хмару в найближчому майбутньому, щоб скористатися всіма перевагами цих технологій [38].

Існує велика кількість хмарних інструментів для управління проектами, які дозволяють командам ефективно організовувати роботу над проектами та співпрацювати в реальному часі. Такі платформи, як Asana, Trello, і Monday.com, дозволяють розподіляти проекти на окремі завдання, що можуть бути організовані у вигляді списків або дощок. Це надає можливість команді чітко відстежувати прогрес роботи, створювати списки справ і делегувати завдання відповідним членам команди, що сприяє кращій структуризації робочих процесів.

Одна з важливих характеристик таких систем – це можливість спільного обговорення завдань у режимі реального часу. Це дозволяє членам команди залишати коментарі та надавати зворотний зв'язок, що забезпечує безперервний обмін ідеями та швидку реакцію на зміни. Ідеальна платформа для управління проектами також повинна інтегруватися з іншими сторонніми системами та інструментами, такими як CRM або системи для обробки даних, що сприяє більшій гнучкості в роботі [32].

Оскільки ці інструменти часто використовуються для підтримки віддалених команд, інтуїтивно зрозумілий інтерфейс є критично важливим. Чим легше новим користувачам освоїти систему, тим швидше команда зможе розпочати роботу. Особливо це важливо для організацій, що часто наймають нових співробітників дистанційно, оскільки адаптація до нових умов відбувається швидше з простим у використанні інструментом.

Хмарне програмне забезпечення для управління проектами також пропонує функцію зберігання даних, поєднуючи можливості управління з безпечним хмарним сховищем. Це дозволяє організувати файли в централізованому сховищі, що доступне користувачам будь-коли та з будь-якого місця за наявності відповідних дозволів та інтернет-з'єднання. Окрім цього, обмін файлами через ці платформи є значно безпечнішим порівняно з

традиційними методами передачі даних, як–от електронна пошта, що є важливим для роботи з конфіденційною інформацією [21].

Багато з цих інструментів, таких як Trello або Wrike, мають безкоштовні базові версії, що дозволяє користуватися основними функціями без додаткових витрат. Однак для розширеного функціоналу, наприклад, для збільшення кількості користувачів або доступу до розширених засобів звітності, компаніям часто вигідно переходити на преміум–версії, які відкривають доступ до більш глибоких інструментів управління проектами та командою.

Електронні листи не завжди зручні для швидкої комунікації між співробітниками, оскільки вони вимагають заголовків і детальних пояснень, що може створити плутанину при великій кількості повідомлень у папці «Вхідні».

Натомість, програми для командного обміну повідомленнями значно полегшують ділове спілкування. Такі інструменти дозволяють оперативно обмінюватися короткими повідомленнями в реальному часі, що особливо корисно для швидкого обговорення робочих питань. Крім того, деякі з цих програм підтримують функції для проведення голосових і відеоконференцій, а також спільне використання екранів і обмін файлами. Це робить такі рішення універсальними інструментами для внутрішньої та зовнішньої комунікації в компанії.

Переваги програм для обміну повідомленнями включають можливість швидкого реагування та економію часу на налаштування довгих конференцій. Окрім цього, ці програми часто містять інструменти для управління завданнями, дозволяють більш активно залучати команди до спільної роботи і підтримують не лише ділові, але й менш формальні обговорення. Щоб забезпечити максимальний рівень безпеки, варто обирати програми з наскрізним шифруванням, що гарантує захист конфіденційних даних компанії.

Коли мова йде про стратегію обслуговування клієнтів, електронна пошта залишається одним із найважливіших інструментів для залучення та утримання клієнтів. Важливо знайти спосіб для розстановки пріоритетів серед повідомлень та оптимізації робочих процесів, що дозволяє скоротити час на відповідь

клієнтам. Такі методи допомагають командам обслуговування клієнтів працювати більш організовано та продуктивно [22].

Основні функції системи керування електронною поштою включають можливість створювати робочі групи, делегувати завдання та інтегруватися з CRM-системами для позначення повідомлень і додавання внутрішніх нотаток.

Частиною успішної стратегії електронного маркетингу є покращення показників доставки електронних листів, щоб уникнути їх потрапляння до папки спаму.

Інтернет-телефонія стала важливим елементом корпоративної співпраці, дозволяючи працівникам спілкуватися незалежно від їхнього місця розташування і залишатися на зв'язку на будь-якому пристрої. Це допомагає їм вирішувати потенційні проблеми на ранніх етапах, до того, як вони стануть серйозними [24].

Працівники можуть легко підтримувати зв'язок із клієнтами, навіть коли вони не знаходяться біля свого робочого місця, а команди мають можливість співпрацювати і знаходити творчі рішення без будь-яких обмежень. Багато VoIP-пакетів включають послуги переадресації дзвінків, що гарантує, що компанії не втратять можливість спілкування з клієнтами.

Зазвичай дзвінки між співробітниками є безкоштовними, і немає необхідності в додаткових інвестиціях у нове програмне чи апаратне забезпечення, оскільки зустрічі можуть проводитися за допомогою наявних пристроїв, із відео або без нього. Крім того, для покращення обслуговування клієнтів компанії можуть запропонувати безкоштовні телефонні номери для зручності своїх клієнтів.

Платформи для планування контенту в соціальних мережах надають можливість краще організувати співпрацю навколо вашого контенту на таких платформах, як Facebook, Twitter, Instagram та інші. Завдяки таким інструментам команди можуть працювати разом, щоб ефективно донести єдині повідомлення бренду до своєї аудиторії, включаючи клієнтів, читачів або споживачів [33].

Ці платформи також оснащені аналітичними інструментами, що допомагають командам аналізувати ефективність різних публікацій і визначати, які з них мають найбільший вплив.

Інструменти, такі як Hootsuite, створені для того, щоб сприяти командній роботі: кожен учасник команди може налаштовувати звіти під свої потреби та мати доступ до інформації, яка допомагає йому ефективно працювати. Крім того, такі платформи легко інтегруються з різноманітними зовнішніми сервісами, що дозволяє створювати цілісні маркетингові стратегії та ефективніше співпрацювати в межах однієї команди, незалежно від проєкту, наприклад, це може бути стратегія SEO для SaaS або інший напрямок маркетингу [40].

## РОЗДІЛ 3

### ПРОПОЗИЦІЇ ЩОДО ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ХМАРНИМИ ТЕХНОЛОГІЯМИ

#### 3.1 Стратегія впровадження хмарних технологій для організації

Сучасна торговельна компанія, незалежно від масштабу діяльності (від невеликого магазину до розгалуженої мережі), функціонує у висококонкурентному середовищі, що вимагає наявності ефективної та надійної інформаційно-технологічної інфраструктури. ІТ-інфраструктура виступає не лише підтримкою операційної діяльності, але й інструментом для управління бізнес-процесами, збору аналітичних даних, роботи з клієнтами та забезпечення багатоканальної торгівлі (омніканальності). Порівняємо традиційну ІТ-інфраструктуру та Хмарні технології (див. табл. 3.1).

Основні компоненти ІТ-інфраструктури середньостатистичної торговельної компанії:

Обладнання (апаратна частина): Робочі станції для касирів, адміністраторів, менеджерів; POS-термінали, касові апарати, сканери штрихкодів; Сервери для локального зберігання даних або внутрішніх систем; Мережеве обладнання: маршрутизатори, комутатори, точки доступу Wi-Fi; Відеоспостереження, системи сигналізації, електронні ваги (для роздрібно торгівлі).

Програмне забезпечення: Обліково-товарні системи (POS/Back-Office): 1С, BAS, Торгсофт, R-Keeper, Poster тощо; CRM-системи для управління клієнтськими даними, програмами лояльності; ERP-системи для управління ресурсами (зазвичай у великих компаніях); ПЗ для аналітики, складу, фінансів, документообігу; Операційні системи, офісні пакети, системи захисту (антивіруси, брандмауери).

Комунікаційна інфраструктура:

Корпоративна локальна мережа (LAN) або VPN для з'єднання віддалених об'єктів; Канали зв'язку з головним офісом, інтернет-доступ;

Телефонія (часто IP-телефонія), месенджери, електронна пошта.

Системи резервного копіювання та захисту даних: Сховища резервних копій (на локальних серверах або у хмарі); Протоколи захисту персональних даних клієнтів і фінансової інформації; Контроль доступу, журналювання подій, системи безперервності бізнесу. ІТ-персонал (або аутсорсинг): Власний ІТ-відділ (у великих компаніях) або ІТ-адміністратор; Аутсорсингові компанії, які надають техпідтримку, супровід ПЗ, хостинг.

Типові виклики для традиційної ІТ-інфраструктури - висока вартість утримання локального обладнання та оновлення ПЗ; нестача гнучкості та масштабованості при розширенні бізнесу; складність централізованого управління філіями або віддаленими точками; залежність від людського чинника в обслуговуванні; низький рівень автоматизації звітності й аналітики; Ризики втрати даних при аваріях або кібератаках.

Впровадження хмарних технологій сприяє:

### 1. Спрощенню ІТ-інфраструктури

Було: Локальні сервери, мережеві сховища, спеціалізоване обладнання; Постійна потреба в ІТ-фахівцях для обслуговування систем; Необхідність ручного оновлення програм, резервного копіювання, моніторингу.

Стає: Відмова від фізичних серверів – обчислювальні потужності та зберігання даних перенесені в хмару; Мінімізація локального ПЗ – багато систем доступні через браузер; Автоматичне оновлення та підтримка забезпечується провайдером; Менше точок відмови, зменшується складність мережевої інфраструктури.

Приклад: Замість того щоб розгортати 1С на кожному комп'ютері – компанія використовує хмарну BAS або 1С:Підприємство через SaaS-сервіс.

### 2. Оптимізації витрат

До переходу: значні капітальні витрати (CAPEX) на сервери, ліцензії, мережеве обладнання; витрати на обслуговування, електроенергію, охолодження; постійні витрати на підтримку ІТ-персоналу або аутсорс.

Після переходу:

Модель оплати за використання (Pay-as-you-go): платиш лише за обсяг зберігання, обчислення або користувачів; немає потреби в складному апаратному забезпеченні; прозоре бюджетування – зрозумілі та передбачувані щомісячні платежі; можливість масштабування без значних інвестицій.

Приклад: фізичний сервер для магазину може коштувати 30–50 тис. грн. У хмарі – це умовно 800–2000 грн/міс залежно від конфігурації.

### 3. Доступність даних 24/7 з будь-якого пристрою

Дані розміщуються в дата-центрах, які мають резервні канали живлення, Інтернету та захисту; Доступ до облікових систем, CRM, аналітики можливий через браузер або мобільний додаток; Можна працювати з будь-якої локації: офіс, віддалено, з дому, з планшета в дорозі; Надійні провайдери гарантують SLA до 99,9% доступності.

Приклад: адміністратор мережі магазинів може перевірити залишки на складах або змінити ціни навіть з телефону.

### 4. Швидка інтеграція нових сервісів

Більшість сучасних хмарних рішень підтримують API та модульну архітектуру; Можна легко додати нові функції: аналітика, онлайн-оплата, синхронізація з маркетплейсами, доставка; Можливість об'єднання з POS, CRM, ERP системами без потреби створювати все «з нуля»; Хмарні провайдери часто мають готові інтеграції (наприклад, Shopify + Google Analytics + Zoho CRM).

Приклад: інтернет-магазин на базі Shopify або Rozetka Marketplace інтегрується з Nova Poshta API, Google Ads, складською BAS-системою в кілька кліків або через стандартні модулі.

Таблиця 3.1 – Порівняльна таблиця: Традиційна ІТ-інфраструктура vs Хмарні технології

Критерій	Традиційна ІТ-інфраструктура	Хмарні технології
Витрати на обладнання	Високі капітальні витрати (сервери, СХД, мережеве обладнання)	Мінімальні початкові витрати, модель оренди (ОРЕХ)
Витрати на ПЗ	Купівля ліцензій, інсталяція, оновлення вручну	SaaS-модель, ліцензії включені, автоматичне оновлення
Підтримка та обслуговування	Потреба в штатних ІТ-фахівцях або аутсорсі	Обслуговування – на стороні провайдера
Масштабування	Складне, потребує нового обладнання	Швидке, гнучке – зміна тарифного плану, кількості користувачів
Доступ до систем	Лише з робочих місць в офісі	24/7 з будь-якого пристрою через Інтернет
Надійність і безпека	Залежить від локальної мережі, ризик втрати даних	Резервування, шифрування, дата-центри Tier 3+
Резервне копіювання	Ручне або локальне, часто ігнорується	Автоматичне, у хмарі, з історією версій
Інтеграція з іншими сервісами	Вимагає розробки або доопрацювання ПЗ	Більшість сервісів мають відкриті АРІ та модулі інтеграції
Швидкість впровадження	Від тижнів до місяців	Від кількох годин до кількох днів
Гнучкість роботи (віддалено)	Обмежена, VPN або віддалений доступ	Повна гнучкість — браузерний або мобільний доступ

### 3.2 Оптимізація управління ресурсами в хмарі

Оптимізація управління ресурсами в хмарних технологіях є важливим аспектом, що дозволяє організаціям знижувати витрати, підвищувати ефективність та забезпечувати гнучкість у використанні обчислювальних потужностей. Ефективне управління ресурсами допомагає компаніям максимально використовувати переваги хмари, забезпечуючи оптимальну продуктивність і безпеку даних [7].

Динамічне управління ресурсами в хмарних технологіях є одним із найважливіших аспектів, який дозволяє компаніям адаптуватися до змін у попиту, оптимізувати витрати та забезпечувати ефективність своїх ІТ-систем. Ось кілька способів, як організації можуть здійснювати таке динамічне управління:

### 1. Автоматичне масштабування

Автоматичне масштабування – це процес, який дозволяє системам автоматично збільшувати або зменшувати обчислювальну потужність в залежності від навантаження. Більшість хмарних провайдерів, таких як AWS, Azure та Google Cloud, надають інструменти для автоматичного масштабування. Наприклад:

– AWS Auto Scaling: ця служба дозволяє компаніям налаштувати правила, за якими ресурси автоматично додаються або видаляються на основі заданих параметрів, таких як завантаження процесора, обсяги пам'яті чи кількість запитів.

– Azure Scale Sets: дозволяють автоматично змінювати кількість віртуальних машин у залежності від фактичного навантаження.

### 2. Оптимізація використання ресурсів

Хмара дозволяє організаціям оптимізувати використання ресурсів, що допомагає уникати перевитрат. Це включає в себе:

– Моніторинг в реальному часі: за допомогою аналітичних інструментів компанії можуть відстежувати використання ресурсів у реальному часі та коригувати їх відповідно до потреб.

– Аналіз історичних даних: оцінка попередніх піків навантаження та планування ресурсів на основі отриманих даних дозволяє зменшити витрати під час періодів спаду.

### 3. Використання безсерверних технологій (FaaS)

Безсерверні обчислення (Function as a Service, FaaS) дозволяють компаніям запускати код без необхідності управління серверами. Це означає, що компанії

платять лише за виконання функцій, коли вони необхідні, що може суттєво зменшити витрати. Приклади включають:

- AWS Lambda: дозволяє запускати код у відповідь на події без необхідності управляти серверною інфраструктурою.

- Azure Functions: пропонує аналогічну можливість запускати невеликі фрагменти коду на вимогу.

#### 4. Гнучка тарифікація.

Хмарні провайдери часто пропонують гнучкі моделі тарифікації, які дозволяють компаніям платити лише за фактичне використання ресурсів. Це означає, що організації можуть вибрати різні тарифи, такі як "оплата за використання" або "знижки на передплату", що допомагає зменшити витрати:

- Пейза за використання: компанії платять лише за обчислювальні ресурси, які вони використовують, а не за заброньовані [18].

- Передплати: компанії можуть зафіксувати знижки на ресурси, якщо вони готові платити наперед за певний обсяг використання.

#### 5. Ресурси з короткостроковою орендою

Багато хмарних провайдерів надають можливість оренди ресурсів на короткий термін. Це дозволяє компаніям масштабувати свої ресурси лише на період пікових навантажень, що допомагає знизити витрати на час, коли ресурси не використовуються.

Динамічне розширення та скорочення ресурсів у хмарі дозволяє компаніям адаптуватися до змінюваних умов ринку та оптимізувати свої витрати. Використовуючи автоматичне масштабування, безсерверні технології, моніторинг в реальному часі та гнучку тарифікацію, організації можуть ефективно управляти ресурсами, уникати перевитрат і покращувати загальну продуктивність своїх бізнес-процесів. Це створює можливість для зростання та інновацій у бізнесі, зменшуючи при цьому фінансові ризики [12].

Таблиця 3.2 – Порівняння фіксованої ІТ-інфраструктури та гнучких хмарних рішень

Критерій	Фіксована ІТ-інфраструктура	Гнучкі хмарні рішення
Витрати	Високі початкові витрати на обладнання та програмне забезпечення; постійні витрати на обслуговування.	Оплата за використання; можливість знижок при передплаті.
Масштабованість	Складно та витратно масштабувати; потрібно додаткове обладнання.	Легко масштабується вгору або вниз залежно від потреб; доступні ресурси на вимогу.
Гнучкість	Обмежена гнучкість; зміни в інфраструктурі можуть вимагати значних затрат часу та ресурсів.	Висока гнучкість; швидке впровадження нових рішень та сервісів.
Управління	Вимагає постійного управління та технічної підтримки.	Можливість автоматизації управління ресурсами; знижує потребу в постійній підтримці.
Безпека	Відповідальність за безпеку покладається на компанію; можуть виникнути ризики з точки зору захисту даних.	Хмарні провайдери забезпечують високий рівень безпеки, проте відповідальність за безпеку частково лежить на користувачеві.

Автоматизація в хмарних технологіях забезпечує високий рівень гнучкості та ефективності в управлінні ресурсами (див таб. 3.2) (на рис. 3.1).



Рисунок 3.1 – Автоматизація в хмарних технологіях [3]

Це особливо важливо в умовах змінного навантаження, коли компанії повинні швидко реагувати на коливання попиту [4].

Постійний моніторинг ресурсів у хмарних середовищах є критично важливим аспектом управління IT-інфраструктурою. Він дозволяє організаціям не лише контролювати використання ресурсів, але й виявляти проблеми, оптимізувати витрати та підвищувати загальну продуктивність.

По-перше, постійний моніторинг допомагає виявляти невикористані або недозавантажені ресурси, що дозволяє компаніям зменшувати витрати. Наприклад, якщо компанія має віртуальні машини, які постійно працюють, але їх використання невелике, то їх можна вимкнути або зменшити їх обсяги. Це дає можливість знизити витрати на обслуговування хмарних ресурсів.

По-друге, моніторинг підвищує продуктивність системи. Виявлення вузьких місць є важливим для забезпечення стабільної роботи додатків. Якщо моніторинг виявляє повільну обробку запитів або недостатню пропускну здатність мережі, це дозволяє оперативно вживати заходів для стабільності роботи.

Завдяки аналізу даних, отриманих в результаті моніторингу, організації можуть прогнозувати зміни у навантаженні. Це дозволяє планувати масштабування ресурсів у відповідь на підвищення або зниження попиту, що знижує ризики перевитрат і забезпечує оптимальну продуктивність [18].

Останнім важливим аспектом є покращення безпеки. Моніторинг дозволяє виявляти аномалії, які можуть свідчити про можливі загрози або атаки. Це дає можливість швидко реагувати на інциденти безпеки та захищати дані компанії.

Одним із найбільш популярних інструментів для моніторингу є Azure Monitor. Це комплексний сервіс, який надає детальну інформацію про продуктивність додатків, віртуальних машин, контейнерів та інших ресурсів, що працюють на платформі Azure. Інструмент забезпечує збори та аналіз даних у реальному часі, дозволяючи створювати інтуїтивно зрозумілі дашборди та отримувати сповіщення про аномальні ситуації.

Ще одним потужним рішенням є Google Cloud Monitoring (раніше Stackdriver). Цей інструмент дозволяє організаціям відстежувати продуктивність своїх ресурсів на Google Cloud Platform і за її межами. Він пропонує можливість налаштування дашбордів, що відображають метрики, а також сповіщення на основі заданих умов.

Для користувачів Amazon Web Services існує AWS CloudWatch. Цей інструмент моніторингу дозволяє відстежувати різноманітні метрики, налаштовувати сповіщення і збирати журнали. CloudWatch також підтримує автоматизацію дій у відповідь на події, що відбуваються в системі, що робить його важливим для управління ресурсами.

Постійний моніторинг ресурсів у хмарних технологіях є основою для оптимізації витрат, підвищення продуктивності та забезпечення безпеки. Використання інструментів, таких як Azure Monitor, Google Cloud Monitoring та AWS CloudWatch, дозволяє організаціям ефективно управляти своїми ресурсами, швидко реагувати на проблеми та оптимізувати свої витрати в умовах динамічного бізнес-середовища.

### **3.3 Моделі кібербезпеки та захист даних в хмарних середовищах**

З розвитком хмарних технологій питання кібербезпеки та захисту даних стали надзвичайно важливими для організацій. Хмарні середовища надають величезні можливості для зберігання та обробки даних, але водночас вони несуть нові ризики та виклики в плані безпеки. Для забезпечення належного рівня захисту даних та кібербезпеки важливо впроваджувати ефективні моделі безпеки [20].

Сьогодні кібербезпека та захист даних у хмарних середовищах стали надзвичайно важливими для компаній усіх масштабів. З розвитком хмарних технологій виникає потреба в ефективних методах захисту даних, щоб запобігти несанкціонованому доступу і забезпечити конфіденційність інформації. Хмарні провайдери, такі як Amazon Web Services (AWS) і Microsoft Azure, активно

використовують шифрування для захисту даних як під час їх зберігання, так і під час передачі. (на таб. 3.3)

Одним із способів захисту даних є шифрування, коли інформація, що зберігається на серверах, перетворюється в код, який не може бути прочитаний без відповідного ключа. Наприклад, AWS пропонує AWS KMS (Key Management Service), який дозволяє створювати та керувати шифрувальними ключами. Це дуже зручно, оскільки KMS інтегрується з іншими сервісами AWS, такими як S3 і RDS, автоматично шифруючи дані, коли вони зберігаються. Це забезпечує високий рівень захисту, навіть якщо дані потраплять до рук зломисників [21].

З іншого боку, Microsoft Azure також має своє рішення – Azure Storage Service Encryption (SSE). Ця функція автоматично шифрує дані, що зберігаються в Azure Storage, за допомогою потужного алгоритму AES. Користувачі можуть бути впевнені, що їхня інформація захищена на всіх етапах – від зберігання до доступу.

Шифрування даних під час їх передачі – це ще один критичний аспект безпеки. Тут на допомогу приходять протоколи SSL/TLS, які шифрують інформацію під час передачі через мережу, щоб ніхто не міг її перехопити. AWS та Azure використовують ці протоколи для забезпечення безпечного з'єднання між клієнтами та своїми сервісами.

Наприклад, AWS VPC (Virtual Private Cloud) дозволяє створювати ізольовані мережі, які забезпечують додатковий рівень безпеки. Включення VPN (Virtual Private Network) також дозволяє шифрувати дані, що передаються через публічні мережі.

А в Azure існує Azure ExpressRoute, який забезпечує приватне з'єднання між користувачами та хмарними сервісами. Це означає, що дані передаються безпосередньо без виходу в Інтернет, що зменшує ризик їх перехоплення.

Крім шифрування, важливим аспектом безпеки є управління шифрувальними ключами. Тут хмарні провайдери також пропонують зручні рішення. Наприклад, AWS KMS дозволяє автоматизувати процес керування ключами, забезпечуючи легкий доступ до них, а також контроль над тим, хто і

коли може їх використовувати. Це дуже зручно для компаній, які прагнуть підтримувати високий рівень безпеки.

На аналогічному рівні Azure Key Vault надає централізоване сховище для зберігання шифрувальних ключів, сертифікатів та секретів. Це рішення допомагає організаціям контролювати доступ до їхніх ключів і забезпечує додатковий рівень захисту даних.

Постійний моніторинг загроз та використання інструментів для виявлення підозрілої активності – це основа безпеки в будь-якій сучасній організації. Особливо це важливо, коли йдеться про хмарні сервіси, такі як Amazon Web Services (AWS) або Google Cloud, де дані постійно передаються і змінюються.

Уявіть, що у вас є бізнес, який зберігає всю свою інформацію в хмарі. Без моніторингу, ви не знатимете, що відбувається в реальному часі. Це як залишити свій будинок відкритим і не мати камер спостереження – якщо хтось увійде, ви дізнаєтесь про це лише тоді, коли вже щось зникне [8].

Таблиця 3.3 – Інструменти безпеки та моніторингу [10]

Інструмент	Опис	Моніторинг
Фаєрволі (брандмауери)	Захищають мережу від несанкціонованого доступу, фільтруючи трафік на основі визначених правил.	Фільтрація трафіку на основі правил та протоколів
Антивірусне програмне забезпечення	Виявлення та видалення шкідливих програм, таких як віруси, трояни та інші види зловмисного ПЗ.	Постійне оновлення бази даних шкідливого ПЗ та системи регулярних перевірок
Системи виявлення та запобігання вторгненню (IDS/IPS)	Моніторинг мережевого трафіку для виявлення підозрілих дій і запобігання атакам.	аналіз мережевого трафіку для аномальних дій
Шифрування даних	Захищає конфіденційні дані шляхом їх шифрування як під час передачі, так і при зберіганні.	Контроль доступу до зашифрованих даних та використання ключів
Керування доступом та аутентифікація	Контроль доступу до інформаційних систем та забезпечення ідентифікації користувачів, багатофакторна аутентифікація (MFA).	Аудит користувачів і системи, моніторинг доступу
Резервне копіювання даних	Відновлення даних у разі втрати або пошкодження, зменшення наслідків атак, таких як програми-вимагачі.	Регулярне збереження даних та перевірка резервних копій

AWS CloudTrail і Google Cloud Security Command Center (SCC) – це інструменти, які виконують роль цих "камер спостереження" в хмарі. AWS CloudTrail записує всі дії, що відбуваються у вашій інфраструктурі AWS. Це означає, що якщо хтось увійшов у систему або змінив якісь ресурси, ви матимете точний журнал цих подій. Таким чином, якщо відбувається щось підозріле, ви це швидко помітите і зможете реагувати.

Google Cloud SCC діє подібним чином. Він постійно стежить за тим, що відбувається у вашій хмарній інфраструктурі Google і допомагає виявляти проблеми, як-от неправильно налаштовані ресурси або підозрілу активність. Якщо, наприклад, хтось намагається отримати доступ до ваших даних з невідомої локації або завантажує підозрілий файл, SCC сповістить вас про це і допоможе вжити заходів. (див таб. 3.4)

Таблиця 3.4 – Основні загрози в хмарі та інструменти для їх подолання [11, 26]

Загроза	Опис загрози	Інструменти для подолання
Несанкціонований доступ	Отримання доступу до ресурсів хмари без належної автентифікації чи права доступу	Багатофакторна автентифікація (MFA), контроль доступу через IAM (Identity and Access Management)
Конфігураційні помилки	Неправильні налаштування хмарних ресурсів, що призводять до вразливостей	Використовуйте інструменти для перевірки конфігурації, такі як AWS Config або Google Cloud SCC
Вітік даних	Незахищені або помилково налаштовані бази даних можуть спричинити втік конфіденційної інформації	Шифрування даних у стані спокою і під час передачі, моніторинг доступу до бази даних
Зловмісні дії середини	Небезпечні або недобросовісні дії працівників компанії.	Журнали аудиту дій користувачів, системи моніторингу, такі як AWS CloudTrail або Google Cloud SCC
DDoS-атаки	Перевантаження серверів хмари за допомогою великого обсягу трафіку, який можна призвести до зупинки сервісу	Системи захисту від DDoS, як-от AWS Shield або Google Cloud Armor
Компрометація облікових даних	Компрометація паролів або ключів доступу, що дозволяє зловмисникам отримати контроль над ресурсами	Використовуйте інструменти для управління обліковими даними, наприклад AWS Secrets Manager або Google Cloud Identity

Такі інструменти – це не просто зручність, а необхідність. Без них ви ризикуєте пропустити важливі сигнали, що може призвести до великих втрат даних або навіть до зупинки вашого бізнесу.

Організація може дотримуватися міжнародних стандартів безпеки, таких як GDPR (Загальний регламент захисту даних ЄС) або HIPAA (Закон США про перенесення та підзвітність медичного страхування), впроваджуючи чіткі політики захисту даних і забезпечуючи належне управління конфіденційною інформацією. Хмарні провайдери, такі як AWS, Google Cloud або Microsoft Azure, відіграють важливу роль у підтримці цих стандартів, надаючи інструменти та сервіси для управління даними відповідно до вимог.

Основні кроки для дотримання міжнародних стандартів безпеки:

1. Розробка політики безпеки:

– Організація повинна мати чітко визначені політики захисту даних, які відповідатимуть вимогам таких стандартів, як GDPR або HIPAA. Це включає зобов'язання щодо конфіденційності, збереження, обробки та передачі даних.

– Наприклад, згідно з GDPR, організації повинні отримати явну згоду користувачів на обробку їхніх персональних даних і забезпечити можливість виправлення або видалення цих даних на вимогу [7].

2. Контроль доступу до даних:

– Важливо забезпечити багатофакторну автентифікацію (MFA) та інші засоби контролю доступу для захисту від несанкціонованого доступу до конфіденційної інформації.

– Потрібно створювати журнали аудиту для відстеження всіх дій з доступом до даних, особливо до медичних записів або персональних даних.

3. Шифрування даних:

– GDPR та HIPAA вимагають шифрування даних як при їх зберіганні, так і під час передачі. Організація повинна використовувати сучасні методи шифрування для забезпечення цілісності даних та запобігання їх компрометації.

4. Управління інцидентами:

– Потрібно мати чіткий план реагування на інциденти безпеки, який дозволить швидко виявляти та реагувати на загрози. GDPR, наприклад, вимагає повідомляти про порушення даних у межах 72 годин після їхнього виявлення.

#### 5. Регулярні аудити та перевірки:

– Потрібно проводити регулярні аудити для перевірки відповідності стандартам безпеки та постійно вдосконалювати процеси безпеки. Це допоможе виявляти вразливі місця та ефективно запобігати порушенням.

Як хмарні провайдери допомагають у дотриманні вимог:

#### 1. Сертифікації відповідності:

– Провайдери хмарних послуг, такі як AWS, Google Cloud та Microsoft Azure, мають сертифікації відповідності міжнародним стандартам, включаючи GDPR та HIPAA. Це означає, що їхні хмарні сервіси вже налаштовані з урахуванням необхідних вимог щодо захисту даних [18].

– Наприклад, AWS та Google Cloud надають інструменти для відповідності HIPAA, дозволяючи організаціям зберігати та обробляти медичні записи відповідно до вимог.

#### 2. Шифрування даних:

– Хмарні провайдери забезпечують автоматичне шифрування даних на своїх платформах як при зберіганні, так і при передачі. Це дозволяє організаціям легко дотримуватися вимог щодо безпеки, визначених в GDPR та HIPAA, без необхідності налаштовувати складні механізми самостійно.

– Наприклад, AWS Key Management Service (KMS) або Google Cloud Key Management дозволяють керувати ключами шифрування і забезпечувати безпечне шифрування даних.

#### 3. Контроль доступу та автентифікація:

– Хмарні провайдери надають інструменти для управління доступом, такі як Identity and Access Management (IAM) в AWS або Cloud Identity у Google Cloud. Вони дозволяють налаштовувати доступ на основі ролей і вимагають багатофакторну автентифікацію (MFA), що відповідає вимогам GDPR та HIPAA.

– Провайдери також ведуть журнали активності користувачів і надають організаціям можливість відстежувати всі дії з доступом до даних, що є обов'язковим для відповідності GDPR та HIPAA.

#### 4. Інструменти для моніторингу та звітності:

– Хмарні провайдери надають інструменти для моніторингу, такі як AWS CloudTrail, Google Cloud Security Command Center (SCC) та Azure Security Center. Ці інструменти дозволяють відстежувати події безпеки, налаштовувати сповіщення про підозрілу активність та вести журнали для відповідності вимогам аудиту.

– Для організацій, які працюють під GDPR, це допомагає забезпечити належний рівень захисту та можливість надання звітів про порушення даних.

#### 5. Резервування даних і відновлення після катастроф:

– Провайдери хмарних послуг пропонують рішення для автоматичного резервування даних та відновлення після катастроф, що є критично важливим для відповідності стандартам безпеки, особливо для медичних організацій під HIPAA.

Для організації дотримання міжнародних стандартів безпеки, таких як GDPR і HIPAA, необхідно мати чіткі політики безпеки, шифрувати дані, контролювати доступ і регулярно проводити аудити. Хмарні провайдери допомагають у дотриманні цих вимог, надаючи готові рішення для управління конфіденційною інформацією, інструменти для шифрування, моніторингу, резервування даних і ведення журналів активності. Завдяки цим послугам організації можуть легко відповідати вимогам і забезпечувати захист своїх даних [12].

## ВИСНОВКИ

Дослідження, проведене в рамках цієї бакалаврської роботи, дало змогу всебічно вивчити теоретичні основи та практичні аспекти впровадження хмарних технологій в сучасних організаціях. В результаті аналізу основних моделей хмарних послуг – IaaS (інфраструктура як послуга), PaaS (платформа як послуга) та SaaS (програмне забезпечення як послуга) – було встановлено, що ці моделі забезпечують значну економію ресурсів, підвищення гнучкості та масштабованості бізнес-процесів, а також сприяють швидкому реагуванню на зміни у ринковому середовищі.

Завдяки впровадженню хмарних технологій, організації отримують можливість скоротити витрати на утримання фізичної ІТ-інфраструктури, оскільки знижується потреба в обладнанні та технічному персоналі. Крім того, хмарні рішення дозволяють зосередитись на стратегічних цілях і розвитку бізнесу, надаючи можливість швидко налаштовувати та розгорнути нові сервіси або програми. Особливо це актуально для малих та середніх підприємств, які можуть використовувати високоякісні ІТ-інфраструктури, не маючи значних капітальних витрат.

Однією з ключових переваг хмарних технологій є автоматизація бізнес-процесів, зокрема таких, як управління взаємовідносинами з клієнтами (CRM), управління ресурсами підприємства (ERP), управління персоналом (HRM), а також використання систем роботизованої автоматизації процесів (RPA). Дані рішення сприяють підвищенню продуктивності, ефективності управління та покращенню взаємодії з клієнтами, що є важливим для збереження конкурентоспроможності на ринку.

Окрім того, дослідження виявило важливість безпеки даних у хмарних середовищах. Було проаналізовано міжнародні стандарти, такі як GDPR та HIPAA, які визначають основні вимоги до захисту конфіденційної інформації. Хмарні провайдери, такі як AWS, Google Cloud та Microsoft Azure, надають широкі можливості для дотримання цих стандартів, включаючи такі

інструменти, як шифрування даних, контроль доступу, багатофакторна автентифікація та моніторинг активності. Ці рішення дозволяють компаніям знижувати ризики втрати або компрометації даних, забезпечуючи дотримання регуляторних вимог і стандартів безпеки.

У практичній частині роботи були розроблені рекомендації щодо поетапного впровадження хмарних технологій у бізнес–процеси організацій. Це включає:

1. Оцінку потреб компанії у хмарних рішеннях, що дозволяє визначити, які сервіси або інфраструктурні елементи мають бути перенесені в хмару.

2. Вибір відповідного хмарного провайдера, який відповідає вимогам бізнесу щодо надійності, безпеки та вартості.

3. Тестування та налаштування хмарного середовища, зокрема зосередження на налаштуванні контролю доступу, шифруванні даних та інших безпекових аспектах.

4. Масштабування ресурсів відповідно до поточних потреб організації завдяки використанню автоматизованих інструментів, таких як AWS Auto Scaling або Azure Scale Sets. Це дозволяє уникати зайвих витрат на ресурси, які не використовуються повністю.

Також було підкреслено, що автоматичне масштабування ресурсів, використання безсерверних технологій і гнучка тарифікація допомагають організаціям оптимізувати витрати на використання хмарних обчислювальних потужностей. Це дозволяє не лише підвищити ефективність, але й швидко адаптувати ресурси до змін ринку або збільшення навантаження на IT–інфраструктуру.

Отже, результати дослідження підтверджують, що впровадження хмарних технологій є важливим інструментом для підвищення продуктивності, ефективності та конкурентоспроможності сучасних організацій. Завдяки хмарним рішенням компанії можуть значно знижувати свої витрати, підвищувати гнучкість бізнес–процесів і забезпечувати високий рівень безпеки та відповідності міжнародним стандартам.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алгоритмізація та програмування. Частина 2 | Кафедра "Інформаційні системи та мережі". Головна сторінка | Кафедра "Інформаційні системи та мережі". URL: <https://ism.lpnu.ua/uk/content/algorytmizaciya-ta-programuvannya-chastyna-2???history=0&pfid=1&sample=55&ref=2> (дата звернення: 24.10.2024).
2. Воронов В. О. Використання хмарних технологій в освітньому середовищі. Welcome to – Digital Library NAES of Ukraine. URL: [https://lib.iitta.gov.ua/id/eprint/710437/1/283-293\\_Voronov.pdf???history=0&pfid=1&sample=11&ref=0](https://lib.iitta.gov.ua/id/eprint/710437/1/283-293_Voronov.pdf???history=0&pfid=1&sample=11&ref=0) (дата звернення: 24.10.2024).
3. Гнучкі інструменти спільної роботи, які допомагають адаптуватися до змін. Google Workspace. URL: <https://workspace.google.com/intl/uk/enterprise/???history=0&pfid=1&sample=35&ref=0> (дата звернення: 24.10.2024).
4. Дюлічева Ю. Ю. Упровадження хмарних технологій в освіту: проблеми та перспективи / Ю. Ю. Дюлічева // Інформаційні технології в освіті. – 2013. – № 14. – С. 58–64.
5. Єчкало Ю. В. Сервіси Google як складова частина навчального середовища з фізики / Ю. В. Єчкало // Хмарні технології в освіті : матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг – Київ – Черкаси – Харків, 21 грудня 2012 р.). – Кривий Ріг : Видавничий відділ КМІ, 2012. – С. 140.
6. Кібербезпека в хмарних сервісах: як покращити, головні загрози та інструменти захисту | Kyivstar Business Hub. Kyivstar Business Hub – корпоративний блог для бізнесу. URL: <https://hub.kyivstar.ua/articles/yak-pokrashhyty-kiberbezpeku-v-hmarah-golovni-zagrozy-ta-instrumenty-zahystu???history=0&pfid=1&sample=5&ref=2> (дата звернення: 24.10.2024).

7. Моделі хмарних сервісів: різниця між IaaS, SaaS, PaaS та приклади. SIM–Networks – Your Goals, our Tech. IT Infrastructure from German Provider. URL: <https://www.sim-networks.com/ukr/blog/cloud-computing-service-models???history=0&pfid=1&sample=23&ref=0> (дата звернення: 24.10.2024).

8. Моделі хмарних сервісів: різниця між IaaS, SaaS, PaaS та приклади. SIM–Networks – Your Goals, our Tech. IT Infrastructure from German Provider. URL: <https://www.sim-networks.com/ukr/blog/cloud-computing-service-models???history=0&pfid=1&sample=23&ref=0> (дата звернення: 24.10.2024).

9. Морзе Н. В. Педагогічні аспекти використання хмарних обчислень / Н. В. Морзе, О. Г. Кузьмінська // Інформаційні технології в освіті. – 2011. – № 9. – С. 20–29.

10. Огляд HRM: ТОП–5 кращих Human Resource Management систем для HR–ів. Пошук та найм персоналу, вакансії в Україні – Fillin. URL: <https://fillin.ua/stati/oglyad-hrm-top-5-krashchikh-human-resource-management-sistem/???history=0&pfid=1&sample=35&ref=2> (дата звернення: 24.10.2024).

11. Права суб'єкта персональних даних. Уповноважений Верховної Ради України з прав людини – Головна. URL: <https://ombudsman.gov.ua/storage/app/media/uploaded-files/prava-prava-subekta-personalnikh-danikh-1.pdf???history=0&pfid=1&sample=111&ref=1> (дата звернення: 24.10.2024).

12. Сільське господарство як послуга (FaaS): Потенціал та вичерпний посібник – agtecher: The Agri Tech Place. agtecher: The Agri Tech Place. URL: <https://agtecher.com/uk/faas-farming-as-a-service/???history=0&pfid=1&sample=79&ref=0> (дата звернення: 24.10.2024).

13. Ткачук В. В. Хмарні обчислення як основа мобільного навчання / В. В. Ткачук // Хмарні технології в освіті : матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг – Київ – Черкаси – Харків, 21 грудня 2012 р.). – Кривий Ріг : Видавничий відділ КМІ, 2012. – С. 54.

14. Топ 5 хмарних провайдерів: плюси та мінуси. IT Education Center Blog. URL: <https://itedu.center/ua/blog/sysadministration/top-5-cloud-providers-advantages-and-disadvantages/???history=0&pfid=1&sample=73&ref=0> (дата звернення: 24.10.2024).

15. Хмарні сервіси для бізнесу: що це, які бувають | Огляд п'яти рішень. Kyivstar Business Hub – корпоративний блог для бізнесу. URL: <https://hub.kyivstar.ua/articles/hmarni-servisi-dlya-biznesu-oglyad-p-yati-rishen???history=0&pfid=1&sample=79&ref=1> (дата звернення: 24.10.2024).

16. Хмарні технології 2024 – що це таке та які хмари найкращі?. UCloud. URL: <https://ucloud.ua/hmarni-tehnologiyi-shho-cze-take/???history=0&pfid=1&sample=29&ref=0> (дата звернення: 24.10.2024).

17. Хто такий хмарний провайдер і як його вибрати. blog.colobridge.net. URL: <https://blog.colobridge.net/uk/2024/02/cloud-service-provider-ua/???history=0&pfid=1&sample=73&ref=2> (дата звернення: 24.10.2024).

18. Чому хмарна безпека критично важлива для захисту даних і безпеки бізнесу? | Lead Panda Media. Медіа-проект PANDA MEDIA у сфері affiliate marketing та арбітражу трафіку | Lead Panda Media. URL: <https://leadpanda.media/blog/chomu-xmarna-bezpeka-tak-bajliva/???history=0&pfid=1&sample=5&ref=0> (дата звернення: 24.10.2024).

19. Що таке хмара? | Визначення хмари.  
URL: <https://www.cloudflare.com/ru-ru/learning/cloud/what-is-the-cloud/> (дата звернення: 22.10.2024).
20. Як хмарні технології оптимізують бізнес? | Wezom. IT-компанія повного цикла розробки програмних продуктів WEZOM – Київ, Україна.  
URL: <https://wezom.com.ua/ua/blog/integratsiya-hmarnih-tehnologiy-dlya-optimizatsiyi-biznesu-yak-tse-pratsyuje???history=0&pfid=1&sample=17&ref=2> (дата звернення: 24.10.2024).
21. 5 cloud collaboration technologies that are driving productivity. Onehub – Cloud Storage & Data Room Services – Share Files Online.  
URL: <https://www.onehub.com/blog/2020/10/20/5-cloud-collaboration-technologies-that-are-driving-productivity/> (дата звернення: 22.10.2024).
22. 6 architectural diagramming tools for cloud infrastructure. Red Hat – We make open source technologies for the enterprise.  
URL: <https://www.redhat.com/en/blog/diagramming-tools-cloud-infrastructure> (дата звернення: 22.10.2024).
23. 6 причин, чому хмарне середовище дозволяє поліпшити результати бізнесу – BDO. Міжнародна аудиторська компанія BDO – BDO.  
URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2021/6-ways-the-cloud-enables-better-business-outcomes???history=0&pfid=1&sample=47&ref=0> (дата звернення: 24.10.2024).
24. Adetunji D. Cloud Computing Abstractions – IaaS, PaaS, FaaS, and SaaS Explained. freeCodeCamp.org. URL: <https://www.freecodecamp.org/news/cloud-computing-abstractions-explained/> (дата звернення: 22.10.2024).
25. AWS: все, що потрібно знати про хмарну платформу. IT Education Center Blog. URL: <https://itedu.center/ua/blog/guides/aws-vse-shho-potribno-znati-pro-hmarnu->

platformu/???history=0&pfid=1&sample=47&ref=2 (дата звернення: 24.10.2024).

26. Cloud Architecture Diagrams: The Complete Guide | Gliffy by Perforce. Gliffy by Perforce. URL: <https://www.gliffy.com/resources/cloud-architecture-diagrams> (дата звернення: 22.10.2024).

27. Free Office 365 for Students and Educators | Microsoft Education. Your request has been blocked. This could be due to several reasons. URL: <https://www.microsoft.com/en-us/education/products/office?legRedir=true&CorrelationId=e3861708-a46d-47ac-9ccb-33a96c95cc3b?legRedir=true&CorrelationId=e3861708-a46d-47ac-9ccb-33a96c95cc3b> (дата звернення: 24.10.2024).

28. GDPR Compliance in the Cloud: Ensuring Data Security and Privacy – GDPR Advisor. GDPR Advisor. URL: <https://www.gdpr-advisor.com/gdpr-compliance-in-the-cloud-ensuring-data-security-and-privacy/> (дата звернення: 22.10.2024).

29. Guide to Cloud Compliance: HIPAA, GDPR, SOX & More. Veeam Software Official Blog. URL: <https://www.veeam.com/blog/guide-to-cloud-compliance.html> (дата звернення: 22.10.2024).

30. HIPAA vs. GDPR compliance: what's the difference?. Responsible AI and Data Solutions | OneTrust. URL: <https://www.onetrust.com/blog/hipaa-vs-gdpr-compliance/> (дата звернення: 22.10.2024).

31. How CIOs and CTOs can accelerate digital transformations through cloud platforms / J. Giemzo et al. McKinsey & Company. URL: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms> (дата звернення: 22.10.2024).

32. IaaS vs. PaaS vs. SaaS – Differences, Examples and Diagram | LeanIX. SAP LeanIX | Enterprise Architecture Transformation. URL: <https://www.leanix.net/en/wiki/apm/iaas-vs-paas-vs-saas> (дата звернення: 22.10.2024).

33. IaaS, SaaS та PaaS хмарні моделі сервісів: що це таке, порівняння та приклади – Блог Colobridge. [blog.colobridge.net](https://blog.colobridge.net/uk/2022/08/iaas_saas_paas_ua/?history=0&pfid=1&sample=17&ref=0). URL: [https://blog.colobridge.net/uk/2022/08/iaas\\_saas\\_paas\\_ua/?history=0&pfid=1&sample=17&ref=0](https://blog.colobridge.net/uk/2022/08/iaas_saas_paas_ua/?history=0&pfid=1&sample=17&ref=0) (дата звернення: 24.10.2024).

34. IBM. Що таке хмарні обчислення?. IBM – United States. URL: <https://www.ibm.com/topics/cloud-computing> (дата звернення: 22.10.2024).

35. Inc B. G. Unlock Business Productivity with Cloud-Based Automation. Leaders in Process Automation – Design, Implementation, and Support. URL: <https://www.bp-3.com/blog/unlock-business-productivity-with-cloud-based-automation> (дата звернення: 22.10.2024).

36. MyCloudIT. Here Are Some of the Benefits of Cloud Computing Automation. Unified Cloud Management and Cost Optimization | MyCloudIT. URL: <https://mycloudit.com/blog/cloud-computing-automation-benefits> (дата звернення: 22.10.2024).

37. Oteir N. Що таке віртуалізація сервера?. INTROSERV. URL: <https://introserv.com/ua/blog/shho-take-virtualizacziya-servera/?history=0&pfid=1&sample=41&ref=1> (дата звернення: 24.10.2024).

38. Rud A. Що таке віртуалізація серверів і чому вона корисна? | Блог HyperHost.UA. Український хостинг провайдер HyperHost. Купити хостинг для сайту. URL: <https://hyperhost.ua/info/uk/shho-take-virtualizaciya-serveriv-i-comu-vona-korisna/?history=0&pfid=1&sample=41&ref=0> (дата звернення: 24.10.2024).

39. The NIST Definition of Cloud Computing. NIST Technical Series Publications. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf> (дата звернення: 22.10.2024).

40. Top 8 Cloud Computing Architecture Diagrams. Visual Paradigm – Online Productivity Suite. URL: <https://online.visual->

[paradigm.com/knowledge/cloud-architecture-diagrams/top-8-cloud-computing-architecture-diagrams/](https://paradigm.com/knowledge/cloud-architecture-diagrams/top-8-cloud-computing-architecture-diagrams/) (дата звернення: 22.10.2024).

## ДОДАТОК А – ПЕРЕВАГИ ХМАР

### Cloud benefits vary by consumption models.

Increasing agility, automation, access to innovation, and scalability

Consumption model		Traditional	Lift-and-shift virtual machines			
			IaaS	PaaS	FaaS	
App- lication maturity	Application architecture	Multi-tier	Multi-tier	Fault-tolerant machine images	Loosely coupled services, using containers	Event driven, serverless, fully stateless
	Automation of app-development operating model	Traditional, bespoke development	Traditional, bespoke development	Move toward product-based, agile development	Move toward DevSecOps	Move toward proprietary, cloud-native development
Infra- structure maturity	Tenancy	Dedicated	Dedicated or shared	Dedicated or shared	Mostly shared and managed	Shared
	Hosting	Mostly on-premises, co-location	Off-premises <sup>2</sup>	Off-premises <sup>2</sup>	Off-premises <sup>2</sup>	Off-premises <sup>2</sup>
	Automation of infrastructure operating model	Basic automation, but with people-dependent processes	Basic automation, but with people-dependent processes; continuous integration	Fault-tolerant and resilient infrastructure (eg, mature auto-scaling); CI/CD <sup>3</sup>	Highly automated; default use of native managed services (eg, stateless, self-healing); CI/CD <sup>3</sup>	3rd-party orchestration; no management needed from the customer; CI/CD <sup>3</sup>
Run-rate benefits & KPIs	% productivity increase vs IT spend	Baseline	-5-0%	10-20%	20-30%	30-40%
	Time to market	Quarterly	Quarterly	Monthly to every 2 weeks	Every 2 weeks/as needed	Daily/multiple times a day
	Change vs run ratio	30:70	30:70	40:60	50:50	70:30
One-time transition costs	% transition cost vs IT spend	Baseline	10%	10-20%	20-60%	80-120%
	IT payback period <sup>1</sup> (varies by workload type)	N/A	May not pay back	1-2 years	2-3 years	2-3 years

<sup>1</sup>IT benefits only (infrastructure and application development/maintenance); does not include business-acceleration benefits.

<sup>2</sup> Primarily off-premises; can be on-premises or edge for specific regulatory, security, or network-connectivity-constrained situations.

<sup>3</sup> Continuous integration/continuous delivery.