Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)
Кафедра «Інформаційна безпека та наноелектроніка»
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)
магістра
(ступінь вищої освіти)

на тему Аналіз методів захисту інформації в системі хмарних обчислень в Україні

Виконав(ла) студент (ка) II курсу,групи БКз-812м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
ПРУДКА Н.С.
(ПРІЗВИЩЕ та ініціали)
Керівник РОМАНЕНКО С. М.
(ПРІЗВИЩЕ та ініціали)
Рецензент МАЛИЙ О.Ю.
(ПРІЗВИЩЕ та ініціали)

2023

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Факультет Інформаційної безпеки та електронних комунікацій
Кафедра Інформаційна безпека та наноелектроніка
Ступінь магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
_____ Андрій КОРОТУН
«_____» _____ 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТА(КИ)

ПРУДКОЇ Наталі Сергіївни
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проекту (роботи) Аналіз методів захисту інформації в системі хмарних обчислень в Україні, Analysis of information protection methods in the cloud computing system in Ukraine
керівник проекту (роботи) к.ф.-м.н., доцент, РОМАНЕНКО Сергій Миколайович
(науковий ступінь, вчене звання , ПРІЗВИЩЕ, ім'я, по батькові,)
затверджені наказом закладу вищої освіти від «28» листопада 2023 р № 476
2. Строк подання студентом проекту (роботи) 10 грудня 2023 р.
3. Вихідні дані до проекту (роботи) методи захисту інформації в системі хмарних обчислень в Україні

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Основи хмарних обчислень; Загрози, вразливості хмарних обчислень та по захисту; Регулювання хмарних обчислень та їх методів захисту; Визначення вартості хмарних обчислень

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) 10 рисунків (структура хмарних технологій; розмежування сфер відповідальності; калькулятори вартості хмарних сервісів). Презентація доповіді (підготовлена в Microsoft PowerPoint)

6. Консультанти розділів проекту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	РОМАНЕНКО С. М., доцент кафедри ІБтаН	04.09.23	01.12.23
Нормоконтроль	КОРОЛЬКОВ Р.Ю., доцент кафедри ІБтаН		04.12.23

7. Дата видачі завдання 04 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження	04.09.23 – 21.09.23	Виконано
2.	Дослідження основ хмарних обчислень	22.09.23 – 07.10.23	Виконано
3.	Аналіз загроз, вразливостей та рішень по захисту	08.10.23 – 20.10.23	Виконано
4.	Огляд актів щодо регулювання хмарних обчислень	21.10.23 – 17.11.23	Виконано
5.	Визначення вартості хмарних обчислень	18.11.23 – 25.11.23	Виконано
6.	Виконання графічної пояснювальної записки	26.11.23 – 03.12.23	Виконано
7.	Оформлення матеріалів магістерської роботи	04.12.23 – 10.12.23	Виконано

Студент(ка) _____ Наталя ПРУДКА
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проекту (роботи) _____ Сергій РОМАНЕНКО
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 95 сторінок, 6 таблиць, 10 рисунків, 60 джерел.

ТЕХНОЛОГІЯ ХМАРНИХ ОБЧИСЛЕНЬ, ХМАРА, ХМАРНА ІНФРАСТРУКТУРА, ХМАРНА ПОСЛУГА, ХМАРНІ РЕСУРСИ

Об'єкт дослідження – методи захисту інформації в системі хмарних обчислень в Україні.

Мета роботи – оцінка ідентифікованих загроз і вразливостей в системі хмарних обчислень, та аналіз практик у галузі захисту інформації в хмарних обчисленнях на міжнародному рівні та їх адаптація в Україні.

Методи дослідження – наукова абстракція, аналіз і синтез (для розкриття теоретичних положень), формалізація (для опису вимог щодо захисту інформації у хмарних обчисленнях) порівняння (для оцінки переваг і недоліків) та методи системного підходу.

У роботі аналізується розвиток і захист інформації в системі хмарних обчислень у світі та Україні. Розглядаються особливості регулювання хмарних обчислень в Україні

ABSTRACT

Explanatory note to the master's thesis: 95 pages, 6 tables, 10 figures, 60 sources.

CLOUD, CLOUD COMPUTING TECHNOLOGY, CLOUD INFRASTRUCTURE, CLOUD RESOURCES, CLOUD SERVICE.

Object of research is information protection methods in the cloud computing system in Ukraine.

The purpose of the work is to evaluate the identified threats and vulnerabilities in the cloud computing system, and to analyse practices in the field of information protection in cloud computing at the international level and their adaptation in Ukraine.

The research methods are scientific abstraction, analysis and synthesis (to reveal theoretical propositions), formalisation (to describe the requirements for information security in cloud computing), comparison (to assess advantages and disadvantages) and methods of a systematic approach.

The research analyses the development and protection of information in the cloud computing system in the world and Ukraine. The peculiarities of cloud computing regulation in Ukraine are considered.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ВДТ – Візуальний дисплейний термінал

ВМ - Віртуальна машина

ЄС - Європейський союз

ІТ – Інформаційні технології

ОС - Операційна система

ПЗ - Програмне забезпечення

ПК - Персональний комп’ютер

ШІ – Штучний інтелект

AWS - Amazon Web Services, дочірня компанія Amazon.com, що надає платформу хмарних обчислень в оренду приватним особам, компаніям та урядам

CaaS - Communications as a Service, зв'язок як сервіс

CEN - European Committee for Standardization, Європейський комітет зі стандартизації

CENELEC - European Committee for Electrotechnical Standardization, Європейський комітет з електротехнічної стандартизації

Cisco - Cisco Systems, Inc. — американська транснаціональна корпорація, яка є найбільшим у світі виробником мережевого обладнання, призначеного для обслуговування мереж віддаленого доступу, сервісів безпеки, мереж зберігання даних, маршрутизації та комутації

CompaaS - Compute as a Service, обчислення як послуга

CSA - Cloud Security Alliance, Альянс хмарної безпеки

DMaaS - Data Storage as a Service, зберігання даних як послуга

DMTF - Distributed Management Task Force, Робоча група розподіленого управління

ENISA - European Union Agency for Network and Information Security, Європейська агенція мереж та інформаційної безпеки

ETSI - European Telecommunications Standards Institute, Європейський інститут телекомунікаційних стандартів

GICTF - Global Inter-Cloud Technology Forum, Глобальний форум з хмарних технологій

IaaS - Infrastructure as a Service, Інфраструктура як послуга

IEC - International Electrotechnical Commission, Міжнародна електротехнічна комісія

ISO - International Organization for Standardization, Міжнародна організація зі стандартизації

ML - Machine learning, машинне навчання

NaaS - Network as a Service, мережа як послуга

NIST - National Institute of Standards and Technology, Національний інститут стандартів і технологій

OCC - Open Cloud Consortium, Відкритий хмарний консорціум

OGF - Open Grid Forum, Відкритий Грід форум

PaaS - Platform as a Service, Платформа як послуга

SaaS - Software as a Service, Програмне забезпечення як послуга

SNIA - Storage Networking Industry Association, Асоціація виробників мереж зберігання даних

SQL - Structured query language, мова структурованих запитів

TCO - Total cost of ownership, загальна вартість володіння

VM - Virtual machine, віртуальна машина

ВСТУП

Розвиток технологій і швидке зростання використання хмарних обчислень створили нові виклики для захисту інформації в Україні. Забезпечення конфіденційності, цілісності та доступності даних в системах хмарних обчислень стало надзвичайно важливим завданням, оскільки користувачі довіряють свою інформацію стороннім постачальникам хмарних послуг. У зв'язку з цим, аналіз методів захисту інформації в системах хмарних обчислень стає актуальним завданням.

Актуальність цієї теми обумовлена кількома факторами. Ріст обсягів електронної інформації, яка зберігається та обробляється в хмарних обчисленнях, створює необхідність забезпечення її надійного захисту від потенційних загроз. Швидкий розвиток технологій і кіберзагрози створюють необхідність у постійному оновленні методів та засобів захисту інформації.

Метою дослідження є аналіз методів та засобів захисту інформації в системах хмарних обчислень з метою застосування їх в Україні.

Для досягнення поставленої мети будуть розглянуті наступні питання:

- аналіз загальних вимог до захисту інформації в хмарних обчисленнях: оцінка стандартів та нормативів, які регулюють вимоги до безпеки даних в хмарних обчисленнях;

- класифікація методів та засобів захисту інформації: визначення різноманітних підходів та інструментів, які використовуються для забезпечення безпеки даних в хмарних системах;

- оцінка особливостей застосування методів захисту в українських умовах: вивчення внутрішніх вимог та специфіки українського ринку щодо захисту інформації в хмарних обчисленнях.

1 ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ

1.1 Розвиток хмарних обчислень

У шістдесятих роках XX століття почала створюватися концепція хмари.

Було запропоновано поняття величезного ресурсу, який могли б використовувати багато осіб.

Ближче до XXI століття експерти з інформаційних технологій використовували термін «хмара», щоб описати мережеві пристрої, які використовуються звичайними людьми. Наприклад, вони намагалися пояснити, що процеси обчислення та зберігання даних, які виконуються в Інтернеті, відбуваються в центрах обробки даних, відомих як «хмара».

Термін «хмара» [1] сягає корінням у телефонний зв'язок, оскільки телекомунікаційні компанії надавали схеми передачі «точка-точка» переважно для своїх клієнтів до дев'яностих років. Віртуальні приватні мережі (VPN) були введені в телефонію пізніше. Послуги, які вони надали, були такого ж рівня, але за значно нижчою ціною. Завдяки використанню перемикання каналів вони змогли оптимізувати використання мережі.

Сферу хмарних технологій вперше дослідив Дуглас Ф. Паркхілл у своїй книзі «Проблема комп'ютерної корисності» [2] в 1966 році, де він представив її особливості, порівняння їх з електроенергетикою та використання приватних, публічних та громадських моделей.

Тим не менш, інші ресурси зазначають, що хмарні обчислення існують з 1950-х років, через заяви, зроблені вченим у галузі комп'ютерних технологій Хербом Грошем. Він стверджував, що врешті - решт весь світ працюватиме на терміналах, контрольованих великими центрами обробки даних.

У 1970 році американський науковець Джозеф Ліклайдер (відомий як JCR або «Лік» у науковій та IT-спільноті) вперше висловив ідею того, що на сьогоднішній день називають обчисленням хмарних технологій. У цей період він

був відповідальним за створення ARPANET (Advanced Research Projects Agency Network - мережі Агентства передових досліджень), яка вважається початком Інтернету [1]. Мета вказаного проекту зводилася до того, щоб об’єднати людей у всьому світі в мережу, яка могла б надавати їм не лише дані та програми, але й інші форми інформації.

Думку про надання обчислювальної потужності як послуги (сервісу) споживачам запропонував Джон Маккарті, другий американський вчений з інформатики [1].

Однак датою сучасної комп'ютерної історії є 2006 рік, коли Amazon представила свою інфраструктуру Інтернет-послуг, яка змогла забезпечити користувача не тільки хостингом, але й віддаленими обчислювальними можливостями клієнта. Новинку прийняли такі гіганти, як Google, Sun та IBM, і в 2008 році Microsoft заявила про свою зацікавленість у цій галузі [3].

Хмарні технології пропонують масштабовану інфраструктуру та програмне забезпечення без прямого підключення до фізичних машин, заощаджуючи при цьому витрати, енергію сервера та простої.

Хмарні технології - це здатність декількох фізичних серверів бути одним обчислювальним середовищем. Як правило, хмарні обчислення - це програми, доступ до яких здійснюється через Інтернет через браузер або інші мережеві програми, такі як FTP-клієнт.

Основна відмінність від звичайного методу роботи з програмним забезпеченням полягає в тому, що користувач не використовує ресурси свого комп’ютера або сервера своєї локальної мережі і потужність, що надається йому як послуга Інтернету.

Користувач має повний доступ до власних даних та можливість працювати з ними з будь-якої точки світу та з будь-якого пристрою, але він не турбується управлінням операційною системою, програмним забезпеченням, обчислювальною потужністю, з якою відбувається ця робота.

Зберігання в хмарі не тільки даних, але і додатків змінює обчислювальну парадигму на традиційну модель клієнт-сервер, в якій веб-сайт користувача підтримує мінімально необхідну функціональність. Тож необхідність інсталювати необхідні оновлення програмного забезпечення, перевірку вірусів та інші заходи технічного обслуговування покладається на постачальника хмарних послуг. Це також означає, що обмін даними, редагування версій та редагування стають набагато простішими, ніж коли програми та дані розміщуються на власних ПК.

Найширше використовуваним визначенням хмарних обчислень є визначення Національного інституту стандартів і технологій США (NIST): «Хмарні обчислення – це модель для забезпечення повсюдного зручного мережевого доступу на вимогу до спільного пулу конфігурованих обчислювальних ресурсів (наприклад, мережі, сервери, сховища, програми та служби), які можна швидко надати та вивільнити з мінімальними зусиллями адміністратора або через взаємодію з постачальником послуг» [4].

Подібне визначення хмарних обчислень було наведено в міжнародному стандарті ISO/IEC 17788:2014: «Хмарні обчислення – це парадигма для забезпечення мережевого доступу до масштабованого та еластичного пулу фізичних або віртуальних ресурсів з наданням самообслуговування і адмініструванням на вимогу» [5].

Як визначено NIST, хмарні обчислення - це модель зручного мережевого доступу до загального фонду обчислювальних ресурсів (наприклад, мереж, серверів, файлів даних, програмного забезпечення та послуг), яку можна швидко забезпечити з мінімальними зусиллями управління та взаємодії з постачальником.

Хмарні обчислення - це розподілена обчислювальна технологія, при якій ресурси та потужність комп’ютера стають доступними користувачеві як веб-служба, тобто робоча станція на віддаленому сервері. Наприклад, якщо ви використовуєте електронну пошту на веб-сайті служби (наприклад, gmail), який дозволяє вам використовувати цю електронну пошту або обробку зображень вашого браузера через Picasa, ви використовуєте хмарну службу.

Хмарні сервіси - послуги, що надають користувачеві доступ до мережі до масштабованого та гнучко організованого пулу розподілених фізичних або віртуальних ресурсів, що надаються в режимі самообслуговування та адміністрування на його запит (наприклад, програмне забезпечення, дисковий простір, обчислювальна потужність тощо).

Терміни "хмарна технологія" / "хмарний сервіс" із їхнім загальноприйнятим графічним поданням у формі "хмар" лише заплутують користувачів, адже їх структуру можна легко зрозуміти, якщо уявити її такою пірамідою, як на рисунку 1.1.

Основою піраміди - «інфраструктура» - є набір фізичних пристроїв (сервери, жорсткі диски тощо), вона побудована на «платформі» - наборі послуг, а зверху - програмному забезпеченні, що надається на запит.

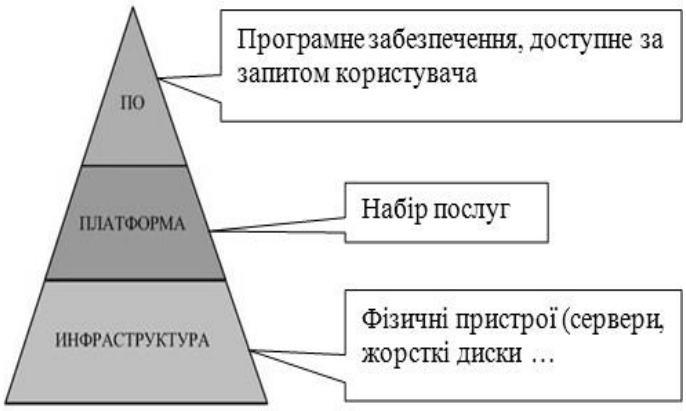

Рисунок 1.1 - Структура хмарних технологій

Хмарні обчислення - це певний основний вектор, отриманий в результаті синтезу ряду технологій та підходів.

Хмарні технології - це набір інструментів, які виконують обчислення за допомогою віддалених серверів та програм без безпосереднього залучення комп'ютерних ресурсів користувача. Не виключено, що в майбутньому комп’ютери матимуть лише один мікропроцесорний екран, і всі обчислення та потужність будуть розташовані та виконуватися віддалено на хмарних серверах.

Забезпечення декількох рівнів безпеки в «хмарі» забезпечує надійність інформації, що зберігається в службі. Технології цього типу популярні не тільки серед компаній, але також використовуються для державних цілей.

Україна також розглядає можливість використання «хмарних» послуг.

17 лютого 2022 року було прийнято Закон «Про хмарні послуги», який набрав чинності 19 вересня 2022 року. У вказаному законі визначено ряд термінів: технологія хмарних обчислень, хмара (хмарна інфраструктура), хмарна послуга, хмарні ресурси.

Технологія хмарних обчислень - технологія забезпечення дистанційного доступу на вимогу користувача до хмарної інфраструктури через електронні комунікаційні мережі.

Хмара (хмарна інфраструктура) - сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних.

Хмарна послуга - послуга з надання хмарних ресурсів за допомогою технології хмарних обчислень.

Хмарні ресурси - будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких забезпечують технології хмарних обчислень, зокрема процесорний час (обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп’ютерні програми [5].

П'ять основних компонентів визначаються еталонною архітектурою хмарних обчислень NIST, як показано на рисунку 1.2: споживач хмарних послуг, постачальник хмарних послуг, передавач хмарних послуг, аудитор хмарних послуг і брокер хмарних послуг. Транзакція, процес або завдання в хмарних обчисленнях виконується суб’єктом (фізичною особою, організацією), яким є кожен учасник.

Рисунок 1.2 - Еталонна модель

У таблиці 1.1 коротко перераховані суб'єкти, визначені в еталонній архітектурі хмарних обчислень NIST.

Таблиця 1.1 - Суб’єкти в хмарних обчисленнях [4].

Суб’єкт	Визначення
Споживач хмарних послуг	Особа або організація, яка підтримує ділові відносини та використовує послуги Постачальників хмарних послуг.
Постачальник хмарних послуг	Особа, організація або суб'єкт, відповідальний за доступність послуг для зацікавлених сторін
Аудитор хмарних послуг	Сторона, яка може проводити незалежну оцінку хмарних послуг, операцій інформаційної системи, продуктивності та безпеки впровадження хмарних послуг
Брокер хмарних послуг	Суб’єкт, який керує використанням, продуктивністю і доставкою хмарних послуг, а також веде переговори про відносини між постачальниками хмарних послуг та споживачами хмарних послуг

Кінець таблиці 1.1

Суб’єкт	Визначення
Передавач хмарних послуг	Посередник, який надає можливість підключення та передавання хмарних сервісів між постачальниками хмарних послуг та споживачами хмарних послуг

Закон України «Про хмарні послуги» визначає, що в Україні учасниками відносин у сфері хмарних послуг є:

- користувач хмарних послуг, включаючи публічного користувача;
- надавач хмарних послуг;
- надавач послуг центру обробки даних;
- органи державної влади.

Особливістю Закону України «Про хмарні обчислення» є те, що органи державної влади розглядаються і як публічний користувач хмарних послуг, і як частина системи державного управління і регулювання при наданні хмарних послуг. А саме, стаття 1 Закону України «Про хмарні послуги» містить термін публічний користувач хмарних послуг (далі - публічний користувач). Це орган державної влади, орган влади Автономної Республіки Крим, орган місцевого самоврядування, державне підприємство, державна установа, державна організація чи інший суб’єкт владних повноважень або інший суб’єкт, якому делеговані такі повноваження. Стаття 5 цього ж закону встановлює організаційну систему державного управління і регулювання при наданні хмарних послуг. Ця система складається з Кабінету Міністрів України; регулятора комунікаційних послуг; центрального органу виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг; органу, уповноваженого здійснювати контроль за додержанням законодавства про захист персональних даних; Міністерства оборони України; Національного банку України; Центральної виборчої комісії [6].

NIST визначає хмарні обчислення як такі, що мають п’ять ключових особливостей.

По перше - якість самообслуговування на вимогу (англ. on-demand self-service). Це означає, що клієнт може приймати самостійні рішення щодо обчислювальних потреб, таких як доступ до даних і швидкість обробки, а також обсяг збережених даних, без необхідності взаємодії з представником постачальника послуг.

По друге, доступ до послуг, що пропонуються через мережі передачі інформації, є універсальним (англ. broad network access). Тобто коли доступ надається через усі термінальні пристрої, незалежно від типу.

Наступна особливість (англ. resource sharing) - ступінь об’єднання ресурсів. Використовуючи багатокористувальницьку модель, яка містить різноманітні фізичні та віртуальні ресурси, які динамічно розподіляються та перерозподіляються між різними користувачами відповідно до попиту, постачальник послуг об’єднує ресурси для обслуговування більшої кількості клієнтів. У цей момент клієнт не може визначати місце знаходження ресурсу, але може надати альтернативне розташування на вищому рівні абстракції (наприклад, на основі визначення «країни», штату або центру обробки даних). Такі ресурси включають сховища даних, обчислювальну потужність, пам’ять і пропускну здатність мережі.

Четверта особливість (англ. rapid elasticity) – це достатня еластичність, що означає, що послуги можуть бути надані, розширені або звужені в будь-який момент часу без додаткових витрат на взаємодію з постачальником, як правило, автоматично. Для клієнтів такі можливості провайдера здаються безмежними, оскільки вони можуть надавати послуги в будь-який момент.

Остання особливість (англ. measured service) - облік споживання, коли хмарний сервіс використовує вимірювання на певному рівні абстракції, щоб автоматично керувати та оптимізувати використання ресурсів користувачами. Ці вимірювання включають обсяг збережених даних, пропускну здатність, кількість

користувачів і кількість транзакцій. Прозорість забезпечується як для постачальника, так і для споживача послуг за допомогою можливості управління ресурсами, контролю над використанням ресурсів і звіту з споживання [4].

1.2 Переваги та недоліки хмарних обчислень

Основною перевагою використання хмарних обчислень, яка є базою технології, є балансування робочого навантаження, що дозволяє використовувати ресурси обчислювальної системи більш ефективно. Основні переваги технологій включають:

- здатність отримати доступ до ресурсів у хмарі за допомогою Інтернет-з’єднання, звичайного браузера та невимогливого терміналу кінцевого користувача;

- швидко запускати власні сервіси та/або збільшити обсяг роботи існуючого постачальника хмарних послуг;

- реалізація самовідновлення, масштабування та резервування для підвищення надійності системи та мінімізації потенційних ризиків у разі збоїв програмного та апаратного забезпечення;

- моніторинг виконання завдань у режимі реального часу, включаючи пакетні операції та фонові програми, які взаємодіють з користувачами;

- відстеження у режимі реального часу завантаження, балансу системи та розподілу ресурсів [7].

- вищий рівень економічної продуктивності: хмарні обчислення стають все більш популярними серед компаній, оскільки потребують менше початкових інвестицій, ніж будь-яка локальна технологія. Завдяки наявності великого простору для зберігання в хмарі можна заощадити гроші та ресурси;

- мобільність: за наявності Інтернету всі хмарні служби доступні працівникам, незалежно від місцезнаходження працівників;

- необмежений обсяг пам’яті. Хмара постачається з майже необмеженою ємністю для зберігання, яку можна розширити в будь-який час за дуже номінальну щомісячну плату;

- простоте використаннія: більшість хмарних платформ оснащено інтуїтивно зрозумілу панель керування, яку можна використовувати для підключення ресурсів, коли це потрібно [8].

Хмарні обчислення пропонують такі переваги для гарантування захисту даних:

- експертні робітники: для досягнення високого рівня безпеки, хмарний провайдер наймає спеціалістів з інформаційної безпеки, які зосереджені тільки на питаннях гарантування хмарної безпеки (що не можливо забезпечити у маленьких компаніях);

- централізоване управління, налаштування системи безпеки і оцінка її роботи;

- стійкість платформ: конфігурація апаратного та програмного забезпечення платформ з більшою одноманітністю розгортання хмари порівняно з традиційними обчислювальними центрами полегшує автоматизацію завдань перевірки безпеки, виявлення помилок і виправлення у елементах платформ;

- існування ресурсів: підвищеної стійкості проти атак типу «відмова в обслуговуванні», а також швидкого відновлення після серйозних інцидентів можна досягти за допомогою існуючої можливості динамічного масштабування, резервування та аварійного відновлення;

- резервне копіювання та відновлення: на відміну від традиційних центрів обробки даних, постачальники хмарних послуг можуть забезпечити більший рівень резервного копіювання та відновлення, а також забезпечити зберігання резервних копій за географічними вимогами;

- мобільність кінцевого споживача: хмарна архітектура дозволяє клієнтам отримувати доступ до основних обчислювальних ресурсів через різні пристрої з мінімальною обчислювальною потужністю, доступом до Інтернету, браузером та/або кількома встановленими додатками;

- консолідація даних: у певних ситуаціях хмара може забезпечити більший рівень безпеки, ніж зберігання даних на мобільних пристроях, вбудованих пристроях або на знімних носіях, оскільки вона забезпечує центральне розташування для зберігання та обробки всіх даних.

Крім перелічених переваг існують недоліки та проблемні питання, які гальмують впровадження хмарних обчислень, а саме:

- робота з хмарними службами вимагає постійного підключення до Інтернету та мережевих з'єднань. Щоб скористатися перевагами хмарних обчислень, компанії потрібен надійний і безперебійний Інтернет-сервіс, а також швидке з'єднання та пропускна здатність;

- перехід або заміна одного надавача хмарних послуг на іншого може бути складним або не здійсненим завданням;

- не існує єдиної глобальної нормативно – правової бази щодо хмарних обчислень і обробки інформації;

- довіра до постачальника послуг користувачів;

- проблеми із забезпеченням безпеки даних користувачів, які оброблені і збережені у хмарі [7];

- час зупинення роботи: він рахується одним із суттєвих недоліків хмарних обчислень. У постачальника хмарних послуг можуть виникати технічні збої через відключення електроенергії, низький рівень підключення до Інтернету та зупинки центру обробки даних. Це може призвести до призупинення роботи у споживачів послуг;

- блокування постачальника хмарних сервісів: переміщення компанії з однієї хмарної платформи на іншу може призвести до значних проблем. Це може статися через суттєві відмінності між платформами провайдерів . Перехід може

призвести до проблем з підтримкою сервісів, збільшенням витрат споживачів. Також під час міграції конфіденційні дані компанії також можуть залишатися доступними для атак.

З точки зору безпеки даних, недоліки використання хмарних обчислень включають:

- ускладнена система: загальна хмара набагато складніша, ніж звичайний центр обробки даних. Атаки можуть виконуватися на різних рівнях абстракції через велику кількість компонентів у хмарі. Окрім загальних обчислювальних компонентів, таких як розгортання додатків, монітори віртуальних машин, гостьові віртуальні машини та зберігання даних, існують також елементи керування, такі як самообслуговування, облік ресурсів, керування квотами, реплікацію даних і відновлення, моніторинг рівня обслуговування, управління навантаженням;

- спільне середовище для багатьох користувачів: головним недоліком публічної хмари є те, що споживачі розподіляють ресурси та компоненти з особами, які їм не відомі на логічному рівні, що може дозволити зловмисникам, користуючись вразливостями у хмарі, здолати систему розподілу ресурсів між користувачами для отримання несанкціонованого доступу до даних;

- через уніфікацію програмного та апаратного забезпечення платформи, один недолік може виникнути у всій хмарі та вплинути на всіх споживачів сервісу;

- користування Інтернетом: незахищена Інтернет-мережа використовується хмарними службами та програмами для адміністрування та керування програмами. Коли компанія переходить на використання хмарних обчислень, її внутрішні захищені мережі та ресурси стикаються з новими типами інформаційних небезпек, які вимагають вирішення. Крім того, необхідне віддалене адміністрування за допомогою незахищеного каналу передачі даних;

- втрата контролю: коли користувачі використовують сервіси хмари, вони передають контроль над інформацією хмарному постачальнику, що утворює

додатковий ризик для безпеки даних. Особа може втратити як логічний, так і фізичний контроль над інформацією, оскільки вона залежить від провайдера хмари [7].

1.3 Види послуг, що надаються хмарними сервісами

Згідно з визначеннями наведеними NIST визначено наступні послуги, що можуть надаватися за допомогою хмарних сервісів:

- інфраструктура як сервіс (Infrastructure as a Service або IaaS);
- платформа як сервіс (Platform as a Service або PaaS);
- програмне забезпечення як сервіс (Software as a Service або SaaS).

Необхідно більш детально розглянути кожну модель.

Інфраструктура як сервіс (Infrastructure as a Service, IaaS) – можливість надана споживачу, яка полягає в забезпеченні обробки, зберігання, мережі та інших основних обчислювальних ресурсів, де споживач може розгортати і запускати довільне програмне забезпечення, яке може включати операційні системи і прикладні програми.

Споживач не управляє та не контролює основу хмарної інфраструктури, однак контролює операційні системи, сховища, розгорнуті прикладні програми, та, можливо, обмежено контролює деякі мережеві компоненти (наприклад, основні фаєрволи) [4].

Даний підхід полягає в тому, що виділяється інфраструктура на вимогу, наприклад, кілька віртуальних машин, на які можна встановити будь-які операційні системи. Замовник сам налаштовує маршрутизацію, балансування навантаження, бази даних і т.д. Йому просто виділяють інфраструктуру, що працює в датацентрі, про місце положенні якого замовник ніяким чином не може знати.

IaaS складається з трьох основних компонентів:

- апаратні засоби (сервери, системи зберігання даних, клієнтські системи, мережеве обладнання і т.д.);

- операційні системи та системне ПЗ (засоби віртуалізації, автоматизації, основні засоби управління ресурсами);

- зв’язне ПЗ (наприклад, для управління системами).

IaaS заснована на технології віртуалізації, що дозволяє користувачеві обладнання ділити його на частини, які відповідають поточним потребам бізнесу, тим самим збільшуючи ефективність використання наявних обчислювальних потужностей.

Користувач повинен буде оплачувати лише реально необхідні йому для роботи серверний час, дисковий простір, мережеву пропускну здатність і інші ресурси. Крім того, IaaS надає в розпорядження клієнта весь набір функцій управління в одній інтегрованої платформі. Однією з головної цінності для бізнесу моделі IaaS, є процес вивантаження завдань в хмару в період необхідності максимальної кількості обчислювальних ресурсів. У цьому випадку досягається непогана економія, за рахунок того, що підприємствам не потрібно вкладати кошти в придбання додаткових серверів, завантажених на 70% потужності двічі або тричі на рік, а в решту часу працюють з символічним навантаженням.

Приклади IaaS сервісів: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (Compute Engine), CenturyLink Cloud, VMware vCloud Air, IBM(SoftLayer), Niche Players, Rackspace Managed Cloud, DigitalOcean, Linode, OpenStack Cloud Software [8].

Платформа як сервіс (Platform as a Service, PaaS) – можливість, надана споживачу, яка полягає у розгортанні на хмарній інфраструктурі прикладних програм, створених або отриманих користувачем з використанням мов програмування та інструментів, наданих постачальником.

Споживач не управляє та не контролює основу хмарної інфраструктури, включаючи мережу, сервери, операційні системи, сховища, але контролює

розгорнуті прикладні програми та, можливо, налаштування середовища розміщення прикладних програм [4].

Рішення PaaS наймолодша модель хмарних сервісів. Суть PaaS рішень в тому, що виділяється не набір простих віртуальних машин, а ціла платформа. Це дозволяє не думати який стоїть сервер, а просто розробити і розгорнути свій додаток в хмарі. Унікальність PaaS полягає в тому, що вона дозволяє розробникам створювати і розгортати додатки на пропонованої інфраструктурі. Іншими словами, PaaS дозволяє скористатися практично безмежними обчислювальними ресурсами хмарної інфраструктури. Існуючі сьогодні PaaS-рішення настільки різноманітні за характером вирішуваних завдань, що виділити їх родове властивість досить важко. Якщо говорити в загальному, то все PaaS-рішення дозволяють підвищити ефективність праці розробників додатків [9]. Двома головними компонентами PaaS є обчислювальна платформа і стек рішень. Обчислювальна платформа в своєму простому вигляді являє собою місце, де може без проблем працювати програмне забезпечення, якщо воно відповідає стандартам цієї платформи. Типовими прикладами платформ є: Windows, OS X і Linux для операційних систем; Google Android, Windows Phone і iOS для мобільних обчислень [10]. Приклади PaaS сервісів: Amazon Web Services, Salesforce.com(Force.com, Heruko), Microsoft Azure, IBM Smart Cloud, RedHat OpenShift, LongJump, Cloud Foundry, Google App Engine, CloudBees, Engine Yard та інші [8].

Програмне забезпечення як сервіс (Software as a Service, SaaS) – можливість, надана споживачу, яка полягає у використанні прикладних програм постачальника, працюючих на хмарній інфраструктурі. Прикладні програми доступні з різних клієнтських пристроїв через інтерфейс тонкого клієнта, такого як веб-браузер (наприклад, веб-пошта). Споживач не управляє та не контролює основу хмарної інфраструктури, включаючи мережу, сервери, операційні системи, сховища або навіть окремі можливості прикладної програми, з можливим виключенням або обмеженням специфічних для користувача налаштувань

конфігурації прикладної програми [4]. Сервіс за запитом, коли користувач взагалі нічого не робить в плані налаштування, а тільки споживає. Найстарша різновид хмарних послуг, що з'явилася раніше, ніж сам термін хмарні обчислення. З усіх хмарних рішень тільки SaaS додатки безпосередньо доступні кінцевому користувачеві, і цим вони принципово відрізняються від рішень класу IaaS і PaaS, які спрямовані не на користувачів, а на розробників і власників IT-систем. SaaS надає дешевий спосіб використання програмного забезпечення – використання на вимогу замість покупки ліцензії на кожен комп'ютер, особливо коли більшість комп'ютерів не використовується майже 70-80% часу. SaaS «хмари», безліч різних обчислювальних ресурсів, які створюють загальний обчислювальний кластер, здатний виконувати велику кількість примірників програмного забезпечення, необхідного для обслуговування клієнтів по всьому світу.

SaaS - системи займають стійкі позиції в сфері корпоративних рішень класу CRM і ERP. Використання електронної пошти за моделлю SaaS дозволяє заощадити на зарплаті системного адміністратора, а бухгалтерські SaaS сервіси дозволяють малим компаніям економити на зарплаті бухгалтера і співробітників, що займаються обліком. Хоча ці системи і не можуть конкурувати в повній мірі з традиційним бухгалтерським програмним забезпеченням, вони дозволяють вирішувати більшу частину повсякденних завдань, з якими стикаються індивідуальні підприємці, а також істотно підмога бухгалтерам, які працюють за сумісництвом. Одна з багатообіцяючих тенденцій розвитку SaaS додатків – це взаємна інтеграція різних SaaS - сервісів, що забезпечує комбінацію функціональних можливостей. Яскравим прикладом SaaS додатки – Office 365 від Microsoft. Це єдине хмарне пропозиція, що містить настільний пакет Office, доступний за передплатою і інструменти для спільної роботи – портал, обмін повідомленнями, об'єднані комунікації. Розгорнуте рішення не вимагає обслуговування з боку IT-фахівців і витрат на дороге серверне обладнання, тому Office 365 особливо привабливий для компаній, які прагнуть скласти з себе непрофільні IT-витрати. Приклади SaaS сервісів: Google Apps(Gmail, Docs, Sheets,

Slides, Forms), Microsoft Office 365, Salesforce, Amazon Web Service, DropBox, LinkedIn, Exact Online, Outlook Web Access, Adobe Creative, Google Analytics, JIRA [8].

Прийняттям у 2023 році міжнародним стандартом ISO/IEC 22123-1:2023 (E) [11] регламентовано сім категорій хмарних послуг. Стандарт ISO/IEC 22123-1:2023 замінює стандарт ISO/IEC 22123-1:2021 та ISO/IEC 17788:2014, які відкликані.

Окрім IaaS (Infrastructure as a Service – Інфраструктура як послуга), PaaS (Platform as a Service – Платформа як послуга), SaaS (Software as a Service – Програмне забезпечення як послуга), ISO/IEC 22123-1:2023 (E) виділяються наступні категорії:

- CaaS (Communications as a Service – Зв'язок як сервіс) категорія хмарних сервісів, в якій можливість, що надається клієнту хмарного сервісу взаємодія та співпраця в режимі реального часу;

- CompaaS (Compute as a Service – Обчислення як послуга) категорія хмарних сервісів, в якій можливості, що надаються замовнику хмарного сервісу, є надання та використання обчислювальних ресурсів, необхідних для розгортання та запуску програмного забезпечення;

- DSaaS (Data Storage as a Service – Зберігання даних як послуга), категорія хмарних послуг, в якій можливість, що надається клієнту хмарних послуг, полягає у наданні та використанні сховища даних та пов'язаних з ним можливостей;

- NaaS (Network as a Service – Мережа як послуга), категорія хмарних поссуг, в якій можливості, що надаються клієнту хмарної служби, є транспортне підключення та пов'язані з ним мережеві можливості.

В Україні стаття 3 Закону «Про хмарні послуги» встановлює наступні види хмарних послуг і формулює їх визначення:

- інфраструктура як послуга - хмарна послуга, що полягає у наданні користувачу хмарних послуг обчислювальних ресурсів, ресурсів зберігання або систем електронних комунікацій за допомогою технології хмарних обчислень;

- платформа як послуга - хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до інфраструктури та наборів комп'ютерних програм (операційних систем, системних комп'ютерних програм, програмних засобів для комп'ютерного програмування, програмних засобів управління базами даних) за допомогою технології хмарних обчислень;

- програмне забезпечення як послуга - хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до прикладних комп'ютерних програм за допомогою технології хмарних обчислень через онлайн-сервіс або комп'ютерні програми-агенти;

- безпека як послуга - послуга з кіберзахисту, що надається користувачу хмарних послуг з використанням хмарних ресурсів;

- інші послуги, що відповідають визначенню хмарних послуг.

Слід пам'ятати, що різні види хмарних послуг пропонують різні рівні автономії.

Рисунок 1.3 - Розмежування сфер впливу споживачів і провайдерів у розрізі основних послуг

1.4 Класифікація хмарних сервісів

Із марними обчисленнями також пов’язані моделі розгортання хмарного середовища. Під моделлю хмарного розгортання (англ. cloud deployment model) розуміють спосіб організації хмарних обчислень на основі контролю та спільного використання фізичних або віртуальних ресурсів [12].

Зазвичай, до моделей розгортання хмари належать:

- приватна хмара (англ.private cloud);
- громадська хмара (англ. community cloud);
- публічна хмара (англ.public cloud);
- гібридна хмара (англ.hybrid cloud).

Приватна хмара – це хмарна інфраструктура, що обслуговує тільки одну організацію, яка містить з кілька користувачів (приміром, декілька підрозділів).

Управління, експлуатація та право власності на приватну хмару можуть належати як організації, так і третій стороні (або деякій комбінації обох).

Така хмара може фізично знаходитися в юрисдикції власника або поза нею.

Приватна хмара, на відміну від публічної передбачає, що вся обчислювальна інфраструктура знаходиться під повним контролем самої організації. По суті, мова йде про гнучку, глибоко віртуалізовану платформу, ресурси якої знаходяться в розпорядженні однієї компанії. Фактично, мова йде про гнучку, глибоко віртуалізовану платформу, ресурси якої можуть використовувати лише одна організація. IT - інфраструктура може фізично розташовуватися в дата-центрі користувача або за його межами. Немає значення, де вона розташована. Не є рідкістю ситуація, коли приватна хмара складається з мережі з кількох корпоративних дата-центрів.

Приватна хмара має цілий перелік переваг порівнянно з публічною платформою. Наприклад, через те що обчислювальні ресурси розташовані в мережі організації, вона забезпечує більш високу швидкість роботи. Це може бути

важливим, особливо при роботі з потужними аналітичними системами або інструментами інженерного моделювання, при роботі з професійною графікою. Приватна хмара також, як прийнято вважати, пропонує найвищий рівень кібербезпеки, оскільки дані не виходять за межі традиційного внутрішнього периметра безпеки. Але треба враховувати, що насправді існує достатня кількість загроз для внутрішньої мережі. Крім того, використання приватних хмар може бути пов’язане з певними законодавчими положеннями, такими як заборона передачі персональних даних до сторонніх центрів обробки даних. Коли справа доходить до приватної хмари, ідеально, щоб вона була розташована на території компанії, що обслуговується, керована та контрольована персоналом цієї компанії.

Публічна хмара — це хмарна інфраструктура, призначена для вільного використання широким загалом. Публічна хмара може належати, керуватися та експлуатуватися комерційними, академічними (освітніми та дослідницькими) або державними організаціями. Публічна хмара знаходиться в юрисдикції постачальника хмарних послуг.

Найпоширенішим підходом до надання хмарних послуг є публічна хмара. У цьому сценарії IT - інфраструктура постачальника послуг повністю знаходиться в його компетенції. Оператор купує та управляє орендою серверів, систем зберігання даних, мережевого обладнання, ліцензій на програмне забезпечення та забезпечує поточне обслуговування.

При цьому сервіс-провайдер надає хмарні послуги великій кількості незалежних замовників, які спільно використовують одну і ту ж IT-інфраструктуру, що знаходиться під його керуванням і контролем. Компанія-клієнт в свою чергу отримує доступ до необхідного обсягу IT-ресурсів за певну абонентську плату. Абонентом пропонованих сервісів може стати будь-яка організація або особа. Вони пропонують легкий і доступний за ціною спосіб розгортання веб-сайтів або бізнес-систем, з великими можливостями масштабування, які в інших рішеннях були б недоступні. Приклади: онлайн

сервіси Amazon EC2 і Simple Storage Service (S3), Google Apps / Docs, Salesforce.com, Microsoft Office Web. У цьому випадку можна провести аналогію з офісами – коворкінгами, де клієнтам передається в користування зручний робочий простір, але вони мають ділитися ним з сусідами по поверху, яких вони не можуть обирати.

Гібридна хмара – це хмарна інфраструктура, яка складається з двох або більше окремих хмарних інфраструктур (приватних, громадських або публічних), які залишаються окремими об'єктами, але поєднані між собою стандартизованими або приватними технологіями, які дозволяють переміщувати дані та прикладні програми (наприклад, використання загальнодоступних хмарних ресурсів для розподілу навантаження між різними хмарами).

У більшості випадків, і останнім часом все частіше, необхідно, щоб як приватні, так і публічні хмари співіснували в одній IT-системі. Ця вимога може бути реалізована за допомогою гібридної хмари, яка об'єднує переваги двох попередніх методів. Публічна хмара забезпечує гнучкість, тоді як приватна хмара забезпечує кращий контроль ресурсів і високу безпеку. У цьому випадку, дата-центр, який контролює компанія, відповідає за найважливішу частину IT-інфраструктури. Менш важливі додатки можуть бути передані публічним операторам. Гібридний підхід передбачає, що вся хмарна інфраструктура функціонує як одна система під загальним централізованим управлінням. У ідеальному випадку це буде схоже на однорідний віртуальний пул, який дозволяє динамічно виділяти ресурси відповідно до потреб, повністю відповідно до внутрішніх правил безпеки та політик доступу. Великі компанії, яким доводиться регулярно взаємодіяти з великою кількістю зовнішніх користувачів, особливо потребують гібридної хмари.

Це можуть бути, наприклад, банки, держструктури, великі майданчики онлайн-торгівлі, авіакомпанії і безліч інших організацій.

Часто такий тип хмар використовується, коли організація має сезонні періоди активності, іншими словами, як тільки внутрішня IT-інфраструктура не

справляється з поточними завданнями, частина потужностей перекидається на публічну хмару (наприклад великі обсяги статистичної інформації, які в необробленому вигляді не являють цінності для підприємства), а також для надання доступу користувачам до ресурсів підприємства (до приватної хмари) через публічну хмару.

Громадська хмара (англ. community cloud) – це хмарна інфраструктура, призначена для використання конкретною спільнотою споживачів із організацій, які мають спільні цілі (наприклад, місію, вимоги щодо безпеки, політику та відповідність різним стандартам). Громадська хмара може перебувати у спільній власності, керуванні та експлуатації однієї чи більше організацій зі спільноти або третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Стаття 3 Закону «Про хмарні послуги» встановлює, що марні послуги в Україні надаються в один із таких способів:

- приватна хмара - хмарна інфраструктура, що підготовлена для використання єдиним користувачем хмарних послуг та контролюється ним;

- колективна хмара - хмарна інфраструктура, що поділена між визначеною групою взаємопов’язаних користувачів хмарних послуг, які мають спільні потреби, та контролюється користувачами хмарних послуг самостійно або їх представниками;

- публічна хмара - хмарна інфраструктура, що потенційно доступна для невизначеного кола користувачів хмарних послуг та контролюється надавачем хмарних послуг;

- гібридна хмара - хмарна інфраструктура, що є композицією з двох або більше різних хмарних інфраструктур (приватні, колективні або публічні), що є самостійними об’єктами, пов’язаними між собою технологіями, що дозволяють переносити дані або комп’ютерні програми між цими об’єктами [6].

1.5 Висновки до першого розділу

У світі розвиток хмарних технологій триває вже кілька десятиліть, з першими спробами створення віртуальних хмарних інфраструктур в 2000-х роках. У цей час хмарні обчислення значно поліпшили швидкість доступу до обчислювальних ресурсів та зменшили витрати на обладнання та обслуговування.

Україна почала розвивати регулювання хмарних технологій. Прийнятий закон "Про хмарні послуги" встановлює ключові терміни та норми, визначає правовий статус провайдерів та користувачів хмарних послуг, а також регулює важливі аспекти стосовно кібербезпеки, захисту даних та ліцензування.

Одночасно змінюється регулювання хмарних технологій на міжнародному рівні, наприклад прийняття міжнародного стандарту ISO/IEC 22123-1:2023, який надає регламентацію для сімох категорій хмарних послуг. Цей стандарт створює загальний мовник для хмарних обчислень, визначаючи структуру та ключові характеристики хмарних послуг.

Українське законодавство впроваджує різноманітні типи хмарних інфраструктур, такі як приватні, колективні, публічні та гібридні хмари, що надає підприємствам можливість обирати найбільш підходящий варіант для розгортання та управління їхніми IT-системами в залежності від конкретних потреб.

Публічні хмари є найпопулярнішою моделлю надання хмарних послуг, надаючи доступ до обчислювальних ресурсів для широкого кола користувачів. Вони спрощують розгортання веб-сайтів та бізнес-систем, забезпечуючи великий рівень масштабування.

Гібридні хмари дозволяють комбінувати переваги публічних та приватних хмар, що особливо актуально для великих організацій та підприємств зі змінними потребами щодо обчислювальних ресурсів та безпеки.

Громадські хмари, спрямовані на конкретні спільноти споживачів, надають можливість спільному використанню інфраструктури відповідно до спільних цілей та вимог.

Однак важливо враховувати і переваги, і недоліки хмарних обчислень. Переваги включають в себе широкий доступ до обчислювальних ресурсів, зниження витрат на обладнання та обслуговування, а також високий рівень масштабування та гнучкості. Проте існують і певні недоліки, включаючи питання приватності та безпеки даних, обмежену багатофункціональність для певних застосувань та залежність від доступу до мережі. Ці фактори варто розглядати при виборі використання хмарних обчислень залежно від конкретних потреб та вимог.

У майбутньому розвиток хмарних обчислень в Україні та світі матиме великий вплив на бізнес-процеси, IT-інфраструктуру та кібербезпеку. Використовуючи хмарні послуги, організації зможуть ефективно розширювати свої можливості, знижувати витрати та підвищувати рівень кібербезпеки.

Хмарні технології продовжують активно розвиватися, і ми можемо очікувати подальшого зростання їхньої популярності як в Україні, так і в світі.

Розвиток видів послуг, що надають хмарні сервіси, може відбуватися в кількох напрямках:

- розширення функціональності інфраструктури. Постачальники хмарних послуг можуть працювати над розширенням спектру обчислювальних ресурсів, включаючи обробку великих даних, інші спеціалізовані сервіси, які дозволять користувачам здійснювати ще більше видів діяльності в хмарному середовищі;

- підвищення безпеки і конфіденційності. Оскільки безпека є однією з основних перешкод для прийняття хмарних послуг, постачальники будуть надалі розвивати технології та стандарти забезпечення конфіденційності та безпеки даних;

- розширення географії інфраструктури. Розгортання діцентрів у різних частинах світу дозволить покращити доступність та швидкість обслуговування для користувачів у різних географічних областях;

- розвиток інтеграції з іншими технологіями. Хмарні послуги будуть інтегруватися з іншими технологіями, такими як штучний інтелект, Інтернет речей, блокчейн тощо, для створення більш інноваційних та комплексних рішень;

- зростання спеціалізованих сервісів. З'являться нові види хмарних сервісів, спеціалізовані для конкретних галузей, такі як охорона здоров'я, фінанси, освіта тощо;

- розширення ринку для індивідуальних користувачів. Більше індивідуальних користувачів зможуть використовувати хмарні послуги для особистих потреб, таких як зберігання фотографій, відео та інших файлів;

- розширення послуг для розвитку бізнесу. Виникнуть нові хмарні рішення для підтримки бізнесу, такі як інструменти для аналітики даних, управління відносинами з клієнтами, електронна комерція тощо;

- розвиток хмарних послуг відбувається відповідно до попиту користувачів та технологічних можливостей. Постачальники постійно працюють над інноваціями, щоб задовольнити зростаючі потреби у зручних та продуктивних хмарних рішеннях.

2 ЗАГРОЗИ ВРАЗЛИВОСТІ ХМАРНИХ ОБЧИСЛЕНЬ ТА РІШЕННЯ ПО ЗАХИСТУ

2.1 Загрози і вразливості хмарних обчислень

В роботі [13] визначено безпеку хмарних обчислень як «піддомен комп'ютерної безпеки, мережевої безпеки та, ширше, інформаційної безпеки. Це стосується широкого набору політик, технологій і елементів керування, які застосовуються для захисту даних, додатків і відповідної інфраструктури хмарних обчислень».

До того як вивчати конкретні загрози, вразливості та рішення, пов'язані з хмарними середовищами, наведемо визначення вразливості та загрози.

Будь-яке потенційне пошкодження активів організації, операцій або системної інформації внаслідок вразливості можна класифікувати як загрозу.

Законом України «Про основні засади забезпечння кібербезпеки України» використовується поняття «вразливість» до кібератак, але визначення цьому терміну не надано. Будь-яка слабкість інформаційної системи, процедур системної безпеки, внутрішнього контролю або реалізації, яка може бути використана або викликана ресурсами загроз, називається вразливістю [14].

Співвідношення загрози та вразливості у кібербезпеці хмарних обчислень визначається численними факторами, включаючи конкретний тип хмарної інфраструктури, структуру додатків, контролюючі механізми, технічні рішення та багато інших.

Перекладаючи критично важливі дані і застосунки організації на хмарні сервіси, треба враховувати їх різні істотні вразливості, основні характеристики хмари, відомі засоби контролю безпеки і найактуальніші хмарні пропозиції.

У таблиці 2.1 наведено короткий опис вразливостей.

Таблиця 2.1 - Аналіз вразливостей у хмарних обчисленнях

D	Вразливості	Опис
01	Незахищені інтерфейси та API	Хмарні провайдери пропонують послуги, до яких можна отримати доступ через API (SOAP, REST або HTTP з XML/JSON) [15]. Безпека хмари залежить від безпеки цих інтерфейсів [16]. Деякі проблеми:
		a) Слабкі облікові дані
		b) Недостатні перевірки авторизації
		c) Недостатня перевірка вхідних даних
		Крім того, хмарні API все ще незрілі, що означає, що вони часто оновлюються. Виправлена помилка може створити ще одну дірку в безпеці програми [17].
02	Необмежений розподіл ресурсів	Неточне моделювання використання ресурсів може призвести до надмірного резервування або надмірного виділення ресурсів [18].
03	Вразливості, пов’язані з даними	a) Дані можуть бути розміщені разом із даними невідомих власників (конкурентів або зловмисників) із слабким розділенням [19].
		b) Дані можуть знаходитися в різних юрисдикціях з різним законодавством [20, 17, 21].
		c) Неповне видалення даних – дані не можуть бути повністю видалені [20,22 - 24].
		d) Резервне копіювання даних, виконане ненадійними сторонніми постачальниками [24,25].
		e) Інформація про місцезнаходження даних зазвичай недоступна або не розкривається користувачам [23].
		f) Дані часто зберігаються, обробляються та передаються у вигляді відкритого тексту

Продовження таблиці 2.1

D	Вразливості	Опис
04	Вразливості у віртуальних машинах	a) Можливі приховані канали в спільному розміщенні віртуальних машин [26 - 28].
		b) Необмежений розподіл і звільнення ресурсів за допомогою віртуальних машин [25].
		c) Неконтрольована міграція – віртуальні машини можна перенести з одного сервера на інший через відмовостійкість, балансування навантаження або технічне обслуговування обладнання [15, 29].
		d) Неконтрольовані снапшоти (знімки файлової системи) – віртуальні машини можна копіювати для забезпечення гнучкості [30], що може призвести до витоку даних.
		e) Неконтрольований відкат (англ. Rollback) може призвести до скидання вразливостей - віртуальні машини можуть створити резервну копію до попереднього стану для відновлення [29], але оновлення та виправлення, застосовані після попереднього стану, зникають.
		f) Віртуальні машини мають IP-адреси, видимі будь-кому в хмарі – зловмисники можуть визначити, де знаходиться цільова віртуальна машина в хмарі (хмарна картографія [27]).
05	Вразливості в образах віртуальних машин	a) Неконтрольоване розміщення образів ВМ у загальнодоступних репозиторіях [31].
		b) Образ VM неможливо виправити, оскільки вони є неактивними артефактами [29].

Кінець таблиці 2.1

D	Вразливості	Опис
06	Вразливості в гіпервізорах	a) Складний код гіпервізора [31].
		b) Можна використовувати гнучку конфігурацію віртуальних машин або гіпервізорів для задоволення потреб організації.
07	Вразливості у віртуальних мережах	Спільне використання віртуальних мостів кількома віртуальними машинами [33].

Цей аналіз зосереджується головним чином на технологічних вразливостях, однак існують інші вразливості, які є спільними для будь-якої організації, і їх слід враховувати, оскільки вони можуть негативно вплинути на безпеку хмари та її базової платформи.

Деякі з цих вразливостей.

Відсутність перевірки працівників і недосконала практика найму на роботу – деякі хмарні постачальники можуть не проводити перевірку своїх співробітників або постачальників. Привілейовані користувачі, наприклад адміністратори хмари, зазвичай мають необмежений доступ до даних хмари.

Відсутність перевірки репутації клієнта – більшість хмарних провайдерів не перевіряють репутацію своїх клієнтів, і майже кожен може відкрити обліковий запис за допомогою дійсної кредитної картки та електронної пошти. «Несправжні» облікові записи можуть дозволити зловмисникам виконувати будь-які зловмисні дії, не будучи ідентифікованими.

Відсутність освіти з безпеки – люди продовжують залишатися слабкою стороною в інформаційній безпеці. Це справедливо для будь-якого типу організації; однак у хмарі це має більший вплив, оскільки з хмарою взаємодіє більше людей [34]. З таблиці 2.1 можна зробити висновок, що зберігання та віртуалізація даних є найбільш критичними, і атака на них може завдати

найбільшої шкоди. У таблиці 2.2 наведено огляд загроз у хмарних обчисленнях. Як і в таблиці 2.1, тут також описуються загрози, пов'язані з технологіями, що використовуються в хмарних середовищах. Ми приділяємо більше уваги загрозам, які пов'язані з віддаленим зберіганням і обробкою даних, спільним використанням ресурсів і використанням віртуалізації.

Таблиця 2.2 - Огляд загроз у хмарних обчисленнях

D	Загрози	Опис
01	Викрадення облікового запису	Крадіжка облікового запису може бути здійснена різними способами, такими як соціальна інженерія та слабкі облікові дані. Якщо зловмисник отримує доступ до облікових даних користувача, він може виконувати зловмисні дії, такі як доступ до конфіденційних даних, маніпулювати даними та перенаправляти будь-які транзакції [16].
02	Видалення даних	Оскільки дані не можуть бути повністю видалені, якщо пристрій не знищено, зловмисники можуть відновити ці дані [18,23].
03	Витік даних	Витік даних відбувається, коли дані потрапляють у чужі руки під час їх передачі, зберігання, аудиту чи обробки [16, 18, 22, 27].
04	Відмова в обслуговуванні	Цілком можливо, що зловмисник забере всі можливі ресурси. Таким чином, система не може задовольнити жодного запиту від інших законних користувачів через недоступність ресурсів.
05	Маніпуляції з даними клієнтів	Користувачі атакують веб-додатки, маніпулюючи даними, які надсилаються з компонента їхньої програми до програми сервера [22]. Наприклад, впровадження SQL, впровадження команд, незахищені прямі посилання на об'єкти та міжсайтовий сценарій.

Кінець таблиці 2.2

D	Загрози	Опис
06	VM escape (вихід)	Він призначений для використання гіпервізора, щоб взяти під контроль базову інфраструктуру. У комп'ютерній безпеці, вихід віртуальної машини — це процес, коли програма вивається з віртуальної машини, на якій вона працює, і взаємодіє з операційною системою хоста [31].
07	VM hopping (Перехід з однієї віртуальної машини на іншу віртуальну машину)	Це трапляється, коли віртуальна машина може отримати доступ до іншої віртуальної машини (тобто, використовуючи деяку вразливість гіпервізора) [18].
08	Створення шкідливої віртуальної машини	Зловмисник, який створює дійсний обліковий запис, може створити образ віртуальної машини, що містить шкідливий код, такий як троянський кінь, і зберегти його в репозиторії провайдера [22].
09	Небезпечна міграція віртуальної машини	Жива міграція віртуальних машин надає доступ до вмісту файлів стану віртуальної машини мережі. Зловмисник може виконувати такі дії: a) Незаконний доступ до даних під час міграції [22]. b) Передача віртуальної машини на ненадійний хост [15]. c) Створення та перенос кількох віртуальних машин, що спричиняють збої або DoS.
10	Перехоплення/підробка віртуальних мереж	Шкідлива віртуальна машина може прослуховувати віртуальну мережу або навіть використовувати ARP-спуфінг для перенаправлення пакетів від/до інших ВМ [31].

Джерела загроз можуть бути як зовнішніми, так і внутрішніми.

У хмарній системі є наступні слабкі точки:

- гіпервізор – це програмне забезпечення, яке можна використовувати для запуску кількох віртуальних машин на одній фізичній машині. Віртуалізоване середовище покладається на гіпервізор для забезпечення надійного захисту. Будь-які проблеми, що торкаються гіпервізору, вплинуть на всі віртуальні машини, що працюють на його основі;

- сервер/консоль керування. Атака на цей об'єкт призведе до повного знищення хмарної інфраструктури;

- віртуальні машини та програми. Найбільш чутливий аспект, оскільки користувачі безпосередньо з ним взаємодіють. Запуск загрози на віртуальній машині може спричинити негативні наслідки ланцюжка на сервер управління та інші віртуальні машини;

- шкідливі інтерфейси та API. У випадку, якщо користувачі використовують шкідливі програми, хмарна система, яка не має інструментів для аналізу коду та програм, може постраждати від виконання таких програм;

- вразливість автентифікації та перехоплення трафіку (сервісів). Найчастіше ця проблема виникає через погані канали зв’язку та погане шифрування передачі. Це можна усунути за допомогою сучасних криптографічних алгоритмів.

При оптимізації системи хмарних обчислень насамперед необхідно визначити, де та які механізми захисту показуватимуть найбільшу ефективність.

Треба враховувати джерело загроз:

- зовнішні зловмисники;
- зловживання користувачів;
- зловмисні інсайдери;
- техногенні причини.

Способи реалізації загрози:

- традиційні атаки на програмне забезпечення;

- атаки на клієнта;
- атаки на гіпервізор;
- атаки на сервери хмари;
- розповсюдження загроз по ланцюгу;
- атаки аутентифікації DDoS-атаки;
- атаки бокового каналу (SideChannel), клас атак, який спрямований на вразливості у реалізації криптосистеми.

Вразливі крапки системи:

- гіпервізор;
- консоль управління;
- віртуальна машина і додаток;
- небезпечні інтерфейси та API;
- неякісні канали зв’язку.

Наслідки реалізації загроз: втрата та виток даних, порушення програм, недоступність сервісів, порушення структури системи.

2.2 Рішення щодо захисту від загроз безпеки хмарних обчислень

Найбільшими організаціями, які сьогодні зосереджені на безпеці в хмарах, є Альянс хмарної безпеки (Cloud Security Alliance, CSA), до якого входять представники IT-індустрії, та дві державні організації в Європі і Сполучених Штатах Америки: Європейська агенція мереж та інформаційної безпеки (ENISA), Національний інститут стандартів і технологій (NIST). Кожна організація сформувала документ для класифікації всіх поточних проблем інформаційної безпеки в хмарах.

CSA була заснована в 2008 році як некомерційна організація великими IT-компаніями, такими як Google, Microsoft, IBM, Salesforce. com і VMware, що були

зацікавлені у впровадженні хмарних технологій. «Керівництво із безпеки критичних областей для хмарних обчислень» є основним ресурсом, який описує проблеми безпеки, пов’язані з хмарою.

Основною метою діяльності Європейського агентства з мережної та інформаційної безпеки (ENISA) є підвищення колективної спроможності Європейського Союзу, держав-членів ЄС і бізнес-спільноти для запобігання або усунення проблем мережевої та інформаційної безпеки.

Документ «Безпека хмарних обчислень та оцінка ризиків» був створений організацією ENISA, де детально описуються виклики інформаційної безпеки в хмарі, включаючи її переваги та недоліки, поточні ризики (включаючи потенційні небезпеки) та можливі рішення для їх зменшення або усунення.

Уряд Сполучених Штатів Америки доручив NIST створити стандарт безпеки та конфіденційності для публічних хмар, щоб запровадити хмарні обчислення. Починаючи з 2011 року NIST опублікував серію документів, які містили інформацію про хмарні обчислення, досліджували проблеми безпеки хмари, пропонували шляхи усунення існуючих ризиків. Документи NIST, такі як «Посібник з безпеки та конфіденційності в громадських хмарних обчисленнях» [7] і «Короткий огляд хмарних обчислень і рекомендації», містять огляд проблем безпеки хмари.

Можна виділити основні методи захисту інформації в сфері хмарних обчислень.

Таблиця 2.3 - Методи захисту інформації в сфері хмарних обчислень [36]

Методи	NIST	CSA
Криптографічні методи		
Управління кіберінцидентами	+	
Управління ідентифікацією	+	+

Кінець таблиці 2.3

Методи	NIST	CSA
Системи управління інформаційною безпекою	+	
Оцінка інформаційної безпеки IT-систем		+
Мережева інформаційна безпека		+
Автоматизований і неперервний моніторинг інформаційної безпеки		
Гарантований супровід програмного забезпечення		+
Управління ризиками	+	+
Система інженерії інформаційної безпеки		

Розглянемо детальніше деякі методи захисту.

Одним із основних підходів до реалізації хмарної інфраструктури є технологія віртуалізації – надання обчислювальних ресурсів, абстрагованих від їх реальної апаратної реалізації, наприклад, одночасне використання декількох, ізольованих одна від одної, операційних систем (ОС) і додатків на одному комп'ютері. Сукупність комп'ютерних ресурсів, що емулює роботу окремих компонентів апаратного або програмного забезпечення (ПЗ), або комп'ютера, прийнято називати віртуальною машиною (ВМ). Наявність декількох ВМ на одному реальному комп'ютері забезпечує можливість незалежної роботи на одному фізичному сервері (вузлі) декількох операційних систем і додатків.

На даний час існує дві основні технології створення систем хмарних обчислень шляхом віртуалізації серверів. У першому підході віртуалізація здійснюється за допомогою гіпервізора – програмної надбудови над основною ОС, яка відокремлює віртуальні машини від сервера і в міру необхідності динамічно виділяє обчислювальні ресурси для кожної ВМ (Amazon, Azure, VMWare).

Другий підхід має переваги з точки зору обчислювальної продуктивності системи і економії дискових ресурсів завдяки використанню контейнерами ядра основної системи. При цьому користувачі обмежені в виборі ОС виключно дистрибутивами сімейства GNU/Linux, що в більшості випадків сприймається як суттєвий недолік контейнерної віртуалізації. Водночас, суттєвий виграш у продуктивності дозволяє в даному випадку використовувати ресурси хмари навіть для високоефективних обчислень . Останні роки Amazon і Azure, крім традиційної віртуалізації на основі гіпервізора, почали надавати послуги на основі контейнерних технологій . Google використовували дану технологію спочатку як основну. Другим недоліком до недавнього часу були серйозні проблеми в безпеці: оскільки кожен контейнер має доступ до ядра основної системи, то потенційний зловмисник міг отримати привілейовані права в основній системі, зламавши один з контейнерів у хмарі. Слід зазначити, що в останніх розробках системи віртуалізації LXC з'явилася можливість запускати непривілейовані контейнери, зламавши які зловмисник отримає тільки обмежені права користувача в основній системі.

Однак принципи віртуалізації містять потенційні загрози інформаційній безпеці хмарних обчислень, наприклад, пов'язані з використанням загальних сховищ даних різними ВМ. Кожна ВМ зберігається у вигляді образу, який являє собою окремий файл. Розміри цих файлів можуть бути змінені в залежності від поточних потреб користувача сервісу. Зменшення розміру розділу однією з ВМ хмари і збільшення розділу іншої можуть привести до того, що фізичні сектори, що містять інформацію про віддалені файли, перемістяться з однієї ВМ на іншу. В результаті користувач другої ВМ може отримати доступ і відновити дані, які раніше належали іншій організації. Одним із можливих рішень є шифрування всієї інформації. В цьому випадку зашифрована інформація не зможе бути відновлена без відповідних ключів. Однак слід враховувати, що шифрування може призвести до використання додаткових обчислювальних ресурсів і значно уповільнювати процес читання і запису даних.

ВМ динамічні. Вони клонуються і можуть переміщатися між фізичними серверами. Дана мінливість впливає на розробку цілісності системи безпеки. Однак уразливості ОС або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються через деякий проміжку часу (наприклад, при відновленні з резервної копії). У середовищі хмарних обчислень важливо надійно зафіксувати стан захисту системи, незалежно від її місця розташування. Сервери хмарних обчислень і локальні сервери використовують одні й ті самі ОС і додатки. Для хмарних систем висока загроза віддаленого злому або зараження шкідливим ПЗ.

Система виявлення та запобігання вторгненням повинна бути здатною виявляти шкідливу активність на рівні ВМ, незалежно від їх розташування в хмарному середовищі. Навіть коли ВМ вимкнена, вона також наражається на небезпеку зараження. Для цього цілком достатньо доступу до сховища образів ВМ через мережу. При цьому на вимкненій ВМ неможливо запустити захисне програмне забезпечення. В даному випадку має бути реалізованим захист не тільки всередині кожної ВМ, а й на рівні гіпервізора.

При використанні хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що менш захищена частина мережі визначає загальний рівень захищеності. Для розмежування сегментів з різними рівнями довіри в хмарі ВМ повинні самі забезпечувати себе захистом, переміщаючи мережевий периметр до самої ВМ. Корпоративний firewall (міжмережевий екран) – основний компонент для впровадження політики IT-безпеки і розмежування сегментів мережі – не в змозі вплинути на сервери, розміщені в хмарних середовищах .

Стандартно виділяють три основні завдання інформаційної безпеки: конфіденційність, цілісність і доступність . Конфіденційність – це приховування інформації і ресурсів. Цілісність – це достовірність даних або ресурсів, зазвичай пов'язана із запобіганням будь-яких некоректних або неавторизованих змін. Доступність визначається здатністю використовувати інформацію або ресурси.

Принципово вважається, що доступ до даних можуть отримати тільки особи, що пройшли аутентифікацію в якості клієнта сервісу і власника саме цих даних. Один з основних моментів, який необхідно враховувати стосовно безпеки в хмарі, полягає в тому, що відповідальність за використання ресурсів поділяється між клієнтом і постачальником хмарного сервісу. І необхідно розуміти, де закінчується відповідальність провайдера хмарних обчислень і починається відповідальність клієнта. При побудові складних систем (різновидом яких є хмари) застосовують архітектурну концепцію багаторівневої безпеки (Defense-in-Depth) – механізм, який використовує кілька рівнів захисту, щоб збільшити витрати часу атакуючого на злам системи, а також підрахувати кількість спроб зламу для прийняття рішення про блокування атакуючого. Відповідно при побудові системи безпеки середовища хмар також можна виділити свої шари контролю та доступу. Хмара комбінує можливості користувача і постачальника, брандмауери і різновиди способів ізоляції. При цьому окремі елементи безпеки можуть контролюватися користувачем незалежно від провайдера . Для того, щоб створити більш безпечне середовище хмарних обчислень, організації можуть почати з простих кроків, наприклад, з розробки політики та процедури безпеки, підвищення прозорості у використанні хмарних додатків, платформ та інфраструктури і захисту даних з шифруванням і посиленням процедури доступу до елементів управління, таких як багатофакторна аутентифікація. IT-організації повинні зосередитись на посиленні контролю доступу користувачів методом багатофакторної аутентифікації. Це ще більш важливо для компаній, які дають третім сторонам і постачальникам доступ до своїх даних у хмарі. Багатофакторні рішення аутентифікації, керовані централізовано, забезпечать більш безпечний доступ до всіх програм і даних, незалежно від того, чи знаходяться вони в хмарі або в локальній мережі.

Найбільш ефективним і універсальним способом забезпечення захисту даних, їх конфіденційності і цілісності – це використання шифрування даних при їх передачі по інформаційних мережах і при зберіганні всередині хмари.

Наприклад, в керівництві по інформаційній безпеці, розробленому Альянсом хмарної безпеки, стверджується, що шифрування надає переваги найменшої залежності як від провайдера хмарного сервісу, так і від експлуатаційних помилок. Захист даних, заснований на шифруванні, робить ці дані марними для будь-якої особи, що не має ключів для їх дешифрування. І не важливо, знаходяться ці дані в процесі передачі або зберігання, вони залишаються захищеними. Власник ключів шифрування підтримує безпеку даних і приймає рішення, кому і до яких даних надавати доступ. Процедура шифрування може бути вбудована в існуючий робочий процес хмарних сервісів. Наприклад, адміністратор може зашифровувати всі дані резервного копіювання перед відправкою їх в хмарне сховище. Співробітник організації може захистити корпоративну інтелектуальну власність, перш ніж покласти її в приватну хмару. Представник компанії може зашифрувати особисті контракти клієнтів, перш ніж відправити їх в спільне робоче місце в публічній хмарі [37].

В статті 14 Закону України «Про хмарні послуги» визначено тільки загальні принципи захист інформації при наданні хмарних послуг та/або послуг центру обробки даних.

Надавач хмарних послуг та/або послуг центру обробки даних забезпечує та створює належні умови для захисту даних у системі хмарних обчислень у порядку, визначеному законодавством України та договором між сторонами.

На вимогу користувача хмарних послуг та/або у порядку, визначеному договором, надавач хмарних послуг та/або послуг центру обробки даних надає інформацію щодо захисту інформації в системі хмарних обчислень від внутрішніх та зовнішніх загроз, кібератак [6].

Таким чином, в Україні кожен учасник хмарних обчислень за допомогою умов договору може застосувати будь –які рішення та міжнародний досвід щодо захисту від загроз безпеки.

2.3 Майбутнє хмарних обчислень та підвищення ефективності захисту хмарних сервісів

Gartner знову прогнозує ще більше зростання витрат на загальнодоступні хмарні сервіси, згідно з останніми цифрами, які передбачають зростання на 20,7 відсотка у 2023 році, доводячи витрати до 591,8 мільярдів доларів США, а витрати кінцевих користувачів досягнуть майже 600 мільярдів доларів США у 2023 році.

Програмне забезпечення як послуга (SaaS) залишається найбільшим сегментом ринку публічних хмарних послуг, витрати кінцевих користувачів на які у 2023 році, за прогнозами, досягнуть 195,2 мільярдів доларів США. Подібним чином очікується зростання інфраструктури як послуги (IaaS) із 115,7 мільярдів доларів США у 2023 році. 2022 року до прогнозованих 150,2 мільярдів доларів США у 2023 році. Хмарні провайдери також отримують прибуток від нових технологій у хмарних обчисленнях, таких як гіпермасштабовані периферійні обчислення та безпечний доступ. Згідно з оцінками звіту «Дослідження та ринки» за 2022 рік, розмір глобального ринку обчислювальних платформ може сягнути 1240,9 мільярдів доларів США до 2027 року, причому IaaS, ймовірно, зростатиме на 22,5 відсотка на рік.

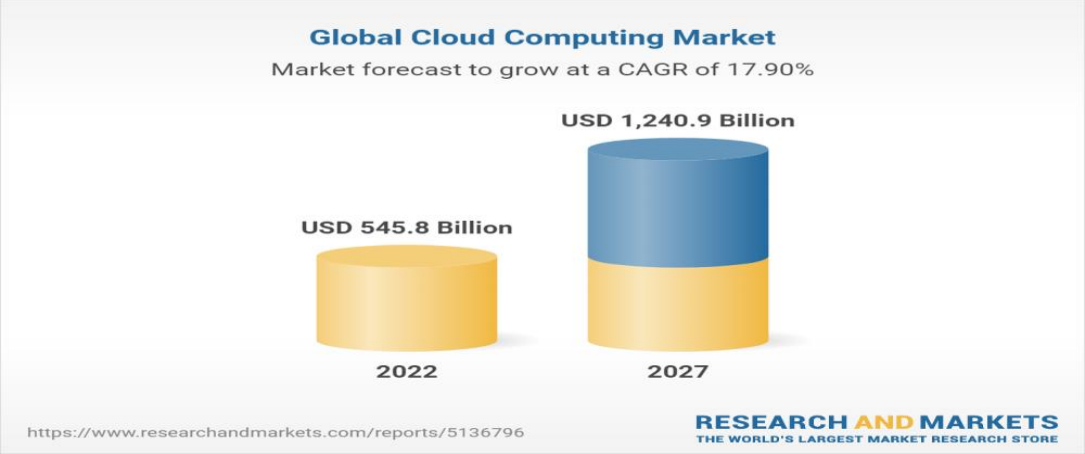

Рисунок 2.1 - Розмір глобального ринку обчислювальних платформ

Опитування користувачів Flexera вказує на те, що сегмент гібридної хмари є найбільшим внеском у загальний розмір ринку хмарних обчислень: 24 відсотки всіх респондентів інвестують у використання виключно публічної хмари [38].

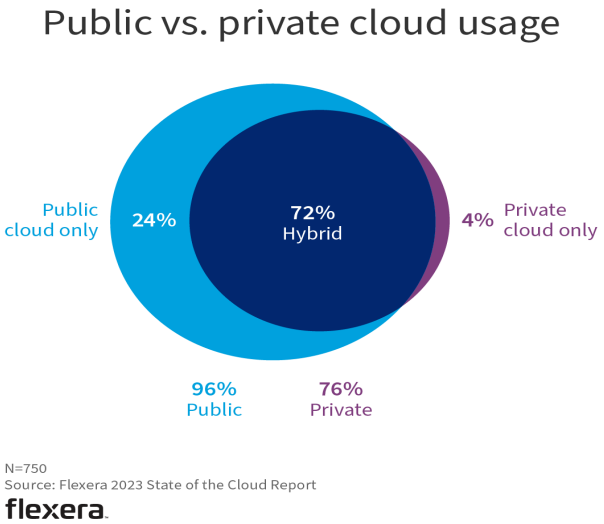

Рисунок 2.2 - Розмір використання публічної та приватної хмари

Постачальники хмарних технологій також швидко використали попит на послуги з підтримкою штучного інтелекту, пропонуючи стандартизовані продукти штучного інтелекту (наприклад, чат-боти, інструменти розпізнавання зображень, інструменти інтелектуального аналізу даних) із функцією штучного інтелекту та автоматизовані способи підвищення справедливості та пом’якшення упередженості в інструментах штучного інтелекту.

Збільшення попиту на хмарні послуги також відображається в диверсифікації використання послуг хмарної інфраструктури (зокрема в охороні здоров’я та державному секторі). Після пандемії хмара підтримує постійні шаблони віддаленої роботи, навчання, ігор і потокового передавання, а також усталені моделі онлайн-покупок споживачів.

Недавнє дослідження Cloud Industry Forum [39] також підкреслює невід’ємну роль, яку хмара продовжує відігравати в поточній трансформації бізнесу. Вісімдесят відсотків респондентів погодилися, що хмарна міграція

спростила завдання, з якими стикаються ІТ-відділи. Також зрозуміло, що компанії вважають хмарні обчислення дуже важливими або критично важливими для цифрової трансформації (враховуючи їхню надійність у підтримці технологічного розвитку в умовах пандемії та недавнього економічного спаду) і глобального здоров'я. Також виявляється, що гібридні ІТ є напрямком руху для більшості організацій.

Безпека даних залишається серйозною проблемою в хмарі, оскільки організації вимагають покращених стандартів безпеки даних, часто для відповідності суворим нормативним вимогам.

Опитування HashiCorp у червні 2023 року [40] також показали, що хоча підприємства прагнуть реалізувати свої мультихмарні амбіції, їхнім планам заважають проблеми з наймом і утриманням персоналу, оскільки брак кваліфікованих хмарних спеціалістів впливає на їх здатність успішно реалізувати хмарну стратегію.

Інші виклики міграції включають оцінку технічної здійсненності, розуміння залежностей додатків і оцінку витрат, пов'язаних із моделями локальної та хмарної доставки. Це з опитування визначило, що, витік паролів/облікових даних/секретів зараз розглядається як найпоширеніша загроза безпеці (на яку посилаються 50% респондентів), займаючи перше місце в широко розголошених, давніх проблемах, таких як крадіжка даних (49%), фішинг (46%) і програми-вимагачі (42%).

Очікувані проблеми частки ринку на хмарному ринку щодо п'яти провідних постачальників IaaS зараз ретельно перевіряються регуляторами, враховуючи, що ринок глибокий, але зовсім не широкий. Цифри за 2023 рік свідчать про те, що Amazon зберіг лідируючу позицію на ринку IaaS, за нею йдуть Microsoft, Google, Alibaba та IBM Cloud, причому на п'ять провідних постачальників, як повідомляється, припадало 70 відсотків ринку в 2023 році.

Amazon продовжує лідирувати на світовому ринку IaaS з 32-відсотковою часткою ринку. Alibaba (третій за величиною постачальник) лідирує на

китайському ринку хмарних технологій, вона також готова стати провідним регіональним постачальником в Індонезії, Малайзії та інших хмарних ринках, що розвиваються.

Аналіз Canalys свідчить про те, що майже дві третини витрат на хмарну інфраструктуру припало на трійку провідних гіпермасштабованих постачальників у світі (таким чином, нібито 6 доларів США з кожних 10 доларів США, витрачених на хмарну інфраструктуру, витрачаються на цих постачальників). У першому кварталі 2023 року на Amazon і Microsoft припало більше половини доходів від хмарної інфраструктури, причому вісім найбільших постачальників контролюють приблизно 80 відсотків ринку [41].

Хмарні обчислення є основною мішенню для кібератак, оскільки вони зберігають величезну кількість конфіденційних даних на хмарних серверах, включаючи фінансову інформацію, дані клієнтів і наукову власність. Тому важливо підвищити безпеку хмарних обчислень, щоб зберегти цінні дані від несанкціонованого доступу та крадіжки.

ML було визнано перспективним методом для підвищення безпеки хмарних обчислень. Різні алгоритми можуть досліджувати величезну ємність даних, визначати домовленості та вивчати дані, щоб визначити потенційні загрози безпеці. Використовуючи машинне навчання, галузі можуть покращити свої заходи безпеки та зменшити ризик витоку даних.

Однією із значних проблем забезпечення безпеки хмарних середовищ є відсутність контролю над фізичною інфраструктурою. Фізична інфраструктура, яка складається із серверів, пристроїв зберігання даних і мережевих пристроїв, повинна підтримуватися постачальниками хмарних пакетів. Таким чином, для забезпечення безпеки даних, що зберігаються на хмарних серверах, довіра між споживачем і постачальником хмарних послуг має вирішальне значення. Іншою проблемою захисту хмарних середовищ є складність системи. Хмарні середовища включають кілька рівнів апаратного забезпечення, програмного забезпечення та мережевих компонентів, що ускладнює ідентифікацію та усунення загроз безпеці.

Деякі основні вразливості в хмарних обчисленнях включають витік даних, інсайдерські загрози, атаки шкідливих програм, атаки на відмову в обслуговуванні (DoS), незахищені API, ризики спільної інфраструктури, відсутність видимості та контролю, відповідність і юридичні ризики, втрата та витік даних, а також відсутність шифрування.

Традиційні заходи безпеки, такі як брандмауери та антивірусне програмне забезпечення, не можуть захистити хмарне середовище від складних кібератак. Використовуючи машинне навчання, галузі можуть покращити свої заходи безпеки та зменшити ризик витоку даних.

Потенціал машинного навчання для покращення ідентифікації загроз і реагування на них є однією з головних переваг його використання для хмарної безпеки. Традиційні засоби безпеки, такі як брандмауери та антивірусне програмне забезпечення, реагують лише на відомі загрози. З іншого боку, машинне навчання може ідентифікувати закономірності в даних, які можуть вказувати на загрозу, навіть якщо вона ще не відома. На основі минулих даних генеруються алгоритми ML для пошуку проектів, які вказують на вразливі місця в безпеці. Алгоритм машинного навчання може бути створений на основі даних мережевого трафіку, щоб ідентифікувати моделі поведінки, що вказують на кібератаку. Після навчання алгоритм може відстежувати мережевий трафік у режимі реального часу та повідомляти співробітникам служби безпеки про будь-які незвичні моделі активності. Додатковою перевагою використання машинних моделей для хмарної безпеки є її здатність автоматизувати певні завдання безпеки. Різні алгоритми машинного навчання можуть бути використані для автоматичної класифікації та визначення пріоритетів сповіщень безпеки, зменшуючи навантаження на персонал служби безпеки. Це може звільнити персонал служби безпеки, щоб зосередитися на більш складних роботах безпеки, що вимагають досвіду людини. Машинне навчання може покращити контроль доступу та управління ідентифікацією. Вивчаючи шаблони поведінки користувачів, алгоритми машинного навчання можуть ідентифікувати незвичайні

дії, які можуть вказувати на несанкціонований доступ. Це може допомогти компаніям запобігти спробам несанкціонованого доступу до того, як вони спричинять будь-яку шкоду.

Однією з проблем використання цих моделей для хмарної безпеки є відсутність прозорості в тому, як алгоритми машинного навчання приймають рішення. Оскільки алгоритми машинного навчання можуть бути складними для читання, працівникам служби безпеки може бути важко зрозуміти, чому було створено певне попередження. Компанії можуть використовувати такі методи, як пояснюваний ШІ, щоб вирішити цю проблему, зробивши алгоритми машинного навчання більш прозорими та доступними для інтерпретації. Іншою проблемою є балансування безпеки та зручності використання. Хоча безпека важлива, компанії також повинні переконатися, що їхні хмарні сервіси прості у використанні та не створюють непотрібних перешкод для користувачів. Машинне навчання може допомогти підприємствам знайти цей баланс, автоматизувавши певні завдання безпеки та зробивши сповіщення системи безпеки більш цілеспрямованими та ефективними. Машинне навчання має потенціал для значного підвищення безпеки хмарних обчислень. Покращуючи виявлення загроз і реагування на них, автоматизуючи завдання безпеки, покращуючи контроль доступу та керування ідентифікацією, машинне навчання може допомогти компаніям знизити ризики витоку даних та інших інцидентів безпеки. Однак компанії повинні усвідомлювати проблеми, пов’язані з використанням методів ML для хмарної безпеки, і інвестувати необхідні ресурси для подолання цих проблем [42].

2.4 Висновки до другого розділу

Хмарні обчислення стають все більш важливими для сучасних організацій та користувачів. Проте, разом з підвищенням популярності хмарних сервісів

зростають і загрози їхній безпеці. Системи хмарних обчислень містять велику кількість конфіденційних даних, і вони залежать від безпеки, щоб захистити ці дані від несанкціонованого доступу та крадіжки.

Загрози для безпеки хмарних обчислень можуть бути різного роду. Вони включають в себе атаки на віртуалізацію, мережі та інфраструктуру, інсайдерські загрози, витоки даних, атаки на відмову в обслуговуванні та інші. Разом з цими загрозами існують різні вразливості хмарних середовищ, такі як недостатнє управління доступом, недостатня ізоляція даних, незахищені API та інші проблеми безпеки.

У хмарних обчисленнях важливо розуміти співвідношення між загрозами і вразливостями, оскільки це допомагає краще зрозуміти, як забезпечити безпеку хмарних сервісів.

Прикладом такого співвідношення є віртуальні машини. Вони є ключовим компонентом хмарних обчислень і, в той же час, потенційною вразливістю. Віртуальні машини можуть стати мішенню для атак, якщо не належним чином налаштовані. Наприклад, якщо віртуальна машина не отримує регулярних оновлень та патчів, вона може залишитися вразливою перед відомими атаками, такими як атаки з використанням вразливостей у операційних системах.

З іншого боку, віртуальні машини можуть також бути частиною рішень для запобігання атакам. Застосування віртуальних машин з ізольованими середовищами може допомогти уникнути розповсюдження атак на інші частини системи. Таким чином, правильна настройка та керування віртуальними машинами є ключовими аспектами забезпечення безпеки хмарних обчислень.

В цілому, співвідношення між загрозами та вразливостями в хмарних обчисленнях вимагає постійного вивчення та вдосконалення методів захисту, оскільки це допоможе зменшити ризики та забезпечити безпеку даних в цьому сучасному інформаційному середовищі.

Загрози такі, як кібератаки, атаки на віртуалізацію, ризики зберігання даних та безпека мереж, наразі ставлять під питання безпеку хмарних сервісів.

Традиційні підходи до безпеки можуть бути неефективними у цих нових умовах, і тому виникає необхідність в нових методах та інструментах для захисту інформації та інфраструктури.

Сучасне машинне навчання та шифрування даних на рівні файлів дозволяють покращити безпеку хмарних обчислень, надаючи можливість виявлення навіть невідомих загроз та забезпечення конфіденційності даних. Моніторинг та реагування на інциденти стають дедалі важливішими для швидкого виявлення та ліквідації загроз.

В Україні, як і в багатьох інших країнах, важливо звернути увагу на законодавство, яке регулює хмарні обчислення та визначає вимоги до безпеки даних. Враховуючи зростаючі кіберзагрози в Україні, розвиток та посилення ініціатив у галузі безпеки є настільки ж важливими, як і в інших країнах.

3 РЕГУЛЮВАННЯ ХМАРНИХ ОБЧИСЛЕНЬ ТА ЇХ МЕТОДІВ ЗАХИСТУ

3.1 Регулювання хмарних обчислень та їх методів захисту в Україні

Український законодавець визнає важливість розвитку хмарних послуг в Україні.

Бачення розвитку хмарних послуг визначено в Національній економічній стратегії на період до 2030 р., затвердженої Кабінетом Міністрів України від 03 березня 2021 р. № 179 [43]. Насамперед у ній зазначається, що «відсутність ефективної системи регулювання хмарних сервісів зменшує потенціал України на одному з найдинамічніших цифрових ринків». Також у Національній економічній стратегії на період до 2030 р. передбачається, що розвиток хмарних послуг має відбуватися шляхом:

- забезпечення впровадження принципу “насамперед, хмарні технології” (Cloud First);

- забезпечення інтеграції України до міжнародного простору хмарних обчислень з одночасним вирішенням питання щодо цифрового суверенітету;

- надання підтримки експорту послуг хмарних обчислень та хмарних сховищ;

- впровадження програми залучення для побудови інфраструктури хмарних сервісів міжнародних інвесторів та високотехнологічних компаній (Microsoft, Amazon, Alphabet, Alibaba, Facebook, Apple).

Ставиться за мету підвищення рівня використання хмарних технологій та віртуалізації для 90 відсотків бізнесу.

16 вересня 2022 року набув чинності Закон України «Про хмарні послуги», який був прийнятий 17 лютого 2022 року.

Цей закон для України вперше визначив правові відносини, що виникають при наданні хмарних послуг, встановив особливості використання хмарних

послуг органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження.

Закон визначив саме для застосування в Україні, терміни, що стосуються хмарних обчислень.

У цьому законі терміни вживаються у такому значенні:

- користувач хмарних послуг - фізична або юридична особа, яка використовує хмарні послуги для забезпечення власних потреб;

- надавач хмарних послуг - юридична особа або фізична особа - підприємець, яка надає одну або більше хмарні послуги самостійно або спільно з іншими надавачами хмарних послуг;

- публічний користувач хмарних послуг (далі - публічний користувач) - орган державної влади, орган влади Автономної Республіки Крим, орган місцевого самоврядування, державне підприємство, державна установа, державна організація чи інший суб'єкт владних повноважень або інший суб'єкт, якому делеговані такі повноваження;

- технологія хмарних обчислень - технологія забезпечення дистанційного доступу на вимогу користувача до хмарної інфраструктури через електронні комунікаційні мережі;

- хмара (хмарна інфраструктура) - сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних;

- хмарна послуга - послуга з надання хмарних ресурсів за допомогою технології хмарних обчислень;

- хмарні ресурси - будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких забезпечують технології хмарних обчислень, зокрема процесорний час

(обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп’ютерні програми;

- центр обробки даних - спеціалізований технічний комплекс, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу.

Інші терміни в цьому Законі вживаються у значеннях, наведених у Цивільному кодексі України, законах України "Про інформацію", "Про електронні довірчі послуги", "Про електронні документи та електронний документообіг", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про стандартизацію", "Про технічні регламенти та оцінку відповідності", "Про наукову і науково-технічну експертизу", "Про Національний банк України", "Про захист персональних даних", "Про авторське право і суміжні права", "Про основні засади забезпечення кібербезпеки України", "Про національну безпеку", "Про електронні комунікації".

Закон «Про хмарні обчислення» визначив види хмарних послуг (інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга, безпека як послуга, інші послуги, що відповідають визначенню хмарних послуг) та способи надання хмарних послуг (приватна хмара, колективна хмара, публічна хмара, гібридна хмара).

Учасниками відносин у сфері хмарних послуг є:

- користувач хмарних послуг, включаючи публічного користувача;

- надавач хмарних послуг;

- надавач послуг центру обробки даних;

- органи державної влади.

Слід відзначити, що закон встановлює систему та процедуру державного управління і регулювання при наданні хмарних послуг.

Організаційну систему державного управління і регулювання при наданні хмарних послуг становлять:

- Кабінет Міністрів України;

- регулятор комунікаційних послуг;

- центральний орган виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг;

- орган, уповноважений здійснювати контроль за додержанням законодавства про захист персональних даних;

- Міністерство оборони України;

- Національний банк України;

- Центральна виборча комісія.

Надавач хмарних послуг та/або послуг центру обробки даних зобов’язаний не використовувати для надання хмарних послуг технічні засоби, розміщені на території, на якій органи державної влади України тимчасово не здійснюють свої повноваження, на території держави, визнаної Верховною Радою України державою-агресором або державою-окупантом, а також не використовувати технічні засоби, якими володіють держави або суб’єкти, до яких застосовано санкції відповідно до Закону України "Про санкції".

Для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об’єктам інфраструктури відомості про надавачів хмарних послуг та/або послуг центру обробки даних мають бути внесені до переліку.

Ведення переліку надавачів хмарних послуг та/або послуг центру обробки даних здійснює регулятор комунікаційних послуг.

Хмарні послуги та/або послуги центру обробки даних надаються на договірних засадах.

Договір про надання хмарних послуг та/або послуг центру обробки даних може включати положення, викладені в іншому електронному документі, включені шляхом посилання на такий електронний документ.

Договір про надання хмарних послуг та/або послуг центру обробки даних укладається у письмовій формі.

Кабінет Міністрів України затверджує Типовий договір про надання хмарних послуг та/або послуг центру обробки даних публічному користувачу та об’єкту критичної інформаційної інфраструктури.

Забороняється обробка інформації, що становить державну таємницю, службової інформації, державних та єдиних реєстрів, створення та забезпечення функціонування яких встановлено законом, за допомогою хмарних ресурсів та/або центрів обробки даних, що розміщені за кордоном або на тимчасово окупованій території України, або належать державі, визнаній Верховною Радою України державою-агресором чи державою окупантом, або належать суб’єктам, діяльність яких підпадає під дію Закону України "Про санкції" та щодо яких прийнято рішення про застосування санкцій в Україні.

Прикінцеві положення Закону «Про хмарні технології» встановили, що Кабінет Міністрів України у шестимісячний строк з дня набрання чинності цим Законом повинен визначити структуру, порядок формування та використання електронних каталогів хмарних послуг та/або послуг центру обробки даних; визначити вимоги до надавачів хмарних послуг та/або послуг центру обробки даних, яким надавач хмарних послуг має відповідати для внесення до переліку за відповідними видами послуг, та порядок підтвердження відповідності цим вимогам; встановити порядок надання хмарних послуг та/або послуг центру обробки даних, пов’язаних з обробкою державних інформаційних ресурсів; визначити порядок підготовки пропозицій щодо використання хмарних послуг та/або послуг центру обробки даних органами державної влади, органами влади Автономної Республіки Крим та їх розгляду.

Подальший розвиток регулювання хмарних обчислень пов'язаний з введенням 24 лютого 2022 року воєнного стану в Україні.

08 березня 2022 року Правління Національного банку України приймає постанову № 42 «Про використання банками хмарних послуг в умовах воєнного стану в Україні». Вказаний документ зазначає, що на період дії воєнного стану та протягом двох років після скасування воєнного стану:

- банки України мають право здійснювати оброблення та зберігання персональних даних клієнтів, а також інформації, що містить банківську таємницю (у тому числі оброблення інформації про банківські операції, щоденне ведення бази даних про вкладників та формування файлів D, Z, M, N архіву бази даних про вкладників згідно з нормативно-правовими актами Фонду гарантування вкладів фізичних осіб тощо), із використанням хмарних сервісів, що надаються з використанням обладнання, яке розташовано в державах – учасницях Європейського Союзу, Європейського співтовариства, Великій Британії, Сполучених Штатах Америки або Канаді (далі – Держави);

- процесинг за операціями із застосуванням електронних платіжних засобів на території України може здійснюватися процесинговими установами резидентами та/або процесинговими установами-нерезидентами, які розташовані в Державах, уключаючи використання процесинговими установами хмарних сервісів, та на обладнанні, яке розташовано в Державах [44].

12 березня 2022 року Кабінетом Міністрів прийнято постанову № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану». Згідно постанови на період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких

вони є, та захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, можуть вживати таких додаткових заходів:

- розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України, та реєструвати доменні імена у домені gov.ua для такого розміщення;

- зберігати резервні копії державних інформаційних ресурсів та публічних електронних реєстрів у зашифрованому вигляді, зокрема за межами України, на хмарних ресурсах та/або окремих фізичних носіях, та/або в ізольованому сегменті центрів обробки даних з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності яким визнає можливим у період дії воєнного стану використання хмарних послуг та/або послуг центру обробки даних (далі - хмарні сервіси) надавачів хмарних сервісів, розташованих в країнах, що є членами Європейського союзу, у Великобританії, Сполучених штатах Америки, Канаді, Україні: Центральним депозитарієм цінних паперів при провадженні ним своєї професійної діяльності на ринках капіталу; Державною установою "Агентство з розвитку інфраструктури фондового ринку України" для забезпечення своєї діяльності на ринках капіталу та організованих товарних ринках; депозитарними установами, яким Центральним депозитарієм цінних паперів відкрито агреговані рахунки; адміністраторами недержавних пенсійних фондів з метою забезпечення захисту та збереження даних систем персоніфікованого обліку [45].

30 грудня 2022 року Кабінет Міністрів України прийняв Постанову № 1500 «Деякі питання забезпечення функціонування державних інформаційних ресурсів». Ця постанова затвердила:

- Порядок передачі, збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) та їх резервних копій, розміщених на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України;

- Порядок укладення договорів володільцями інформації - власниками (держателями) державних інформаційних ресурсів (публічних електронних реєстрів) про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями - постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України. Цей Порядок протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування регулює відносини володільців інформації - власників (держателів) державних інформаційних ресурсів (далі - замовники), які виявили бажання (намір) розмістити державні інформаційні ресурси та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України.

Постачальник послуг (надавач хмарних послуг або ресурсів у центрах обробки даних), до якого передаються (переміщуються) державні інформаційні ресурси або їх резервні копії, повинен мати документ про відповідність впровадження системи інформаційної безпеки міжнародним стандартам.

Передача (переміщення) державних інформаційних ресурсів, що містять конфіденційну інформацію, з використанням електронних комунікаційних мереж повинна здійснюватися з використанням засобів криптографічного захисту інформації.

У засобах криптографічного захисту інформації, які застосовуються для передачі (переміщення) державних інформаційних ресурсів, використовуються криптоалгоритми та криптопротоколи, які визначені національними стандартами, зокрема наведені у переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, визначеному Адміністрацією Держспецзв’язку, та/або ті, на які за результатами експертних

досліджень Адміністрацією Держспецзв’язку видано позитивний експертний висновок.

Прийняті після Закону «Про хмарні послуги» нормативно – правові акти спрямовані на здійснення екстреного збереження певної інформації шляхом використання хмарних послуг та/або послуг центру обробки даних надавачів хмарних сервісів, розташованих в країнах, що є членами Європейського союзу, у Великобританії, Сполучених штатах Америки, Канаді [46].

На даний час потрібно проводити роботу по розробці та приведенню у відповідність підзаконних актів у відповідність до Закону «Про хмарні послуги».

3.2 Міжнародні регуляторні акти

Питанням регулювання використання хмарних послуг в ЄС приділяється значна увага вже протягом тривалого часу. Ще у 2012 році була розроблена Європейська хмарна стратегія, яка вперше визначила пріоритетом на рівні ЄС необхідність сприяння швидшому впровадженню хмарних обчислень у всіх секторах економіки [47].

В ЄС розвиток загальних засад регламентації надання хмарних послуг здійснюється шляхом:

- розробки стандартів діяльності надавачів хмарних послуг. Так, 20 травня 2021 р. було прийнято добровільний до застосування Європейський хмарний кодекс поведінки [48], який було розроблено з метою забезпечення відповідності захисту даних у хмарному середовищі нормам ЄС, а саме Загальному регламенту ЄС про захист даних (далі – GDPR);

- забезпечення сертифікації надавачів хмарних послуг, рекомендації щодо яких розроблені Робочою групою із сертифікації європейських надавачів хмарних

послуг (2019 р.) [49]. Наступним кроком має бути розробка ENISA сертифікаційної схеми кібербезпеки для хмарних інфраструктур і послуг [50];

- підвищення інформаційної обізнаності бізнесу про технічні й правові аспекти хмарних послуг. Із цією метою ЄС опублікувала Керівництво про Стандартизовані угоди про рівень послуг хмарних обчислень [51].

Далі класифікуємо та дослідимо організації та органи, які створюють нормативні документи, пов’язані з хмарними обчисленнями. Вони встановлюють стандарти, що застосовуються по всьому світу, і складаються з наступних ланок:

- Міжнародний (ISO/IEC [52]);
- Міждержавний (форуми і консорціуми (Cisco, CSA));
- Регіональний (європейські органи ETSI, CEN / CENELEC);
- Національний (закони та державні стандарти, відомчі нормативні документи, керівництва, інструкції, наприклад: (NIST) [4].

Якщо учасники процесу надання послуг часто знаходяться в різних країнах і на різних континентах, при стандартизації хмарних технологій кордони держав перестають бути обмежувальним фактором. У зв’язку з відсутністю міжнародних стандартів сертифікації елементи хмарної інфраструктури (такі як центри обробки даних, канали та мережі зв’язку) тепер використовують сертифікати безпеки з суміжних країн. Це є результатом актуалізації забезпечення інформаційної безпеки.

У секторі керування конфігурацією хмарних технологій багато компаній намагаються розробляти специфікації для стандартного інтерфейсу прикладного програмування (API), тобто інтерфейсу через який користувачі та оператори керують хмарними обчисленнями та сховищами. У рамках організації Open Grid Forum (OGF) робоча група Відкритого інтерфейсу хмарних обчислень (Open Cloud Computing Interface Working Group, або OCCI-WG) визначила та оприлюднила API для управління інфраструктурою як сервісом (IaaS). Крім того, API керування IaaS було визначено Open Cloud Standards Incubator (OCSI) робочої групи розподіленого управління (DMTF). Асоціація виробників мереж зберігання

даних (SNIA) розробила специфікації Cloud Data Management Interface (CDMI – Управління інтерфейсом хмарних даних), який є API для управління блоками зберігання даних [52].

Організація нестандартних послуг теж працює в данній області. У липні 2010 року спільнота з відкритим кодом під назвою OpenStack, створена в основному Rackspace і NASA, зробила вихідний код програмного забезпечення для керування IaaS відкритим.

Стандартизація хмарних обчислень розпочата промисловими організаціями, які розробляють так звані “стандартні стандарти”. Інститут інженерів електротехніки та електроніки (IEEE) та Інтернет-технічна робоча група (IETF) були серед органів стандартизації, орієнтованих на інформаційно-телекомунікаційні технології, які почали діяти з кінця 2009 року, а також такі органи, як MCE-T та ISO/IEC JTC1. Крім того, урядові організації в Європі та Сполучених Штатах також обговорюють стандартизацію хмарних обчислень.

Є дві групи органів стандартів форуму, пов’язані з хмарними обчисленнями. У першій групі DMTF, OGF і SNIA активно працюють у сфері мереж і керування розподіленим процесом; останнім часом вони включають хмарні обчислення до своїх завдань. Нещодавно були створені OCC, CSA та GICTF для праці з хмарними обчисленнями як друга група.

DMTF (Distributed Management Task Force – Робоча група розподіленого управління). DMTF розробила формат Open Virtualization Format (OVF), який є загальноприйнятим форматом зображення віртуальної машини. Вона започаткувала OCSI у квітні 2009 року та вивчає стандарти, які сприятимуть взаємозв’язку хмарних систем.

CMWG (The Cloud Management Working Group – Робоча група управління хмарами), в якій VMware, Fujitsu та Oracle пропонують відповідний API, створена у червні 2010 року. У листопаді 2009 року DMTF випустила «Білий документ» щодо сумісності між хмарними системами, а в червні 2010 року вона випустила

ще один «Білий документ» щодо випадків використання управління хмарами та взаємодії. VMware, Microsoft, IBM, Citrix, Cisco та Hitachi входять до Правління.

OGF (Open Grid Forum – Відкритий Грід форум). У квітні 2009 року OGF створив робочу групу OCCI-WG, яка розробила та випустила специфікацію API, яка дозволяє керувати комп'ютерами та робочими навантаженнями через IaaS. У Європі проект OpenNebula реалізує відкритий інтерфейс хмарних обчислень. Основні учасники цього проекту це Fujitsu, EMC і Oracle.

SNIA (Storage Networking Industry Association – Асоціація виробників мереж зберігання даних). У квітні 2009 року SNIA створила Технічну робочу групу хмарних сховищ (Cloud Storage Technical Working Group) та випустила CDMI, що є специфікацією інтерфейсу для керування даними у хмарі. У жовтні 2009 року Асоціація створила підгрупу під назвою CSI (Cloud Storage Initiative – Ініціатива хмарних сховищ) для навчання користувачів та просування ринку хмарних сховищ за допомогою проекту Cloud BUR SIG (Cloud Backup and Recovery Special Interest Group – Група спеціальних інтересів по хмарному резервуванню та відновленню). Серед членів SNIA є EMC, IBM, Fujitsu і Hitachi.

OCC (Open Cloud Consortium – Відкритий хмарний консорціум). OCC - це некомерційна організація, що створена у січні 2009 року під керівництвом університету штату Іллінойс у Чикаго. Консорціум націлений на досягнення сумісності між хмарними системами та розробку еталонних тестів за допомогою хмарного випробувального стенду.

CSA (Cloud Security Alliance – Альянс хмарної безпеки). CSA – це некомерційна організація, створена в березні 2009 року для вивчення найкращих практик забезпечення безпеки хмари та сприяння їх використанню. У квітні 2009 року було опубліковано вказівки щодо забезпечення безпеки хмар.

GICTF (Global Inter-Cloud Technology Forum – Глобальний форум з хмарних технологій). GICTF — це організація в Японії, яка зосереджується на вивченні стандартних інтерфейсів між хмарами, щоб підвищити надійність хмар. До неї входять більше 80 корпоративних членів і організацій з промисловості, уряду і

наукових кіл. У червні 2010 року вона оприлюднила офіційний документ щодо випадків використання міжхмарного об'єднання і функціональних вимог.

Урядові органи США та Європи також активно працюють над стандартизацією хмарних технологій. А саме NIST і ENISA.

NIST (National Institute of Standards and Technology – Національний інститут стандартів та технологій) – це технічний відділ, який належить Торгово-промисловому департаменту США. “The NIST Definition of Cloud Computing” є одним із перших документів NIST, який створив визначення хмарних технологій. В той же час NIST здійснює стандартизацію хмарних технологій за п’ятьма робочими групами. Одна з них – SAJACC (Standards Acceleration to Jumpstart Adoption of Cloud Computing – Прискорення стандартів для швидкого впровадження хмарних обчислень), яка покликана сприяти розробці стандартів хмарних технологій на основі фактичних прикладів та випадків використання.

ENISA (European Union Agency for Network and Information Security – Європейська агенція мереж та інформаційної безпеки). Серед документів, підготовлених ENISA, є «Хмарні обчислення: переваги, ризики та рекомендації щодо інформаційної безпеки», в якому пропонуються пропозиції щодо структурування інформаційної безпеки в хмарних обчисленнях, а також «Система гарантії інформації в хмарних обчисленнях», яка служить основою для підтримки захисту інформації в хмарах.

Незважаючи на те, що багато організацій обговорюють питання стандартизації хмарних технологій, нині немає достатньої діяльності, щоб об’єднати обговорення та приймати рішення. Головне питання полягає в тому, наскільки добре національні та міжнародні органи стандартизації, які розпочали повномасштабні дослідження хмарних технологій, можуть співпрацювати з робочими групами розвитку хмарних технологій утворених бізнесом, щоб допомогти впровадити новітні світові розробки в інформаційний простір нашої держави та закріпити їх у законодавстві України. Розглянемо деякі основні стандарти забезпечення безпеки інформації в хмарних технологіях.

Наразі два технічні підкомітети Об’єднаного технічного комітету 1 ISO (JTC 1) «Інформаційні технології» залучені до розробки міжнародних стандартів, пов’язаних із хмарними технологіями. Нижче наведені документи, які вони підготували.

Стандарт ISO/IEC 17788 “Information technology. Distributed application platforms and services. Cloudcomputing. Overview and vocabulary” (“Інформаційні технології. Розподілені прикладні платформи і сервіси. Хмарні обчислення. Загальні положення та словник”). Стандарт включає багато термінів і визначень для опису хмарних обчислень. Він послужив основою для подальшої роботи зі стандартизації хмарних обчислень. У 2014 році стандарт офіційно опублікували. У лютому та вересні 2023 року відбулася публікація стандарту ISO/IEC 22123-1:2023 [11] та ISO/IEC 22123-2:2023 відповідно [53]. Вказані стандарти замінили стандарт ISO/IEC 17788:2014.

Стандарт ISO/IEC 17789 “Information technology. Cloud computing. Reference architecture” (“Інформаційні технології. Хмарні обчислення. Еталонна архітектура”). У стандарті міститься опис загальних понять і атрибутів хмарних обчислень, а також описи хмар та їх відповідних компонентів. Основна увага зосереджена на передумовах для хмарних сервісів, а не на створенні та впровадженні відповідних рішень. У ньому не йдеться про проблеми проектування та впровадження відповідних рішень, а про те, що повинні забезпечувати хмарні сервіси. У вересні 2023 року відбулася публікація стандарту ISO/IEC 22123-3:2023 [54]. Вказаний стандарт замінив стандарт ISO/IEC 17789.
Технічна специфікаці ISO/IEC TS 27017 “Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002” (“Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг”) [55]. Рекомендації щодо забезпечення інформаційної безпеки хмарних обчислень містяться у ньому. Він базується на переглянутій версії ISO/IEC 27002 і

здебільшого включає поради щодо впровадження заходів інформаційної безпеки, описаних у цьому документі, що стосуються хмарних обчислень.

Стандарт ISO/IEC 27018 “Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors” (“Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII”) [56]. Це стандарт для постачальників сервісів «публічної хмари», які обробляють персональні. У ньому включено вказівки щодо різних аспектів і компонентів захисту персональних даних і невразливості приватної інформації, що зберігається в загальнодоступній хмарі. Рекомендації стандарту ISO/IEC 27002 не повторюються або змінюються в цьому стандарті. У ньому вказуються додаткові потреби та процедури контролю і управління для захисту особистих даних у хмарі.

3.3 Висновки до третього розділу

Регулювання хмарних обчислень - це складний та постійно розвиваючийся процес, який об'єднує міжнародні, національні, технічні та безпекові аспекти.

На світовому рівні існують багато організацій, які стандартизують та регулюють хмарні обчислення. Міжнародні стандарти встановлюють загальні терміни і вимоги для розробників і користувачів хмарних послуг. Науково-технічні організації та ініціативи, такі як ISO, NIST, та інші, розробляють стандарти, які допомагають забезпечити безпеку, надійність та сумісність хмарних послуг.

Україна має можливість використовувати світовий досвід регулювання хмарних обчислень для поліпшення своїх нормативних актів та стандартів. Це

може сприяти створенню більш сприятливого середовища для розвитку хмарних технологій у країні та забезпечити вищий рівень інформаційної безпеки.

Регулювання хмарних обчислень у світі має кілька основних особливостей.

Міжнародні стандарти: важливим аспектом є наявність міжнародних стандартів, які встановлюють загальні терміни, вимоги та рекомендації для хмарних обчислень.

Національні законодавчі акти: кожна країна може регулювати хмарні обчислення на національному рівні через закони та правила, що встановлюються національними органами, які відповідають за інформаційну безпеку та технологічний розвиток.

Безпека та захист даних: регулювання хмарних обчислень включає в себе важливий аспект - захист інформації та даних в хмарних середовищах.

Міжнародна співпраця: багато країн співпрацюють на міжнародному рівні для розробки стандартів та вирішення спільних питань, пов'язаних з хмарними обчисленнями.

Галузеві ініціативи: об'єднання, групи або асоціації компаній і фахівців з певної галузі, які спільно працюють над розробкою стандартів, нормативів, інновацій та рекомендацій для певного сектору чи індустрії. Cloud Security Alliance (CSA) є прикладом індустрійної ініціативи в галузі хмарних обчислень. CSA об'єднує представників галузі та експертів, які працюють разом для створення стандартів та рекомендацій, спрямованих на покращення безпеки та ефективності хмарних обчислень.

Україна, подібно до багатьох інших країн, займається регулюванням хмарних обчислень, і це є важливим кроком для забезпечення безпеки та надійності використання хмарних технологій. Важливо продовжувати співпрацювати як на національному, так і на міжнародному рівні для створення сприятливого середовища для розвитку цих технологій та забезпечення інформаційної безпеки.

4 ВИЗНАЧЕННЯ ВАРТОСТІ ХМАРНИХ ОБЧИСЛЕНЬ

4.1 Фактори, що визначають вартість хмарних обчислень

Міграція компаній у хмару – не лише тренд, а й вимога сучасності.

Gartner прогнозує, що витрати кінцевих користувачів на публічну хмару досягнуть 600 мільярдів доларів у 2023 році. Дослідницька компанія повідомила, що інфраструктура як послуга (IaaS), робочий стіл як послуга (DaaS) і платформа як послуга Сервіс (PaaS) зафіксує найбільше зростання.

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2022	2023	2024
Cloud Application Infrastructure Services (PaaS)	111,976	138,962	170,355
Cloud Application Services (SaaS)	167,342	197,288	232,296
Cloud Business Process Services (BPaaS)	59,861	65,240	71,063
Cloud Desktop-as-a-Service (DaaS)	2,525	3,122	3,535
Cloud Management and Security Services	34,487	42,401	51,871
Cloud System Infrastructure Services (IaaS)	114,786	150,310	195,446
Total Market	**490,977**	**597,325**	**724,566**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.
Source: Gartner (April 2023)

Рисунок 4.1 - Витрати кінцевих користувачів на публічну хмару

В умовах повномасштабної війни український бізнес зіткнувся з серйозними проблемами убезпечення своєї IT-інфраструктури, доступу до робочих ресурсів, а також збереження і захисту як власних даних, так і даних своїх клієнтів.

Кібербезпека та дієві можливості захисту інформації вийшли на перший план.

Перемістивши бізнес-операції в хмару, можна працювати з більшою гнучкістю та безпекою. Фізичні архіви або окремі кімнати з власними серверами

стали неважливими, а лояльність клієнтів набула особливого значення. Облік і дані клієнтів програми лояльності невеликої мережі кав'ярень на півночі Києва зберігалися на матеріальних носіях. У перші кілька днів після повного вторгнення в Росію робітникам довелося евакуюватися, і не було можливості забрати свої комп'ютери чи інше обладнання. Якби вся важлива інформація була заздалегідь перенесена в хмару, компанія швидко повернулася б до роботи на новому майданчику. Зокрема, маючи можливість дистанційного доступу до попередніх робочих документів, клієнтських баз та історії взаємовідносин з клієнтами. Хмарні рішення також забезпечують командну роботу, дозволяючи співробітникам працювати з будь-якої точки світу.

Це помилкова думка, що хмарні технології потрібні лише великим підприємствам. Цінність хмар для малого та середнього бізнесу більша, ніж для корпорацій, оскільки вона сприяє швидкому розвитку їхнього бізнесу без значних інвестицій.

Зокрема, бізнес значно заощаджує на капіталовкладеннях у "залізо", оскільки при використанні хмарних сервісів не потрібно купувати та обслуговувати власні сервери для зберігання інформації.

Ось деякі з популярніших хмарних провайдерів в Україні: Google Cloud Platform; Amazon Web Services (AWS); Microsoft Azure; GigaCloud; TETcloud; DataStore і т.д.

Рисунок 4.2 – Частка учасників українського ринку хмарних сервісів у 2022

Серед чотирьох найбільших провайдерів в Україні — місцеві компанії De Novo (17,3%) та GigaCloud (16,3%). На першому місці Amazon Web Services (20,4%) [57].

Багато факторів беруть участь у виборі правильного рішення для хмарного зберігання — розглянемо деякі з них далі, — але ціноутворення та моделі ціноутворення є великим чинником вибору. У таблиці 4.1 порівнюються ціни шести популярних постачальників хмарних сховищ.

Таблиця 4.1 - Порівняння цін постачальників хмарних сховищ [58]

	Хмарне сховище Alibaba	Amazon S3	Microsoft Azure Blob Storage	Google Cloud Storage	IBM Cloud Object Storage	Oracle Cloud Object Storage
Вільний рівень	50 Гб назавжди	5 ГБ на 1 рік	5 ГБ на 1 рік	5 ГБ назавжди	25 ГБ назавжди	5 ТБ на 30 днів
Ціна за ГБ	1-й 10 ТБ 0,0760 $/ГБ Наступні 40 ТБ 0,0690 $/ГБ Наступні 100 ТБ 0,0600 $/ГБ Більше 150 ТБ 0,0430 $/ГБ	Перші 50 ТБ 0,023 $/ГБ Наступні 450 ТБ 0,022 $/ГБ Понад 500 ТБ 0,021 $/ГБ	Перші 50 ТБ 0,0208 $/ГБ Наступні 450 ТБ 0,020 $/ГБ Понад 500 ТБ 0,0192 $/ГБ	$0,02/ГБ	0-499,99 ТБ 0,022 $/ГБ 500+ ТБ 0,02 дол. США/ГБ	0,0255 доларів США
Дані передаються	0,082 $/Гб	безкоштовно	безкоштовно	безкоштовно	безкоштовно	безкоштовно

Кінець таблиці 4.1

	Хмарне сховище Alibaba	Amazon S3	Microsoft Azure Blob Storage	Google Cloud Storage	IBM Cloud Object Storage	Oracle Cloud Object Storage
Передача даних на вихід	0,082 $/Гб	Перший 1 ГБ безкоштовно Наступні 9,999 ТБ 0,09 $/ГБ Наступні 40 ТБ 0,085 $/ГБ Наступні 100 ТБ 0,07 $/ГБ Понад 150 ТБ 0,05 $/ГБ	Безкоштовно для гарячих даних	0-1 ТБ 0,12 $/ГБ 1-10 ТБ 0,11 $/ГБ 10+ ТБ 0,08 дол. США/ГБ	0-50 ТБ 0,09 $/ГБ Наступні 100 ТБ 0,07 $/ГБ Наступні 350 ГБ 0,05 дол Ціна 500+ ТБ доступна за запитом	безкоштовно
Запити PUT	1 500 мільйонів запитів безкоштовні Більше 500 мільйонів $0,001/10 000 запитів	0,005 доларів США за 1000	0,05 долара за 10 000	$0,004 або $0,05 за 10 000	0,006 долара за 1000	0,0034 долара за 10 000
GET запити	1 100 мільйонів запитів безкоштовні Більше 100 мільйонів $0,016/10 000 запитів	0,004 долара за 1000	0,004 долара за 10 000	$0,004 або $0,05 за 10 000	0,005 доларів США за 10 000	0,0034 долара за 10 000
Оцінка вартості 1 ТБ	14,34 $/місяць $71,40/6 місяців $129,02/рік	34,67 дол. США/ТБ/місяць	24,90 дол. США/ТБ/місяць	24,08 дол. США/ТБ/місяць	26,40 доларів США/ТБ/місяць	27 доларів США/ТБ/місяць

Для визначення вартості хмарних обчислень для споживача можливо використовувати формулу для розрахунку витрат на хмару (фактичних очікуваних поточних витрат).

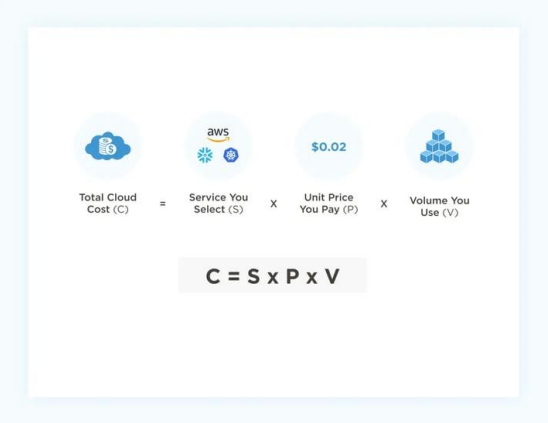

Рисунок 4.3 – Розрахунок загальної вартості хмари

Загальна вартість хмари (C) = послуга, яку ви вибираєте (S) x ціна за одиницю, яку ви платите (P) x обсяг, який ви використовуєте (V).

Ось короткий розподіл факторів вартості хмари:

- «S». Під послугою мається на увазі, якого постачальника(ів) хмарних послуг ви використовуєте, які базові хмарні сервіси вони надають вам і як ви їх використовуєте;

- «P». Ціна за одиницю – це оплата, яку ви сплачуєте постачальнику хмарних послуг за кожну послугу, продукт чи процес;

- «V». Обсяг означає, наскільки часто ви використовуєте хмару та наскільки вона відповідає вашим очікуванням.

Згідно з дослідженням Flexera у 2023 році, організації втрачають від 28% до 32% грошей, які вони витрачають на хмар, через непотрібні витрати.

Непотрібні витрати бувають у вигляді:

- ресурси, які були придбані, але ніколи не використовувалися,

- неприєднані або неактивні ресурси залишаються запущеними без потреби,
- невідповідний розмір ресурсів,
- надлишок ресурсів,
- неправильна конфігурація.

Хмарні обчислення обіцяють заощадити гроші компаній порівняно з підтримкою локального середовища. Однак це не відбувається автоматично або швидко, оскільки команди повинні адаптувати робоче навантаження до нового IT-середовища [59].

4.2 Визначення витрат на хмарні обчислення

Щоб по-справжньому зрозуміти, як хмарні обчислення впливають на прибуток компанії, потрібно застосувати цілісний підхід до розрахунку вартості хмарних обчислень .

Слід не лише розрахувати прямі витрати, але й включити непрямі витрати, такі як вплив можливого простою на продуктивність співробітників і клієнтів.

Розглянемо кроки, які слід виконати, щоб розрахувати справжню вартість хмарних обчислень.

Перший етап – це перевірка поточних витрат на IT-інфраструктуру.

Першим кроком, який слід зробити, є проведення аудиту, щоб краще зрозуміти обсяг і масштаб поточних IT-операцій. Це допоможе: зрозуміти, скільки компанія зараз сплачує за виконання своїх IT-операцій, і визначити, як може виглядати нове хмарне середовище.

Наявність цієї базової лінії допоможе розрахувати потенційну вартість хмарних ресурсів, які компанія буде споживати, і порівняти її з поточними рівнями вартості.

Перше, про що слід пам’ятати, це те, що потрібно враховувати загальну вартість IT-операцій. Тобто загальна вартість використання та підтримки локальних інвестицій у IT протягом певного часу, а не лише сума, яку компанія сплачує за інфраструктуру.

Це включатиме прямі та непрямі витрати.

Прямі витрати - це витрати, пов'язані з виробництвом окремого виду продукції (виконанням певних робіт, наданням окремих послуг), які можуть бути безпосередньо включені в собівартість цієї продукції (робіт, послуг).

Перша категорія прямих витрат – це апаратне та програмне забезпечення, яке складає IT-інфраструктуру.

Це включає фізичні сервери, ліцензії на програмне забезпечення, контракти на технічне обслуговування, гарантії, витратні матеріали, матеріали, запасні частини та все інше, за що компанія безпосередньо платить.

Проаналізувати ці витрати можна через рахунки-фактури, замовлення на купівлю та платіжні записи з кредиторської заборгованості.

Також обов’язково необхідно мати повне розуміння того, скільки пропускної здатності мережі, пам’яті та ємності бази даних компанія споживає своїми серверами та іншими технологіями.

Треба звернути увагу на атрибути та деталі інфраструктури компанії, такі як типи баз даних, кількість серверів і ємність зберігання. Цю інформацію треба використовувати під час розрахунку загальної вартості переходу у хмару.

Другим видом прямих витрат є операційні витрати.

Вони можуть включати: працю (внутрішню та зовнішню) для обслуговування серверів, баз даних та інших IT-компонентів; приміщення, які використовуються для розміщення IT-обладнання; персонал, необхідний для обслуговування цих приміщень, витрати на нерухомість та інші витрати, пов’язані з об’єктами; підключення до інтернету; адміністративні витрати, необхідні для утримання IT-відділу. До них можуть входити витрати з фінансового, кадрового відділу та відділу закупівель, які займаються керуванням IT-персоналом, або

зовнішніми постачальниками послуг. Хоча ці витрати можуть здатися не пов’язаними, інші відділи компанії виділяють велику кількість ресурсів на наймання, навчання та керування внутрішніми IT-працівниками та зовнішніми консультантами, і ці витрати потрібно враховувати. Можна оцінити кількість годин, витрачених на нагляд за IT, опитавши ключових співробітників у цих відділах і перевіривши журнали навчання, а потім помноживши цю загальну суму на середню погодинну оплату праці.

Непрямі витрати може бути складніше підрахувати, але вони так само важливі, як і прямі. Найбільшим джерелом непрямих витрат є час простою та втрата продуктивності співробітників і клієнтів, якщо IT-інфраструктура виходить з ладу. Можна розрахувати ці витрати, переглянувши файли журналів, щоб визначити, як часто сервери перестають працювати та як довго, і помножити цей час на середню погодинну ставку. Якщо компанія може оцінити дохід, який вона може втратити через простої, це також слід включити в розрахунок. Непрямі витрати важко оцінити, але їх дуже важливо враховувати, оскільки вони можуть становити значну частину загальних витрат на IT.

Другий етап - обчислити приблизні витрати на хмарну інфраструктуру.

Після визначення поточних витрат на локальну інфраструктуру наступним кроком буде обчислення потенційної вартості використання хмарної інфраструктури. Після завершення аудиту потрібно добре розуміти мережевий потенціал, сховище та базу даних, необхідні для запуску всіх програм компанії.

Хоча раніше хмарне ціноутворення було надзвичайно складним, тепер постачальники спростили свої структури ціноутворення, щоб потенційні клієнти могли їх легше зрозуміти.

Можна скористатися одним із безлічі доступних калькуляторів вартості хмари, щоб отримати уявлення про вартість хмарної інфраструктури.

Ось короткий список:

- калькулятор загальної вартості володіння (TCO - total cost of ownership) Amazon Web Services (AWS) і більш поглиблений калькулятор місячних витрат;

- калькулятор цін Google Cloud Platform;
- калькулятор цін Microsoft Azure;
- калькулятор Rackspace;
- калькулятор IBM Bluemix.

Розглянемо калькулятор TCO від AWS.

Перший крок, який потрібно зробити, це ввести існуючу або заплановану локальну інфраструктуру.

Якщо починаєте з базового калькулятора, потрібно буде ввести таку інформацію: сервери, тип сервера, кількість віртуальних машин, ядра процесора, пам'ять в Гб, гіпервізор, гостьову операційну систему, підсистему зберігання, тип зберігання.

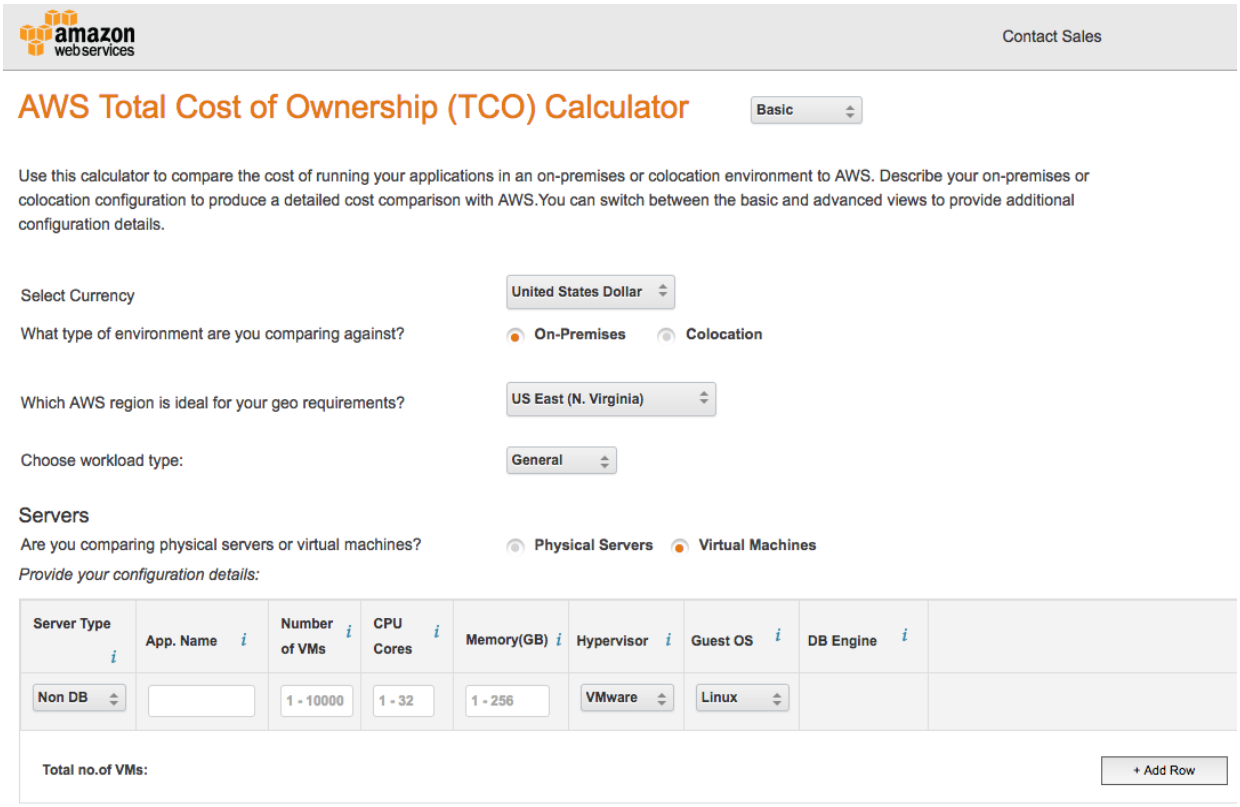

Рисунок 4.4 – Калькулятор Amazon Web Services

За потреби можна додати рядки для кількох типів серверів і сховищ.

Розширений калькулятор запитає детальнішу інформацію про сервери та сховище, а також включить роботу мережі та IT до розрахунку.

Після того, як буде введено всю інформацію, калькулятор миттєво створить звіт із підсумковим порівнянням трирічної загальної вартості за категоріями витрат. Потім можна завантажити повний звіт із детальним розподілом витрат, припущеннями моделі, методологією та поширеними запитаннями.

AWS також надає калькулятор для порівняння вартості роботи програм резервного копіювання та архівування в локальному середовищі порівняно з AWS.

На додаток до загального калькулятора, AWS також надає калькулятор місячних витрат, який дає змогу отримати надзвичайно детальний розрахунок місячного рахунку.

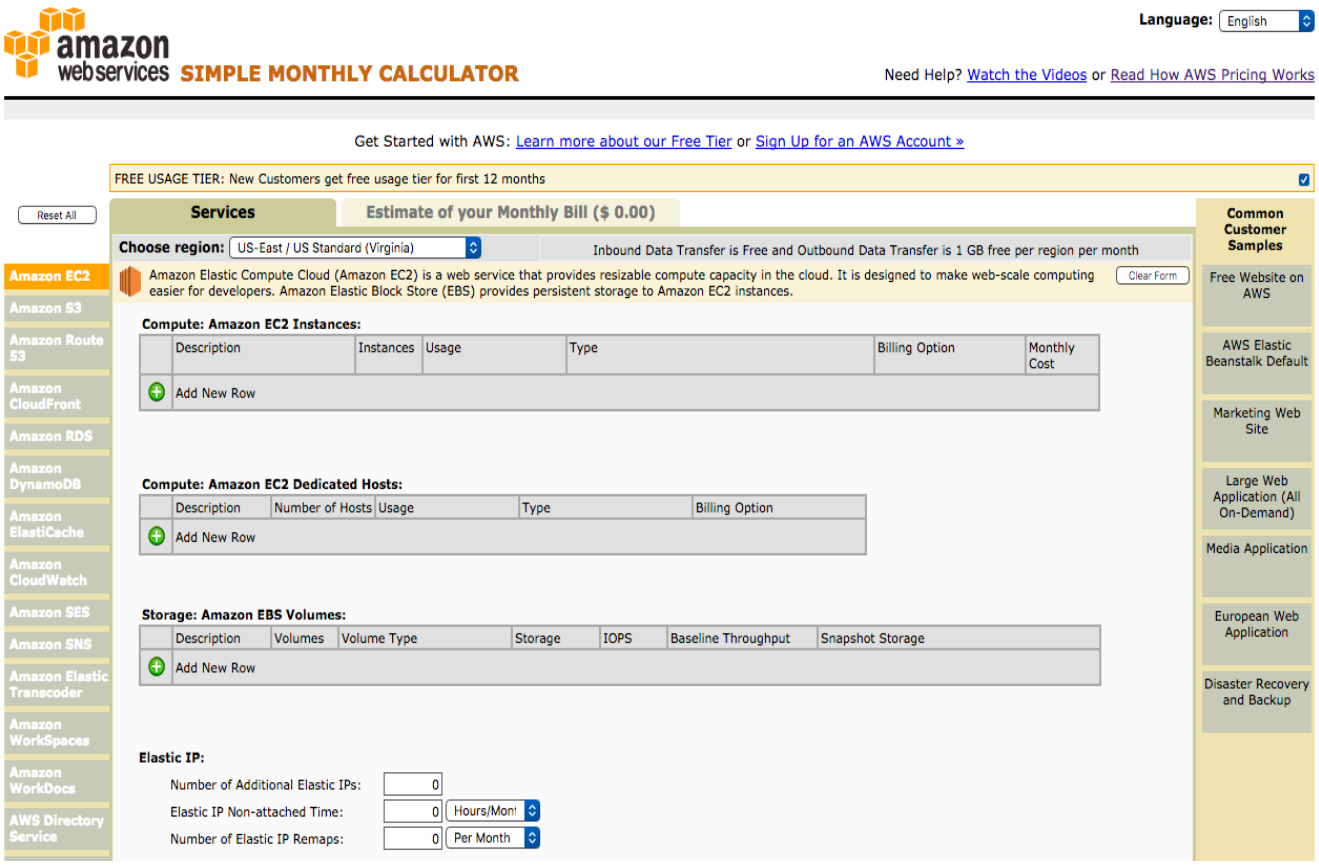

Рисунок 4.5 – Калькулятор місячних витрат Amazon Web Services

Обов’язково потрібно буде знати, які компоненти AWS можуть знадобитися, обсяг даних, який потрібно зберігати, і багато інших аспектів потенційного хмарного середовища.

Якщо немає всіх цих даних, AWS надає кілька поширених прикладів клієнтів, наприклад маркетинговий веб-сайт, великий веб-додаток на вимогу та сценарій аварійного відновлення та резервного копіювання.

Можна використовувати ці шаблони як відправні точки та налаштувати їх, щоб краще відповідати поточній ситуації.

Третій етап - оцінити витрати на впровадження хмарної міграції.

Також необхідно врахувати витрати, пов’язані з перенесенням IT-операцій у хмару.

Залежно від обсягу IT-інфраструктури та того, яку її частину планують перемістити в хмару, процес міграції може бути великим завданням.

Ось три компоненти, які слід враховувати під час розрахунку вартості процесу виконання хмарної міграції – переміщення даних у хмару, інтеграція та тестування додатків, гонорари консультантів.

Переміщення даних у хмару.

Дані є джерелом життя кожної компанії, і переміщення цих даних із локальних серверів у хмару є одним із найважливіших кроків у будь-якій хмарній міграції.

Переміщення даних може потребувати витрат на підключення до мережі, оскільки постачальники хмарних послуг можуть стягувати плату за передачу даних у свої системи.

Компанія, швидше за все, продовжуватиме використовувати бізнес-додатки, поки триватиме хмарна міграція, тому потрібно витратити час і гроші, щоб гарантувати, що дані у локальних системах не виходять із синхронізації з даними в хмарі.

Інтеграція та тестування додатків.

Деякі програми просто не зовсім готові до хмари. Незалежно від того, чи це застаріле програмне забезпечення чи більші системи планування ресурсів підприємства із функціональністю, яка залежить від локальної інфраструктури, вартість інтеграції та тестування цих програм після їх переміщення в хмару слід враховувати у розрахунках.

По-перше, потрібно буде витратити час на розуміння того, як ці програмні платформи взаємодіють із поточними операційними системами та інфраструктурою. Далі доведеться визначити зміни, необхідні для того, щоб ці системи добре взаємодіяли з хмарною інфраструктурою. Потім потрібно внести ці зміни та протестувати програми в хмарному середовищі. Все це вимагає часу та грошей, тому треба переконайтеся, що це виділено у бюджеті.

Гонорари консультантів.

Компанія може не мати всіх навичок і ресурсів, необхідних для повного виконання хмарної міграції. Хмарна міграція — це непросте завдання, і можуть знадобитися сторонні експерти, щоб допомогти у цьому. Знання та досвід консультантів у багатьох галузях і ситуаціях можуть бути дуже цінними, будь то складання стратегії, розробка рішення, виконання міграції чи все вищезазначене. Глибоке розуміння сильних і слабких сторін компанії, які стосуються хмарних обчислень і міграції, визначить, чи потрібна допомога експертів з хмарних технологій. Тоді компанія зможе приблизно оцінити витрати часу цих експертів на основі рівня допомоги, яка потрібна.

Четвертий етап - визначити приблизні витрати після міграції.

Основне питання, що доведеться оплачувати компанії після завершення міграції в хмару? Звичайно, доведеться сплачувати щомісячні витрати на інфраструктуру, які розрахували раніше. Але також треба взяти до уваги прямі та непрямі витрати, які доведеться заплатити, щоб підтримувати та покращувати нове хмарне середовище. Такі витрати, як безперервна інтеграція та тестування додатків, навчання, оплата праці, безпека та відповідність вимогам,

адміністрування та інші, потрібно спрогнозувати, щоб визначити точний бюджет після міграції.

П’ятий етап - порівняти витрати з матеріальними та нематеріальними вигодами.

Підрахувавши всі витрати, можна отримати велике число. Проте дуже ймовірно, що це число менше, ніж усі витрати, які зараз компанія може сплачувати за локальну інфраструктуру. Також необхідно розуміти, що хмара також приносить безліч нематеріальних переваг, які може бути важко безпосередньо виміряти. Це дозволить компанії бути набагато гнучкою, щоб швидше тестувати та запускати продукти та краще реагувати на зміни ринкових умов.

Компанії не доведеться турбуватися про покупку та налаштування нових серверів для задоволення високого попиту, оскільки можна миттєво автоматично масштабувати хмарні сервери.

Так, ключовою перевагою хмарних обчислень є реальна економія коштів, але ці менші переваги також є вагомою причиною розглянути можливість переходу до хмари.

Визначення вартості та переваг хмари вимагає стратегічного, цілісного підходу. Треба переконатися, що в компанії розуміють та враховують всі прямі та непрямі фактори, які впливають на хмарну міграцію. Тільки тоді можна по-справжньому розрахувати вплив хмари на бізнес [60].

ВИСНОВКИ

Розвиток хмарних обчислень у світі і в Україні має важливе значення для сучасного інформаційного суспільства. На даний час в Україні на законодавчому рівні закріплені такі поняття як «технологія хмарних обчислень», «хмара (хмарна інфраструктура)», «хмарна послуга», «хмарні ресурси», завдяки прийнятому у 2022 році Закону «Про хмарні послуги».

Подальше регулювання цього питання в Україні повинно здійснюватися з урахуванням світового досвіду та враховувати наявність війни в країні.

Акцент повинен бути зроблений на аналізі рішень та практик щодо безпеки хмарних обчислень, які вже успішно впроваджені у Європі, США та Канаді.

Для ефективного захисту інформації в системах хмарних обчислень в Україні, важливо враховувати міжнародний досвід і співпрацювати з відповідними організаціями.

Для цього потрібно:

- забезпечити активну участь України у міжнародних стандартизаційних організаціях і галузевих ініціативах, які ведуть розробку стандартів та рекомендацій для хмарних обчислень. Це допоможе впровадити найсучасніші світові практики в регулювання хмарних послуг;

- спрямувати зусилля на адаптацію світових стандартів та норм щодо безпеки інформації до умов України. Це включає в себе врахування особливостей, пов'язаних з війною, та розробку національних документів, які відповідали б унікальним вимогам країни;

- використовувати надійні заходи захисту даних та конфіденційності в хмарних обчисленнях в Україні. Це передбачає впровадження криптографічних методів, двофакторної аутентифікації, аудиту та моніторингу безпеки;

- взважено підходити до можливості передачі українськими державними органами, банками, іншими фінансовими організаціями інформації для зберігання на закордонні сервери. Вирішення цього питання повинно

враховувати ризики, пов'язані з іноземними регуляторними вимогами та забезпечувати надійний захист даних в будь-якому місці їх зберігання.

В цілому, успішне регулювання хмарних обчислень в Україні вимагає інтеграції світового досвіду, ретельного аналізу ризиків та надійного захисту інформації. Завдання полягає в створенні ефективної та безпечної інфраструктури хмарних обчислень, яка сприятиме розвитку сучасних інформаційних технологій в Україні.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Mohamed A. A history of cloud computing | Computer Weekly. ComputerWeekly.com. URL: http://www.computerweekly.com/feature/A-history-of-cloud-computing (date of access: 08.09.2023).

2. Douglas F. Parkhill. The Challenge of the Computer Utility. - Addison-Wesley Publishing Company, 1966 –246pp.

3. McFedries P. The cloud is the computer // IEEE Spectrum Online.-2008

4. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011.

5. Iso/iec 17788:2014. ISO. URL: https://www.iso.org/standard/60544.html (date of access: 08.09.2023).

6. Про хмарні послуги. Закон України від 17.02.2022 № 2075-IX URL: https://zakon.rada.gov.ua/laws/show/2075-20/ed20220217#n11 (дата звернення: 09.09.2023).

7. Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі / І.Ф. Аулов, І.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 194–201.

8. Андрощук, О., Головченко, О., Литовченко, Г., & Петрушен, М. (2021). Аналіз поняття хмарні технології: види, категорії, переваги та недоліки. Молодий вчений, 6 (94), 83-87, URL: https://doi.org/10.32839/2304-5809/2021-6-94-19 (дата звернення: 09.09.2023).

9. Андрейчиков А.В. Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. Москва : Финансы и статистика, 2000. 368 с.

10. Васильева И.В., Осипова Е.М., Петрова Н.Н. Психологические аспекты применения информационных технологий. Вопросы психологи. 2002. URL: http://www.vash-psiholog.info/voprospsih/219/18247-konferenciyapo-problemam-perinatalnoj-psixologii-i-mediciny.html (дата звернення: 10.09.2023)

11. International Organization for Standardization. ISO/IEC 22123-1:2023 (E), Information technology. Cloud computing. Part 1: Vocabulary vocabulary. (second edition 2023-02) URL: https://www.iso.org/standard/82758.html (date of access: 10.09.2023).

12. Rountree D., Castrillo I. Cloud Deployment Models. The Basics of Cloud Computing. Understanding the Fundamentals of Cloud Computing in Theory and Practice. Elsevier. 2014. P.35-47 URL:http://www.iqytechnicalcollege.com/The%20Basics%20of%20Cloud%20Computing.pdf (date of access: 10.09.2023).

13. Cloud computing security URL: http://en.wikipedia.org/wiki/Cloud_ computing_security (date of access: 11.09.2023).

14. Bertino E. L. Security for Web Services and Service-Oriented Architectures [Text] / E. L. Bertino // Proceedings of the 2th Annual International Conference on Information Security, New York, USA., September 2-7, 2012 y. - pp. 35-69.

15. Dawoud W, Takouna I, Meinel C: Infrastructure as a service security: Challenges and solutions. In the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. Washington, DC, USA: IEEE Computer Society; 2010:1–8. URL: https://ieeexplore.ieee.org/abstract/document/5461732 (date of access: 11.09.2023).

16. Top threats working group | CSA. Home | CSA. URL: https://cloudsecurityalliance.org/research/top-threats (date of access: 11.09.2023).

17. Carlin S, Curran K: Cloud Computing Security. International Journal of Ambient Computing and Intelligence 2011, 3(1):38–46. URL: https://www.igi-global.com/chapter/cloud-computing-security/68920 (date of access: 12.09.2023).

18. ENISA: Cloud Computing: benefits, risks and recommendations for information Security. 2009. URL: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (date of access: 12.09.2023).

19. Viega J: Cloud Computing and the common Man. Computer 2009, 42 (8): 106 – 108
URL:https://www.computer.org/csdl/magazine/co/2009/08/mco2009080106/13rRUwghdcy (date of access: 12.09.2023).

20. Ertaul L, Singhal S, Gökay S: Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM' 10. Las Vegas, US: CSREA Press; 2010:36–42. URL: https://www.researchgate.net/profile/Levent-Ertaul-2/publication/267697749_Security_Challenges_in_Cloud_Computing/links/54984b260cf2519f5a1dddb4/Security-Challenges-in-Cloud-Computing.pdf (date of access: 13.09.2023).

21. Bisong A., M. Rahman S. S. An overview of the security concerns in enterprise cloud computing. International journal of network security & its applications. 2011. Vol. 3, no. 1. P. 30–45. URL: https://doi.org/10.5121/ijnsa.2011.3103 (date of access: 13.09.2023).

22. Grobauer B., Walloschek T., Stocker E. Understanding cloud computing vulnerabilities. IEEE security & privacy magazine. 2011. Vol. 9, no. 2. P. 50–57. URL: https://doi.org/10.1109/msp.2010.115 (date of access: 14.09.2023).

23. Jansen W. A. Cloud hooks: security and privacy issues in cloud computing. 2011 44th hawaii international conference on system sciences (HICSS 2011), Kauai, HI, 4–7 January 2011. 2011. URL: https://doi.org/10.1109/hicss.2011.103 (date of access: 14.09.2023).

24. Townsend M. Managing a security program in a cloud computing environment. 2009 information security curriculum development conference, Kennesaw, Georgia, 25–26 September 2009. New York, New York, USA, 2009. URL: https://doi.org/10.1145/1940976.1941001 (date of access: 14.09.2023).

25. Winkler V: Securing the Cloud: Cloud computer Security techniques and tactics. Waltham, MA: Elsevier Inc; 2011.

26. Ranjith P., Priya C., Shalini K. On covert channels between virtual machines. Journal in computer virology. 2012. Vol. 8, no. 3. P. 85–97. URL: https://doi.org/10.1007/s11416-012-0168-x (date of access: 15.09.2023).

27. Hey, you, get off of my cloud / T. Ristenpart et al. The 16th ACM conference, Chicago, Illinois, USA, 9–13 November 2009. New York, New York, USA, 2009. URL: https://doi.org/10.1145/1653662.1653687 (date of access: 15.09.2023).

28. Cross-VM side channels and their use to extract private keys / Y. Zhang et al. The 2012 ACM conference, Raleigh, North Carolina, USA, 16–18 October 2012. New York, New York, USA, 2012. URL: https://doi.org/10.1145/2382196.2382230 (date of access: 15.09.2023).

29. Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley; 2005:227–229. URL: https://www.usenix.org/legacy/events/hotos05/final_papers/full_papers/garfinkel/garfinkel.pdf (date of access: 16.09.2023).

30. Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

31. Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.

32. Wang Z., Jiang X. HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. 2010 IEEE symposium on security and privacy, Oakland, CA, USA, 16–19 May 2010. 2010. URL: https://doi.org/10.1109/sp.2010.30 (date of access: 16.09.2023).

33. Network security for virtual machine in cloud computing / Hanqian Wu et al. 2010 5th international conference on computer sciences and convergence information technology (ICCIT 2010), Seoul, 30 November – 2 December 2010. 2010. URL: https://doi.org/10.1109/iccit.2010.5711022 (date of access: 16.09.2023).

34 An analysis of security issues for cloud computing/ K. Hashizume et al. Journal of Internet Services and Applications. 2013. Vol. 4, no. 1. P. 5. URL: https://doi.org/10.1186/1869-0238-4-5 (date of access: 17.09.2023).

35. Коломійцев О., Голубничий Д., Третяк В., Рибальченко А., Любченко О., Полтавський Е., Кривчун В., Крамар О., Шутіков О., Туленко М., & Третяк А. (2023). Використання методів рангового підходу до рішення задачі оптимізації розміщення засобів захисту інформації в хмарному середовищі. Scientific Collection «InterConf+», (29 (139), 274–292. URL: https://doi.org/10.51582/interconf.19-20.01.2023.028 (дата звернення: 17.09.2023).

36. Жилін, А. Проблематика захисту інформаційних ресурсів при використанні хмарних технологій / Артем Жилін, Андрій Дівіцький, Анна Козачок // Information Technology and Security. – 2019. – Vol. 7, Iss. 2 (13). – Pp. 171–182. – Bibliogr.: 17 ref.

37. Червякова Т.І. Інформаційна безпека технології хмарних обчислень. / Т.І. Червякова // Вісник Національного транспортного університету. Серія «Технічні науки». Науково-технічний збірник. – К.: НТУ, 2020. – Вип. 1 (46).

38. 2023 State of the Cloud Report. URL: https://info.flexera.com/CM-REPORT-State-of-the-Cloud (date of access: 17.09.2023).

39. Home - Cloud Industry Forum. URL: https://cloudindustryforum.org/wp-content/uploads/2022/11/transformational-impact-cloud-Fujitsu-2022.pdf (date of access: 17.09.2023).

40. HashiCorp state of cloud. HashiCorp. URL: https://www.hashicorp.com/state-of-the-cloud (date of access: 17.09.2023).

41. Pearl M., Blest A. Cloud computing: global overview. Lexology. URL: https://www.lexology.com/library/detail.aspx?g=9041b95a-8d2f-4dd8-8647-5b2a2d2ea9fd (date of access: 18.09.2023).

42. Abbas, Zaheer, and Seunghwan Myeong. 2023. "Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through

Machine Learning Tools in Cloud Computing Environment" Electronics 12, no. 12: 2650. URL : https://doi.org/10.3390/electronics12122650 (date of access: 18.09.2023).

43. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179 : станом на 4 травня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/179-2021-п#Text (дата звернення: 18.09.2023).

44. Про використання банками хмарних послуг в умовах воєнного стану в Україні: Постанова Національного банку України від 08.03.2022 р. № 42. URL: https://zakon.rada.gov.ua/laws/show/v0042500-22#Text (дата звернення: 18.09.2023).

45. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12 березня № 263 URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення: 18.09.2023).

46. Деякі питання забезпечення функціонування державних інформаційних ресурсів: Постанова Кабінету Міністрів України від 30.12.2022 р. № 1500. URL: https://zakon.rada.gov.ua/laws/show/1500-2022-п#Text (дата звернення: 19.09.2023).

47. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «Unleashing the Potential of Cloud Computing in Europe». 2012. COM/2012/0529 final. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:en:PDF (date of access: 19.09.2023).

48. About EU cloud coc: EU cloud coc. Home: EU Cloud CoC. URL: https://eucoc.cloud/en/about/about-eu-cloud-coc/ (date of access: 19.09.2023).

49. ECP | Platform voor de InformatieSamenleving. URL: https://ecp.nl/wp-content/uploads/2020/01/PT-2019-CSP-CERT-WG-Recommendations-for-the-implementation-of-the-CSP-Certification-scheme-20190607-Final-version.pdf (date of access: 19.09.2023).

50. Cybersecurity Certification: Candidate EUCC Scheme V1.1.1. ENISA. URL: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1 (date of access: 19.09.2023).

51. Cloud Service Level Agreement Standardisation Guidelines. 24 June 2014. URL: https://digital-strategy.ec.europa.eu/en/news/cloudservice-level-agreement-standardisation-guidelines (date of access: 20.09.2023)

52. Cloud Data Management Interface (CDMI™) | SNIA. SNIA | Experts on Data. URL: https://www.snia.org/cdmi (date of access: 20.09.2023).

53. International Organization for Standardization. ISO/IEC 22123-1:2023 (E), Information technology — Cloud computing — Part 2: Concepts. URL: https://www.iso.org/standard/80351.html (date of access: 20.09.2023)

54. International Organization for Standardization. ISO/IEC 22123-1:2023 (E), Information technology — Cloud computing — Part 3: Reference architecture Information technology. URL: https://www.iso.org/standard/82759.html (date of access: 20.09.2023).

55. International Organization for Standardization. (2015, Dec. 8). ISO/IEC TS 27017, Information technology. Security techniques. Information security management. Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002. URL: https://www.iso.org/standard/43757.html (date of access: 20.09.2023).

56. International Organization for Standardization. (2019, Jan. 24). ISO/IEC 27018, Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. URL: https://www.iso.org/standard/76559.html (date of access: 21.09.2023).

57. Гогілашвілі Є. Що чекає на ринок хмарних послуг в Україні. Speka - онлайн медіа про технології та підприємництво | SPEKA.media | SPEKA.media. URL: https://speka.media/shho-cekaje-na-rinok-xmarnix-poslug-v-ukrayini-pjkq19 (дата звернення: 21.09.2023).

58. Cloud Storage Pricing in 2023: Everything You Need to Know. Enterprise Storage Forum. URL: https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing (date of access: 21.09.2023).

59. How To Determine The Cost Of Cloud Computing (2023 UPDATE). CloudZero. URL: https://www.cloudzero.com/blog/cost-of-cloud-computing (date of access: 21.09.2023).

60. Cost of Cloud Computing: How to Calculate the True Cost of Moving to the Cloud - Thorn Technologies. Thorn Technologies. URL: https://thorntech.com/cost-of-cloud-computing-how-to-calculate-the-true-cost-of-moving-to-the-cloud/ (date of access: 21.09.2023).