ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

+

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення безпеки мережевих систем у сфері інтернет-провайдингу; хмарні сховища та стратегії резервування»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

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

_____ Артур КОРНУС
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД-42
Артур КОРНУС
Ім'я, ПРІЗВИЩЕ
Керівник: Іван ШАХМАТОВ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Корнусу Артуру Віталійовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Удосконалення безпеки мережевих систем у сфері інтернет-провайдингу; хмарні сховища та стратегії резервування

керівник кваліфікаційної роботи Іван ШАХМАТОВ
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1.Науково-технічна література з теми бакалаврської роботи.
2.Принцип функціонування мережі «Інтернет»
3.Основні принципи кібер-безпеки

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Захист інтернет-провайдера від зовнішніх кібер-загроз
2.Хмарні сховища та їх реалізація у сфері надання послуги інтернет
3.Розробка найдоцільнішої стратегії резервування для інтернет-провайдера
4.Розробка додатку для перегляду подій, логів, резервування та шифрування/дешифрування даних

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	27.02-05.03.2024	
2	Обгрунтування актуальності роботи	06.03-11.03.2024	
3	Аналіз принципів та методів безпеки	12.03-27.03.2024	
4	Аналіз існуючих хмарних рішень	28.03-10.04.2024	
5	Розробка додатку для моніторингу, бекапу та шифрування	11.04-15.05.2024	
7	Оформлення роботи: вступ, висновки, реферат	16.05-22.05.2024	
8	Розробка демонстраційних матеріалів	23.05-24.05.2024	

Здобувач вищої освіти _____ Артур КОРНУС
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Іван ШАХМАТОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавр: 68 стор., 9 табл., 6 рис., 15 джерел.

Мета роботи – Вивчення усіх можливих загроз та методів уникнення цих загроз інтернет-провайдерами, з використанням хмарних сховищ.

Об'єкт дослідження- мережеві системи інтернет провайдерів.

Предмет дослідження – механізми забезпечення безпеки даних у мережах інтернет-провайдингу, з особливим акцентом на хмарні сховища та стратегії резервування.

Короткий зміст роботи: У роботі проаналізовано можливі вектори атак, типи та їх види; типи хмарних сховищ, які можна використати у сфері інтернет-провайдингу, а також типи резервування, та стратегії їх використання. Також була створена программа, за допомогою якої можна проводити аудит безпеки, перегляд логів, шифрування файлів, та резервування у хмарне сховище.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ-ПРОВАЙДЕР, ХМАРНІ СХОВИЩА, DDoS, ФІШИНГ, ШИФРУВАННЯ, РЕЗЕРВНЕ КОПІЮВАННЯ, АУДИТ БЕЗПЕКИ, ПОЛІТИКИ БЕЗПЕКИ

ABSTRACT

Text part of the bachelor level qualification work: 68 pages, 6 pictures, 9 table, 15 sources.

The purpose of the work - is to study all possible threats and methods of avoiding these threats by Internet providers using cloud storage.

Object of research is network systems of internet service providers.

Subject of research is data security mechanisms in Internet service networks, with a special emphasis on cloud storage and backup strategies.

Summary of the work: The work analyzes possible attack vectors, types and their types; types of cloud storage that can be used in the field of Internet provision, as well as types of backup, and strategies for their use. Also, a program was created that allows you to conduct security audits, view logs, encrypt files, and back up to cloud storage..

KEYWORDS: INTERNET SERVICE PROVIDER, CLOUD STORAGE, DDoS, PHISHING, ENCRYPTION, BACKUP, SECURITY AUDIT, SECURITY POLICIES

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут _____

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

Направляється здобувач _____ до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю _____
(код, найменування спеціальності)
освітньо-професійної програми _____
(назва)
на тему:
«_____».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ _____
(підпис) (Ім'я, ПРІЗВИЩЕ)

Висновок керівника кваліфікаційної роботи

Здобувач _____
_____
_____
_____

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача _____ на оцінку «_____» та присвоїти йому кваліфікацію _____.

Керівник кваліфікаційної роботи _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) _____ допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою _____ _____ _____
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня бакалавра

здобувача вищої освіти _____
(прізвище, ім'я, по батькові)
на тему «_____»

Актуальність.
_____
_____
_____

Позитивні сторони.
1.
2.
3.

Недоліки.
1.
2.
Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи бакалаврської.

Висновок: *кваліфікаційна робота на здобуття ступеня бакалавра заслуговує оцінку "_____", а здобувач _____ заслуговує присвоєння кваліфікації: ……..*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП

В сучасному світі, де інформація стала одним із ключових активів ведення бізнесу, забезпечення безпеки мережевих систем набуває особливої важливості. Інтернет-провайдери, що управляють великими обсягами чутливих даних, стикаються з необхідністю захисту цих даних від зовнішніх загроз та внутрішніх вразливостей. В рамках даної дипломної роботи розглядається проблематика удосконалення безпеки мережевих систем у сфері інтернет-провайдингу через впровадження хмарних сховищ та стратегій резервування[1].

Актуальність дослідження обумовлена зростанням кіберзагроз і складністю захисту великих даних у мережевих системах. За останні роки збільшилась кількість кібератак, що спрямовані на провайдерів інтернет-послуг, що підкреслює потребу у вдосконаленні існуючих механізмів безпеки. Використання хмарних технологій та стратегій резервування може стати ефективним рішенням для мінімізації потенційних ризиків і забезпечення стійкості до кіберзагроз.

Актуальність цієї теми підкріплюється не тільки зростаючою потребою у захисті інформації в інтернет-середовищі, але й стрімким розвитком хмарних технологій, що пропонують нові можливості для забезпечення безпеки. Захист даних стає особливо критичним у контексті постійно зростаючої кількості кібератак, зокрема у сфері інтернет-провайдингу. Враховуючи, що провайдери є основними "воротами" до мережі для багатьох користувачів, їх роль у захисті приватної інформації є незаперечною.

Предметом дослідження тут будуть механізми забезпечення безпеки даних у мережах інтернет-провайдингу, з особливим акцентом на хмарні сховища та стратегії резервування. Дослідження охоплює аналіз вразливостей, загроз і методів захисту, а також розгляд сучасних технологічних рішень.

Предмет дослідження розширюється на аналіз сучасних і потенційно нових методологій управління та захисту інформації в хмарних середовищах, включно з критичним оцінюванням їх вразливостей і ефективності. Це охоплює дослідження новітніх розробок у сфері криптографічного захисту даних, ідентифікацію та

оцінку надійності хмарних сервісів і технологій. Спеціальна увага приділяється вивченню механізмів виявлення і реагування на інциденти безпеки, що є особливо важливим в контексті постійно змінюваних загроз у кіберпросторі. Такий підхід дозволяє не лише захистити існуючі системи, але й адаптувати інтернет-провайдерів до майбутніх викликів у галузі мережевої безпеки[2].

Мета роботи полягає у вдосконаленні стратегій безпеки мережевих систем, що використовуються інтернет-провайдерами, через аналіз та впровадження ефективних технологій хмарного зберігання та резервного копіювання даних. Робота передбачає розробку комплексних підходів для зміцнення безпеки і забезпечення високого рівня надійності і доступності оброблюваних даних.

Мета роботи детально виражає прагнення не лише розробити, але й глибоко інтегрувати новітні хмарні технології і стратегії резервування для зміцнення безпеки мережевих систем інтернет-провайдерів. Окрім того, ця мета включає в себе розробку настанов та рекомендацій для оптимізації існуючих заходів безпеки, що дозволить провайдерам пристосуватися до постійно мінливих умов кіберпростору та ефективно реагувати на нові загрози. Завдяки цьому можна досягти не тільки зниження ризиків пов’язаних із втратою або компрометацією даних, а й підвищення загальної надійності та доступності сервісів інтернет-провайдерів[3].

Об'єктом дослідження цієї дипломної роботи виступають мережеві системи інтернет-провайдерів. Ці системи є критично важливими інфраструктурами, що забезпечують доступ до інтернет-ресурсів та обробку великих обсягів даних.

З огляду на вищезазначене, дана робота має важливе значення для підвищення рівня безпеки в індустрії інтернет-провайдингу. Вона сприяє розумінню поточних викликів та визначенню шляхів вдосконалення існуючих систем захисту. Аналіз сучасних підходів до резервування даних та використання хмарних сховищ дасть можливість виявити найбільш ефективні стратегії для забезпечення надійної роботи мережевих систем, що в свою чергу дозволить

інтернет-провайдерам впроваджувати інноваційні технології, спрямовані на зміцнення їхньої конкурентоспроможності у цій галузі.

Ця дипломна робота спрямована на глибокий аналіз та впровадження передових рішень, що дозволять інтернет-провайдерам підвищити ефективність своїх мережевих систем і гарантувати надійний захист даних.

1. ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Огляд мережевих систем і їх вразливостей

В цьому підрозділі ми зосереджуємося на глибокому аналізі мережевих систем, які використовуються інтернет-провайдерами, з особливим акцентом на виявлення їх потенційних вразливостей. Мережеві системи відіграють ключову роль у забезпеченні доступу до інтернету і управлінні трафіком даних, включаючи особисту інформацію користувачів, комерційні дані та інші чутливі ресурси. Охорона цих систем від зловмисників стає все більш складною задачею через широкий спектр потенційних кіберзагроз.

Типи мережевих систем

Мережеві системи можуть бути класифіковані за різними критеріями: за масштабами (локальні, корпоративні, глобальні), за типом використання (приватні, публічні, гібридні) та за технологією фізичної реалізації (дротові, бездротові). Кожен тип має свої унікальні вразливості, які потребують специфічних заходів безпеки. Наприклад, бездротові мережі часто схильні до атак на перехоплення даних через відкритий характер сигналів[4].

Вразливості мережевих систем

Вразливості в мережевих системах можуть бути викликані різними факторами, включаючи:

1. Технічні недоліки: слабкі місця в програмному забезпеченні, такі як невиправлені баги або застаріле програмне забезпечення, можуть дозволити зловмисникам здійснювати атаки.
2. Конфігураційні помилки: неправильне налаштування мережевих компонентів може залишити "відкриті двері" для несанкціонованого доступу.
3. Фізичний доступ: незахищене місцезнаходження обладнання може спричинити його фізичне пошкодження або несанкціонований доступ.

4. Людський фактор: помилки з боку співробітників або недостатнє навчання можуть спричинити випадкові або умисні порушення безпеки.

Загрози для мережевих систем

Загрози для мережевих систем інтернет-провайдерів різноманітні та включають[5]:

- Denial-of-Service (DoS) атаки: направлені на перевантаження ресурсів системи, що робить її недоступною для легітимних користувачів.
- Man-in-the-Middle (MitM) атаки: зловмисники перехоплюють та можуть модифікувати дані, що передаються між двома сторонами.
- Розповсюдження шкідливого програмного забезпечення: Віруси та трояни, які можуть бути розповсюджені через мережу, інфікуючи хости та поширюючи зловмисне програмне забезпечення.
- Phishing та інші види соціальної інженерії: спрямовані на отримання конфіденційної інформації від користувачів через обман.

Методи захисту мережевих систем

Для захисту мережевих систем використовуються різноманітні методи:

1. Шифрування: захист даних від несанкціонованого доступу через шифрування інформації, передаваної між мережевими вузлами.
2. Використання файрволів: контроль трафіку, що входить і виходить з мережі, для виявлення та блокування підозрілих або шкідливих пакетів.
3. Інтрузійні системи виявлення та запобігання (IDS/IPS): моніторинг мережі на предмет ознак атак та активне втручання для запобігання потенційних загроз.
4. Регулярні аудити безпеки та пенетраційні тести: перевірка систем на вразливості та їх усунення перед тим, як зловмисники зможуть їх використати.
5. Політика безпеки та навчання співробітників: розробка чітких правил та процедур для забезпечення безпеки, а також проведення навчань для підвищення обізнаності персоналу щодо потенційних кіберзагроз.

Здійснений аналіз мережевих систем і їх вразливостей виявив, що комплексність сучасних мережевих інфраструктур і різноманіття можливих загроз вимагають ретельного підходу до захисту даних. Вразливості можуть виникати на різних рівнях, від фізичного доступу до технологічних недоліків, і кожна з них може стати потенційним вектором для атак. Основні загрози, такі як DoS, MitM, шкідливе програмне забезпечення та соціальна інженерія, демонструють потребу в інтегрованих заходах безпеки, що включають шифрування, використання файрволів, системи IDS/IPS, а також регулярні аудити та пенетраційні тести. Важливість правильної настройки і обслуговування систем, а також постійне навчання персоналу щодо кібербезпеки є ключовими елементами для захисту мережевих ресурсів інтернет-провайдерів. Цей огляд не тільки виявляє основні слабкі місця і загрози, але й підкреслює важливість інтегрованого підходу до захисту мережевих систем. В наступних розділах будуть розглянуті конкретні технології та методики, які можуть бути використані для покращення мережевої безпеки[6].

1.2 Принципи і методи забезпечення мережевої безпеки

Забезпечення мережевої безпеки є складним процесом, що включає в себе багатошаровий підхід до захисту інформації та інфраструктури. Цей підхід обумовлений необхідністю забезпечення конфіденційності, цілісності та доступності (CIA - Confidentiality, Integrity, and Availability) інформаційних активів. Для ефективного захисту мережевих систем інтернет-провайдерів важливо розуміти основні принципи та методи, які використовуються у мережевій безпеці.

Основні принципи мережевої безпеки

Конфіденційність вимагає, щоб доступ до інформації мав лише авторизований персонал. Це забезпечується за допомогою методів шифрування, аутентифікації користувачів та контролю доступу[7].

Цілісність означає захист даних від несанкціонованих змін, як під час передачі, так і при зберіганні. Методи, які забезпечують цілісність, включають криптографічні хеш-функції та цифрові підписи, які дозволяють перевіряти, чи була інформація змінена під час передачі[7].

Доступність забезпечується через надійність мережевої інфраструктури та швидке відновлення системи після збоїв. Заходи, такі як резервне копіювання даних та балансування навантаження, критично важливі для підтримання доступності ресурсів[7].

Методи забезпечення мережевої безпеки

Забезпечення мережевої безпеки включає різноманітні технології та практики, серед яких:

1. Шифрування: використання сильного шифрування для захисту даних, що передаються через мережу або зберігаються на серверах. Важливим є вибір надійних алгоритмів та ключів достатньої довжини.
2. Брандмауери (Firewalls): конфігурування брандмауерів для контролю трафіку, що входить і виходить із мережі, допомагає запобігти несанкціонованому доступу та атакам.
3. Системи виявлення та запобігання вторгненням (IDS/IPS): моніторинг мережі на наявність підозрілих активностей та відповідне реагування на потенційні загрози.
4. Менеджмент патчів і оновлень: регулярне оновлення програмного забезпечення, операційних систем та мережевого обладнання для виправлення вразливостей.
5. Фізичний захист: забезпечення захисту фізичного доступу до мережевого обладнання, що може включати блокування серверних приміщень та охоронні системи.
6. Багаторівневий захист (Defense in Depth): використання комбінації різних заходів безпеки на різних рівнях мережі, щоб забезпечити, що в разі прориву одного захисту інші залишаться на місці.

7. Політики безпеки і процедури: розробка та впровадження стандартів і процедур, які регулюють використання та управління мережевими ресурсами, включаючи політики доступу, парольну політику та політики відповіді на інциденти.
8. Навчання та обізнаність персоналу: проведення регулярних тренінгів з безпеки для збільшення обізнаності працівників щодо потенційних кіберзагроз та навчання правильним реакціям на інциденти безпеки.

Ефективне забезпечення мережевої безпеки вимагає інтеграції різноманітних заходів та методик, заснованих на принципах конфіденційності, цілісності та доступності інформації. Важливими компонентами такої системи безпеки є впровадження сучасних технологій шифрування, налаштування брандмауерів, застосування систем виявлення та запобігання вторгненням, постійний менеджмент патчів і оновлень, а також фізичний захист інфраструктури. Окрім технічних заходів, велике значення мають розробка та дотримання суворих політик безпеки, а також регулярне навчання персоналу для підвищення рівня обізнаності щодо кіберзагроз. Такий всеохоплюючий підхід дозволяє створити надійну систему захисту, яка може адаптуватися до змін у сфері кіберзагроз та технологій. Успішне впровадження цих методів вимагає комплексного підходу та постійної уваги до динамічного ландшафту кіберзагроз. Наступний розділ більш детально розгляне роль хмарних технологій у забезпеченні мережевої безпеки, враховуючи їх все зростаючу популярність та використання в інфраструктурі інтернет-провайдингу.

1.3 Роль хмарних технологій у мережевій безпеці

Хмарні технології стали невід'ємною частиною сучасних мережевих систем, пропонуючи значні переваги у термінах масштабованості, гнучкості та вартості зберігання даних. Водночас, інтеграція хмарних рішень у мережеві системи також вносить нові виклики для безпеки, які потребують уважного розгляду та адресації[8].

Вплив хмарних технологій на мережеву безпеку

Хмарні сервіси змінюють традиційні підходи до мережевої безпеки, оскільки дані та обчислювальні процеси переміщуються з локальних центрів обробки даних до віддалених хмарних серверів. Ця трансформація вимагає нових методів захисту даних, а також розгляду нових векторів атак, які стають можливими завдяки централізації ресурсів.

Доступ до даних

Хмарні сервіси дозволяють користувачам доступ до даних з будь-якої точки світу, що збільшує ризики несанкціонованого доступу та вимагає суровіших методів аутентифікації та авторизації.

Керування ідентичністю та доступом (IAM)

Ефективне управління ідентичностями та доступом є критичним для забезпечення того, щоб тільки уповноважені користувачі мали доступ до хмарних ресурсів. Це включає в себе застосування політик мінімальних привілеїв та сегментацію доступу до ресурсів.

Шифрування даних

Використання сильного шифрування для захисту даних, що передаються та зберігаються в хмарі, є необхідним для запобігання їх витоку чи зловмисного використання.

Моніторинг

Належне ведення журналів та моніторинг активності в хмарному середовищі допомагає виявляти та реагувати на безпекові інциденти в реальному часі.

Виклики безпеки хмарних технологій

Під час впровадження хмарних технологій організації стикаються з низкою викликів, які необхідно вирішувати для забезпечення належного рівня безпеки:

— Керування вендорами: оскільки дані та обчислювальні процеси часто обробляються третіми сторонами, необхідно мати суворі угоди про рівень сервісу (SLA) та ретельно відслідковувати їх дотримання.

— Комплаєнс та відповідність стандартам: забезпечення відповідності діяльності хмарних сервісів регуляторним вимогам та стандартам безпеки є складним, але важливим аспектом.
— Кіберзагрози: хмарні платформи є привабливими цілями для кібератак, оскільки вони зберігають велику кількість цінних даних. Необхідно постійно аналізувати та адаптуватися до нових типів атак.

Переваги використання хмарних технологій для безпеки

Використання хмарних рішень також пропонує значні переваги для забезпечення безпеки:

1. Масштабування безпеки

Хмарні платформи дозволяють швидко збільшувати обсяги ресурсів для безпеки у відповідь на змінні потреби без необхідності великих капіталовкладень.

2. Вдосконалені інструменти безпеки

Багато хмарних провайдерів пропонують передові інструменти для керування безпекою, які включають штучний інтелект та машинне навчання для виявлення загроз.

3. Розподіл відповідальності

Хмарні сервіси часто пропонують модель спільної відповідальності, де хмарний провайдер відповідає за безпеку інфраструктури, а клієнт — за захист своїх даних і додатків.

Узагальнюючи, хмарні технології відіграють ключову роль у сучасній мережевій безпеці, пропонуючи нові можливості для захисту та управління даними. Однак, їх впровадження має бути супроводжене стратегічним підходом до кібербезпеки, що враховує нові виклики та можливості, які пропонують хмарні рішення. В наступному підрозділі буде розглянуто конкретні види хмарних сховищ та їхні особливості з точки зору мережевої безпеки.

1.4 Види хмарних сховищ: публічні, приватні, гібридні

Хмарні сховища відіграють важливу роль у сучасній інформаційній інфраструктурі, надаючи організаціям гнучкість у зберіганні, обробці та доступі до даних. Залежно від моделі впровадження, хмарні сховища класифікуються на публічні, приватні та гібридні, кожен із яких має свої переваги та недоліки, особливо з точки зору безпеки.

Публічні хмарні сховища забезпечують послуги зберігання даних на інфраструктурі, яка належить та управляється зовнішніми провайдерами. Ці провайдери пропонують ресурси, такі як сервери та сховища, які користувачі можуть використовувати на основі підписки. Публічні хмарні сховища привабливі через їх масштабованість та відносно низьку вартість впровадження, оскільки користувачі платять лише за те, що використовують. Однак, цей тип хмарних сховищ також має підвищені ризики безпеки через менший контроль над інфраструктурою та спільне використання ресурсів з іншими організаціями, що може створювати додаткові вектори атак.

Приватні хмарні сховища, в свою чергу, є ексклюзивними для однієї організації та зазвичай розміщуються на власній території або у дата-центрі, який контролюється організацією. Це дозволяє компаніям мати повний контроль над своїми даними та інфраструктурою, що значно збільшує безпеку та знижує залежність від третіх сторін. Приватні хмарні сховища часто використовуються для обробки особливо чутливої інформації або для виконання бізнес-операцій, що вимагають високого рівня контролю та налаштувань безпеки.

Гібридні хмарні сховища комбінують елементи публічних та приватних хмар, дозволяючи організаціям використовувати переваги обох світів. В такому випадку, чутливі або критично важливі операції можуть оброблятися в приватному хмарному сховищі, тоді як менш чутливі функції можуть бути делеговані публічним хмарним сервісам. Гібридні хмарні сховища особливо корисні для досягнення балансу між гнучкістю та контролем, дозволяючи

компаніям масштабувати свої IT-операції залежно від поточних потреб і бізнес-вимог.

Хмарні сховища, які поділені на публічні, приватні та гібридні типи, відіграють критичну роль у забезпеченні гнучкості, масштабованості та доступності ресурсів для сучасних організацій. Публічні хмарні сховища пропонують економію та простоту використання, але часто мають більші ризики безпеки через спільне використання ресурсів. Приватні хмарні сховища надають більший контроль та безпеку, ідеально підходячи для обробки чутливої інформації. Гібридні моделі, поєднуючи елементи обох, дозволяють досягнути оптимального балансу між контролем та гнучкістю, вирішуючи тим самим різні бізнес-потреби з урахуванням вимог безпеки. Вибір між цими типами хмарних сховищ залежить від специфічних потреб організації у сфері безпеки, регуляторних вимог, фінансових можливостей та стратегічних цілей. Кожен тип пропонує різні рівні гнучкості, контролю та безпеки, і рішення про впровадження тієї чи іншої моделі повинно базуватися на ретельному аналізі цих факторів. Незалежно від обраної моделі, ключовим аспектом залишається впровадження строгих політик безпеки та постійний моніторинг системи для захисту даних та IT-інфраструктури.

2. ПРОБЛЕМИ БЕЗПЕКИ В СФЕРІ ІНТЕРНЕТ-ПРОВАЙДИНГУ

2.1 Аналіз типових загроз і атак на мережеві системи провайдерів

Інтернет-провайдери стикаються з постійно зростаючою кількістю загроз, які вимагають складних і постійно адаптованих методів захисту. Внаслідок їхньої ролі як медіаторів в доступі до інтернету для користувачів та організацій, мережеві системи провайдерів стають цілями для різноманітних атак, що мають на меті перехоплення, зміну чи знищення даних[9].

Однією з основних загроз для мережевих систем є **Distributed Denial of Service (DDoS) атаки**, при яких зловмисники використовують велику кількість зомбі-комп'ютерів або ботів для генерації величезної кількості трафіку, що перевантажує системи і робить їх недоступними для легітимних користувачів. Такі атаки не тільки порушують нормальну роботу мережі, але й можуть слугувати прикриттям для інших маліційних дій, таких як вторгнення в систему чи крадіжка даних.

Атаки на інфраструктуру можуть включати вразливості в роутерах, комутаторах та іншому мережевому обладнанні. Хакери можуть використовувати відомі баги у програмному забезпеченні, щоб отримати несанкціонований доступ до мережі та маніпулювати мережевим трафіком. Це може призвести до серйозних проблем з безпекою, таких як перехоплення чутливої інформації або внесення змін до трафіку даних.

Атаки на програмне забезпечення, такі як експлуатація нульових днів (zero-day exploits), стають все більш звичним явищем. Зловмисники використовують неопубліковані вразливості у програмному забезпеченні, що встановлене на мережевому обладнанні, для впровадження шкідливого коду або для отримання контролю над системою.

Для кращого розуміння всіх основних типів кіберзагроз, з якими можуть стикатися інтернет-провайдери, було створено таблицю. Для кожної загрози надано детальний опис та перелічено стратегії реагування, які можуть бути

застосовані для мінімізації ризиків і забезпечення захисту мережевих ресурсів. Ця таблиця допоможе зрозуміти, які специфічні виклики існують у сфері інтернет-провайдингу та які кращі практики можуть бути впроваджені для ефективного управління кібербезпекою. Знання про ці загрози та способи їхнього нейтралізування є важливим для забезпечення надійності та безпеки мережевих сервісів, а також для захисту конфіденційності та цілісності даних користувачів.

Таблиця 2.1.

Основні типи кіберзагроз

Тип загрози	**Опис**	**Стратегії реагування**
DDoS	Перевантаження мережі великою кількістю запитів для зупинки сервісу	Мережеве обладнання, здатне витримувати високе навантаження, IDS/IPS
Фішинг	Видобуток конфіденційних даних через обманні повідомлення або веб-сайти	Навчання співробітників, антифішингові технології
Malware	Зловмисне програмне забезпечення, яке заражає системи для крадіжки даних або завдання шкоди	Антивірусне програмне забезпечення, регулярні оновлення системи

Продовження таблиці 2.1

Ransomware	Зловмисне програмне забезпечення, яке блокує доступ до системи до виплати викупу	Бекапи даних, використання захищених систем зберігання
Man-in-the-Middle	Перехоплення і зміна даних, переданих між двома сторонами	Шифрування даних, безпечні протоколи передачі даних

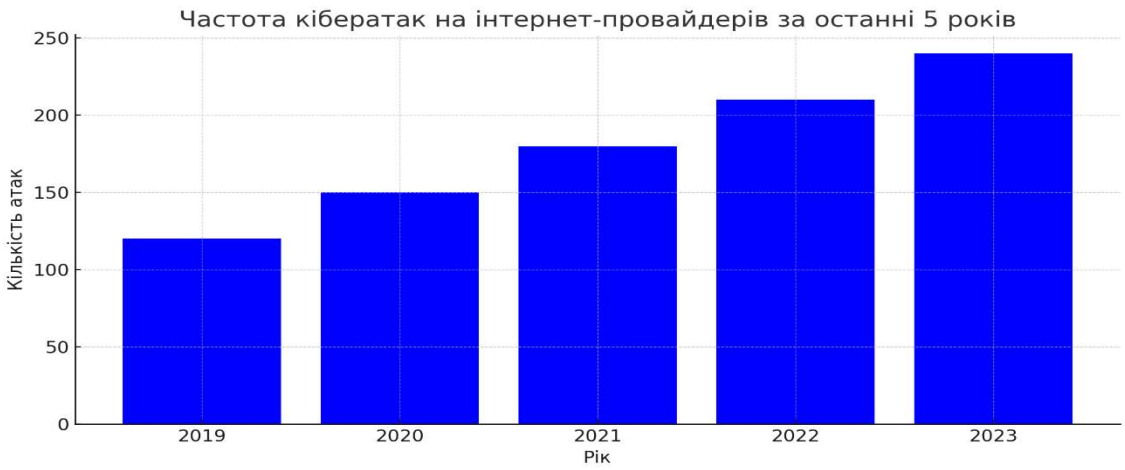


Рис. 2.1 – Частота кібератак на інтернет-провайдерів

На рисунку 2.1 представлено частоту кібератак на інтернет-провайдерів за останні 5 років. Як видно, кількість атак щороку зростає, що підкреслює зростаючу тенденцію кіберзагроз в цій галузі.

Соціальна інженерія та фішинг є іншими значними загрозами. Зловмисники можуть використовувати інженерні та психологічні прийоми, щоб обдурити співробітників інтернет-провайдера, спонукаючи їх викрити конфіденційну інформацію або надати доступ до захищених систем.

Розвиток захисних стратегій

Для протидії цим загрозам інтернет-провайдери мають розробити та впровадити комплексні стратегії безпеки, що включають регулярні аудити безпеки, використання розширених систем виявлення та запобігання вторгненням, а також забезпечення шифрування даних[10].

1. **Розвиток безпекової інфраструктури**, включаючи оновлення обладнання та програмного забезпечення, є критично важливим для захисту від відомих вразливостей. Водночас, навчання персоналу щодо ризиків і методів протидії кіберзагрозам є не менш важливим, оскільки людський фактор часто залишається найслабшою ланкою у ланцюгу безпеки.
2. **Впровадження політик безпеки**, що регулюють використання інформаційних ресурсів і встановлюють процедури відповіді на інциденти, стає основою для створення надійної системи захисту. Інтеграція цих політик із загальними бізнес-процесами та їх дотримання дозволяє не тільки мінімізувати потенційні ризики, але й швидко реагувати на безпекові інциденти, забезпечуючи стійкість бізнесу в умовах постійно змінюваних загроз.

Інтернет-провайдери виступають ключовими медіаторами у забезпеченні доступу до інтернету, тому їхні мережеві системи часто стають мішенями для різноманітних кібератак. Значними загрозами є DDoS атаки, що паралізують роботу систем, атаки на інфраструктуру через вразливості в мережевому обладнанні, експлуатація нульових днів та соціальна інженерія. Внаслідок цих загроз, інтернет-провайдери мають приділяти особливу увагу розробці і впровадженню комплексних стратегій безпеки, що включають технічні рішення та організаційні заходи, такі як регулярні аудити, розширене моніторинг, навчання персоналу, і розробка детальних політик відповіді на інциденти. Такий підхід дозволяє не тільки мінімізувати наслідки потенційних атак, але й забезпечити більшу стійкість мережевих систем до майбутніх загроз.

2.2 Специфіка хмарних сервісів у контексті інтернет-провайдингу

Хмарні технології набули значного поширення у сфері інтернет-провайдингу завдяки своїй ефективності, масштабованості та зручності у використанні. Однак, інтеграція хмарних сервісів вносить певні виклики та специфічні ризики у сферу мережевої безпеки, які вимагають особливого підходу з боку інтернет-провайдерів.

Загальний вплив хмарних технологій на інтернет-провайдинг

Хмарні сервіси пропонують інтернет-провайдерам можливість оптимізації ресурсів, зменшення витрат на обладнання та підтримку інфраструктури, а також підвищення гнучкості в управлінні даними і мережевими ресурсами. Ці переваги зробили хмарні сервіси привабливими для великих та малих провайдерів. Також хмарні сервіси сприяють інноваціям, дозволяючи швидко розгортати нові послуги та впроваджувати передові технологічні рішення[11].

Виклики безпеки хмарних сервісів

1. Контроль доступу та управління ідентичністю: управління доступом в хмарних сервісах є критично важливим, оскільки помилки у конфігурації можуть відкрити шлях до витоку даних. Провайдери мають забезпечити належні політики безпеки та строге дотримання процедур авторизації та аутентифікації.
2. Захист даних: хмарні сервіси вимагають комплексного підходу до шифрування даних, як на етапі передачі, так і при зберіганні. Необхідно впроваджувати сучасні технології шифрування та регулярно оновлювати ключі шифрування.
3. Розділення відповідальності: провайдери повинні чітко розуміти, що хмарні провайдери забезпечують захист інфраструктури, але відповідальність за захист самих даних лежить вже безпосередньо на користувачі. Це вимагає ретельного планування та ведення документації з боку інтернет-провайдерів.

4. Відповідність нормативам: провайдери повинні дотримуватися нормативних вимог у сфері зберігання та обробки даних, що може включати використання хмарних сервісів, розташованих у певних юрисдикціях або з певним рівнем сертифікації безпеки.

Стратегії мінімізації ризиків

Інтернет-провайдери мають розробити стратегії для мінімізації ризиків, пов'язаних з використанням хмарних технологій. Це включає регулярне проведення оцінок ризиків, впровадження багаторівневої системи безпеки та здійснення постійного моніторингу мережевих ресурсів. Також критично важливою є розробка плану реагування на інциденти, який дозволить швидко виявляти та нейтралізувати загрози.

Освіта та тренінги

Освіта та тренінги персоналу є необхідними для забезпечення високого рівня безпеки в хмарних сервісах. Персонал повинен бути обізнаний з основними принципами кібербезпеки, знати про потенційні загрози та вміти застосовувати на практиці політики безпеки компанії.

Хмарні технології внесли істотні зміни у сферу інтернет-провайдингу, пропонуючи оптимізацію ресурсів, зниження оперативних витрат та підвищення гнучкості управління даними. Однак, їхня інтеграція також створює нові виклики у забезпеченні безпеки, які потребують ретельного управління та стратегічного підходу з боку провайдерів. Проблеми контролю доступу, захисту даних, розділення відповідальності, та дотримання нормативних вимог є ключовими аспектами, які потребують невідкладного вирішення для запобігання витокам даних та іншим безпековим інцидентам. Відповідальне впровадження хмарних рішень, супроводжене суворими політиками безпеки, регулярними оцінками ризиків, та постійним моніторингом, може значно зменшити потенційні ризики та забезпечити ефективне використання хмарних технологій в інтернет-провайдингу.

Враховуючи вищевказане, важливо розуміти, що хмарні технології можуть значно покращити ефективність інтернет-провайдингу, але вони також вимагають від провайдерів підвищеного фокусу на аспекти безпеки. Кожен аспект

впровадження хмарних технологій має бути ретельно проаналізований з метою ідентифікації та зниження можливих ризиків.

2.3 Випадки порушення даних і їх наслідки для провайдерів та користувачів

Випадки порушення даних в інтернет-провайдингу можуть мати далекосяжні наслідки, починаючи від втрати довіри клієнтів до серйозних фінансових втрат та юридичних наслідків для провайдерів. Важливість захисту даних у цій індустрії зумовлена величезною кількістю чутливої інформації, яку провайдери зберігають та передають.

Причини порушень даних

Порушення даних можуть бути викликані різними факторами, включаючи зловмисні атаки, помилки співробітників, технічні несправності, а також недоліки в політиках безпеки. Зловмисні атаки часто здійснюються через фішинг, віруси, троянські програми або через вразливості в застосуваннях та системах. Помилки співробітників можуть включати несанкціонований доступ до даних, неправильне керування доступом або ненавмисне витоку інформації[12].

Типи порушень даних

- Витоки даних: несанкціонований доступ до даних, що може включати особисті дані, фінансову інформацію, корпоративну таємницю. Витоки можуть відбуватися через вразливості в програмному забезпеченні, несанкціонований доступ або недбале зберігання даних.
- Втрати даних: це може статися через випадкове видалення, пошкодження даних або збої в системі зберігання. Втрата даних може призвести до серйозних наслідків, особливо якщо це стосується критично важливих бізнес-інформацій.
- Модифікація даних: несанкціоноване змінення даних може мати серйозні наслідки, зокрема фальсифікацію фінансових записів або інших важливих документів.

Наслідки порушень даних

1. Фінансові збитки: витрати на розслідування порушення, відновлення даних, юридичні витрати та штрафи можуть суттєво вплинути на фінансове становище компанії.
2. Втрата довіри клієнтів: порушення даних може суттєво підірвати довіру користувачів, що може привести до втрати клієнтів і доходу.
3. Репутаційні втрати: втрата даних може пошкодити репутацію компанії, що може мати довготривалі наслідки для бізнесу.
4. Юридичні наслідки: порушення можуть привести до судових позовів, штрафів та інших юридичних наслідків, особливо якщо були порушені закони про захист даних.

Заходи щодо запобігання порушень

З метою запобігання порушенням даних, інтернет-провайдерам необхідно впроваджувати ряд заходів:

1. Посилення політик безпеки

Створення чітких політик безпеки, що регулюють доступ до даних та їх зберігання.

2. Регулярні аудити та моніторинг

Проведення регулярних аудитів та моніторингу системи на предмет вразливостей і несанкціонованих дій.

3. Навчання персоналу

Освіта та тренінги для співробітників щодо методів захисту даних та розуміння потенційних загроз.

4. Технологічні інвестиції

Інвестування в сучасні технології захисту даних, включно з шифруванням, брандмауерами та системами виявлення інцидентів.

Порушення даних в інтернет-провайдингу може мати катастрофічні наслідки, що включають фінансові втрати, втрату довіри з боку клієнтів, серйозні репутаційні пошкодження та юридичні наслідки. Важливість належного +інтернет-провайдери управляють великим обсягом чутливої інформації.

Порушення можуть статися через різні причини, включно з зловмисними атаками, технічними неполадками, помилками співробітників чи недоліками в політиках безпеки. Ефективне реагування на такі інциденти, ретельне планування безпеки та регулярне навчання персоналу є ключовими для забезпечення захисту інфраструктури та даних клієнтів. Враховуючи серйозність можливих наслідків порушення даних, для інтернет-провайдерів важливо не лише визнавати ризики, але й активно діяти для їхнього мінімізування, застосовуючи всеохоплюючий підхід до кібербезпеки[12].

3. ХМАРНІ СХОВИЩА ТА СТРАТЕГІЇ РЕЗЕРВУВАННЯ

3.1 Технології хмарного зберігання даних.

Хмарне зберігання даних сьогодні є фундаментальною частиною інфраструктури сучасних інформаційних технологій. Воно надає можливість користувачам та організаціям зберігати дані в інтернеті, що забезпечує легкий доступ, високу доступність та масштабованість. Оскільки ці технології постійно розвиваються, важливо зрозуміти не тільки їх технічні аспекти, але й історію розвитку, яка підкреслює їхню еволюцію і значення.

Основним завданням цієї курсової роботи є дослідження технологій хмарного зберігання даних, вивчення їх архітектурних та технічних аспектів та аналіз питань безпеки, які є критичними для захисту збереженої інформації.

Нижче наведено таблицю, яка ілюструє основні етапи розвитку хмарних технологій зберігання:

Таблиця 3.1

Ілюстрація основних етапів розвитку хмарних технологій зберігання[13]

	Подія	**Вплив на розвиток технологій**
1960-ті	Початок концепції розділеного обчислення	Введення ідеї обчислювальних "хмар"
1999	Salesforce.com запускає один із перших хмарних сервісів	Старт комерціалізації хмарних послуг
2006	Amazon запускає AWS	Великий крок у наданні хмарних інфраструктурних послуг
2009	Google та Microsoft запускають хмарні платформи	Поширення хмарних сервісів серед широкого кола користувачів
Сучасність	Широкий розвиток штучного інтелекту та машинного навчання в хмарах	Перетворення хмарних сервісів на ще більш інтелектуалізовані та інтегровані системи

Таблиця 3.1 демонструє ключові моменти у розвитку технології, які сприяли зростанню і популяризації хмарних сервісів. У наступних розділах ми детальніше розглянемо кожен з цих аспектів.

Для другого розділу курсової роботи, "Основні поняття та технології", ми розглянемо визначення хмарного зберігання, історію його розвитку, та класифікацію хмарних сервісів. Для наглядності, включимо таблицю, що перелічує основних провайдерів хмарних сервісів за категоріями IaaS, PaaS, SaaS, а також діаграму, яка покаже розподіл ринку між цими провайдерами.

Хмарне зберігання — це модель зберігання даних, яка дозволяє інформації зберігатися на віддалених серверах, до яких можна отримати доступ через інтернет. Це забезпечує зручність, масштабованість та оптимізацію витрат, а також відсутність необхідності в обслуговуванні власних локальних серверів[14].

Історія хмарного зберігання бере свій початок з 1960-х років з концепції часоподільних систем, яка еволюціонувала до сучасних масштабних хмарних платформ. Розвиток інтернет-технологій та швидкісних мереж значно сприяли поширенню хмарних технологій, а відкриття сервісу Amazon Web Services у 2006 році позначило нову еру в індустрії IT.

Хмарні сервіси можна класифікувати на три основні категорії:

- IaaS (Infrastructure as a Service): Забезпечує користувачам віртуальні ресурси, такі як віртуальні машини та сховища.

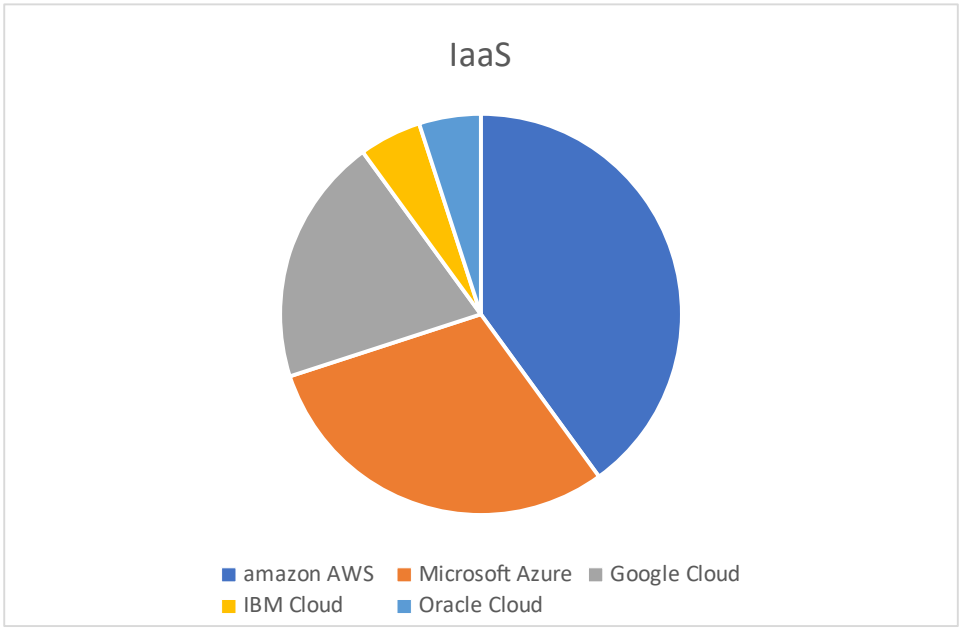
- PaaS (Platform as a Service): Надає користувачам платформи для розробки, тестування та розгортання програмного забезпечення.

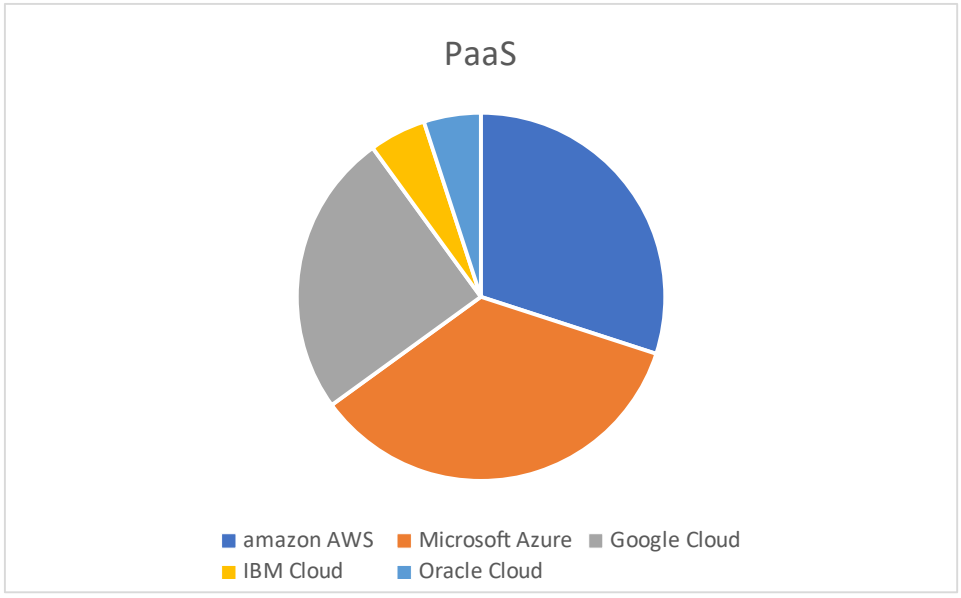
- SaaS (Software as a Service): Надає користувачам доступ до програмного забезпечення та його функцій через інтернет.

Таблиця 3.2

Перелік основних провайдерів для кожного типу сервісу

Тип сервісу	**Провайдери**
IaaS	Amazon AWS, Microsoft Azure, Google Cloud
PaaS	Heroku, Google App Engine, Microsoft Azure
SaaS	Google Workspace, Microsoft 365, Salesforce





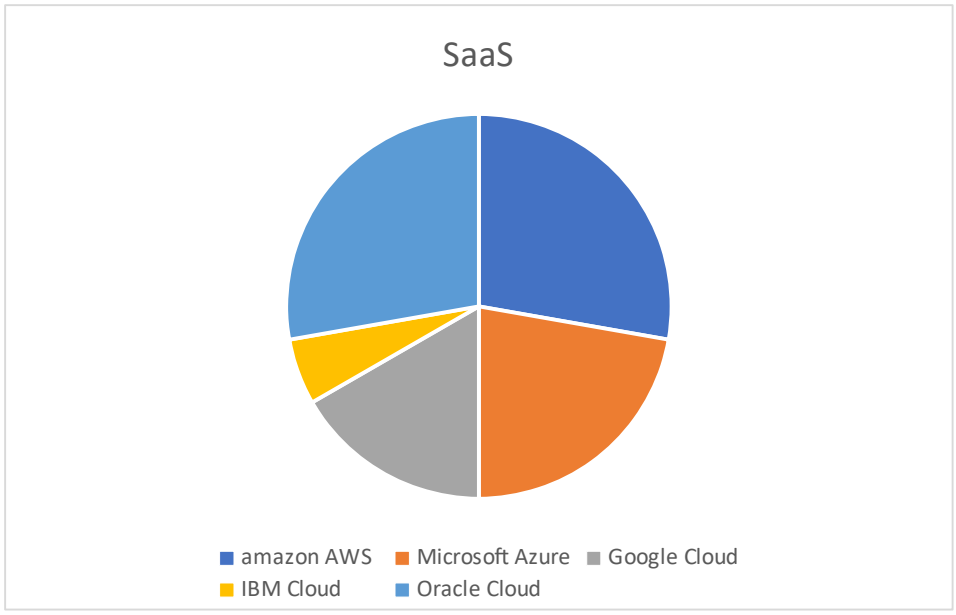


Рис. 3.1 - Перелік основних провайдерів для кожного типу сервісу

Рисунок 3.1 показує, як ринок хмарних сервісів розділений між різними провайдерами, де кожен тип сервісу демонструє особливості конкурентного розподілу.

Хмарне зберігання засноване на архітектурі, яка дозволяє ефективно масштабувати ресурси та надавати високу доступність і надійність. Основні компоненти включають віртуальні сервери, сховища даних, мережеві елементи та інтерфейси управління. Ці компоненти спільно працюють для забезпечення безперервного доступу до даних і ресурсів через інтернет.

Основні компоненти системи хмарного зберігання включають[15]:

— Віртуальні машини: Забезпечують виконання програм і обробку даних.

— Сховища даних: Відповідають за зберігання великих обсягів інформації.

— Мережеві компоненти: Забезпечують зв'язок між ресурсами в хмарі та користувачами.

— Управління ресурсами: Інструменти та сервіси для контролю та розподілу ресурсів.

Технічні аспекти включають різноманітність серверних платформ, мережевих протоколів та стандартів безпеки. Ці аспекти визначають ефективність, безпеку та масштабованість хмарних рішень.

Таблиця 3.2

Ключові технічні аспекти компонентів

Компонент	**Технічні характеристики**	**Важливість**
Віртуальні машини	Тип ОС, кількість ядер	Висока
Сховища даних	Типи дисків, пропускна здатність	Висока
Мережеві компоненти	Протоколи, швидкість передачі даних	Висока
Управління ресурсами	Автоматизація, моніторинг	Висока

Таблиця 3.3

Структурна схема типової архітектури хмарного зберігання

Компонент	Опис	Функції
Клієнтські пристрої	Точки доступу користувачів (комп'ютери, мобільні телефони, інші пристрої)	Забезпечення доступу до хмарних ресурсів, інтерфейс користувача
Веб-сервери	Сервери, що обробляють запити від клієнтів та управляють веб-інтерфейсами	Обробка запитів до хмарних сервісів, відправлення та отримання даних
Прикладні сервери	Сервери, які запускають специфічні додатки або сервіси хмарної платформи	Виконання програмного забезпечення, яке потребує великих обчислювальних потужностей
Сервери баз даних	Спеціалізовані сервери для зберігання та управління даними	Зберігання великих обсягів даних, забезпечення високої швидкості читання та запису
Сховища даних	Системи зберігання, що використовуються для архівації, резервного копіювання та відновлення даних	Зберігання даних з високою доступністю та надійністю, оптимізація використання дискового простору
Мережева інфраструктура	Маршрутизатори, комутатори, балансувальники навантаження	Забезпечення зв'язності та оптимального розподілу трафіку між серверами та пристроями
Управління та моніторинг	Системи для контролю стану хмарної інфраструктури та управління ресурсами	Моніторинг стану системи, автоматичне масштабування ресурсів, забезпечення безпеки

Таблиця 3.3 ілюструє основні компоненти хмарної системи зберігання та їхній взаємозв'язок, підкреслюючи, як дані пересуваються між користувачем та сховищем.

Хмарне зберігання, хоч і забезпечує значні переваги в плані доступності та масштабованості, також вносить унікальні виклики для безпеки даних. Основні загрози включають несанкціонований доступ, втрату даних, зламування акаунтів та інтерфейсів, а також загрози від внутрішніх користувачів.

Для захисту даних у хмарі використовуються різні технічні та адміністративні методи. Серед них:

— Шифрування даних: Використання сучасних алгоритмів шифрування для захисту даних на віддалених серверах та під час їх передачі.

— Множинна аутентифікація: Застосування багатофакторної аутентифікації для забезпечення додаткових рівнів перевірки користувачів.

— Розмежування доступу: Строге контролювання доступу до даних на основі ролей та відповідальностей користувачів.

Хмарні провайдери і користувачі мають дотримуватися встановлених політик і стандартів безпеки, які гарантують захист даних та відповідність регуляторним вимогам. Це включає стандарти, такі як ISO 27001, SOC 2, та GDPR.

Таблиця 3.4

Перелік основних стандартів безпеки для хмарних сервісів

Стандарт	**Опис**
ISO 27001	Міжнародний стандарт з управління інформаційною безпекою, що забезпечує комплексний підхід.
SOC 2	Стандарт, що вимагає управління даними на основі п'яти "трастових принципів": безпека, доступність, обробка, конфіденційність та конфіденційність.
GDPR	Загальний регламент захисту даних у Європейському Союзі, регулює обробку та передачу персональних даних.
HIPAA	Стандарт у США для захисту медичної інформації та забезпечення конфіденційності пацієнтів.

Хмарне зберігання пропонує значні економічні переваги порівняно з традиційними методами зберігання даних. Найважливішими з них є[1]:

- Скорочення капітальних витрат: замість великих витрат на придбання та обслуговування власного серверного обладнання, компанії можуть використовувати ресурси на основі плати за використання, що знижує первісні витрати.

- Економія на управлінні та обслуговуванні: хмарні провайдери беруть на себе всі зобов’язання щодо технічного обслуговування, забезпечуючи оновлення та управління обладнанням.

Технічні аспекти хмарного зберігання також пропонують важливі переваги:

- Масштабованість: хмарні рішення можуть швидко масштабуватися, щоб задовольнити змінювані потреби в обсягах даних.

- Доступність: дані можна легко доступати з будь-якої точки світу, де є доступ до інтернету, що забезпечує високу гнучкість в роботі.

Незважаючи на значні переваги, існують також недоліки та ризики:

- Залежність від інтернет-з'єднання: доступ до даних можливий тільки при наявності інтернету, що може бути проблемою в областях з поганим зв'язком.

- Проблеми з конфіденційністю та безпекою: зберігання даних на зовнішніх серверах вносить ризики щодо конфіденційності та може привести до витоків інформації.

Для шостого розділу курсової роботи, який розглядає майбутнє хмарних технологій, я висвітлю ключові тенденції та інновації, які можуть формувати розвиток хмарного зберігання. Це дозволить оцінити, як хмарні технології можуть змінити IT-ландшафт у майбутньому.

Хмарне зберігання невпинно розвивається, адаптуючись до зростаючих вимог ринку та технологічних інновацій. Наступні тенденції є особливо важливими для майбутнього розвитку цієї галузі:

- Гібридні хмарні рішення: комбінація локальних і хмарних ресурсів стає все популярнішою, оскільки організації шукають баланс між контролем та гнучкістю.

- Контейнеризація та мікросервіси: використання контейнерів, таких як Docker та Kubernetes, дозволяє ефективніше управляти розгортанням і масштабуванням додатків у хмарі.

- Штучний інтелект та машинне навчання: інтеграція ШІ та машинного навчання в хмарні платформи забезпечує автоматизацію та підвищення інтелектуального аналізу даних.

Штучний інтелект (ШІ) та машинне навчання (МН) стають критично важливими компонентами хмарних сервісів. Вони допомагають у таких аспектах:

- Автоматизація обслуговування: ШІ може автоматизувати багато аспектів управління хмарною інфраструктурою, включаючи виявлення та виправлення помилок.

- Оптимізація ресурсів: МН алгоритми можуть прогнозувати потреби в ресурсах, оптимізуючи їх використання та знижуючи витрати.

Розвиток хмарних технологій сприяє значним змінам у способах зберігання, обробки та аналізу даних. В майбутньому можна очікувати ще більшої інтеграції хмарних сервісів у всі аспекти ділової діяльності, що забезпечить нові можливості для інновацій та ефективності.

Для завершального розділу курсової роботи, я підготую висновки, які підсумують основні знахідки роботи, важливість дослідження для розвитку технологій хмарного зберігання та перспективи майбутнього розвитку. Це допоможе оформити заключну частину, підкресливши основні аспекти дослідження[8].

3.2 Політики і методи резервного копіювання даних.

У сучасному світі, де дані є одним з найцінніших активів для будь-якої організації, належне резервне копіювання даних стає не просто додатковою можливістю, а необхідністю. Резервне копіювання даних захищає інформацію від випадкової втрати, пошкодження внаслідок технічних неполадок, а також зловмисних атак і природних катастроф. Завдяки ефективній стратегії резервного копіювання компанії можуть швидко відновлювати свою роботу після аварій, мінімізуючи час простою та фінансові втрати.

Цей розділ курсової роботи має на меті дослідити різні політики і методи резервного копіювання, які можуть бути застосовані в організаціях для забезпечення цілісності та доступності даних. Ми розглянемо основні типи резервного копіювання, такі як повне, інкрементальне, та диференційне копіювання, а також оцінимо переваги та недоліки кожного з методів. Включення таблиць і Рисуноків допоможе візуалізувати порівняльний аналіз цих методів і

підкреслити найбільш релевантні технології та інструменти в сфері резервного копіювання[9].

Таблиця 3.5

Основні характеристики методів резервного копіювання

Метод копіювання	**Частота виконання**	**Обсяг даних**	**Вплив на системні ресурси**	**Час відновлення**
Повне копіювання	Низька (щотижня)	Великий (всі дані)	Високий	Швидке
Інкрементальне копіювання	Висока (щодня)	Невеликий (тільки зміни)	Середній	Помірне
Диференційне копіювання	Середня (кожні 2-3 дні)	Середній (зміни від останнього повного копіювання)	Середній	Помірне

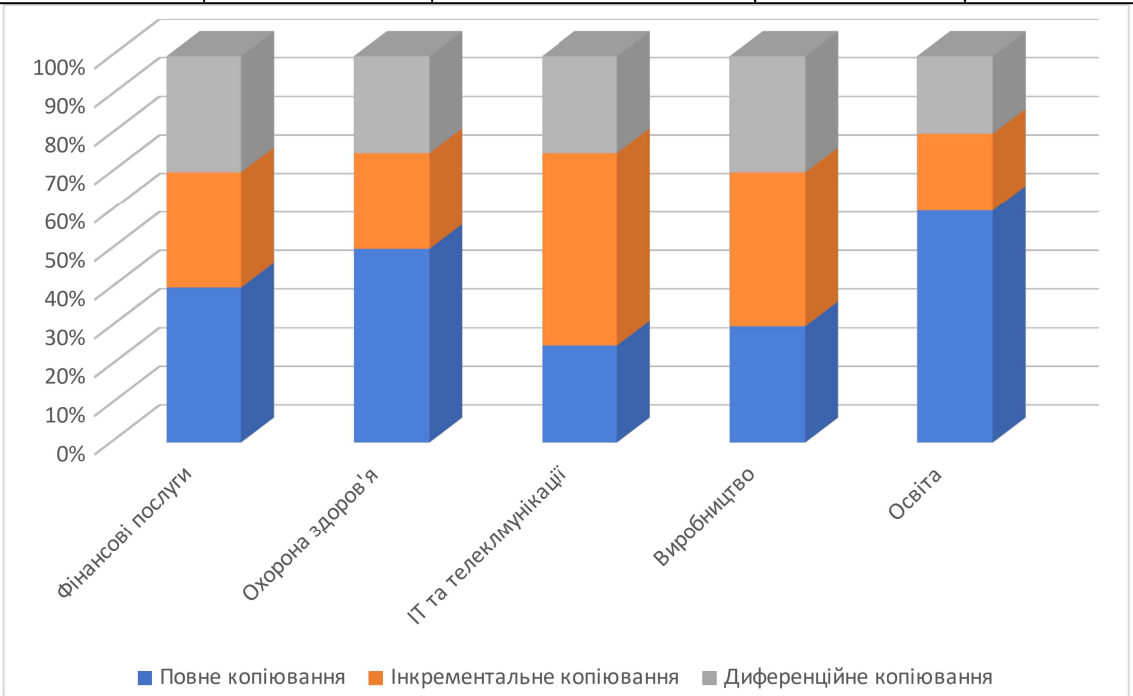


Рис. 3.2 – Процентне співвідношення використання методів резервного копіювання

Політика резервного копіювання — це набір правил та процедур, розроблених для управління процесом резервного копіювання даних в організації. Ці політики забезпечують, що всі критичні дані регулярно копіюються таким чином, що вони можуть бути відновлені у випадку їх втрати чи пошкодження. Основними цілями таких політик є мінімізація ризиків втрати даних, забезпечення

їх доступності у будь-який час та впорядкування процесу відновлення після аварій.

Локальне резервне копіювання включає зберігання копій даних на фізичних носіях, що знаходяться в тому самому фізичному місці, де вони використовуються. Цей метод часто використовується для швидкого доступу та відновлення даних, але він має недоліки у вигляді високого ризику втрати даних через місцеві події, такі як пожежі чи повені[13].

- Переваги: Швидкість доступу та відновлення.

- Недоліки: Обмежена захищеність від місцевих ризиків.

Віддалене резервне копіювання передбачає зберігання даних на фізичних носіях або в серверних центрах, які знаходяться за межами основного місця використання даних. Цей підхід дозволяє захистити дані від місцевих катастроф і забезпечує вищий рівень безпеки.

- Переваги: Захист від місцевих катастроф, підвищена безпека.

- Недоліки: Можливі затримки при відновленні даних через відстань.

Хмарне резервне копіювання використовує хмарні сервіси для зберігання даних. Цей метод стає все більш популярним завдяки своїй гнучкості, масштабованості та економічності.

- Переваги: Гнучкість, доступність з будь-якого місця, низькі початкові витрати.

- Недоліки: Залежність від інтернет-з'єднання, питання конфіденційності та безпеки даних.

Повне резервне копіювання включає створення одноразової копії всіх даних, що зберігаються на сервері або в іншому місці зберігання. Цей метод є найбільш надійним з точки зору відновлення даних, оскільки кожне повторне копіювання забезпечує вам останню повну версію всіх файлів.

- Переваги: Повністю відновлює всі дані з однієї копії.

- Недоліки: Високі витрати на зберігання, тривалий час копіювання.

Інкрементальне копіювання зберігає лише ті дані, які змінились після останнього будь-якого копіювання (повного або інкрементального). Це значно

скорочує час копіювання та місце для зберігання, але відновлення даних може займати більше часу, оскільки потрібно об'єднати кілька копій.

- Переваги: Менше займає місця для зберігання, швидше виконується.

- Недоліки: Відновлення вимагає більше часу та всіх попередніх копій.

Диференційне копіювання зберігає дані, що змінилися від часу останнього повного копіювання. Цей метод швидший за повне копіювання, але вимагає більше місця для зберігання, ніж інкрементальне, оскільки кількість даних, що копіюються, збільшується з кожним разом до наступного повного копіювання.

- Переваги: Швидше відновлення ніж інкрементальне копіювання.

- Недоліки: Вимагає більше місця для зберігання, ніж інкрементальне копіювання.

Синтетичне резервне копіювання є комбінацією повного та інкрементального копіювання. Перше повне копіювання створює основу, а потім інкрементальні копії об'єднуються з нею, формуючи нову "повну" копію. Це знижує необхідність частих повних копіювань та скорочує час відновлення.

- Переваги: Зменшує частоту повного копіювання, прискорює відновлення.

- Недоліки: Складність у реалізації та вимога до програмного забезпечення.

Здзеркалення даних включає постійну синхронізацію копій даних між двома або більше місцями зберігання. Це забезпечує високий рівень доступності даних і дозволяє майже миттєво відновити дані у випадку втрати або пошкодження.

- Переваги: Висока доступність даних, швидке відновлення.

- Недоліки: Високі витрати та потреба у великій пропускній здатності мережі.

Вибір правильних технологій та інструментів для резервного копіювання є критичним для ефективної імплементації політик резервного копіювання. На ринку існує широкий спектр рішень, які варіюються за функціональністю, ціною та складністю. Далі ми розглянемо декілька популярних інструментів, які допомагають автоматизувати процес резервного копіювання та забезпечують надійність збереження даних.

Acronis True Image — це комплексне рішення, яке пропонує як локальне, так і хмарне резервне копіювання. Воно включає можливості повного, інкрементального та диференційного копіювання. Також, інструмент забезпечує потужні опції для кіберзахисту, включаючи захист від рансомваре.

Veeam є лідером у сфері резервного копіювання для віртуалізованих та хмарних середовищ. Це рішення забезпечує швидке відновлення даних та має високу масштабованість, що робить його ідеальним для великих підприємств.

Veritas Backup Exec підтримує широкий спектр платформ і пропонує розширені функції для забезпечення відновлення після аварій. Це рішення відоме своїми потужними можливостями управління та високим рівнем інтеграції з існуючими інфраструктурами.

Google Cloud Backup пропонує просте у використанні, але ефективне хмарне резервне копіювання. Цей сервіс ідеально підходить для компаній, що вже використовують хмарні рішення Google та шукають інтегроване рішення для захисту своїх даних.

Для кращого розуміння відмінностей між цими інструментами, нижче представлено порівняльну таблицю, яка включає основні характеристики кожного рішення.

Таблиця 3.6

Порівняльні характеристики інструментів резервного копіювання

Інструмент	**Тип копіювання**	**Підтримка платформ**	**Особливості безпеки**	**Цільова аудиторія**
Acronis True Image	Повне, інкрементальне, диференційне	Всі основні	Захист від рансомваре	СМБ, домашні користувачі
Veeam Backup & Replication	Повне, інкрементальне	Віртуалізація, хмара	Висока масштабованість	Середні та великі підприємства
Veritas Backup Exec	Повне, інкрементальне, диференційне	Всі основні	Потужні опції управління	Середні та великі підприємства
Google Cloud Backup	Повне, інкрементальне	Хмара	Інтеграція з хмарними сервісами	СМБ, хмарні підприємства

Таблиця 3.6 допомагає виявити які інструменти найкраще підходять для різних типів підприємств та їх специфічних потреб у резервному копіюванні[2].

Вибір правильного інструмента для резервного копіювання залежить від багатьох факторів, включаючи розмір організації, типи даних, що зберігаються, і вимоги до швидкості відновлення. Розуміння властивостей та функціональності різних інструментів є ключем до вибору найбільш підходящої системи резервного копіювання для вашої організації.

Розробка ефективної політики резервного копіювання даних вимагає грунтовного підходу, який забезпечить комплексну захисту інформації в організації. Процес можна розділити на наступні ключові етапи:

1. Аналіз потреб і визначення критично важливих даних: Ідентифікація даних, які потребують резервного копіювання, на основі їх значущості для бізнес-процесів.

2. Вибір методу резервного копіювання: Рішення про використання повного, інкрементального, диференційного копіювання чи їх комбінацій.

3. Вибір технологій та інструментів: Селекція відповідного програмного забезпечення та обладнання для резервного копіювання.

4. Розробка процедур відновлення даних: Встановлення чітких кроків для відновлення даних у разі їх втрати.

5. Тестування та оцінка політики: Регулярне тестування процедур відновлення для перевірки їх ефективності та внесення необхідних коректив.

Після розробки політики резервного копіювання, важливо ефективно впровадити її в діяльність організації:

1. Навчання персоналу: Забезпечення, щоб усі відповідальні співробітники були належно проінструктовані щодо процедур резервного копіювання.

2. Автоматизація процесів: Максимальне використання автоматизації для зниження ризику людської помилки.

3. Регулярний моніторинг та аудит: Постійний нагляд за процесом резервного копіювання для виявлення та усунення можливих проблем.

Розробка та впровадження політики резервного копіювання може зіткнутися з рядом викликів, включаючи:

- Технічні обмеження: Оснащення та підтримка інфраструктури для резервного копіювання може вимагати значних інвестицій.

- Спротив змінам: Співробітники можуть сприймати нові процедури як додаткове навантаження.

- Дотримання законодавчих норм: Забезпечення відповідності політики вимогам законодавства щодо захисту даних.

Для подолання цих викликів рекомендується:

1. Інвестувати в надійну технічну підтримку: Забезпечення технічного обслуговування та оновлення інфраструктури.

2. Прозорість процесів: Забезпечення відкритого діалогу зі співробітниками для з'ясування переваг резервного копіювання.

3. Дотримання нормативних вимог: Регулярне оновлення політик з урахуванням змін у законодавстві.

Резервне копіювання даних є критично важливим аспектом управління інформаційними системами будь-якої організації. Правильно розроблені та впроваджені політики і методи резервного копіювання можуть значно знизити ризики пов'язані з втратою даних, що, в свою чергу, забезпечує безперервність бізнес-процесів та захист від фінансових втрат.

Ми розглянули основні типи резервного копіювання, такі як повне, інкрементальне, диференційне, синтетичне копіювання та здзеркалення даних, кожен з яких має свої переваги та недоліки і може бути використаний в залежності від конкретних потреб організації. Також було висвітлено різні інструменти, що надають ці послуги, та з'ясовано, які з них найбільше підходять для різних типів бізнесу.

1. Дослідження інноваційних технологій: Технологічний прогрес не зупиняється, і нові інноваційні рішення для резервного копіювання даних з'являються регулярно. Рекомендується відстежувати ці нововведення, щоб використовувати найефективніші та безпечні рішення.

2. Аналіз впливу хмарних технологій: Хмарні рішення продовжують набирати популярність, і аналіз їх впливу на політики резервного копіювання допоможе організаціям зрозуміти, як найкраще використовувати хмарні сервіси для забезпечення безпеки даних.

3. Зосередження на відновленні після катастроф: Важливо не тільки зосереджуватись на резервному копіюванні, але й на стратегіях відновлення даних після можливих катастроф. Дослідження в цій області можуть допомогти підвищити стійкість організацій до непередбачених подій.

3.3 Надійність і доступність даних у хмарних сховищах.

Хмарне сховище — це модель зберігання даних, в якій цифрові дані зберігаються в логічних пулах, які керуються третьою стороною (хмарними провайдерами), забезпечуючи доступ до даних через інтернет. Надійність у контексті хмарних сховищ визначається як здатність системи зберігати і забезпечувати неперервний доступ до даних при різних умовах експлуатації. Доступність відноситься до ступеня доступу до цих даних для користувачів у будь-який потрібний момент[15].

В епоху цифровізації, надійність і доступність даних у хмарних сховищах стають критично важливими для ефективного функціонування бізнесу та задоволення потреб користувачів. Хмарні сховища пропонують значні переваги, такі як масштабованість, зниження витрат та спрощення управління даними, але також вимагають гарантій щодо надійності і доступності цих даних. Без гарантій це може спричинити фінансові збитки, втрату репутації та юридичні проблеми.

Для бізнесу, що залежить від постійного доступу до своїх даних, збої у доступності або надійності можуть мати драматичні наслідки. Забезпечення високого рівня доступності та надійності — це не тільки про технічне обладнання, а й про вибір відповідних стратегій та практик, які здатні мінімізувати ризики і забезпечити безперебійне обслуговування клієнтів. Наступні розділи детально

розглянуть теоретичні основи, аналізують поточні технології та практики, що дозволяють досягти цих критичних для хмарних сервісів характеристик.

Хмарні сховища можуть бути реалізовані в різних архітектурних моделях, кожна з яких має свої особливості щодо надійності та доступності:

- Приватні хмари: Це ексклюзивні хмарні середовища, які повністю контролюються і управляються внутрішніми ресурсами компанії. Вони пропонують вищий рівень контролю та безпеки, але вимагають значних капіталовкладень у фізичну інфраструктуру та управління.

- Публічні хмари: Публічні хмарні платформи, такі як AWS, Google Cloud та Microsoft Azure, пропонують послуги зберігання даних на спільно використовуваних ресурсах. Вони забезпечують високу масштабованість і еластичність, але можуть представляти виклики у плані персоналізації безпеки.

- Гібридні хмари: Комбінація приватних та публічних хмар, що дозволяє компаніям максимально використовувати переваги обох типів. Гібридні моделі часто використовуються для балансування між контролем та масштабованістю, оптимізуючи доступність та надійність даних.

Надійність і доступність даних у хмарних сервісах тісно пов'язані з застосуванням стандартів та протоколів безпеки[3]:

- HTTPS та SSL/TLS: Ці протоколи забезпечують шифрування даних під час їх передачі, що є критично важливим для захисту даних від несанкціонованого доступу. SSL/TLS створює безпечний канал між користувачем та хмарним сервісом, навіть якщо дані передаються через небезпечні мережі.

- ISO/IEC 27001: Міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою. Він включає аспекти збереження конфіденційності, цілісності та доступності інформації.

- PCI DSS: Стандарт безпеки даних для всіх організацій, що обробляють платіжні картки. Важливий для хмарних сховищ, що зберігають фінансову інформацію, PCI DSS вимагає захисту даних через різні технічні та оперативні заходи.

Ці протоколи і стандарти служать основою для створення надійних та безпечних хмарних сховищ, забезпечуючи захист даних на кожному етапі їх обробки та зберігання. Наступний розділ розгляне аналіз надійності та доступності даних, де буде представлено детальний огляд поточних технологій та методів, використовуваних для забезпечення цих критично важливих характеристик хмарних сервісів.

Service Level Agreements (SLA) визначають стандартизовані рівні обслуговування, які хмарні провайдери зобов'язуються надавати своїм клієнтам. SLA включають гарантії щодо доступності сервісу, часу реагування на запити та інші ключові показники ефективності, які впливають на надійність хмарних сервісів.

- Параметри SLA: Типові параметри SLA включають процентний час доступності сервісів, зазвичай відомий як "uptime", і межі дозволених перерв у роботі сервісу, або "downtime".

- Вплив на бізнес: Неналежне виконання SLA може призвести до фінансових втрат для клієнтів, тому важливо розуміти, які компенсаційні заходи пропонуються у випадку невиконання цих умов.

Хмарні провайдери використовують кілька технічних методів для забезпечення надійності хмарних сервісів:

- Резервне копіювання даних: Періодичне копіювання даних на окремі сервери або в інші дата-центри забезпечує, що важлива інформація не буде втрачена у разі системних збоїв або фізичних пошкоджень.

- Реплікація даних: Створення копій даних у реальному часі і їхнє розміщення в різних локаціях знижує ризик даних через місцеві збої та забезпечує високий рівень доступності.

- Використання несучасних центрів обробки даних: Розташування дата-центрів в географічно різних регіонах дозволяє хмарним провайдерам забезпечувати послуги без перебоїв навіть у випадку значних катастроф.

Хмарні сервіси можуть зіткнутися з різними викликами, які впливають на надійність даних:

- Технічні збої: Поломки обладнання або програмне забезпечення можуть призвести до втрати даних. Регулярні технічні перевірки та оновлення програмного забезпечення є критично важливими для мінімізації цих ризиків.

- Кібератаки: Атаки типу ransomware або DDoS можуть порушити нормальне функціонування хмарних сервісів. Застосування передових методів кібербезпеки та шифрування даних допомагає уникнути таких проблем.

- Людський фактор: Помилки в налаштуваннях або управлінні доступом можуть також призвести до втрати даних. Освіта та тренінги для співробітників, а також детальні політики доступу можуть значно знизити такі ризики.

Доступність у хмарних сховищах вимагає використання спеціалізованих технологій і практик, що забезпечують неперервний доступ до даних, незалежно від технічних збоїв або фізичних катастроф:

- Load balancing (Балансування навантаження): Ця технологія розподіляє вхідний трафік між кількома серверами або центрами обробки даних, зменшуючи ризик перевантаження одного сервера і забезпечуючи високу продуктивність і доступність сервісів.

- Redundancy (Резервування): Створення резервних копій систем і даних у декількох місцях забезпечує, що навіть у разі повного виходу одного центру з ладу, сервіси продовжують функціонувати без перебоїв.

- Auto-scaling (Автоматичне масштабування): Автоматичне масштабування дозволяє хмарним системам автоматично збільшувати або зменшувати ресурси залежно від поточного навантаження, підтримуючи оптимальну продуктивність без зайвих витрат.

Розробка ефективних планів відновлення після аварій (Disaster Recovery Plan, DRP) є критично важливою для забезпечення доступності хмарних сервісів:

- Відновлення після аварій (Disaster Recovery): Хмарні провайдери створюють стратегії для швидкого відновлення сервісів після збоїв, включаючи технічні несправності, природні катастрофи або кібератаки.

- Geographic redundancy (Географічне резервування): Розміщення дата-центрів у різних географічних регіонах забезпечує, що місцеві події не впливають на загальну доступність даних.

- Testing (Тестування планів): Регулярне тестування DRP забезпечує, що вони залишаються актуальними і ефективними у реальних умовах.

Для забезпечення високої доступності даних, хмарні провайдери застосовують ряд технологій:

- Балансування навантаження: Розподіл трафіку між кількома серверами забезпечує, що жоден окремий сервер не перевантажується, що сприяє підвищенню загальної доступності та надійності системи.

- Автоматичне масштабування: Системи можуть автоматично збільшувати або зменшувати кількість ресурсів відповідно до поточного навантаження, забезпечуючи стабільну доступність ресурсів навіть при пікових навантаженнях.

- Георезервування: Дані дублюються у декількох географічних регіонах, що забезпечує їх доступність у випадку локальних збоїв або катастроф.

Підготовка до потенційних збоїв є ключовою складовою забезпечення доступності хмарних сервісів:

- Disaster Recovery Plan (DRP): Стратегічний план, який визначає, як організація відновить свою IT-інфраструктуру та послуги у найкоротші терміни після катастрофічного збою.

- High Availability (HA) архітектура: Дизайн системи, що мінімізує час простою за рахунок розподілу критично важливих компонентів на декілька незалежних вузлів, які можуть взаємозамінювати один одного у випадку збою.

Проаналізуємо реальні приклади впровадження технологій доступності:

1. AWS Multi-AZ Deployments:

- Опис: Amazon Web Services забезпечує високу доступність своїх сервісів за допомогою автоматичного розподілу запущених екземплярів та даних між кількома зонами доступності.

- Результат: Значне зниження ризику недоступності послуг через локальні збої, забезпечення безперервної роботи критично важливих застосунків.

2. Google Cloud Global Load Balancing:

- Опис: Google Cloud використовує глобальне балансування навантаження для оптимізації розподілу користувацького трафіку по своїх дата-центрах, розташованих по всьому світу.

- Результат: Висока продуктивність та доступність веб-застосунків незалежно від географічного розташування користувачів.

Цей дослідження надійності та доступності хмарних сховищ демонструє, що вибір хмарної архітектури та провайдера має критичне значення для забезпечення безпечного і надійного доступу до даних. Важливо вибрати рішення, яке не тільки задовольняє поточні потреби бізнесу, але й має гнучкість для адаптації до майбутніх викликів.

- Надійність: Застосування методів резервного копіювання, реплікації даних, і використання розподілених дата-центрів допомагає зменшити ризики втрати даних і забезпечує високий рівень надійності.

- Доступність: Балансування навантаження, автоматичне масштабування, і георезервування є ключовими технологіями, що забезпечують високу доступність сервісів навіть у разі локальних збоїв.

На основі проведеного аналізу, можна надати кілька рекомендацій для організацій, які планують імплементацію або оптимізацію своїх хмарних рішень:

1. Вибір провайдера: Оберіть хмарного провайдера з міцною репутацією у сфері надійності і доступності. Вивчення SLA, відгуків від інших користувачів та історії роботи може допомогти у виборі.

2. Регулярні аудити безпеки: Проводьте регулярні аудити вашої хмарної інфраструктури для виявлення та усунення потенційних слабких місць.

3. Планування на випадок збоїв: Розробка комплексного плану відновлення після аварій є важливим для забезпечення бізнес-стійкості. Переконайтеся, що ваші стратегії відновлення враховують всі можливі сценарії.

4. Освіта та тренінги для співробітників: Забезпечення співробітників знаннями і навичками для роботи з хмарними технологіями може значно покращити загальну безпеку та ефективність.

Хмарні сховища продовжують бути життєво важливим компонентом інформаційної інфраструктури сучасних організацій. Розуміння та впровадження найкращих практик у галузі надійності та доступності допоможе організаціям забезпечити безперебійний доступ до даних та послуг, тим самим підвищуючи їхню конкурентоспроможність та операційну ефективність на довгі роки.

3.4 Сучасні інструменти та програмні рішення для резервування і відновлення.

Резервування даних є критично важливим аспектом інформаційної безпеки у будь-якій організації. Вибір правильного методу та інструментів для резервування може значно вплинути на ефективність відновлення даних у випадку їх втрати або пошкодження. Розглянемо основні типи рішень, які застосовуються в сучасних практиках управління даними[11].

Традиційно, одним з найпоширеніших методів резервування даних було використання магнітних носіїв, таких як стрічки та жорсткі диски.

- Опис: Цей метод передбачає використання магнітних стрічок або зовнішніх жорстких дисків для зберігання копій даних. Магнітні стрічки часто використовуються для зберігання великих обсягів даних через їх високу місткість і низьку вартість.

- Переваги: Висока місткість зберігання при відносно низькій вартості. Магнітні стрічки здатні зберігати дані протягом довгих періодів.

- Недоліки: Доступ до даних може бути повільним, оскільки вимагається фізичний доступ до стрічки. Ці носії також більш вразливі до фізичних пошкоджень та зношування.

Дискове резервування стало популярним через свою швидкість доступу та зручність управління порівняно з магнітними стрічками.

- Опис: Дискові системи, такі як RAID-масиви або мережеві системи зберігання (NAS), забезпечують швидкий доступ до даних та можливість швидкого відновлення.

- Переваги: Швидкий доступ до резервних копій. RAID-масиви можуть надавати додаткову надійність через редундантне зберігання даних.

- Недоліки: Висока вартість у порівнянні з магнітними носіями. Диски також можуть вийти з ладу, що вимагає їхньої регулярної заміни та обслуговування.

Хмарне резервування стає все більш популярним завдяки своїй масштабованості та гнучкості.

- Опис: Хмарне резервування передбачає зберігання даних у віртуальному сховищі, що обслуговується постачальником хмарних послуг. Дані можуть бути доступні з будь-якого місця, де є доступ до Інтернету.

- Переваги: Легке масштабування зберігання, висока доступність і можливість швидкого відновлення з будь-якого місця.

- Недоліки: Залежність від інтернет-з'єднання та потенційні питання з конфіденційністю і безпекою даних.

Кожен з цих методів має свої специфічні переваги та недоліки, тому вибір залежить від конкретних потреб бізнесу, включаючи розмір і тип даних, що потребують захисту, а також доступний бюджет. Важливо розглянути всі варіанти перед прийняттям остаточного рішення.

У міру розвитку технологій з'являються все більш ефективні програмні рішення для резервування даних, які пропонують поліпшену зручність, безпеку та швидкість відновлення. Розглянемо детальніше основні категорії програмного забезпечення, які використовуються в сучасних системах резервного копіювання.

Дискове резервування стає все більш популярним завдяки своїй швидкості та зручності. Програмне забезпечення для дискового резервування дозволяє автоматизувати процес створення та управління резервними копіями.

- Приклади:

- Acronis True Image: Забезпечує повне резервування диска, що включає операційну систему, додатки, налаштування та особисті файли. Підтримує шифрування для збільшення безпеки.

- EaseUS Todo Backup: Просте в користуванні рішення, яке дозволяє користувачам виконувати повне, диференціальне та інкрементальне резервування.

- Особливості:

- Шифрування даних: Захищає резервні копії від несанкціонованого доступу.

- Інкрементальне резервування: Дозволяє зберігати тільки зміни, що відбулися після останнього резервного копіювання, знижуючи час резервування та потребу у зберіганні.

Хмарні рішення стають все більш вибором для багатьох організацій через їх масштабованість та доступність.

- Приклади:

- Google Drive: Інтегрується з широким спектром додатків та пристроїв, забезпечуючи легке резервування документів та фотографій.

- Microsoft OneDrive: Пропонує вбудовані можливості для резервування робочих файлів і інтеграцію з Office 365.

- Amazon S3: Надає надійне рішення для великих обсягів даних з розширеними можливостями управління та налаштування.

- Особливості:

- Автоматичне резервування: Дозволяє налаштувати регулярне резервування

без втручання користувача.

- Відновлення з будь-якого пристрою: Доступ до резервних копій можливий з будь-якого місця, де є доступ до інтернету.

Гібридні системи комбінують локальне та хмарне резервування, надаючи баланс між безпекою та доступністю.

- Опис: Гібридні рішення використовують локальні ресурси для швидкого доступу до даних та хмарні сервіси для додаткового рівня резервування та захисту.

- Переваги: Забезпечують високий рівень безпеки за рахунок локальних копій та гнучкість відновлення завдяки хмарним технологіям.

- Недоліки: Можуть бути дорожчими через необхідність підтримки як локальної, так і хмарної інфраструктури.

Розуміння цих категорій та їх особливостей допоможе організаціям зробити обґрунтований вибір програмного забезпечення для резервного копіювання, виходячи з їх конкретних потреб та ресурсів. Важливо зважати на баланс між швидкістю відновлення, безпекою даних, зручністю управління та вартістю рішення.

Вибір оптимального рішення для резервування даних вимагає розуміння критеріїв, які мають вирішальне значення для забезпечення безпеки, доступності та економічної ефективності. Розглянемо ключові критерії та сценарії використання, які допоможуть організаціям у прийнятті відповідальних рішень щодо систем резервного копіювання.

Безпека даних є одним з основних пріоритетів при виборі рішення для резервування. Важливо враховувати рівень шифрування, яке пропонує програмне забезпечення, а також можливості фізичного захисту даних у випадку локальних рішень.

Доступність резервних копій є критичною, особливо у випадку непередбачених обставин, які вимагають швидкого відновлення. Ключовими параметрами є частота резервування та швидкість доступу до резервних копій.

Вартість рішення для резервування даних включає не тільки початкові інвестиції у придбання обладнання або програмного забезпечення, але й тривалі витрати на його обслуговування та управління. Вибір економічно ефективного рішення, яке задовольняє всі потреби, є ключовим для бюджетної дисципліни[7].

Для малих та середніх підприємств ідеальним може бути використання хмарних рішень для резервування через їх низьку початкову вартість і

масштабованість. Хмарні сервіси забезпечують гнучкість і знижують потребу у великих інвестиціях у локальне обладнання.

Великі організації, як правило, воліють гібридні рішення, які поєднують локальне резервування з хмарним для забезпечення вищого рівня безпеки та оперативного доступу до даних. Це дозволяє їм оптимізувати доступність даних і одночасно забезпечити їх захист від різних ризиків.

Вибір системи для резервування даних залежить від багатьох факторів, включаючи розмір та тип бізнесу, специфічні потреби в захисті даних, а також бюджетні обмеження. Важливо обрати рішення, яке не тільки відповідає поточним вимогам, але й здатне адаптуватися до змін у майбутньому, щоб забезпечити надійне та ефективне відновлення даних у будь-якій ситуації.

4. ВДОСКОНАЛЕННЯ СТРАТЕГІЙ БЕЗПЕКИ МЕРЕЖЕВИХ СИСТЕМ

4.1 Розробка комплексних підходів до зміцнення мережевої безпеки

Мережева безпека є ключовим компонентом інформаційної безпеки у всіх організаціях, що забезпечує захист даних і ресурсів від несанкціонованого доступу, зловмисних атак та інших загроз. З розвитком технологій та збільшенням числа кібератак, важливість надійних стратегій мережевої безпеки набуває ще більшої актуальності. Цей розділ має на меті розробити комплексні підходи для зміцнення мережевої безпеки, враховуючи сучасні виклики та можливі загрози.

Кіберпростір сьогодні наповнений різноманітними загрозами, від вірусів та шкідливого програмного забезпечення до складних кібератак, таких як фішинг, ransomware атаки, і атаки на інфраструктуру. Наприклад, за даними останніх досліджень, фішинг став однією з найпоширеніших причин витоку даних, а кіберзлочинці все частіше використовують інноваційні методи для обходу традиційних заходів безпеки[14].

Традиційні методи забезпечення мережевої безпеки часто не встигають за швидкістю розвитку кіберзагроз. Багато існуючих систем захисту базуються на застарілих технологіях, які не можуть ефективно протистояти сучасним методам кібератак. Крім того, недостатня увага до обучення персоналу та оновлення програмного забезпечення також сприяють підвищенню ризику безпеки.

Щоб зміцнити мережеву безпеку, необхідно спочатку чітко визначити, які активи є найбільш важливими для організації та які загрози є найбільш актуальними. Важливо оцінити, які системи мають критичне значення для діяльності організації та які дані можуть становити особливий інтерес для зловмисників.

- Ключові активи: Сервери, бази даних, мережеве обладнання.

- Критичні ресурси: Конфіденційна інформація, фінансові дані, особисті дані співробітників.

- Оцінка ризиків: Оцінка потенційних загроз та вразливостей, що можуть вплинути на ці активи та ресурси.

1. Технологічні інновації:

- Апаратне забезпечення: Впровадження сучасних апаратних засобів, таких як мережеві сканери безпеки та інтегровані системи захисту.

- Штучний інтелект: Розробка систем, що використовують машинне навчання для виявлення аномалій у поведінці мережі та швидкого реагування на потенційні атаки.

2. Політика та процедури:

- Політики безпеки: Створення чітких правил та процедур, які регулюють доступ до мережевих ресурсів та управління ними.

- Реагування на інциденти: Розробка планів реагування на інциденти, що дозволять оперативно ідентифікувати та локалізувати безпекові порушення.

3. Освіта та тренінг:

- Навчання співробітників: Регулярні тренінги та семінари для підвищення обізнаності з питань кібербезпеки серед всіх рівнів персоналу.

- Свідомість про безпеку: Заходи щодо виховання культури безпеки в організації, з акцентом на проактивний захист інформації.

Таблиця 4.1

Оцінка ризиків

Актив	**Ризик**	**Ймовірність**	**Вплив**	**Заходи зі зниження**
Сервери	Хакерські атаки	Висока	Критичний	Шифрування, бекапи
Бази даних	Витік даних	Середня	Високий	Доступ за ролями, аудит
Мережеве обладнання	Фізичний доступ	Низька	Високий	Біометричний контроль

В цій секції розглядаються ключові технології та засоби, що можуть бути використані для зміцнення мережевої безпеки. Включають файрволи, антивірусні програми, шифрування, а також сучасні системи виявлення і реагування на інциденти (SIEM).

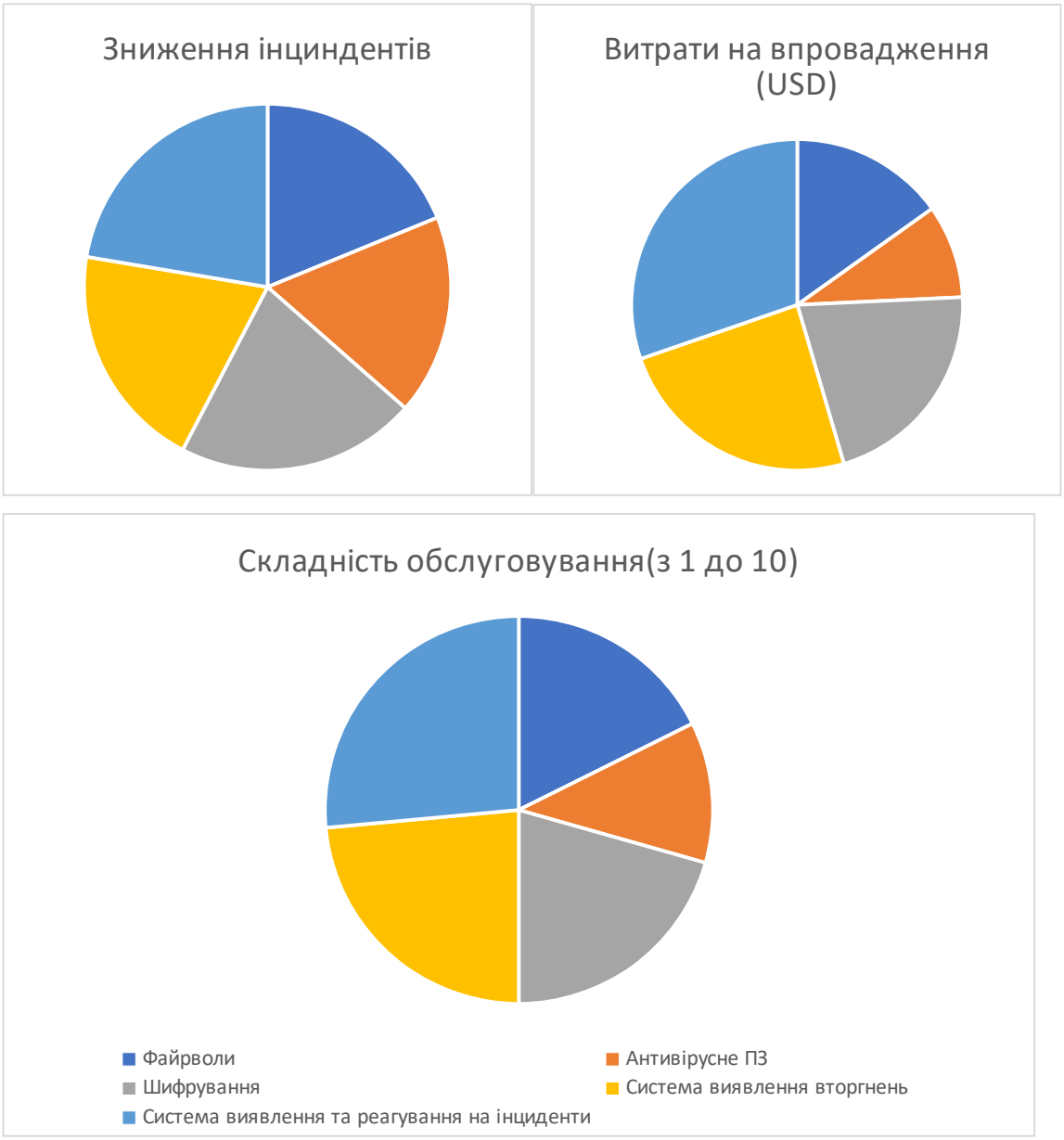


Рис. 4.1 – Ефективність різних заходів безпеки[12]

Рисунок 4.1 демонструє порівняльну ефективність різних технологій та методів за останні 5 років. Заходи оцінюються за такими критеріями, як зниження інцидентів, витрати на впровадження та складність обслуговування.

1. Технологічні інновації значно підвищують рівень безпеки, особливо коли вони інтегровані у комплексний захист, що включає шифрування, використання фаєрволів, антивірусного програмного забезпечення, та сучасних систем виявлення та реагування на інциденти (SIEM).

2. Політика та процедури відіграють критичну роль у захисті мережевих ресурсів, включаючи чітке визначення доступу та реакції на інциденти.

Правильно розроблені та систематично оновлювані політики можуть значно знизити ризик кібератак та їхні наслідки.

3. Освіта та тренінг сприяють підвищенню рівня освіченості співробітників щодо потенційних загроз і найкращих практик безпеки. Регулярне навчання допомагає мінімізувати людський фактор, який часто є слабкою ланкою у забезпеченні безпеки.

У майбутньому дослідження мережевої безпеки повинно зосередитися на кількох ключових аспектах:

1. Розвиток штучного інтелекту та машинного навчання для створення більш авансованих систем виявлення загроз, які можуть прогнозувати і запобігати атакам у реальному часі.

2. Розробка засобів захисту інтернету речей (IoT), який швидко впроваджується у багатьох секторах, вимагає нових підходів до безпеки через велику кількість підключених пристроїв і потенційних точок втручання.

3. Забезпечення безпеки великих даних та їх аналізу, що включає розробку методів захисту даних від внутрішніх та зовнішніх загроз у процесі їх зберігання та обробки.

4.2 Приклади успішних стратегій резервування та їх імплементація

Стратегії резервування відіграють вирішальну роль у сучасному управлінні ризиками, надаючи організаціям можливість ефективно реагувати на фінансові та операційні непередбаченості. Цей розділ розглядає теоретичні аспекти стратегій резервування та висвітлює приклади їх успішного застосування в різних галузях. Через аналіз конкретних кейсів та визначення основних викликів і рекомендацій, текст покликаний надати глибоке розуміння цієї критично важливої частини управління ризиками.

Стратегії резервування базуються на принципах актуарних наук, статистики та фінансового аналізу, дозволяючи оцінити ймовірність та потенційні наслідки різноманітних ризиків. Основні компоненти цих стратегій включають:

1. Математичне резервування: Використання математичних моделей для обрахунку необхідних резервів, що забезпечують фінансову стабільність компанії у випадку реалізації ризиків.

2. Статистичне прогнозування: Аналіз історичних даних для прогнозування майбутніх потреб у резервах. Цей підхід дозволяє адаптувати резерви до поточної ділової ситуації та ринкових умов.

3. Технологічне забезпечення: Інтеграція сучасних IT-систем для збору, обробки та аналізу даних, що підвищує точність розрахунків та ефективність управління резервами.

Приклади успішних стратегій резервування

Один із провідних банків використовує стратегію динамічного резервування для мінімізації кредитних ризиків. Через розробку алгоритмічного підходу, банк зміг адаптувати свої резерви у відповідь на зміни кредитоспроможності клієнтів та коливання економічного середовища. Це забезпечило зниження втрат і підвищення фінансової стабільності[6].

Страхова компанія впровадила комплексну систему катастрофічного резервування, що дозволило їй ефективно реагувати на наслідки природних катастроф. Використання передових моделей оцінки ризиків та широкомасштабних даних допомогло знизити фінансовий тиск та оптимізувати розподіл ресурсів.

Ось декілька рекомендацій, які можуть допомогти компаніям ефективно впровадити та управляти стратегіями резервування:

1. Підвищення кваліфікації персоналу: Навчання та розвиток персоналу у сфері передових аналітичних методів і IT-інструментів забезпечить високий рівень компетенції у формуванні та управлінні резервами.

2. Інвестиції в технології: Впровадження сучасних IT-систем та аналітичного програмного забезпечення дозволить компаніям ефективно обробляти великі дані, покращуючи якість прогнозів та оптимізацію резервів.

3. Гнучке реагування на зміни умов: Розробка адаптивних моделей, що можуть швидко відображати зміни в економічному та ринковому середовищі, є ключовим аспектом успішної стратегії резервування.

4. Стратегічне планування: Регулярний перегляд та оновлення стратегій резервування допоможуть компанії залишатися на крок попереду потенційних ризиків та забезпечити фінансову стійкість.

Впровадження ефективних стратегій резервування є важливим елементом загальної політики управління ризиками будь-якої організації. Ці стратегії дозволяють не тільки мінімізувати потенційні втрати від несподіваних подій, але й підвищують загальну резистентність компанії до зовнішніх викликів. Успішна імплементація таких стратегій вимагає комплексного підходу, що включає належне теоретичне підгрунтя, залучення кваліфікованих фахівців, інвестиції в передові технології, а також гнучку адаптацію до змінних ринкових умов. Завдяки цьому компанії можуть ефективно управляти своїми ресурсами та гарантувати свою стабільність та розвиток у майбутньому.

4.3 Оцінка ефективності запропонованих рішень

Оцінка ефективності запропонованих рішень є ключовим елементом у процесі управління проектами та розробки стратегічних планів у бізнесі та науці. Цей процес допомагає організаціям та дослідникам визначати, наскільки добре рішення відповідають поставленим цілям, які ресурси вони вимагають, і які результати вони приносять. Відповідно, ефективність може оцінюватися як ступінь досягнення специфічних, заздалегідь визначених цілей з мінімальними витратами ресурсів або з максимальним можливим покращенням[13].

Цей розділ має на меті обговорити теоретичні підходи до оцінки ефективності, визначити найпоширеніші методики, які використовуються для цього процесу, а також представити різні критерії, які можна застосувати для аналізу ефективності рішень у різних контекстах. Особлива увага буде приділена

збалансуванню між кількісними та якісними показниками, що є критично важливим для всебічного розуміння впливу рішень.

Управління проектами і стратегічне планування часто включають комплексну оцінку ефективності запропонованих рішень. Теоретичні основи оцінки ефективності охоплюють різні підходи, які можуть бути класифіковані як кількісні і якісні методи оцінки. Кількісні методи оцінки ефективності зосереджені на числових показниках, таких як дохід, прибуток, віддача інвестицій (ROI), чиста поточна вартість (NPV) або внутрішня норма прибутку (IRR). Ці методи дозволяють виміряти ефективність у стандартизованих умовах і надають об'єктивну основу для порівняння альтернативних рішень.

ВИСНОВКИ

Було детально розглянуто проблематику забезпечення безпеки мережевих систем інтернет-провайдерів з особливим акцентом на використання хмарних технологій та стратегій резервного копіювання даних. Аналіз сучасних загроз та вразливостей підтвердив важливість комплексного підходу до забезпечення безпеки, який включає застосування новітніх технологій та методик.

Дослідження показало, що інтеграція хмарних рішень може суттєво підвищити ефективність мережевих систем, забезпечуючи при цьому високий рівень захисту та гнучкості управління даними. Однак, важливою є постійна увага до питань кібербезпеки, зокрема, контролю доступу та шифрування даних.

Дипломна робота також виявила ряд рекомендацій для покращення мережевої безпеки, зокрема розробку та впровадження політик безпеки, регулярне навчання персоналу, та використання передових технологій IDS/IPS та шифрування даних. Ці заходи можуть значно знизити ризики, пов'язані з кіберзагрозами, та забезпечити надійну роботу мережевих ресурсів інтернет-провайдерів.

На основі проведеного дослідження, пропонується подальше вивчення інноваційних технологій в області хмарних обчислень, які можуть бути інтегровані в мережеві системи для підвищення їхньої ефективності та безпеки. Також рекомендується розширення дослідження стосовно впливу регуляторних змін на використання хмарних сервісів в інтернет-провайдингу.

Дослідження підкреслило важливість міждисциплінарного підходу в аналізі та вирішенні проблем мережевої безпеки, вимагаючи від фахівців глибоких знань у сферах інформаційних технологій, кібербезпеки та управління даними.

ПЕРЕЛІК ПОСИЛАНЬ

1. Stallings, W. "Cryptography and Network Security: Principles and Practice." Pearson Education.

2. Vacca, J. R. "Computer and Information Security Handbook." Morgan Kaufmann Publishers.

3. Zwicky, E. D., Cooper, S., Chapman, D. B. "Building Internet Firewalls." O'Reilly Media.

4. Tipton, H. F., & Krause, M. "Information Security Management Handbook." Auerbach Publications, останнє видання.

5. Loshin, P. "Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph." Elsevier.

6. Chou, T. "Precision: Principles, Practices and Solutions for the Internet of Things." Prentice Hall.

7. Whitman, M. E., & Mattord, H. J. "Management of Information Security." Cengage Learning.

8. Northcutt, S. "Network Intrusion Detection." New Riders Publishing, останнє видання.

9. Caloyannides, M. A. "Privacy Protection and Computer Forensics." Artech House Publishers.

10. Peltier, T. R. "Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management." Auerbach Publications.

11. Kaeo, M. "Designing Network Security." Cisco Press.

12. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. "Firewalls and Internet Security: Repelling the Wily Hacker." Addison-Wesley Professional.

13. Barker, S., & Smith, D. "Cloud Computing: Concepts, Technology & Architecture." Prentice Hall.

14. Krutz, R. L., & Vines, R. D. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing." Wiley Publishing.

15. Clarke, J. "Protecting Networks with SATAN." O'Reilly Media.

ДОДАТОК А

Для створення програми на Python, яка підтримує удосконалення безпеки мережевих систем для інтернет-провайдерів, ми складемо основні компоненти. Ось загальний огляд того, як ми можемо розробити кожен модуль:

1. Модуль аутентифікації

Цей модуль буде використовувати бібліотеку `flask` для створення веб-сервера, а також `pyotp` для двофакторної аутентифікації.

2. Модуль шифрування

Для шифрування даних перед зберіганням використаємо `cryptography`. Ми реалізуємо шифрування і дешифрування даних, що зберігаються.

3. Модуль резервного копіювання

Цей модуль може використовувати `boto3` для взаємодії з AWS S3 як хмарним сховищем. Ми налаштуємо автоматичне резервне копіювання з використанням розкладу.

4. Модуль моніторингу та аудиту

Використовуючи `logging` для журналювання подій і `flask` для веб-інтерфейсу аудиту, створимо систему моніторингу активності.

Щодо використання цього коду, нам потрібно буде створити файл для ключа шифрування та налаштувати наше середовище для використання `boto3` та `pyotp`.

Код програми Python буде мати наступний вигляд:

```
from flask import Flask, request, render_template, redirect, url_for, flash, session
import pyotp
from cryptography.fernet import Fernet
import logging
from google_auth_oauthlib.flow import InstalledAppFlow
from googleapiclient.discovery import build
from googleapiclient.http import MediaFileUpload
import os
```

```
app = Flask(name)
app.secret_key = 'your_super_secret_key'

# Setup logging for monitoring and auditing
logging.basicConfig(level=logging.INFO)

# Load encryption key or generate if doesn't exist
def load_or_generate_key():
    try:
        return open("secret.key", "rb").read()
    except FileNotFoundError:
        key = Fernet.generate_key()
        with open("secret.key", "wb") as key_file:
            key_file.write(key)
        return key

key = load_or_generate_key()
cipher_suite = Fernet(key)

class GoogleDriveBackup:
    def init(self, client_secrets_file):
        self.service = self.authenticate_google_drive(client_secrets_file)

    def authenticate_google_drive(self, client_secrets_file):
        flow = InstalledAppFlow.from_client_secrets_file(
            client_secrets_file,
            scopes=['https://drive.google.com/drive/folders/1coUrSN48H6ry86A3zXs
WehJBO-2kb8H5?usp=sharing '])
        creds = flow.run_local_server(port=8080)
```

```
            return build('drive', 'v3', credentials=creds)

        def upload_file(self, file_name, path_to_file):
            file_metadata = {'name': file_name}
            media = MediaFileUpload(path_to_file, mimetype='text/plain')
                file = self.service.files().create(body=file_metadata, media_body=media,
fields='id').execute()
            logging.info(f'Uploaded file ID: {file.get("id")}')
            return file.get('id')

    gdrive = GoogleDriveBackup('C:\\Users\\txxrbeena\\Desktop\\1\\CURSEach\\
soft\\client_secret.json')

    @app.route('/')
    def index():
        return render_template('index.html')

    @app.route('/encrypt', methods=['POST'])
    def encrypt():
        data = request.form['data']
        if data:
            encrypted_text = cipher_suite.encrypt(data.encode())
                    return render_template('result.html', result=encrypted_text.decode(),
action='Encrypt')
            else:
                flash('No data provided')
                return redirect(url_for('index'))

    @app.route('/decrypt', methods=['POST'])
    def decrypt():
```

```
        data = request.form['data']
        if data:
            decrypted_text = cipher_suite.decrypt(data.encode())
                return render_template('result.html', result=decrypted_text.decode(), action='Decrypt')
        else:
            flash('No data provided')
            return redirect(url_for('index'))

    @app.route('/upload', methods=['POST'])
    def upload_file_to_drive():
        if 'file' not in request.files:
            flash('No file part')
            return redirect(request.url)
        file = request.files['file']
        if file.filename == '':
            flash('No selected file')
            return redirect(request.url)
        if file:
                file_path = os.path.join('C:\\Users\\коте\\OneDrive\\Рабочий стол', file.filename)
            file.save(file_path)
            file_id = gdrive.upload_file(file.filename, file_path)
            flash(f'File successfully uploaded with ID {file_id}')
            return redirect(url_for('index'))

    if name == 'main':
        app.run(debug=True, port=8080)
```

До цього коду необхідно створити два файли HTML, які будуть мати наступний вигляд:

Index.html:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Secure App</title>
</head>
<body>
    <h1>Welcome to the Secure App</h1>
    <h2>Encrypt Data</h2>
    <form action="/encrypt" method="post">
        <input type="text" name="data" placeholder="Enter data to encrypt">
        <button type="submit">Encrypt</button>
    </form>
    <h2>Decrypt Data</h2>
    <form action="/decrypt" method="post">
        <input type="text" name="data" placeholder="Enter data to decrypt">
        <button type="submit">Decrypt</button>
    </form>
    <h2>Upload File to Google Drive</h2>
    <form action="/upload" method="post" enctype="multipart/form-data">
        <input type="file" name="file">
        <button type="submit">Upload</button>
    </form>
</body>
</html>
```

Result.html:

```
<!DOCTYPE html>
<html lang="en">
```

```
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Result | Secure App</title>
</head>
<body>
    <h1>Result</h1>
    <p><strong>Action:</strong> {{ action }}</p>
    <p><strong>Result:</strong> {{ result }}</p>
    <a href="/">Back to Home</a>
</body>
</html>
```

Також необхідно взяти файл JSON, який можна взяти з Google Cloud Console, у цій роботі не буде вказано зміст цього файлу з ціллю безпеки даних.

Інтерфейс програми буде мати вигляд:

Рис. 5.1 – Інтерфейс програми

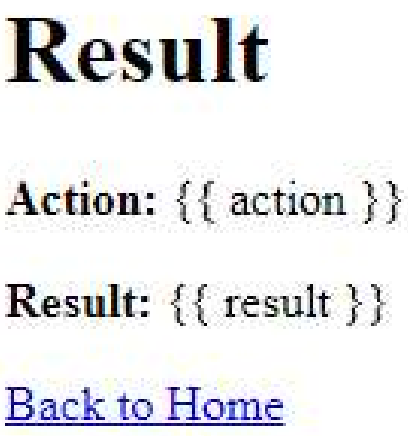


Рис. 5.2 – Інтерфейс результату програми

ДОДАТОК Б

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«УДОСКОНАЛЕННЯ БЕЗПЕКИ МЕРЕЖЕВИХ СИСТЕМ У СФЕРІ ІНТЕРНЕТ ПРОВАЙДИНГУ: ХМАРНІ СХОВИЩА ТА СТРАТЕГІЇ РЕЗЕРВУВАННЯ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: Корнус А.В., ІСД-42
Науковий керівник роботи:
Шахматов І. О.

Київ - 2024

Актуальність теми обумовлена зростаючою тенденцією цілеспрямованих атак, складності захисту великого обсягу даних, та, передусім, конфіденційність даних, які передаються через мережу.

Об'єкт дослідження: функціонування мережевих системи інтернет-провайдерів. ***Предмет дослідження:*** механізми забезпечення безпеки даних у мережах інтернет-провайдингу, з особливим акцентом на хмарні сховища та стратегії резервування.

Мета дослідження: вдосконалення стратегій безпеки мережевих систем, що використовуються інтернет-провайдерами

Завдання дослідження:

1. Забезпечити належний захист даних та інфраструктури інтернет-провайдерів.
2. Дослідити можливості використання хмарних сховищ у сфері безпеки.
3. Вивчення можливих стратегій для резервування, та їх використання.

Рис. 1.1 – Класифікація комп'ютерних мереж

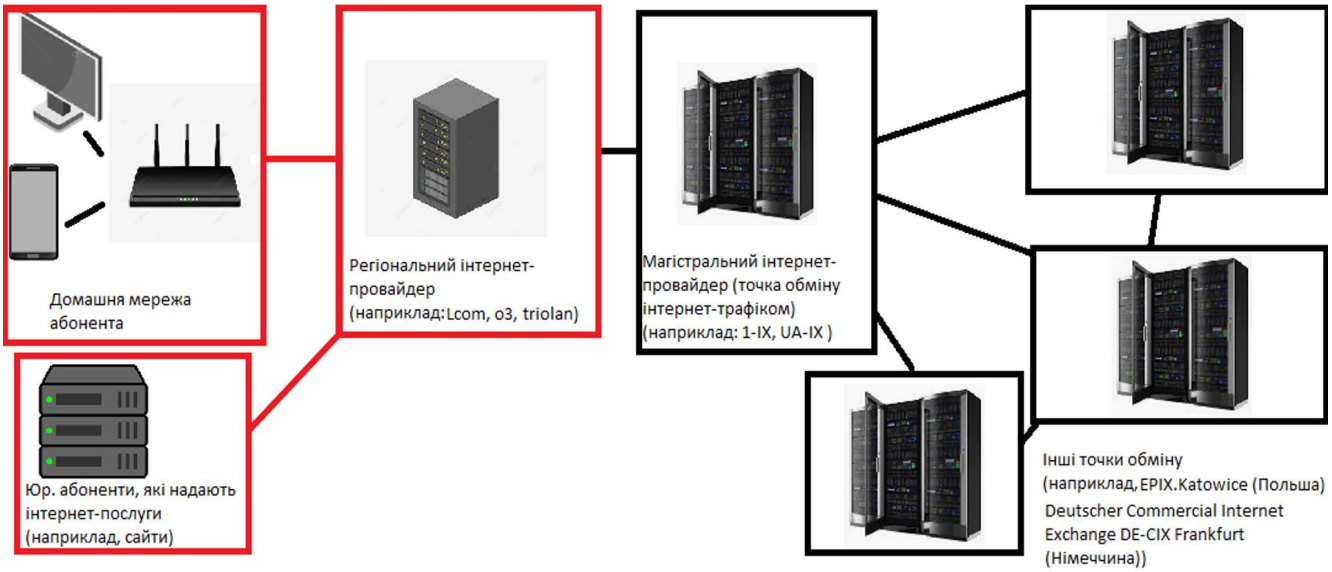


Рис 1.2 Приблизна схема функціонування Інтернет

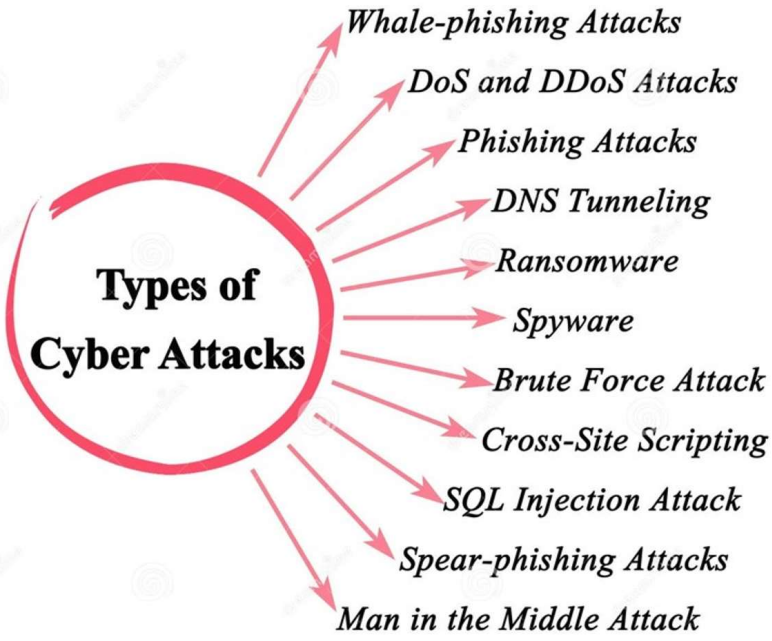


Рис 2.1 – Типи зовнішніх кібер-загроз

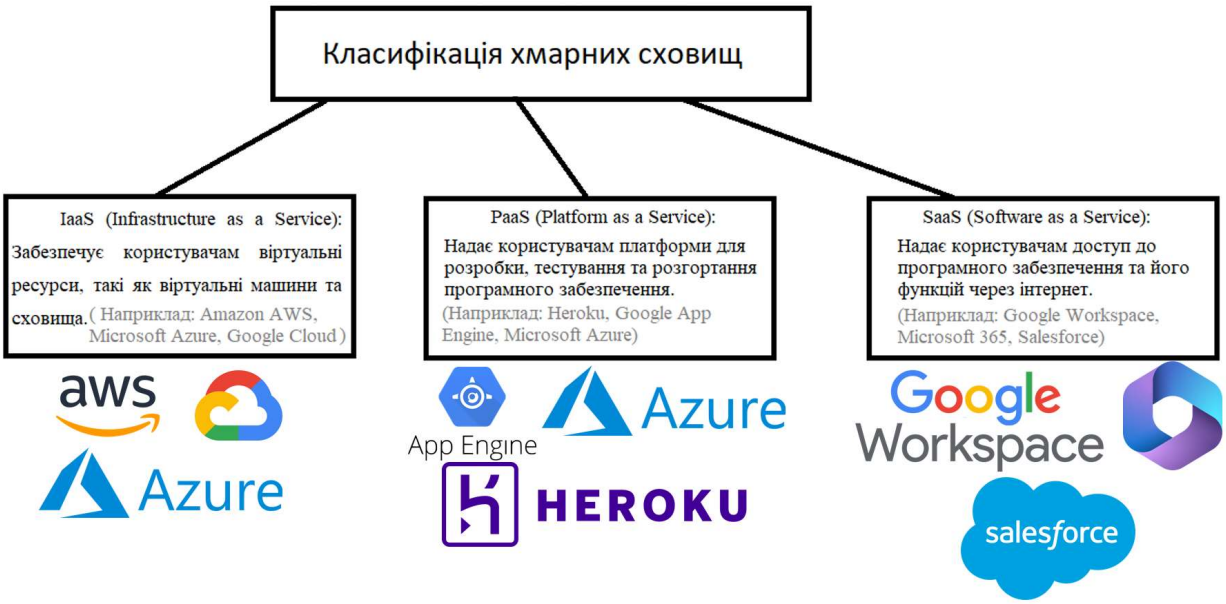


Рис 3.1 – Основна класифікація хмарних сховищ

Компонент	Опис	Функції
Клієнтські пристрої	Точки доступу користувачів (комп'ютери, мобільні телефони, інші пристрої)	Забезпечення доступу до хмарних ресурсів, інтерфейс користувача
Веб-сервери	Сервери, що обробляють запити від клієнтів та управляють веб-інтерфейсами	Обробка запитів до хмарних сервісів, відправлення та отримання даних
Прикладні сервери	Сервери, які запускають специфічні додатки або сервіси хмарної платформи	Виконання програмного забезпечення, яке потребує великих обчислювальних потужностей
Сервери баз даних	Спеціалізовані сервери для зберігання та управління даними	Зберігання великих обсягів даних, забезпечення високої швидкості читання та запису
Сховища даних	Системи зберігання, що використовуються для архівації, резервного копіювання та відновлення даних	Зберігання даних з високою доступністю та надійністю, оптимізація використання дискового простору
Мережева інфраструктура	Маршрутизатори, комутатори, балансувальники навантаження	Забезпечення зв'язності та оптимального розподілу трафіку між серверами та пристроями
Управління та моніторинг	Системи для контролю стану хмарної інфраструктури та управління ресурсами	Моніторинг стану системи, автоматичне масштабування ресурсів, забезпечення безпеки

Рис 3.2 - Структурна схема типової архітектури хмарного зберігання

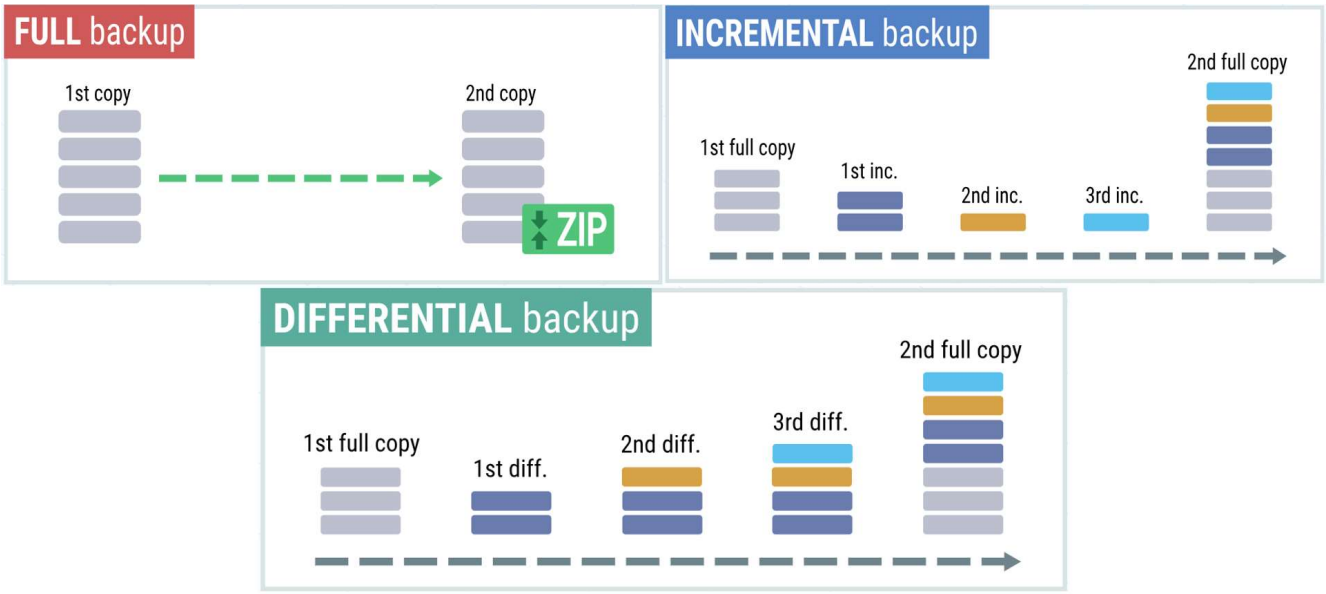


Рис 4.1 – візуалізація типів резервного копіювання

Актив	Ризик	Ймовірність	Вплив	Заходи зі зниження
Сервери	Хакерські атаки	Висока	Критичний	Шифрування, бекапи
Бази даних	Витік даних	Середня	Високий	Доступ за ролями, аудит
Мережеве обладнання	Фізичний доступ	Низька	Високий	Біометричний контроль

Рис 4.2 – Ключові активи інтернет провайдера та зв’язані з ними ризики

Також в цю класифікацію було б доречно додати актив «Співробітники», так як це першооснова функціонування любої мережі.

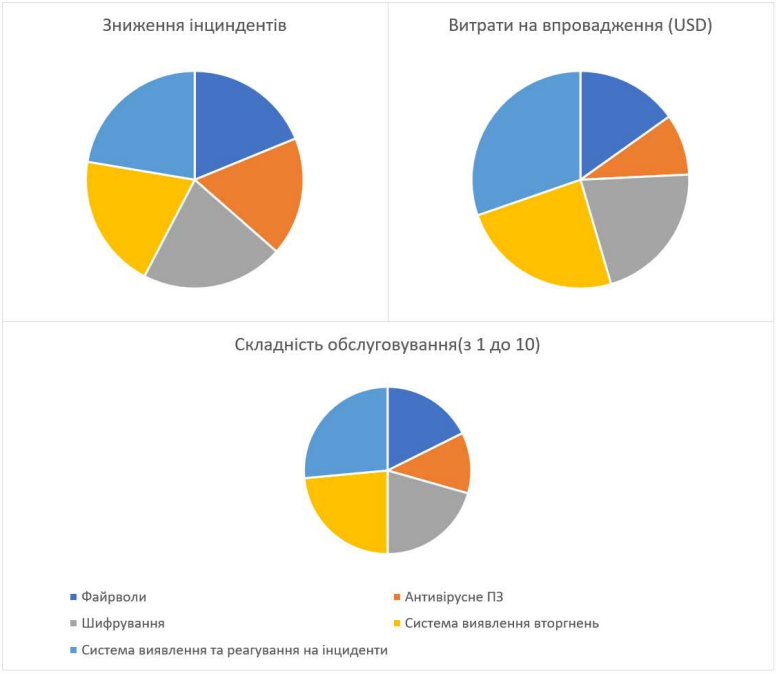


Рис 4.3 – Співвідношення ефективності різних заходів безпеки