НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАХИСТ ХМАРНИХ ПРОГРАМ, КОРИСТУВАЧІВ І ПОВ'ЯЗАНИХ ТЕХНОЛОГІЙ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Гандзій Ілля Ігорович

Керівник: д.ф-м.н., професор
Василенко Микола Дмитрович

Рецензент: к.ф. – м. н., доцент
Чепурна Олена Євгенівна

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____»_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (магістерську) роботу
здобувачу Гандзія Іллі Ігоровича

1. Тема роботи: «Захист хмарних програм, користувачів і пов'язаних технологій при використанні хмарних обчислень»
Керівник роботи: д. ф.-м. н, професор Василенко Микола Дмитрович
затверджені наказом НУ ОЮА від *«_____»_____№ _____*
2. Строк подання здобувачем роботи *«20» травня 2024 року*
3. Дата видачі завдання *«15» вересня 2023 року*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Захист хмарних програм, користувачів і пов’язаних технологій при використанні хмарних обчислень» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальності 125 «Кібербезпека».

Містить 7 рисунків, 4 таблиць, 18 літературних джерел за переліком посилань. Робота виконана на 64 сторінках загального тексту і 55 сторінках основного тексту.

У цій кваліфікаційній роботі досліджується проблема безпеки в хмарних обчисленнях. Розглядається сучасний стан захисту хмарних програм, користувачів та пов'язаних технологій, аналізуються основні виклики і переваги. Перший розділ включає огляд систем забезпечення безпеки для користувачів хмарних послуг, охоплюючи механізми захисту даних і конфіденційності, а також питання аутентифікації, авторизації та керування доступом.

Другий розділ аналізує стан програмного забезпечення для захисту в хмарних обчисленнях, включаючи вимоги до захисту програм і даних у хмарних сервісах та роль інтеграції технологій безпеки під час розгортання хмарних рішень. Особлива увага приділяється автоматизації та моніторингу заходів безпеки в хмарному середовищі.

У завершальному розділі надаються практичні рекомендації та висновки щодо сучасних стратегій і підходів до захисту в хмарних обчисленнях, а також практичні поради для користувачів і розробників хмарних додатків. Результати дослідження сприятимуть кращому розумінню проблем безпеки в хмарних обчисленнях і допоможуть у розробці ефективних стратегій та інструментів для забезпечення безпеки.

ХМАРНІ ОБЧИСЛЕННЯ, ЗАХИСТ ДАНИХ, БЕЗПЕКА ХМАРНИХ СЕРВІСІВ, АВТОМАТИЗАЦІЯ БЕЗПЕКИ.

ABSTRACT

Qualification Work on the Topic "Protection of Cloud Applications, Users, and Related Technologies in Cloud Computing" for Obtaining the First (Bachelor's) Level of Higher Education in Specialty 125 "Cybersecurity." Contains 7 figures, 4 tables, and 18 literary sources listed in the references. The work is composed of 64 pages of total text and 55 pages of main text.

This qualification work explores the problem of security in cloud computing. It examines the current state of protection for cloud applications, users, and related technologies, analyzing the main challenges and advantages. The first chapter provides an overview of security systems for cloud service users, covering data protection and privacy mechanisms, as well as issues of authentication, authorization, and access control.

The second chapter analyzes the state of software for protection in cloud computing, including the requirements for protecting applications and data in cloud services and the role of integrating security technologies during the deployment of cloud solutions. Special attention is given to the automation and monitoring of security measures in the cloud environment.

The final chapter offers practical recommendations and conclusions on modern strategies and approaches to cloud computing security, as well as practical advice for users and developers of cloud applications. The research results will contribute to a better understanding of security issues in cloud computing and aid in the development of effective strategies and tools for ensuring security.

CLOUD COMPUTING, DATA PROTECTION, CLOUD SERVICE SECURITY, SECURITY AUTOMATION

ЗМІСТ

ВСТУП

У сучасному інформаційному середовищі хмарні обчислення здобувають все більшу популярність як ефективний спосіб забезпечення доступу до обчислювальних ресурсів та послуг через Інтернет. Однак разом із зростанням використання хмарних технологій зростає і важливість питань безпеки та захисту інформації в хмарних середовищах. Це обумовлено потребою у забезпеченні конфіденційності, цілісності та доступності даних, що зберігаються і оброблюються в хмарних системах.

Актуальність Дослідження забезпечення безпеки в хмарних обчисленнях є актуальним завданням у зв'язку зі зростанням обсягів конфіденційної і критичної інформації, яка зберігається в хмарних середовищах. Недостатній рівень захисту може призвести до різноманітних загроз, включаючи несанкціонований доступ, втрату даних або порушення конфіденційності.

Мета роботи даної кваліфікаційної роботи є дослідження сучасних стратегій, методів та інструментів забезпечення безпеки в хмарних обчисленнях з метою розробки рекомендацій щодо підвищення рівня захисту даних у хмарних середовищах.

Об’єкт та Предмет дослідження Об’єктом дослідження є процес забезпечення безпеки в хмарних обчисленнях. Предметом дослідження є методи, технології та інструменти, спрямовані на захист даних та систем хмарних обчислень.

Мета дослідження

Основною метою дослідження є:

- Огляд і аналіз сучасного стану засобів забезпечення безпеки в хмарних системах.
- Вивчення основних викликів та переваг захисту даних у хмарних середовищах.
- Виявлення і розгляд систем забезпечення безпеки для користувачів та програм в хмарних обчисленнях.

- Розробка практичних рекомендацій з підвищення рівня захисту інформації в хмарних обчисленнях.

Структура кваліфікаційної роботи

Робота складається з трьох основних розділів:

1. Аналіз сучасного стану захисту хмарних програм, користувачів та пов'язаних технологій - у цьому розділі розглядаються основні виклики та переваги забезпечення безпеки в хмарних середовищах, системи захисту для користувачів хмарних послуг, а також порівняльний аналіз засобів безпеки.

2. Стан програмного забезпечення для захисту в хмарних обчисленнях - у другому розділі досліджується вимоги до засобів захисту програм та даних у хмарних сервісах, а також роль інтеграції технологій безпеки в розгортанні хмарних рішень.

3. Практичні рекомендації та висновки - у завершальному розділі надаються сучасні стратегії та підходи до захисту в хмарних обчисленнях, а також практичні поради забезпечення безпеки для користувачів та розробників хмарних додатків.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАХИСТУ ХМАРНИХ ПРОГРАМ

Хмарні технології означають набір інструментів і методів, які дозволяють віддалено зберігати та обробляти дані.

До загальних категорій хмарних сервісів входять такі види: Інфраструктура як сервіс (IaaS), Платформа як сервіс (PaaS), Програмне забезпечення як сервіс (SaaS), хмарне сховище даних, хмарні сервіси обробки даних, хмарні сервіси для розробників (DevOps).[1].

Системи господарства складаються з спеціалізованих підприємств, об'єднаних за галузями та діяльністю, кожна з яких має свої цілі, мету і упорядкованість. Використання хмарних технологій для підвищення ефективності цих систем є важливим і доцільним. Попит на хмарні сервіси для систем господарства зростає з кожним днем, що сприяє розвитку цих систем та поступовому вдосконаленню хмарних технологій.

У моїй роботі я хочу проаналізувати переваги та недоліки використання хмарних технологій для різних систем господарства. Досліджуючи джерела, я згрупував наступні переваги та недоліки.

До переваг використання хмарних технологій як сервісів для різноманітних систем господарства можна віднести:

Гнучкість та масштабність, надійність, доступність, глобальний доступ, економічність (для певних обсягів інформації).

До деяких недоліків використання хмарних технологій як сервісів для різноманітних систем господарства можна віднести [1]:

- Питання безпеки даних за рахунок постачальників послуг;
- На перший погляд хмарні послуги можуть здаватися економічно вигідними, але треба ураховувати додаткові витрати на розвиток та несподівані обставини;

- Обмеження налаштування. Деякі хмарні сервіси можуть обмежувати можливість налаштування з боку клієнтів;
- Зміна вартості послуг;
- Залежність від інтернет-з’єднання.

Сучасні хмарні технології є передовим та перспективним рішенням, що входить у складну «третю ІТ-платформу». Їх швидке поширення є одним з ключових трендів, що значно впливають на глобальний розвиток. У розвинених регіонах, таких як США та ЄС, вже розроблені стратегічні рішення та плани дій для системного та комплексного розвитку хмарних сервісів. [3].

Використання хмарних технологій призводить не лише до значного зниження витрат і підвищення продуктивності, але також пов'язане зі значними ризиками для конфіденційності даних (зокрема, ризики зберігання та передачі даних). Проте хмарні рішення постійно вдосконалюються, і сьогодні хмарні провайдери можуть забезпечити прийнятний рівень безпеки, дотримуючись відповідних вимог.

Україна працює над розробкою національних стандартів, які встановлюватимуть необхідні вимоги до якості та надійності хмарних технологій і послуг. У майбутньому ці стандарти очікується гармонізувати зі стандартами ISO та ЄС.

Хмарний сервіс - це тип інтернет-сервера, який надає віртуальні обчислювальні ресурси на запит для інших пристроїв. Використання хмарних послуг дозволяє зручний мережевий доступ до різноманітних ресурсів, таких як сховища, програми та сервіси, без необхідності встановлювати їх окремо на власний комп'ютер.

Існує три основні типи хмарних сервісів: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS). Давайте розберемо види хмарних сервісів [9]:

IaaS – це найпростіший тип хмарних послуг, що надає клієнтам доступ до інфраструктури, такої як сервери та сховища. Такі хмарні послуги підходять для системних адміністраторів.

PaaS йде на крок далі, ніж IaaS, надаючи клієнтам доступ до всієї платформи для розробки та розгортання програм. Насамперед це інструмент для розробників.

SaaS – це найпередовіший тип хмарного сервісу, що надає клієнтам доступ до сервісів, які вони можуть використовувати на будь-якому пристрої з підключенням до Інтернету. Цей варіант найбільше підходить для бізнесу – CRM-системи, тайм-трекери, платформи для керування завданнями та ін.

Таблиця 1.1 - Порівняння моделей хмарних служб

Тип	Споживач	Служба, яка надається хмарою	Область дії рівня обслуговування	Налаштування
SaaS	Кінцеві користувачі	Готовий додаток	Час роботи додатку, продуктивність додатку	Мінімальне або відсутнє. Можливості, визначаються ринком або постачальником
Закінчення таблиці 1.1 Тип	Споживач	Служба, яка надається хмарою	Область дії рівня обслуговування	Налаштування
IaaS	Власник додатку або компанія, що забезпечує підтримку ОС, ПЗ і додатків	Віртуальний сервер, хмарне сховище	Доступність віртуального сервера, час для підготовки до роботи. Не розповсюджується на платформу або додатки	Мінімальні обмеження для додатків, встановлених в стандартизованих віртуальних збірках ОС

З такою кількістю доступних варіантів може бути складно зрозуміти, який підходить саме вам. Але ми знаємо, як зробити правильний вибір.

Під час вибору постачальника хмарного сховища слід враховувати такі фактори, як вартість, безпека та доступний функціонал. Зібрали для вас кілька порад щодо вибору відповідного хмарного сервісу:

Визначеня своїх потреб. Перший крок – визначити, що вам потрібно від хмарного сервісу. Які завдання він має вирішити? Які бізнес-процеси охоплювати? Чи бажаєте ви керувати всіма сферами бізнесу на одній платформі або шукайте окремий інструмент для вирішення певних завдань? Вам слід обрати хмарний сервіс, відштовхуючись від проблем, які потрібно вирішити.

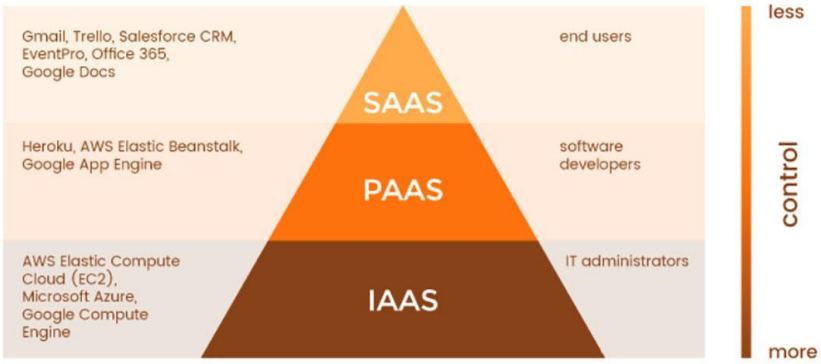

Рисунок 1.1 – Скріншот Піраміди хмарних сервісів

Враховути вартість. Одним із важливих факторів, який слід враховувати при виборі хмарного сервісу, є ціна. Обов'язково порівняйте тарифні плани різних постачальників, перш ніж приймати рішення.

Читати огляди. Ще один чудовий спосіб звузити свій вибір – прочитати відгуки інших користувачів. Це допоможе вам отримати уявлення про те, які постачальники хмарних послуг пропонують найвищу якість.

Порівняти функції. При порівнянні різних постачальників обов'язково порівняйте функції, які вони пропонують, щоб знайти найбільш підходящий для вашого бізнесу варіант. Також не бійтеся запитувати колег, перевіряти, чим

користуються конкуренти, та проводити власні міні дослідження шляхом спроб та помилок, щоб знайти безпечний та надійний сервіс.

Рівень надійності хмарних сховищ "А раптом все пропаде?" – Дуже популярний страх людей, які тільки починають отримувати свій "хмарний" досвід. Це не дивно, коли справа доходить до віртуальних сервісів, безпека завжди є головним пріоритетом. Врешті-решт ви довіряєте свої дані сторонньому постачальнику, тому вам потрібно бути впевненим, що вони в надійних руках.

Тому при виборі постачальника послуг хмари слід звертати увагу на кілька моментів [8]:

Шифрування даних: переконайтеся, що постачальник використовує стандартне шифрування трафіку за допомогою SSL-сертифіката для захисту потрібного обсягу даних.

Двофакторна аутентифікація: це додатковий рівень безпеки, який вимагає, щоб ви вводили не тільки свій пароль, але й інший код (зазвичай надсилається в текстовому повідомленні або електронною поштою), перш ніж ви зможете отримати доступ до свого облікового запису.

Надійність дата-центру: усі дані користувачів повинні зберігатися на серверах із найвищим рівнем безпеки.

Регулярне резервне копіювання: уточніть, як часто постачальник створює резервні копії даних клієнтів, щоб убезпечити себе у разі аварії.

Дотримання конфіденційності: постачальники хмарних послуг повинні гарантувати нерозголошення та захист персональних даних усім користувачам без винятку.

1.1 Основні виклики та переваги забезпечення безпеки в хмарному середовищі

Хмарні обчислення відкривають широкі можливості для зберігання та обробки даних, проте їх використання також ставить перед собою ряд викликів у сфері безпеки. Основні виклики та переваги забезпечення безпеки в хмарному середовищі включають:

Основні виклики:

1. *Конфіденційність даних:* Один з основних викликів полягає в збереженні конфіденційності даних, коли вони зберігаються та обробляються на віддалених серверах хмарних постачальників.

2. *Безпека доступу:* Забезпечення безпеки доступу до хмарних ресурсів для авторизованих користувачів є складною задачею через віддалену природу хмарних сервісів.

3. *Загрози безпеки:* Хмарні середовища піддаються різноманітним загрозам, таким як атаки злому, віруси, фішинг та інші види кібератак.

4. *Цілісність даних:* Збереження цілісності даних в хмарних середовищах вимагає ефективних методів виявлення та запобігання несанкціонованим змінам.

5. *Управління ідентифікацією:* Ефективне управління ідентифікацією та аутентифікацією користувачів є ключовим для забезпечення безпеки хмарних обчислень.

Основні переваги:

1. *Масштабованість:* Хмарні сервіси дозволяють масштабувати заходи безпеки відповідно до змінних потреб користувачів.

2. *Резервне копіювання та відновлення:* Хмарні рішення забезпечують ефективне резервне копіювання та відновлення даних, що дозволяє підвищити надійність та безпеку інформації.

3. *Автоматизація безпеки:* Використання інструментів автоматизації дозволяє підвищити ефективність заходів забезпечення безпеки в хмарних середовищах.

4. *Еластичність:* Хмарні сервіси забезпечують еластичність та доступність заходів безпеки, що дозволяє користувачам адаптувати їх до змінюваних умов.

5. *Спільне використання ресурсів:* Використання спільних ресурсів у хмарних середовищах дозволяє ефективніше реалізувати заходи безпеки через об'єднання зусиль.

Зберігання даних у хмарі – це не просто спосіб уникнути значних інвестицій у нові програмні платформи, а й забезпечення додаткового доходу за допомогою корисного функціоналу. Фірми, які використовують хмарні рішення, заощаджують кошти, продовжуючи при цьому підтримувати потреби бізнесу найбільш гнучким та ефективним способом. Це козир, який може визначити хід усієї гри на полі малого та середнього бізнесу як під час кризи. [14]

Розглянемо переваги використання хмарних послуг на приклади на прикладі RemOnline. RemOnline – це хмарна CRM-система, яка дозволяє автоматизувати робочі процеси, контролювати співробітників, фінанси та склад компанії. Для використання сервісу не потрібно завантажувати або встановлювати, що дає переваги компаніям, які його використовують.

Коли ринок пропонує власникам бізнесів коробкові та хмарні сервіси, важливо розуміти, як виправдати свій вибір у сучасних реаліях. Ми за фактами розклали те, про що вам не розкажуть користувачі локальних CRM-систем: які мінуси передбачає використання такого рішення та як хмарні послуги допоможуть економити.

Навіть якщо кількість замовлень зменшується під час кризи і здається, що інвестиції в хмарну CRM-систему можуть не окупитися, не відкладайте це рішення. Ось чому: деякі платформи надають широкий спектр можливостей, які можуть допомогти бізнесу швидше реагувати на зміни і залишатися на плаву у важкі часи. Ті, хто вже використовує таку програму, набагато легше адаптуються до кризи, ніж ті, хто цього ще не зробив.

Наприклад, програма RemOnline пропонує функції, які будуть особливо корисні для малого та середнього бізнесу в нинішніх умовах:

- Інтеграції з соцмережами, сайтами та месенджерами: дозволяють знаходити більше клієнтів і не упустити жодну заявку.
- Система обліку руху коштів: допомагає оптимізувати бюджет і скоротити непотрібні витрати.
- Аналіз великих обсягів даних: забезпечує доступ до ключових показників, що допомагає швидко реагувати на зміни і приймати важливі рішення вчасно.
- Облік клієнтів та замовлень: клієнтська база з історією візитів дозволяє ефективно спілкуватися з клієнтами, нагадувати про себе і пропонувати вигідні пропозиції на основі затребуваності послуг.

Впровадження хмарних CRM-систем дозволяє комплексно вирішувати проблеми, викликані кризою, особливо якщо ви не зупиняєте роботу свого бізнесу.

Аналіз сучасного стану забезпечення безпеки в хмарних обчисленнях дозволяє зрозуміти складність цієї проблеми та визначити оптимальні підходи до її вирішення з метою забезпечення надійності та безпеки у хмарних середовищах.

1.2 Системи забезпечення безпеки для користувачів хмарних послуг

Механізми захисту даних та конфіденційності в системах хмарних послуг включають різноманітні технології та практики, що забезпечують безпеку і конфіденційність інформації, яка зберігається та обробляється в хмарних оточеннях. Ось деякі ключові механізми захисту:

1. Шифрування даних: Це один з основних механізмів захисту даних у хмарних системах. Дані можуть бути шифровані під час передачі і під час зберігання в хмарі. Шифрування забезпечує захист інформації від несанкціонованого доступу, включаючи постачальників хмарних послуг.

Шифрування даних є одним з основних механізмів захисту інформації в хмарних системах. Цей процес використовує математичні алгоритми для перетворення звичайного тексту (даних) в нечитабельний шифрований формат, який

може бути розкодований лише за допомогою спеціального ключа. Важливими аспектами шифрування даних в хмарних сервісах є його застосування під час передачі даних через мережу та зберігання даних на серверах хмарних провайдерів.

Шифрування під час передачі даних: Під час передачі даних між користувачем і хмарним сервісом або між різними компонентами хмарної інфраструктури, важливо забезпечити конфіденційність даних. За допомогою шифрування, дані перетворюються в зашифрований вигляд перед їхнім відправленням через мережу. Це унеможливлює несанкціонованим особам або зловмисникам читати або зрозуміти перехоплені дані, оскільки вони будуть представлені у вигляді незрозумілого шифрованого тексту.

Шифрування під час зберігання даних в хмарі: Після того як дані потрапляють на сервери хмарного постачальника, вони зберігаються в зашифрованому вигляді. Це означає, що навіть персонал хмарного провайдера, який має фізичний доступ до серверів, не може прочитати або отримати доступ до розшифрованих даних без відповідного ключа шифрування. Шифрування даних на стороні сервера хмарних послуг додає додатковий шар захисту і забезпечує конфіденційність інформації навіть у разі компрометації фізичної безпеки серверів.

Типи шифрування: В хмарних системах часто використовуються різні методи шифрування, такі як симетричне шифрування (де один ключ використовується для шифрування та розшифрування даних) та асиметричне шифрування (де використовуються два ключі: публічний та приватний). Також використовується шифрування з відкритим ключем (TLS/SSL) для забезпечення безпечної передачі даних через мережу.

Узагальнюючи, шифрування даних в хмарних системах є важливим заходом забезпечення безпеки, який дозволяє захистити інформацію від несанкціонованого доступу та зберігати її конфіденційність під час передачі і зберігання.

2. Аутентифікація та авторизація: Системи хмарних послуг повинні мати механізми для ідентифікації користувачів (аутентифікація) і керування їх доступом до

ресурсів (авторизація). Сильна аутентифікація (наприклад, двофакторна аутентифікація) допомагає уникнути несанкціонованого доступу до даних.

Аутентифікація та авторизація є важливими аспектами безпеки в системах хмарних послуг. Давайте розглянемо їх детальніше:

Аутентифікація: Аутентифікація - це процес підтвердження ідентичності користувача або пристрою перед наданням доступу до системи або ресурсів. У хмарних послугах це зазвичай означає перевірку того, чи є користувач правильною особою, яка намагається отримати доступ.

Механізми аутентифікації можуть включати:

Введення пароля: Користувач повинен ввести правильний пароль для підтвердження своєї ідентичності.

Біометричні дані: Використання відбитків пальців, розпізнавання обличчя або інших біометричних параметрів для ідентифікації.

Токени: Використання токенів або ключів доступу.

Двофакторна аутентифікація (2FA): Використання двох різних методів аутентифікації, наприклад, пароля і одноразового коду, для підвищення безпеки.

Сильна аутентифікація, така як двофакторна аутентифікація, є особливо ефективним заходом, оскільки вона вимагає від користувача надання двох різних форм ідентифікації, що ускладнює спроби несанкціонованого доступу до даних.

Авторизація: Авторизація - це процес визначення прав доступу користувача після успішної аутентифікації. Це означає визначення того, які дії або ресурси може виконувати аутентифікований користувач.

Механізми авторизації включають: Установлення ролей: Визначення прав доступу на основі ролі користувача (наприклад, адміністратор, користувач, гість).

Управління дозволами: Налаштування конкретних дозволів або обмежень доступу для кожного користувача.

Політики безпеки: Визначення правил і обмежень для доступу до ресурсів на основі бізнес-правил або вимог безпеки.

Правильна авторизація дозволяє обмежити доступ користувачів тільки до необхідних ресурсів або дій, забезпечуючи відповідність з принципом найменших привілеїв (least privilege principle) і зменшуючи ризик несанкціонованого використання або витоку даних.

Заключні думки: Аутентифікація та авторизація є ключовими складовими ефективних систем безпеки в хмарних послугах. Вони дозволяють постачальникам хмарних сервісів ефективно керувати доступом до даних та ресурсів, забезпечуючи безпеку та конфіденційність інформації. Сильна аутентифікація, така як двофакторна аутентифікація, є рекомендованим заходом для запобігання несанкціонованому доступу до даних у хмарних середовищах.

3. Керування ключами: Ефективне керування ключами шифрування дозволяє забезпечити безпеку шифрованої інформації. Це включає генерацію, зберігання, обмін і видалення ключів шифрування.

Керування ключами є критично важливим аспектом забезпечення безпеки в системах шифрування, зокрема в хмарних послугах. Ефективне керування ключами дозволяє забезпечити конфіденційність і цілісність шифрованих даних. Основні етапи керування ключами включають:

1. Генерація ключів: Перший крок у керуванні ключами - це генерація ключів шифрування. Ключі є параметрами, які використовуються для шифрування і розшифрування даних. Важливо використовувати стійкі до криптоаналізу алгоритми генерації ключів для забезпечення безпеки.

2. Зберігання ключів: Безпечне зберігання ключів є критичним, оскільки втрата чи компрометація ключа може призвести до розкриття конфіденційної інформації. Ключі повинні зберігатися в захищених інфраструктурах, таких як апаратне забезпечення безпеки (HSM), облачні ключові хранилища або безпечні програмні контейнери.

3. Обмін ключами: Ключі шифрування можуть бути обмінювані між сторонами, які спілкуються, для забезпечення безпеки комунікації. Зазвичай цей процес включає

узгодження ключів за допомогою протоколів обміну ключами, таких як Diffie-Hellman.

4. Регенерація ключів: Час від часу ключі шифрування можуть бути регенеровані для забезпечення високого рівня безпеки. Регулярна зміна ключів допомагає уникнути можливих атак, заснованих на аналізі довготривалого використання одного й того ж ключа.

5. Видалення ключів: Після того як ключі вже не потрібні, їх слід безпечно видаляти або знищувати. Це запобігає можливості використання старих ключів для доступу до даних.

Керування ключами в хмарних послугах має свої виклики, оскільки ключі можуть зберігатися в розподілених середовищах. Важливо мати ефективні механізми для захисту ключів від несанкціонованого доступу та для забезпечення їх безпеки і цілісності протягом усього їхнього життєвого циклу. Такі практики забезпечують надійний захист шифрованих даних у хмарних середовищах.

4. Моніторинг та аудит безпеки: Системи хмарних послуг повинні забезпечувати механізми для моніторингу активності користувачів і обробки даних. Аудит безпеки допомагає виявляти аномальну діяльність та виявляти можливі порушення безпеки.

Моніторинг та аудит безпеки є важливими компонентами систем безпеки в хмарних послугах. Ці процеси спрямовані на постійне виявлення, відстеження і аналіз активності користувачів та обробки даних з метою виявлення потенційних загроз і порушень безпеки. Давайте розглянемо їхні ключові аспекти:

Моніторинг активності користувачів і обробки даних:

Логування подій: Системи хмарних послуг повинні реєструвати події і дії користувачів, такі як вхід в систему, доступ до ресурсів, зміни конфігурацій і т.д.

Аналіз трафіку і даних: Виявлення аномальних патернів у використанні мережі та обробці даних, що можуть свідчити про потенційні загрози або вразливості.

Спостереження за системними ресурсами: Моніторинг використання ресурсів (пам'яті, обчислювальної потужності) для виявлення аномалій, які можуть бути пов'язані зі зловживанням або атакою.

Моніторинг дозволяє оперативно реагувати на події і активності, що можуть вказувати на можливі проблеми з безпекою або атаки.

Аудит безпеки: Перевірка відповідності: Аналіз системи на відповідність внутрішнім політикам безпеки, стандартам і вимогам.

Виявлення порушень безпеки: Виявлення незвичайних або підозрілих активностей, які можуть бути пов'язані зі зловживанням або атакою.

Зберігання журналів і аналіз подій: Зберігання і аналіз журналів подій для виявлення вразливостей, атак або незвичайних дій.

Аудит безпеки допомагає виявляти потенційні порушення безпеки, аналізувати причини виникнення проблем і приймати заходи щодо їх виправлення.

Застосування моніторингу та аудиту безпеки в хмарних послугах:

У контексті хмарних послуг моніторинг та аудит безпеки можуть бути реалізовані за допомогою спеціальних сервісів або інструментів, які забезпечують збір і аналіз журналів подій, моніторинг мережі та системних ресурсів. Ці сервіси дозволяють постачальникам хмарних послуг оперативно реагувати на можливі загрози, забезпечуючи високий рівень безпеки для користувачів.

Узагальнюючи, моніторинг та аудит безпеки є важливими інструментами для забезпечення безпеки і конфіденційності в хмарних послугах. Вони дозволяють виявляти потенційні загрози і порушення, що допомагає підтримувати надійність і безпеку в хмарних середовищах.

5. Фізична безпека даних: Постачальники хмарних послуг повинні забезпечувати фізичну безпеку центрів обробки даних, включаючи контроль доступу, моніторинг і захист від природних катастроф або надзвичайних ситуацій.

Фізична безпека даних є критичним аспектом у забезпеченні безпеки і конфіденційності в хмарних послугах. Постачальники хмарних послуг повинні

вживати ряд заходів для забезпечення безпеки центрів обробки даних, щоб захистити інфраструктуру від несанкціонованого доступу, крадіжок, природних катастроф і надзвичайних ситуацій. Основні аспекти фізичної безпеки даних включають:

Контроль доступу: Фізичні бар'єри: Встановлення фізичних бар'єрів (наприклад, огорожі, стіни, двері з електронним доступом) для обмеження доступу до приміщень центру обробки даних.

Електронний доступ: Використання систем електронного контролю доступу, таких як картки доступу або біометричні сканери, для ідентифікації і автентифікації персоналу.

Моніторинг і відеоспостереження: Системи відеоспостереження: Встановлення камер відеоспостереження для моніторингу активності в об'єктах центру обробки даних.

Моніторинг в реальному часі: Постійний моніторинг в реальному часі за допомогою спеціальних систем для виявлення непередбачених подій або вторгнень.

Захист від природних катастроф і надзвичайних ситуацій:

Резервне живлення: Використання систем резервного живлення (наприклад, дизель-генераторів) для забезпечення неперервного живлення у випадку відключення електромережі.

Запобігання повеням і пожежам: Використання спеціальних заходів (наприклад, систем пожежогасіння і водовідведення) для захисту від пожеж та повеней.

Фізичний захист обладнання: Захист пристроїв і серверів: Розташування серверів і обладнання в захищених приміщеннях з контрольованим доступом.

Захист від крадіжок: Використання систем антикрадіжкового захисту для запобігання крадіжок обладнання і даних.

Політики і процедури безпеки: Стандарти безпеки: Встановлення і дотримання стандартів безпеки для фізичного захисту даних відповідно до вимог і рекомендацій.

Навчання персоналу: Проведення навчання персоналу щодо правил фізичної безпеки та процедур дії у випадку надзвичайних ситуацій.

Заключення: Фізична безпека даних у хмарних послугах є важливим фактором для забезпечення безпеки і конфіденційності інформації користувачів. Постачальники хмарних послуг повинні використовувати різноманітні технічні та організаційні заходи для захисту інфраструктури від можливих загроз і небезпек. Регулярне оновлення та вдосконалення політик та процедур фізичної безпеки є ключовими для забезпечення надійного захисту даних у хмарних середовищах.

6. Заходи проти витоку даних: Механізми, що перешкоджають ненавмисному або випадковому розголошенню конфіденційної інформації, наприклад, за допомогою контролю доступу, політик безпеки та моніторингу даних.

Заходи проти витоку даних є важливими для забезпечення конфіденційності інформації та запобігання ненавмисному або випадковому розголошенню конфіденційної інформації. Давайте розглянемо деякі з найефективніших механізмів:

Контроль доступу: Рольова модель доступу: Встановлення прав доступу на основі ролей користувачів, що обмежує доступ до конфіденційної інформації тільки до тих, хто має необхідні повноваження.

Обмеження доступу до потрібних даних: Персонал отримує доступ лише до тієї інформації, яка є необхідною для виконання їхніх робочих обов'язків.

Політики безпеки: Класифікація даних: Визначення рівня конфіденційності для кожного типу даних і встановлення відповідних заходів захисту.

Шифрування даних: Застосування шифрування для захисту даних під час передачі та зберігання.

Моніторинг даних: Системи виявлення вторгнень (IDS): Використання систем, які виявляють аномальну або підозрілу активність, яка може свідчити про спроби витоку даних.

Аналіз активності користувачів: Відстеження та аналіз активності користувачів для виявлення незвичайної або підозрілої поведінки.

Освіта персоналу: Навчання з безпеки: Проведення навчання для персоналу щодо правил обробки та захисту конфіденційної інформації.

Усвідомлення ризиків: Залучення персоналу до усвідомлення потенційних ризиків витоку даних та методів їх запобігання.

Захист зовнішнього доступу:

Фірмові мережеві межі (Firewalls): Використання фірмових мережевих меж для контролю та фільтрації вхідного та вихідного мережевого трафіку.

Використання віртуальних приватних мереж (VPN): Забезпечення безпечного зовнішнього з'єднання до корпоративної мережі через зашифрований тунель.

Планування відновлення після інциденту:

Резервне копіювання даних: Проведення регулярного резервного копіювання даних для швидкого відновлення після можливого витоку даних.

Планування відновлення: Розроблення плану відновлення після інциденту для ефективного відновлення нормального функціонування після виявлення витоку даних.

Загальний підхід до заходів проти витоку даних полягає в комбінації технічних, організаційних і процедурних заходів, які спрямовані на запобігання, виявлення та відновлення після можливих витоків даних.

Ці механізми допомагають забезпечити високий рівень безпеки і захисту конфіденційної інформації в хмарних системах, дозволяючи користувачам використовувати хмарні послуги з впевненістю в їх безпеці.

Аутентифікація, авторизація та керування доступом є ключовими компонентами систем забезпечення безпеки в хмарних послугах. Вони спрямовані на перевірку і керування правами доступу користувачів до ресурсів і даних. Ось їхні основні аспекти:

1. Аутентифікація:

- Чому служить: Аутентифікація визначає, чи є користувач правильною особою, яка намагається отримати доступ до системи або ресурсів.

- Механізми: Включає різні методи перевірки ідентичності, такі як паролі, біометричні дані (відбитки пальців, розпізнавання обличчя), токени або двофакторна аутентифікація (2FA).
- Ціль: Забезпечення впевненості у тому, що особа, яка намагається отримати доступ, є та, за кого вона себе видає.

2. Авторизація:

- Чому служить: Авторизація визначає, які дії або ресурси може виконати аутентифікований користувач після успішного входу.
- Механізми: Встановлення прав доступу на основі ідентифікованої особи, наприклад, визначення ролей або набору дозволів для кожного користувача.
- Ціль: Обмеження доступу користувачів та забезпечення відповідності принципу найменших привілеїв (least privilege principle).

3. Керування доступом:

- Чому служить: Керування доступом визначає, які ресурси або функції системи можуть бути доступні користувачам під час роботи з системою.
- Механізми: Включає управління рівнями доступу, аудит доступу, управління політиками безпеки, розгортання механізмів двофакторної аутентифікації тощо.
- Ціль: Забезпечення контролю за тим, хто, коли і яким чином отримує доступ до ресурсів, і запобігання несанкціонованому доступу.

Ролі в системах хмарних послуг: У системах хмарних послуг ці механізми дозволяють постачальникам хмарних сервісів ефективно керувати безпекою і надавати користувачам тільки необхідний рівень доступу до ресурсів. Це допомагає уникнути витоку даних, забезпечити конфіденційність і цілісність інформації, а також забезпечити відповідність з правовими вимогами щодо захисту даних.

Ці механізми є основою для забезпечення безпеки в хмарних послугах і допомагають створити надійні та захищені середовища для обробки та зберігання даних користувачів.

1.3 Порівняльний аналіз засобів забезпечення безпеки в хмарних системах

Порівняльний аналіз засобів забезпечення безпеки в хмарних системах дозволяє визначити найефективніші методи і технології для захисту даних та забезпечення конфіденційності. Розглянемо основні засоби забезпечення безпеки в хмарних системах і порівняємо їх за ключовими характеристиками.

У таблиці 2.1 наводитися порівняння функціоналу, розглянутого в цьому розділі, систем управління. З таблиці видно, що найбільш універсальною та повнофункціональною - безкоштовна система CloudStack

Таблиця 2.1 - Порівняння можливостей систем управління інфраструктурами

Можливості	Cloudstack	Eucalyptus	Openstack	vCloud Director
Інтеграція з AD	+	-	-	+
Консоль управління	+	Тільки в платній версії	+	+
Веб доступ до консолі віртуальних машин	+	Тільки для KVM	+	+
API	+	+	+	+
Multi–role	+	+	+	+
Можливості	Cloudstack	Eucalyptus	Openstack	vCloud Director
VLAN	+	+	+	+
Гіпервізори	KVM, XEN, ESXi, OVM, BareMetal	KVM, XEN, ESXi(Тільки для комп. версії)	KVM, XEN	ESXi
Простий процес	+	-	-	+

створення шаблонів				
Снепшот	+	+	+	+
Тривоги і повідомлення	+	-	-	+
Обсяги (Volumes)	+	+	+	+
Підтримка гостьових ОС	Як у гіпервізора	linux	Як у гіпервізора	Як у гіпервізора
Live migration	+	-	-	+
Безкоштовність	+	+/-	+	-
Сумісність з Amazon API	+	+	+	-
Rightscale	+	+	+	+
High Availability components	+	+	-	+
Складність впровадження	-	+	+	-

1. Шифрування даних

- Використання: Шифрування даних під час передачі та зберігання.
- Переваги: Забезпечує високий рівень захисту від несанкціонованого доступу.
- Недоліки: Може вимагати значних обчислювальних ресурсів; управління ключами може бути складним завданням.
- Приклади: AES (Advanced Encryption Standard), TLS (Transport Layer Security).

2. Аутентифікація

- Використання: Перевірка ідентичності користувачів перед наданням доступу до ресурсів.
- Переваги: Захист від несанкціонованого доступу за допомогою сильних методів аутентифікації (наприклад, двофакторна аутентифікація).
- Недоліки: Складність у налаштуванні та підтримці, можливі проблеми з користувацьким досвідом.
- Приклади: Паролі, двофакторна аутентифікація (2FA), біометричні дані.

3. Авторизація

- Використання: Визначення прав доступу аутентифікованих користувачів.
- Переваги: Гнучкість у налаштуванні прав доступу на основі ролей та політик.
- Недоліки: Потребує ретельного налаштування та підтримки; ризик помилок у налаштуваннях.
- Приклади: Рольове управління доступом (RBAC), атрибутивне управління доступом (ABAC).

4. Керування ключами

- Використання: Управління життєвим циклом ключів шифрування (генерація, зберігання, обмін, видалення).
- Переваги: Забезпечує надійне управління ключами, що є критичним для безпеки шифрованих даних.
- Недоліки: Може бути складним і дорогим у реалізації; потребує високого рівня довіри до постачальника.
- Приклади: AWS Key Management Service (KMS), Google Cloud Key Management.

5. Моніторинг та аудит безпеки

- Використання: Відстеження та аналіз активності користувачів і системних подій для виявлення аномалій і загроз.

- Переваги: Допомагає виявляти порушення безпеки та реагувати на них у реальному часі.
- Недоліки: Може генерувати велику кількість даних, що потребує аналізу; можливість пропущення загроз.
- Приклади: Splunk, Azure Security Center, AWS CloudTrail.

6. Фізична безпека даних

- Використання: Забезпечення фізичної безпеки центрів обробки даних.
- Переваги: Захист від фізичних загроз, таких як крадіжка обладнання, природні катастрофи.
- Недоліки: Вимагає значних інвестицій у інфраструктуру; складність управління.
- Приклади: Контроль доступу, системи відеоспостереження, резервне живлення.

7. Заходи проти витоку даних

- Використання: Механізми запобігання ненавмисному або випадковому розголошенню конфіденційної інформації.
- Переваги: Захист від внутрішніх загроз та помилок користувачів.
- Недоліки: Може вимагати значних зусиль для впровадження та підтримки; ризик помилок у налаштуваннях.
- Приклади: Data Loss Prevention (DLP) системи, політики контролю доступу.

Порівняння за основними критеріями:

1. Рівень захисту: Шифрування та сильна аутентифікація забезпечують високий рівень захисту.
2. Впровадження: Фізична безпека та керування ключами вимагають значних ресурсів для впровадження.
3. Гнучкість: Авторизація та моніторинг дозволяють налаштувати детальні політики безпеки та реагувати на загрози.

4. Вартість: Висока вартість фізичної безпеки та розгортання систем моніторингу й аудиту.

5. Користувацький досвід: Складність використання сильних аутентифікаційних методів може впливати на зручність користувачів.

Кожен з описаних методів має свої переваги і недоліки, і їхнє використання залежить від конкретних вимог і можливостей організації. Для забезпечення оптимальної безпеки в хмарних системах необхідно комбінувати різні методи, забезпечуючи комплексний підхід до захисту даних та інфраструктури.

Огляд методів виявлення та реагування на загрози в хмарному середовищі

Виявлення та реагування на загрози в хмарному середовищі є критичними для підтримки безпеки та цілісності даних. Розглянемо основні методи, які використовуються для виявлення загроз і реагування на них у хмарних середовищах:

Методи виявлення загроз

1. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS):

- Функції: IDS аналізують мережевий трафік та журнали подій для виявлення підозрілої активності. IPS не тільки виявляють, але й запобігають виявленим загрозам.
- Переваги: Висока ефективність у виявленні відомих загроз і патернів атак.
- Недоліки: Можуть давати хибні спрацьовування; потребують регулярного оновлення сигнатур.

2. Моніторинг мережевого трафіку:

- Функції: Аналіз мережевого трафіку для виявлення аномалій, які можуть свідчити про загрози.
- Переваги: Може виявляти нові та невідомі загрози через аналіз поведінки.
- Недоліки: Великий обсяг даних для аналізу може вимагати значних ресурсів.

3. Системи управління інформацією та подіями безпеки (SIEM):

- Функції: Збирають, аналізують і корелюють дані з різних джерел для виявлення загроз.
- Переваги: Централізоване управління та аналіз даних безпеки; здатність виявляти комплексні атаки.
- Недоліки: Висока вартість та складність налаштування і підтримки.

4. Машинне навчання та штучний інтелект (AI):

- Функції: Використання алгоритмів машинного навчання для аналізу великих обсягів даних та виявлення аномальної поведінки.
- Переваги: Можливість виявлення нових, невідомих загроз; адаптивність.
- Недоліки: Потребує якісних даних для навчання; можливість хибних позитивних або негативних результатів.

Методи реагування на загрози

1. Автоматичне реагування:

- Функції: Виконання автоматизованих дій у відповідь на виявлені загрози (наприклад, блокування IP-адреси, ізоляція системи).
- Переваги: Швидке реагування на загрози, мінімізація впливу інциденту.
- Недоліки: Можливість помилкових спрацьовувань; потреба у ретельній настройці.

2. Ручне реагування:

- Функції: Аналіз та реагування на загрози вручну безпековими аналітиками.
- Переваги: Гнучкість і можливість більш детального аналізу.
- Недоліки: Більший час реагування; потребує наявності кваліфікованих спеціалістів.

3. Оркестрація та автоматизація процесів безпеки (SOAR):

- Функції: Автоматизація процесів реагування на інциденти з використанням сценаріїв та інтеграція з іншими інструментами безпеки.

- Переваги: Підвищення ефективності процесів реагування; зменшення часу реагування.
- Недоліки: Складність у налаштуванні та інтеграції; потребує належного управління сценаріями.

4. Резервне копіювання та відновлення:

- Функції: Регулярне створення резервних копій даних та систем для швидкого відновлення після інциденту.
- Переваги: Забезпечення безперервності бізнесу; можливість відновлення після атак типу ransomware.
- Недоліки: Потребує управління та захисту резервних копій.

Ефективне виявлення та реагування на загрози в хмарних середовищах вимагає використання комбінованих методів і технологій. Інтеграція IDS/IPS, SIEM, машинного навчання та AI з автоматизацією процесів безпеки (SOAR) дозволяє забезпечити комплексний підхід до безпеки. Важливо також мати план резервного копіювання та відновлення для забезпечення безперервності бізнесу у випадку серйозних інцидентів. Регулярне оновлення та налаштування цих систем є критично важливим для підтримки їхньої ефективності у виявленні та реагуванні на нові загрози.

Порівняння можливостей систем управління інфрастуктурами

У таблиці 2.1 наводитися порівняння функціоналу, розглянутого в цьому розділі, систем управління. З таблиці видно, що найбільш універсальною та повнофункціональною - безкоштовна система CloudStack.

Таблиця 2.1 - Порівняння можливостей систем управління інфраструктурами

Можливості	Cloudstack	Eucalyptus	Openstack	vCloud Director
Інтеграція з AD	+	-	-	+
Консоль управління	+	Тільки в платній версії	+	+

Веб доступ до консолі віртуальних машин	+	Тільки для KVM	+	+
API	+	+	+	+
Multi–role	+	+	+	+
Можливості	Cloudstack	Eucalyptus	Openstack	vCloud Director
VLAN	+	+	+	+
Гіпервізори	KVM, XEN, ESXi, OVM, BareMetal	KVM, XEN, ESXi(Тільки для комп. версії)	KVM, XEN	ESXi
Простий процес створення шаблонів	+	-	-	+
Снепшот	+	+	+	+
Тривоги і повідомлення	+	-	-	+
Обсяги (Volumes)	+	+	+	+
Підтримка гостьових ОС	Як у гіпервізора	linux	Як у гіпервізора	Як у гіпервізора
Live migration	+	-	-	+
Безкоштовність	+	+/-	+	-
Сумісність з Amazon API	+	+	+	-
Rightscale	+	+	+	+

High Availability components	+	+	-	+
Складність впровадження	-	+	+	-

Щоб правильно вибрати набір послуг, пропонованих IaaS-провайдерами, важливо чітко розуміти потреби вашого підприємства щодо цілей, потужностей і обсягу ресурсів. Крім цього, необхідно ознайомитися з функціональними можливостями та умовами, на яких різні компанії надають ці послуги.

Для даного порівняння ми зосередимося на провайдерах IaaS, послуги яких можна придбати онлайн без укладення контракту.

Amazon Elastic Compute Cloud (Amazon EC2) – веб-сервіс, що забезпечує безпечну та змінну обчислювальну потужність у хмарі, створений для спрощення хмарних обчислень для розробників. Прості інтерфейси веб-служби Amazon EC2 дозволяють отримувати та налаштовувати потужність з мінімальними труднощами. Amazon EC2 надає повний контроль над обчислювальними ресурсами і дозволяє працювати в надійному середовищі Amazon.

З Amazon EC2 можна:

- створювати Amazon Machine Image (AMI), який містить ваші програми, бібліотеки, дані і конфігураційні параметри, або використовувати готові шаблони;
- завантажувати AMI в Amazon S3, який забезпечує безпечне та надійне сховище;
- використовувати веб-сервіс Amazon EC2 для налаштування безпеки і мережевого доступу;
- вибирати типи операційних систем, запускати, завершувати або контролювати кілька AMI за допомогою API або різних інструментів управління;

- працювати в декількох місцях, використовувати статичний IP або інші опції;
- платити тільки за ресурси, які використовуються, наприклад, за час або передачу даних.

Bit Refinery – корпоративний постачальник хмарних обчислень, що пропонує як державні, так і приватні хмари для компаній різного розміру. Заснована у 1996 році в Денвері, компанія співпрацює з такими бізнесами, як Digital Fortress, Cloudera та Fortrust. Bit Refinery має центри обробки даних по всій США та в Англії, і забезпечує виділені приватні мережеві шляхи до своєї хмари.

Bit Refinery пропонує послугу Disaster-Recovery-as-a-Service (DRaaS), що допомагає бізнесу захищати виробничі додатки з мінімальними витратами за допомогою Zerto Virtual Replication. Це рішення забезпечує реальновимірну хмарну відновлюваність, роблячи хмарний DR більш доступним і простим для численних організацій. Зовсім недавно Bluelock також запустив аналогічне рішення на основі Zerto Virtual Replication, роблячи хмарний DR ще більш життєздатним.

Оскільки технологія Zerto є програмною і апаратно-агностичною, компанії можуть використовувати DR-as-a-Service від Bit Refinery для реплікації даних з будь-якого типу сховища на будь-який інший тип сховища. Наразі Bit Refinery пропонує чотири варіанти реплікації хмарних даних:

- Реплікація Zerto у реальному часі;
- Реплікація VMware™ SRM (диспетчер відновлення сайтів);
- Реплікація Veeam;
- Хмарне зберігання.

Крім реплікації даних, нова послуга DR захищає від логічних помилок і забезпечує відновлення програм шляхом частого тестування на відмову.

Go Daddy – приватна американська компанія, що надає послуги хостингу та реєстрації доменних імен для малого бізнесу та приватних осіб. Вона є найбільшим у

світі реєстратором доменних імен, підтримуючи близько 30 мільйонів доменних імен у найбільших доменних зонах першого рівня, таких як .com, .org, .net, .biz, .info.

GoGrid – хмарна інфраструктура для обслуговування і хостингу віртуальних машин на базі Linux і Windows. Управління здійснюється за допомогою декількох серверів через панель управління і RESTful API. GoGrid дозволяє компаніям швидко, надійно і безпечно працювати з декількома віртуальними машинами, забезпечуючи економічно ефективне хмарне сховище. Маючи понад десятирічний досвід у керованих хмарних сховищах і виділеному хостингу, GoGrid надає рішення для управління та інтеграції з відкритими, комерційними і фірмовими технологіями. З понад 15 000 клієнтів і більше 600 000 розгорнутих віртуальних машин, GoGrid є основою хмарної інфраструктури для компаній, таких як Condé Nast, Merkle і Preventice.

Hosting.com – компанія, що працює з 1997 року, пропонує рішення для гібридного хостингу, хмарного хостингу, виділеного хостингу, керованого хостингу, аварійного відновлення та підтримки бізнесу для глобальної клієнтури. Штаб-квартира знаходиться в Денвері, штат Колорадо, з центрами обробки даних в Ірваїні, Каліфорнія; Луїсвіллі, Кентуккі; Ньюарку, Нью-Джерсі; та Сан-Франциско, Каліфорнія.

Мета компанії полягає в забезпеченні рішень для клієнтів "Always On". Вона веде моніторинг, управління та оптимізацію веб-платформ компаній Web 2.0 та постачальників програмного забезпечення як послуг (IaaS).

Послуги компанії Hosting.com поділяються на чотири категорії:

- Послуги платформи (хмарний, виділений, колокаційний та гібридний хостинг).
- Керовані служби (зберігання та захист даних, мережа, моніторинг, виправлення та безпека).
- Прикладні послуги (реєстрація доменів, хостинг Microsoft Exchange, Microsoft SharePoint 2010 та SmarterTools).

- Професійні послуги (міграція та розумні руки).

NephoScale розробив хмарне розповсюдження програмного забезпечення на базі NephOS OpenStack. NephOS - це єдине рішення на базі OpenStack, яке працює з багатьма постачальниками послуг під ключ. Для створення хмар за допомогою NephOS не потрібні експерти з OpenStack. Завдяки технології автоматизації "Brewer" від NephoScale один адміністратор системних лінійних систем може встановлювати, модернізувати, масштабувати та керувати загальнодоступними, приватними та гібридними хмарами.

ReliaCloud FLEX - це IT-хмарна інфраструктура корпоративного класу як платформа сервісу (IaaS). З ReliaCloud FLEX ви отримуєте приватне обчислювальне середовище на високонадійній та гнучкій інфраструктурі, ціноутворення, яке масштабується передбачуваним чином із кроком в 1 ГБ на основі щомісячного використання, високодоступну архітектуру та інше.

Softlayer - набір послуг хмарних обчислень для бізнесу, пропонованих компанією IBM. Він поєднує платформу як послугу (PaaS) з інфраструктурою як послугу (IaaS) та глобально розміщений у центрах обробки даних по всьому світу.

Компанія Terremark Worldwide планує розширити свої центри обробки даних, що може сприяти збільшенню її присутності на ринку хмарних послуг.

Для порівняння хмарних сервісів для різних систем господарства потрібно визначити критерії, які охоплювали б ключові аспекти хмарних обчислень, такі як зменшення витрат та економія на масштабуванні, рівень сервісу, гнучкість конфігурації серверів та аспекти безпеки, надійності та підтримки. У результаті було виокремлено 15 критеріїв:

1. План оплати: Різноманітність опцій оплати, зокрема плата за фактичне використання, членські знижки та їх комбінації.

2. Середньомісячна ціна: Орієнтовна вартість хмарного сервера на місяць, стандартизована для порівняння між різними провайдерами.

3. Угода про рівень сервісу (SLA): Процентна гарантія доступності сервісу, незалежно від попередньої продуктивності.

4. Кількість датацентрів: Кількість датацентрів, які підтримують хмарні сервери.

5. Сертифікації: Наявність сертифікатів безпеки і надійності, таких як PCI або SAS 70.

6. Вертикальне масштабування: Можливість збільшення ресурсів сервера (пам'ять, CPU, сховище).

7. Горизонтальне масштабування: Швидкість розгортання нових серверів.

8. Підтримка користувачів: Рівень доступної та безкоштовної підтримки.

9. Моніторинг: Наявність і якість інструментів моніторингу та оповіщення.

10. API: Наявність API для взаємодії з серверами.

11. Безкоштовний тарифний план: Можливість використання безкоштовної пробної версії для тестування.

12. Підтримувані операційні системи: Кількість підтримуваних ОС та їх версій.

13. Різноманітність типів серверів: Кількість різних конфігурацій серверів, включаючи можливість налаштування.

14. Вартість вихідного та вхідного трафіку: Вартість передачі даних в інтернет, як вихідних, так і вхідних.

Використовуючи ці критерії, можна провести аналіз та порівняти різних провайдерів хмарних послуг.

2 СТАН ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ В ХМАРНИХ ОБЧИСЛЕННЯХ

2.1 Вимоги до засобів захисту програм та даних у хмарних сервісах

Засоби захисту програм і даних у хмарних сервісах повинні відповідати численним вимогам для забезпечення належного рівня безпеки, конфіденційності та цілісності інформації. Основні вимоги включають:

1. Аутентифікація та авторизація

- Сильна аутентифікація: Включає багатофакторну аутентифікацію (MFA), біометричну аутентифікацію та використання одноразових паролів (OTP).
- Рольове управління доступом (RBAC): Надання доступу на основі ролей користувачів з мінімальними необхідними привілеями.
- Атрибутивне управління доступом (ABAC): Динамічне управління доступом на основі атрибутів користувача, середовища та інших факторів.

2. Шифрування

- Шифрування даних під час передачі: Використання протоколів SSL/TLS для захисту даних під час їх пересилання між користувачем і хмарним сервісом.
- Шифрування даних на зберіганні: Захист даних у стані спокою за допомогою алгоритмів шифрування, таких як AES.
- Керування ключами шифрування: Ефективне управління життєвим циклом ключів, включаючи їх генерацію, зберігання та ротацію.

3. Безпека мережі

- Мережеві межі та фаєрволи: Використання фаєрволів для захисту від несанкціонованого доступу та контролю трафіку між різними сегментами мережі.
- Сегментація мережі: Розділення мережі на окремі сегменти для обмеження поширення атак.

- Віртуальні приватні мережі (VPN): Забезпечення безпечного доступу до хмарних ресурсів через зашифровані канали.

4. Моніторинг і аудит

- Моніторинг у реальному часі: Відстеження активності користувачів та системних подій для виявлення аномалій та підозрілої поведінки.
- Журнали та аудит: Ведення детальних журналів подій та аудит безпеки для аналізу та виявлення потенційних загроз.
- Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS): Виявлення та запобігання загрозам у реальному часі.

5. Захист від витоку даних

- Системи запобігання втратам даних (DLP): Використання технологій для захисту конфіденційної інформації та запобігання її несанкціонованому поширенню.
- Класифікація та маркування даних: Визначення рівнів конфіденційності даних та відповідні заходи захисту.
- Політики контролю доступу: Встановлення та дотримання політик доступу для різних категорій даних.

6. Захист від шкідливого ПЗ

- Антивірусне та антишпигунське програмне забезпечення: Використання програм для виявлення та видалення шкідливих програм.
- Сканування на уразливості: Регулярне сканування системи на предмет уразливостей та їх усунення.
- Захист кінцевих точок (EDR): Моніторинг і захист кінцевих точок від шкідливих дій.

7. Фізична безпека

- Контроль доступу до центрів обробки даних: Забезпечення фізичного захисту серверів та інфраструктури через системи контролю доступу, відеоспостереження та охорону.

- Захист від природних катастроф: Забезпечення стійкості до природних катастроф через використання резервних систем живлення, пожежогасіння та інших заходів.

8. Відновлення після інцидентів

- Резервне копіювання та відновлення: Регулярне резервне копіювання даних та тестування процедур відновлення.
- Планування неперервності бізнесу (BCP): Розробка та впровадження планів для забезпечення неперервності бізнесу у випадку інцидентів.
- Планування відновлення після аварій (DRP): Створення планів відновлення для швидкого відновлення нормальної роботи після серйозних інцидентів.

9. Відповідність регуляторним вимогам

- Дотримання стандартів та нормативів: Виконання вимог таких стандартів, як GDPR, HIPAA, ISO/IEC 27001, SOC 2 та інших.
- Проведення регулярних аудитів: Регулярні перевірки та аудити для забезпечення відповідності встановленим стандартам та нормативам.

Вимоги до засобів захисту програм та даних у хмарних сервісах включають широкий спектр заходів, спрямованих на забезпечення всебічного захисту інформації та інфраструктури. Від ефективної аутентифікації та шифрування до постійного моніторингу та планування відновлення, кожен з цих елементів є критичним для підтримання безпеки у хмарному середовищі.

2.2 Роль інтеграції технологій безпеки в розгортанні хмарних рішень

Інтеграція технологій безпеки відіграє ключову роль у розгортанні хмарних рішень, забезпечуючи захист даних, додатків і інфраструктури від численних загроз. Розглянемо основні аспекти і переваги інтеграції технологій безпеки в хмарні рішення.

1. Комплексний захист даних

- Шифрування даних: Інтеграція технологій шифрування забезпечує конфіденційність і цілісність даних під час їх передачі та зберігання. Це дозволяє захистити дані від несанкціонованого доступу, навіть якщо зловмисники отримають фізичний доступ до носіїв інформації.
- Управління ключами: Інтеграція систем управління ключами дозволяє ефективно генерувати, зберігати та управляти криптографічними ключами, що підвищує безпеку шифрованих даних.

2. Покращення управління доступом

- Аутентифікація та авторизація: Інтеграція багатофакторної аутентифікації (MFA) та рольового управління доступом (RBAC) дозволяє значно підвищити рівень безпеки, запобігаючи несанкціонованому доступу до хмарних ресурсів.
- Single Sign-On (SSO): Інтеграція SSO технологій спрощує процес входу для користувачів, підвищуючи зручність та безпеку, оскільки користувачі мають один набір облікових даних для доступу до різних хмарних додатків і сервісів.

3. Моніторинг і реагування на загрози

- Системи управління інформацією та подіями безпеки (SIEM): Інтеграція SIEM систем дозволяє збирати, аналізувати та корелювати дані з різних джерел у режимі реального часу, що забезпечує оперативне виявлення загроз і реагування на них.
- Моніторинг мережевого трафіку: Інтеграція рішень для моніторингу мережевого трафіку допомагає виявляти аномалії та підозрілу активність, забезпечуючи своєчасне виявлення потенційних загроз.

4. Автоматизація процесів безпеки

- Оркестрація та автоматизація (SOAR): Інтеграція SOAR рішень дозволяє автоматизувати процеси реагування на інциденти, що підвищує швидкість і ефективність реагування, зменшуючи вплив інцидентів на бізнес.

- Автоматичне виправлення вразливостей: Інтеграція автоматизованих систем виправлення вразливостей допомагає швидко виправляти знайдені вразливості, зменшуючи ризик експлуатації.

5. Відповідність нормативним вимогам

- Стандарти та нормативи: Інтеграція технологій безпеки допомагає забезпечити відповідність нормативним вимогам і стандартам, таким як GDPR, HIPAA, ISO/IEC 27001. Це не тільки підвищує безпеку, але й дозволяє уникнути штрафів та санкцій за недотримання вимог.
- Аудити та звітність: Інтеграція інструментів для автоматичного ведення журналів подій та створення звітів полегшує проведення аудитів та надання звітності регуляторам.

6. Покращення безпеки додатків

- Захист від шкідливого ПЗ: Інтеграція антивірусного програмного забезпечення та рішень для захисту кінцевих точок (EDR) забезпечує захист від шкідливих програм та кібератак.
- Контроль версій та патчів: Інтеграція систем для автоматичного оновлення програмного забезпечення та управління патчами допомагає забезпечити актуальність додатків і зменшити ризики експлуатації вразливостей.

7. Підвищення стійкості до атак

- Резервне копіювання та відновлення: Інтеграція систем резервного копіювання та відновлення даних забезпечує збереження даних і можливість швидкого відновлення після інцидентів, таких як атаки типу ransomware.
- Планування неперервності бізнесу (BCP) та відновлення після аварій (DRP): Інтеграція рішень для планування неперервності бізнесу та відновлення після аварій допомагає забезпечити безперервність операцій навіть у разі серйозних інцидентів.

Інтеграція технологій безпеки в розгортанні хмарних рішень є важливим аспектом забезпечення надійності та безпеки хмарних сервісів. Вона дозволяє

комплексно захистити дані, додатки та інфраструктуру від численних загроз, підвищити ефективність управління безпекою, забезпечити відповідність нормативним вимогам та зменшити ризики для бізнесу. Комплексний підхід до інтеграції безпеки включає використання різних технологій та рішень, що працюють разом для забезпечення всебічного захисту хмарних середовищ.

Автоматизація та моніторинг заходів безпеки є ключовими компонентами забезпечення надійного захисту хмарних середовищ. Ці процеси допомагають не тільки виявляти загрози в режимі реального часу, але й автоматично реагувати на них, що значно підвищує рівень безпеки. Розглянемо детальніше роль автоматизації та моніторингу в контексті хмарних обчислень.

Автоматизація безпеки включає використання технологій та інструментів, які виконують рутинні завдання без втручання людини. Це дозволяє зменшити ризики, пов’язані з людським фактором, і забезпечити більш швидке реагування на інциденти.

1. Автоматичне виявлення загроз

- Машинне навчання та штучний інтелект (AI): Використання алгоритмів машинного навчання для аналізу великих обсягів даних з метою виявлення аномалій та підозрілої активності. AI може швидко адаптуватися до нових загроз і виявляти патерни, які важко розпізнати вручну.
- Системи управління інформацією та подіями безпеки (SIEM): Збирають, корелюють та аналізують дані з різних джерел, включаючи журнали подій, мережевий трафік та поведінку користувачів. SIEM дозволяє автоматично виявляти загрози та відправляти сповіщення у разі виявлення аномалій.

2. Автоматичне реагування на інциденти

- Оркестрація та автоматизація процесів безпеки (SOAR): Інтеграція SOAR систем дозволяє автоматизувати реагування на інциденти, включаючи блокування підозрілої активності, ізоляцію уражених систем та повідомлення відповідальних осіб. Це значно зменшує час реагування та мінімізує вплив інцидентів.

- Автоматичне виправлення вразливостей: Використання інструментів для автоматичного виявлення та виправлення вразливостей у програмному забезпеченні та інфраструктурі. Це включає застосування патчів та оновлень без втручання людини.

Моніторинг безпеки передбачає постійне відстеження стану хмарного середовища для виявлення та аналізу потенційних загроз. Ефективний моніторинг дозволяє оперативно реагувати на інциденти та забезпечувати безперервний захист.

1. Моніторинг у реальному часі

- Мережевий моніторинг: Відстеження мережевого трафіку для виявлення аномальної активності та потенційних загроз. Це включає аналіз вхідного та вихідного трафіку, а також виявлення підозрілих з'єднань.
- Моніторинг активності користувачів: Відстеження дій користувачів для виявлення підозрілої поведінки, такої як несанкціоновані спроби доступу або незвичні дії з даними.

2. Журнали та аудит

- Збирання журналів подій: Автоматизований збір та зберігання журналів подій з різних систем і додатків. Це включає журнали входу, дії з даними, зміни конфігурацій тощо.
- Аудит безпеки: Регулярний аналіз журналів подій для виявлення аномалій, слідів можливих атак та інших загроз. Аудит допомагає виявити слабкі місця в системі безпеки та підготувати рекомендації для їх усунення.

3. Аналіз загроз та вразливостей

- Сканування на вразливості: Регулярне сканування хмарного середовища на предмет відомих вразливостей. Це дозволяє виявити та усунути потенційні загрози до їх експлуатації зловмисниками.
- Тестування на проникнення (Penetration Testing): Проведення контрольованих атак на систему з метою виявлення вразливостей та оцінки ефективності заходів безпеки.

Інтеграція автоматизації та моніторингу заходів безпеки є невід’ємною частиною сучасного підходу до забезпечення безпеки в хмарних середовищах. Автоматизація дозволяє значно підвищити швидкість реагування на інциденти, знизити навантаження на команди безпеки та забезпечити безперервний захист даних та інфраструктури. Моніторинг забезпечує постійний контроль за станом безпеки, виявлення потенційних загроз та їх оперативне усунення. Разом ці підходи створюють надійну систему захисту, що адаптується до сучасних викликів та загроз у хмарному середовищі.

3 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ТА ВИСНОВКИ

3.1 Сучасні стратегії та підходи до захисту в хмарних обчисленнях

Сучасні стратегії та підходи до захисту в хмарних обчисленнях включають різноманітні методи та технології, що дозволяють забезпечити високий рівень безпеки та відповідність нормативним вимогам. Нижче наведені ключові стратегії, які можуть бути застосовані для ефективного захисту хмарних середовищ.

1. Стратегія "Zero Trust" (Нульова довіра)

- Мінімізація довіри: У цій стратегії передбачається, що жоден користувач або пристрій не повинен автоматично вважатися надійним, навіть якщо вони знаходяться всередині корпоративної мережі. Кожен доступ має бути перевірений.
- Постійна верифікація: Регулярна перевірка і підтвердження ідентичності користувачів та пристроїв при кожному запиті на доступ до ресурсів.
- Мікросегментація: Розбиття мережі на менші сегменти з метою зменшення ризику поширення атак.

Наведем приклад моделі «Zero Trust»

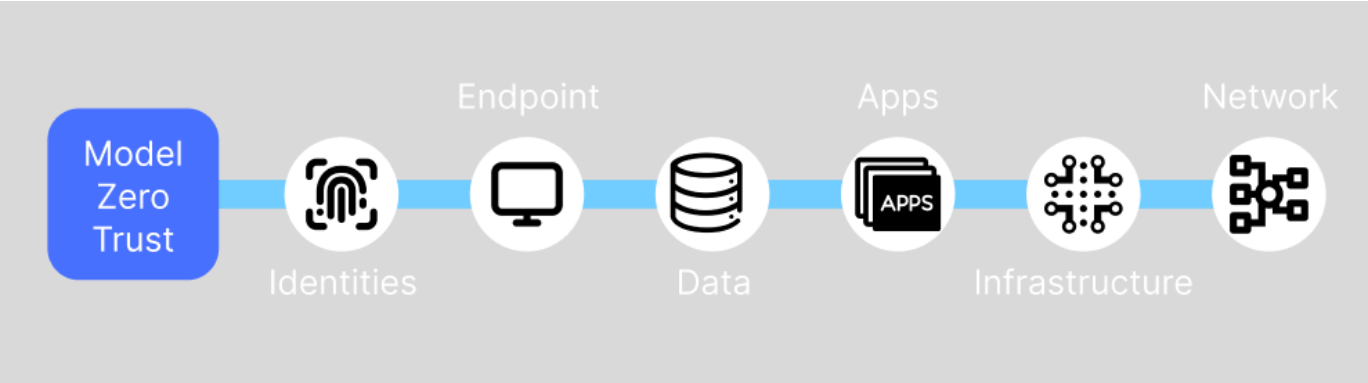

Рисунок. 3.1. - Скріншот моделі «Zero Trust»

2. Використання багатофакторної аутентифікації (MFA)

- Додаткові рівні безпеки: MFA додає додаткові рівні аутентифікації, що значно ускладнює завдання зловмисникам отримати несанкціонований доступ.

- Захист облікових записів: Використання MFA для захисту облікових записів адміністраторів та користувачів з високими привілеями.

3. Шифрування даних

- Шифрування під час передачі: Використання SSL/TLS для забезпечення безпеки даних під час їх пересилання між клієнтами та серверами.
- Шифрування на зберіганні: Застосування алгоритмів шифрування для захисту даних, що зберігаються у хмарі.
- Керування ключами: Використання надійних систем управління ключами для забезпечення цілісності та конфіденційності шифрованих даних.

4. Контейнеризація та оркестрація

- Контейнери: Використання контейнерних технологій для ізоляції додатків та забезпечення безпеки їхнього виконання.
- Ортестрація: Застосування оркестраційних платформ (наприклад, Kubernetes) для автоматичного управління контейнерними додатками та їх безпекою.

5. Моніторинг та реагування на інциденти

- Системи SIEM: Використання систем управління інформацією та подіями безпеки (SIEM) для збору, кореляції та аналізу даних з різних джерел у режимі реального часу.
- Моніторинг мережі: Постійний моніторинг мережевого трафіку для виявлення аномалій та потенційних загроз.
- Автоматизація реагування: Використання SOAR-платформ для автоматизації процесів реагування на інциденти, що зменшує час реагування та мінімізує вплив інцидентів на бізнес.

6. Політики безпеки та відповідність нормативним вимогам

- Політики контролю доступу: Встановлення та дотримання чітких політик доступу для різних категорій користувачів та даних.
- Відповідність стандартам: Забезпечення відповідності нормативним вимогам та стандартам безпеки, таким як GDPR, HIPAA, ISO/IEC 27001.

- Регулярні аудити: Проведення регулярних аудитів безпеки для виявлення слабких місць та перевірки відповідності вимогам.

7. Навчання та підвищення обізнаності

- Тренінги для співробітників: Регулярне проведення тренінгів з безпеки для співробітників, щоб підвищити їхню обізнаність про загрози та найкращі практики безпеки.
- Симуляції атак: Проведення симуляцій фішингових атак та інших видів кібератак для підготовки співробітників до реальних загроз.

8. Планування неперервності бізнесу та відновлення після аварій

- Резервне копіювання даних: Регулярне резервне копіювання важливих даних та тестування процедур відновлення.
- BCP та DRP: Розробка та впровадження планів неперервності бізнесу (BCP) та відновлення після аварій (DRP), що забезпечують швидке відновлення операцій у разі інцидентів.

Сучасні стратегії та підходи до захисту в хмарних обчисленнях включають комбінацію технологічних рішень, політик та процедур, що забезпечують всебічний захист даних та інфраструктури. Інтеграція цих стратегій дозволяє ефективно протидіяти сучасним кіберзагрозам та забезпечувати безперервність бізнес-процесів у хмарному середовищі.

3.2 Практичні поради забезпечення безпеки для користувачів та розробників хмарних додатків

Безпека хмарних додатків є спільною відповідальністю постачальників послуг, розробників та користувачів. Нижче наведені практичні поради для обох груп щодо забезпечення безпеки в хмарному середовищі.

Ціноутворення відрізняється серед провайдерів хмарних послуг, поділяючись на два основних підходи: плата за фактичне використання та щомісячна оплата.

Плата за фактичне використання застосовується до таких провайдерів, як Amazon EC2, GoGrid, NephoScale, OpSource, Rackspace, Softlayer і Terremark. З іншого боку, щомісячна оплата використовується в BitRefinery, GoDaddy, Hosting.com, GoGrid, OpSource, ReliaCloud і Softlayer.

На підставі цих результатів можна зробити логічний висновок, що для великих компаній з високими потребами найбільш доцільно розглядати варіанти щомісячної оплати.

Середня ціна за місяць. Орієнтовна вартість в доларах за хмарий сервер з 1 CPU, 2GB RAM (і хороші аналоги), усереднена для датацентрів і серверів Windows / Linux. При доступної інформації погодинна оплата розраховувалася на основі 730 годинного місяця. Інакше використовувалася місячна ціна, виключаючи ціни за передачу трафіку.

На рисунку 3.1 можна побачити результати експерименту.

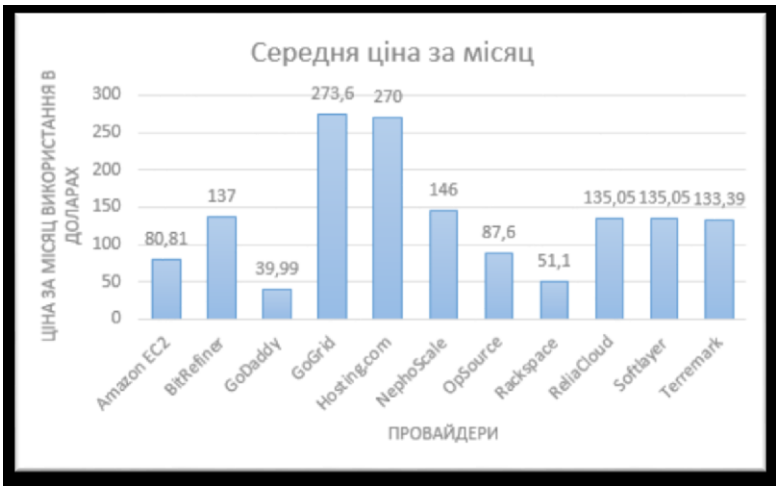

Рисунок 3.2 – Порівняння цін за послуги провайдерів

На основі отриманих результатів можна виділити двох найбільш дорогих провайдера – це GoGrid та Hosting.com, а також двох найбільш дешевих – GoDaddy та Rackspace.

SLA або угоди по рівню сервісу. В даному критерії порівняння майже всі провайдери показали сто відсотковий показник, окрім Softlayer дані яких, не було знайдено.

Кількість дата центрів. На рисунку 3.3 можна побачити діаграму порівняння кількості дата центрів.

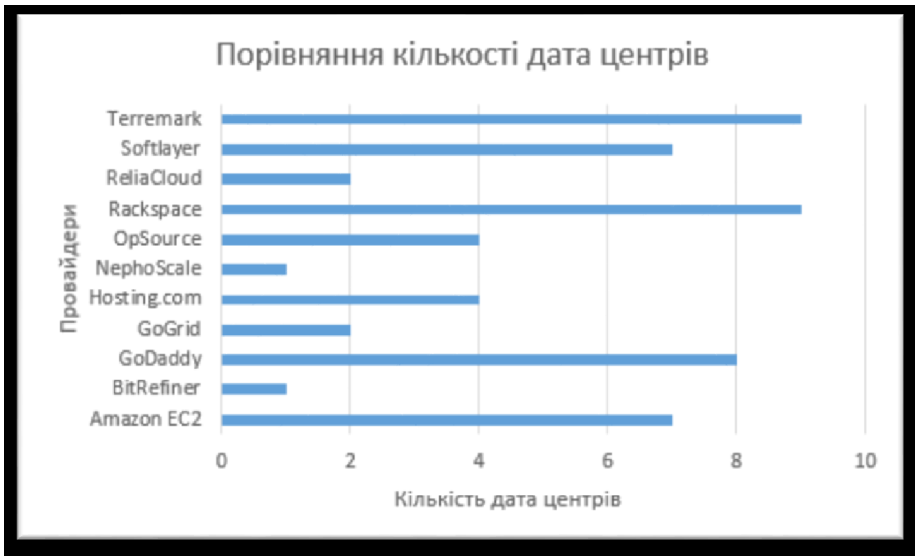

Рисунок 3.3 – Порівняння кількості дата центрів

З аналізу діаграми видно, що Terremark і Rackspace виділяються серед інших провайдерів за кількістю датацентрів.

Щодо сертифікації, позитивний відгук ставився у випадку, якщо у провайдера були сертифікати безпеки і надійності, такі як PCI або SAS 70. Проте серед представлених компаній відсутні відповідні сертифікати у GoDaddy, GoGrid і NephoScale.

Вертикальне масштабування випробувалося шляхом аналізу можливості додавання більшої кількості пам'яті, процесорних ресурсів та збільшення обсягу сховища. Загальні висновки показали, що провайдери такі як BitRefinery, GoGrid, Hosting.com, NephoScale, OpSource, Rackspace та Terremark підтримують можливості вертикального масштабування.

Щодо горизонтального масштабування, експеримент показав, що швидке розгортання нових серверів підтримується провайдерами, такими як Amazon EC2, BitRefinery, GoDaddy, GoGrid, Hosting.com, NephoScale, OpSource, Rackspace, ReliaCloud, Softlayer, Terremark.

Оцінка сервісної підтримки проводилась з використанням суб'єктивної шкали, де "Poor" означає низьку якість, "Average" - середню, "Extensive" - високу. Найкращу професійну експертну підтримку надали провайдери BitRefinery, GoDaddy, Hosting.com, OpSource та Rackspace. Середню якість обслуговування продемонстрували NephoScale та ReliaCloud. Найнижчу оцінку у цій категорії отримали Amazon EC2, Softlayer та Terremark.

У випробуванні моніторингу компанії були оцінені за допомогою суб'єктивної шкали, де "Poor" вказує на низьку якість, "Average" - середню, "Extensive" - високу. Оцінку "Poor" отримали провайдери BitRefinery, GoDaddy, GoGrid, NephoScale, ReliaCloud, Terremark. Оцінку "Average" отримали Hosting.com та OpSource. Оцінку "Extensive" отримали Amazon EC2, OpSource та Softlayer.

Наявність API. Наявність можливості взаємодії с серверами важлива складова порівняння провайдерів. Експеримент проводився завдяки суб’єктивній шкалі оцінювання де: None – зовсім немає, Average – компанії з дуже простим набором можливостей внутрішньої API, Extensive – компанії з повноцінним безкоштовним API.

Провайдери Amazon EC2, NephoScale, OpSource, Rackspace, Extensiv показали оцінку «Extensive». Провайдери GoGrid, ReliaCloud, Terremark показали оцінку «Average». Провайдери BitRefinery, GoDaddy, Hosting.com взагалі не мають можливості взаємодії с сервером за допомогою API.

Безкоштовна версія. Експеримент проводився на наявність у провайдера безкоштовної версії для тестування роботи з сервісом. Єдиним провайдером який забезпечую користувачів безкоштовною версією виявився Amazon EC2.

Кількість доступних ОС. Експеримент проводився на кількість підтримуваних операційних систем не залежно від версій. На рисунку 3.4 можна побачити кількість ОС доступних у різних провайдерів.

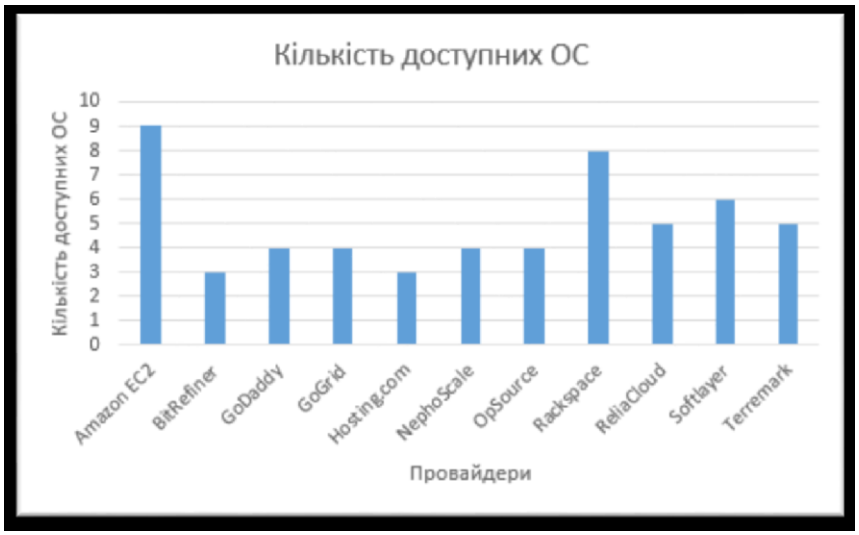

Рисунок 3.4 – Результат експерименту на кількість доступних ОС

На основі графіка можна зробити висновок, що найбільшу кількість операційних систем підтримують провайдери Amazon EC2 і Rackspace.

Кількість доступних конфігурацій серверів досліджувалась у експерименті. Деякі провайдери пропонують повністю налаштовувані сервери, які в таблиці 3.1 позначені як "configurable".

Вартість вихідного трафіку визначалась у доларах за кожен гігабайт. Компанії, що надають безкоштовний вихідний трафік, мають значення ціни рівне 0.

На рисунку 3.4 представлена діаграма вартості одного гігабайту вихідного трафіку.

Таблиця 3.1 - Кількість конфігурованих серверів

Провайдери	Кількість конфігурованих серверів
Amazon EC2	12
BitRefiner	configurable
GoDaddy	5
GoGrid	1
Hosting.com	configurable
NephoScale	6

OpSource	configurable
Rackspace	8
ReliaCloud	5
Softlayer	13
Terremark	configurable

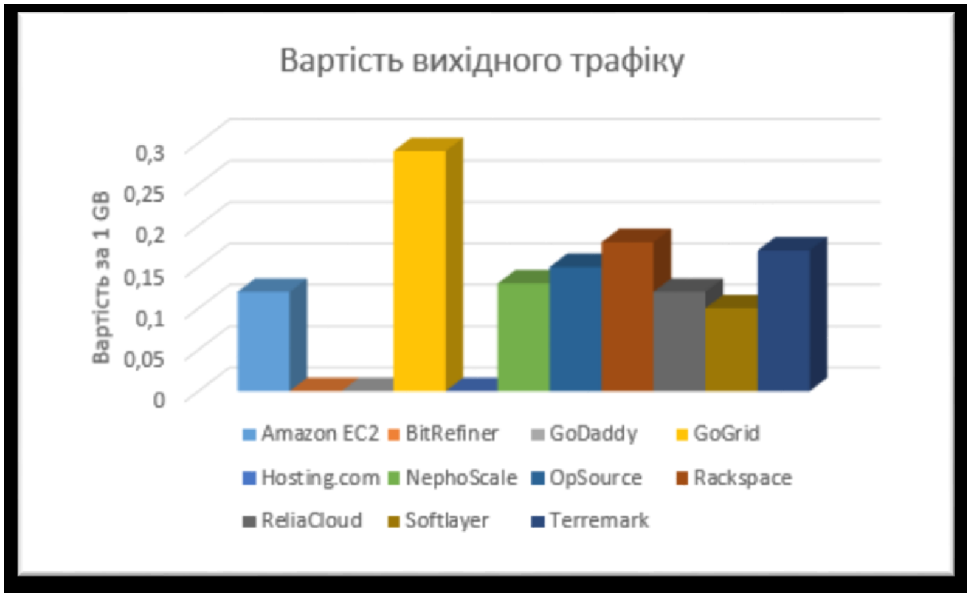

Рисунок 3.5 – Вартість вихідного трафіку

З аналізу діаграми видно, що провайдер GoGrid має найвищу ціну на вихідний трафік, а провайдери BitRefinery, GoDaddy і Hosting.com не встановлюють ціну на вихідний трафік.

Щодо вартості вхідного трафіку, експеримент визначав ціну за кожен гігабайт в доларах. Компанії, що пропонують безкоштовний вхідний трафік, мають значення ціни рівне 0. На діаграмі у розділі 3.6 можна побачити ціни за один гігабайт вхідного трафіку.

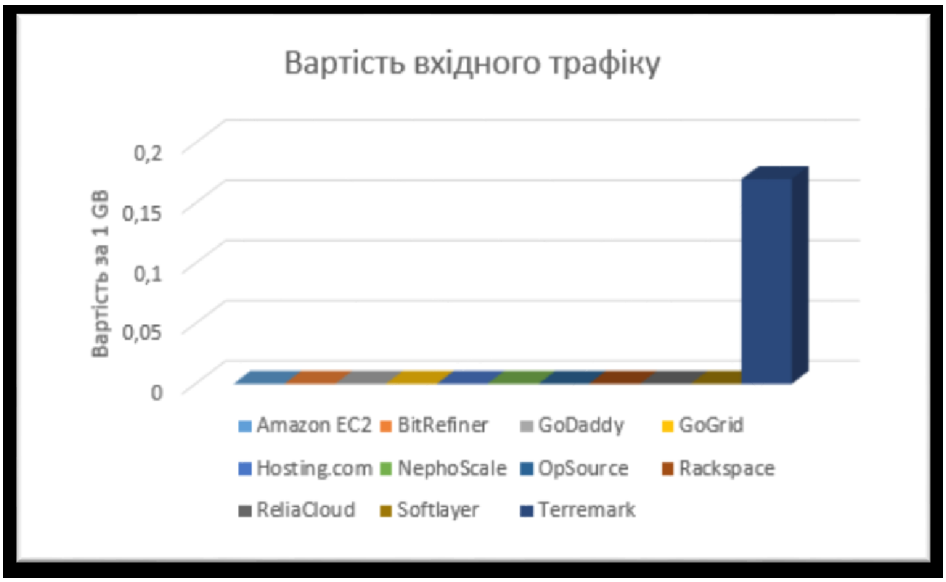

Рисунок 3.6 – Вартість вхідного трафіку

На підставі діаграми можна зробити висновок, що провайдер Terremark єдиний з провайдерів який бере плату за вхідний трафік.

Розглянемо більш докладно сервіси найвідомішого провайдера хмарних технологій - Amazon.

Amazon Web Services (AWS) пропонує можливість створення різноманітної розподіленої мережевої інфраструктури, використовуючи свої сервіси. Крім того, Amazon пропонує безкоштовний перший рік використання сервісу, за умови, що не будуть перевищені ліміти, встановлені для безкоштовного використання (в іншому випадку застосовується звичайний тариф). Це дозволяє випробувати хмарний хостинг безкоштовно. AWS особливо зручний, коли потрібно розгортати багато однакових екземплярів об'єктів. Безкоштовний пакет AWS Free Usage Tier включає в себе:

– EC2 (екземпляри об’єктів - віртуальні машини ОС)

– 750 годин використання віртуальної машини з Linux або Windows Server (613 Мб ОЗУ, 32 бітна або 64-бітна платформа) – достатня кількість годин для роботи екземплярів об’єктів щомісяця

– 750 годин Elastic Load Balancer плюс 15 Гб обробки трафіку

– 30 Гб Amazon Elastic Block Storage, плюс 2 мільйони операцій введення / виводу і 1 Гб для зберігання снепшотів.

–15 Гб трафіку S3 (файлове сховище)

– 5 Гб Amazon S3 стандартного сховища, 20000 Get запитів і 2000 Put запитів

Relational Database Service (служба реляційних баз даних, RDS)

– 750 годин сервісу для запуску MySQL, Oracle BYOL або SQL Server

– 20 Гб сховище бази даних

–10 мільйонів операцій введення / виводу

– 20 Гб сховище для автоматичного резервного копіювання вашої бази даних і можливістю створити снепшоти бази даних.

На Amazon існує калькулятор, який допомагає розрахувати витрати на надані послуги. Є три типи тарифів: "on-demand", "spot" та "reserved". "On-demand" - це звичайний VPS на основі віртуалізації Xen. "Spot" - це схоже на "on-demand", але без гарантії такого ж високого часу безвідмовної роботи. "Spot" працює, доки ціна, яку ви запропонували, вища за середню ціну за той самий екземпляр об'єкта. "Reserved" - це знижка при тривалому користуванні "on-demand" екземплярами об'єктів, яку можна придбати. Іншими словами, якщо ви довгий час використовуєте "on-demand" екземпляри об'єктів за 23 долари, то для переходу на тариф "reserved" і сплати 12 доларів щомісяця, вам потрібно одноразово заплатити 50 доларів.

Крім того, варто зазначити глобальну інфраструктуру Amazon, зокрема, велику кількість дата-центрів у різних частинах світу. Це означає, що ви можете отримати непогану швидкість і пінг практично з будь-якої точки світу.

Для користувачів хмарних додатків

1. Використовуйте сильні та унікальні паролі

- Використовуйте довгі паролі, що містять комбінацію великих і малих літер, цифр та спеціальних символів.
- Уникайте використання однакових паролів для різних облікових записів.

2. Активуйте багатофакторну аутентифікацію (MFA)

- Впроваджуйте MFA для всіх облікових записів, що забезпечує додатковий рівень захисту навіть у випадку компрометації пароля.

3. Регулярно оновлюйте програмне забезпечення

- Завжди встановлюйте останні оновлення та патчі для додатків та операційних систем, щоб захистити себе від відомих вразливостей.

4. Навчайтеся розпізнавати фішинг атаки

- Будьте обережні з підозрілими електронними листами та повідомленнями. Ніколи не відкривайте посилання або вкладення з неперевірених джерел.

5. Використовуйте антивірусне програмне забезпечення

- Встановіть і регулярно оновлюйте антивірусне ПЗ, щоб захистити свої пристрої від шкідливих програм.

6. Забезпечте резервне копіювання даних

- Регулярно створюйте резервні копії важливих даних і зберігайте їх у безпечному місці. Використовуйте хмарні сервіси резервного копіювання з шифруванням даних.

Для розробників хмарних додатків

1. Впроваджуйте безпечні методи кодування

- Використовуйте перевірені бібліотеки та фреймворки.
- Дотримуйтеся принципів безпечного кодування, таких як валідація вхідних даних, уникнення SQL-ін'єкцій та захист від міжсайтових скриптів (XSS).

2. Використовуйте DevSecOps підхід

- Інтегруйте безпеку у всі етапи життєвого циклу розробки програмного забезпечення, включаючи планування, розробку, тестування та розгортання.
- Автоматизуйте сканування на вразливості та тестування безпеки.

3. Забезпечуйте шифрування даних

- Шифруйте дані як під час передачі (використовуйте TLS), так і під час зберігання.

- Використовуйте надійні алгоритми шифрування та управління ключами.

4. Захищайте API

- Впроваджуйте аутентифікацію та авторизацію для всіх API.
- Обмежуйте доступ до API, використовуючи принцип найменших привілеїв.

5. Проводьте регулярні аудити та тестування на проникнення

- Регулярно проводьте незалежні аудити безпеки та тестування на проникнення, щоб виявити та усунути вразливості.

6. Використовуйте інструменти для моніторингу безпеки

- Впроваджуйте системи моніторингу для виявлення аномальної активності та швидкого реагування на інциденти.

7. Розробляйте плани реагування на інциденти

- Розробіть та тестуйте плани реагування на інциденти, щоб забезпечити швидке та ефективне реагування на можливі загрози.

8. Забезпечуйте навчання та обізнаність

- Проводьте регулярні тренінги для команди розробників щодо найкращих практик безпеки та сучасних загроз.
- Створюйте культуру безпеки у своїй організації.

Безпека хмарних додатків вимагає всебічного підходу, що включає як технологічні рішення, так і навчання користувачів та розробників. Дотримання вищезазначених порад допоможе значно знизити ризики та підвищити рівень захисту хмарних обчислень.

3.3 Практичне використання навичок шифрування та розшифрування у хмарних обчисленнях.

Встановлення бібліотеки cryptography:

```
pip install cryptography
```

Імпорт необхідних модулів

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.primitives import padding
from cryptography.hazmat.backends import default_backend
import os
```

Функції для шифрування та розшифрування даних:

```
def generate_key():
    # Генерація випадкового ключа
    return os.urandom(32)

def encrypt_data(data, key):
    # Ініціалізаційний вектор для режиму CBC
    iv = os.urandom(16)
    cipher = Cipher(algorithms.AES(key), modes.CBC(iv), backend=default_backend())
    encryptor = cipher.encryptor()

    # Паддінг даних до блочного розміру AES
    padder = padding.PKCS7(algorithms.AES.block_size).padder()
    padded_data = padder.update(data) + padder.finalize()

    # Шифрування даних
    encrypted_data = encryptor.update(padded_data) + encryptor.finalize()
    return iv + encrypted_data  # Повертаємо iv разом з зашифрованими даними
```

```
    def decrypt_data(encrypted_data, key):
        # Відділення ініціалізаційного вектора
        iv = encrypted_data[:16]
        encrypted_data = encrypted_data[16:]
        cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
        decryptor = cipher.decryptor()

        # Розшифрування даних
        padded_data = decryptor.update(encrypted_data) +
decryptor.finalize()

        # Вилучення паддінгу
        unpadder =
padding.PKCS7(algorithms.AES.block_size).unpadder()
        data = unpadder.update(padded_data) +
unpadder.finalize()
        return data
```

Приклад використання функцій шифрування та розшифрування:

```
    if __name__ == "__main__":
        # Дані для шифрування
        data = b"Це приклад конфіденційних даних, які потрібно
захистити."

        # Генерація ключа
        key = generate_key()
```

```
        # Шифрування даних
        encrypted_data = encrypt_data(data, key)
        print(f"Зашифровані дані: {encrypted_data}")

        # Розшифрування даних
        decrypted_data = decrypt_data(encrypted_data, key)
        print(f"Розшифровані                                    дані:
{decrypted_data.decode('utf-8')}")
```

generate_key(): Генерує випадковий ключ довжиною 32 байти для використання в AES-шифруванні.

encrypt_data(data, key): Шифрує дані з використанням алгоритму AES в режимі CBC. Дані попередньо доповнюються (padding) до потрібного розміру.

decrypt_data(encrypted_data, key): Розшифровує дані, відділяє ініціалізаційний вектор, знімає паддінг і повертає початкові дані.

if name == "main": Демонструє приклад використання функцій шифрування та розшифрування.

Реальне використання цього методу може бути:

Захист конфіденційних даних: Використовується для шифрування чутливих даних перед їх збереженням або передачею у хмару.

Безпека хмарних сервісів: Забезпечує, що дані залишаються захищеними навіть у випадку несанкціонованого доступу до сховища.

Використання криптографії для захисту даних є важливим аспектом безпеки в хмарних обчисленнях. Цей приклад показує, як можна використовувати бібліотеку cryptography для шифрування та розшифрування даних, забезпечуючи їх конфіденційність і захист від несанкціонованого доступу.

ВИСНОВКИ

У цьому дослідженні ми розглянули різні аспекти забезпечення безпеки в хмарних обчисленнях, включаючи механізми захисту даних, аутентифікацію та авторизацію, керування ключами, моніторинг та аудит безпеки, фізичну безпеку даних, а також заходи проти витоку даних. Крім того, ми провели порівняльний аналіз засобів забезпечення безпеки в хмарних системах, ознайомилися з вимогами до засобів захисту програм та даних у хмарних сервісах, і дослідили роль інтеграції технологій безпеки в розгортанні хмарних рішень. Нарешті, ми запропонували практичні рекомендації для користувачів і розробників хмарних додатків.

Основні висновки:

1. Механізми захисту даних та конфіденційності є ключовими елементами безпеки в хмарних обчисленнях. Шифрування даних під час їх передачі та зберігання забезпечує захист від несанкціонованого доступу.

2. Аутентифікація та авторизація грають критичну роль у забезпеченні безпеки доступу до хмарних ресурсів. Використання сильних методів аутентифікації, таких як двофакторна аутентифікація, допомагає уникнути несанкціонованого доступу.

3. Керування ключами шифрування є важливим аспектом захисту даних. Ефективне керування ключами включає генерацію, зберігання, обмін і видалення ключів.

4. Моніторинг та аудит безпеки допомагають виявляти аномальну активність і можливі порушення безпеки. Системи моніторингу та аналізу безпеки, такі як SIEM, є необхідними для забезпечення безперервного контролю.

5. Фізична безпека даних в центрах обробки даних хмарних провайдерів є фундаментальною для захисту від фізичних загроз, таких як несанкціонований доступ або природні катастрофи.

6. Заходи проти витоку даних повинні включати контроль доступу, політики безпеки та моніторинг, щоб запобігти ненавмисному або випадковому розголошенню конфіденційної інформації.

7. Сучасні стратегії та підходи до захисту в хмарних обчисленнях включають стратегію "Zero Trust", багатофакторну аутентифікацію, шифрування даних, контейнеризацію, моніторинг та автоматизацію заходів безпеки, а також відповідність нормативним вимогам.

8. Практичні поради для користувачів хмарних додатків включають використання сильних паролів, активацію MFA, регулярне оновлення ПЗ, розпізнавання фішинг-атак, використання антивірусного ПЗ та резервне копіювання даних.

9. Практичні поради для розробників хмарних додатків включають безпечні методи кодування, інтеграцію безпеки в процес розробки (DevSecOps), шифрування даних, захист API, регулярні аудити та тестування, використання інструментів для моніторингу безпеки, планування реагування на інциденти та навчання команди безпеки.

Забезпечення безпеки в хмарних обчисленнях є багатогранним завданням, що вимагає злагодженого підходу з боку постачальників послуг, розробників та кінцевих користувачів. Використання сучасних технологій, дотримання найкращих практик безпеки та постійне навчання всіх учасників процесу є критичними для створення безпечного хмарного середовища. Виконання рекомендацій, наведених у цьому дослідженні, допоможе мінімізувати ризики та забезпечити надійний захист даних та додатків у хмарі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A.E. Kononyuk, Fundamental theory of cloudy technologies : Scientific approaches of forming of the systems of cloudy technologies. Kiev, Ukraine: Osvita Ukrayini, b 1, 2018/

2. K.O. Volska, ta A.P. Dikiy, "Record-keeping in a "cloud": order of transition and adaptation of the informative system of enterprise ", Problemi teoriyi ta metodologiyi buhgalterskogo obliku, kontrolyu i analizu, ZhDTU, №2(37), pp. 24-29,. 2017. DOI: 10.26642/pbo-2017-2(37)-24-29. (In Ukrainian).

3. Наказ «Про затвердження Правил пожежної безпеки в Україні». 2020. URL: http://surl.li/uebxi

4. Cloud computing. URL: http://surl.li/uebxl

5. The NIST Definition of Cloud Computing. URL: http://surl.li/uebxn. Accessed on: January 26, 2020. (in English).

2. Fernando Doglio, "Content as a Service: Your Guide to the What, Why, and How" ButterCMS, May 7, 2019.

3. Mike Roberts, " Serverless Architectures", May 22, 2018. URL: http://surl.li/uebxq

4. Antony Ananich, "What is IaaS?", Mar 2, 2016. URL: http://surl.li/uebxx

5. Donovan Jones, "Blackstone Acquires Cloudreach For Access To iPaaS Market", February 21, 2017. URL: http://surl.li/uebxz

6. Zachary Flower, "Weigh the benefits of PaaS providers against lock-in risks", May 29, 2018. URL: http://surl.li/uebyg

7. Alibaba Cloud EHPC Empowers New Manufacturing – SAIC Simulation Computing Cloud (SSCC), September 13, 2018. URL: http://surl.li/uebyi

8. ANSYS. URL: http://znaimo.com.ua/ANSYS

9. Хмарні обчислення проти розподілених обчислень: сучасні перспективи / Ю.О. Бабій, В.П. Нездоровін, Є.Г. Махрова, Л.П. Луцкова. Вісник Хмельницького національного університету. Сер.: Технічні науки. 2011. № 6. С. 80-85.

10. Яковицький І.Л. Технологія «хмарних обчислень» як інструмент створення інформаційної інфраструктури управління. Комунальне господарство міст. Сер.: Економічні науки. 2012. Випуск 102. С. 320-327.

11. Youssef Bassil - "Steganography: 3 Black Magic Magic of Science: TheSecret Art of Deception".

12. Jessica Fridrich ”Steganography в Digital Media: Principles, Algorithms, and Applications”.

13. Tang W., Li B., Tan S., Barni M., Huang J. CNN Based Adversarial Embedding with Minimum Alteration for Image Steganography. 2018. URL: https://arxiv.org/abs/1803.09043

14. Nerds rejoice: Google just released its internal tool to collaborate on AI. Quartz. URL: http://surl.li/uebyk

15. Open in Colab GitHub repository. GitHub. URL: https://github.com/googlecolab/open_in_colab

16. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. 1998. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98

17. Державної стратегії регіонального розвитку на 2021-2027 роки. URL: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text

18. CRM-система для сфери послуг. URL: https://remonline.ua/features/crm