Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Засоби та механізми захисту інформації в хмарних середовищах

Виконавець: студент IV курсу, групи КБ-42

Владислав ВАСИЛЕНКО
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Яніна ШЕСТАК	

Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студента **КБ-42** **Владислава Юрійовича ВАСИЛЕНКА**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби та механізми захисту інформації в хмарних середовищах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ
Хмарні середовища, Salesforse, засоби захисту інформації в хмарних середовищах.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ
Дослідження типів хмарних середовищ, проведення аналізу типів хмарних середовищ, визначення існуючих засобів захисту інформації та їх порівняльний аналіз, розробка рекомендацій для захисту інформації в хмарному середовищі Salesforse

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність полягає визначенні найкращих методів за засобів захисту інформації.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав ВАСИЛЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Ознайомлення з видами хмарних технологій	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз існуючих аспектів в захисті безпеки в хмарному середовищі	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження існуючих засобів захисту інформації в хмарному середовищі	22.03.2023 – 08.04.2023	*виконано*
7	Розробити рекомендації для підвищення рівня захисту інформації в хмарному середовищі Salesforce.	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав ВАСИЛЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Засоби та механізми захисту інформації в хмарних середовищах» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 78 сторінки. Робота містить 10 рисунків. Список використаних джерел включає 15 джерел.

Метою роботи є розробка рекомендації щодо покращення захисту інформації в хмарному середовищі Salesforce.

Об'єкт дослідження засоби захисту інформації в хмарних середовищах для безпеки користувачів.

Предметом дослідження методи та засоби захисту інформації в хмарному середовищі.

Практична цінність роботи полягає визначенні найкращих методів за засобів захисту інформації. Оскільки дані та додатки зберігаються та обробляються на серверах, що належать хмарному провайдеру, необхідно вживати заходів для захисту конфіденційності, цілісності та доступності інформації. Ця робота повинна зробити внесок у постійні зусилля, спрямовані на підвищення безпеки в хмарному середовищі.

Ключові слова: хмарні середовища, захист даних, шифрування даних

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

CRM	-	Customer Relationship Management
ПЗ	-	Програмне забезпечення
IDPS	-	Intrusion Detection and Prevention Systems
DoS	-	Disk Operating System
IDS	-	Intrusion Detection System
VPCs	-	Virtual Private Clouds
IPS	-	Image Packaging System
EC2	-	Elastic Compute Cloud
IoT	-	Internet-of-Things
AD	-	Active Directory
IT	-	Information Technology
EBS	-	Elastic Block Store
TLS	-	Transport Layer Security
VPN	-	Virtual Private Network
SSL	-	Secure Sockets Layer
PaaS	-	Platform as a service

ЗМІСТ

ВСТУП

Безпека в хмарному середовищі є важливою темою і є предметом особливої уваги для хмарних постачальників та користувачів. Ось деякі аспекти безпеки в хмарному середовищі:

Фізична безпека: Хмарні постачальники мають вживати заходів для забезпечення фізичної безпеки своїх дата-центрів. Це може включати контроль доступу, відеоспостереження, пожежну безпеку та захист від природних лих.

Фізична безпека в хмарному середовищі відіграє важливу роль у захисті даних та забезпеченні безперебійної роботи хмарної інфраструктури. Ось деякі аспекти фізичної безпеки в хмарному середовищі:

Дата-центри: Хмарні постачальники зазвичай мають власні дата-центри, де розміщуються фізичні сервери та обладнання. Ці дата-центри повинні бути фізично захищені, з контролем доступу, відеоспостереженням та системами виявлення вторгнень.

Контроль доступу: Дата-центри повинні мати системи контролю доступу, такі як картки доступу, біометричні системи, системи розпізнавання обличчя тощо. Це дозволяє обмежувати доступ до фізичних приміщень тільки авторизованим працівникам.

Резервне живлення: Дата-центри повинні мати резервне живлення для забезпечення безперебійної роботи хмарної інфраструктури навіть в разі відмови електромережі. Це можуть бути генератори або безперебійні джерела живлення.

Контроль температури та вологості: В дата-центрах необхідно підтримувати оптимальні умови температури та вологості, щоб запобігти пошкодженню обладнання. Це досягається за допомогою систем кондиціонування повітря та вентиляції.

Пожежна безпека: Дата-центри повинні бути оснащені системами пожежної безпеки, включаючи детектори диму, пожежні тривоги та автоматичні системи гасіння пожежі. Важливо проводити регулярні перевірки та тести систем пожежної безпеки.

Конфіденційність даних

Конфіденційність даних є одним із найважливіших аспектів безпеки в хмарному середовищі.

Публічні хмарні постачальники зазвичай використовують механізми шифрування для захисту конфіденційності даних. Важливо використовувати сильне шифрування під час передачі та зберігання даних в хмарі. Ось деякі заходи, які зазвичай вживаються для забезпечення конфіденційності даних в хмарі

Шифрування: Шифрування даних вважається одним з найефективніших методів захисту конфіденційності. Хмарні постачальники можуть застосовувати шифрування для захисту даних під час їх передачі і зберігання. Зазвичай використовується шифрування на рівні даних, де дані шифруються перед тим, як вони залишають контроль користувача, і розшифровуються лише після того, як вони повертаються користувачеві.

Управління ключами: Управління ключами шифрування є важливим аспектом забезпечення конфіденційності даних в хмарному середовищі. Це означає безпечне зберігання та управління шифрувальними ключами, які використовуються для шифрування та розшифрування даних. Ключі повинні бути добре захищені від несанкціонованого доступу.

Розсіяне сховище даних: Деякі хмарні постачальники використовують розсіяне сховище даних, де дані розсіюються на різних фізичних серверах та місцях. Це допомагає ускладнити доступ до даних несанкціонованим особам, оскільки вони зберігаються у фрагментах на різних місцях.

Ідентифікація та автентифікація: Хмарні постачальники надають механізми ідентифікації та автентифікації, такі як багатофакторна автентифікація (MFA) та управління доступом, для забезпечення тільки авторизованого доступу до хмарних ресурсів.

Захист від зломів: Хмарні постачальники повинні вживати заходів для захисту від зломів, таких як виявлення та запобігання вторгнень (Intrusion Detection and Prevention Systems), системи моніторингу та аналізу журналів подій.

РОЗДІЛ 1. ПОНЯТТЯ ПРО БЕЗПЕКУ В ХМАРНОМУ СЕРЕДОВИЩІ

1.1 Визначення безпеки в хмарному середовищі

Безпека в хмарному середовищі є важливим аспектом, оскільки користувачі довіряють постачальникам хмарних послуг зберігання та обробку своїх даних. Визначення безпеки в хмарному середовищі включає ряд заходів та політик, спрямованих на захист даних, забезпечення конфіденційності, цілісності та доступності інформації, а також запобігання несанкціонованому доступу до ресурсів хмари.

Основні аспекти безпеки в хмарному середовищі включають:

Фізична безпека

Фізична безпека в хмарному середовищі відноситься до заходів, спрямованих на захист фізичної інфраструктури дата-центру або серверних приміщень, де розташовані хмарні ресурси. Основна мета - забезпечити фізичний доступ тільки авторизованим особам і запобігти несанкціонованому доступу до обладнання та даних.

Нижче перераховані деякі ключові аспекти фізичної безпеки в хмарному середовищі:

Дата-центри: Постачальники хмарних послуг зазвичай володіють або орендують великі дата-центри, де розташовані сервери та інфраструктура. Фізична безпека цих дата-центрів може включати охоронні служби, системи контролю доступу, відеоспостереження, біометричну ідентифікацію та інші заходи безпеки.

Контроль доступу: Доступ до дата-центрів або серверних приміщень повинен бути обмежений і контрольований. Це досягається за допомогою фізичних бар'єрів, таких як двері з електронними замками або біометричними системами ідентифікації, карточок доступу та обмежень щодо присутності у відповідних зонах.

Пожежна безпека: Дата-центри повинні бути обладнані системами пожежної безпеки, такими як детектори диму, пожежні спринклери, газові загасники тощо, щоб уникнути поширення вогню та мінімізувати ризик втрати даних.

Захист фізичної інфраструктури дата-центру, включаючи сервери, мережеве обладнання, системи охорони, контроль доступу та захист від природних катастроф.

Захист даних

Шифрування даних, яке забезпечує конфіденційність інформації під час зберігання та передачі. Керування ключами шифрування і забезпечення безпеки ключів також важливі аспекти.

Захист даних в хмарному середовищі - це одна з ключових складових безпеки в цьому середовищі, оскільки воно містить велику кількість конфіденційної інформації про користувачів та компанії, які користуються хмарними сервісами. Це означає, що захист даних в хмарному середовищі повинен бути комплексним і забезпечувати захист на різних рівнях, таких як:

Шифрування: Шифрування є ключовим елементом захисту даних в хмарному середовищі. Користувачі повинні мати можливість шифрувати дані перед їх відправкою до хмарного сервісу, щоб запобігти несанкціонованому доступу до цих даних. Крім того, постачальники хмарних послуг повинні забезпечувати шифрування даних від певних загроз, таких як крадіжка даних або віддалений доступ до хмарних ресурсів.

Контроль доступу: Контроль доступу повинен бути обов'язковим елементом захисту даних в хмарному середовищі. Це означає, що доступ до даних повинен бути обмежений і контрольований. Крім того, постачальники хмарних послуг повинні вживати заходів безпеки, таких як двофакторна аутентифікація та рівні доступу до даних, щоб запобігти несанкціонованому доступу до конфіденційних даних.

Захист від кібератак: Постачальники хмарних послуг повинні забезпечувати захист від різних типів кібератак, таких як віруси, зламування, фішинг, DDoS-атаки та інші. Це може бути досягнуто за допомогою захисту мережі, захисту від програм шпигунів та інших програм шкідливого ПЗ.

Захист мережі

Захист мережевих з'єднань та комунікації між компонентами хмарної інфраструктури, включаючи використання брандмауерів, виявлення та запобігання вторгнень (IDS/IPS), VPN-з'єднання та інші мережеві заходи безпеки.

Захист мережі в хмарному середовищі є важливим аспектом безпеки, оскільки мережа є ключовим елементом хмарної інфраструктури. Ось деякі заходи, які зазвичай вживаються для захисту мережі в хмарному середовищі:

Фірмове програмне забезпечення: Хмарні постачальники встановлюють фірмове програмне забезпечення для захисту мережі від атак. Це програмне забезпечення включає в себе механізми виявлення вторгнень, блокування шкідливих дій та інші інструменти захисту.

Віртуальні мережі: Віртуальні мережі дозволяють розділити фізичну мережу на декілька логічних мереж з окремими адресами IP. Це дозволяє обмежити доступ до різних частин мережі та зменшити ризики несанкціонованого доступу до мережевих ресурсів.

Фізична ізоляція: Фізична ізоляція означає, що хмарна мережа повинна бути фізично відокремлена від зовнішнього середовища. Це може включати фізичне розміщення мережевих серверів та обладнання в безпечних приміщеннях, які мають обмежений доступ.

Ідентифікація та автентифікація: Хмарні постачальники надають інструменти для управління ідентифікацією та автентифікацією користувачів мережі. Це може включати багаторівневу аутентифікацію, контроль доступу на основі ролей та інші інструменти.

Захист від DDoS-атак: Хмарні постачальники можуть використовувати захисні механізми від DDoS-атак, які можуть призвести до перевантаження мережі та зниження її продуктивності.

Аутентифікація та авторизація

Використання сильних механізмів аутентифікації, таких як багатофакторна аутентифікація (Multi-Factor Authentication, MFA), для перевірки ідентичності користувачів. Контроль доступу до ресурсів хмари, встановлення правильних рівнів доступу та автоматизована управління правами користувачів.

Аутентифікація та авторизація є важливими аспектами безпеки в хмарних середовищах і використовуються для контролю доступу користувачів до ресурсів та послуг хмари. Ось що означає аутентифікація та авторизація в хмарних середовищах:

Аутентифікація: Аутентифікація в хмарних середовищах визначає ідентифікацію користувача та перевірку його автентичності перед наданням доступу до ресурсів хмари. Це може включати використання імен користувачів та паролів, двофакторної аутентифікації, біометричних методів (наприклад, розпізнавання відбитків пальців) або використання сертифікатів.

Авторизація: Авторизація встановлює, які ресурси та послуги користувач має право використовувати після успішної аутентифікації. Після того, як користувач буде ідентифікований, система перевіряє його права доступу до конкретних ресурсів. Це може бути здійснено на основі ролей користувачів або інших критеріїв, які визначають рівень доступу до певних ресурсів або функцій.

Синхронізація ідентифікації та авторизації: В хмарному середовищі можуть бути використані різні послуги та додатки, тому важливо мати механізм синхронізації ідентифікації та авторизації між ними. Це забезпечує, що один раз аутентифікований користувач може отримати доступ до різних ресурсів і послуг в межах хмарного середовища без необхідності повторної аутентифікації.

1.1.1 Загальнодоступні хмарні середовища

Загальнодоступні хмарні середовища (public cloud environments) - це тип хмарного обчислення, в якому хмарні ресурси доступні широкому колу користувачів через Інтернет. Це означає, що одна фізична інфраструктура використовується для надання послуг багатьом користувачам з різних організацій чи індивідуальних клієнтів.

Основні характеристики загальнодоступних хмарних середовищ включають:

Ресурси на вимогу: Загальнодоступні хмарні середовища надають гнучкість та масштабованість, дозволяючи користувачам отримати доступ до необхідних ресурсів (обчислювальних потужностей, сховища даних, мережевих ресурсів) за потреби.

Користувачі можуть збільшувати або зменшувати обсяг ресурсів, що використовуються, в залежності від своїх потреб.

Широкий доступ: Загальнодоступні хмарні середовища надають послуги через Інтернет, що дозволяє користувачам отримувати доступ до хмарних ресурсів з будь-якого місця та пристрою з підключенням до мережі. Це робить їх доступними для організацій та користувачів з різних географічних регіонів.

Спільне використання ресурсів: У загальнодоступних хмарних середовищах ресурси спільно використовуються різними користувачами. Інфраструктура, така як сервери, сховища даних та мережеві ресурси, розділяються між багатьма користувачами, що дозволяє оптимізувати використання ресурсів та знижує витрати на обладнання для окремих користувачів.

Деякі приклади загальнодоступних хмарних середовищ включають:

Amazon Web Services (AWS): AWS є одним з найбільших та найпопулярніших загальнодоступних хмарних середовищ. Вони надають широкий спектр послуг, включаючи обчислювальні потужності, сховища даних, мережеві ресурси, бази даних та інші сервіси. Ознайомитись з інтерфейсом Amazon Web Services (AWS) можна ознайомитись на рисунку 1.1

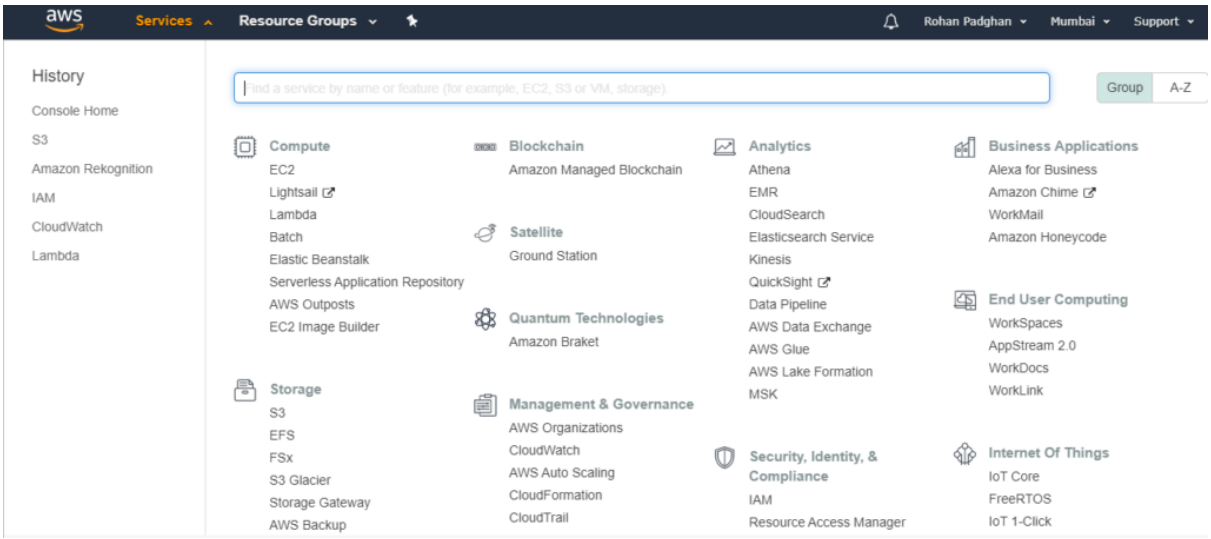

Рисунок 1.1 - інтерфейс Amazon Web Services (AWS)

Amazon Web Services (AWS) є провідним загальнодоступним хмарним середовищем, розробленим Amazon.com. AWS пропонує широкий спектр послуг та

ресурсів, які дозволяють організаціям будувати та розгортати різноманітні хмарні рішення. Ось деякі ключові компоненти та послуги, які надає AWS:

Elastic Compute Cloud (EC2): EC2 надає віртуальні сервери в хмарі, що дозволяє користувачам масштабувати обчислювальні потужності за потребою і гнучко керувати ресурсами.

Simple Storage Service (S3): S3 - це сховище об'єктів для зберігання і управління великими обсягами даних, забезпечуючи високу масштабованість, доступність та безпеку.

Elastic Block Store (EBS): EBS надає блочні сховища даних для використання з EC2 і забезпечує постійне зберігання для віртуальних машин.

Virtual Private Cloud (VPC): VPC дозволяє налаштувати віртуальну мережу, в якій можна створювати і управляти ресурсами AWS з власним набором IP-адрес та мережевими налаштуваннями.

Amazon RDS: Amazon Relational Database Service (RDS) - це керована послуга баз даних, яка дозволяє легко розгортати та керувати реляційними базами даних, такими як MySQL, PostgreSQL, Oracle і інші.

Microsoft Azure: Microsoft Azure є іншим популярним загальнодоступним хмарним середовищем, розробленим Microsoft. Вони пропонують послуги обчислення, сховищ даних, штучного інтелекту, мереж та інших ресурсів. Ознайомитись з інтерфейсом Microsoft Azure можна ознайомитись на рисунку 1.2.

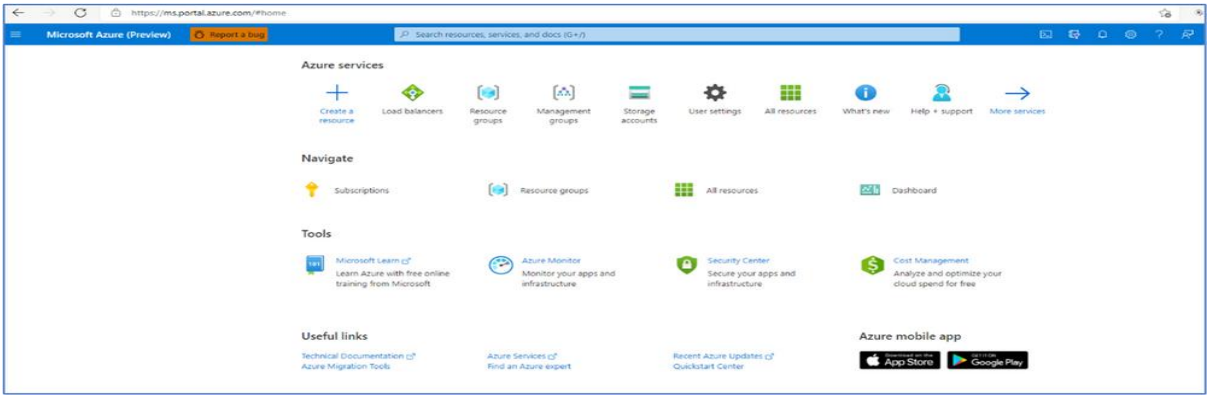

Рисунок 1.2 - інтерфейс Microsoft Azure

Microsoft Azure є іншим відомим загальнодоступним хмарним середовищем, розробленим Microsoft. Воно надає широкий спектр послуг та інструментів для

розробки, розгортання та керування хмарними додатками. Ось деякі основні компоненти та послуги, які пропонує Azure:

Virtual Machines: Azure дозволяє розгортати віртуальні машини на базі Windows або Linux з різноманітними обчислювальними ресурсами та конфігураціями.

Azure App Service: Це платформа для розгортання, швидкого масштабування та керування веб-додатками та службами. Включає рішення для розгортання веб-сайтів, веб-служб, контейнеризованих додатків тощо.

Azure Storage: Azure надає різні типи сховищ даних, включаючи Blob Storage для зберігання об'єктів, File Storage для файлових систем та Disk Storage для блочного сховища даних.

Azure SQL Database: Це повністю керована реляційна база даних, яка пропонує високу доступність, масштабованість та безпеку.

Google Cloud Platform (GCP): GCP - це хмарне середовище, розроблене Google. Вони надають послуги обчислення, сховищ даних, штучного інтелекту, мереж та інші ресурси, а також мають широкий спектр інструментів для розробки та управління хмарними додатками. Ознайомитись з інтерфейсом Google Cloud Platform (GCP) можна ознайомитись на рисунку 1.3.

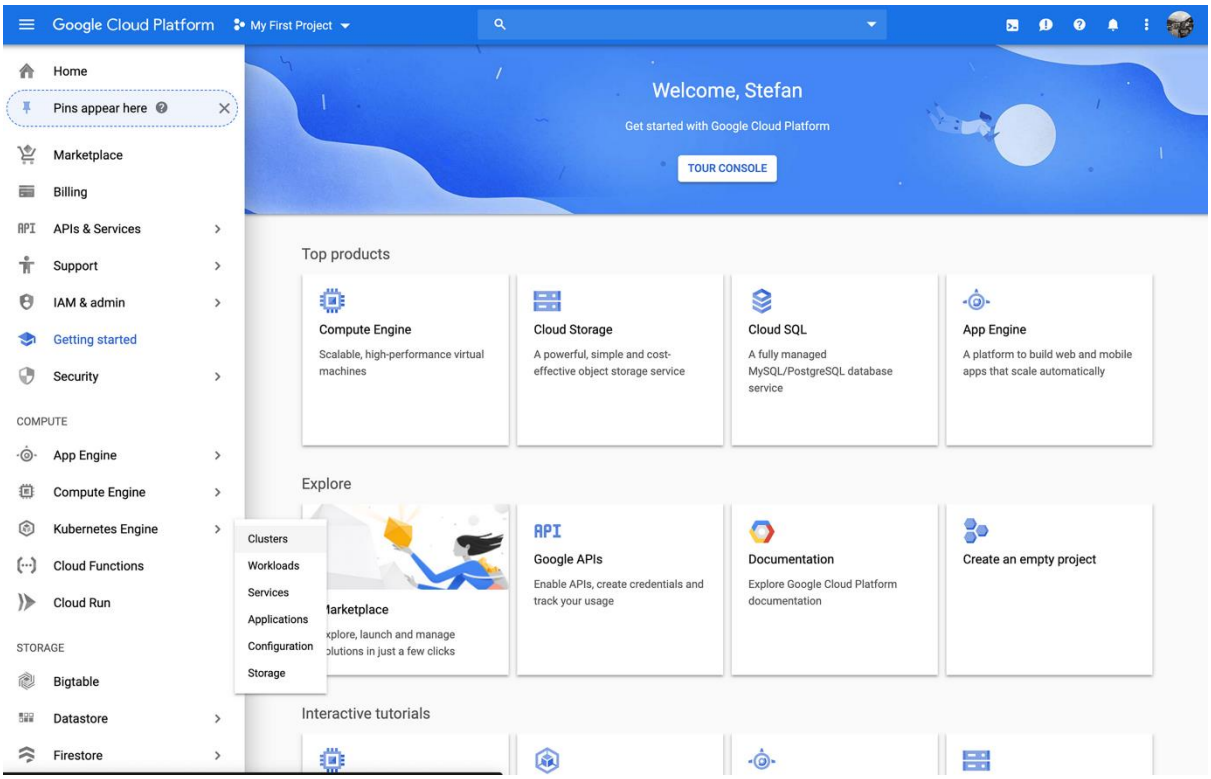

Рисунок 1.3 - інтерфейс Google Cloud Platform (GCP)

Google Cloud Platform (GCP) - це загальнодоступне хмарне середовище, розроблене Google. Воно надає набір послуг та інфраструктури для розробки, тестування, розгортання та керування додатками в хмарі. Ось деякі ключові компоненти та послуги, які надає GCP:

Compute Engine: Це інфраструктура віртуальних машин, що дозволяє розгортати та керувати віртуальними серверами з різноманітними обчислювальними ресурсами.

App Engine: Це платформа для розгортання та масштабування веб-додатків з автоматичним управлінням інфраструктурою.

Cloud Storage: Це сховище об'єктів для зберігання та управління великими обсягами даних, забезпечуючи надійність, доступність та швидкий доступ до даних.

Cloud SQL: Це керована послуга баз даних, яка підтримує реляційні бази даних MySQL та PostgreSQL.

Kubernetes Engine: Це керована послуга контейнерів, яка дозволяє розгортати та керувати контейнеризованими додатками з використанням Kubernetes.

IBM Cloud: IBM Cloud - це хмарне середовище, розроблене компанією IBM. Вони надають різноманітні послуги, включаючи обчислення, сховища даних, інструменти для розробки та управління додатками. Ознайомитись з інтерфейсом IBM Cloud можна ознайомитись на рисунку 1.4.

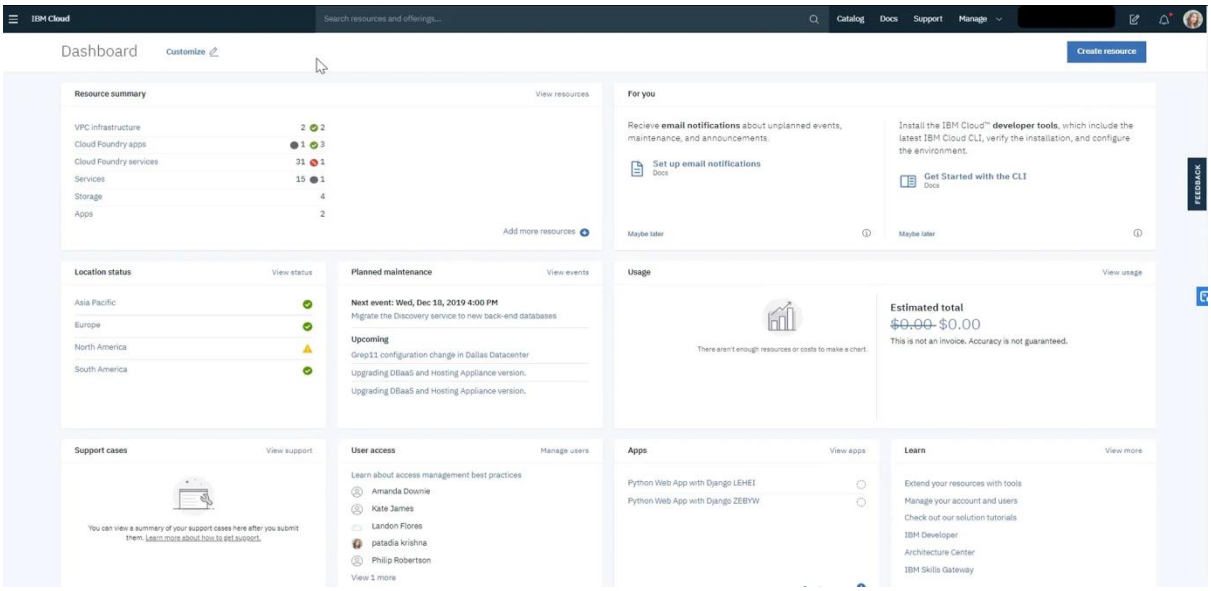

Рисунок 1.4 - інтерфейс IBM Cloud

IBM Cloud є загальнодоступним хмарним середовищем, розробленим компанією IBM. Воно надає набір інфраструктурних та платформених послуг для розробки, розгортання та керування додатками в хмарі. Ось деякі ключові компоненти та послуги, які надає IBM Cloud:

Virtual Servers: IBM Cloud дозволяє створювати та керувати віртуальними серверами з різноманітними обчислювальними ресурсами на базі віртуалізації.

IBM Kubernetes Service: Це керована послуга контейнерів, яка надає платформу для розгортання та керування контейнеризованими додатками з використанням Kubernetes.

IBM Watson: Watson - це набір послуг штучного інтелекту, які включають розпізнавання мови, обробку природної мови, машинне навчання та інші інтелектуальні функції.

IBM Cloud Object Storage: Це сховище об'єктів для зберігання великих обсягів даних зі скаліруванням, високою доступністю та захистом даних.

IBM Cloud Functions: Це рішення для виконання коду "функцій як сервіс" (FaaS), де ви можете реагувати на події та виконувати функції без необхідності керування інфраструктурою.

Oracle Cloud: Oracle Cloud - це хмарне середовище, розроблене компанією Oracle. Вони пропонують послуги обчислення, сховищ даних, інтегровані послуги та інші хмарні ресурси. Ознайомитись з інтерфейсом Oracle Cloud можна ознайомитись на рисунку 1.5

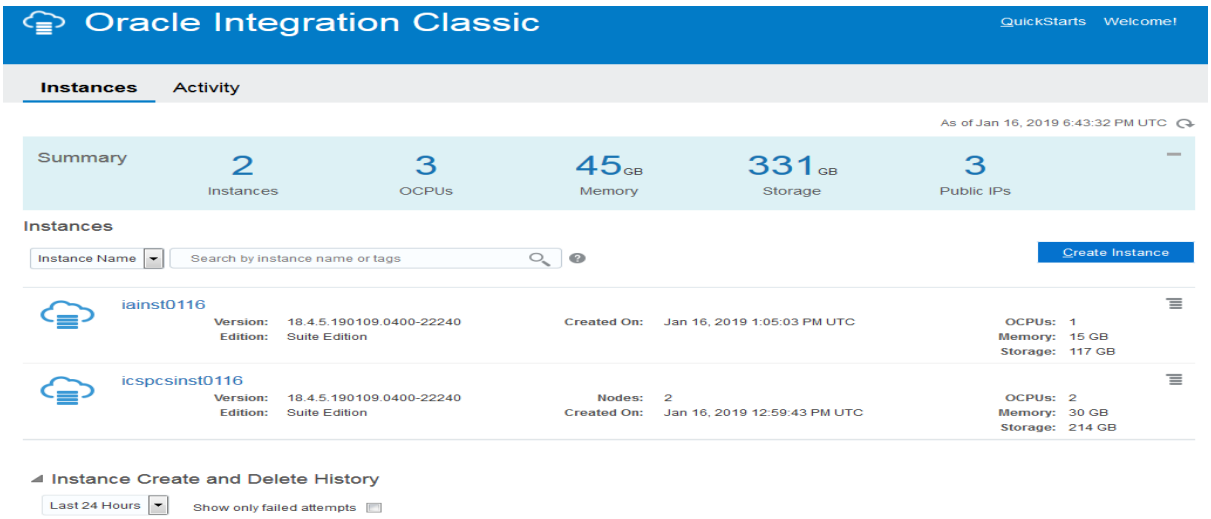

Рисунок 1.5 - інтерфейс Oracle Cloud

Oracle Cloud є загальнодоступним хмарним середовищем, розробленим компанією Oracle. Воно надає широкий спектр послуг та ресурсів для розробки, розгортання та керування додатками в хмарі. Ось деякі ключові компоненти та послуги, які надає Oracle Cloud:

Compute: Oracle Cloud надає віртуальні сервери та контейнери для розгортання та керування обчислювальними ресурсами.

Storage: Oracle Cloud пропонує сховища даних, включаючи об'єктне сховище, файлове сховище та блочне сховище для зберігання різноманітних типів даних.

Virtual Servers: IBM Cloud дозволяє створювати та керувати віртуальними серверами з різноманітними обчислювальними ресурсами на базі віртуалізації.

Database: Oracle Cloud надає керовані послуги баз даних, включаючи Oracle Autonomous Database, яка забезпечує автоматичне управління та оптимізацію баз даних.

Networking: Oracle Cloud пропонує можливості мережевого планування та налаштування, включаючи віртуальні мережі, VPN, балансувальники навантаження та інші рішення для забезпечення мережевої інфраструктури.

Identity and Access Management: Це служба керування доступом та ідентифікації, яка дозволяє контролювати доступ до ресурсів та застосовувати політики безпеки.

Application Development: Oracle Cloud має інструменти для розробки та розгортання додатків, включаючи середовища розробки, контейнеризацію, DevOps і інші рішення.

AI and Machine Learning: Oracle Cloud надає послуги інтелектуального аналізу даних, машинного навчання та штучного інтелекту, що дозволяє розробляти та розгортати інтелектуальні додатки.

Це лише кілька прикладів загальнодоступних хмарних середовищ, існує багато інших провайдерів, які пропонують подібні послуги. Кожен з них має свої особливості та набір сервісів, що варто розглянути в контексті ваших потреб та вимог.

1.1.2 Приватні хмарні середовища

Приватні хмарні середовища - це інфраструктурні рішення, що дозволяють організаціям будувати власні хмарні середовища для зберігання, обробки та управління своїми даними та додатками. Основна відмінність приватного хмарного середовища полягає у тому, що воно розгортається всередині організації і використовується виключно для внутрішніх потреб.

Приватні хмарні середовища є альтернативою загальнодоступним публічним хмарним платформам, і вони спроектовані для використання лише в межах конкретної організації. Основна відмінність полягає в тому, що інфраструктура приватного хмарного середовища фізично розташована всередині організації або управляється організацією, що дозволяє забезпечити більшу контроль, безпеку та конфіденційність даних.

Приватні хмарні середовища можуть бути побудовані за допомогою різних технологій, включаючи:

On-Premises Private Clouds: В цьому випадку хмарна інфраструктура будується та управляється безпосередньо організацією на її власних фізичних серверах та мережевому обладнанні. Це дає повний контроль над інфраструктурою, але вимагає великих витрат на обладнання, обслуговування та експлуатацію.

Локальні приватні хмари, також відомі як самостійні приватні хмари або внутрішні приватні хмари, стосуються хмарної інфраструктури, яка розгортається та працює у власних приміщеннях організації, як правило, у власному центрі обробки даних або серверних кімнатах. На відміну від публічних хмар, які розміщуються сторонніми постачальниками та доступ до яких здійснюється через Інтернет, локальні приватні хмари надають організаціям повний контроль і право власності на свою хмарну інфраструктуру.

Ось деякі ключові характеристики та міркування щодо локальних приватних хмар:

Контроль інфраструктури: організації мають повний контроль над обладнанням, мережею та інфраструктурою зберігання даних у своїй приватній хмарі. Вони можуть налаштувати та оптимізувати інфраструктуру відповідно до своїх конкретних вимог і політики безпеки.

Безпека та відповідність: локальні приватні хмари пропонують покращені можливості безпеки та відповідності, оскільки дані та програми знаходяться у власній мережевій інфраструктурі організації. Це дозволяє організаціям впроваджувати суворі заходи безпеки та підтримувати відповідність галузевим нормам.

Суверенітет даних: за допомогою локальної приватної хмари організації можуть гарантувати, що їхні дані залишаються в межах фізичних кордонів і відповідають правилам суверенітету даних. Це може бути особливо важливим для галузей із суворими вимогами до управління даними та конфіденційності.

Продуктивність і затримка: розміщуючи хмарну інфраструктуру на місці, організації можуть зменшити затримку мережі та досягти кращої продуктивності своїх програм і служб, оскільки даним не потрібно передаватись через зовнішні мережі.

Масштабованість і гнучкість: локальні приватні хмари пропонують масштабованість і гнучкість, дозволяючи організаціям розподіляти ресурси на основі своїх конкретних потреб. Вони можуть додавати або видаляти апаратне забезпечення, сховище та мережеві компоненти відповідно до потреб, щоб відповідати мінливим навантаженням.

Капітальні та операційні витрати. Розгортання локальної приватної хмари потребує початкових капіталовкладень у придбання та обслуговування обладнання, мережевого обладнання та компонентів інфраструктури. Організації також несуть відповідальність за поточні операційні витрати, включаючи технічне обслуговування, оновлення та споживання електроенергії.

IT-експертиза та управління: для керування локальною приватною хмарою потрібні власні IT-спеціалісти або партнерство з постачальниками керованих послуг. Організації повинні переконатися, що вони мають необхідні навички та ресурси для ефективного розгортання, моніторингу та підтримки хмарної інфраструктури.

Локальні приватні хмари надають організаціям детальний контроль, підвищену безпеку та можливості відповідності. Однак вони вимагають значних початкових інвестицій і постійного управління, що робить їх придатними для організацій зі специфічними вимогами або нормативними обмеженнями, які вимагають внутрішньої хмарної інфраструктури.

Virtual Private Clouds (VPCs): Це модель, в якій організація орендує віртуальну інфраструктуру від постачальника хмарних послуг, присвоюючи їй приватну сегментовану область з власними мережевими ресурсами та політиками безпеки. Це надає більшу гнучкість та масштабованість, але інфраструктура все ще керується організацією.

Віртуальні приватні хмари (VPC) — це тип приватного хмарного середовища, який надає організаціям логічно ізольовану частину в інфраструктурі публічної хмари. У VPC постачальник хмарних послуг (CSP) виділяє віртуальний мережевий простір виключно для організації, гарантуючи, що їхні ресурси та дані залишаються відокремленими від інших орендарів у тій самій публічній хмарі.

Ось деякі основні функції та переваги віртуальних приватних хмар:

Ізоляція та безпека: VPC пропонують логічну ізоляцію, дозволяючи організаціям створювати власні віртуальні мережі, підмережі та діапазони IP-адрес у загальнодоступній хмарі. Ця ізоляція забезпечує підвищену безпеку, оскільки трафік усередині VPC зберігається окремо від інших орендарів і захищений заходами безпеки мережі, такими як брандмауери та політики контролю доступу.

Налаштування та контроль. Організації мають контроль над своєю конфігурацією VPC, включаючи можливість визначати мережеві топології, підмережі, таблиці маршрутизації та політики безпеки. Це дає їм змогу пристосувати середовище VPC до своїх конкретних вимог і потреб безпеки.

Масштабованість: VPC забезпечують гнучкість збільшення або зменшення ресурсів залежно від попиту. Організації можуть легко додавати або видаляти віртуальні машини, сховища та інші хмарні служби в межах свого VPC, не впливаючи на інших орендарів і не вимагаючи змін фізичної інфраструктури.

Підключення: VPC часто надають варіанти безпечного підключення до локальних центрів обробки даних або інших хмарних середовищ. Це можна зробити за допомогою з'єднань віртуальної приватної мережі (VPN), виділених виділених ліній або прямих з'єднань, що дозволяє створювати гібридні хмарні або багатохмарні архітектури.

Відповідність: VPC можуть допомогти організаціям виконати вимоги відповідності, надаючи необхідні засоби контролю та заходи безпеки. Організації можуть запроваджувати шифрування, контроль доступу та інші політики, пов'язані з відповідністю, у своїх VPC, щоб захистити конфіденційні дані та забезпечити відповідність нормативним вимогам.

Економічна ефективність: VPC пропонують економічні переваги порівняно з локальними приватними хмарами, оскільки організаціям не потрібно інвестувати та підтримувати власну фізичну інфраструктуру. Натомість вони платять за хмарні ресурси, які вони використовують у своєму VPC, на основі споживання, що дозволяє використовувати ресурси більш рентабельно.

Популярні публічні хмарні постачальники, такі як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform, пропонують послуги VPC як частину своїх хмарних пропозицій. Кожен провайдер має власну термінологію та особливості, але основна концепція надання логічно ізольованої приватної мережі в рамках публічної хмарної інфраструктури залишається незмінною.

VPC надають організаціям переваги хмарних обчислень, зберігаючи при цьому контроль, безпеку та конфіденційність, подібні до локальних середовищ. Вони добре підходять для організацій, яким потрібна гнучкість і масштабованість хмари, зберігаючи при цьому високий рівень ізоляції та безпеки.

Основні характеристики приватного хмарного середовища включають:

Контроль: Приватні хмарні середовища надають організації повний контроль над інфраструктурою, мережами та даними. Це дозволяє налаштувати та управляти середовищем згідно з внутрішніми політиками безпеки та вимогами організації.

Безпека: Приватні хмарні середовища забезпечують вищий рівень безпеки, оскільки організація контролює фізичний доступ до серверів, мережеві з'єднання та застосовує внутрішні політики безпеки.

Витрати: Хоча вартість розгортання та управління приватним хмарним середовищем може бути вищою порівняно з публічними хмарами, воно дозволяє організації економити на додаткових витратах, пов'язаних з публічними послугами хмарних провайдерів.

Гнучкість: Приватні хмарні середовища надають організації гнучкість у розробці та розгортанні додатків, оскільки вони можуть бути налаштовані під конкретні потреби та вимоги організації.

Ось кілька прикладів приватних хмарних середовищ:

VMware vSphere: VMware vSphere є одним з найпопулярніших рішень для побудови приватних хмарних середовищ. Воно дозволяє віртуалізувати сервери, зберігання та мережі, створюючи віртуальну інфраструктуру, яка може бути керована централізовано.

Ознайомитись з інтерфейсом VMware vSphere можна ознайомитись на рисунку 1.6.

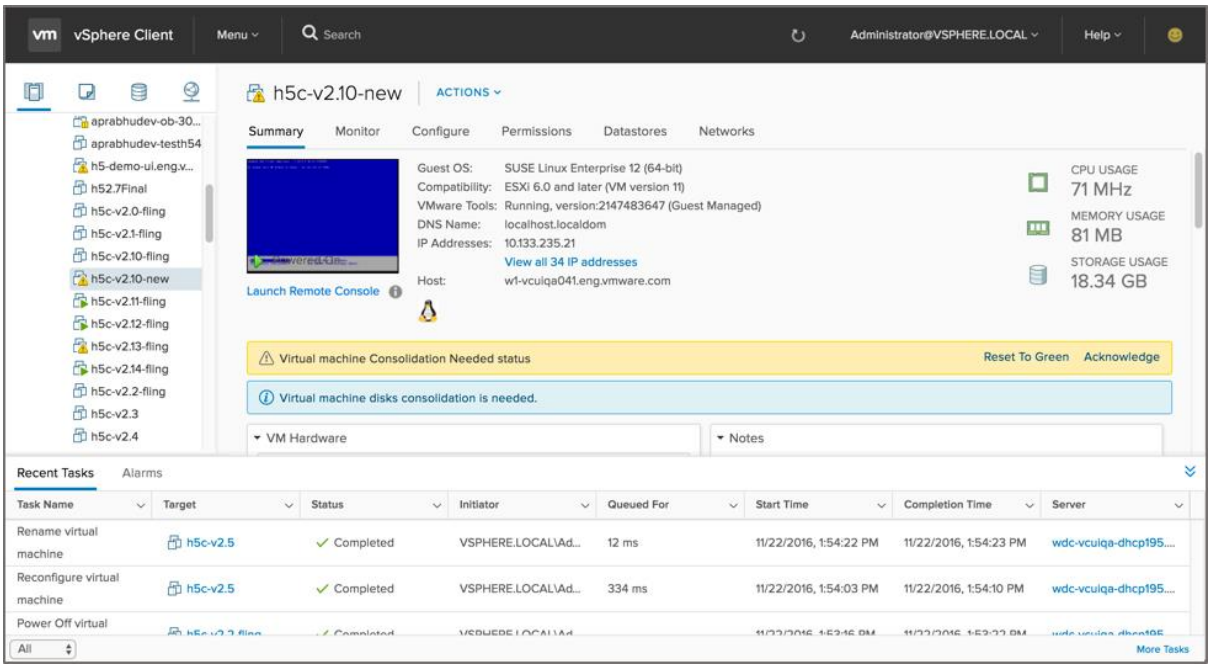

Рисунок 1.6 - інтерфейс VMware vSphere

VMware vSphere є відомою і широко використовуваною платформою для віртуалізації і побудови приватних хмарних середовищ. Вона надає інфраструктуру віртуалізації на основі гіпервізора, що дозволяє організаціям створювати та управляти віртуальними серверами, зберіганням та мережами.

Основні компоненти VMware vSphere включають:

ESXi Hypervisor: ESXi є гіпервізором VMware, який дозволяє віртуалізувати фізичні сервери. Він дозволяє запускати та керувати віртуальними машинами, які виконують різноманітні операційні системи та додатки.

vCenter Server: vCenter Server є центральним керуючим компонентом VMware vSphere. Він надає централізоване керування віртуальними ресурсами, включаючи віртуальні машини, сховища даних, мережі та безпеку. Крім того, vCenter Server забезпечує функції моніторингу, управління міграцією та резервного копіювання.

vSphere Client: vSphere Client є інтерфейсом користувача для взаємодії з VMware vSphere. Він дозволяє адміністраторам створювати, конфігурувати та керувати віртуальними машинами, мережами, зберіганням та іншими ресурсами.

Microsoft Azure Stack: Microsoft Azure Stack - це рішення, яке дозволяє організаціям розгортати приватні хмарні середовища на основі технологій Azure власними силами. Воно забезпечує консистентність з публічним хмарним середовищем Azure та дозволяє використовувати подібні сервіси та інструменти. Ознайомитись з інтерфейсом Microsoft Azure Stack можна ознайомитись на рисунку 1.7.

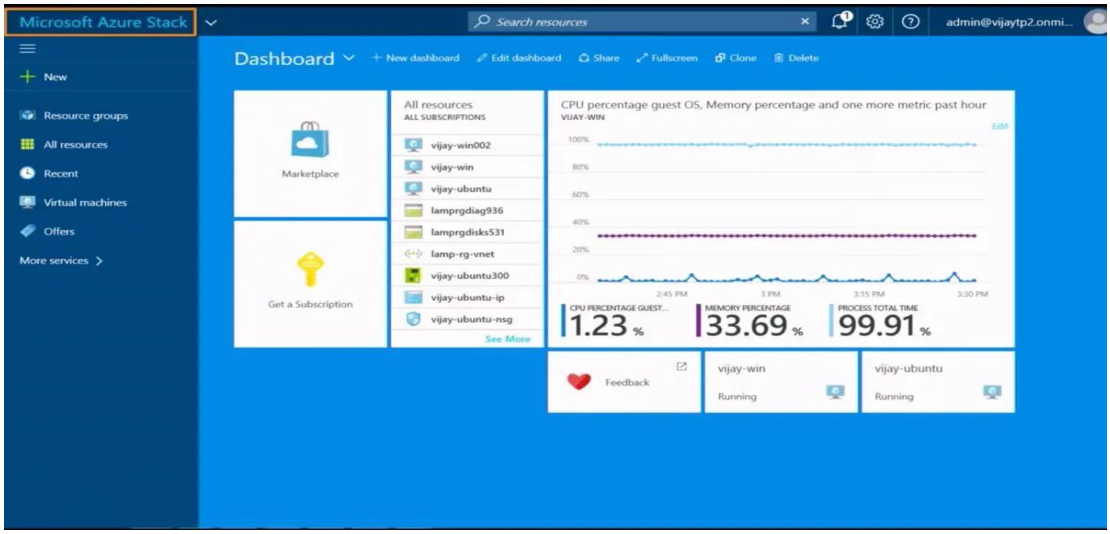

Рисунок 1.7 - інтерфейс Microsoft Azure Stack

Microsoft Azure Stack є рішенням, яке дозволяє побудувати приватне хмарне середовище на основі технологій Microsoft Azure у власному дата-центрі організації. Воно надає консистентність з публічним хмарним середовищем Azure, що дозволяє використовувати схожі сервіси, інструменти та моделі розгортання.

Основні компоненти та можливості Microsoft Azure Stack включають:

Azure Resource Manager: Azure Stack використовує Azure Resource Manager для організації та управління ресурсами в хмарному середовищі. Він надає централізоване керування ресурсами, створення та управління шаблонами розгортання.

Azure Services: Azure Stack надає широкий спектр сервісів, які доступні в публічному хмарному середовищі Azure, включаючи віртуальні машини, контейнери, бази даних, аналітику, штучний інтелект, мережеві сервіси та багато іншого. Це дозволяє розробникам та адміністраторам використовувати знайомі сервіси та інструменти для розгортання та управління своїми додатками та інфраструктурою.

OpenStack: OpenStack - це відкрите програмне забезпечення для побудови приватних та гібридних хмарних середовищ. Воно надає набір інструментів та сервісів для віртуалізації серверів, зберігання та мереж, що дозволяє організаціям створювати та керувати своїми власними приватними хмарами. Ознайомитись з інтерфейсом OpenStack можна ознайомитись на рисунку 1.8.

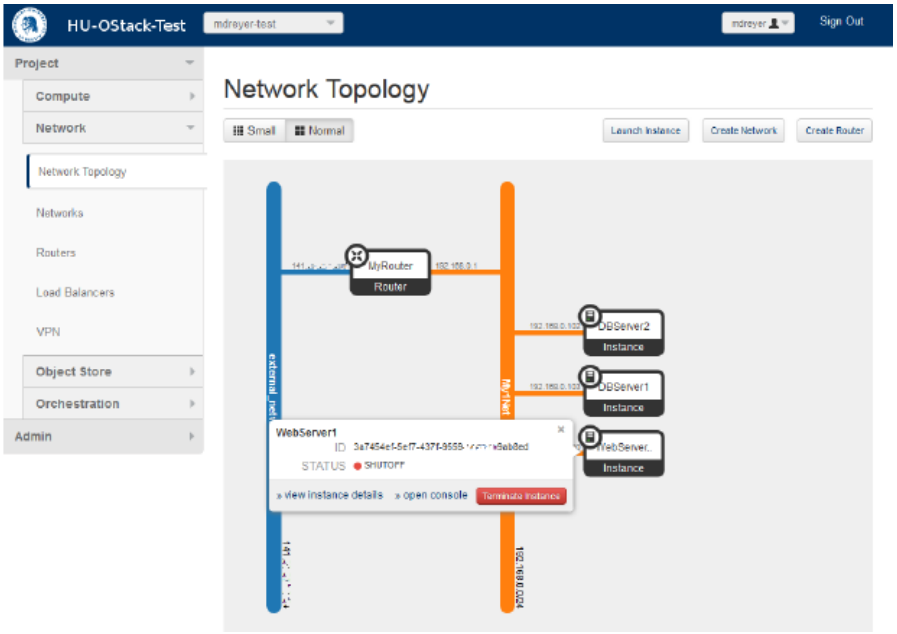

Рисунок 1.8 - інтерфейс OpenStack

OpenStack - це відкрите програмне забезпечення для побудови приватних та гібридних хмарних середовищ. Воно надає набір інструментів та сервісів, які дозволяють організаціям створювати та керувати власними приватними хмарами, що базуються на віртуалізації серверів, зберігання та мереж.

Основні компоненти OpenStack включають:

Nova: Nova є компонентом OpenStack, що відповідає за управління обчислювальними ресурсами. Він дозволяє розгортати та керувати віртуальними машинами та контейнерами, налаштовувати мережеві параметри та масштабувати обчислювальні потужності.

Neutron: Neutron відповідає за управління мережевими ресурсами у хмарному середовищі OpenStack. Він дозволяє створювати та налаштовувати віртуальні мережі, підсистеми мережевої безпеки, маршрутизацію та балансування навантаження.

Swift: Swift є компонентом OpenStack, що відповідає за управління об'єктним сховищем даних. Він надає масштабоване та високодоступне сховище для зберігання об'єктів, таких як файли, зображення та відео.

Nutanix Enterprise Cloud: Nutanix Enterprise Cloud - це інтегроване рішення, що поєднує в собі віртуалізацію, зберігання та мережі для побудови приватних хмарних середовищ. Воно надає гнучкість, масштабованість та високу доступність для додатків та сервісів організації.

Ознайомитись з інтерфейсом Nutanix Enterprise Cloud можна ознайомитись на рисунку 1.9.

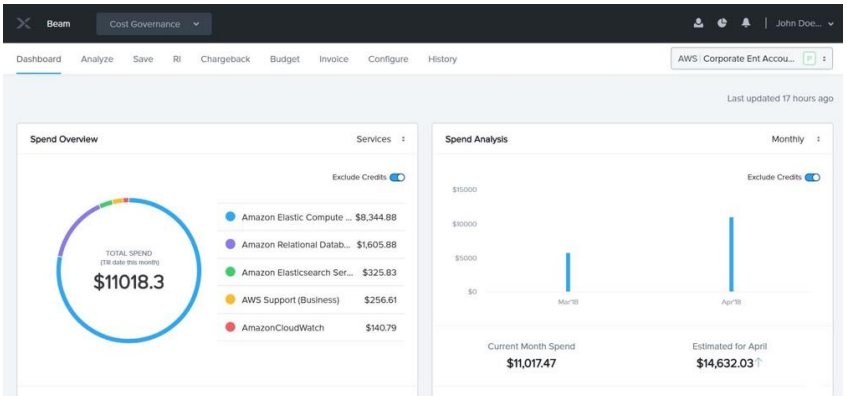

Рисунок 1.9 - інтерфейс Nutanix Enterprise Cloud

Nutanix Enterprise Cloud є інтегрованою платформою, що об'єднує в собі віртуалізацію, зберігання та мережі для побудови приватних хмарних середовищ. Це

рішення дозволяє організаціям швидко розгортати та керувати інфраструктурою своїх додатків та сервісів.

Основні компоненти та можливості Nutanix Enterprise Cloud включають:

Nutanix Prism: Nutanix Prism - це централізована консоль управління, яка надає інструменти для керування та моніторингу хмарної інфраструктури. Вона дозволяє адміністраторам здійснювати розгортання, конфігурацію, моніторинг та оптимізацію ресурсів у приватному хмарному середовищі.

Acropolis Hypervisor (AHV): AHV є гіпервізором, розробленим Nutanix, який дозволяє віртуалізувати фізичні сервери. Він надає можливості віртуалізації та управління віртуальними машинами у приватному хмарному середовищі.

Prism Central: Prism Central - це централізована консоль керування, яка дозволяє управляти багатьма хмарними кластерами Nutanix з одного інтерфейсу. Вона забезпечує глобальне керування, моніторинг та управління ресурсами в розподілених середовищах.

Nutanix Calm: Nutanix Calm - це інструмент автоматизації та оркестрації, який дозволяє автоматизувати розгортання та управління додатками у приватному хмарному середовищі. Він спрощує процес розгортання та управління додатками, роблячи їх більш ефективними та масштабованими.

HPE Helion CloudSystem: HPE Helion CloudSystem - це інтегрована платформа для побудови приватних хмарних середовищ, що включає в себе віртуалізацію, автоматизацію та оркестрацію ресурсів.

HPE Helion CloudSystem була інтегрованою платформою, розробленою компанією Hewlett Packard Enterprise (HPE) для побудови приватних, гібридних та хмарних середовищ. Проте, важливо відзначити, що на початку 2021 року HPE оголосила про припинення підтримки та розвитку Helion CloudSystem.

Історично HPE Helion CloudSystem включала такі компоненти:

HPE Helion OpenStack: Це була реалізація відкритої платформи OpenStack, яку HPE інтегрувала в своє хмарне рішення. OpenStack дозволяла створювати та керувати обчислювальними, мережевими та зберігальними ресурсами у приватному хмарному середовищі.

HPE Helion Stackato: Це була платформа для розгортання та керування застосунками у хмарному середовищі. HPE Helion Stackato підтримувала різні мови програмування та фреймворки, що дозволяло розробникам легко створювати та масштабувати додатки.

HPE Cloud Service Automation (CSA): CSA був компонентом, що надавав інфраструктуру для автоматизації управління розгортанням, конфігурацією та управлінням хмарними ресурсами. Він надавав централізоване керування різними сервісами, включаючи віртуалізацію, мережі та зберігання.

HPE Helion Development Platform: Це була платформа розробки, яка надавала інфраструктуру для розробки, тестування та розгортання додатків у хмарному середовищі. Вона підтримувала різні мови програмування та інструменти розробки.

1.1.3 Гібридні хмарні середовища

Гібридні хмарні середовища поєднують в собі елементи приватних та публічних хмар, щоб створити інтегровану інфраструктуру, яка комбінує переваги обох підходів. Такі середовища дозволяють організаціям гнучко розгортати та управляти своїми додатками та даними, використовуючи як внутрішні ресурси, так і ресурси публічних хмар.

Основні переваги гібридних хмарних середовищ включають:

Гнучкість та масштабованість: Гібридні хмари дозволяють організаціям масштабувати свої обчислювальні та зберігальні ресурси в залежності від потреб. Вони можуть використовувати внутрішні ресурси для завдань з низькими вимогами до продуктивності, а публічні хмари - для роботи зі зростаючими або непередбачуваними навантаженнями.

Безпека та контроль: Гібридні хмарні середовища дозволяють організаціям зберігати конфіденційні дані та критичні додатки на приватних серверах, забезпечуючи високий рівень безпеки та контролю. У той же час, вони можуть використовувати публічні хмари для менш чутливих даних або для проведення тестувань та розробки.

Економічність: Гібридні хмари дозволяють організаціям оптимізувати витрати на IT-інфраструктуру, використовуючи приватні ресурси для завдань, що потребують високої продуктивності або додержання регуляторних вимог, а публічні ресурси - для більш незначних робіт або тимчасових потреб.

Ось деякі приклади гібридних хмарних середовищ:

Microsoft Azure Stack: Azure Stack є розширенням публічного хмарного рішення Microsoft Azure, яке дозволяє організаціям будувати приватні хмарні середовища, які сумісні з Azure. Воно надає спільну управлінням, мобільність додатків та консистентність з Azure. Приклад роботи Azure Stack можна побачити на рисунку 1.10.

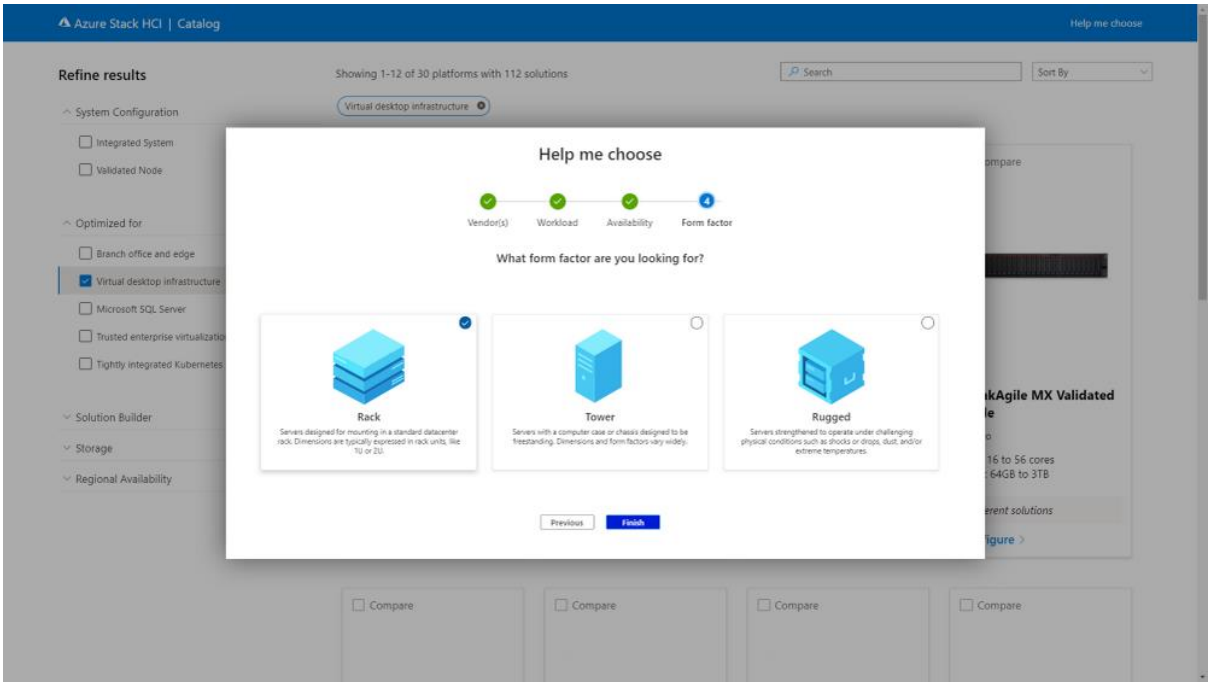

Рисунок 1.10 Приклад роботи Azure Stack

Microsoft Azure Stack є рішенням для побудови гібридних хмарних середовищ, розробленим компанією Microsoft. Воно дозволяє організаціям розгортати приватні хмарні середовища, які є сумісними з публічним хмарним сервісом Microsoft Azure.

Основні компоненти та можливості Azure Stack включають:

Azure Stack Hub: Це центральна складова Azure Stack, яка забезпечує інфраструктуру для розгортання та керування хмарними ресурсами. Azure Stack Hub

надає можливості для створення віртуальних машин, мереж та зберігання, а також підтримку контейнерів.

Сумісність з Azure: Azure Stack забезпечує консистентність з публічним хмарним сервісом Azure. Це означає, що додатки, розроблені для Azure, можуть бути легко перенесені та запущені в Azure Stack, що дозволяє організаціям використовувати однакові інструменти та підходи до розробки та управління.

Гібридна коннективність: Azure Stack дозволяє організаціям розширити свою інфраструктуру, підключившись до Azure публічної хмари. Це дозволяє забезпечити гнучкість, масштабованість та резервне копіювання даних між приватним та публічним хмарним середовищами.

Управління та автоматизація: Azure Stack надає інструменти для централізованого управління та автоматизації хмарних ресурсів. Це включає моніторинг, оркестрацію, резервне копіювання та інші функції, що полегшують управління хмарною інфраструктурою.

Загалом, Microsoft Azure Stack надає організаціям можливість будувати гібних хмар.

AWS Outposts: AWS Outposts є рішенням від Amazon Web Services (AWS), яке дозволяє розгортати обчислювальні та зберігальні ресурси AWS в приватних дата-центрах. Воно забезпечує сумісність з AWS та інтегрується з управлінням AWS.

AWS Outposts - це сервіс від Amazon Web Services (AWS), який дозволяє розширити хмарні можливості AWS до приватного або розподіленого середовища на місці вашої організації.

Основні риси та можливості AWS Outposts:

Розширення AWS на місце: AWS Outposts дозволяє вам розгортати фізичне обладнання AWS в приватних дата-центрах або у розподілених середовищах, зберігаючи при цьому консистентність з публічним хмарним сервісом AWS. Ви можете використовувати ті ж інструменти, API, сервіси та політики управління, що й в AWS.

Управління Outposts: AWS Outposts забезпечує централізоване управління розгортаннями на місці через консоль AWS або за допомогою API. Ви можете керувати ресурсами, моніторити їх стан, здійснювати резервне копіювання та регулярні оновлення.

Сумісність з AWS сервісами: За допомогою AWS Outposts ви можете використовувати широкий спектр AWS сервісів, включаючи обчислювальні, зберігальні, бази даних, аналітичні та інші сервіси. Це дозволяє вам розгортати й управляти додатками в приватному хмарному середовищі з використанням знайомих AWS інструментів та сервісів.

Ізольованість та безпека: AWS Outposts забезпечує ізольованість вашого приватного середовища від інших клієнтів AWS. Ви можете контролювати доступ до своїх ресурсів та застосовувати політики безпеки, відповідно до ваших вимог і стандартів.

Google Cloud Anthos: Google Cloud Anthos дозволяє побудувати гібридні хмарні середовища, об'єднуючи Google Cloud з приватними інфраструктурами. Воно надає єдине управлінням, безпеку та моніторинг додатків незалежно від їх розташування.

Google Cloud Anthos є рішенням для розгортання та керування додатками в гібридних та багатохмарних середовищах. Воно дозволяє організаціям розгортати додатки на публічній хмарі Google Cloud, приватних центрах обробки даних та на інших хмарних платформах.

Основні компоненти та можливості Google Cloud Anthos:

Anthos GKE (Google Kubernetes Engine): Anthos GKE є керованим сервісом кластера Kubernetes в Google Cloud. Він дозволяє розгортати й керувати контейнеризованими додатками на хмарі Google Cloud або в приватних центрах даних.

Anthos Config Management: Цей компонент дозволяє вам управляти конфігурацією і політиками для всіх кластерів Kubernetes у вашому гібридному середовищі. Ви можете використовувати шаблони конфігурації та політик, щоб забезпечити консистентність і безпеку додатків у всьому середовищі.

Anthos Service Mesh: Цей компонент забезпечує керування мережевим трафіком і безпеку додатків, що працюють на кластерах Kubernetes. Він використовує інструменти, такі як Istio, для управління мережевими політиками, балансування навантаження та моніторингу мережевого трафіку.

Anthos Migrate: Цей компонент дозволяє мігрувати додатки з фізичних серверів або віртуальних машин в кластери Kubernetes на Google Cloud або в приватному центрі обробки даних. Він автоматизує процес міграції, що спрощує перенесення додатків у гібридне середовище.

IBM Cloud Private: IBM Cloud Private дозволяє організаціям створювати приватні хмарні середовища, які базуються на контейнерах та віртуалізації. Воно надає інструменти для розгортання, керування та моніторингу додатків у гібридній інфраструктурі.

IBM Cloud Private (ICP) є рішенням для розгортання приватної хмарної інфраструктури в середовищі організації. Воно базується на контейнерній платформі Kubernetes та надає інструменти для розгортання, управління та моніторингу додатків у приватному хмарному середовищі.

Основні компоненти та можливості IBM Cloud Private:

Kubernetes: ICP використовує Kubernetes як основну контейнерну платформу. Вона забезпечує оркестрацію контейнерів, автоматизацію масштабування та управління додатками.

Helm: Helm є інструментом для управління пакетами додатків в середовищі Kubernetes. Він дозволяє розгортати, оновлювати та керувати додатками з використанням пакетних конфігурацій.

DevOps інтеграція: ICP надає інструменти та практики для розробки додатків у середовищі DevOps. Ви можете використовувати інструменти, такі як Jenkins, Git і UrbanCode, для автоматизації процесу розробки, тестування та розгортання додатків.

Моніторинг та логування: ICP має вбудовані інструменти для моніторингу та аналізу працездатності додатків. Ви можете відстежувати метрики продуктивності, аналізувати журнали подій та виявляти проблеми в хмарному середовищі.

Безпека: ICP надає можливості для забезпечення безпеки додатків у приватному хмарному середовищі. Ви можете застосовувати політики доступу, шифрування даних та інші заходи безпеки для захисту своїх додатків та ресурсів.

Ці приклади представляють рішення від провідних провайдерів хмарних послуг, які дозволяють організаціям поєднувати публічні та приватні ресурси в гібридні хмарні середовища.

1.1.4 Багатохмарні середовища

Багатохмарні середовища (multi-cloud environments) - це ситуація, коли організація використовує послуги більш ніж одного хмарного провайдера для своїх інформаційних технологій та розгортання додатків. Це може включати використання публічних хмарних провайдерів, приватних хмар, а також традиційних офісних серверів.

Основні переваги багатохмарних середовищ включають:

Гнучкість та вибір: Багатохмарні середовища дають організаціям можливість вибирати найкращі рішення для кожного конкретного завдання. Різні хмарні провайдери можуть мати свої унікальні переваги та функціональність, і багатохмарне середовище дозволяє використовувати їх разом.

Забезпечення безпеки: Використання багатохмарних середовищ дозволяє розподіляти дані та ресурси між різними провайдерами, що може покращити безпеку. Якщо один провайдер має проблеми, інші можуть продовжувати працювати, забезпечуючи більшу стійкість та надійність.

Масштабованість: Багатохмарні середовища дозволяють організаціям масштабувати свої обчислювальні та зберігальні потреби шляхом використання ресурсів різних провайдерів. Це дозволяє ефективно використовувати ресурси та забезпечити потрібний рівень продуктивності.

Один з прикладів багатохмарних середовищ може включати в себе використання публічних хмарних провайдерів, таких як Amazon Web Services (AWS),

Microsoft Azure та Google Cloud Platform (GCP), разом з приватними хмарними рішеннями.

Наприклад, організація може використовувати AWS для розгортання інфраструктури та обчислювальних ресурсів, Azure для розгортання баз даних та аналітичних сервісів, а GCP для використання інструментів штучного інтелекту та машинного навчання. Приватні хмарні рішення, такі як OpenStack або VMware, можуть використовуватись для розгортання власних серверів і додаткових ресурсів в приватних центрах обробки даних організації.

Це дозволяє організації використовувати найкращі можливості кожного провайдера, оптимізувати витрати, забезпечити високу доступність та надійність, а також мати контроль над критичними даними та дотримуватись вимог щодо безпеки та регулятивних вимог.

Проте, багатохмарні середовища також можуть потребувати додаткового управління, інтеграції між різними провайдерами, а також вирішення питань щодо даних, безпеки та мережевої інтеграції між різними хмарними середовищами.

1.2 Важливість безпеки в хмарному середовищі та визначення існуючих загроз

Важливість безпеки в хмарному середовищі не може бути недооцінена. Оскільки дані та додатки зберігаються та обробляються на серверах, що належать хмарному провайдеру, необхідно вживати заходів для захисту конфіденційності, цілісності та доступності інформації.

Важливість безпеки в хмарному середовищі полягає в тому, що організації передають свої дані та додатки провайдеру хмарних послуг. Деякі основні причини, чому безпека в хмарному середовищі є важливою:

Конфіденційність даних: Компанії зберігають важливі дані, такі як фінансові дані клієнтів, особисту інформацію та комерційну інтелектуальну власність, у хмарному середовищі. Безпека даних є критичною, оскільки викриття чутливих даних

може призвести до фінансових втрат, порушення вимог щодо конфіденційності та втрати довіри клієнтів.

Цілісність даних: Важливо забезпечити, щоб дані у хмарному середовищі залишалися недоторканими і не піддалися змінам без належної авторизації. Порушення цілісності даних може призвести до спотворення інформації, помилкових рішень та проблем в роботі бізнесу.

Доступність сервісів: Важливо, щоб хмарні послуги були доступні в будь-який час для користувачів. Зловмисники можуть намагатися збити сервіс або завдати шкоди мережевим інфраструктурам, що може призвести до перерви у роботі бізнесу, втрати прибутку та негативного впливу на репутацію.

Деякі існуючі загрози безпеці в хмарному середовищі включають:

Несанкціонований доступ: Зловмисники можуть намагатися отримати несанкціонований доступ до хмарних ресурсів та даних. Це може включати атаки на облікові записи користувачів, слабкі паролі, фішингові атаки або використання недостатньо захищених мережевих з'єднань.

Втрата або крадіжка даних: Наявність великого обсягу даних у хмарі робить його привабливою ціллю для зловмисників. Можливі загрози включають втрату даних через технічні збої, несправності обладнання або крадіжку даних.

Вразливості програмного забезпечення: Якщо в хмарному середовищі використовуються застарілі або недостатньо оновлювані програмні продукти, це може створити вразливості, які можуть бути використані зловмисниками для отримання доступу або перешкоджання роботі сервісів.

Недостатня ізоляція даних: Якщо в хмарному середовищі недостатньо забезпечена ізоляція між різними користувачами або тенантами, це може призвести до небажаного доступу до чужих даних або витоку конфіденційної інформації.

1.3 Принцип роботи безпеки в хмарі

Принципи роботи безпеки в хмарному середовищі включають ряд заходів та підходів, спрямованих на захист даних, систем та інфраструктури. Основні принципи безпеки в хмарному середовищі включають наступне:

Конфіденційність: Захист конфіденційності даних є основним принципом безпеки. Використовуються різні механізми шифрування для захисту даних під час передачі, зберігання та обробки в хмарі. Крім того, контролюються доступ та автентифікація користувачів, щоб забезпечити, що лише авторизовані особи мають доступ до конфіденційної інформації.

Конфіденційність в хмарному середовищі є однією з найважливіших аспектів безпеки. Вона забезпечує захист конфіденційної інформації, що зберігається та обробляється в хмарі від несанкціонованого доступу. Основні аспекти конфіденційності в хмарному середовищі включають наступні:

Шифрування даних: Застосування шифрування даних є ключовим для забезпечення конфіденційності в хмарі. Дані можуть бути зашифровані перед їх передачею, зберіганням або обробкою, забезпечуючи, що лише особи з правильними ключами можуть розшифрувати та отримати доступ до цих даних.

Управління доступом: Контроль доступу грає важливу роль у забезпеченні конфіденційності в хмарному середовищі. Механізми автентифікації та авторизації використовуються для ідентифікації користувачів, перевірки їх прав доступу та обмеження доступу до конфіденційної інформації лише для відповідних осіб.

Фізична безпека: Хмарні провайдери зазвичай приділяють значну увагу фізичній безпеці своїх дата-центрів. Це включає заходи, такі як фізичний доступ до серверів тільки обмеженому персоналу, використання відеоспостереження, біометричної ідентифікації та інших заходів для запобігання несанкціонованому доступу до фізичної інфраструктури.

Цілісність: Цілісність в хмарному середовищі відноситься до збереження та забезпечення недоторканості даних, систем та ресурсів. Основні аспекти цілісності в хмарному середовищі включають наступне:

Захист від несанкціонованих змін: Хмарні провайдери вживають заходів для запобігання несанкціонованим змінам даних. Це включає застосування механізмів контролю цілісності, таких як хеш-функції або цифрові підписи, які дозволяють виявляти будь-які зміни у даних та підтверджувати їх автентичність.

Захист від вразливостей програмного забезпечення: Забезпечення цілісності також включає захист від вразливостей програмного забезпечення, які можуть призвести до змін у системі або даних. Хмарні провайдери регулярно оновлюють та патчують програмне забезпечення, щоб виправляти виявлені вразливості та забезпечувати цілісність систем.

Аудит та моніторинг: Хмарні провайдери здійснюють аудит та моніторинг систем, щоб виявляти будь-які зміни або несправності. Це допомагає виявити порушення цілісності та прийняти відповідні заходи для відновлення даних до надійного стану.

Резервне копіювання та відновлення: Для забезпечення цілісності даних в хмарному середовищі важливо мати механізми резервного копіювання та відновлення. Регулярні резервні копії даних дозволяють відновити дані в разі втрати або пошкодження, забезпечуючи цілісність і доступність інформації.

Захист цілісності даних гарантує, що дані не піддаються незаконним змінам або спотворенню. Використовуються механізми контролю цілісності, такі як хеш-функції або цифрові підписи, для виявлення будь-яких змін у даній та переконання, що дані залишаються недоторканими.

Доступність: Доступність в хмарному середовищі означає, що хмарні послуги повинні бути доступні користувачам у будь-який час і забезпечувати надійну роботу систем та додатків. Основні аспекти доступності в хмарному середовищі включають наступне:

Висока доступність: Хмарні провайдери зазвичай працюють над створенням високодоступних сервісів та інфраструктури. Це означає, що системи хмари мають

бути доступними протягом більшої частини часу, мінімізуючи відмови у роботі та перерви у послугах.

Резервне копіювання та відновлення: Хмарні провайдери зазвичай забезпечують механізми резервного копіювання даних та відновлення систем. Це дозволяє відновлювати дані та послуги в разі виникнення непередбачених проблем, таких як відмови обладнання або природні катастрофи.

Моніторинг та виявлення відмов: Хмарні провайдери використовують системи моніторингу та виявлення відмов для оперативного виявлення проблем і прийняття відповідних заходів для їх вирішення. Це допомагає попереджати відмови та забезпечувати безперебійну роботу сервісів.

Географічна реплікація: Деякі хмарні провайдери пропонують можливість розміщення даних та сервісів на різних географічно розташованих місцях. Це дозволяє забезпечити високу доступність, навіть у разі проблем у конкретному регіоні або дата-центрі.

Безпека в хмарному середовищі також орієнтована на забезпечення надійності та доступності послуг. Застосовуються заходи для попередження відмови обслуговування (DoS) та захисту мережевої інфраструктури від атак. Резервне копіювання даних та реплікація систем забезпечують відновлення послуг у разі виникнення проблем.

1.4 Основні аспекти в захисті безпеки в хмарному середовищі

Основні аспекти в забезпеченні безпеки в хмарному середовищі включають наступні:

Аутентифікація та авторизація: Це включає механізми ідентифікації користувачів і перевірки їх прав доступу до ресурсів. Системи аутентифікації перевіряють ідентичність користувача, тоді як системи авторизації контролюють, до яких ресурсів користувач має доступ.

Шифрування даних: Шифрування даних в хмарному середовищі є ключовим аспектом безпеки. Воно забезпечує конфіденційність та захист від несанкціонованого доступу до даних під час їх передачі та зберігання.

Фізична безпека: Хмарні провайдери повинні забезпечувати фізичну безпеку своїх дата-центрів, де зберігаються сервери та інфраструктура. Це включає контроль доступу до фізичних приміщень, використання систем відеоспостереження, біометричної ідентифікації та інших заходів для запобігання несанкціонованому доступу.

Моніторинг та виявлення вторгнень: Системи моніторингу та виявлення вторгнень використовуються для виявлення аномальної активності або незвичних поведінкових патернів, які можуть свідчити про можливі атаки або порушення безпеки. Це допомагає вчасно реагувати та приймати заходи для запобігання вторгненням.

1.4.1 Обмеження доступу

Обмеження доступу є одним з основних аспектів забезпечення безпеки в хмарному середовищі. Це означає, що лише авторизовані користувачі мають доступ до даних та ресурсів, що знаходяться в хмарі.

Основні методи обмеження доступу в хмарному середовищі включають:

- Автентифікація користувачів за допомогою унікального ідентифікатора та пароля;
- Авторизація доступу до конкретних ресурсів на основі ролей та прав доступу;
- Керування доступом на рівні мережі, що забезпечує контроль доступу до мережевих ресурсів;
- Захист даних під час їх передачі та зберігання в хмарі за допомогою шифрування.

При налагодженні обмежень доступу до хмарних ресурсів необхідно враховувати вимоги до безпеки даних та ресурсів, а також потреби користувачів в доступі до необхідної інформації.

1.4.2 Захист даних

Захист даних в хмарному середовищі є критичним аспектом безпеки. Оскільки дані можуть бути розташовані на серверах, що належать хмарному провайдеру, необхідно приділяти належну увагу їх конфіденційності, цілісності та доступності. Основні аспекти захисту даних в хмарному середовищі включають наступне:

Шифрування даних: Важливим аспектом є шифрування даних під час їх передачі і зберігання. Зашифровані дані непристойні для несанкціонованого доступу, якщо зловмисник отримає доступ до них. Хмарні провайдери зазвичай надають можливості шифрування на різних рівнях, включаючи шифрування на рівні даних, мережі та системи.

Керування доступом: Системи керування доступом встановлюють правила та політики для контролю доступу до даних. Це включає аутентифікацію користувачів, надання різних рівнів авторизації та управління ролями користувачів. Забезпечення потрібних рівнів доступу до даних допомагає уникнути несанкціонованого використання та розголошення інформації.

Резервне копіювання та відновлення: Хмарні провайдери зазвичай надають можливості резервного копіювання даних та відновлення в разі випадкового видалення, помилки або відмови обладнання. Це дозволяє відновити дані до попереднього стану та запобігти втраті важливої інформації.

1.4.3 Відновлення даних

Відновлення даних в хмарному середовищі є важливим аспектом забезпечення безпеки та доступності інформації. Хмарні провайдери зазвичай надають різні механізми та інструменти для відновлення даних в разі випадків, коли виникають проблеми або втрати даних.

Основні методи відновлення даних в хмарному середовищі включають:

Резервне копіювання: Хмарні провайдери зазвичай надають можливості регулярного резервного копіювання даних. Це означає, що ваші дані регулярно

копіюються та зберігаються в іншому місці. У разі втрати або пошкодження даних ви можете відновити їх з резервної копії.

Резервне копіювання є важливим аспектом забезпечення безпеки та відновлення даних в хмарному середовищі. Цей процес включає створення резервних копій даних і їх зберігання в безпечному місці, що дозволяє відновити дані в разі їх втрати або пошкодження.

Основні аспекти резервного копіювання в хмарному середовищі включають:

Регулярність: Резервне копіювання повинно бути проведене регулярно, залежно від потреб вашої організації і важливості даних. Це забезпечить актуальність резервних копій і дозволить відновити дані до останнього збереженого стану.

Політики зберігання: Важливо встановити політики зберігання резервних копій, включаючи тривалість зберігання, частоту створення копій і місце їх зберігання. Наприклад, можна встановити, що копії зберігаються протягом 30 днів і зберігаються на віддаленому сервері або у віртуальному приватному хмарному середовищі.

Перевірка цілісності: Після створення резервної копії важливо перевірити її цілісність. Це можна зробити шляхом порівняння хеш-суми або контрольної суми резервної копії з оригінальними даними. Якщо ці значення збігаються, це означає, що копія була створена правильно і не пошкоджена.

Snapshot-знімки: Snapshot-знімки (знімки стану системи) дозволяють зберегти стан системи та дані на певний момент часу. Вони є корисним інструментом для відновлення системи до попереднього стану у разі виникнення проблем або втрати даних.

Snapshot-знімки (або миттєві знімки) є важливою функцією в хмарних середовищах, яка дозволяє створювати точки відновлення системи або віртуальних машин. Snapshot-знімки фіксують стан системи на певний момент часу, включаючи дані, конфігурацію і стан всіх віртуальних ресурсів.

Основні аспекти snapshot-знімків в хмарному середовищі включають:

Швидкість і ефективність: Створення snapshot-знімків зазвичай відбувається швидко і без впливу на роботу системи. Snapshot-знімки зберігають тільки змінені дані від останнього знімку, що забезпечує ефективне використання ресурсів.

Відновлення та тестування: Snapshot-знімки дозволяють відновити систему до попереднього стану швидко і безпечно. Вони також можуть бути використані для тестування нових конфігурацій або програмного забезпечення без впливу на продуктивні середовища.

Множинні знімки: Хмарні середовища часто дозволяють створювати багато snapshot-знімків, що дозволяє зберігати кілька точок відновлення. Це дає можливість відновлюватися до різних станів системи або вибирати знімок, який найбільш підходить для конкретних потреб.

Маніпуляції зі знімками: Snapshot-знімки можуть бути використані для різних маніпуляцій з системою, наприклад, клонування віртуальних машин, міграції між хмарними обліковими записами або переміщення на інші сервери.

Disaster Recovery: Хмарні провайдери можуть надавати послуги з відновлення після надзвичайних ситуацій (Disaster Recovery). Це включає реплікацію даних на різних географічних місцях, щоб у разі виникнення аварійної ситуації в одному центрі обробки даних, інші резервні копії можна було використовувати для відновлення.

Disaster Recovery (відновлення після надзвичайних ситуацій) в хмарному середовищі є процесом відновлення системи, даних та послуг після виникнення серйозних подій, таких як природні катастрофи, технічні збої, кібератаки або інші надзвичайні обставини. Метою Disaster Recovery є забезпечення безперебійного функціонування бізнесу та мінімізація впливу подій на організацію.

Основні аспекти Disaster Recovery в хмарному середовищі включають:

Реплікація даних: Хмарні провайдери зазвичай забезпечують можливості реплікації даних на різних географічних місцях. Це дозволяє мати резервні копії даних, які можуть бути використані для відновлення після надзвичайних ситуацій.

Відновлення на іншому сервері: У випадку відмови або недоступності одного сервера, Disaster Recovery передбачає відновлення системи та даних на іншому

сервері або в іншому географічному регіоні. Це дозволяє продовжити роботу бізнесу з мінімальними перервами.

Тестування та вправи: Часто проводяться тестування та вправи, щоб перевірити ефективність та ефективність планів відновлення після надзвичайних ситуацій. Це дозволяє виявити слабкі місця та внести необхідні корективи для поліпшення процесу відновлення.

Відновлення на рівні об'єктів: Деякі хмарні середовища надають можливість відновлення окремих об'єктів або файлів без необхідності відновлення всієї системи. Це дозволяє більш гнучко відновлювати окремі компоненти та дані.

Відновлення на рівні об'єктів є важливою можливістю в хмарних середовищах, яка дозволяє відновлювати окремі об'єкти або файли без необхідності відновлення всієї системи. Це надає більшу гнучкість та швидкість відновлення після непередбачених подій або помилок.

Основні аспекти відновлення на рівні об'єктів в хмарному середовищі включають:

Гранульованість відновлення: Замість відновлення всієї системи або віртуальної машини, можна відновлювати лише потрібні об'єкти або файли. Це дозволяє економити час і ресурси, особливо коли необхідно відновити лише окремі компоненти системи.

Швидкість відновлення: Відновлення на рівні об'єктів може бути швидшим, оскільки не потрібно відновлювати всю систему. Відновлення окремих об'єктів може бути виконане швидко та безперервно, що забезпечує мінімальний час перерви в роботі системи.

Вибірковість відновлення: За допомогою відновлення на рівні об'єктів можна вибрати конкретні об'єкти, які потрібно відновити, залежно від їх важливості або пріоритету. Це дозволяє пріоритезувати відновлення і сконцентрувати зусилля на найкритичніших компонентах системи.

1.4.4 План реагування

План реагування на безпеку в хмарному середовищі - це документ, який визначає стратегію та процедури, які необхідно вжити для ефективної реакції на потенційні безпечні події або інциденти. Основна мета плану реагування на безпеку - забезпечити швидку відповідь, відновлення і захист хмарного середовища та даних в разі виникнення проблем.

Основні етапи плану реагування на безпеку в хмарному середовищі включають:

Визначення загроз та ризиків: Ідентифікація потенційних загроз безпеці, таких як кібератаки, витоки даних, втрати доступу тощо. Аналіз ризиків допомагає визначити, наскільки серйозними є ці загрози та як їх можна уникнути або пом'якшити.

Розробка плану реагування на безпеку: Створення документованого плану, який визначає ролі та відповідальність учасників команди реагування на безпеку, процедури виявлення та звітування про інциденти, засоби комунікації, потрібні докладні кроки дій для реагування на різні типи інцидентів.

Виявлення та відстеження інцидентів: Розробка системи виявлення безпекових інцидентів, яка включає в себе використання моніторингових інструментів, журналів подій та систем автоматичного сповіщення. Це дозволяє оперативно виявляти потенційні проблеми і реагувати на них.

Висновки за розділом 1

Під час написання даного розділу було виявленно, які існують хмарні середовища, а саме: загальнодоступні хмарні середовища, приватні хмарні середовища, гібридні хмарні середовища, багатохмарні. Визначено для кого саме вони створені та яким підприємствам підходять.

Також визначені основні аспекти в безпеці хмарного середовища, та визначений принцип роботи безпеки в хмарі.

РОЗДІЛ 2. ВИЗНАЧЕННЯ ІСНУЮЧИХ МЕХАНІЗМІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНОМУ СЕРЕДОВИЩІ

2.1 Засоби захисту інформації в хмарних середовищах

Аналіз засобів захисту інформації в хмарних середовищах - це процес оцінки та вибору найбільш ефективних технологій та практик, щоб захистити дані в хмарі від можливих загроз безпеці. Основні засоби захисту інформації в хмарних середовищах включають:

Криптографію - шифрування даних для захисту їх від несанкціонованого доступу. Криптографічні технології можуть використовуватися для шифрування даних в покоївках хмари, а також для забезпечення безпечного каналу зв'язку між користувачем та хмарою.

Аутентифікацію та авторизацію - це процеси перевірки ідентифікації користувача та визначення прав доступу до різних даних та ресурсів в хмарі.

Мережеві засоби захисту - включають в себе файрволи, системи виявлення вторгнень та інші засоби, які можуть бути використані для захисту мережевих з'єднань та даних в хмарі.

Засоби моніторингу та аудиту - слідкування за даними в хмарі, щоб виявити можливі атаки або незвичайну поведінку.

Захист резервних копій - забезпечення збереження резервних копій даних в безпечному місці та забезпечення їх достатньої захищеності для забезпечення можливості відновлення даних у разі втрати.

Політики та процедури безпеки - документовані процедури, які визначають, які дії слід здійснювати у разі виявлення атак або інших загроз для безпеки в хмарному середовищі.

Освіта користувачів - надання користувачам хмарних сервісів необхідної освіти та навчання з питань безпеки, щоб забезпечити свідоме використання сервісів та зменшити ризики.

Важливо враховувати, що безпека в хмарних середовищах - це спільна відповідальність між хмарним провайдером і користувачем. Перед вибором хмарного провайдера рекомендується детально ознайомитись з його заходами безпеки та політиками, а також заслухати рекомендації та кращі практики від провайдера для забезпечення найвищого рівня безпеки даних.

Аналіз засобів захисту інформації в хмарних середовищах включає оцінку різних аспектів безпеки, які забезпечуються хмарним провайдером. Ось деякі ключові засоби захисту, які слід розглянути:

Аутентифікація та авторизація: Хмарні середовища повинні мати механізми аутентифікації, що дозволяють перевіряти ідентичність користувачів та надавати їм відповідний рівень доступу до ресурсів. Це може включати використання множини факторів аутентифікації, таких як паролі, токени або біометричні дані.

Шифрування даних: Важлива функція забезпечення конфіденційності даних в хмарних середовищах. Дані повинні бути шифровані під час передачі між користувачем та хмарним сервером, а також під час зберігання на серверах. Використання шифрування забезпечує захист від несанкціонованого доступу до даних.

Фізична безпека дата-центру: Хмарні провайдери повинні забезпечувати високий рівень фізичної безпеки своїх дата-центрів, включаючи контроль доступу, відеоспостереження, пожежну безпеку та захист від стихійних лих. Це допомагає захистити фізичні ресурси, на яких зберігаються дані користувачів.

Виявлення та запобігання інцидентів безпеки: Хмарні середовища повинні мати механізми для виявлення та моніторингу потенційних загроз безпеці. Це може включати системи реєстрації подій (логування), системи виявлення вторгнень (IDS/IPS) та автоматизовані механізми виявлення зламів.

Резервне копіювання та відновлення: Хмарні провайдери зазвичай забезпечують можливості резервного копіювання та відновлення даних. Це включає створення резервних копій даних та можливість швидкого відновлення в разі випадкового видалення або випадку відмови.

Сегрегація даних: Забезпечення відокремленості даних між різними користувачами та організаціями в хмарному середовищі. Це допомагає запобігти несанкціонованому доступу до чужих даних та зберегти конфіденційність.

Аудит безпеки: Хмарні провайдери повинні мати механізми аудиту безпеки, які відстежують активності користувачів і системи для виявлення вразливостей або недоліків у захисті.

Ці засоби захисту в хмарних середовищах можуть варіюватися залежно від конкретного хмарного провайдера та рівня послуг, які надаються. Важливо здійснювати оцінку безпеки перед вибором хмарного провайдера та добре розуміти, які заходи захисту вони надають.

Основні аспекти відновлення на рівні об'єктів в хмарному середовищі включають:

Гранульованість відновлення: Замість відновлення всієї системи або віртуальної машини, можна відновлювати лише потрібні об'єкти або файли. Це дозволяє економити час і ресурси, особливо коли необхідно відновити лише окремі компоненти системи.

Швидкість відновлення: Відновлення на рівні об'єктів може бути швидшим, оскільки не потрібно відновлювати всю систему. Відновлення окремих об'єктів може бути виконане швидко та безперервно, що забезпечує мінімальний час перерви в роботі системи.

Вибірковість відновлення: За допомогою відновлення на рівні об'єктів можна вибрати конкретні об'єкти, які потрібно відновити, залежно від їх важливості або пріоритету. Це дозволяє пріоритезувати відновлення і сконцентрувати зусилля на найкритичніших компонентах системи.

2.2 Шифрування даних

Шифрування даних в хмарному середовищі є важливим механізмом захисту, який допомагає забезпечити конфіденційність і цілісність інформації. Ось декілька

аспектів, які можна проаналізувати при вивченні засобів шифрування даних в хмарному середовищі:

Типи шифрування: Перевірте, які типи шифрування підтримуються хмарним провайдером. Це може включати шифрування на рівні даних, дискове шифрування і шифрування каналу зв'язку.

Керування ключами: Розгляньте, як відбувається керування ключами шифрування. Важливо, щоб ключі були належним чином керовані і захищені від несанкціонованого доступу.

Локалізація шифрування: Де точно відбувається шифрування даних? Де знаходяться ключі шифрування? Важливо визначити, чи шифруються дані в хмарному середовищі, на клієнтському пристрої або в обох місцях.

Аутентифікація та авторизація: Розгляньте, як відбувається аутентифікація та авторизація для доступу до зашифрованих даних. Чи використовуються додаткові механізми безпеки, такі як багаторівнева аутентифікація?

Аудит та журналювання: Переконайтеся, що в хмарному середовищі ведеться аудит та журналювання шифрування даних. Це допоможе виявити можливі проблеми з безпекою та вести слідство в разі інцидентів.

Зовнішнє шифрування: Деякі хмарні середовища надають можливість застосовувати зовнішнє шифрування, коли дані шифруються перед тим, як вони надходять в хмарне середовище. Розгляньте цю опцію для додаткового рівня захисту.

Виконання стандартів безпеки: Переконайтеся, що хмарний провайдер виконує відповідні стандарти безпеки, такі як ISO 27001, SOC 2, HIPAA, GDPR та інші, залежно від контексту вашої організації.

Кожен хмарний провайдер може мати власні механізми та інструменти для шифрування даних. Важливо оцінити їхні можливості та відповідність вашим потребам з точки зору конфіденційності і безпеки даних.

Застосування шифрування даних під час збереження, передачі і обробки є важливим аспектом безпеки в хмарному середовищі. Використовуються різні види шифрування, включаючи шифрування на рівні даних, дискове шифрування і шифрування каналу зв'язку.

Шифрування даних є важливим засобом захисту інформації в хмарному середовищі. Для шифрування даних в хмарних середовищах можуть використовуватися різні методи і засоби. Основні з них:

Шифрування на рівні додатку: програми використовують шифрування для захисту конфіденційної інформації перед її передачею в хмарне середовище.

Шифрування на рівні з'єднання: транспортний протокол TLS / SSL забезпечує шифрування даних між клієнтом і сервером під час передачі через мережу.

Шифрування на рівні зберігання: деякі хмарні сервіси надають можливість шифрування даних на рівні зберігання за допомогою різних методів, таких як серверне шифрування, шифрування на стороні клієнта та шифрування на рівні об'єкту.

Шифрування на рівні бази даних: багато реляційних баз даних підтримують шифрування на рівні бази даних, що дозволяє шифрувати дані в репліках та резервних копіях.

Шифрування на рівні файлової системи: деякі хмарні сервіси підтримують шифрування на рівні файлової системи, яке дозволяє захистити дані від несанкціонованого доступу, в тому числі під час зберігання на мережевих пристроях.

Вибір методу та засобу шифрування даних залежить від типу даних, які потрібно захистити, а також від можливостей та обмежень хмарного середовища, в якому вони зберігаються.

2.3 Засоби виявлення та запобігання вторгнень (IDS/IPS)

Засоби виявлення та запобігання вторгнень (IDS/IPS) в хмарних середовищах мають важливе значення для забезпечення безпеки і захисту даних користувачів. Такі засоби дозволяють виявляти та блокувати шкідливі атаки на ранніх стадіях та зменшують ризик витоку конфіденційної інформації.

Основні функції IDS/IPS включають виявлення та аналіз мережевих та системних подій, визначення вразливостей та потенційних загроз, виявлення аномальної поведінки та блокування шкідливих атак. IDS/IPS здатні реагувати на

різні типи атак, такі як DDoS-атаки, атаки на рівні додатків, атаки на рівні мережі, віруси, шпигунське програмне забезпечення та інші.

Деякі хмарні платформи, такі як Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure, пропонують власні засоби IDS/IPS для захисту користувачів. Крім того, існують такі популярні засоби IDS/IPS для хмарних середовищ, як Alert Logic, Dome9 Security, Sophos та інші.

При виборі засобу IDS/IPS важливо враховувати такі фактори, як підтримка хмарних платформ, можливості конфігурації та інтеграції з іншими засобами захисту даних. Також слід звернути увагу на вартість та обсяг послуг, які надає засіб, і переконатися, що він відповідає потребам та бюджету компанії.

Засоби виявлення та запобігання вторгнень (Intrusion Detection and Prevention Systems, IDS/IPS) є важливою складовою безпеки в хмарних середовищах. Вони допомагають виявляти та реагувати на потенційні загрози та атаки на інфраструктуру хмарного середовища. Деякі ключові аспекти засобів виявлення та запобігання вторгнень в хмарних середовищах включають:

Моніторинг мережевої активності: IDS/IPS аналізують мережевий трафік у реальному часі, виявляючи аномальну або підозрілу активність. Це включає виявлення незвичайного трафіку, спроб злому, відправку шкідливих пакетів тощо.

Аналіз журналів подій: IDS/IPS аналізують журнали подій, що відображають активність в хмарному середовищі, для виявлення підозрілих дій або подій, що вказують на вторгнення.

Виявлення шкідливого програмного забезпечення: IDS/IPS використовують різні методи, такі як сигнатури, поведінковий аналіз та машинне навчання, для виявлення шкідливих програм або коду в хмарному середовищі.

Запобігання атакам: IDS/IPS виконують проактивні заходи для запобігання атакам, таким як блокування IP-адрес, фільтрація пакетів, відмова в обслуговуванні (DoS) тощо.

Реагування на вторгнення: IDS/IPS можуть надавати можливості автоматичної реакції на виявлені вторгнення, наприклад, блокування атакуючого джерела або виконання інших заходів для забезпечення безпеки.

Важливо враховувати, що засоби виявлення та запобігання вторгнень в хмарних середовищах повинні бути настроєні та підтримувані відповідно до специфічних потреб та вимог організації. Також слід поєднувати їх з іншими заходами безпеки, такими як сегментація мережі, автентифікація та авторизація, шифрування даних та резервне копіювання, для створення комплексної системи захисту в хмарному середовищі.

Ці засоби виявляють і блокують спроби несанкціонованого доступу, атаки і небажану активність в хмарному середовищі.

Засоби виявлення та запобігання вторгнень (Intrusion Detection and Prevention Systems, IDS/IPS) в хмарних середовищах відіграють важливу роль у забезпеченні безпеки. Деякі основні аспекти та засоби, які використовуються для виявлення та запобігання вторгнень в хмарному середовищі, включають:

Моніторинг мережі: IDS/IPS системи надають здатність до моніторингу мережевого трафіку в хмарному середовищі. Вони аналізують мережеві пакети, щоб виявити незвичайні або підозрілі активності, такі як невдалі спроби аутентифікації, сканування портів або атаки DDoS.

Виявлення вторгнень в хмарні сервіси: IDS/IPS системи можуть бути налаштовані для виявлення вторгнень в різні хмарні сервіси, такі як веб-сервери, бази даних або сховища даних. Вони аналізують активність та знаки незвичайної поведінки, що може вказувати на спроби несанкціонованого доступу до цих сервісів.

Аналіз журналів подій: IDS/IPS системи можуть аналізувати журнали подій в хмарному середовищі, щоб виявляти незвичайні або підозрілі активності. Вони шукають патерни або ознаки, що можуть свідчити про атаки або компрометацію системи.

Правила та сигнатури: IDS/IPS системи використовують набори правил та сигнатур, які визначають типові атаки та аномалії. Вони порівнюють активність в хмарному середовищі з цими правилами та сигнатурами, щоб виявити вторгнення.

Реал-тайм сповіщення та реагування: IDS/IPS системи надають можливість реагування в реальному часі на виявлені вторгнення. Вони можуть надсилати сповіщення адміністраторам про підозрілу активність та вживати заходів для

запобігання подальшим атакам, таких як блокування IP-адрес атакуючого або відключення скомпрометованого ресурсу.

Враховуючи швидкість зміни загроз та характеристики хмарних середовищ, ефективні засоби виявлення та запобігання вторгнень повинні мати гнучкість, масштабованість та здатність до автоматизації, щоб виявляти нові типи атак та захищати ресурси в реальному часі.

2.4 Файрволи

Фаєрвол - це засіб контролю руху мережевих пакетів на вході та виході з мережі. У хмарному середовищі фаєрвол може бути використаний для захисту віртуальних машин та додатків від шкідливих атак з мережі Інтернет.

Основні функції фаєрволу в хмарному середовищі:

Контроль доступу: Фаєрвол може бути налаштований для блокування небезпечного трафіку з мережі Інтернет та обмеження доступу до віртуальних машин або додатків з певних мереж.

Виявлення та блокування вторгнень: Фаєрвол може бути налаштований для виявлення та блокування шкідливого трафіку з мережі Інтернет, що спрямовується на віртуальні машини та додатки.

Контроль мережевих портів: Фаєрвол може бути налаштований для контролю доступу до певних мережевих портів на віртуальних машинах та додатках. Це може бути корисним для обмеження доступу до певних послуг або даних.

Моніторинг трафіку: Фаєрвол може вести журнал дій, пов'язаних з мережевим трафіком, що проходить через нього. Це дозволяє виявляти аномальну поведінку та атаки на віртуальні машини та додатки.

В хмарному середовищі фаєрвол може бути надійним засобом захисту від шкідливого трафіку з мережі Інтернет. Однак, варто пам'ятати, що налаштування фаєрволу повинно бути відповідним до потреб конкретної хмарної інфраструктури та дотримуватись найкращих практик захисту від атак з мережі.

Фаєрвол (firewall) в хмарному середовищі є одним з основних засобів захисту мережі та даних від несанкціонованого доступу та зловмисних атак. Він дозволяє контролювати трафік, що входить і виходить з хмарного середовища, і виконує функції фільтрації, маршрутизації та мережевої безпеки. Основні аспекти та переваги фаєрволу в хмарному середовищі включають:

Контроль доступу: Фаєрвол встановлює правила контролю доступу, які визначають, які мережеві з'єднання та протоколи дозволені або заборонені. Це дозволяє обмежити доступ до ресурсів хмарного середовища лише для авторизованих користувачів або систем.

Фільтрація трафіку: Фаєрвол аналізує мережевий трафік, фільтрує його і виявляє підозрілі або шкідливі пакети. Він може блокувати атаки, такі як переповнення буферу, SQL-ін'єкції, кросс-сайтові скрипти та інші.

Захист мережевого периметру: Фаєрвол служить як захисний шар на мережевому периметрі хмарного середовища. Він виконує функцію мережевої безпеки, що допомагає захистити ресурси від зовнішніх загроз, таких як атаки з мережі Інтернет.

Інтеграція з іншими засобами безпеки: Фаєрволи в хмарному середовищі можуть інтегруватись з іншими засобами безпеки, такими як системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), для створення багатошарового підходу до безпеки.

Масштабованість: Фаєрволи в хмарному середовищі повинні мати можливість масштабування в залежності від потреби. Вони повинні бути здатні обробляти великий обсяг мережевого трафіку і забезпечувати ефективний контроль доступу навіть у розподіленому середовищі.

Автоматизація: Фаєрволи в хмарному середовищі можуть бути управляні за допомогою інструментів автоматизації, таких як API або інструменти інфраструктури як коду. Це дозволяє швидко налаштовувати, розгортати та керувати політиками безпеки.

Журналювання та аудит: Фаєрволи можуть вести журнал подій та аудитувати мережеву активність. Це дозволяє адміністраторам відстежувати та аналізувати події,

виявляти вразливості та зловмисні дії, а також забезпечувати відповідність вимогам регуляторів.

Ураховуючи потреби безпеки в хмарних середовищах, важливо ретельно аналізувати функціональність, можливості та сумісність фаєрволів, щоб вибрати найбільш підходящий засіб захисту інформації в конкретному випадку.

Фаєрвол (firewall) в хмарному середовищі відіграє важливу роль у забезпеченні безпеки мережі та даних. Він допомагає контролювати трафік, що входить і виходить з хмарного середовища, та застосовує набір правил для фільтрації та блокування небажаного трафіку. Основні аспекти та переваги фаєрволу в хмарному середовищі включають:

Сегментація мережі: Фаєрвол дозволяє створювати віртуальні мережеві сегменти (сегментування) в хмарному середовищі. Це дозволяє ізолювати різні частини інфраструктури та додатків одна від одної, забезпечуючи вищий рівень безпеки.

Контроль доступу: Фаєрвол встановлює правила доступу, які визначають, які типи трафіку можуть пройти через мережу хмарного середовища. Це дозволяє обмежувати доступ до ресурсів та додатків лише для авторизованих користувачів та джерел.

Фільтрація трафіку: Фаєрвол може фільтрувати трафік згідно заданих правил, включаючи блокування шкідливого, небажаного або небезпечного трафіку. Він може розпізнавати і блокувати атаки, спам, шкідливі програми та інші загрози безпеці.

Журналювання та аудит: Фаєрвол може здійснювати журналювання подій та аудит активності мережі. Це дозволяє виявляти та відстежувати ненормальну або підозрілу активність, а також аналізувати історію подій для виявлення потенційних загроз безпеці.

Автоматизація та оркестрація: Фаєрволи в хмарних середовищах можуть бути інтегровані з інструментами автоматизації та оркестрації, що дозволяє реалізувати автоматичне впровадження та управління правилами фаєрволу.

Масштабованість: Фаєрвол в хмарному середовищі повинен бути здатний масштабуватися відповідно до зростання обсягу трафіку та мережевих ресурсів. Він

повинен забезпечувати ефективне управління трафіком навіть при великому обсязі даних.

У хмарних середовищах можуть бути використані як внутрішні, так і зовнішні фаєрволи. Внутрішні фаєрволи контролюють трафік в межах хмарного середовища, в той час як зовнішні фаєрволи контролюють трафік між хмарним середовищем та зовнішніми мережами.

2.5 Ідентифікація та аутентифікація

Засоби ідентифікації та аутентифікації в хмарному середовищі грають важливу роль у забезпеченні безпеки доступу до ресурсів та даних. Основні аспекти та функціональні можливості засобів ідентифікації та аутентифікації в хмарному середовищі включають:

Багаторівнева аутентифікація: Засоби ідентифікації та аутентифікації в хмарному середовищі підтримують багаторівневу аутентифікацію, що дозволяє встановити кілька рівнів перевірки для підтвердження ідентичності користувача. Це може включати використання паролів, одноразових паролів, біометричних даних, апаратних токенів тощо.

Одноосібна ідентифікація: Засоби ідентифікації в хмарному середовищі дозволяють створювати унікальні ідентифікатори для кожного користувача та ресурсу. Це дозволяє встановити точну ідентичність користувача, що отримує доступ до ресурсів.

Централізоване управління доступом: Засоби ідентифікації та аутентифікації в хмарному середовищі дозволяють централізовано управляти доступом до ресурсів. Це означає, що адміністратори можуть встановлювати та керувати правами доступу користувачів до окремих ресурсів, додатків та сервісів.

Одноакаунтна аутентифікація: Засоби ідентифікації в хмарному середовищі дозволяють користувачам використовувати один обліковий запис (акаунт) для доступу до різних сервісів та ресурсів. Це спрощує процес аутентифікації та забезпечує єдиноцтво керування доступом.

Федерація ідентичності: Засоби ідентифікації в хмарному середовищі підтримують федерацію ідентичності, що дозволяє обмінюватися інформацією про ідентичність користувача між різними хмарними сервісами та постачальниками. Це забезпечує зручність та безпеку при роботі з різними сервісами в хмарному середовищі.

Множинні фактори аутентифікації: Засоби ідентифікації в хмарному середовищі підтримують використання множинних факторів аутентифікації, таких як щось, що ви знаєте (наприклад, пароль), щось, що ви маєте (наприклад, фізичний токен), і щось, що ви є (наприклад, біометричні дані). Це покращує безпеку доступу до хмарних ресурсів.

Журналювання та моніторинг: Засоби ідентифікації та аутентифікації в хмарному середовищі забезпечують журналювання та моніторинг дій користувачів, що мають доступ до ресурсів. Це дозволяє виявляти та реагувати на можливі незвичайні або підозрілі активності.

Ці засоби сприяють забезпеченню безпеки доступу та захисту інформації в хмарному середовищі. Вибір конкретних засобів залежить від потреб організації, рівня конфіденційності даних та регуляторних вимог.

Засоби ідентифікації та аутентифікації в хмарних середовищах грають ключову роль у забезпеченні безпеки та доступу до ресурсів. Вони дозволяють перевіряти та підтверджувати ідентичність користувачів та контролювати їх доступ до різних сервісів та даних. Деякі засоби ідентифікації та аутентифікації, які використовуються в хмарних середовищах, включають:

Логін та пароль: Це найпоширеніший метод аутентифікації, при якому користувачі вводять свій ідентифікатор (логін) та пароль для входу в хмарне середовище. Цей метод може бути посилено за допомогою вимог до складності паролів, багатофакторної аутентифікації та інших заходів безпеки.

Багатофакторна аутентифікація (MFA): Цей метод включає в себе використання двох або більше факторів для підтвердження ідентичності користувача. Це може бути поєднання логіну та пароля з кодом, отриманим на мобільний пристрій, відбитком пальця, візуальним підтвердженням та іншими факторами.

Сертифікати та ключі: Використання цифрових сертифікатів та ключів дозволяє аутентифікувати користувачів та перевіряти цілісність та конфіденційність даних. Це особливо важливо для захисту комунікації між різними компонентами хмарного середовища.

Федерація та один раз ідентифікація (Single Sign-On, SSO): Ці механізми дозволяють користувачам використовувати одні й ті ж облікові дані для доступу до різних сервісів і додатків в хмарному середовищі. Вони спрощують процес аутентифікації та поліпшують зручність для користувачів.

Рольова модель доступу: Цей механізм дозволяє адміністраторам хмарного середовища призначати різні ролі та права доступу для користувачів в залежності від їхніх обов'язків та потреб. Це дозволяє забезпечити принцип найменшого привілею та обмежити доступ користувачів лише до необхідних ресурсів.

Управління ідентичністю та доступом (Identity and Access Management, IAM): Це комплексні системи, які дозволяють управляти ідентифікацією, аутентифікацією та авторизацією користувачів в хмарному середовищі. Вони забезпечують централізоване керування правами доступу, аудит дій користувачів та інші функції безпеки.

Ці засоби захисту ідентифікації та аутентифікації в хмарних середовищах допомагають забезпечити безпеку доступу до ресурсів та запобігти несанкціонованому доступу до даних та сервісів. Важливо враховувати вимоги безпеки та вибрати найбільш підходящі засоби залежно від конкретних потреб та вимог вашого хмарного середовища.

2.6 Фізична безпека

Фізична безпека в хмарному середовищі є критично важливим аспектом забезпечення безпеки даних та інфраструктури. Організації, що надають хмарні послуги, забезпечують різноманітні заходи для фізичної безпеки своїх дата-центрів та інфраструктури. Ось деякі аспекти, які слід враховувати при аналізі засобів фізичної безпеки в хмарному середовищі:

Дата-центри: Провайдери хмарних послуг зазвичай розміщують свої сервери та інфраструктуру в власних дата-центрах. Ці дата-центри мають бути фізично захищені, з контрольованим доступом та обмеженим фізичним доступом до них. Фізична безпека включає в себе заходи, такі як відеоспостереження, системи контролю доступу, багаторівневу аутентифікацію та фізичні бар'єри для запобігання несанкціонованому доступу.

Резервне живлення: Дата-центри хмарних послуг мають мати надійні системи резервного живлення, такі як дизель-генератори, UPS (несперeджуючі джерела живлення) та інші резервні джерела живлення. Це дозволяє забезпечити неперервну роботу інфраструктури хмарного середовища навіть у випадку відключення основного живлення.

Фізичне розташування: Розташування дата-центрів може бути важливим аспектом фізичної безпеки. Деякі провайдери хмарних послуг розташовують свої дата-центри в географічно розподілених областях для забезпечення відмовостійкості та захисту від природних катастроф.

Захист від вторгнень: Фізична безпека також включає захист від фізичних вторгнень до дата-центрів. Це може включати системи контролю доступу, відеоспостереження, безпекову охорону та інші заходи для запобігання несанкціонованому доступу до інфраструктури.

Захист обладнання: Важливо також забезпечити фізичний захист обладнання, яке зберігає та обробляє дані в хмарному середовищі. Це може включати захист від відключення обладнання, крадіжки або пошкодження фізичних пристроїв.

Враховуючи ці аспекти фізичної безпеки, важливо обрати провайдера хмарних послуг, який надає високі стандарти безпеки та захисту даних. Ретельне аудитування та оцінка фізичної безпеки провайдера може допомогти вам забезпечити надійність та конфіденційність ваших даних в хмарному середовищі.

Фізична безпека в хмарному середовищі включає заходи, що забезпечують безпеку фізичного інфраструктурного середовища, включаючи дата-центри та обладнання, що використовується для зберігання та обробки даних в хмарному середовищі. Деякі з аспектів фізичної безпеки в хмарних середовищах включають:

Доступ до дата-центру: Хмарні провайдери мають контролювати та обмежувати фізичний доступ до своїх дата-центрів. Це може включати фізичні бар'єри, такі як огорожі, шлагбауми та контроль доступу, також ідентифікацію і аутентифікацію персоналу, що має доступ до дата-центру.

Відеоспостереження: Використання відеоспостереження в дата-центрах може забезпечити постійний моніторинг і виявлення незвичайних або підозрілих дій. Відеокамери можуть бути розташовані на ключових місцях, щоб фіксувати всі дії, а також реєструвати доступ до приміщень.

Контроль доступу: Застосування систем контролю доступу, таких як електронні картки або біометричні системи, дозволяє обмежити фізичний доступ до обладнання та приміщень в дата-центрі. Це допомагає запобігти несанкціонованому доступу та забезпечити, що тільки авторизованим особам надається фізичний доступ.

Безпека приміщень: Заходи безпеки повинні бути прийняті для захисту фізичних приміщень, включаючи вогнестійкість, контроль температури та вологості, захист від повені та інших природних катастроф.

Резервне живлення: Забезпечення безперебійного живлення та резервного джерела живлення є важливим аспектом фізичної безпеки в хмарних середовищах. Це гарантує, що дата-центр продовжує працювати навіть при випадку відмови основного джерела живлення.

Ці заходи фізичної безпеки спрямовані на забезпечення надійності та захисту фізичної інфраструктури хмарного середовища. Важливо, щоб хмарні провайдери дотримувалися найвищих стандартів безпеки та забезпечували відповідність з регуляторними вимогами та нормативами.

Фізична безпека в хмарному середовищі включає заходи, спрямовані на захист фізичної інфраструктури, де знаходяться сервери, мережеве обладнання та інші компоненти хмарного середовища. Основна мета фізичної безпеки полягає в запобіганні фізичному доступу до цих пристроїв та забезпеченні їхньої безперебійної роботи. Деякі засоби фізичної безпеки, які використовуються в хмарних середовищах, включають:

Дата-центри: Хмарні постачальники використовують власні дата-центри для розміщення своєї інфраструктури. Ці дата-центри зазвичай мають високу рівень безпеки, включаючи фізичні бар'єри, контроль доступу, відеоспостереження, пожежну безпеку та інші заходи.

Контроль доступу: У дата-центрах хмарних постачальників встановлюються строгі заходи контролю доступу. Це можуть бути фізичні бар'єри, які обмежують фізичний доступ до приміщень з серверами, використання пропускних систем, біометричних методів ідентифікації, карточок доступу та інших технологій.

Відеоспостереження: В дата-центрах зазвичай встановлюються системи відеоспостереження, які наглядають за зонами з розміщеними серверами та іншими цінними активами. Це допомагає виявляти незвичайну або підозрілу активність та забезпечує ведення журналів для аналізу подій.

Контроль пожежі та аварійного відновлення: Дата-центри хмарних постачальників мають системи пожежної безпеки, такі як пожежний спринклерний системи, детектори диму, автоматичні системи гасіння та інші протипожежні заходи. Крім того, вони також використовують механізми аварійного відновлення, щоб забезпечити безперебійну роботу в разі виникнення непередбачених ситуацій.

Резервне копіювання та відновлення: Хмарні постачальники зазвичай мають механізми резервного копіювання та відновлення даних. Це включає регулярне створення резервних копій даних та можливість відновлення даних в разі втрати або пошкодження.

Фізична охорона: Дата-центри можуть бути охороняються фізичною охороною, яка забезпечує безпеку і контроль доступу до обладнання та приміщень.

Аудит та ведення журналів: Хмарні постачальники зазвичай ведуть журнали подій та забезпечують аудит доступу до систем і даних. Це дозволяє виявляти та реагувати на потенційні загрози безпеці та проводити аналіз інцидентів.

Ці заходи фізичної безпеки в хмарних середовищах допомагають забезпечити безпеку і недоступність фізичної інфраструктури від несанкціонованого доступу та можливих загроз. Вони сприяють забезпеченню надійності та безперебійності хмарних сервісів для користувачів.

2.7 Резервне копіювання та відновлення

Засоби резервного копіювання та відновлення в хмарному середовищі грають важливу роль у забезпеченні безпеки та доступності даних. Основна мета цих засобів полягає в створенні резервних копій даних і можливості відновлення їх в разі втрати, пошкодження або непередбачених подій. Основні аспекти аналізу засобу резервного копіювання та відновлення в хмарному середовищі включають:

Широкий вибір рішень: Хмарні постачальники пропонують різноманітні засоби резервного копіювання та відновлення, які можуть включати автоматичне резервне копіювання, реплікацію даних, снапшоти, резервне копіювання на зовнішні носії, облікові записи на відновлення та інші. Користувачі мають можливість вибрати найбільш підходящі рішення залежно від своїх потреб та бюджету.

Автоматизація процесу: Хмарні постачальники забезпечують можливість автоматизованого резервного копіювання та відновлення даних. Це означає, що користувачам не потрібно вручну налаштовувати та виконувати процес резервного копіювання, а замість цього вони можуть використовувати автоматичні рішення, які періодично створюють резервні копії даних згідно з визначеними політиками.

Гнучкість політик резервного копіювання: Засоби резервного копіювання в хмарному середовищі дозволяють користувачам налаштовувати різні політики резервного копіювання залежно від потреб. Це включає регулярність створення резервних копій, тривалість зберігання, інтервали архівування та інші параметри. Користувачі можуть налаштувати політики резервного копіювання згідно зі своїми вимогами та враховувати рівень критичності даних.

Можливість відновлення на різних рівнях: Засоби резервного копіювання в хмарному середовищі зазвичай надають можливість відновлення даних на різних рівнях. Це може включати відновлення окремих файлів, баз даних, віртуальних машин або навіть цілих середовищ. Користувачі мають можливість вибрати необхідний рівень відновлення залежно від обсягу даних та часу, необхідного для відновлення.

Захист даних: Засоби резервного копіювання в хмарному середовищі забезпечують захист даних під час їх передачі та зберігання. Вони використовують різні механізми шифрування для забезпечення конфіденційності та цілісності даних під час резервного копіювання та відновлення.

Моніторинг та керування: Засоби резервного копіювання в хмарному середовищі забезпечують можливість моніторингу та керування процесом резервного копіювання. Користувачі можуть отримувати звіти, сповіщення та статистику щодо виконання резервного копіювання, а також керувати параметрами та політиками через веб-інтерфейс або API.

Аналіз засобу резервного копіювання та відновлення в хмарному середовищі допомагає оцінити його ефективність, гнучкість та відповідність вимогам безпеки та бізнесу користувача. Кожен засіб має свої переваги та обмеження, тому важливо враховувати конкретні потреби організації та здійснювати вибір засобу, що найкраще відповідає вимогам безпеки та відновлення даних в хмарному середовищі.

Засоби резервного копіювання та відновлення в хмарному середовищі грають важливу роль у забезпеченні безпеки даних та можливості їх відновлення в разі втрати або пошкодження. Основні характеристики та переваги таких засобів можуть включати:

Автоматичність: Засоби резервного копіювання в хмарних середовищах часто пропонують автоматичне планування та виконання резервного копіювання. Це дозволяє налаштувати регулярні резервні копії відповідно до заданих правил без необхідності ручного втручання.

Гнучкість: Засоби резервного копіювання в хмарних середовищах зазвичай надають гнучкі налаштування, що дозволяє визначати, які дані копіювати, як часто виконувати резервне копіювання та як триватиме зберігання копій. Це дозволяє вам вибрати оптимальні параметри відповідно до потреб вашої організації.

Інкрементальне копіювання: Засоби резервного копіювання в хмарних середовищах зазвичай підтримують інкрементальне копіювання, що означає, що лише змінені або нові дані копіюються, замість повного копіювання всієї інформації.

Це ефективно використовує обсяг сховища і зменшує час, необхідний для виконання резервного копіювання.

Планування відновлення: Засоби відновлення в хмарних середовищах надають можливості для планування процесу відновлення, включаючи пріоритет відновлення різних систем і додатків, відновлення поетапно чи масштабоване відновлення. Це дозволяє бізнесу ефективно відновлювати послуги після інциденту та зменшує вплив на продуктивність.

Тестування відновлення: Деякі засоби резервного копіювання в хмарних середовищах надають можливість проводити тестування відновлення, що дозволяє перевірити ефективність процесу відновлення та впевнитися, що дані можуть бути успішно відновлені у разі необхідності.

Географічна розподіленість: Деякі хмарні постачальники пропонують можливість зберігання резервних копій даних у різних географічних регіонах. Це забезпечує додатковий рівень захисту від природних або технологічних катастроф, що можуть спричинити втрату даних.

Враховуючи ці аспекти, засоби резервного копіювання та відновлення в хмарних середовищах забезпечують надійний і ефективний механізм забезпечення безпеки даних та можливості швидкого відновлення у разі виникнення непередбачених ситуацій.

Висновки за розділом 2

В ході написання даного розділу було проведено аналіз засобів захисту інформації в хмарних середовищах та виокремено найбільш ефективних технологій та практики, щоб захистити дані в хмарі від можливих загроз безпеці.

Також важливо враховувати, що безпека в хмарних середовищах - це спільна відповідальність між хмарним провайдером і користувачем. Перед вибором хмарного провайдера рекомендується детально ознайомитись з його заходами безпеки та політиками, а також заслухати рекомендації та кращі практики від провайдера для забезпечення найвищого рівня безпеки даних.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ДЛЯ ПОКРАЩЕННЯ ЗАХИСТУ В ХМАРНОМУ СЕРЕДОВИЩІ SALESFORSE

3.1 Розгляд хмарного середовища Salesforse

Salesforce - це хмарне середовище, спеціалізоване на CRM (управління взаємодіями з клієнтами) та автоматизації маркетингу. Воно пропонує набір рішень для підтримки різних аспектів бізнесу, зокрема продажів, обслуговування клієнтів, маркетингу та аналітики.

Особливості та переваги хмарного середовища Salesforce:

CRM-орієнтовані послуги: Salesforce надає широкий спектр послуг, спрямованих на управління клієнтами. Це включає управління продажами, контактами, обслуговуванням клієнтів, маркетингом та аналітикою. Salesforce CRM дозволяє організаціям ефективно взаємодіяти зі своїми клієнтами та забезпечує інструменти для покращення процесів продажу та обслуговування.

Хмарна архітектура: Salesforce базується на хмарній архітектурі, що означає, що вся інфраструктура та програмне забезпечення знаходяться в хмарі. Це забезпечує високу доступність, гнучкість та масштабованість, оскільки користувачі можуть отримувати доступ до системи з будь-якого місця за допомогою Інтернету.

Персоналізованість та розширюваність: Salesforce надає можливість налаштування та розширення функціональності відповідно до потреб конкретної організації. Це означає, що бізнес може налаштовувати модулі та робочі процеси, щоб вони відповідали їх унікальним вимогам.

Маркетплейс додатків: Salesforce має широкий вибір додатків та розширень, які можуть бути використані для розширення функціональності платформи. Це дозволяє організаціям знаходити та використовувати готові рішення для покращення бізнес-процесів.

Аналітика та звітність: Salesforce надає розширені можливості аналітики та звітності, що дозволяють організаціям отримувати уявлення про важливі дані, тренди

та ключові показники продуктивності. Це допомагає приймати обґрунтовані рішення та визначати стратегії для покращення результатів.

Безпека та захист даних: Salesforce приділяє велику увагу безпеці та захисту даних. Вони використовують різноманітні заходи безпеки, такі як шифрування даних, механізми автентифікації та авторизації, захист від злому та моніторинг безпеки, щоб забезпечити конфіденційність, цілісність та доступність даних.

Мобільність: Salesforce надає можливість доступу до системи з різних мобільних пристроїв, що дозволяє користувачам працювати в хмарному середовищі з будь-якого місця і в будь-який час. Це дозволяє бізнесу бути більш гнучким і забезпечує зручність для користувачів.

Соціальна колаборація: Salesforce має вбудовані інструменти соціальної колаборації, такі як Черга новин та Chatter, що дозволяють спілкуватися, співпрацювати та обмінюватися ідеями всередині організації. Це сприяє покращенню комунікації та залученню співробітників.

Інтеграція з іншими системами: Salesforce надає можливість інтеграції з іншими корпоративними системами, такими як електронна пошта, системи управління ресурсами підприємства (ERP), системи аналітики та інші. Це дозволяє обмінюватися даними та забезпечує єдиноцентральне управління бізнес-процесами.

Складність налаштування: Оскільки Salesforce надає широкий спектр функціональності, воно може вимагати певного рівня експертизи та налаштувань для повного використання його можливостей. Для впровадження та налагодження системи Salesforce, може знадобитися досвідний адміністратор або консультант.

Ці особливості роблять хмарне середовище Salesforce потужним інструментом для управління клієнтами та маркетингових потреб. Враховуючи його спеціалізацію на CRM, Salesforce є популярним вибором для компаній, що прагнуть покращити взаємодію з клієнтами, оптимізувати процеси продажу та розширити свій бізнес.

3.2 Customer Relationship Management

CRM (Customer Relationship Management) - це підхід до управління взаємодією з клієнтами, що базується на використанні спеціалізованих програмних рішень та технологій. CRM допомагає компаніям збирати, аналізувати та використовувати інформацію про своїх клієнтів з метою поліпшення взаємодії з ними і підвищення рівня задоволеності.

Основна мета CRM полягає в тому, щоб компанії були більш ефективними у взаємодії з клієнтами, залученні нових клієнтів, збереженні існуючих і підвищенні рівня лояльності. Для досягнення цих цілей використовуються різні функції та можливості CRM-систем, такі як:

Збір та зберігання даних: CRM-системи дозволяють збирати та зберігати різноманітну інформацію про клієнтів, включаючи контактні дані, історію взаємодії, покупки, запити та інші дані, які допомагають зрозуміти потреби та поведінку клієнтів.

Аналітика та звітність: CRM-системи надають можливість аналізувати дані про клієнтів та створювати звіти, що допомагають виявляти тенденції, розуміти ефективність маркетингових кампаній, продажів та обслуговування клієнтів.

Автоматизація процесів: CRM-системи допомагають автоматизувати багато рутинних завдань, таких як обробка замовлень, відстеження контактів з клієнтами, розсилка листів та інше. Це дозволяє підвищити продуктивність та ефективність роботи команди.

Управління взаємодією з клієнтами: CRM-системи допомагають відстежувати всі етапи взаємодії з клієнтами, від початкового контакту до післяпродажного обслуговування. Це сприяє забезпеченню консистентної та персоналізованої комунікації з клієнтами.

Управління продажами: CRM-системи надають інструменти для ефективного керування процесом продажів, включаючи управління лідами, прогнозування продажів, контроль за виконанням цілей та інше.

Використання CRM-систем дозволяє підвищити ефективність роботи з клієнтами, забезпечити краще їх обслуговування та підвищити задоволеність клієнтів, що в свою чергу сприяє зростанню бізнесу та досягненню успіху.

3.3 Переваги хмарного середовища Salesforce

Хмарне середовище Salesforce має декілька переваг, які сприяють його популярності та використанню в бізнесі. Ось деякі з них:

Гнучкість та масштабованість: Salesforce дозволяє організаціям гнучко адаптуватися до змін у своєму бізнесі. Ви можете легко налаштувати та настроїти функціональність Salesforce відповідно до своїх потреб, додавати нові модулі та розширювати функціональність з використанням різноманітних додатків. Крім того, ви можете масштабувати свою інфраструктуру в хмарі, додавати нових користувачів та ресурси при необхідності.

Висока доступність та надійність: Salesforce має високий рівень доступності та надійності, оскільки його інфраструктура розподілена по різних центрах обробки даних. Це забезпечує неперервну роботу системи та уникнення відмов. Крім того, Salesforce забезпечує резервне копіювання даних та відновлення в разі непередбачених ситуацій.

Безпека даних: Salesforce приділяє велику увагу безпеці даних. Вони використовують різні заходи безпеки, такі як шифрування даних в спокої та під час передачі, механізми автентифікації та авторизації, моніторинг безпеки та захист від злому. Ваші дані залишаються конфіденційними та захищеними в середовищі Salesforce.

Інтеграція з іншими системами: Salesforce надає можливість інтеграції з іншими системами, що дозволяє обмінюватися даними та забезпечує єдиноцентральне управління бізнес-процесами. Ви можете інтегрувати Salesforce з електронною поштою, ERP-системами, системами аналітики та багатьма іншими, що допомагає вам отримувати повну картину вашого бізнесу.

Автоматизація процесів: Salesforce надає можливість автоматизувати багато бізнес-процесів, що спрощує роботу та забезпечує ефективність. Ви можете автоматизувати процеси продажу, маркетингу, обслуговування клієнтів та багато інших, що допомагає збільшити продуктивність та знизити ризики помилок.

Завершуючи аналіз хмарного середовища Salesforce, варто зазначити додаткові переваги:

Система управління взаємодіями з клієнтами (CRM): Salesforce є одним з найпопулярніших і потужних CRM-середовищ. Він надає широкий спектр інструментів для управління клієнтами, включаючи керування продажами, маркетингові автоматизацію, обслуговування клієнтів та аналітику. Завдяки цьому, Salesforce допомагає покращити відносини з клієнтами та збільшити продуктивність команди з продажу.

Спільна робота та комунікація: Salesforce надає можливості для спільної роботи та комунікації всередині команди. Інструменти, такі як Chatter, дозволяють співробітникам обмінюватися ідеями, файлами та спілкуватися на центральній платформі. Це підвищує комунікацію, сприяє колаборації та забезпечує кращу координацію роботи.

Підтримка клієнтів: Salesforce має інструменти та функціональність для підтримки клієнтів і надання якісного обслуговування. Інтегрована система керування запитами та тікетами допомагає відстежувати та вирішувати проблеми клієнтів, а інструменти аналітики дозволяють виявляти та вдосконалювати процеси обслуговування.

Розширені можливості аналітики: Salesforce пропонує потужні засоби аналітики даних, такі як Salesforce Analytics, що дозволяють вам отримувати цінні інсайти зі своїх даних. Ви можете візуалізувати дані, створювати звіти та панелі управління для аналізу продажів, відстеження ключових показників ефективності та прийняття обґрунтованих рішень.

Екосистема додатків та розширень: Salesforce має велику екосистему додатків та розширень, що дозволяють розширити функціональність середовища. Ви можете

знайти додатки в Salesforce AppExchange, які задовольнять ваші конкретні потреби та допоможуть вам розширити можливості вашої системи Salesforce.

Ці переваги роблять Salesforce одним з провідних хмарних середовищ для управління клієнтами та автоматизації бізнес-процесів. Ця платформа пропонує широкий спектр інструментів та функцій, які сприяють покращенню продуктивності, залученню клієнтів та зростанню бізнесу.

3.4 Недоліки хмарного середовища Salesforce

Хоча хмарне середовище Salesforce має багато переваг, воно також має кілька потенційних недоліків, які варто враховувати:

Вартість: Використання Salesforce може бути витратним, особливо для менших компаній або підприємств з обмеженими бюджетами. Ліцензійні витрати, підписка на послуги та додаткові витрати на налаштування, інтеграцію та навчання можуть становити значну суму.

Складність налаштування: Salesforce є потужною та розширеною платформою, що може вимагати певного рівня експертизи для правильної настройки та налаштування. Налаштування системи та інтеграція з іншими додатками можуть бути складними завданнями, особливо для менш технічної компетентності.

Залежність від Інтернету: Використання хмарних середовищ, включаючи Salesforce, передбачає постійний доступ до Інтернету. Це означає, що без доступу до Інтернету ви не зможете отримувати доступ до своїх даних або працювати з платформою Salesforce.

Контроль над даними: Використання хмарного середовища означає, що ваші дані зберігаються на серверах Salesforce або стороннього постачальника хмарних послуг. Це може породжувати певні стурбованості щодо контролю над вашими даними та їх безпекою.

Залежність від постачальника: Використання хмарного середовища означає, що ви стаєте залежними від постачальника хмарних послуг, у цьому випадку Salesforce.

Якщо постачальник має технічні проблеми або відмовляється від послуг, це може призвести до перерв у роботі та недоступності ваших даних.

Обмежена гнучкість: Хмарні середовища, включаючи Salesforce, можуть мати обмеження в розширенні функціональності або налаштування під конкретні потреби вашої компанії. Деякі специфічні функціональності або налаштування можуть бути обмеженими або вимагати додаткових ресурсів.

Можливість збоїв та недоступності: Хмарні середовища, включаючи Salesforce, можуть стикатись з технічними проблемами, збоями або періодами недоступності. Це може призвести до тимчасової втрати доступу до даних або послуг, що може вплинути на роботу вашої компанії та відносини з клієнтами.

Вплив змін у політиках та умовах використання: Як користувач хмарного середовища Salesforce, ви залежите від політик і умов використання, встановлених Salesforce. Зміни в цих політиках можуть вплинути на ваші права та обмеження використання платформи.

Ризики безпеки даних: Незважаючи на наявність заходів безпеки в хмарних середовищах, існує ризик злому безпеки та несанкціонованого доступу до ваших даних. Це може бути проблемою, особливо якщо ви зберігаєте чутливу інформацію або робите бізнес у регульованій сфері.

Віддалений контроль: Використання хмарного середовища означає, що ви не маєте повного контролю над інфраструктурою та обслуговуванням, оскільки це здійснюється з боку постачальника хмарних послуг. Ви повинні довіряти постачальнику та його здатності забезпечити безпеку та доступність.

Ці недоліки необхідно враховувати та оцінювати їх в контексті своїх бізнес-потреб та вимог. Варто провести аналіз ризиків та оцінку вартості для забезпечення вибору правильного хмарного середовища, яке відповідає вашим потребам та забезпечує необхідний рівень безпеки та ефективності.Перед прийняттям рішення важливо зважити на переваги та недоліки, а також розглянути конкретні потреби вашої компанії.

3.5 Захист даних в хмарному середовищі Salesforce

Salesforce має великий фокус на безпеці даних та використовує різні заходи для захисту інформації в хмарному середовищі. Ось декілька ключових заходів безпеки, які використовуються в Salesforce:

Контроль доступу: Salesforce надає рівні доступу до даних та функціональності, що дозволяє обмежувати доступ до конфіденційної інформації лише необхідним користувачам. Це забезпечуєся за допомогою налаштування ролей, профілів, прав доступу та механізмів аутентифікації.

Шифрування даних: Salesforce використовує шифрування для захисту даних під час передачі та зберігання. Дані, що передаються між користувачем та серверами Salesforce, шифруються за допомогою протоколу SSL / TLS. Крім того, дані, збережені на серверах Salesforce, шифруються з використанням сильних шифрувальних алгоритмів.

Захист від несанкціонованого доступу: Salesforce використовує різні заходи для захисту від несанкціонованого доступу до даних, включаючи захист паролів, механізми аутентифікації (такі як двофакторна аутентифікація) та моніторинг активності користувачів.

Моніторинг та аудит: Salesforce здійснює постійний моніторинг системи та реєструє дії користувачів для виявлення ненормальної або підозрілої активності. Це дозволяє вчасно виявляти потенційні загрози безпеці та реагувати на них.

Резервне копіювання та відновлення: Salesforce забезпечує регулярне резервне копіювання даних і можливість відновлення даних в разі потреби. Це дозволяє відновити дані в разі випадкового видалення або системного збою.

Фізична безпека: Salesforce має фізичні заходи безпеки, щоб захистити серверні приміщення та обладнання від несанкціонованого доступу, пожеж, повеней та інших небезпек.

Регуляторні вимоги: Salesforce виконує вимоги регуляторних органів та стандартів безпеки, таких як GDPR, HIPAA, ISO 27001 та інші, що забезпечують високий рівень захисту даних.

Варто зазначити, що безпека в хмарному середовищі Salesforce є спільною відповідальністю між Salesforce як постачальником хмарних послуг та користувачами, які використовують платформу. Salesforce надає інструменти та можливості для налаштування і керування безпекою, але належить користувачам забезпечити правильну конфігурацію та виконання політик безпеки в межах їх власних організацій.

3.5 Недоліки захищеності даних в хмарному середовищі Salesforce

Хоча Salesforce має широкий спектр заходів безпеки для захисту даних в хмарному середовищі, все ж є деякі потенційні недоліки, про які варто знати:

Залежність від постачальника послуг: Ви покладаєтеся на Salesforce як постачальника хмарних послуг для забезпечення безпеки даних. Це означає, що ви не маєте повного контролю над інфраструктурою та заходами безпеки. Якщо постачальник хмарних послуг не забезпечує належну безпеку, це може створити ризики для ваших даних.

Збереження даних на зовнішньому сервері: Використання хмарного середовища означає, що ваші дані зберігаються на зовнішньому сервері, не під вашим прямим контролем. Це може викликати почуття небезпеки, особливо якщо ви зберігаєте конфіденційну чи чутливу інформацію.

Ризики безпеки даних при передачі: Хоча Salesforce використовує шифрування при передачі даних, існує ризик перехоплення або несанкціонованого доступу до даних під час їх транспортування до та з хмарного середовища. Тому важливо використовувати безпечні канали комунікації та дотримуватись кращих практик забезпечення безпеки при передачі даних.

Ризики залежності від інтернет-з'єднання: Використання хмарного середовища передбачає необхідність постійного та надійного інтернет-з'єднання. Якщо ваше з'єднання переривається або стає недоступним, це може призвести до тимчасової втрати доступу до даних та послуг.

Ризики злому та несанкціонованого доступу: Жодна система не є повністю непроникною, і існує ризик злому або несанкціонованого доступу до даних в хмарному середовищі Salesforce. Незалежно від заходів безпеки, які вживає Salesforce, важливо додатково захищати свої дані за допомогою сильних паролів, механізмів аутентифікації та контролю доступу.

Ризик втрати контролю над даними: Зберігання даних в хмарному середовищі означає, що ви здаєтеся контролю над фізичними серверами і інфраструктурою, на якій вони знаходяться. Це може створити певну небезпеку в разі, якщо ви вирішите припинити використання хмарного середовища або якщо постачальник хмарних послуг зазнає проблем.

Загальний підхід до забезпечення безпеки в хмарному середовищі Salesforce полягає в комбінації заходів безпеки, наданням правильного конфігурування та керування, а також свідомим використанням кращих практик забезпечення безпеки з вашого боку.

Висновки за розділом 3

Хмарне середовище Salesforce є одним з провідних хмарних середовищ у сфері CRM та бізнес-рішень. Воно надає широкі можливості для зберігання, керування та аналізу даних, а також автоматизації бізнес-процесів. З точки зору безпеки, Salesforce приділяє велику увагу захисту даних та використовує різноманітні заходи для забезпечення безпеки інформації в хмарному середовищі.

Переваги хмарного середовища Salesforce включають:

Висока надійність та доступність сервісу, що забезпечує безперебійну роботу та доступ до даних у будь-який час.

Широкий набір функцій та можливостей для управління клієнтськими взаємодіями, маркетингу та продажу.

Зручний інтерфейс та простота використання для користувачів.

Шифрування даних та заходи безпеки при передачі та зберіганні інформації.

Підтримка різних механізмів аутентифікації та контролю доступу.

Недоліки хмарного середовища Salesforce включають:

Залежність від постачальника хмарних послуг та обмежений контроль над інфраструктурою та безпекою даних.

Ризики безпеки даних при передачі та зберіганні, хоча Salesforce вживає заходи для забезпечення безпеки, існує потенційний ризик несанкціонованого доступу або злому даних.

Залежність від стабільного та надійного інтернет-з'єднання для доступу до хмарних послуг.

Ризики втрати контролю над даними, оскільки вони зберігаються на серверах постачальника хмарних послуг.

Незважаючи на ці недоліки, хмарне середовище Salesforce залишається популярним вибором для організацій, оскільки воно надає значні переваги з точки зору функціональності, доступності та безпеки даних. Проте, варто уважно розглянути його з позиції конкретних вимог та ризиків вашої організації перед прийняттям рішення про використання хмарного середовища Salesforce.

ВИСНОВКИ

В ході виконання даної роботи було проведено ознайомлення з типами хмарних середовищами та виявлено, які існують методи та засоби захисту інформації в хмарних середовищах. Таким чином, дослідження, проведене під час написання даної дипломної роботи, було зосереджено на вивченні існуючих методів та засобів захисту інформації в хмарному середовищі. Також був проведений аналіз цих методів і виявлення їх обмежень дозволили отримати цінну інформацію про необхідність постійного вдосконалення механізмів захисту інформації. Вирішенно актуальну проблему з покращенням рівеня безпеки від несанкціонованого доступу до інформації при використанні хмарних середовищ за допомогою різних відомих засобів та механізмів захисту інформації від несанкціонованого доступу до інформації.

Також був проведений аналіз хмарного середовища Salesforce, визначено для яких підприємств воно створене, розглянуті його переваги над іншими хмарними середовищами, та виявлено недоліки, які використовуються в даному середовищі.

Таким чином, у результаті виконання даної роботи було досягнуто початкову мету та виконано усі необхідні для цього завдання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Приватна українська хмара [Електронний ресурс] // - Режим доступу до ресурсу: https://gigacloud.ua#page-block-225

2. Визначення безпеки в хмарі на базі Microsoft [Електронний ресурс] - Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security

3. Загрози для безпеки у хмарі [Електронний ресурс] //Навчальний посібник.- Режим доступу: https://denovo.ua/blog/zagrozi-dlya-bezpeki-u-hmari-vidpovidi-na-chasti-zapitannya-17

4. Ковальчук, О. Оновлення технологій доступу до захищених інформаційних ресурсів. Інформаційна безпека.

5. Johnson, R. . Multi-Factor Authentication: An Effective Approach to Secure Information Access. International Journal of Cybersecurity.

6. Державний університет Телекомунікацій [Електронний ресурс] // - Режим доступу до ресурсу: https://dut.edu.ua/ua/news-1-569-9733-yak-zabezpechiti-zahist-informacii-ta-informaciynu-bezpeku-konfidenciynih-danih-vikoristovuyuchi-hmarni-tehnologii_kafedra-cistem-tehnichnogo-zahistu-informacii

7. Документ України щодо обробки інформації в системах хмарних обчислень [Електронний ресурс] - Режим доступу : http://w1.c1.rada.gov.ua/ pls/zweb2/webproc4_1?pf3511=58527

8. The NIST Definition of Cloud Computing (англ.). [Електронний ресурс]: Режим доступа: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecia lpublication800-145.pdf

9. Ладигіна О.А. Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту [Електронний ресурс] // - Режим доступу до ресурсу: https://core.ac.uk/download/pdf/84826832.pdf

10. Mell P. The NIST Definition of Cloud Computing [Електронний ресурс] / P. Mell, T. Grance // National Institute of Standards and Technology. – 2011. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-145/final

11. Controlling data in the cloud: outsourcing computation without outsourcing control / [J. Staddon, R. Masuoka, J. Molina та ін.]. // ACM Conference on Computer and Communications Securit. – 2009. – No9. – С. 85–90.

12. Bogomolny A. Chinese Remainder Theorem [Електронний ресурс] / Alexander Bogomolny // Interactive Mathematics Miscellany and Puzzles – Режим доступу до ресурсу: https://www.cut-the-knot.org/blue/chinese.shtml

13. Інформаційно-орієнтована концепція забезпечення безпеки хмарних обчислень [Текст] / Пирожков О., Савчук О. // Інфокомунікаційні системи та технології. – 2018. – No 2(2). – С. 32-36

14. NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters, 2011. – 85 с.

15. Yeun C. Cloud computing security management / C. Yeun, S. Almulla. // Engineering Systems Management and Its Applications (ICESMA). – 2010. – 2nd International Conference on Engineering System Management & Applications