Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи забезпечення надійності мультихмарних середовищ
(тема)

Виконав:

студент II курсу, групи СПм-22-1

Важинський Б.В.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: доц. Ткачов В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Важинському Богдану Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи забезпечення надійності мультихмарних середовищ

затверджена наказом по університету від " 06 " листопада 2023 р. № 1299 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 січня 2024 р.

3. Вхідні дані до роботи

1) Відомі хмарні системи
2) Стан та проблематика безпеки мультихмарних середовищ
3) Користувацький досвід використання мультихмар

4. Перелік питань, що потрібно опрацювати у роботі

1) Оглянути історію та поняття хмарних технологій
2) Проаналізувати актуальні хмарні середовища
3) Визначити переваги та недоліки використання мультихмарних середовищ
4) Дослідити з аспекту безпеки вплив хмарних систем на освітню сферу
5) Запропонувати методи забезпечення надійності мультихмарних середовищ
6) Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Слайд – презентація – 9 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд мультихмарних технологій	07.11.2023 – 14.11.2023	
2	Аналіз шляхів вирішення проблем при мульти-	15.11.2023 – 29.11.2023	
	мультихмарності		
3	Дослідження впливу хмарних середовищ	30.11.2023 – 14.12.2023	
	на освітню сферу		
4	Створення критеріїв надійності мультихмар	15.12.2023 – 01.01.2024	
5	Підведення підсумків та висновків	02.01.2024 – 04.01.2024	
6	Оформлення матеріалів кваліфікаційної роботи	05.01.2024 – 08.01.2024	
7	Подання кваліфікаційної роботи керівникові та	09.01.2024 – 11.01.2024	
	Попередній захист		
8	Подання кваліфікаційної роботи на рецензування	10.01.2024 – 12.01.2024	

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Ткачов В.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 62 с., 6 рис., 0 табл., 2 дод., 18 джерел.

МУЛЬТИХМАРНІСТЬ, ОСВІТНІЙ ПРОЦЕС, БЕЗПЕКА, НАДІЙНЕ ХМАРНЕ СЕРЕДОВИЩЕ, ІТ-ІНФРАСТУКТУРА, ХМАРНІ ТЕХНОЛОГІЇ, МУЛЬТИХМАРА, КРИТЕРІЇ НАДІЙНОСТІ, ЗВО, ІТ-СФЕРА

Метою кваліфікаційної роботи є аналіз стану, проблем та їх причин безпеки мультихмарних середовищ, сформувати критерії безпечної хмари. Дослідити вплив хмарних технологій на освітню сферу.

У ході виконання кваліфікаційної роботи розглянуто стан та проблематику мультихмарних середовищ з різних аспектів безпеки. Також проведено аналіз ролі мультихмарності в освітньому процесі. Надані рекомендації щодо вибору та покращення безпеки мультихмарних систем.

ABSTRACT

Explanatory note of the qualification work: 62 pages, 6 figures, 0 tables, 2 appendices, 18 sources.

MULTIMEDIA, EDUCATIONAL PROCESS, SECURITY, RELIABLE CLOUD ENVIRONMENT, IT INFRASTRUCTURE, CLOUD TECHNOLOGIES, MULTIMEDIA, RELIABILITY CRITERIA, ZVO, IT SPHERE

The purpose of the qualification work is to analyze the state, problems and their causes of the security of multi-cloud environments, to form the criteria of a secure cloud. To investigate the impact of cloud technologies on the educational sphere.

In the course of the qualification work, the state and problems of multi-cloud environments from various aspects of security were considered. An analysis of the role of multicloud in the educational process was also carried out. Recommendations for choosing and improving the security of multi-cloud systems are provided.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IaaS - Інфраструктура як послуга (англ., Infrastructure-as-a-Service)

PaaS - Платформа як послуга (англ., Program-as-a-Service)

SaaS - Програмне забезпечення як послуга (англ., Software-as-a-Service)

VPS/VDS – Віртуальний виділений сервер (англ., Virtual Private Server)

API - Інтерфейс програмування застосунків (англ., Application Programming Interface)

MFA - Багатофакторна автентифікація (англ., Multi-Factor Authentication)

SSO - Технологія єдиного входу (англ., Single Sign-On)

ACL - Список контролю доступу (англ., Access Control ist)

RBAC - Керування доступом на основі ролей (англ., Role Based Access Control)

ABAC - Розмежування доступу на основі атрибутів (англ., Attribute-Based Access Control)

GDPR - Загальний регламент із захисту даних (англ., General Data Protection Regulation)

SQL - мова структурованих запитів (англ., Structured Query Language)

ЦОД - Центр обробки даних

ВСТУП

Нарощування об’ємів цифрового кома відбувається в неконтрольованій геометричній прогресії, тому, на сьогодні, ризиковано залишати важливі відомості на локальному носії, для цих випадків вже створений тип програмно-технічного середовища. Прикладом вищеописаного довкілля є хмара, її простий спосіб експлуатації та некоректно налаштований доступ до розташованих в ній об’єктів, становить загрозу надійності всієї системи. Також зі збільшенням кількості хмарних продуктів зростає складність їх інтеграції, контролю, розробки та забезпечення ефективної, стабільної та безпечної роботи. Перераховані міні-проблеми, якщо їх не вирішити або частково не зменшити їх негативний вплив, можуть перетворити надії та гарантії успішності роботи в хаос. У результаті, не релевантні методи забезпечення ефективного рівня безпеки або їх відсутність викликатимуть серйозні занепокоєння щодо втрати або витоку даних організації та її клієнтів. Зараз також в нашому сучасному світі, актуально захистити кожен збережений біт інформації і підібрати наявні підходи або у разі необхідності відновити вже втрачені файли. При бурхливому розвитку хмарних технологій та бажанні бізнесменів, швидко зробити власний продукт максимально легким та зручним, мало приділяли уваги до безпеки. Наразі ключовими факторами сповільнення вирішення питань безпеки все ще є людський фактор, не вигідні втрати продуктивності заради захисту продукту та складність комплаєнсу з урахуванням індивідуальних обмежень компанії в залежності від завдання, таке відношення прирікає будь-який хмарний проект на провал. Хмари все більше вбудовуються в наше життя і тепер з кожним кроком їх розвитку, користувачі переконані, що такий невиправданий темп пов’язаний з потребами жадібного ринку споживачів, які не дають шансу розробникам проектів або стартапів хоча б на середній рівень задовольнити вимоги до безпеки. Таким чином монопольні компанії в маркетинговій гонці за грошима будуть успішно втрачати репутацію,

коли клієнти сконцентруються на більш вигідних унікальних рішеннях конкурентів. Зараз як ніколи це актуально, під час сурової конкуренції між технологічними-технічними компаніями, клієнт має максимальну вигоду за рахунок одночасної взаємодії різних хмарних сервісів з інфраструктурою та платформами серверів. Якщо ми кажемо про масштаби цілої організації, тоді не створюють з нуля нові рішення та відповідно їм додаткові перепони для бізнесу, завжди застосовують і вдосконалюють існуючи стратегії в IT-сфері, наприклад, мультихмарність. Завдяки хмарній інфраструктури, користувачі можуть, будь-де, при наявності доступу до хмари, в зручний час використовувати розподілені ресурси для дій при виконанні різнорідних завдань. Значить будь-яка вразлива частина або вузол, який був зламаний, IT-інфраструктури при задіянні декількох хмар може стати ризиковою системою №1. Окремо, хочеться наголосити, що додатковим економічним тягарем для юридичних та публічних облич є складність забезпечення конфіденційності даних. В хмарних продуктах, при впровадженні хмарних технологій співробітникам корпорацій не вистачає знань та досвіду, щоб перевірити, які елементи інфраструктури під безпекою. Звідси пішла необхідність більш детально досліджувати даний напрям з різних боків в плані безпеки та надійності хмар. На нашу думку, чим більше якісних досліджень ми зробимо, тим швидше наші праці дадуть шанс вирішити поточні проблеми або зменшити поганий вплив на IT-сферу. Освітивши насущні проблеми надійності хмарного сектору і на основі причин їх виникнення, необхідно знайти критерії безпечної хмари, щоб вони стали орієнтиром для знаходження або створення, у майбутньому, методу забезпечення надійності хмарних систем. Звісно необхідно врахувати роботу інших діячів для подальшого якісного та унікального дослідження. Не дивлячись на новизну технології, пов’язаною з хмарами, вони в подальшому обов’язково будуть незамінними ще декілька років та можливо стануть частиною нових винаходів, але без рішень сучасних проблем, хмарні перспективи залишаться нездійсненною мрією.

Мультихмарне середовище – це комбінація двох або більше хмарних

середовищ, власних або підрядних. Воно необхідно для розміщення back-end та front-end сервісів, при цьому кожна хмара може працювати автономно. Частіше всього мультихмарні середовища використовують для з'єднання приватної хмари з кількома загальнодоступними хмарними середовищами задля підвищення загальної продуктивності сервісу.

Використання мультихмарного середовища пропонує: можливість масштабування операцій шляхом додавання та віднімання хмарних ресурсів з часом; зменшення ризиків відключення від мережі через одночасну присутність кількох хмарних середовищ; кращу відповідність нормативним вимогам провайдерів щодо зберігання конфіденційних даних зацікавлених сторін; можливість впровадження останніх інновацій та послуг за допомогою масштабування, не виходячи з мережі.

1 СТАН ТА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ МУЛЬТИХМАРНИХ ТЕХНОЛОГІЙ

1.1 Поняття про хмарні технології

Сьогодні хмарні сервіси стали невід'ємною частиною бізнес-інфраструктури більшості компаній, забезпечуючи гнучкість, масштабованість і доступність. Однак, оскільки хмарні обчислення продовжують розвиватися, з'являються нові можливості. У мультихмарному середовищі організації використовують два або більше хмарних провайдерів для різних цілей, щоб досягти оптимальної ефективності та точності в бізнес-операціях. Тим не менш, підвищена складність створює різні специфічні виклики і загрози безпеці, які вимагають особливої уваги і відповідних стратегій безпеки. Ці стратегії виходять за рамки стандартних хмарних рішень безпеки і передбачають їх розширення та поглиблення.

Хмарна безпека – це сукупність стратегій і заходів, призначених для захисту даних, додатків та інфраструктури в хмарному середовищі. Хоча провайдери хмарних сервісів пропонують бізнесу можливість позбутися витрат, пов'язаних зі створенням і підтримкою власної обчислювальної інфраструктури, надаючи доступ до готових ресурсів і сервісів, ефективність і безпека в більшій чи меншій мірі покладаються на компанії-клієнти.

Залежно від моделі хмарного сервісу, відповідальність за різні аспекти безпеки по-різному розподіляється між провайдером і клієнтом.

У моделі "Інфраструктура як послуга" (IaaS) провайдер надає базову інфраструктуру (сервери, мережу, сховища), а клієнт відповідає за безпеку операційних систем, додатків і даних, які він розгортає в хмарі.

У моделі "Платформа як послуга" (PaaS) постачальник пропонує не лише інфраструктуру, але й платформу для розробки, включаючи операційні системи та інструменти для розробки. Клієнт несе відповідальність за безпе-

ку додатків, які він розробляє, і даних, які ці додатки обробляють.

У моделі "Програмне забезпечення як послуга" (SaaS) постачальник надає готові до використання додатки і відповідає за їхню безпеку. Однак клієнт все одно несе відповідальність за їхню конфігурацію та безпеку даних, які він зберігає і обробляє в цих додатках, а також за управління доступом до цих даних.

Хмарна індустрія розвивається, і з’явилося багато хмарних провайдерів, кожен з яких пропонує унікальні послуги та умови. Це призвело до появи мультихмарної стратегії, в якій понад 76% компаній вже використовують два або більше хмарних провайдерів, і ця тенденція продовжує зростати.

Мультихмарна стратегія – це підхід, коли компанія використовує комбінацію публічних, приватних та гібридних хмар. Це дозволяє використовувати найкращі функції та сервіси хмарних провайдерів для конкретних бізнес-операцій та відповідати нормативним вимогам. Наприклад, один провайдер може запропонувати високопродуктивні обчислювальні ресурси, а інший – передові аналітичні інструменти або більш сприятливі умови зберігання даних, крім того, деякі нормативні акти вимагають зберігати дані про громадян у певних географічних межах.

Мультихмарна безпека – це заходи, що застосовуються для захисту даних, додатків та інфраструктури, розподілених між декількома хмарними платформами. У мультихмарному середовищі дані та програми можуть мігрувати між різними хмарними платформами, кожна з яких має свої стандарти безпеки та механізми контролю. Це ускладнює управління безпекою, оскільки необхідно враховувати ці відмінності та забезпечувати захист на всіх рівнях і компонентах.

Враховуючи складність мультихмарних середовищ та велику кількість компонентів, якими потрібно керувати, автоматизація відіграє ключову роль у забезпеченні безпеки. Автоматизація допомагає забезпечити безперервне дотримання політик безпеки, зменшує ймовірність людських помилок і пришвидшує реагування на інциденти безпеки. Це може включати автоматичне

виявлення та реагування на аномалії в хмарному середовищі, автоматизоване управління доступом та автоматичне оновлення конфігурацій безпеки.

1.2 Переваги та ризики використання мультихмарного або гібридного хмарного середовища

Мультихмара або мультихмарність – це організаційна стратегія для IT-інфраструктури компаній, яка означає використання декількох хмар, хмарних сервісів й інших обчислювальних ресурсів від різних провайдерів. Це робиться з метою уникнути можливої залежності від єдиного провайдера хмарних послуг. Так компанія може орендувати VPS/VDS сервера у одного провайдера, користуватися колокацією в іншого, а розміщувати дані для спільної роботи, наприклад, в публічній хмарі вже у третього провайдера.

Концепція самої хмари виникла ще в 2006 році. З того часу встигли виникнути різні моделі хмарного середовища і обслуговування (на кшталт публічної, приватної, громадської та гібридної хмар). В якусь мить навіть пропонували об’єднати можливості публічної та приватної хмар в одне ціле. Однак таке рішення не виявилося ефективним.

Замість цього стало ще більше з'являтися платформ з публічним хмарним середовищем. Серед відомих провайдерів публічної хмари – Microsoft, Google, HPE, IBM та інші. Приватні та інші моделі хмар теж не відставали по зростанню кількості та якості. Вибір же якогось одного провайдера у клієнтів суто визначався з якихось цілей, потреб і бюджету. Незабаром клієнти зрозуміли, що у кожного хмари та хмарної послуги є як свої переваги, так і недоліки.

Переваги мультихмари:

- у вас є можливість підібрати найкращий набір послуг і відмовитися від зайвих;

- ви не будете повністю прив’язані до інфраструктури одного провайдера;

- так як ви не використовуєте зайві послуги та вибираєте тільки ті послуги, які підходять під ваш бюджет і цілі, ви скорочуєте витрати;

- ви не залежите від одного провайдера. Це підвищує стійкість і гнучкість IT-інфраструктури перед будь-якими катастрофами [1].

Отже, перехід до мультихмарної стратегії пропонує низку переваг, які можуть допомогти організаціям покращити свою діяльність, підвищити ефективність та забезпечити надійність своїх систем.

1) Спеціалізація. Дозволяє організаціям оптимізувати свою інфраструктуру під конкретні робочі навантаження, використовуючи спеціалізовані сервіси від різних хмарних провайдерів. Наприклад, організація може використовувати хмарний сервіс, який пропонує високу пропускну здатність для обробки великих обсягів даних, тоді як інший сервіс можна використовувати для додатків, що вимагають високої надійності та доступності. Це дозволяє організаціям максимізувати переваги кожного хмарного провайдера, враховуючи специфічні вимоги своїх робочих навантажень.

2) Економічна ефективність. Дозволяє організаціям оптимізувати свої витрати. Різні хмарні провайдери можуть пропонувати різні тарифи та умови надання своїх послуг. Організації можуть обирати між ними залежно від своїх поточних потреб і бюджету. Це може включати використання дешевших послуг для менш критичних робочих навантажень або використання більш дорогих, але надійних послуг для критично важливих додатків. До речі, у нас є низка статей, в яких ми ділимося досвідом оптимізації витрат на інфраструктуру та розробку, заснованим на власному досвіді.

3) Аварійне відновлення. Підвищує надійність та доступність систем організації. Якщо в одного хмарного провайдера виникають проблеми, інший провайдер може продовжити обслуговування. Це зменшує ризик простою та забезпечує безперервність бізнесу. Крім того, мультихмарна стратегія дозволяє організаціям швидше відновлюватися після катастроф, оскільки дані та додатки можуть бути розподілені між різними хмарними платформами.

4) Уникнення прив’язки до постачальника. Використовуючи кілька хмар-

них провайдерів, організації можуть уникнути надмірної залежності від одного постачальника. Це забезпечує більшу гнучкість при укладанні контрактів і масштабуванні ресурсів, а також гарантує, що організація не буде залежати від зміни цін або послуг одного постачальника.

5) Покращена безпека та відповідність нормативним вимогам. Використання декількох хмар може забезпечити додатковий рівень безпеки, оскільки дані розподілені в різних середовищах. Крім того, деякі хмарні провайдери можуть запропонувати кращі функції безпеки або відповідність певним стандартам, що мають вирішальне значення для певних частин бізнесу.

6) Географічна присутність. Забезпечує краще глобальне покриття та послуги ближче до кінцевих користувачів. Різні провайдери можуть мати центри обробки даних у різних місцях, які можна використовувати для швидшого реагування та дотримання регіонального законодавства про захист даних.

7) Інновації та доступ до найновіших функцій. Різні хмарні провайдери часто впроваджують нові функції та технології. Маючи мультихмарну стратегію, організації можуть швидко впроваджувати та експериментувати з цими інноваціями, не прив’язуючись до пропозицій одного провайдера.

8) Отже, мультихмарна стратегія пропонує організаціям більшу гнучкість, економічну ефективність, надійність і доступ до спеціалізованих послуг, які можуть допомогти досягти бізнес-цілей і підтримувати надійну та відмовостійку роботу (рисунок 1.1). Однак організаціям необхідно ретельно керувати та організовувати свої мультихмарні середовища, щоб уникнути складнощів та забезпечити повну реалізацію можливостей.

Рисунок 1.1 - Переваги мультихмарної стратегії

Поряд з цими перевагами, мультихмарні середовища створюють низку унікальних викликів.

1) Навчання персоналу. Персонал, який працює з мультихмарними середовищами, повинен бути знайомий із загальними принципами хмарної безпеки та специфічними особливостями кожної хмарної платформи. Це може передбачати навчання роботі з конкретними інструментами та інтерфейсами безпеки, а також розуміння окремих політик безпеки кожного хмарного провайдера. Комплексне навчання персоналу в цих сферах може вимагати значних часових і фінансових інвестицій.

2) Управління міграцією в хмару. Міграція даних і додатків між різними хмарними платформами вимагає ретельного планування та виконання. Вона передбачає забезпечення безпеки даних під час передачі, а також управління доступом до даних на новій платформі. Цей процес може бути складним і вимагає значних зусиль, щоб гарантувати його завершення.

3) Управління політикою безпеки. У мультихмарному середовищі забезпечення узгодженої політики безпеки може бути складним завданням. Кожен хмарний провайдер може мати власні інструменти та процедури для управ-

ління безпекою, які можуть відрізнятися від інших платформ. Це може створювати складнощі в підтримці узгодженості та ефективності політик безпеки.

4) Керування доступом та ідентифікацією. Управління доступом та ідентифікацією в мультихмарному середовищі може бути складним через відмінності в системах ідентифікації та авторизації різних хмарних провайдерів. Це може призвести до необхідності використання складних систем керування ідентичностями або брокерів безпеки доступу до хмарних сервісів.

5) Керування шифруванням. У мультихмарному середовищі керування ключами шифрування може бути складним завданням. Ключі повинні бути доступними на всіх відповідних хмарних платформах, забезпечуючи при цьому їх безпечне зберігання та використання. Для цього можуть знадобитися спеціалізовані рішення для керування ключами шифрування, які підтримують мультихмарні середовища.

6) Керування ресурсами. Управління ресурсами в мультихмарному середовищі може бути складним завданням через відмінності в структурах ціноутворення та механізмах звітності серед хмарних провайдерів. Це може вимагати спеціалізованих інструментів для моніторингу використання ресурсів та оптимізації витрат.

7) Проблеми моніторингу. Моніторинг активності та подій безпеки в мультихмарному середовищі може бути складним через відмінності в журналах і даних аудиту, що надаються різними хмарними платформами. Для цього можуть знадобитися централізовані системи моніторингу безпеки, здатні агрегувати та аналізувати дані з різних джерел.

8) Мультихмарні загрози безпеці. Мультихмарні рішення також можуть бути пов’язані з унікальними загрозами безпеці. Ці загрози можуть виникати через різні фактори, включаючи складність конфігурації, невідповідність нормативним вимогам, вразливості управління доступом та ідентифікацією, а також загрози на різних рівнях, включаючи мережі, додатки та API.

9) Невідповідність конфігурації та управління доступом. Кожен хмарний провайдер має власні інструменти та методи для налаштування безпеки та

управління доступом у мультихмарному середовищі. Це можуть бути різні методи автентифікації, такі як багатофакторна автентифікація (MFA) або єдиний вхід (SSO), різноманітні налаштування мережевого доступу, такі як списки контролю доступу (ACL) або групи безпеки, а також різні політики управління доступом, такі як контроль доступу на основі ролей (RBAC) або контроль доступу на основі атрибутів (ABAC). Ці відмінності необхідно враховувати при налаштуванні безпеки, щоб уникнути невідповідності конфігурації, що збільшує ризик несанкціонованого доступу до конфіденційних даних. Це також може призвести до слабких або несумісних політик доступу, що підвищує ймовірність внутрішніх і зовнішніх загроз безпеці.

10) Невідповідність нормативним вимогам. Кожен хмарний провайдер має свої процедури для забезпечення відповідності різним нормативним вимогам, таким як GDPR, HIPAA або PCI DSS. Це можуть бути різні методи шифрування даних, різні політики управління доступом і різні методи аудиту. Неврахування цих відмінностей при обробці або зберіганні даних може призвести до невідповідності нормативним вимогам і потенційних штрафів.

11) Багаторівневі загрози. У мультихмарному середовищі існує безліч загроз на різних рівнях, включаючи мережі, API та додатки. На мережевому рівні це може бути неправильна конфігурація мережевих пристроїв, таких як брандмауери та балансувальники навантаження, що може призвести до розподілених атак на відмову в обслуговуванні (DDoS) або перехоплення даних. На рівні додатків загрози можуть включати вразливості в коді додатків, що уможливлюють SQL-ін’єкції або міжсайтовий скриптинг, а також вразливості в API, які можуть дозволити зловмисникам обійти контроль доступу або маніпулювати функціоналом API за допомогою атак типу "ін’єкція" або атак грубої сили на основі підбору облікових даних.

12) Загрози шифрування. Шифрування є основним методом захисту даних у хмарі, але воно також несе в собі унікальні загрози. Якщо ключі шифрування втрачені або скомпрометовані, це може призвести до втрати доступу до даних або витоку даних. Це може статися через зовнішню атаку, внутріш-

нє зловживання або просту помилку. Деякі хмарні провайдери також можуть використовувати власні системи управління ключами, які можуть бути несумісними з іншими системами.

13) Внутрішній ризик. У мультихмарному середовищі ризик інсайдерів зростає, оскільки все більше людей отримують доступ до хмарних ресурсів. Співробітники, підрядники, ділові партнери і навіть зловмисники можуть отримати доступ до систем через слабкі або скомпрометовані облікові записи. Це може призвести до витоку інформації, впровадження шкідливого програмного забезпечення або навіть саботажу хмарної інфраструктури (рисунок 1.2).

Рисунок 1.2 - Аспекти мультихмарної безпеки

Хоча спочатку мультихмара може здатися логічним вибором, вона вимагатиме від вас наявності в штаті IT-спеціаліста або команди. Управління кількома хмарними середовищами та підтримка їхньої працездатності – це робота на повний робочий день. Подібним чином, організація безпеки ваших даних може бути складним завданням через наявність багатьох векторів атак для ризиків кібербезпеки. Однак якщо ви можете забезпечити постійну при-

сутність IT-експерта на вашому підприємстві, це не проблема.

Отже, хмара стала невід'ємною частиною роботи онлайн. Завдяки ній зручніше спілкуватися та працювати онлайн, а також стимулювати швидше впровадження інновацій в організації. Але коли друзі поширюють фотографії, колеги співпрацюють над новим продуктом або державні установи керують онлайновими службами, не завжди зрозуміло, де зберігаються дані. Користувачі можуть ненавмисно перемістити дані до менш захищеного розташування й у такий спосіб підвищити ризик несанкціонованого доступу до них. Конфіденційність даних також стає все більш важливою для користувачів і державних установ. Згідно з Генеральним регламентом із захисту персональних даних (GDPR) і Законом про звітність і безпеку медичного страхування (HIPAA), організації мають збирати інформацію прозоро й упроваджувати політики, які допомагають запобігти викраденню або неналежному використанню даних. Недотримання цих вимог може призвести до значних збитків і підриву репутації організації. Організаціям потрібно продовжувати використовувати хмару, щоб залишатися конкурентоспроможними, швидко ітерувати, спрощувати для працівників і клієнтів доступ до служб, а також захищати дані й системи від наведених нижче загроз.

1) Уражені облікові записи. Зловмисники часто використовують фішингові компанії, щоб викрадати паролі працівників і отримувати доступ до систем та важливих корпоративних ресурсів.

2) Уразливості апаратного й програмного забезпечення. Незалежно від того, яку хмару використовує організація (загальнодоступну або приватну), надзвичайно важливо підтримувати апаратне й програмне забезпечення в справному та актуальному стані.

3) Внутрішні загрози. Людський фактор нерідко стає причиною порушення вимог безпеки. Причиною атак можуть стати неправильні конфігурації, небезпечні посилання, за якими часто переходять, не знаючи того, працівники, або переміщення даних до менш захищених розташувань.

4) Недостатня видимість хмарних ресурсів. Цей вид ризиків для хмари

ускладнює виявлення вразливостей і загроз та реагування на них, що може призвести до порушень і втрати даних.

5) Відсутність пріоритезації ризиків. Отримавши видимість хмарних ресурсів, адміністратори безпеки можуть бути перевантажені через величезний наплив рекомендацій щодо посилення захищеності. Важливо визначити пріоритетність ризиків, щоб адміністратори зосереджувалися на найважливішому й максимально ефективно захищали середовище.

6) Дозволи, пов'язані з високими ризиками, у хмарі. Поява нових хмарних служб та ідентичностей призвела до збільшення кількості дозволів, пов'язаних із високими ризиками, у хмарі й розширення векторів атак. Індекс невикористовуваних дозволів (PCI) – це показник того, наскільки великої шкоди можуть заподіяти ідентичності на основі наданих їм дозволів.

7) Поява нових загроз. Ризики для безпеки хмар постійно змінюються й еволюціонують. Щоб захищатися від порушень вимог безпеки й утрати даних, важливо слідкувати за появою нових загроз.

8) Відсутність інтеграції між хмарною розробкою та безпекою. Щоб виявляти й усувати проблеми з кодом до початку розгортання програми в хмарі, команди з безпеки та розробки мають працювати спільно.

Існує декілька основних аспектів безпеки в хмарі, за які відповідають як постачальники, так і клієнти.

1) Обмеження доступу. Оскільки в хмарі всі ресурси доступні через Інтернет, дуже важливо переконатися, що лише належні користувачі матимуть доступ до потрібних їм інструментів протягом визначеного періоду часу.

2) Захист даних. Організації повинні розуміти, де розташовано їхні ресурси, і застосувати відповідні елементи керування для захисту даних та інфраструктури, де їх розміщено.

3) Відновлення даних. У разі порушення безпеки надзвичайно важливо мати надійне рішення для резервного копіювання та план відновлення даних.

4) План реагування. У разі атак організаціям потрібен спеціальний план, який дасть їм змогу зменшити наслідки та запобігти враженню інших систем.

5) Підхід Shift Left Security. Команди з безпеки й розробки мають співпрацювати над хмарними програмами разом, щоб захищати їх на всіх рівнях, починаючи з коду.

6) Комплексна видимість захищеності DevOps. Усувайте сліпі зони за допомогою єдиного рішення для отримання аналітики щодо захищеності DevOps на різних платформах.

7) Зосередженість команди з безпеки на нових загрозах. Зменшуйте кількість проблем із безпекою робочих середовищ, оптимізувавши конфігурації хмарних ресурсів на рівні коду.

1.3 Порівняльний аналіз найвигідніших сучасних хмарних систем

Людство, після цифрової революції минулого сторіччя та реалізації концепції хмарних технологій, настільки пришвидшила свій технологічний прогрес, що вийшла на новий рівень можливостей і паралельно з ними з’являються нові або погіршуються раніше невирішені проблеми надійності інформації. Наприклад: ефективність потужних мереж, низька вартість обладнання та пристроїв зберігання і обробки, а також необхідне масштабне вбудовування віртуалізації. Саме такі досягнення створили основу для проблем із-за пов’язаних з ними потенційних загроз та ризиків інформаційної безпеки, які будуть специфічними для хмар та обчислень. Варто згадати що, єдина перша складова навколишнього світу – це інформація, необмежений доступ до неї став ключовою подією у сучасній історії. Тому зараз, компанії усвідомлюють, що задіяння хмари – це геніальний шанс щоб, легко, швидко та за незначну вартість, отримати доступ до найкращих додатків у своїй галузі. Але із-за зросту конфіденційної інформації, яка розміщується в хмарі, починає зростати занепокоєння з приводу того, наскільки безпечним є це середовище.

Щоб повністю і точно розгледіти всю глибину проблем, потрібно хоча б поверхнево відповісти на ряд логічних питань:

1) З чого почалася ідея зі створення інформаційної хмари і як далі вона розвивалася в ідеал?

2) Наскільки зараз важливі хмарні технології для нас і яка область їх застосування на ринку IT-індустрії?

3) Хто є головними постачальниками хмарних середовищ?

4) Які існують плани, перспективи та шанси у подальшому для хмарного напряму?

Перед послідовної відповіддю на перераховані питання, краще почати з маленької історичної довідки та визначенням хмарних технологій.

Згідно з визначенням Національного інституту стандартів і технології (NIST) США, Хмарні обчислення (від англ. Cloud Computing) — це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та вивільнені з мінімальними управлінськими затратами та зверненнями до провайдера [8, С.1].

Першим же кроком до втілення хмарних технологій можна вважати появу ASP (Application service provider – провайдери послуг доступу до додатків) у другій половині 1990х років. ASP можна вважати одними із перших SaaS сервісів. Пальма першості належить сервісу електронної пошти від компанії Hotmail. Але відсутність на той час широких каналів інтернет та технологій віртуалізації стали на перепоні – за відсутності швидких та стабільних каналів інтернет користувачі не могли отримати якісні послуги, а без технологій віртуалізації неможливо було ефективно та гнучко розподіляти ресурси та масштабувати сервіси (рис. 1.3) [8, С.1].

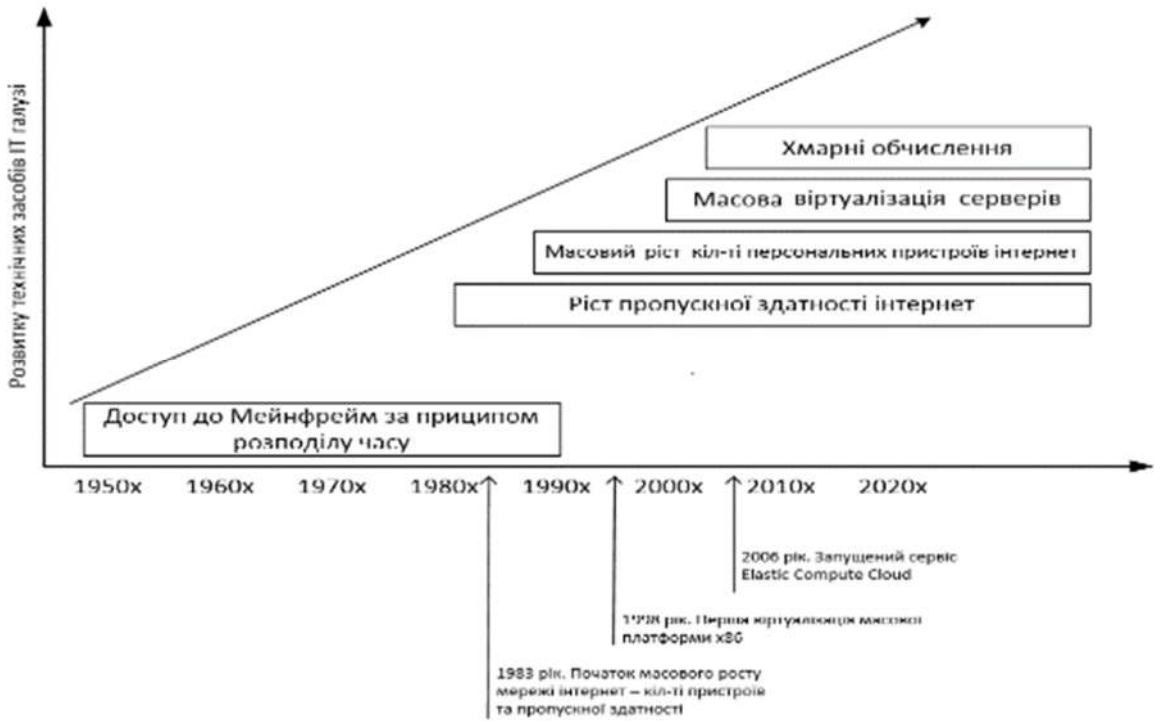

Рисунок 1.3 - Розвиток IT галузі

В цей момент доцільно наголосити що хмарочки залишаються актуальними, тому що на сьогодення задовольняють запити більшості користувачів. Вони це довели не тільки в теорії, але і в своїй справі. У глобальному вимірі, хмарні сервіси розповсюджені у багатьох галузях. Відповідно, за галузевим розподілом перше місце посідає IT-сектор (50 %), друге – сфера фінансових послуг (14 %), третє – державний сектор (рис.1.4) [9, С. 3].

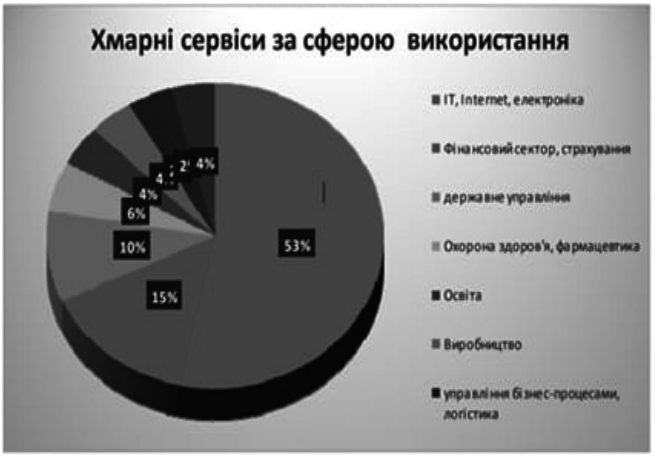

Рисунок 1.4 - Розповсюдженість хмарних сервісів за сферою використання

Для перерахуванням факторів виникнення проблем та їх самих з подальшим описом, важливо проаналізувати проблемні місця – хмарні продукти. За кожною хмарою стоїть свій провайдер, в такому ареалі не багато основних постачальників, згідно статистики приблизно дві третини ринку заняті проектами великих корпорацій такими як: Amazon Web Services, Microsoft Azure, Google Cloud Platform. На їх прикладі, ми можемо побачити більшість сучасних проблем хмар, тому що ці компанії-виробники зараз задають темп розвитку хмар на ринку (рисунок 1.5).

	Google Cloud Platform	**Amazon Web Services**	**Microsoft Azure**
Віртуальні машини	Compute Engine	EC2	Virtual Machines
Хостинг сайтів	App Engine	Elastic Beanstalk	Cloud Services
Системи контейнерів	Container Engine	EC2 Container Service	Container Service
Бази даних	Cloud Bigtable	DynamoDB	CosmosDB
Аналіз даних	BigQuery	Redshift	SQL Database
Обробка даних	Cloud Functions	Lambda	Functions
Бази даних	Cloud Datatastore	DynamoDB	Cosmos DB
Зберігання	Storage	S3	Blob Storage

Рисунок 1.5 - Популярні послуги хмарних технологій за сферою використання

Наприклад, нещодавнє дослідження State of the Cloud, проведене компанією Flexera, показало, що в 2019 році, принаймні на ринках економічно розвинутих країн, доля організацій, що використовують декілька хмарних послуг різних операторів, досягла 84%. Приблизно того ж висновку дійшли і аналітики Gartner — нещодавно проведене опитування представників експертного середовища продемонструвало, що 81% респондентів працюють з двома чи більше провайдерами [11, С.1].

Загальна безпека

В якому місці надійніший захист для даних, в локальних пристроях або на віддалених серверах?

З одного боку, дані користувачів мають кращу безпеку при внутрішньому керуванні, з іншого боку, провайдери хмарних послуг вигідно зберігають стабільну довіру і для цього використовують найбільш доступний рівень безпеки. Важливо врахувати що інформація клієнта фізично знаходиться в різних куточках світу. Тому, перед застосуванням хмарних технологій необхідно врахувати можливі загрози або ризики і для протидії їм, потрібно перевірити наявність механізмів хмарного захисту та контролю.

Недостатність ресурсів та досвіду

Не звертаючи увагу, на те що більшість IT працівників покращують свій досвід, компаніям складно знайти актуального та вагомого фахівця на ринку праці. В даній ситуації технології випереджають ринок, тому різниця в швидкості засвоєння нового стала значуща настільки, що справжні професіонали просто ще не встигли вирости в робочому плані. Високі вимоги по вирішенню та некоректна оцінка поставленого завдання знецінює будь-яку кількість наданих ресурсів. Спільне використання ресурсним потенціалом вірогідно надає тимчасовий доступ сторонньому користувачу у разі випадкового відкриття шляху до самих ресурсів.

Зайві витрати у хмарі

Деякі IT робітники, такі як розробники, вмикають хмарний сервіс з обмеженим часом дії і забувають його вчасно вимкнути. Окремим корпораціям заважає сміття та шум у хмарному трафіку, які не використовується. Бізнесмени інколи забувають, що хмарні проекти не обов’язково гарантують економію витрат, адже організації полюбляють робити зайві резервування або полінитися зробити моніторинг та автоматизацію процесів власних витрат.

Нині виділяють три основні моделі обслуговування хмарних технологій, які іноді називають шарами хмари. Можна сказати, що ці три шари – послуги інфраструктури, послуги платформи і послуги додатків – відображають будову не тільки хмарних технологій, а й інформаційних технологій загалом.

До послуг інфраструктури (Infrastructure as a Service – IaaS) можна віднести набір фізичних ресурсів, таких як сервери, мережеве обладнання та на-

копичувачі, пропоновані замовникам як послуг, що надаються. Послуги інфраструктури вирішують завдання належного оснащення ЦОД, надаючи обчислювальні потужності в міру необхідності. Зазвичай ці послуги підтримують інфраструктуру і набагато більшу кількість споживачів порівняно з з послугами додатків. Окремим прикладом послуг інфраструктури є апаратне забезпечення як послуга (Hardware as a Service – Hardware as a Service – HaaS). Як послугу користувач отримує обладнання, на основі якого розгортає свою власну інфраструктуру з використанням найбільш підходящого ПЗ.

Споживач при цьому не керує базовою інфраструктурою хмари, але має контроль над операційними системами, системами зберігання, розгорнутими додатками і, можливо, обмежений контроль вибору мережевих компонентів (наприклад, хост із мережевими екранами). У такому разі захист платформ і додатків забезпечує сам споживач, а провайдер хмари повинен організувати захист інфраструктури. Для надання ресурсів на вимогу часто використовується віртуалізація.

Переваги. Зниження капіталовкладень в апаратне забезпечення. Оскільки в цій моделі зазвичай використовують методи віртуалізації, можна домогтися економії в результаті більш ефективнішого використання ресурсів. Зменшення ризику втрати інвестицій і порога впровадження, можливість плавного автоматичного масштабування.

Недоліки. Бізнес-ефективність і продуктивність дуже залежать від можливостей постачальника. Існує ймовірність, що будуть потрібні потенційно великі довгострокові витрати.

Прикладами послуг інфраструктури є IBM SmartCloud Enterprise, VMWare, Amazon EC2, Windows Azure, Google Cloud Storage, Parallels Cloud Server і багато інших.

Послуги платформи (Platform as a S ervice – PaaS) – це модель обслуговування, в якій споживачеві надаються додатки (створені або придбані) як набір послуг. В нього входять, зокрема, проміжне ПЗ як послуга, обмін повідомленнями як послуга, інтеграція як послуга, інформація як послуга, зв’язок

як послуга тощо. Наприклад, робоче місце як послуга (Workplace as a Service – WaaS) дає змогу компанії використовувати хмарні обчислення для організації робочих місць своїх співробітників, налаштувавши і встановивши все необхідне для роботи персоналу ПЗ. Дані як послуга (Data as a Service – DaaS) надають користувачеві дисковий простір, який він може використовувати для зберігання великих обсягів інформації. Безпека як послуга (Security as a Service – SaaS) дає можливість користувачам швидко розгортати продукти, що дають змогу забезпечити безпечне використання веб-технологій, безпеку електронного листування, а також безпеку локальної системи. Цей сервіс дає змогу користувачам економити на розгортанні та підтримці своєї власної системи безпеки.

Іншими словами, модель PaaS – це IaaS разом з операційною системою та її інтерфейсом прикладного програмування (API – Application Programming Interface). Споживач при цьому не керує базовою інфраструктурою хмари, зокрема мережами, серверами, операційними системами та системами зберігання даних, але має контроль над розгорнутими додатками і, можливо, деякими параметрами конфігурації середовища хостингу. Таким чином, споживач повинен подбати про забезпечення захисту додатків, які будуть розгорнуті на наданих платформах.

Застосунки можуть працювати як у хмарі, так і в традиційних ЦОД підприємства. Для досягнення масштабованості, необхідної в хмарі, різні пропоновані послуги часто віртуалізуються, як і розглянуті раніше послуги інфраструктури.

Переваги. Плавне розгортання версій. Плавність означає, що в ідеалі користувач має слабко відчувати або навіть взагалі не відчувати зміни ПЗ у хмарі.

Недоліки. Як і в попередньої моделі обслуговування, централізація вимагає надійних заходів безпеки.

Прикладами послуг платформи слугують IBM SmartCloud Application Services, Amazon Web Services, Windows Azure, Boomi, Cast Iron, Google App

Engine та інші.

Послуги додатків (Software as a S ervice – SaaS) передбачають доступ до додатків як до сервісу, тобто додатки провайдера запускаються в хмарі та надаються користувачам на вимогу як послуги. Іншими словами, користувач може отримувати доступ до ПЗ, розгорнутого на віддалених серверах, за допомогою Інтернету, причому всі питання оновлення та ліцензій на дане ПЗ регулюються постачальником цієї послуги. Оплата в цьому випадку здійснюється за фактичне використання ПЗ. Іноді ці послуги постачальники роблять безкоштовними, оскільки в них є можливість отримувати дохід, наприклад, від реклами. Застосунки доступні за допомогою різних клієнтських пристроїв або через інтерфейси тонких клієнтів, такі, наприклад, як веб-браузер, або веб-пошта, або інтерфейси програм. Споживач при цьому не керує базовою інфраструктурою хмари, зокрема мережами, серверами, операційними системами. На кінцевому користувачеві лежить відповідальність тільки за збереження параметрів доступу (логінів, паролів тощо) і виконання рекомендацій провайдера щодо безпечних налаштувань застосунків. Найпоширенішим прикладом додатків цього типу є поштові сервіси GMail, Mail.ru, Yahoo Mail.

Взагалі існують тисячі додатків SaaS, і завдяки технології Web 2.0 їхня кількість зростає з кожним днем. Існує ПЗ, що управляє нарахуванням заробітної плати, кадровими ресурсами, колективною роботою, взаємовідносинами з клієнтами та бізнес-партнерами тощо.

Переваги. Зниження капіталовкладень в апаратне забезпечення та трудові ресурси; зменшення ризику втрати інвестицій; плавне ітеративне оновлення.

Недоліки. Як і в попередніх двох моделях, централізація вимагає надійних заходів безпеки.

Прикладами SaaS є Gmail, Google Docs, Netflix, Photoshop.com, Acrobat.com, Intuit QuickBooks Online, IBM LotusLive, Unyte, Salesforce.com, Sugar CRM і WebEx. Значна частина зростаючого ринку мобільних додатків також є реалізацією SaaS.

2 ШЛЯХИ ВИРІШЕННЯ У ВИПАДКАХ КОМБІНАЦІЇ ХМАРНИХ ПРОДУКТІВ ВІД РІЗНИХ ПРОВАЙДЕРІВ В ІТ-ІНФРАСТРУКТУРІ

2.1 Безпека хмарних даних

У світі, де мультихмарні середовища стають все більш поширеними, безпека цих середовищ є головним пріоритетом. Ось кілька найкращих практик, які допоможуть захистити ваші мультихмарні середовища.

1) Навчання команди. Переконайтеся, що ваша команда глибоко розуміє принципи мультихмарної безпеки, зокрема особливості роботи з різними хмарними платформами та протоколами безпеки.

2) План реагування на інциденти. Розробляйте детальні плани реагування на інциденти, які враховують специфіку кожного хмарного середовища, включаючи процедури виявлення, ізоляції та пом’якшення наслідків інцидентів.

3) Розподіл відповідальності. Чітко визначте межі відповідальності за безпеку між вашою компанією та хмарними провайдерами, враховуючи тип надання послуг, таких як IaaS, PaaS та SaaS, а також специфіку контрактів SLA та особливості SLO та SLI.

4) Уніфікація інструментів безпеки. Стандартизуйте інструменти безпеки та протоколи їх використання, щоб забезпечити узгодженість і можливість швидкого реагування на інциденти в будь-якому хмарному середовищі.

5) Узгоджені політики безпеки. Розробляйте і впроваджуйте єдині політики безпеки, які будуть застосовуватися на всіх хмарних платформах, забезпечуючи тим самим однорідний рівень захисту.

6) Безпека понад усе. Інтегруйте принципи безпеки з самого початку процесів розробки та розгортання, а також пріоритетних критеріїв вибору хмарних провайдерів.

7) Управління ідентифікацією та доступом (IAM). Розробляйте стратегії

IAM, що забезпечують контроль доступу на основі ролей і принцип найменших привілеїв для запобігання несанкціонованому доступу до хмарних ресурсів.

8) Шифрування даних. Застосовуйте методи шифрування на всіх етапах життєвого циклу даних – під час зберігання, передачі та обробки – для забезпечення їх конфіденційності та цілісності.

9) Управління ключами шифрування. Впроваджуйте стратегії управління ключами шифрування, які враховують регуляторні вимоги та необхідність забезпечення доступу до даних у разі потреби.

10) Забезпечення захисту на різних хмарних платформах. Використовуйте інструменти безпеки, такі як CloudGuard від Check Point, які можуть забезпечити безперервний захист даних і додатків під час їх міграції між різними хмарними платформами.

11) Забезпечення видимості в мультихмарному середовищі. Використовуйте інструменти моніторингу та аналітики, такі як Splunk або Datadog, щоб забезпечити повну видимість і контроль над усіма вашими хмарними середовищами, що дозволить своєчасно виявляти інциденти безпеки та реагувати на них.

12) Регулярне тестування безпеки. Регулярно проводьте аудит безпеки та тести на проникнення, щоб вчасно виявляти та усунути вразливості, а також перевіряти ефективність ваших заходів безпеки. Це може включати використання таких інструментів, як OWASP ZAP для тестування на проникнення або послуги інших компаній для проведення аудиту безпеки.

За безпеку в хмарі відповідають як постачальники хмарних служб, так і їхні клієнти. Ступінь відповідальності залежить від типу служб, що пропонуються.

2.2 Критерії безпечної хмари при мультихмарності

У США асоціація Cloud Security Alliance випустила Cloud Controls Matrix. Цей документ являє собою перелік існуючих технологій інформаційної безпеки, які можуть бути використані в хмарних сервісах. Хоча деякі фахівці вважають, що для управління ІБ при побудові хмари SaaS можуть бути використані стандарти ISO 27001 та ISO 27002, все ж необхідна розробка спеціальних стандартів для хмарних технологій (рисунок 2.1) [5, С.1].

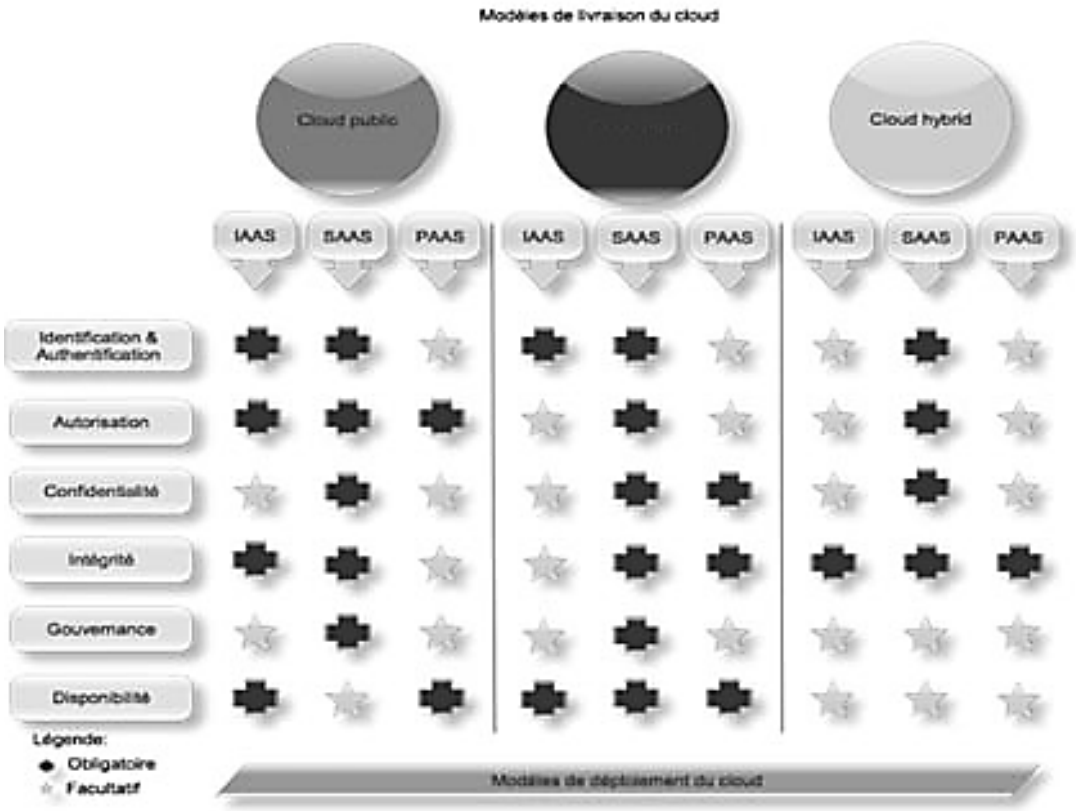

Рисунок 2.1 - Безпека хмарних обчислень

3 ДОСЛІДЖЕННЯ ВПЛИВУ ХМАРНИХ ТЕХНОЛОГІЙ НА ОСВІТНІЙ ПРОЦЕС ЗВО

3.1 Заходи безпеки в хмарі для забезпечення неперервності освітнього процесу

Хмарна безпека ефективно використовується як технологія та політика для суворого маніпулювання послугами в онлайн-системі. Порівнюючи хмарну безпеку між загальнодоступними та локальними системами, то загальнодоступна хмарна безпека може бути вразливою і схильною до кібератак. Найпоширенішою причиною загроз у хмарної безпеки є слабкі системи безпеки та необережні або недосвідчені вразливі інсайдери корпорації, яка покладається або збирається впроваджувати безпеку хмарних сервісів у відкритому доступі.

Оскільки більшість корпорацій, які впроваджують хмарні системи, потребують комплексної безпеки, про яку здебільшого думає кожна організація, що розгортає свої хмарні сервіси для своїх споживачів, які перебувають у відкритому доступі. Хмарні обчислення можна класифікувати як публічні, приватні та гібридні хмари.

Публічна хмара - це модель хмарних технологій, яка використовується для надання хмарних технологій, яка використовується для надання послуг споживачеві через інтернет-з'єднання.

Приватна хмара - це модель хмарних технологій, яка зазвичай призначена для забезпечити бездротове з'єднання, яке використовується для внутрішнього користування в межах однієї організації.

Гібридна хмара - це хмарний підхід, який використовує як публічні, так і приватні хмарні хмарні системи, які використовують як публічні, так і приватні хмари. Більшість корпорацій тримають 38% робочого навантаження в публічній хмарі, а 41% - у приватній, де приватна хмара використовується

для критично важливих де приватна хмара використовується для критично важливої діяльності, а дещо менш життєво важлива робота - у публічній хмарі.

Інфраструктура хмарних технологій надає різноманітні інструменти, які допомагають у досягненні освітніх цілей. Вона широко доступна, що робить її набагато кориснішою для інтеграції хмарних технологій у кожне освітнє середовище. Було підготовлено кілька звітів про впровадження хмарних технологій в освіту, і всі вони схиляються до думки, що хмари є важливим освітнім інструментом, але захист залишається проблемою, яку необхідно вирішити, щоб максимізувати його переваги.

Хмарні додатки в основному використовуються для командної роботи, розповсюдження контенту, мережевої взаємодії та доступу до освітніх заходів, а вища освіта стрімко впроваджує хмарні сервіси через хмарні сервіси через економічні переваги, швидкість, гнучкість, доступність та еластичності.

Загрози комп'ютерного захисту є найбільш суттєвою перешкодою для впровадження хмарних технологій у вищій освіті, а користувачі хмарних систем занепокоєні проблемами безпеки, що, на їх думку, є підтвердженням необхідності вирішення питань безпеки перед широким впровадженням хмарних технологій. Однією з найактуальніших для розробників сьогодні є конфіденційність даних користувачів на хмарних серверах. Хмарні обчислення, згідно зі звітом, надають інтерфейс, форум та освітні ресурси, які забезпечують доступне і творче навчання атмосферу; середовище, яке уможливлює співпрацю між усіма учасниками навчання, а також між різними освітніми установами, що покращує стан та підвищує ефективність освіти.

Освітня екосистема в усьому світі постійно змінюється і розвивається, що пов'язано з через серйозні виклики, пов'язані зі спробами впровадити сучасні та інноваційні технології та навчальні середовища у свої сучасні та інноваційні технології та навчальні середовища у свої процеси викладання та навчання. Вступ, зарахування, навчання та ведення документації - це лише деякі з багатьох аспектів освіти, які стали технологічними. Сервіси хмарних

технологій можна використовувати для підвищення конкурентоспроможності майже у всіх сферах освіти. Парадигма хмарних технологій підтримує як викладачів і студентів, так і академічні установи. Студенти, викладачі, адміністративні асистенти, відділ оцінювання та вступна кампанія є одними з клієнтів освітньої хмарної системи. освітньої хмарної системи.

Розширення доступу до освітніх можливостей має потенціал для покращення академічної успішності студентів. Хмарні сховища також допомагають модернізувати навчання, полегшуючи перехід від традиційної до оновленої педагогіки, яка враховує різноманітність в освіті та навчанні.

Прийняттю та поширенню хмарних обчислень перешкоджають проблеми безпеки. Це пов'язано з тим, що деякі люди стали більш обережними у використанні хмарних технологій через занепокоєння щодо конфіденційності. Незважаючи на численні переваги хмарних технологій, з'являється все більше занепокоєння щодо безпеки хмарної інформації. Багато з основних функцій, які роблять хмарні сховища такими привабливими хмарних сховищ, не лише поставили існуючу інфраструктуру безпеки під сумнів, але й виявили проблеми з безпекою.

У недалекому майбутньому хмарні обчислення стрімко розвиватимуться, збільшуючи вразливість хмарних сервісів до вірусів, хакерів та кібератак, оскільки організована злочинність, терористи та іноземні угруповання розглядатимуть їх як нову концепцію для спроб викрасти приватну інформацію, порушити роботу сервісів та завдати шкоди організації. У хмарних обчисленнях існує багато проблем з безпекою, більшість з них все ще присутні в усіх інших нових технологіях. Залежно від моделі мережевого сервісу, що використовується, ці загрози та вразливості набувають різних типів. Існують такі різноманітні проблеми захисту хмарних технологій:

1) Безпека. Основною проблемою є безпека та конфіденційність: люди просто не знають де зберігаються їхні дані, а також не можуть їх контролювати.

2) Інтероперабельність. Оскільки єдиного хмарного стандарту не розроб-

лено, існує великий ризик для підтримки постачальників.

3) Контроль. Ступінь впливу, який клієнт хмарних сервісів має на свій світ, може бути дуже різним. суттєво різниться.

4) Продуктивність Будь-яке підключення до хмари здійснюється через Інтернет, що вносить затримку в кожне з'єднання між інфраструктурою та клієнтом.

5) Надійність. Багато сучасних хмарних інфраструктур залежать від звичайного обладнання яке часто виходить з ладу в невідповідний час.

6) Продуктивність. Мовна специфіка. Деякі хмарні системи підтримують лише обмежену кількість мов.

Коли інформація зберігається або використовується в хмарі, необхідність захисту даних від можливих атак або вразливостей, які впливають на їхню конфіденційність, стає очевидною.

Аналіз функцій безпеки, які пропонують Google Workspace і Microsoft Office 365 для освітніх закладів свідчить про надійні засоби захисту обох хмарних технологій.

Google Workspace використовує вдосконалений штучний інтелект для автоматичного виявлення та відбиття таких загроз, як фішинг і спам. Він також забезпечує запобігання втраті даних у Gmail і Диску, двоетапну перевірку та примусове застосування ключів безпеки. Google Vault для електронного пошуку та архівування також гарантує, що ви зможете керувати даними вашої організації та зберігати їх для юридичних і нормативних цілей.

Microsoft 365 також пропонує розширені можливості захисту від загроз, зокрема безпечні посилання та безпечні вкладення. До нього входять такі функції, як запобігання втраті даних, eDiscovery та можливості юридичного утримання. Microsoft 365 також забезпечує багатофакторну автентифікацію та включає засоби керування мобільними пристроями, які можуть захистити дані на загублених або викрадених пристроях.

Microsoft 365 надає 30-денну історію файлів і автоматично очищає Корзину, коли досягається ліміт зберігання. Методи архівування, такі як е-

Discovery та Litigation Hold, не забезпечують простого, необмеженого відновлення в будь-який момент часу і можуть бути включені не в усі плани.

Google надає 30-денну історію видалених файлів з автоматичним очищенням кожні 30 днів. Google Vault, хоча і є архівним сховищем, включений не в усі плани Google Диска, а відновлення файлів може бути виснажливим, обмеженим у часі та схильним до помилок.

Однак, ані Microsoft 365, ані Google не пропонують вбудованих додатків для оперативного резервного копіювання та відновлення даних.

3.2 Порівняльний аналіз хмарних технологій у освітньому процесі

Хмарні обчислення приваблюють широке коло осіб та організацій, починаючи від стартапів, телекомунікаційних провайдерів, навчальних закладів, корпорацій, державних установ та навіть початківців. Хмарні обчислення надають споживачам багато переваг і скорочують витрати, дозволяючи їм заощаджувати величезні суми грошей, які мали б витрачатися на сховища даних та інфраструктуру.

Обмін даними також є окремим аспектом хмарних технологій. Можливість обмінюватися файлами закладає основу для створення архівів навчальних ресурсів, доступних для всіх учнів. Спільний доступ до ресурсів серед вчителів допомагає поширювати та повторно використовувати навчальні матеріали. Для сучасної вищої освіти хмарні обчислення мають вирішальне значення. Вони можуть покращити використання та застосування технологій у процесі викладання та навчання, а також забезпечить взаємозв'язок і спільну роботу в освіті. Хмара робить навчання більш інтерактивним і гнучким. Вона розширює межі освіти і навчання далеко за межі шкіл і класів. Як наслідок, хмарні технології, без сумніву, є однією з інновацій які матимуть значний вплив на вищу освіту.

Хмарні технології дозволяють викладачам за допомогою простого та масштабованого інтерфейсом планувати лекції, семінари, конференції та до-

повіді, а також можливість працювати де завгодно і з власного комп'ютера виконувати завдання, готувати онлайн-іспити, виставляти оцінки та складати розклад занять. складати розклад занять. Хмарне навчання також має потенціал відігравати значну роль у цифровому освітньому майбутньому. Щоб задовольнити потребу у використанні нових технологій в освіті, вищі навчальні заклади вищі навчальні заклади перейшли на хмарні технології. Шкільна освіта є визначальним фактором для вдосконалення хмарних обчислень. Хмарні обчислення надають широкий спектр послуг клієнтам, включаючи програмне забезпечення як послугу (SaaS), платформу як послугу (PaaS) та Інфраструктура як послуга (IaaS), багато з яких є корисними в освітній сфері. Сучасні "хмарні" системи, такі як "Microsoft" і "Google", надають студентам і викладачам безкоштовні ресурси навчальних закладів, такі як електронна пошта, списки контактів, розклади, збір баз даних, формування та розповсюдження документів, а також можливість формування та розповсюдження документів, а також можливість створювати веб-сайти. Належне використання хмарних технологій полегшує інтеграцію технологій у навчальні програми. Хмарні технології інфраструктури сприяли впровадженню в різні ЗВО через отримання доступ до хмарних технологій в освіті, а їхні можливості та сервіси - за запитом. Викладачі можуть використовувати хмарні інструменти, щоб допомогти їм спланувати навчальне портфоліо, лекцію про викладання для місцевої аудиторії, презентацію на конференції або чернетку для публікації.

Студенти та працівники можуть мати зручний доступ до освітніх інструментів з хмари за допомогою хмарного програмного забезпечення, такого як Microsoft Office 365. Інфраструктура хмарних обчислень допомагає ідеї масових відкритих онлайн-курсів (МВОК). Зручність використання навчальних ресурсів, що містяться в хмарі, дозволяє викладачам швидко вдосконалювати свої предметні області. Широке використання мобільних пристроїв в останні роки - це розвиток, який часто поєднується з хмарними технологіями. Комп'ютерні обчислення, навчання за допомогою смартфонів, імерсивне навчання та дистанційне навчання - все це завдяки хмарним технологіям. Мобі-

льні технології, такі як смартфони і ноутбуки, широко використовуються учнями, і вони можуть мати зручний доступ до цінного хмарного контенту.

Google Workspace (раніше G Suite) і Microsoft 365 (раніше Office 365) пропонують набір інструментів для продуктивності та співпраці. Google Workspace включає такі програми, як Документи, Таблиці, Слайди та Форми Google, а також інструменти для спілкування, такі як Gmail, Meet і Чат. Microsoft 365 включає такі програми, як Word, Excel, PowerPoint і Outlook, а також інструменти для спілкування, такі як Teams і Skype.

Однією з найбільших відмінностей між цими двома платформами є їхній підхід до зберігання файлів. Google Workspace пропонує Google Диск, який дозволяє користувачам зберігати файли в хмарі, отримувати до них доступ і ділитися ними. Microsoft 365 пропонує OneDrive для бізнесу, який має схожу функціональність. Однак Microsoft 365 також включає SharePoint - потужну платформу для спільної роботи, яка дозволяє командам зберігати й упорядковувати файли, створювати інтранет-сайти та створювати власні робочі процеси.

Обидві платформи пропонують мобільні додатки для пристроїв iOS і Android, а також веб-доступ до своїх додатків. Google Workspace і Microsoft 365 пропонують співпрацю в режимі реального часу, дозволяючи декільком користувачам одночасно працювати над одним документом.

І Google Workspace, і Microsoft 365 відносно прості у використанні, але вони мають деякі відмінності в інтерфейсі та функціональності. Google Workspace має простий, впорядкований інтерфейс, в якому легко орієнтуватися. Набір додатків розроблений для безперебійної спільної роботи, а функції співпраці в режимі реального часу є інтуїтивно зрозумілими і простими у використанні.

Microsoft 365 має складніший інтерфейс, але він також пропонує більше функціональних можливостей, ніж Google Workspace. Набір програм є потужним і налаштовуваним, а функції співпраці в реальному часі - надійними. Однак деякі користувачі можуть вважати інтерфейс перевантаженим і

складним для навігації.

Існує кілька основних відмінностей між Microsoft і Google, які часто не беруть до уваги, коли вирішують, яку з них обрати. Здається, що вони обидві пропонують чудові сервіси. Іноді основна різниця полягає в тому, як кожна з компаній здійснює свою діяльність. Microsoft - це компанія, що займається розробкою програмного забезпечення. Її мета проста: політика Microsoft полягає в тому, щоб використовувати ваші дані лише для того, за що ви нам платите - для підтримки та надання онлайнових служб Microsoft. Ми зобов'язуємося не використовувати їх для інших цілей. Наші бізнес-служби розроблені та функціонують повністю окремо від споживчих служб корпорації Майкрософт. Хоча деякі дані можуть зберігатися або оброблятися в системах, що використовуються як для споживчих, так і для бізнес-служб, дані бізнес-служб не передаються системам, що використовуються для реклами.

Google - це зовсім інше. Це, по суті, рекламна компанія. Для того, щоб користуватися Microsoft, потрібна покупка. Google пропонує свої послуги безкоштовно. Зрештою, їхній стимул полягає в тому, щоб зібрати якомога більше ваших даних - електронних листів, документів, файлів, записів у календарі та розмов - щоб дізнатися про вас більше, що зробить їхню рекламу більш ефективною. Щоб побачити це в дії, достатньо лише поглянути на Умови використання Google. "Коли ви завантажуєте або іншим чином надаєте контент до наших Сервісів, ви надаєте компанії Google (і тим, з ким ми співпрацюємо) всесвітню ліцензію на використання, розміщення, зберігання, відтворення, модифікацію, створення похідних робіт (наприклад, в результаті перекладів, адаптацій або інших змін, які ми вносимо, щоб ваш контент краще працював з нашими Сервісами), передачу, публікацію, публічне виконання, публічний показ і розповсюдження такого контенту. Права, які ви надаєте за цією ліцензією, надаються з обмеженою метою експлуатації, просування та вдосконалення наших Сервісів, а також для розробки нових Сервісів. Ця ліцензія продовжує діяти, навіть якщо ви припиняєте користуватися нашими Службами (наприклад, для списку компаній, який ви додали на Карти

Google)".

За останні кілька років компанія Google дійсно досягла значних успіхів у створенні освітніх онлайн-інструментів. Українські вчителі активно використовувати Google Classroom як повсякденний інструмент! Існує багато інших онлайн-додатків, до яких користувачі можуть отримати доступ і використовувати їх на свою користь. Найбільша перевага полягає в кількох моментах. Дані зберігаються автоматично. Вам не потрібно турбуватися про те, що ви втратите свою роботу! Працювати на основі сервісів Google можна з будь-якого місця! Можна ділитися та співпрацювати з іншими людьми в режимі реального часу. Це робить проекти та завдання набагато швидшими. Співпраця є ключовим фактором для шкіл та бізнесу. Той факт, що всі сервіси Google об'єднані в пакет і безперебійно працюють разом, робить їх дуже привабливими для цих установ.

Microsoft Office 365, тепер відомий просто як Microsoft 365, - це набір хмарних програм для підвищення продуктивності, які можна використовувати онлайн або на робочому столі. До нього входять такі популярні програми, як Microsoft Word, Microsoft PowerPoint і Microsoft Excel, а також доступ до хмарного сховища, ділової електронної пошти та інших інструментів для співпраці.

Office 365 бере класичні офісні програми Microsoft і робить їх доступними в хмарі для покращення співпраці між членами команди. Гібридна система настільних програм і браузерних додатків дозволяє вам і вашій команді легко працювати над важливими проектами з будь-якого пристрою. Office 365 також має адміністративний інтерфейс, який дозволяє легко керувати:

- безпекою;
- дозволами користувачів;
- відповідністю нормативним вимогам.

Окрім базових продуктів, Microsoft 365 відомий своїми розширеними функціями, зокрема автоматизацією робочих процесів для електронної пошти, плануванням тощо. Це робить Microsoft 365 чудовим вибором для освітніх

закладів, які шукають способи оптимізувати свої процеси та підвищити ефективність адміністративних операцій.

Проведення відеозустрічей є відмінною рисою сучасного дистанційного формату навчання. У Google Workspace для проведення конференцій використовується платформа Meet, а в Office 365 - Microsoft Teams. Для базових можливостей відеоконференцій, Google Meet пропонує безліч опцій для спільного використання екранів, налаштування окремих кімнат і використання чату під час наради. Однак Teams має надійну платформу, яка перевершує Meet у кількох сферах. У Teams надано вражаючий ліміт в 300 учасників порівняно зі 100 учасниками для базового рівня Google Workspace. Наради можуть тривати до 30 годин, що перевищує 24-годинний ліміт Meet.

Google Workspace - явний переможець, коли справа доходить до спільної роботи. Хоча обидві платформи мають опції для спільної роботи, вебналаштування Workspace полегшує взаємодію кількох людей у режимі реального часу. Зокрема, оскільки всі документи Google Workspace зберігаються в хмарі, користувачі можуть легко отримати доступ до спільного документа в будь-який час.

З іншого боку, оскільки освітні заклади, які використовують Office 365, мають можливість працювати на своїх робочих столах, їм, можливо, доведеться завантажувати свої документи в хмару, щоб ділитися ними з іншими в Інтернеті.

Важливо, щоб ваш цифровий робочий простір забезпечував безпеку всієї інформації вашого бізнесу. І Office 365, і Google Workspace надають пріоритет безпеці своїх клієнтів, забезпечуючи протоколи автентифікації, спеціальні адміністративні ролі та функції конфіденційності даних.

Office 365 включає додаткову аналітику безпеки у своїх планах вищого рівня, що може бути корисним для підприємств зі складними вимогами до безпеки.

Хоча Office 365 має більше різноманітних функцій безпеки, Workspace, як і раніше, забезпечує надійний захист конфіденційності, щоб зберегти вашу

інформацію в хмарі в безпеці.

3.3 Рекомендації щодо вибору технологій та покращення рівня безпеки хмарних сервісів закладів освіти

Клієнти значною мірою покладаються на технології для підключення до хмарних обчислень, і більшість цих сервісів вразливі до крадіжки даних, відмови в обслуговуванні, збору інформації, спуфінгу, впровадження шкідливого програмного забезпечення та фішингу. Витік інформації є поширеною проблемою безпеки в хмарних сховищах, і вона виникає, коли конфіденційна інформація потрапляє в чужі руки під час передачі, запису або аналізу. Як наслідок, незалежно від того, чи є мережа або сервер незахищеними, це зробить хмарні сервіси більш вразливими до атак. Найважливішими проблемами безпеки, з якими стикаються вищі навчальні заклади, що використовують різні хмарні сервіси є наступні:

- погана видимість. Кожен хмарний провайдер використовує свій підхід до захисту, що робить уніфіковані політики та реалістичну видимість надзвичайно складним завданням;

- відсутність інтеграції та координації. Фрагментарні та ізольовані заходи безпеки є поширеним явищем;

- реактивна безпека. Школи не можуть дозволити собі реактивну політику захисту в епоху атак "нульового дня" і скорочення періоду між вторгненням і зломом вікна.

Приватні особи та організації повинні оцінювати ризики, пов'язані з хмарними платформами, перш ніж використовувати їх. Це пов'язано з тим, що в той час, як аналітики намагаються вирішити проблеми безпеки хмарних технологій, виникають нові загрози, що ще більше ускладнює вирішення питань безпеки хмарних технологій. Це означає, що хмарні провайдери повинні виділяти більше ресурсів на захист даних, щоб зберегти довіру та лояльність своїх клієнтів. Установи, які бажають передати свою інформацію на аутсор-

синг у хмару, можуть вжити наступних заходів, щоб перевірити та оцінити захист у хмарі, пропонований постачальником хмарних послуг, як-от розуміння хмари починається з розуміння того, як особлива вільна організація хмари впливає на конфіденційність даних, що подаються туди. Це вимагає глибокого розуміння того, як хмарні обчислення передають дані та керують ними.

Рекомендації щодо вибору хмарного сервісу, постачальника та покращення рівня безпеки хмарних сервісів для освітніх установ:

- вимагайте прозорості, підтверджуючи, що тепер постачальник хмарних послуг здатний приймати планові перевірки безпеки та запропонує конкретні деталі своєї архітектури безпеки;

- посилити внутрішній захист, переконавшись, що внутрішні технології та політики безпеки постачальника послуг, такі як брандмауери та списки контролю доступу, є надійними та сумісними з хмарними протоколами безпеки, а також враховувати юридичні наслідки, розуміючи, як правила та законодавство можуть вплинути на все, що ви завантажуєте в хмару;

- також слідкуйте за будь-якими розробками або вдосконаленнями хмарних технологій і процедур, які можуть вплинути на захист ваших файлів;

- контроль доступу, використання цифрових підписів і хешів, а також використання систем запобігання вторгненням - це лише кілька прикладів;

- надійне шифрування - сильний регуляторний механізм для покарання хакерів. Автентифікація та авторизація - це два терміни, які використовуються як взаємозамінні;

Необхідно підвищувати обізнаність користувачів щодо питань захисту в хмарі. На випадок катастрофи необхідно мати резервну копію даних. Для запобігання інсайдерським атакам необхідна належна перевірка співробітників і користувачів.

Розгортання баз даних, хмарних сервісів і робочих навантажень додатків у декількох публічних хмарах збільшує поверхню атаки організації, надаючи цифровим супротивникам більше можливостей атакувати інфра-

структуру (наприклад, за допомогою бот-мереж, шкідливих програм і експлойтів "нульового дня"), а також підвищує ризик витоку даних.

Деякі прихильники мультихмарних технологій стверджують, що розподіл активів між загальнодоступними хмарами може зменшити ризик кібератаки, але також існує ймовірність того, що порушення безпеки в одній хмарі може горизонтально поширитися на інші хмари у вашому мультихмарному середовищі.

Методи забезпечення надійності використання мультихмарних середовищ полягають у створенні контрольних точок і операцій з відновлення станів програмних засобів. Як правило, такі інформаційні структури є розподіленими і використовують кілька вузлів. Тому, методи забезпечення надійності використання мультихмарних середовищх спрямовані на ефективне створення контрольних точок та операцій з відновлення станів прикладних розподілених систем.

Разом з тим, існують проблеми, які пов'язані з забезпеченням надійності мультихмарних середовищ. Під час роботи інформаційних структур із забезпечення надійності мультихмарних середовищ найбільш вразливими є процеси. Через те, що інформаційні структури на основі хмарних обчислень є розподіленими, то проблеми здебільшого відбуваються на рівні синхронізації.

До одного з дієвих методів розв'язання цієї проблеми належить пошук рішень збереження станів процесів, що знаходяться на розподілених вузлах за допомогою контрольних точок. Цей метод дає змогу досить ефективно відновлювати стан процесів у разі виникнення відмов у хмарних інформаційних структурах. Для цього необхідно, щоб процеси обмінювалися повідомленнями між собою для контролю їхніх станів. У результаті цього відбувається узгоджене збереження стану необхідних процесів.

Інший, нестандартний метод підвищення забезпечення надійності мультихмарних середовищ базується на неузгодженому збереженні станів процесів. Цей метод полягає в тому, що кожен процес віддаленого вузла само-

стійно виконує збереження контрольних точок. Однак, у цьому випадку, виникають проблеми із синхронізацією, яка може призводити до втрат даних у базах даних, неправильного виконання транзакцій після відкату в початкові стани, зниження продуктивності при відновленні станів після збоїв. Не дивлячись на такі побічні дії, цей метод широко використовується на великих розподілених хмарних платформах.

Під час використання методів забезпечення надійності використання мультихмарних середовищ важливою особливістю є порядок збереження контрольних точок у розглянутих методах полягає в послідовності дій і має певний життєвий цикл реалізації комплексу таких послідовних дій. Життєвий цикл визначає етапи збереження контрольних точок де відбувається виконання перевірки здійснюваних операцій і прийняття рішення про необхідність створення такої точки. Така послідовність дій виражена в деякому розгалуженому алгоритмі дій, де задіяно низку важливих модулів системи.

Робота системи забезпечення надійності мультихмарних середовищ дає змогу ефективно створювати контрольні точки, які якісно відновлюють задані стани розподіленої інформаційної структури.

Для відновлення стану розподіленої інформаційної структури застосовується відкат до контрольної точки процесу на вузлі, у якого виникли збої. Разом із тим, виконується відновлення повідомлень, які були відправлені в період часу між відмовою у вузлі розподіленої інформаційною структурою та контрольною точкою. Це відбувається за допомогою ведення протоколів дій, які зберігаються в базах даних серверів. Таким чином, існує можливість відновлення процесу повторно за допомогою генерації копій повідомлень, які відправлені до відмови віддаленого вузла розподіленої структури. Також, існують різні механізми управління системи забезпечення надійності мультихмарних середовищ які прописуються в конфігураційних файлах. Так, час закінчення роботи системи може відповідати такому параметру як загальна тривалість моніторингу інформаційної структури. Час початку роботи систе-

ми може бути визначено в планувальнику використовуваної операційної системи.

Ще одним способом організації забезпечення надійності мультихмарних середовищ є використання методу збереження повідомлень. Такий алгоритм організації відмовостійкої роботи хмарних обчислень передбачає запис кожного повідомлення в базу даних сервера асинхронно без зупинки процесу виконання. Такі записи можуть виконуватися централізовано (на сервері) або розподілено (на вузлах), залежно від конфігурації (налаштувань) системи. Це дає змогу відновлювати систему після помилок (або збоїв) без надлишкового синхронного збереження повідомлень у базах даних.

Щоб запобігти втраті конфіденційної інформації в сфері освіти створювати корпоративні сервери, що пропонуються надійними сторонніми постачальниками, для збереження критичних даних.

Після проведеного аналізу небезпек мультихмарного середовища, пропоную:

Метод «Повітряна кулька» - створення програмного забезпечення здатного якісно та своєчасно, одночасно не допускати перевантаження трафіку, перерозподіляючи його на інші напрямки, і у разі кібер -атаки, автоматично, без збою у системі роботи хмари, переміщувати дані на новий вузел, ховаючи шлях переміщення.

Метод « Розумна хмара» - використання штучного інтелекту для боротьби з повторно спливаючими сповіщеннями, з частковою заміною деяких функцій експертів з кібербезпеки.

ВИСНОВКИ

Хмарні обчислення стають потужною силою в освіті, але споживачі все ще стурбовані питаннями безпеки. Проблеми захисту хмарних технологій стримують їх використання в освіті та ставлять під загрозу приватність і конфіденційність користувачів хмарних технологій. У дослідженні робиться висновок, що хмарні обчислення надають студентам, викладачам та академічним установам низку освітніх переваг, серед яких ресурси для відкриття та використання освітніх технологій, економія та усунення витрат, мережева взаємодія та співпраця. Деякі навчальні заклади вже перейшли до хмарних технологій, щоб зробити свою роботу більш ефективною.

Однак зростаючі проблеми з безпекою в хмарі можуть утримати навчальні заклади від впровадження цієї технології. Як наслідок, для того, щоб усунути хмарні атаки, необхідно вдосконалити інфраструктуру захисту хмарних технологій. В результаті цього люди зможуть скористатися всіма перевагами хмарних обчислень. Це також зробить значний внесок у забезпечення студентів необхідними IT-навичками, що покращить перспективи працевлаштування, успіх та конкуренцію на сучасному цифровому робочому місці.

Google Workspace і Microsoft Office 365 - це два найкращі рішення для підвищення продуктивності, доступні на ринку для освітніх навчальних закладів. Кожна платформа обслуговує різну аудиторію, тому прийняття однозначного рішення може бути складним завданням. Проведений порівняльний аналіз Google Workspace і Microsoft 365 за такими параметрами, як безпека, ціна, налаштування, співпраця та інструменти для підвищення продуктивності, допоможуть зважити всі "за" і "проти" та вирішити, яка з платформ найбільше підійде для освітнього процесу закладу освіти.

Однак зауважимо, що і Google Workspace, і Microsoft 365, згідно з моделлю спільної відповідальності, покладають тягар захисту даних на заклад освіти. Хоча і Google Workspace, і Microsoft 365 надійно захищені, вони не

можуть захистити вас від поширених причин втрати даних, таких як випадкове видалення, зловмисне пошкодження, помилки синхронізації, програми-вимагачі та шкідливе програмне забезпечення.

Запропоновані методи, при належному програмному забезпеченні можуть:

- вести боротьбу з повторно спливаючими сповіщеннями, рекламними продуктами;
- небезпечними групами у соціальних мережах по типу «Синього кита»;
- призвести до полегшення праці експертів з безпеки;
- підвищення рівня освіти;
- зміцнення захисту персональних даних системи освіти.

Вважаю доцільним у подальшому працювати над створенням програмного забезпечення розвитку наданих методів підтримання безпеки мультихмарних середовищ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мультихмара: особливості та переваги. On your business. URL: https://onbiz.biz/multi-cloud-strategy/

2. Найпоширініші види хмарних сервісів для бізнесу. [Електронний ресурс]:Режим доступу: https://provse.te.ua/2019/05/nayposhyrenishi-vydy-khmarnykh-servisiv-dlia-biznesu/

3. What is multicloud? [Електронний ресурс] // Режим доступу: https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud

4. Miller R. Who Has the Most Web Servers? 2012. URL: http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/

5. Amrhein D., Quint S. Cloud computing for the enterprise: Part 1: Capturing the cloud. 2012. URL:http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html

6. Parse Cloud Code Getting Started. URL https://parseplatform.github.io/docs/cloudcode/guide/. Online

7. .Cloud Foundry and Iron.io Deliver Serverless. URL https://www.iron.io/cloudfoundry-and-ironio-deliver-serverless/. Online

8. Хмарні обчислення URL: http://surl.li/hdptk (дата звернення: 11.07.2023)

9. Рубцова М. Ю. Хмарні технології як інструмент поглиблення віртуалізації фінансового сектору Електронне наукове фахове видання «Електронна економіка» 2020. С.7 http://www.economy.nayka.com.ua/pdf/5_2020/112.pdf

10. Дідківська С.О. Платформи хмарних технологій: порівняльний аналіз наукова робота студентки Житомирського державного університет імені Івана Франка С.136 http://surl.li/kxurb

11. Multicloud – перевага чи проблема URL: https://denovo.ua/blog/multicloud-perevega-chi-problema-75 (дата звернення: 11.07.2023)

12. Никишин Д.Д., Федюшин О.И. Ризики інформаційної безпеки в хмарних сервісах матеріали першого міжнародного науково-практичного форуму 2019. С. 80–81 http://surl.li/kxvhq

13. Безпека хмарних технологій URL: http://surl.li/kxuvd (дата звернення: 11.07.2023)

14. Balani, Zina, & Varol, Hacer. (2020). Cloud Computing Security Challenges and Threats. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–4.

15. Alsaadi, Elham Mohammed Thabit A, Fayadh, Sabah Mohammed, & Alabaichi, Ashwak. (2020). A review on security challenges and approaches in the cloud computing. AIP Conference Proceedings, 2290(1). https://doi.org/10.1063/5.0027460

16. Chitturi, A. K., & Swarnalatha, P. (2020). Exploration of various cloud security challenges and threats. In Soft Computing for Problem Solving (pp. 891-899). Springer, Singapore.

17. Jonathan, N. (2018). Overcoming multi-cloud Security Challenges in Education. Published by FORTINET. Retrieved from online via www.fortinet.com/blog/industry - trends/overcoming-multi-cloud-security. Accessed August, 2019.

18. Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(12), 9493-9532.