Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І. І. _____

« » 2023р.

Пояснювальна записка

до кваліфікаційної роботи магістра

за спеціальністю: 125 – Кібербезпека

на тему: «Аналіз та дослідження безпеки хмарних послуг»

оцінка « » Керівник к.т.н БІСТ Єсіна М. В.

Голова ЕК Рецензент к.т.н Бобух В. А.

Лемешко О.В. _____ Виконавець : студент групи КБ-41

Толок А.В.

Харків – 2023

РЕФЕРАТ

Робота обсягом 51 сторінок містить 8 ілюстрацій, 6 таблиць та 22 літературних посилань.

Метою роботи є дослідження сучасних методів та технологій забезпечення безпеки в хмарних сервісах, аналіз ідентифікованих загроз та ризиків і розробка рекомендацій щодо покращення безпеки в хмарному середовищі.

Методи дослідження: Аналіз літературних джерел, статей, наукових публікацій та інших документів, які стосуються теми дослідження

У роботі проаналізовані дослідження щодо безпеки хмарних послуг, у зростаючому ландшафті загроз. Наведено методи виявлення та пом’якшення наслідків різних видів атак. Сформовано стратегії для моделювання загроз.

Результати дослідження можуть бути використані для побудови системи безпеки для хмарних послуг в організація будь-якого розміру. Застосування наданих методів захисту дозволить забезпечити надійну роботу з хмарними послугами, зменшити ризики втрати даних та порушення конфіденційності.

Ключові слова: ЗАГРОЗИ ХМАРНИХ ПОСЛУГ, МОДЕЛІ ЗАГРОЗ, МОДЕЛІ ПОРУШНИКА, СИСТЕМИ МОДЕЛЮВАННЯ, ХМАРНІ ОБЧИСЛЕННЯ.

ABSTRACT

The paper consists of 51 pages, 8 illustrations, 6 tables and 22 references.

The objective of the work is to study modern methods and technologies for ensuring security in cloud services, analyze identified threats and risks, and develop recommendations for improving security in the cloud environment.

Research methods: Analysis of literature sources, articles, scientific publications and other documents related to the research topic

The paper analyzes research on the security of cloud services in the growing threat landscape. Methods for detecting and mitigating the effects of various types of attacks are presented. Strategies for modeling threats are formed.

The results of the study can be used to build a security system for cloud services in an organization of any size. The application of the provided protection methods will ensure reliable work with cloud services, reduce the risks of data loss and privacy violations.

Keywords: THREATS TO CLOUD SERVICES, THREAT MODELS, ATTACKER MODELS, MODELING SYSTEMS, CLOUD COMPUTING

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IaaS – Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

FaaS – Function as a Service

BMaaS – Bare Metal as a Service

DBaaS – Database as a Service

DDoS – Distributed Denial of Service

API – Application Programming Interface

DevOps – Development and Operations

ВСТУП

Хмарні обчислення – це нова модель надання обчислювальних послуг, коли обчислення надаються як послуга через Інтернет. Хмарні обчислення є дуже популярним вибором серед користувачів та бізнесу, оскільки обчислювальні послуги надаються за значно нижчими цінами порівняно з власною IT-інфраструктурою. У моделі хмарних обчислень обчислювальні послуги та зберігання даних передаються на аутсорсинг постачальникам хмарних послуг. Клієнти не мають повного контролю над програмами та їхніми даними. Таким чином, з'являється додаткове навантаження, пов'язане з ризиками безпеки, і безпека даних стає основною проблемою для клієнтів хмарних сервісів при розгляді хмарних послуг.

Одним з головних викликів є забезпечення конфіденційності даних в хмарному середовищі. Клієнти повинні мати гарантію, що їхні дані не доступні для сторонніх осіб без належного дозволу. Крім того, важливо забезпечити цілісність даних, щоб уникнути несанкціонованих змін чи втрати інформації.

Гарантування безпеки даних у хмарних сервісах стає надзвичайно важливим завданням, яке вимагає систематичного аналізу, дослідження та застосування ефективних методів і практик. Розуміння ризиків та викликів у сфері безпеки, а також впровадження відповідних стратегій та заходів безпеки допоможе забезпечити високий рівень захисту даних у хмарних сервісах та підтримати довіру клієнтів до використання цієї технології.

Актуальність роботи: За останні роки хмарні технології стають все більш популярними і використовуються в різних галузях, таких як бізнес, медицина, освіта, наука та інші. Водночас, зростання кількості ресурсів та підключених до мережі об'єктів, а також збільшення обсягів інформації, ставлять нові виклики щодо безпеки хмарних послуг.

Метою роботи є дослідження сучасних методів та технологій забезпечення безпеки в хмарних сервісах, аналіз ідентифікованих загроз та ризиків і розробка рекомендацій щодо покращення безпеки в хмарному середовищі.

Для досягнення поставленої мети необхідно вирішити наступні завдання: проаналізувати основні поняття, принципи та технології хмарних послуг; проаналізувати методи та технології виявлення та захисту від атак на хмарні сервіси; провести порівняльний аналіз різних хмарних платформ з точки зору їх безпеки та відповідності вимогам нормативних документів; розробити рекомендації щодо підвищення рівня безпеки при використанні хмарних послуг.

Об’єктом дослідження є захищеність інформації хмарних обчислень.

Предметом дослідження є аналіз та дослідження питань, пов'язаних з безпекою хмарних послуг, зокрема, вивчення проблем безпеки, які виникають під час роботи з хмарними послугами, а також методів та засобів забезпечення безпеки хмарних послуг.

Методи дослідження*:* аналіз літературних джерел, статей, наукових публікацій і інших документів, що стосуються теми дослідження.

1 ОГЛЯД, АНАЛІЗ ТА ДОСВІД ВИКОРИСТАННЯ ХМАРНИХ ПОСЛУГ

1.1 Основні поняття хмарних послуг

Хмара – це сервери, доступ до яких здійснюється через Інтернет, а також програмне забезпечення та бази даних, які працюють на цих серверах. Хмарні сервери розташовані в центрах обробки даних по всьому світу. Використовуючи хмарні обчислення, користувачам і компаніям не потрібно самостійно керувати фізичними серверами або запускати програмні додатки на власних комп'ютерах [1].

"Хмара" виникла як сленговий термін технічної індустрії. На початку розвитку Інтернету на технічних схемах часто зображували сервери та мережеву інфраструктуру, з яких складається Інтернет, як хмару. У міру того, як все більше обчислювальних процесів переміщалося в цю серверно-інфраструктурну частину Інтернету, люди почали говорити про перехід до "хмари" як про скорочений спосіб вираження місця, де відбуваються обчислювальні процеси. Сьогодні "хмара" є загальноприйнятим терміном для позначення цього стилю обчислень.

Хмара дозволяє користувачам отримувати доступ до одних і тих самих файлів і додатків практично з будь-якого пристрою, оскільки обчислення і зберігання відбуваються на серверах у дата-центрі, а не локально на пристрої користувача. Ось чому користувач може увійти до свого облікового запису в соціальній мережі на новому телефоні і все одно знайти свій старий обліковий запис, з усіма своїми фотографіями, відео та історією розмов.

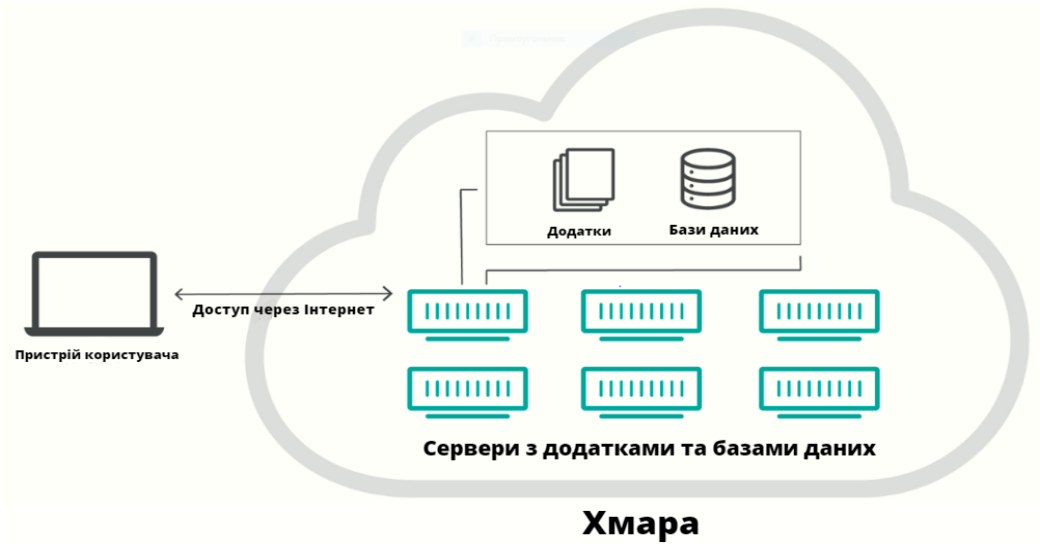

Рисунок 1.1 – Модель доступу до хмари

Хмарні сервіси – це інфраструктура, платформи або програмне забезпечення, які розміщуються у сторонніх провайдерів і стають доступними для користувачів через Інтернет [16].

Хмарні сервіси полегшують потік даних користувачів від зовнішніх клієнтів (наприклад, серверів, планшетів, настільних комп'ютерів, ноутбуків – будь-чого на стороні користувача) через Інтернет до систем провайдера і назад. Хмарні сервіси сприяють створенню хмарних додатків і гнучкості роботи в хмарі. Як і всі інші IT-ресурси, хмарні сервіси покладаються на апаратне та програмне забезпечення. Однак, на відміну від традиційних апаратних і програмних рішень, для доступу до хмарних сервісів користувачам не потрібно нічого, окрім комп'ютера, підключення до мережі та операційної системи. Хмарні обчислення дозволяють клієнтським пристроям отримувати доступ до даних і хмарних додатків через Інтернет з віддалених фізичних серверів, баз даних і комп'ютерів.

Підключення до мережі Інтернет з'єднує front-end частину, яка включає клієнтський пристрій, браузер, мережеві та хмарні програми, із back-end частиною, яка складається з баз даних, серверів і комп'ютерів. Back-end функціонує як репозиторій, зберігаючи дані, до яких має доступ front-end. Зв'язком між зовнішнім і внутрішнім інтерфейсами керує центральний сервер. Центральний сервер покладається на протоколи для полегшення

обміну даними. Центральний сервер використовує як програмне, так і проміжне програмне забезпечення для управління зв'язком між різними клієнтськими пристроями та хмарними серверами. Як правило, для кожної окремої програми або робочого навантаження існує виділений сервер.

Хмарні обчислення значною мірою покладаються на технології віртуалізації та автоматизації. Віртуалізація дозволяє легко абстрагуватися і надавати послуги та базові хмарні системи у вигляді логічних об'єктів, які користувачі можуть запитувати і використовувати. Автоматизація та супутні можливості керування надають користувачам високий ступінь самообслуговування для надання ресурсів, підключення послуг і розгортання робочих навантажень без прямого втручання IT-персоналу хмарного провайдера.

Хмарні платформи сьогодні пропонують ряд значних переваг, які спонукають компанії впроваджувати хмарні обчислення. Ці основні переваги включають в себе [2]:

1) Швидкість: Якщо вам потрібен IT-ресурс або послуга з хмари, вони стають доступними майже миттєво, і практично в той же час готові до виробництва. Це означає, що продукт, послуга та дата запуску з'являються на ринку майже миттєво, що є значною перевагою порівняно з використанням застарілого середовища. Це допомогло багатьом компаніям почати отримувати прибуток набагато швидше після запуску.

2) Вартість: Планування та купівля правильного обладнання завжди було складним завданням у традиційному застарілому середовищі. Якщо ви придбаєте обладнання, яке не відповідає вашим потребам, то, швидше за все, вам доведеться працювати з ним протягом невизначеного часу. Однак це не є проблемою для хмари, оскільки вам не потрібно купувати жодного обладнання. Замість цього ви платите за використання обладнання постачальника, і якщо воно не відповідає вашим потребам, ви можете звільнити його і замінити на кращу конфігурацію. Таким чином, ви

заощаджуєте багато грошей, оскільки платите лише за час, який використовуєте.

3) Масштабованість: У застарілому середовищі прогнозування попиту вимагає повного робочого дня, але за допомогою хмарних сервісів ви можете легко налаштувати автоматизований інструмент моніторингу, який зробить цю роботу за вас. Ця інформація дозволить вам точно збільшувати або зменшувати обсяг роботи залежно від потреб.

4) Доступність: Хмарні обчислення дозволяють вам отримувати доступ до ресурсів, даних, сервісів і додатків з будь-якого місця, якщо ви підключені до Інтернету. Якщо ви не підключені до Інтернету, деякі інструменти та методи дозволять вам отримати доступ до хмари, коли це буде потрібно.

5) Безпека: Забезпечення надійного та безпечного зберігання даних є пріоритетом для будь-якого бізнесу. Хмара забезпечує надійне зберігання даних клієнтів, Крім того, всі дані, що зберігаються в хмарі, зашифровані та захищені, щоб унеможливити їх несанкціоноване використання.

1.2 Моделі розгортання хмарних послуг

У хмарних обчисленнях ми маємо доступ до спільного сховища комп'ютерних ресурсів у хмарі. Вам просто потрібно запросити додаткові ресурси, коли вони вам потрібні. Завдяки хмарам ресурси швидко запускаються і працюють без проблем. Можна звільнити ресурси, які більше не потрібні. Цей метод дозволяє платити лише за те, що ви використовуєте. Ваш хмарний провайдер відповідає за все обслуговування.

Хмарна модель розгортання функціонує як віртуальне обчислювальне середовище з архітектурою розгортання, яка змінюється залежно від обсягу даних, які ви хочете зберігати, і від того, хто має доступ до інфраструктури. Модель розгортання хмари визначає конкретний тип хмарного середовища на основі права власності, масштабу та доступу, а також природи та призначення хмари. Розташування серверів, які ви використовуєте, і хто ними керує, визначаються моделлю розгортання хмари. Вона визначає, як

виглядатиме ваша хмарна інфраструктура, що ви можете змінювати, і чи будуть вам надані сервіси, чи вам доведеться створювати все самостійно. Взаємовідносини між інфраструктурою та вашими користувачами також визначаються типами розгортання хмари. Нижче описані типи моделей розгортання хмарних обчислень [3]:

– Публічна хмара: Публічна хмара дає можливість будь-кому отримати доступ до систем і сервісів. Публічна хмара може бути менш захищеною, оскільки вона відкрита для всіх. Публічна хмара – це хмара, в якій послуги хмарної інфраструктури надаються через Інтернет широкому загалу або великим галузевим групам. Інфраструктура в цій хмарній моделі належить організації, яка надає хмарні послуги, а не споживачеві. Це тип хмарного хостингу, який дозволяє клієнтам і користувачам легко отримати доступ до систем і сервісів. Ця форма хмарних обчислень є чудовим прикладом хмарного хостингу, в якому постачальники послуг надають послуги різним клієнтам. За такої схеми послуги з резервного копіювання та пошуку даних у сховищі надаються безкоштовно, за підпискою або на індивідуальній основі.

Рисунок 1.2 – Модель розгортання «публічна хмара»

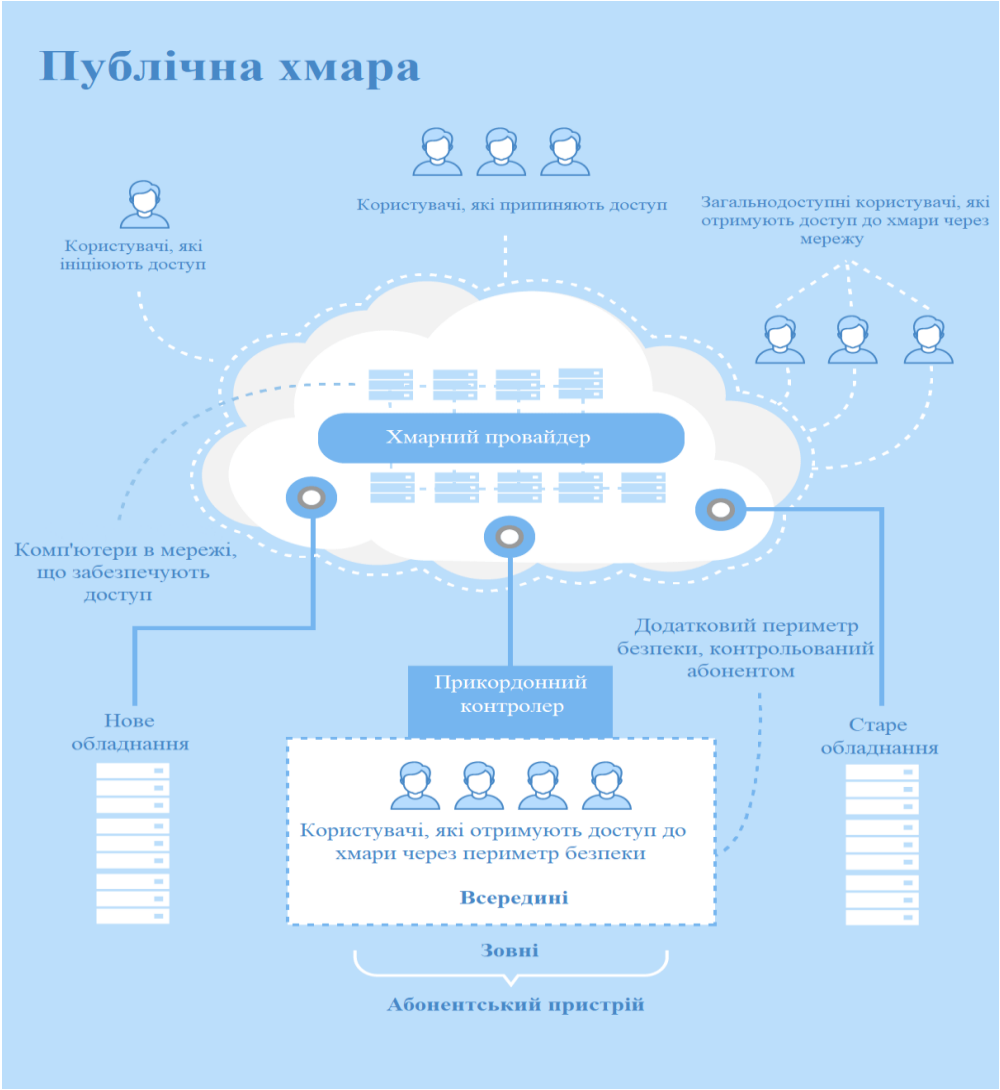

Рисунок.1 3 – Приклад роботи моделі «Публічна хмара»

Переваги моделі публічної хмари:

1) Оскільки це послуга з оплатою за використання, вона не вимагає значних авансових платежів, що робить її ідеальним рішенням для підприємств, які потребують негайного доступу до ресурсів. Вся інфраструктура повністю субсидується постачальниками хмарних послуг, тому немає необхідності встановлювати будь-яке обладнання.

2) Використання публічної хмари не потребує управління інфраструктурою.

3) Роботи з технічного обслуговування виконує постачальник послуг (а не користувачі).

4) Для задоволення потреб вашої компанії доступні ресурси на вимогу, що забезпечує динамічну масштабованість.

Недоліки моделі публічної хмари:

1) Публічна хмара менш безпечна, оскільки ресурси є загальнодоступними, тому немає гарантії високого рівня безпеки.

2) Доступ до хмари відкритий для всіх, тому її не можна налаштувати відповідно до особистих потреб.

– Приватна хмара: Модель розгортання приватної хмари є повною протилежністю моделі розгортання публічної хмари. Це індивідуальне середовище для одного користувача (клієнта). Немає необхідності ділитися своїм обладнанням з кимось іншим. Різниця між приватними та публічними хмарами полягає в тому, як ви працюєте з усім обладнанням. Це також називається "внутрішньою хмарою" і стосується можливості доступу до систем і сервісів у межах певного кордону або організації. Хмарна платформа реалізована в хмарному безпечному середовищі, яке захищене потужними брандмауерами і знаходиться під наглядом IT-відділу організації. Приватна хмара дає більшу гнучкість контролю над хмарними ресурсами.

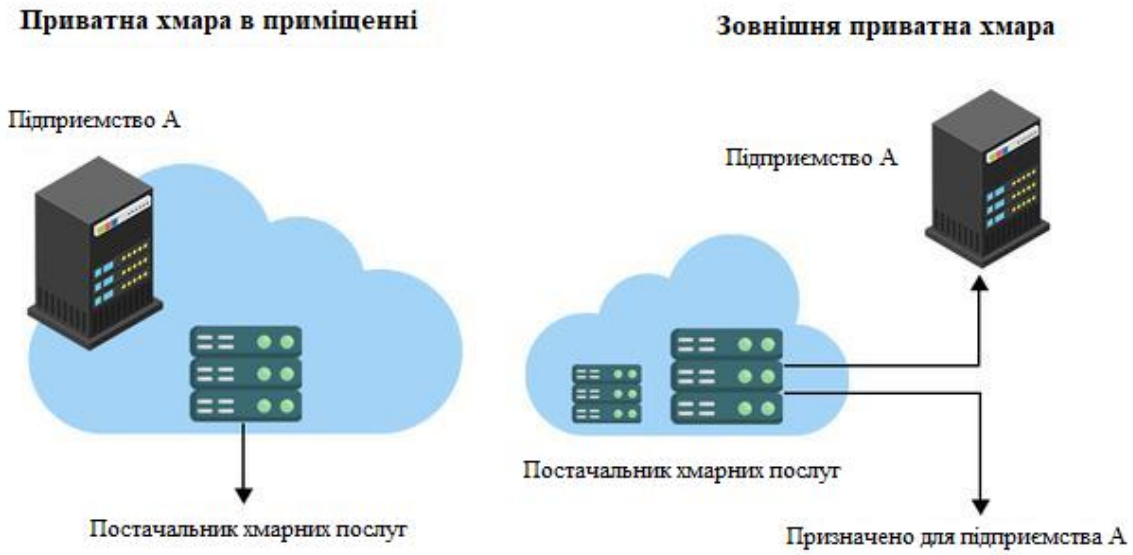

Рисунок 1.4 – Модель розгортання «приватна хмара»

Рисунок 1.5 – Приклад роботи моделі «Приватна хмара»

Переваги моделі приватної хмари:

1) Ви є єдиним власником майна. Ви отримуєте повний контроль над інтеграцією послуг, IT-операціями, політиками та поведінкою користувачів.

2) Підходить для зберігання корпоративної інформації, до якої мають доступ лише уповноважені співробітники. Завдяки сегментації ресурсів в межах однієї інфраструктури можна досягти покращеного доступу та безпеки.

3) Цей підхід призначений для роботи із застарілими системами, які не мають доступу до публічної хмари.

4) На відміну від розгортання публічної хмари, приватна хмара дозволяє компанії адаптувати своє рішення до конкретних потреб.

Недоліки моделі приватної хмари:

1) Приватні хмари масштабуються в межах певного діапазону, оскільки кількість клієнтів менша.

2) Приватні хмари дорожчі, оскільки надають персоналізовані можливості.

– Гібридна хмара: Поєднуючи публічний і приватний світ за допомогою власного програмного забезпечення, гібридні хмарні обчислення дають найкраще з обох моделей. Завдяки гібридному рішенню ви можете розміщувати додаток у безпечному середовищі, водночас користуючись перевагами економії витрат у публічній хмарі. Організації можуть переміщувати дані та додатки між різними хмарами, використовуючи комбінацію двох або більше методів розгортання хмар, залежно від своїх потреб.

Рисунок 1.6 – Модель розгортання «гібридна хмара»

Переваги гібридної хмарної моделі:

1) Досить висока гнучкість та забезпечення контролю. Компанії з більшою гнучкістю можуть розробляти персоналізовані рішення, які відповідають їхнім конкретним потребам.

2) Оскільки публічні хмари забезпечують масштабованість, ви будете платити за додаткову потужність лише тоді, коли вона вам знадобиться.

3) Оскільки дані належним чином розділені, шанси на їх крадіжку зловмисниками значно зменшуються.

Недоліки гібридної хмарної моделі:

1) Гібридними хмарами важко керувати, оскільки вони є поєднанням публічної та приватної хмар.

2) Передача даних у гібридній хмарі відбувається через публічну хмару, тому виникають затримки.

– Суспільна хмара: Дозволяє надавати доступ до систем і сервісів групі організацій. Це розподілена система, яка створюється шляхом інтеграції сервісів різних хмар для задоволення конкретних потреб спільноти, галузі або бізнесу. Інфраструктура спільноти може бути спільною для організацій, які мають спільні проблеми або завдання. Зазвичай вона управляється третьою стороною або поєднанням однієї чи кількох організацій у спільноті.

Рисунок 1.7 – Модель розгортання «Суспільна хмара»

Переваги суспільної хмарної моделі:

1) Вона є економічно ефективною, оскільки хмару використовують декілька організацій або спільнот.

2) Спільна хмара забезпечує кращу безпеку.

3) Дозволяє ділитися ресурсами, інфраструктурою тощо з кількома організаціями.

4) Підходить як для спільної роботи, так і для обміну даними.

Недоліки суспільної хмарної моделі:

1) Суспільна хмара є відносно менш масштабованою, оскільки багато організацій користуються одними й тими ж ресурсами відповідно до своїх спільних інтересів.

2) Оскільки дані та ресурси розподіляються між різними організаціями відповідно до їхніх спільних інтересів, якщо організація бажає внести певні зміни відповідно до своїх потреб, вона не може цього зробити, оскільки це матиме вплив на інші організації.

Таблиця 1.1 – Порівняння моделей розгортання

Фактори	Публічна хмара	Приватна хмара	Гібридна хмара	Суспільна хмара
Початкове налаштування	Просте	Складне, потребує професійної команди для налаштування	Складне, потребує професійної команди для налаштування	Складне, потребує професійної команди для налаштування
Масштабованість і гнучкість	Висока	Висока	Фіксована	Висока
Порівняння витрат	Економічно ефективна	Дорога	Розподіл витрат між учасниками	Між публічною та приватною хмарою
Надійність	Низька	Низька	Висока	Висока
Безпека даних	Низька	Висока	Висока	Висока
Конфіденційність даних	Низька	Висока	Висока	Висока

Вибір моделі розгортання визначає основні характеристики , що стосуються обслуговування, власності, розташування та доступу до інфраструктури [4].

Таблиця 1.2 – Обслуговування та управління різними видами хмарних ресурсів

Вид хмари	Ким обслуговується	Хто є власником	Де знаходиться інфраструктура	У кого є доступ
Публічна	Зовнішнім провайдером	Зовнішній провайдер	У зовнішнього провайдера	У будь-якого користувача
Приватна/ Суспільна	Користувачем або зовнішнім провайдером	Користувач або зовнішній провайдер	У зовнішнього провайдера або у користувача	У авторизованого користувача
Гібридна	Користувачем і зовнішнім провайдером	Користувач і зовнішній провайдер	У зовнішнього провайдера і у користувача	У авторизованих і у будь-яких зовнішніх користувачів

1.3 Моделі обслуговування хмарних технологій

Однією з найважливіших частин вашої хмарної стратегії є вибір правильної моделі хмарного сервісу для вашої організації. Тип сервісу, який ви оберете, залежить від наявної у вас інфраструктури, ресурсів IT-персоналу, міркувань щодо вартості та потреб у хмарній безпеці. Існує три основні моделі хмарних сервісів: програмне забезпечення як послуга (SaaS), інфраструктура як послуга (IaaS) та платформа як послуга (PaaS) [5].

З інфраструктурою як послугою (IaaS) постачальник хмарних послуг володіє та керує апаратним забезпеченням (сервери, мережа та сховище), на якому працює стек програмного забезпечення. Це може бути чудовою стратегією зниження витрат, якщо ви хочете уникнути покупки та підтримки

інфраструктури. IaaS – це система самообслуговування, яка дозволяє вашій IT-команді за потреби отримувати доступ до ресурсів через API або інформаційну панель.

Щодо переваг IaaS можна віднести економічну ефективність та масштабованість. Модель спрощує, прискорює та робить економічно ефективною роботу. Хмарна інфраструктура гарантує, що компанії мають доступ до всіх необхідних ресурсів. До недоліків відносять технічні проблеми та питання безпеки. У середовищі IaaS організації передають контроль над безпекою сторонньому постачальнику, тому витік даних, який не вплинув безпосередньо на дані компанії, може поставити під загрозу її діяльність. Приклади використання IaaS: хостинг веб-сайтів, розгортання програмного забезпечення, тестування та розробка.

Наступний рівень послуг – це платформа як послуга (PaaS). PaaS схожа на IaaS, за винятком того, що ваш постачальник хмарних послуг також надає операційну систему та бази даних. Це означає менше роботи для вашої IT-команди. Ваша організація, як і раніше, відповідає за програми, функції та дані. PaaS надає вашим розробникам просту, масштабовану платформу для створення додатків. Як і у випадку з IaaS, ви можете придбати більше ресурсів за потреби. А оскільки декілька користувачів можуть отримати доступ до програми одночасно, PaaS може впорядкувати робочі процеси та покращити координацію.

Простота, зручність та швидка розробка – основні переваги PaaS. Провайдери надають більшість інфраструктурних та інших IT-послуг, до яких користувачі можуть отримати доступ, якщо в них є підключення до Інтернету та веб-браузер. До мінусів можна віднести відсутність масштабованості та прив’язку до постачальника. Оскільки постачальники мають унікальні вимоги до конфігурації, організаціям може бути складно перейти від одного постачальника до іншого. Приклади використання PaaS: розробка API, бізнес-аналітика.

Програмне забезпечення як послуга (SaaS) пропонує найбільшу підтримку і є найпростішою з усіх моделей доставки для кінцевого користувача. SaaS може працювати в багатокористувацькій архітектурі, в якій один екземпляр програмного забезпечення обслуговує кількох користувачів. Як правило, продукти SaaS не потребують завантаження чи встановлення, що позбавляє кінцевих користувачів необхідності керувати оновленнями програмного забезпечення. Все, за що вони відповідають, - це їхні дані.

Основна перевага продуктів SaaS полягає в тому, що організації можуть використовувати їх одразу після підписки, оскільки це найпростіша в налаштуванні хмарна модель. Щоб додати нових користувачів організаціям достатньо оновити свої існуючі підписки. Відсутність контролю – основний недолік. Організації не мають контролю на хмарної інфраструктурою. Отже, якщо у провайдера трапляються перебої в роботі, то і них теж. Приклади використання SaaS: корпоративні додатки, фінансовий менеджмент [17].

Таблиця 1.3 – Моделі обслуговування за засобами доступу і управління

Моделі обслуговування	Засоби доступу і управління	Вміст
ПЗ як сервіс (SaaS)	Веб-браузер	Хмарні програми: соціальні мережі, офісні застосунки, системи управління вмістом, інтелектуальна обробка даних.
Платформа як сервіс (PaaS)	Хмарне середовище розробки	Хмарна платформа: мови програмування, бібліотеки, утиліти конфігурації композицій сервісів, структуровані дані

Моделі обслуговування	Засоби доступу і управління	Вміст
Інфраструктура як сервіс(IaaS)	Система управління віртуальної інфраструктурою	Хмарна інфраструктура: обчислювальні сервера, сховища даних, організація мережевих з'єднань.

Продовження таблиці 1.3 – Моделі обслуговування за засобами доступу і управління

Окрім IaaS, PaaS та SaaS, є ще кілька типів моделей хмарних сервісів, про які варто знати[5]:

• Функція як послуга (FaaS) – це ще один, більш глибокий рівень обслуговування. За допомогою FaaS ваші користувачі керують лише функціями та даними. Постачальник хмарних послуг керує додатками, які ви використовуєте. Цей варіант особливо популярний серед розробників, оскільки ви не платите за послуги, коли ваш код не працює. Поширені функції включають обробку даних, перевірку або сортування даних, а також бекенд для мобільних додатків.

• Фізична інфраструктура як послуга (BMaaS) – деякі підприємства відчувають труднощі з перенесенням робочих навантажень у віртуальне хмарне середовище, яке використовується спільно з іншими клієнтами. Альтернативою IaaS і PaaS є "фізична інфраструктура як послуга", або BMaaS. Це спосіб для підприємств доповнити віртуалізовані хмарні сервіси виділеним серверним середовищем з такою ж гнучкістю, масштабованістю та ефективністю, як у хмарі. Зокрема, BMaaS є чудовим вибором для підприємств, яким потрібно виконувати короткострокову обробку великих обсягів даних, наприклад, кодування медіафайлів або рендерингові ферми, без затримок або додаткових витрат.

• База даних як послуга (DBaaS) – це тип PaaS, який надає доступ до бази даних. DBaaS може бути чудовим способом реалізації гібридної хмари,

оскільки додатки можна переміщувати між локальною та хмарною інфраструктурою без жодного впливу на кінцевих користувачів. Також за допомогою DBaaS набагато легше інтегрувати нові технології, оскільки розробникам додатків не потрібні додаткові ресурси для їх використання.

Незважаючи на схожість, вибір між програмним забезпеченням як послугою, платформою як послугою та інфраструктурою як послугою означає, що компанії повинні знайти правильний баланс між відмовою від контролю та економією часу і зусиль своїх співробітників, щоб вони могли бути більш продуктивними. Розмір вашої організації може допомогти визначити, яку хмарну модель використовувати.

Малі, середні та великі компанії з малими ресурсами – SaaS. Компанії можуть заощадити гроші, використовуючи програмне забезпечення як послугу, тому що їм не потрібно самостійно проектувати і розробляти програмне забезпечення. Компаніям має сенс використовувати SaaS-продукти, які відповідають їхнім бізнес-вимогам, оскільки вони можуть швидко стати більш продуктивними.

Середні/великі організації з середніми ресурсами – PaaS. Середнім і великим компаніям з IT-відділами варто розглядати платформу як послугу як варіант, особливо якщо їм потрібні налаштовані додатки, які легше інтегруються з їхніми робочими процесами і технологіями.

Середні/великі підприємства з великими ресурсами – IaaS. Середнім і великим підприємствам, які мають необхідні IT-ресурси, варто використовувати інфраструктуру як послугу. Майже повний контроль, який забезпечує IaaS, означає, що вони можуть створювати технологічні стеки, які відповідають конкретним бізнес-вимогам організації. IaaS також дозволяє легко адаптувати технологію, якщо бізнес-вимоги змінюються.

1.4 Основні властивості хмарних технологій

Хмара включає в себе постійно зростаючий список інструментів і методів, але ключові характеристики хмарних обчислень залишаються незмінними. У міру того, як хмарні обчислення розвиваються в

комерційному та технологічному плані, компанії користуються їхніми численними перевагами. Ознайомлення з основними характеристиками хмарних обчислень може допомогти вам максимізувати ці переваги для розвитку та зміцнення вашого бізнесу.

Національний інститут стандартів США (NIST) перераховує п'ять основних характеристик хмарних обчислень: самообслуговування на вимогу, широкий доступ до мережі, об'єднання ресурсів, швидка масштабованість і дозоване обслуговування [6].

Рисунок 1.8 – Основні властивості хмарних обчислень

Хмарні обчислення дозволяють надавати самообслуговування на вимогу. Послуги включають зберігання, мережу, аналіз тощо. Користувачі можуть вибирати і використовувати одну або декілька послуг залежно від своїх потреб. За допомогою хмарних обчислень ви можете надавати обчислювальні послуги, такі як серверний час і мережеве сховище, автоматично. Вам не потрібно взаємодіяти з постачальником послуг. Клієнти хмарних обчислень можуть отримати доступ до своїх хмарних облікових записів через веб-портал самообслуговування, щоб переглядати свої хмарні сервіси, відстежувати їх використання, а також надавати та відключати послуги.

Ще однією важливою характеристикою хмарних обчислень є широкий доступ до мережі. Ви можете отримати доступ до хмарних сервісів через мережу та на портативних пристроях, таких як мобільні телефони, планшети, ноутбуки та стаціонарні комп'ютери. Публічна хмара використовує Інтернет, а приватна – локальну мережу. Затримка і пропускна здатність відіграють важливу роль у хмарних обчисленнях і широкому мережевому доступі, оскільки вони впливають на якість послуг. Хмарний провайдер повинен пропонувати своїм клієнтам численні варіанти доступу до мережі. Широкий мережевий доступ містить конфігурацію для безпечного віддаленого доступу. В результаті хмарні обчислення усувають перешкоди і кордони, оскільки доступ до них можливий з будь-якого місця.

Об'єднання ресурсів є одним з основних компонентів хмарних обчислень. Постачальник хмарних послуг може надавати кожному клієнту різні послуги відповідно до його потреб, використовуючи об'єднання ресурсів для розподілу ресурсів між багатьма клієнтами. Така модель дозволяє клієнтам спільно використовувати одні й ті ж програми або інфраструктуру, зберігаючи при цьому конфіденційність і безпеку.

Здатність системи справлятися зі зростаючим обсягом роботи шляхом додавання ресурсів називається масштабованістю (адаптивність). Хмарні сервіси повинні швидко розвиватися, щоб не відставати від постійного розширення бізнесу. Крім того, що хмарні сервіси мають потенціал для збільшення кількості серверів або інфраструктури у відповідь на попит, вони також пропонують значну кількість функцій, які задовольняють потреби своїх клієнтів. Масштабованість ще більше підвищує економічну ефективність хмарних обчислень та їх придатність для використання в бізнесі.

У хмарних системах можливість вимірювання оптимізує використання ресурсів на рівні абстракції, що відповідає типу послуги. Наприклад, ви можете використовувати дозовану послугу для зберігання або обробки. Оплата здійснюється на основі фактичного споживання клієнтом за моделлю

"плати за те, що використовуєш". Споживання ресурсів відстежується для кожної програми та користувача; це дає змогу як користувачеві, так і постачальнику ресурсів отримати звіт про те, що було використано. Моніторинг, регулювання та звітування про використання ресурсів забезпечує прозорість для постачальника та користувача послуг.

Існує декілька характеристик, які не входять до переліку основних характеристик NIST, але можуть принести користь клієнтам під час використання хмарних обчислень [18]:

– Безпека: Користувачі хмарних обчислень особливо стурбовані безпекою даних. Постачальники хмарних послуг зберігають зашифровані дані користувачів і пропонують додаткові функції безпеки, такі як автентифікація користувачів і захист від зломів та інших загроз. Сервери даних фізично захищені. Ці сервери зазвичай зберігаються в безпечному, ізольованому місці, щоб запобігти несанкціонованому доступу або порушенню роботи.

– Автоматизація: Автоматизація в хмарних обчисленнях означає здатність хмарного сервісу встановлюватися, налаштовуватися та обслуговуватися автоматично. Однак автоматизувати хмарну екосистему не так просто. Це вимагає розгортання значних сховищ, серверів та віртуальних машин. Після успішного розгортання ці ресурси потрібно підтримувати.

– Відмовостійкість: Відмовостійкість у хмарних обчисленнях – це здатність сервісу швидко відновлюватися після будь-яких збоїв. Швидкість, з якою сервери, бази даних і мережеві системи хмари перезапускаються і відновлюються після пошкоджень, є мірою її відмовостійкості.

2 ОГЛЯД, АНАЛІЗ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ ПОСЛУГ

2.1 Безпека хмарних послуг

Хмарні обчислення дозволяють знизити витрати за рахунок спільного використання ресурсів і віртуалізації сховищ, об'єднаних з механізмом надання послуг, який спирається на бізнес-архітектуру, що працює за принципом "оплата за фактом". Незважаючи на вплив та ефективні послуги, які пропонують ці додатки, все ще існують проблеми безпеки та конфіденційності, пов'язані з тим, як ці хмарні провайдери обробляють дані користувачів. Безпечне впровадження хмарних технологій вимагає адаптивного механізму безпеки, який допоможе користувачам мати значний рівень довіри до хмари. Без здатності таких методів гарантувати значний рівень безпеки та конфіденційності, продовжуватиме існувати великий ризик втрати конфіденційності та витоку конфіденційних даних, що є значними перешкодами та вирішальними факторами у повному впровадженні хмарних сервісів.

Хмарна безпека – це галузь комп'ютерної та мережевої безпеки, яка контролюється технологіями, що підвищують конфіденційність, і регулюється набором правил політики для захисту розгортання даних, програмних додатків і супутніх послуг, переданих на аутсорсинг у хмару. Найпоширеніші терміни у сфері безпеки [7, 19]:

- Конфіденційність: Забезпечення доступу до інформації лише авторизованим користувачам.
- Цілісність: Підтримувати повноту і точність кожної частини інформації.
- Доступність: Інформація доступна лише авторизованим користувачам.

- Збереження приватності: Здатність маскувати ідентичність та особисту інформацію, що дозволяє ідентифікувати особу.
- Підзвітність: Зобов'язання або готовність нести відповідальність за дії відповідно до визначеного набору правил.
- Можливість аудиту: Підтримання системи для інших з метою підвищення її ефективності.
- Автентифікація: Встановлення правильної ідентичності користувача в системі.
- Авторизація: Доступ до ресурсів обмежений лише для уповноваженого персоналу.

2.2 Загрози хмарних послуг

Великий обсяг даних, що циркулюють між організаціями та постачальниками хмарних послуг, створює можливості для випадкового та зловмисного витоку конфіденційних даних до ненадійних третіх сторін. Людські помилки, внутрішні загрози, шкідливе програмне забезпечення, слабкі облікові дані та злочинна діяльність є причинами більшості витоків даних у хмарних сервісах. Зловмисники намагаються використати вразливості хмарних сервісів для витоку даних з мережі організації-жертви з метою отримання прибутку або в інших незаконних цілях [8, 20].

Хмарна атака – це кібератака, націлена на платформи хмарних послуг, наприклад: обчислювальні служби, служби зберігання даних або програмне забезпечення. Хмарні атаки можуть мати серйозні наслідки, такі як витік даних, втрата даних, несанкціонований доступ до конфіденційної інформації та збої в роботі служб. Оскільки все більше організацій і окремих осіб покладаються на хмарні обчислення для зберігання та обробки даних, відповідно збільшується і кількість потенційних цілей для зловмисників.

Атака на відмову в обслуговуванні (DDoS) – це тип кібератаки, метою якої є зробити комп'ютер або мережевий ресурс недоступним для користувачів. DoS-атаки зазвичай полягають у переповненні хмарного сервісу великим обсягом трафіку, що може перевантажити систему і зробити

її нездатною обробляти легітимні запити. Захист від DoS-атаки може бути особливо складними, оскільки масштаб і складність хмарних середовищ можуть ускладнювати виявлення та пом'якшення наслідків атаки. Як наслідок, DoS-атаки становлять значну загрозу для хмарних ресурсів організації.

Викрадення облікового запису в хмарі – це несанкціонований доступ або контроль зловмисником облікового запису. Це може дозволити зловмиснику використовувати пов'язані з ним ресурси у власних цілях, викрадати або маніпулювати даними, що зберігаються в хмарі. Багато людей мають вкрай слабку безпеку паролів, включаючи повторне використання паролів і використання слабких паролів. Ця проблема посилює вплив фішингових атак і витоків даних, оскільки дозволяє використовувати один вкрадений пароль для кількох різних акаунтів. Викрадення облікових записів є однією з найсерйозніших проблем безпеки хмарних технологій, оскільки організації все більше покладаються на хмарну інфраструктуру та додатки для виконання основних бізнес-функцій. Крім того, в хмарі організації часто не мають можливості виявляти ці загрози та реагувати на них так само ефективно, як у випадку з локальною інфраструктурою.

Внутрішні загрози в хмарному середовищі – це ризик несанкціонованого доступу або зловживання ресурсами хмарних обчислень окремими особами в організації, наприклад, працівниками або підрядниками. Ці особи можуть мати законний доступ до хмарних ресурсів, але можуть зловживати цим доступом у власних цілях або випадково наражати ресурси на ризик своїми діями. Внутрішні загрози може бути особливо складно виявити та запобігти, оскільки вони часто стосуються осіб, які мають дозвіл на доступ до хмарних активів і можуть діяти без зловмисних намірів. Їх також важко зменшити, оскільки вони часто пов'язані з високим рівнем довіри та доступу в організації. При розгортанні хмарних технологій компанії втрачають контроль над своєю базовою інфраструктурою, що

робить багато традиційних рішень для забезпечення безпеки менш ефективними.

Неправильна конфігурація безпеки – нездатність належним чином налаштувати ресурси та інфраструктуру хмарних обчислень для захисту від кіберзагроз. Це може включати неналежне налаштування контролю доступу, неналежне налаштування та захист систем і додатків, а також нерегулярне оновлення та виправлення систем і додатків. Хмарна інфраструктура спроектована так, щоб нею було легко користуватися і вона дозволяла легко обмінюватися даними, що ускладнює організаціям забезпечення доступу до даних лише авторизованим особам. Крім того, організації, що використовують хмарну інфраструктуру, не мають повної видимості та контролю над своєю інфраструктурою, а це означає, що їм доводиться покладатися на засоби контролю безпеки, які надає постачальник хмарних послуг. Неправильна конфігурація або недогляд за безпекою можуть призвести до того, що хмарні ресурси організації стануть вразливими до атак зловмисників.

Зараження файлами cookie в хмарних додатках – це несанкціонована модифікація або впровадження шкідливого контенту в файл cookie, який є невеликим фрагментом даних, що зберігається на комп'ютері користувача. Файли cookie використовуються для зберігання інформації про вподобання користувача та історію переглядів, а також часто застосовуються для персоналізації досвіду користувача або для відстеження його активності. У SaaS та інших хмарних додатках файли cookie часто містять облікові дані, тому зловмисники можуть отруїти файли cookie, щоб отримати доступ до додатків.

Частиною хмарних сервісів для взаємодії користувачів на всіх рівнях є публікація API для легкого розгортання або розробки програмних додатків. Ці інтерфейси надають додатковий рівень хмарній структурі для підвищення складності. Незахищені API мають вразливості, які можуть бути використані

зловмисниками для отримання несанкціонованого доступу до систем або даних, або для порушення роботи API.

– Тіньові API: API, які не мають належного документування або авторизації, і можуть бути невідомі організації, яка володіє API. Ці API створені розробниками або іншими користувачами всередині організації, і можуть надавати конфіденційні дані або функціональність неавторизованим особам.

– Параметри API: Вхідні та вихідні дані API, які можуть бути вразливими до атак типу "ін'єкція", якщо вони не будуть належним чином перевірені та очищені.

Однією з важливих проблем хмарних обчислень є витік даних. Хмарні середовища дозволяють легко ділитися даними, що зберігаються в них. Ці середовища доступні безпосередньо з загальнодоступного Інтернету і включають в себе можливість легко ділитися даними з іншими сторонами за допомогою прямих запрошень електронною поштою або публічного посилання на дані. Легкість обміну даними в хмарі – хоча і є основною перевагою і ключем до співпраці в хмарі – викликає серйозні ризики щодо втрати або витоку даних. Причинами втрати даних є слабкі схеми автентифікації та шифрування, дефектні центри обробки даних та відсутність контролю.

2.3 Вразливості хмарних послуг

У хмарних обчисленнях вразливість – це недогляд, прогалина або слабке місце в системі безпеки. Ці вразливості використовують кіберзлочинці, щоб отримати несанкціонований доступ до корпоративних облікових записів. Потрапивши всередину, вони можуть викрасти, змінити або видалити конфіденційні дані компанії, такі як фінансова звітність або записи про клієнтів. Існує багато видів вразливостей хмарних обчислень. Знання того, як їх виявити та усунути, є життєво важливим для запобігання витоку даних. В результаті це може допомогти компанії захистити свої конфіденційні дані, підвищити довіру клієнтів, запобігти катастрофі у сфері

зв'язків з громадськістю та уникнути штрафних санкцій за недотримання вимог.

Важливо розуміти різницю між вразливістю хмарних обчислень і загрозою, оскільки іноді їх плутають. Загроза – це безпосередня небезпека, дія або поведінка, що відбувається в режимі реального часу. Якщо її не зупинити, вона може призвести до серйозних наслідків. На відміну від цього, вразливість – це слабкість або стан, який наражає на можливість атаки, а не сам акт атаки. Вона відноситься до обставин, які роблять можливим здійснення шкідливої дії. Основні вразливості хмарних послуг та способи боротьби з ними [9]:

1) Недостатній контроль доступу: Це один з найпоширеніших ризиків для безпеки даних у хмарі. Неправильні або слабкі обмеження доступу означають, що неавторизований персонал може отримати доступ до даних, на які він не уповноважений. Встановлення належного контролю доступу означає, що тільки уповноважені особи можуть отримати доступ до певних даних, документів і додатків. Процес перевірки осіб, яким слід дозволити доступ, а яким ні, називається авторизацією. Відсутність управління доступом на основі ролей, відключення доступу неактивним користувачам або колишнім працівникам, а також наявність декількох облікових записів для входу в систему можуть призвести до ризику безпеки з точки зору належного управління доступом.

Для боротьби з недостатнім управлінням доступом у хмарних сервісах підприємствам необхідно розробити систему управління даними для облікових записів користувачів. Для всіх користувачів облікові записи повинні бути пов'язані безпосередньо з центральними службами каталогів, які відповідають за надання, моніторинг та відкликання привілеїв доступу з централізованого сховища. Організації також повинні забезпечити наявність механізмів реєстрації та моніторингу подій у хмарних середовищах для виявлення незвичної активності або несанкціонованих змін. Ключі доступу

повинні суворо контролюватися і управлятися, щоб уникнути неналежної обробки даних або їх витоку.

2) Невідповідність: Кожна галузь і компанії, які в ній працюють, мають певні галузеві стандарти та правила, яких вони повинні суворо дотримуватися. Це називається відповідністю. Вони в основному стосуються захисту даних, а також оцінюють кроки, зроблені кожною компанією для того, щоб дотримуватися перерахованих правил і не відставати від них. Це гарантує, що організація є надійною з точки зору забезпечення безпеки, що всі засоби контролю та обмеження доступу є функціональними та належними, а також забезпечують безпеку даних. Слід зазначити, що підтримка безпеки хмарних сервісів не покладається лише на провайдерів. Це відома як модель спільної відповідальності, коли безпеку хмари підтримує провайдер, але безпеку даних можуть і повинні підтримувати клієнти.

Ознайомтеся з відповідними галузевими стандартами та правилами, які застосовуються до вашої організації та хмарних сервісів, якими ви користуєтеся. Слідкуйте за будь-якими змінами чи оновленнями цих нормативних актів, щоб забезпечити постійну відповідність. Впровадьте надійні практики управління даними, включаючи класифікацію даних, щоб забезпечити належну обробку та захист даних відповідно до чинних нормативних актів. Класифікуйте дані на основі їхньої чутливості та відповідно до цього встановлюйте контроль доступу, строки зберігання та політику видалення.

3) Захист даних та конфіденційність: Кожна організація підпадає під дію законів про захист даних та конфіденційність. Ці закони можуть бути встановлені галуззю, країною або відповідним міжнародним органом зі стандартизації. У контексті хмарних обчислень відповідність – це акт дотримання нормативних стандартів використання хмарних технологій, які застосовуються до відповідних галузевих керівних принципів, а також місцевих і міжнародних законів. Орієнтуватися в питаннях хмарної відповідності може бути непросто. Особливо для малих та середніх

підприємств, які не знайомі з хмарним законодавством. Використання декількох постачальників хмарних послуг одночасно може ще більше ускладнити дотримання вимог. Звичайно, хоча безпека хмарних сервісів є спільною відповідальністю – між користувачем і постачальником послуг – саме користувач несе відповідальність за вибір постачальника послуг, який відповідає його потребам.

Захист даних можна гарантувати за допомогою контроля доступу та управління ідентифікацією. Впроваджуйте надійний механізм контролю доступу та управління ідентифікацією, щоб забезпечити доступ до даних у хмарі та маніпулювання ними лише уповноваженим особам. Шифрування даних гарантує що дані не можна буде прочитати та використати несанкціонованим особам.

4) Неможливість поділу між кількома клієнтами: Нездатність підтримувати надійне розділення між клієнтами в хмарному середовищі, яке підтримує багатокористувацьку оренду, може виявитися однією з найсерйозніших вразливостей хмарних технологій. Зловмисники можуть легко скористатися цим недоліком, щоб отримати доступ до активів або даних організації через ресурс іншого користувача. Багатокористувацька оренда, при неналежному поводженні, може збільшити поверхню атаки і призвести до витоку даних, якщо не спрацює контроль за їхнім розділенням. Ця вразливість, якщо її негайно не усунути, може серйозно загрожувати безпеці даних і конфіденційності організації.

Надійна багатокористувацька архітектура – найкращий метод для протидії. Переконайтеся, що хмарний провайдер має надійну багатокористувацьку архітектуру. Ця архітектура повинна забезпечувати суворі механізми ізоляції, такі як виділені віртуальні машини, контейнери або віртуальні мережі, щоб відокремити ресурси та дані різних користувачів. Впровадьте сегментацію мережі, щоб ізолювати трафік користувачів та запобігти несанкціонованому доступу між орендарями. Використовуйте віртуальні локальні мережі (VLAN), віртуальні приватні мережі (VPN) або

програмно-визначені мережі (SDN) для створення логічних меж мережі та забезпечення суворого контролю доступу між середовищами орендарів.

2.4 Основні методи захисту хмарних послуг

Від самого початку ери хмарних обчислень безпека була найбільшою проблемою для підприємств, які розглядали можливість використання хмарних сервісів. Для багатьох організацій ідея зберігання даних або запуску додатків на інфраструктурі, якою вони не керують безпосередньо, здається небезпечною за своєю суттю, а також ризик того, що дані будуть переміщуватися через загальнодоступну мережу Інтернет для доступу до цих сервісів і з них. Підприємства, які не хочуть бути частиною статистики про кількість атак на хмарні послуги, повинні розуміти та впроваджувати найкращі практики та інструменти кібербезпеки для захисту своєї хмарної інфраструктури. Хоча ці заходи не запобігають кожній атаці, вони допомагають компаніям зміцнити свій захист, захистити свої дані та впровадити надійні практики безпеки хмарних технологій [10].

1) Використання надійних паролів: Уникайте використання слабких паролів і повторного використання облікових даних для входу в декількох облікових записах. Хакери використовують тактику злому паролів і купують списки часто використовуваних паролів, щоб отримати несанкціонований доступ до онлайн-акаунтів. Це означає, що навіть паролі, які містять щонайменше вісім символів і поєднують цифри, літери та спеціальні символи, недостатньо надійні проти програмного забезпечення, яке може допомогти зловмисникам зламувати коди.

Тому обмежте можливість зловмисників проникнути до важливих облікових записів, використовуючи надійний та унікальний пароль для кожного облікового запису. Менеджери паролів також допомагають користувачам безпечно зберігати свої облікові дані. Вони також позбавляють користувачів необхідності запам'ятовувати кожен пароль для кожного облікового запису.

2) Впровадження багатофакторної автентифікації (MFA): Для забезпечення безпеки в хмарі іноді недостатньо використовувати тільки пароль. Користувачам слід додавати багатофакторну автентифікацію для підвищення рівню захисту. Після введення імені користувача та пароля для входу в обліковий запис користувачам буде запропоновано підтвердити свою особу. Це може бути код у додатку для автентифікації на мобільному телефоні, введення одноразового пароля або сканування відбитків пальців. MFA ускладнює зловмисникам доступ до додатків і систем і не дозволяє їм використовувати вкрадені паролі для доступу до облікових записів користувачів.

3) Використання вдосконаленого брандмауера: Організації можуть захистити себе від різних проблем безпеки за допомогою вдосконалених брандмауерів, таких як брандмауери нового покоління (NGFW) і брандмауери для веб-додатків (WAF). NGFW виявляє і блокує сучасні загрози, такі як шкідливе програмне забезпечення і вектори атак на рівні додатків. Він також забезпечує оновлення відповідно до мінливого ландшафту загроз безпеці, щоб підприємства завжди були захищені від новітніх кібератак. WAF захищає хмарні додатки від експлойтів і можуть бути модифіковані за допомогою спеціальних правил, наприклад, дозволяючи трафік лише з певних IP-адрес.

4) Шифрування даних: Це процес перетворення даних з початкового формату звичайного тексту в нечитабельний формат, наприклад, зашифрований текст, перед передачею та зберіганням у хмарі. Як і будь-яка інша форма шифрування даних, хмарне шифрування робить інформацію нерозбірливою без ключів шифрування. Це стосується навіть тих випадків, коли дані втрачено, викрадено або надано доступ до них неавторизованому користувачеві. Шифрування вважається одним з найефективніших компонентів стратегії кібербезпеки організації.

5) Використання віртуальних приватних мереж (VPN): VPN допомагають користувачам отримувати безпечний і анонімний доступ до

Інтернету, що усуває ризик того, що їхні дії в мережі та дані можуть бути викрадені хакерами. VPN використовують шифрування для приховування такої інформації, як місцезнаходження користувача та пристрій, з якого він користується Інтернетом.

6) Керування контролем доступу: Організаціям необхідно впроваджувати контроль доступу, який управляє ризиками і гарантує, що користувачі мають доступ лише до тих мереж, ресурсів і систем, які необхідні їм для ефективного виконання своєї роботи. Розуміння того, хто і до яких даних має доступ, є важливим для подолання ризиків безпеки в хмарах.

7) Постійний моніторинг трафіку: Моніторинг трафіку – це безперервний аналіз мережі з метою виявлення та виправлення будь-яких проблем з продуктивністю мережевої інфраструктури. Інструменти моніторингу дозволяють організаціям перевіряти трафік з Інтернету та спроби доступу до їхніх мереж і ресурсів.

8) Автоматизація засобів захисту: Зловмисники все частіше використовують автоматизацію для виявлення та використання вразливостей. Організації повинні дотримуватися того ж принципу, щоб випереджати кіберзлочинців, автоматизуючи свої засоби захисту. Це включає в себе автоматизацію створення звітів та усунення вразливостей.

9) Підготовка працівників: Співробітники організації – це її перша лінія захисту від проблем безпеки хмар. Компанії повинні переконатися, що їхні працівники розуміють ризики доступу до хмарних сервісів, і навчити їх найкращим практикам безпеки в публічних хмарах, щоб мінімізувати рівень ризиків. Кожен співробітник компанії повинен усвідомлювати постійну загрозу та необхідність безпечного доступу до хмарних сервісів.

10) План реагування: Постраждати від витоку даних або будь-якої іншої події, пов'язаної з безпекою, майже неминуче для більшості організацій. Тому дуже важливо бути готовим до найгіршого і мати план, як реагувати на загрозу та пом'якшувати її наслідки.

3 МОДЕЛІ ЗАГРОЗ, ПОРУШНИКА ТА БЕЗПЕКИ ХМАРНИХ ПОСЛУГ

3.1 Моделювання загроз

Моделювання загроз – це процес визначення, оцінки та зменшення ризиків безпеки в додатку або системі. Використовуючи систему моделювання загроз, ви можете розподілити ресурси для протидії ймовірним загрозам, захисту життєво важливих активів і підтримки безперервності бізнесу. Існують методології та стратегії, які допоможуть зрозуміти, як ваша організація вписується в зростаючий ландшафт загроз і, що ви можете зробити для його захисту.

Моделювання загроз працює шляхом визначення типів загроз, які завдають шкоди програмі або комп'ютерній системі. Під час моделювання загроз організації проводять ретельний аналіз архітектури програмного забезпечення, бізнес-контексту та інших даних (наприклад, функціональні специфікації, користувацькі документації). Цей процес дозволяє глибше зрозуміти та виявити важливі аспекти системи. Зазвичай організації проводять моделювання загроз на етапі проектування нового додатку, щоб допомогти розробникам знайти вразливості та усвідомити наслідки для безпеки їхніх рішень щодо дизайну, коду та конфігурації [11].

Таблиця 3.1 – Етапи моделювання загроз

Етап моделювання	Завдання
Діаграма	Визначення структури проекту
Ідентифікувати загрози	Визначення можливих загроз та їх мети
Пом'якшення	Визначення можливих методів для протидії та пом’якшення
Перевірка	Перевірка виконання попередніх етапів

При правильному виконанні моделювання загроз може забезпечити чітку лінію захисту в програмному проекті, допомагаючи обґрунтувати зусилля з безпеки. Процес моделювання загроз допомагає організації

документувати відомі загрози безпеці та приймати раціональні рішення про те, як їх усунути. Загалом, добре задокументована модель загроз забезпечує гарантії, які корисні для захисту стану безпеки програми або комп'ютерної системи. Найкращі методи моделювання загроз у хмарному середовищі:

– Автоматизація: Розгляд можливості використання автоматизованих інструментів для оптимізації процесу моделювання і зниження ризику помилок або пропущених загроз

– Безперервне моделювання: Використання моделювання загроз в процесі розробки і оновлення в міру розвитку додатку

– Моделювання загроз для мікросервісів: Моделювання загроз для кожного компоненту окремо, щоб забезпечити повне покриття.

– Інтеграція з тестуванням безпеки: Інтеграція моделювання загроз з тестуванням безпеки підтверджує ефективність стратегій пом’якшення наслідків та виявлення нових загроз

– Співпраця: Залучення розробників та експертів з безпеки для забезпечення комплексного та цілісного підходу до моделювання загроз

3.2 Фреймворки та методики моделювання загроз

Моделювання загроз – це метод, спрямований на виявлення потенційних загроз і векторів атак, які існують для системи. На основі цієї інформації можна виконати аналіз ризиків і розробити контрзаходи та стратегії для управління та зменшення цих ризиків. Однак виявлення загроз у вакуумі може бути складним і схильним до помилок. Використання систем (фреймворків) моделювання загроз надає структуру процесу моделювання загроз і може включати інші переваги, такі як запропоновані стратегії виявлення та контрзаходи [12].

Існує кілька доступних методологій та фреймворків, які можна використовувати для моделювання загроз. Методології моделювання загроз можна класифікувати відповідно до фокусу підходів. Ці підходи включають ті, що зосереджені на активах системи, що моделюється (asset-centric), ті, що зосереджені на зловмисниках (attack-centric), а також підходи, що

зосереджені на програмному забезпеченні або системі (software-centric або system-centric). Фреймворки та методи моделювання загроз, які зазвичай використовуються сьогодні [13]:

1) STRIDE: розроблений у 1999 році, щоб керувати виявленням загроз у системі. Використовується в поєднанні з моделлю цільової системи, яка може бути побудована паралельно. Це включає повну розбивку процесів, сховищ даних, потоків даних і меж довіри. STRIDE – це абревіатура типів загроз, на які вона спрямована.

Таблиця 3.2 – Загрози якими керує STRIDE

Тип загрози	Що було порушено?	Як було порушено?
Спуфінг (Spoofing)	Автентичність	Видавання себе за когось або за щось, ким ви не є
Підробка (Tampering)	Порушення цілісності	Підміна даних у системі для досягнення зловмисної мети.
Відмова від відповідальності (Repudiation)	Не підлягає відмові	Ствердження, що ви не несете відповідальності за дію
Розкриття інформації (Information disclosure)	Конфіденційність	Витік захищеної інформації стороннім особам.
Відмова в обслуговуванні (DoS)	Доступність	Вичерпання або відмова в доступі до ресурсів
Підвищення привілеїв	Авторизація	Дозвіл комусь робити те, на що він не уповноважений

2) Trike: фреймворк з відкритим вихідним кодом для моделювання загроз та оцінки ризиків. Проект почався у 2006 році, з метою підвищення ефективності та результативності існуючих методик моделювання загроз. Trike орієнтований на задоволення процесу аудиту безпеки з точки зору управління кібер-ризиками. Основою моделювання загроз Trike є модель вимог, яка гарантує, що встановлений рівень ризику для кожного активу є прийнятним для різних зацікавлених сторін.

3) PASTA: Процес моделювання атак та аналізу загроз PASTA – це семиетапна орієнтована на атаки методологія, розроблена у 2015 році, щоб допомогти організаціям узгодити технічні вимоги з бізнес-цілями, враховуючи при цьому аналіз впливу на бізнес і вимоги до відповідності. Мета цієї методології – забезпечити динамічний процес ідентифікації, переліку та оцінки загроз. PASTA орієнтована на те, щоб допомогти командам динамічно ідентифікувати та визначати пріоритети загроз.

Таблиця 3.3 – Ступені процесу PASTA

Назва процесу	Опис дій
Визначення мети	Визначення бізнес цілей Визначення вимог до безпеки та відповідності вимогам Аналіз впливу на бізнес
Визначення технічної галузі	Фіксація меж технічного середовища Фіксація залежності інфраструктури, додатків.
Розподіл додатку	Визначення випадків використання Визначення учасників Побудова діаграм потоків даних
Аналіз загроз	Аналіз імовірнісних сценаріїв атак Аналітика даних про загрози
Аналіз вразливостей	Використання дерев загроз Аналіз недоліків розробки/дизайну
Моделювання атак	Аналіз поверхні атаки Розробка дерева атак
Аналіз ризиків	Оцінка впливу на бізнес Виявлення контрзаходів та аналіз

Після того, як модель загроз завершена, можна розробити детальний аналіз виявлених загроз і відповідні засоби контролю безпеки. Моделювання загроз PASTA ідеально підходить для організацій, які бажають узгодити свої

дії зі стратегічними цілями, оскільки воно включає аналіз впливу на бізнес як невід'ємну частину процесу.

4) Моделювання загроз NIST: Національній інститут стандартів і технологій США (NIST) у 2016 році опублікував власну методологію моделювання загроз, орієнтовану на дані, яка фокусується на захисті цінних даних у системах. Вона моделює аспекти атаки та захисту для вибраних даних. У цій моделі аналіз ризиків здійснюється за допомогою наступних чотирьох важливих кроків: 1. Ідентифікація та опис системи і даних, що становлять інтерес. 2. Ідентифікація та вибір векторів атак для включення в модель. 3. Охарактеризування засобів контролю безпеки для пом'якшення векторів атаки. 4. Аналіз моделі загроз. Методи орієнтовані на менеджерів з безпеки, інженерів/архітекторів безпеки, системних адміністраторів, аудиторів та інших осіб, відповідальних за безпеку систем і даних.

5) VAST: високомасштабована концепція моделювання, яка унікальним чином вирішує проблеми як розробників, так і інфраструктурних команд. Автоматизація, інтеграція та співпраця є основою моделювання загроз VAST. Використовується дві моделі загроз: моделі загроз додатків для команд розробників та моделі операційних загроз для команд інфраструктури. Моделі загроз для команд розробників створюються за допомогою діаграм потоків процесів – блок-схем, які допомагають описати загальний потік бізнес-процесу і те, як користувач буде взаємодіяти з системою.

Зважаючи на різноманітність методологій моделювання загроз, вибір правильної для вашого бізнесу та середовища може бути непростим завданням. Не всі методології моделювання загроз створені з однаковим підходом. Деякі з них зосереджуються на моделюванні активів системи, інші – на зловмисниках.

Хоча всі методології моделювання загроз можуть ідентифікувати потенційні загрози, кількість і тип виявлених загроз будуть значно відрізнятися, включаючи якість, узгодженість і цінність, отриману від цих

моделей загроз. Те, що ідеально підходить з точки зору особливостей і підходів до моделювання для однієї організації, може не підійти для іншої. Щоб переконатися, що дані про загрози є дієвими, команди безпеки повинні розшифрувати, який метод відповідає їхнім конкретним бізнес-цілям і завданням.

Необхідно враховувати безліч факторів, таких як система або тип загроз, які моделюються, і з якою метою, підхід до моделювання (орієнтований на активи, орієнтований на атаки або орієнтований на програмне забезпечення), який найкраще відповідає вашим потребам, бажаний результат, здатність до масштабування, можливість генерувати звіти і здатність вимірювати ефективність моделювання загроз, серед інших.

3.3 Модель порушника

Модель порушника в хмарних послугах – це концептуальна уява про типові характеристики, поведінку та можливості осіб або груп, які можуть здійснювати атаки на хмарні сервіси і інфраструктуру. Модель порушника в хмарних послугах використовується для аналізу та оцінки потенційних загроз безпеці хмарних послуг. Вона допомагає розуміти типи осіб або груп, які можуть здійснювати атаки, їх мотивації та цілі [14, 21].

Це дозволяє розробляти стратегії та заходи безпеки, які враховують специфіку потенційних порушників і спрямовані на запобігання атакам, захист даних та забезпечення надійності хмарних послуг. Крім того, модель порушника може бути використана для розробки сценаріїв загроз та проведення імітаційних тестів, що сприяє виявленню слабких місць і поліпшенню системи безпеки. Основні складові моделі порушника:

1) Типи порушників: Модель може ідентифікувати різні типи осіб та груп, які можуть порушувати безпеку хмарних послуг. Це можуть бути хакери, конкуренти, внутрішні зловмисники.

2) Характеристики порушників: Модель включає опис характеристик порушників, таких як мотивація, доступні ресурси та знання, способи атаки, використані інструменти та технології.

3) Мотивація: Модель може аналізувати мотивацію порушників, таку як отримання фінансової вигоди, нанесення шкоди конкурентам або просто бажання порушити систему.

4) Методи атаки: Модель може описувати різні методи атак, які можуть бути використані порушниками для злому хмарних послуг. Це можуть бути атаки на мережевий рівень, злам протоколів або використання вразливостей.

5) Ризики та наслідки: Модель оцінює ризики, пов’язані з різними типами порушників та передбачає потенційні наслідки їх дій. Це допомагає розуміти вплив атак на безпеку хмарних послуг та розробляти відповідні стратегії захисту

Таким чином, модель порушника в хмарних послугах є інструментом для аналізу ризиків та розробки стратегій безпеки, що сприяє поліпшенню захисту хмарних послуг від потенційних атак та забезпеченню високого рівня безпеки даних та інфраструктури.

3.4 Модель безпеки хмарних послуг

Безпека хмари – це відповідальність, яка розподіляється між хмарним провайдером і клієнтом. В основному існує три категорії відповідальності в моделі спільної відповідальності: відповідальність, яка завжди лежить на провайдері, відповідальність, яка завжди лежить на клієнті, і відповідальність, яка змінюється в залежності від моделі обслуговування: Інфраструктура як послуга (IaaS), платформа як послуга (PaaS) або програмне забезпечення як послуга (SaaS) [22].

Безпека хмарних технологій починається з архітектури безпеки хмарних технологій. Організація повинна спочатку зрозуміти свій поточний стан безпеки хмарних технологій, а потім спланувати засоби контролю та рішення для захисту хмарних технологій, які вона використовуватиме для запобігання та пом'якшення загроз. Таке планування має вирішальне значення для захисту надскладних середовищ, які можуть включати кілька публічних хмар, сервіси SaaS і PaaS, локальні ресурси, доступ до яких

здійснюється як з корпоративних, так і з незахищених персональних пристроїв [15].

Відповідальність за безпеку, яка завжди лежить на провайдері, пов'язана із захистом самої інфраструктури, а також з доступом до фізичних хостів і фізичної мережі, на яких працюють обчислювальні екземпляри, сховища та інші ресурси, встановленням виправлень і конфігурацією.

Відповідальність за безпеку, яка завжди лежить на замовнику, включає управління користувачами та їхніми правами доступу (управління ідентифікацією та доступом), захист хмарних облікових записів від несанкціонованого доступу, шифрування та захист хмарних даних, а також управління станом безпеки.

Оскільки хмара не має чітких периметрів, вона представляє принципово іншу безпекову систему. Це стає ще більш складним завданням, коли застосовуються сучасні хмарні підходи, такі як автоматизовані методи безперервної інтеграції та безперервного розгортання, розподілені безсерверні архітектури та непостійні ресурси.

Деякі з найсучасніших проблем безпеки в хмарних середовищах та численні рівні ризиків, з якими стикаються сучасні хмаро орієнтовані організації [16]:

1) Збільшення поверхні атаки: хмарне середовище стало великою і дуже привабливою поверхнею для атак хакерів, які використовують погано захищені хмарні порти для доступу до робочих навантажень і даних у хмарі та їх порушення. Шкідливе програмне забезпечення, захоплення облікових записів та багато інших зловмисних загроз стали повсякденною реальністю.

2) Відсутність видимості та відстеження: У моделі IaaS хмарні провайдери повністю контролюють рівень інфраструктури і не показують його своїм клієнтам. Відсутність видимості та контролю ще більше посилюється в хмарних моделях PaaS та SaaS. Клієнти хмарних сервісів часто не можуть ефективно ідентифікувати та кількісно оцінити свої хмарні активи або візуалізувати своє хмарне середовище.

3) Постійно мінливі робочі навантаження: Хмарні ресурси надаються і виводяться з експлуатації динамічно – в масштабі і з великою швидкістю. Традиційні засоби безпеки просто не здатні забезпечити дотримання політик захисту в такому гнучкому і динамічному середовищі з його постійно мінливими робочими навантаженнями.

4) DevOps та автоматизація: Організації, які прийняли високоавтоматизовану модель DevOps, повинні переконатися, що відповідні засоби контролю безпеки визначені і вбудовані в код і шаблони на ранній стадії циклу розробки. Зміни, пов'язані з безпекою, що вносяться після того, як робоче навантаження було розгорнуто у виробництві, можуть підірвати систему безпеки організації, а також збільшити час виходу на ринок.

5) Детальне управління привілеями та ключами: Часто ролі користувачів у хмарі налаштовуються дуже вільно, надаючи широкі привілеї, які виходять за рамки необхідних. Одним із поширених прикладів є надання прав на видалення або запис даних у базі даних непідготовленим користувачам або користувачам, які не мають бізнес-потреби видаляти або додавати активи бази даних. На рівні програми неправильно налаштовані ключі та привілеї наражають роботу сеансів на ризики безпеки.

6) Складне середовище: Для послідовного керування безпекою в гібридних і мультихмарних середовищах, яким сьогодні віддають перевагу підприємства, потрібні методи та інструменти, які безперебійно працюють у публічних хмарних середовищах, приватних хмарних середовищах і локальних розгортаннях, включно із захистом периферії мережі для географічно розподілених організацій.

7) Відповідність хмарним вимогам та управління: Однак клієнти несуть відповідальність за те, щоб їхнє робоче навантаження та процеси обробки даних відповідали вимогам. Враховуючи погану візуалізацію, а також динамічність хмарного середовища, процес аудиту відповідності стає майже нездійсненним, якщо не використовувати інструменти для

безперервної перевірки відповідності та видачі сповіщень в режимі реального часу про неправильні конфігурації.

Приступаючи до розробки надійної архітектури хмарної безпеки, важливо витратити час на розуміння моделі спільної відповідальності, різних передових практик хмарної безпеки і того, як найкраще підійти до забезпечення безпеки хмарних сервісів в контексті потреб, зобов'язань і ризиків вашого бізнесу. Залежно від типів хмарних сервісів, які використовує ваша організація, архітектура хмарної безпеки може бути складною. Важливо не недооцінювати час і навички, необхідні для розробки надійної та ефективної архітектури безпеки. Розгляньте можливість співпраці з постачальником послуг хмарної безпеки замість того, щоб намагатися створити індивідуальну архітектуру безпеки хмарних сервісів самостійно.

ВИСНОВКИ

У даній роботі проведено аналіз та дослідження безпеки хмарних послуг. За допомогою вивчення літератури, проведення аналізу ризиків та використання методів дослідження, було виявлено різноманітні загрози та виклики, пов'язані з хмарними послугами, а також розглянуто основні методи та стратегії захисту.

Безпека хмарних послуг є критично важливим аспектом для організацій, що використовують хмарні технології для зберігання, обробки та обміну даними. З моменту впровадження хмарних послуг, з’являються потенційні загрози та ризики пов’язані з безпекою, які потрібно враховувати.

Аналіз та дослідження безпеки хмарних послуг дозволяє виявити різні загрози, такі як: несанкціонований доступ, втрата даних, зловживання привілеями та інші. Ці загрози можуть виникати як зовні, так і всередині організації. Розуміння цих загроз дозволяє розробити ефективні стратегії та заходи безпеки для їх запобігання та виявлення.

Для запобігання та мінімізації ризиків безпеки хмарних послуг необхідно впроваджувати відповідні методи та практики. Це включає розробку політики безпеки, автентифікацію та авторизацію користувачів, шифрування даних, захист мережевої інфраструктури, моніторинг інцидентів та інші. Ефективне застосування цих методів допоможе знизити ризики та забезпечити надійність, конфіденційність та доступність хмарних послуг для користувачів

Аналіз та дослідження безпеки хмарних послуг є важливим кроком для організацій, які планують або вже використовують хмарні технології. Впровадження відповідних методів захисту допомагає підвищити рівень захисту інформації, забезпечити довіру користувачів та успішне впровадження хмарних технологій у різних сферах діяльності.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cloudflare. "What is the cloud? | Cloud definition" URL: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (дата звернення: 20.04.2023)
2. Techtarget. "What is public cloud? Everything you need to know" URL: https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing (дата звернення: 21.04.2023)
3. Geeksforgeeks. "Cloud Deployment Models" URL: https://www.geeksforgeeks.org/cloud-deployment-models/ (дата звернення: 24.04.2023)
4. Intel. "An Overview of Cloud Deployment Models" URL: https://www.intel.com/content/www/us/en/cloud-computing/deployment-models.html (дата звернення 25.04.2023)
5. Techtarget. "SaaS vs. IaaS vs. PaaS: Differences, Pros, Cons and Examples" URL: https://www.techtarget.com/whatis/SaaS-IaaS-PaaS-Comparing-Cloud-Service-Models (дата звернення 25.04.2023)
6. Synopsys. "Essential Cloud Computing Characteristics" URL: https://www.synopsys.com/cloud/insights/essential-cloud-computing-characteristics.html (дата звернення 30.04.2023)
7. IBM. "What is cloud security" URL: https://www.ibm.com/topics/cloud-security (дата звернення 03.05.2023)
8. Vectra. "What are Cloud Security Threats?" URL: https://www.vectra.ai/learning/cloud-security-threats (дата звернення 05.05.2023)
9. Astra. "Cloud Vulnerability Management: The Detailed Guide" URL: https://www.getastra.com/blog/security-audit/cloud-vulnerability-management/ (дата звернення 07.05.2023)
10. Ekran. "Cloud Infrastructure Security: 7 Best Practices to Secure Your

Sensitive Data" URL: https://www.ekransystem.com/en/blog/cloud-infrastructure-security (дата звернення 10.05.2023)

11. Synopsys. "Threat Modeling" URL: https://www.synopsys.com/glossary/what-is-threat-modeling.html (дата звернення 12.05.2023)
12. Threatmodeler. "HOW TO DO THREAT MODELING FOR CLOUD APPLICATIONS" URL: https://threatmodeler.com/how-to-do-threat-modeling-for-cloud-applications/ – 15.05.2023
13. Welekwe A. "Threat Modeling Guide" URL: https://www.comparitech.com/net-admin/threat-modeling-guide/ (дата звернення 20.05.2023)
14. Cox P. "Intrusion detection in a cloud computing environment. " URL: https://www.techtarget.com/searchcloudcomputing/tip/Intrusion-detection-in-a-cloud-computing-environment (дата звернення 22.05.2023)
15. Guidepoint security. "Cloud Security Architecture" URL: https://www.guidepointsecurity.com/education-center/cloud-security-architecture/ (дата звернення 25.05.2023)
16. GCFGlobal. "What is the cloud?" URL: https://edu.gcfglobal.org/en/computerbasics/understanding-the-cloud/1/ (дата звернення 20.04.2023)
17. IBM "IaaS vs. PaaS vs. SaaS" URL: https://www.ibm.com/topics/iaas-paas-saas (дата звернення 30.04.2023)
18. Vora S. "Characteristics of Cloud Computing." URL: https://www.tutorialspoint.com/characteristics-of-cloud-computing (дата звернення 30.04.2023)
19. Checkpoint. "What is Cloud Security?" URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/ (дата звернення 03.05.2023)
20. Cloud native wiki. "What Are Cloud Attacks?" URL: https://www.aquasec.com/cloud-native-academy/cloud-attacks/ (дата

звернення 05.05.2023)

21. CPI OpenFox. "Top Benefits For Cloud-Based Computing In Law Enforcement" URL: https://www.openfox.com/top-benefits-for-cloud-based-computing-in-law-enforcement/ (дата звернення 22.05.2023)
22. NetApp BlueXP. "Cloud Security Architecture for IaaS, PaaS and SaaS" URL: https://bluexp.netapp.com/blog/blg-cloud-security-architecture-for-iaas-paas-and-saas (дата звернення 25.05.2023)