Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: «Дослідження впливу хмарних технологій в задачах забезпечення неперервності бізнес-процесів»

Виконала: студентка 6 курсу, групи СБмз-61
спеціальності 125 - Кібербезпека
(шифр і назва спеціальності)

(підпис) (прізвище та ініціали)

Керівник
(підпис) (прізвище та ініціали)

Нормоконтроль
(підпис) Лобур Т.Б (прізвище та ініціали)

Завідувач кафедри
(підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент
(підпис) (прізвище та ініціали)

Тернопіль
2020

АНОТАЦІЯ

Дослідження впливу хмарних технологій в задачах забезпечення неперервності бізнес-процесів // Кваліфікаційна робота «Магістр» // Фершлядин Мар'яна Миронівна// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2020 // С.69 , рис. 3 , табл. 13, кресл. – , додат. 3 .

Ключові слова: ХМАРНІ ТЕХНОЛОГІЇ, БЕЗПЕКА, НЕПЕРЕРВНІСТЬ БІЗНЕС-ПРОЦЕСІВ

Під час виконання кваліфікаційної роботи було розроблено гібридну модель хмарних технологій та систему рекомендацій їх застосування для забезпечення неперервності бізнес-процесів малого підприємства "Яреш" на основі проведеного порівняльного аналізу хмарних технологій.

В першому розділі описано характеристики, моделі та типи хмарних сервісів, наведено переваги та недоліки хмарних обчислень. Розділ 2 присвячений питанням безпеки хмарних сервісів. В третьому розділі розроблено модель та рекомендації розгортання хмарних сервісів для досліджуваного підприємства з врахуванням вимог забезпечення бізнес-процесів. В четвертому розділі описано окремі питання охорони праці та безпеки життєдіяльності в надзвичайних ситуаціях.

ANNOTATION

Research of cloud technologies impact in the problems on business processes continuity maintaining // Thesis of the Master Degree // Fershliadyn Mariana Myronivna // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2020 // P. 69, Fig. 3, Tables 13, Diagrams. - , Annexes.-, References 3.

Keywords: CLOUD TECHNOLOGIES, SECURITY, BUSINESS PROCESS CONTINUITY.

As a result of Master Thesis, a hybrid model of cloud technologies and a system of recommendations for its application were developed to ensure the continuity of business processes of the small enterprise "Yaresh" on the basis of a comparative analysis of cloud technologies.

The first section describes the characteristics, models and types of cloud services, the advantages and disadvantages of cloud computing. Section 2 focuses on cloud service security. In the third section the model and recommendations of deployment of cloud services for the chosen enterprise are developed taking into account requirements of maintenance of business processes. The fourth section describes some issues of labor protection and occupational safety in emergencies.

СПИСОК СКОРОЧЕНЬ

КПО Коефіцієнт природнього освітлення;

ПБ Політика безпеки;

ПЗ Програмне забезпечення;

BaaS (анг. Backup as a Service) — сервісом резервного копіювання даних;

DRaaS (анг. disaster recovery as a service) аварійне відновлення даних;

IaaS (англ. nfrastructure as a service) інфраструктура як послуга;

NIST (англ. National Institute of Standards and Technology) Національний інститут стандартів та технології США;.

PaaS (англ. Platform as a Service) платформа, як сервіс;

STaaS (англ.Storage as a Service) сховище як послуга;

VPN (англ.Virtual Private Network) віртуальна приватна мережа;

SaaS (англ.Software as a service) Програмне забезпечення як послуга.

ЗМІСТ

ВСТУП

Технологічні інновації та їх впровадження – це два важливі фактори успіху для будь-якого бізнесу/організації. Швидке реагування на потреби та зміну ринку, адаптація та швидкий вихід бізнес продуктів це найцінніші критерії для бізнесу. З появою хмарних технологій в компаній появилася можливість забезпечити швидкий вихід на ринок з власним бізнес-продуктом та забезпечити неперервність бізнес-процесів, не створюючи при цьому власної IT-інфраструктури.

Хмарні обчислення завдяки своїм характеристикам дозволяють організаціям або приватним особам обмінюватися різними послугами безперешкодно та економічно ефективно.

Актуальність теми досліджень. У сучасному світі практично будь-яка послуга, яка не вимагає від вас фізичної близькості до комп'ютерного обладнання, яке ви використовуєте, тепер може бути доставлена через хмару. Сьогоднішня ситуація з пандемією зробила тему хмарних технологій та неперервності бізнес-процесів як ніколи актуальною. Тому, що вірус практично припинив діяльність багатьох організації, які до сьогодні не використовувати хмарні сервіси або не мали власної розвиненої IT-інфраструктури. Хмарні сервіси стали практично незамінними для малого та середнього бізнесу. Через актуальність теми, її досліджує багато науковців. Багато статей та робіт на цю тему можна зустріти і в авторів ТНТУ, зокрема, Загородна Н.В [1], Кареліна О.В. [2] Лобур Т.Б. [3] Боднарук І.О. [4] Карпінський[5]

Метою даної роботи є розробка рекомендацій та моделі застосування хмарних технологій для забезпечення неперервності бізнес-процесів малого підприємства на основі проведеного порівняльного аналізу хмарних технологій.

Щоб досягнути поставлену мету дипломного проекту необхідно розв'язати *наступні задачі*:

1. Здійснити аналіз сучасних хмарних сервісів.
2. Вибрати сервіси які впливають на неперервність бізнес-процесів .

3. Розробити модель розгортання хмарної інфраструктури, яка буде забезпечувати поставлені задачі досліджуваної компанії.

4. Обрати критерії для порівняння хмарних провайдерів та сервісів.

5. На основі порівняння зробити висновки, щодо вибору хмарного провайдера та сервісів.

6. Надати рекомендації щодо підвищення рівня захисту хмарних сервісів.

Об'єкт дослідження – хмарні сервіси.

Предметом дослідження моделі та характеристики хмарних технологій.

Методи дослідження: загальнонаукові методи пізнання та порівняння.

Наукова новизна даної роботи: В роботі проведено порівняльний аналіз хмарних сервісів з огляду на забезпечення неперервності бізнес-процесів та сформовано рекомендації їх використання для підприємств малого бізнесу.

Практичне значення роботи розгортання гібридної хмарної інфраструктури для компанії «Яреш» відповідно до потреб, для забезпечення неперервності бізнес-процесів.

Апробація результатів дослідження. Окремі результати роботи публікувались на III міжнародній студентській науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, грудень 2020 р.

Структура роботи. Дипломний проект складається зі вступу, 4-ох розділів, висновків, списку використаних джерел із найменувань, додатків. У роботі міститься 3 рисунка, 13 таблиць. Обсяг основного тексту роботи становить 48 ст. перелік використаних джерел 5 ст., додатки 6 ст, загальний обсяг 69 ст.

РОЗДІЛ 1

1.1 Історія та ключові фактори у розвитку хмарних технологій

Концепція хмари вперше почала з'являтися у 60-тих роках 20століття. Тоді це було уявлення про великий ресурс, яким би могла користуватися велика кількість людей. Вже ближче до 21 століття. фахівці сфери інформаційних технологій терміном “хмара” намагались пояснити звичайним користувачам мережеві пристрої, тобто що інтернет процеси (обчислення та зберігання даних) знаходяться в центрах обробки даних так званій “хмарі”. Сам термін «хмара» [6] бере свій початок з телефонного зв'язку, оскільки телекомунікаційні компанії, пропонували виділені схеми передачі «точка-точка» в основному для своїх клієнтів до 1990-х років. Після чого, телефонія почала пропонувати віртуальні приватні мережі (VPN). Якість обслуговування у них була порівняною, але тепер це потребувало набагато менших витратах. Вони змогли ефективніше використовувати мережу, за допомогою перемикання трафіку для оптимального використання каналів.

Перші дослідження у свфері хмарних технологій в 1966 році, провів канадський технолог Дуглас Ф. Паркхілл (англ.Douglas Parkhill), у своїй книзі «The Challenge of the Computer Utility» він [7] дає характеристики хмарних обчислень, порівняння їх з електроенергетикою та використання приватних, публічних та громадських моделей. Проте інші джерела стверджують, що хмарні обчислення беруть свій початок ще з 50-х років 20століття. А саме через твердження, які висунув вчени, в галузі комп'ютерних технологій, Херба Гроша (англ.Herb Grosch). Його твердження було в тому, що колись увесь що весь світ працюватиме на терміналах, які керуватимуться великими центрами обробки даних.

Сама ідея того, що на сьогоднішній день називають обчисленням хмарних технологій озвучувалась ще у 1970 році американським науковцем Джозефом Ліклайдером (англ. J.C.R. Licklider), який бувних обчис відомий у

науковій та IT-середовищі як JCR або «Лік». У 70-ті роки він відповідав за створення ARPANET (Мережа Агентства передових досліджень) цю мережу вважають початком Інтернету), [6] ідея цього проекту полягала в тому, щоб будь яка людина землі буде підключена до мережі, через яку вона зможе отримувати не лише дані а й програми.

Інший американський вчений в галузі інформатики Джон Маккарті (англ. John McCarthy) висловлював свою ідею про те, що можна надавати користувачам обчислювальні потужності як сервіс (послугу). [6] На жаль, розвиток хмарних технологій на цьому припинився до 90-х років. Проте наступний ряд факторів дав поштовх швидкому подальшому розвитку хмарних технологій. Ряд факторів наведений у Таблиці 1.1

Таблиця 1.1 Фактори розвитку хмарних технологій

№	Фактор який вплинув на розвиток
1	В 90-ті роки вчені старалися через збільшення пропускної здатності Інтернету, отримати значний стрибок у розвитку в хмарної технології, але їм це не вдалося, оскільки жодна компанія та технології тих часів не були готові до цього. Але саме це підштовхнуло розвиток хмарних технологій.
2	У 1999 році поява компанії Salesforce.com., яка стала першою компанією що змогла надати доступ до свого додатку через сайт. По факту ця компанія стала першою хто надав своє програмне забезпечення як сервіс (SaaS)
3	Компанія Amazon у 2002 році, завдяки своїй розробці хмарного веб-сервісу, який дозволяв робити обчислення а також зберігати інформацію.

Продовження Таблиці 1.1

4	У 2006 році запущений компанією Amazon сервіс Elastic Compute cloud (EC2) . Цей веб-сервіс дозволяє користувачеві запускати свої власні додатки. Саме Amazon EC2 і Amazon S3 стали першими сервісами доступними для хмарних обчислень. Компанія завдяки модернізації своїх центрів обробки даних, вони, як і більша частина комп'ютерних мереж в один момент часу використовували лише 10 % своєї потужності, задля забезпечення надійності під час стрибку навантаження. Знаючи, про те що, що нова хмарна архітектура може забезпечувати значне внутрішнє підвищення ефективності, компанія
5	Amazon розпочинає нові дослідження, після чого вона, для зовнішніх клієнтів,в галузі розвитку продуктів забезпечення хмарних обчислень ,запускає, на основі розподілених обчислень , Amazon Web Service (AWS).
6	Після того як компанія Google створила платформу Google Apps для веб-додатків в бізнес секторі, зараз ця платформа відома, як G Suite for Education, розвиток хмарних обчислень повернув в іншу гілку.
7	Розвиток апаратного забезпезпечення. Він надав доступність до хмарних технологій приватним особам та малому бізнесу.

Саме ряд цих семи факторів дав поштовх швидкому подальшому розвитку хмарних технологій.

1.2. Характеристики, моделі та типи хмарних сервісів

Найбільшою популярністю серед різних визначень, користується визначення Національного інституту стандартів та технологій NIST (National Institute of Standards and Technology). Це визначення тлумачить нам, що [8]

хмарні обчислення - це така модель для забезпечення, зручного мережевого доступу всюди на вимогу до спільного набору об'єктів (які можуть виконувати одну, спільну для них функцію) конфігурованих обчислювальних ресурсів (для прикладу, мереж, серверів, сховищ, додатків та послуг), які можна швидко забезпечити та випустити з мінімальними зусиллями управління або взаємодія з постачальником послуг. Також, Національний інститут стандартів та технологій пропонує, щоб [8] в основі хмарних технологій було п'ять основних характеристик, три рівні обслуговування, а також чотири моделі розгортання.

1.2.1 Характеристики хмарних сервісів

Згідно з NIST в ідеалі кожна хмара повинна мати п’ять характеристик.

Таблиця 1.2 Характеристики хмари:

Характеристика	Означення
On-demand self-service (самообслуговування на замовлення(вимогу))	Ця характеристика означає що означає, що кожен споживач може отримувати та вимагати(запитувати) доступ до послуг без адміністратора або без допомоги будь-якого іншого персоналу, який би виконував запит вручну. [9] On-demand self-service виконує процеси та запити автоматично. Ця автоматизація дає перевагу, як для постачальника, так і для користувача.
Broad network access (широкий доступ до мережі)	Ця харастика надає можливості доступні через мережу. Доступ до цих можливостей здійснюється за допомогою стандартних механізмів. Ці механізми сприяють використанню різнорідних тонких або товстих клієнтських платформ (мобільних телефонів, ноутбуків,планшетів).

Продовження таблиці 1.2

Rapid elasticity *(швидка еластичність)*	Цей термін використовують для масштабованого забезпечення або можливості надання масштабованих послуг. Для користувача такі можливості, доступності для забезпечення, часто здаються необмеженими і можуть бути надані в будь-якій кількості в будь-який час.
Measured service *(мірне обслуговування).*	Цей термін означає, що користувач використовуючи хмарні ресурси - незалежно від того, працюють екземпляри віртуальних серверів чи зберігаються в хмарі - отримує контроль, вимірювання та звітування провайдером хмарних послуг. Так, як використання ресурсів хмарних обчислень вимірюється, і виробничі організації платять відповідно за те, що вони використали. Таким чином, використання ресурсів можна оптимізовують, використовуючи можливості оплати за використання. Така модель витрат базується на понятті “платити за те, що використовується ".

Крім наведених вище характеристик, в стандарті ISO 17788, згадується ще одна додаткова характеристика Multi-tenancy. Multi-tenancy (колективна оренда).У приватній хмарі користувачів називають називають орендарями. Вони можуть мати різні підрозділи бізнесу всередині однієї компанії. У загальнодоступній хмарі [9] споживачами є часто абсолютно різні організації. У більшості випадків державні хмарні провайдери використовують саме цю модель. Колективна оренда дозволяє своїм клієнтам запускати один екземпляр

сервера, що є дешевшим і полегшує розгортання оновлень для великої кількості клієнтів. По принципу multi-tenancy влаштований сервіс публічної хмари.

1.2.2. Моделі обслуговування хмарних сховищ

На сьогоднішній день в Україні виділяють не менш, як 11 популярних моделей хмарних сховищ [11]. І вони щороку розширюють спектр хмарних послуг. Як правило, провайдери хмарних послуг, пропонують послуги, які можна згрупувати у три категорії: інфраструктура як послуга, платформа як послуга та програмне забезпечення як послуга. Основні послуги хмарних сервісів наведені в Таблиці 1.3

Таблиця 1.3 Основні хмарні сервіси

Послуга	Означення
IaaS (Infrastructure as a Service) інфраструктура як послуга.	Така модель послуг [10] дає можливість використовувати хмарну інфраструктуру для самостійного зберігання та обчислень, також для володіння обмеженим контролем за набором доступних мережевих сервісів (наприклад, фаєрволом, DNS). Системи зберігання даних, сервери, комутатори, маршрутизатори та інші системи об'єднуються та надаються для зберігання робочих навантажень, які видозмінюються від компонентів програми до високопродуктивних обчислювальних програм. В Україні одними з найбільш використовуваних сервісів типу IaaS є VPS (Virtual Private Server) або VDS (Virtual Dedicated Server).
PaaS (Platform as a Service) платформа як послуга.	Модель PaaS означає, [10] що споживач може отримати доступ до використання інформаційно-технологічних платформ завдяки хмарним сервісам, які розміщуються у хмарного провайдера та може використовуватися для створення служб вищого рівня.

Продовження Таблиці 1.3

SaaS (Software as a Service) - програмне забезпечення як послуга	Модель SaaS означає надання програмної послуги на вимогу означає, що [10] кілька кінцевих користувачів або організацій можуть використовувати одну єдину програму за допомогою хмарного сервісу. Одним з найбільш відомих прикладів використання моделі SaaS є salesforce.com, хоча багато інших прикладів оживляють ринок, включаючи Google Apps. Вони пропонують основні корпоративні послуги, включаючи обробку електронної пошти та обробки текстів.

У таблиці нижче наведено порівняння різних підходів організації в IT-інфраструктури. Символом “+” позначається що системою керує власник, а символом “-” позначається керування провайдером

Таблиця 1.4 Порівняння підходів організації в IT- інфраструктурі

	Власна IT-інфраструктура	IaaS	Paas	SaaS
Додатки	+	+	+	-
Дані	+	+	+	-
Середовище виконання	+	+	-	-
Операційна система	+	+	-	-
Платформи віртуалізації	+	-	-	-

Продовження Таблиці 1.4

	Власна IT-інфраструктура	IaaS	Paas	SaaS
Сервери	+	-	-	-
Системи зберігання даних	+	-	-	-
Мережеве обладнання	+	-	-	-

Фахівці налічують не менш як два десятки підкритерій, різних моделей, послуг IaaS, SaaS, PaaS. Також варто відзначити що в Україні як і всьому світі, більша частка ринку хмарних послуг належить IaaS та SaaS, а частина PaaS є відносно невеликою (особливо в Україні) і її частка продовжує зменшуватись. Також варто відмітити, що моделі Infrastructure as a Service, Software as a Service та Platform as a Service застосовуються до всіх типів хмар (публічних, приватних, гібридних, суспільних).

До інших моделей які також часто використовуються, та користуються популярністю в Україні можна віднести[11]:

Таблиця 1.5 Сервіси які використовують в Україні

Назва	Пояснення
CaaS (Container as a Service)	вміст як послуга або керований контент як послуга
DRaaS (Disaster Recovery as a Service)	аварійне відновлення як сервіс

Продовження Таблиці 1.5

Назва	Пояснення
DBaaS (Database as a service)	база даних як сервіс
MaaS (Mobility as a Service)	мобільність як послуга
DaaS (Desktop as a Service)	робочий стіл як послуга
NaaS (Network As A Service)	мережа як сервіс
STaaS (Storage as a Service)	сховище як послуга

Самими популярними та бажаними залишаються такі моделі як PaaS, SaaS, STaaS і BaaS. Якщо будь-яка організація буде використовувати послуги від одного або декількох хмарних сховищ, то це дозволить її реалізувати повний цикл бізнес-процесів. Наприклад, можна створити віртуальну платформу для автоматизації управлінської системи. Модель STaaS є заключною моделлю хмарного сервісу, оскільки вона дозволяє отримати необхідний обсяг віртуального дискового простору для реалізації всіх завдань. Для користувача або організації достатньо лише вибрати кращу комплексну пропозицію. А вона в свою чергу гарантуватиме повний цикл робіт в рамках одного хмарного сервісу. Вартість надання таких послуг буде залежати від обсягу послуг яких обере користувач.

1.2.3 Моделі розгортання хмарних сервісів

У загальному хмари для різних за розміром структур (від приватних організацій, до держустанов) можна розділити на 4 типи хмарних сервісів:

1. Публічні хмари.

2. Мультихмара.

3. Приватні хмари.

4. Гібридні хмари.

Відповідно до своїх потреб кожна організація розгортає таку модель хмарних сервісів, яка підходить дня неї найбільше. Відомо, що більшість організацій надають перевагу гібридній моделі розгортання. Але, не можна стверджувати, що така модель підходить для всіх, оскільки значна частина організацій надає перевагу приватним хмарам. Нижче наведемо детальнішу характеристику для кожної з хмар.

Публічна - це хмарна інфраструктура, яка надається [12] для відкритого використання широкому загалу. Вона може належати може бути власністю, управлінням та управлінням бізнесу, академічної чи державної організації, або їх поєднання.

Інфраструктура публічної хмари розгортається в приміщенні хмарного провайдера. Користувачі таких типів хмар не мають можливості керувати та обслуговувати цю хмару. Вся відповідальність за обслуговування такою хмарою покладається на власника цієї хмари. Користувачем запропонованих сервісів може стати як будь-яка компанія так і будь-який індивідуальний користувач. Вони пропонують легку та доступний за ціною спосіб розгортання веб-сайтів чи бізнес систем, з великими можливостями для масштабування, які в інших рішеннях були б не доступними. Серед відомих компаній які надають такі сервіси є: Amazon EC2 та Simple Storage Service (S3), Google Apps/Docs, Salesforce.com, Microsoft Office Web.

У таблиці нижче наведені основні переваги та недоліки використання публічної хмари.

Таблиця 1.6 Переваги та недоліки публічної хмари

Переваги	Недоліки
Простота та ефективність у використанні	Контроль IT- інфраструктури сторонньою компанією (оператором)
Гнучкість як фінансова так і технологічна	
Перетворення капітальних витрат в операційні	
Економія на обслуговуючому персоналі	Залежність від стабільності доступу та швидкості Інтернету
Споживання IT-послуг в необхідному обсязі (відсутність переплат)	
Легкість масштабування	Постійна абонплата в незалежності від успіхів компанії
Швидка відповідь та реакція на пікові навантаження систем	
Надійність та відмовостійкість	Необхідність особливих підходів до організації кіберзахисту
Оновлення обладнання комплектуючих та ПЗ	

Приватна хмара - такий тип хмарної інфраструктури [12] призначений виключно для використання однією єдиною організацією, що складається з декількох споживачів (наприклад, бізнес-підрозділів). Такий тип хмар може керуватися організацією самостійно, або організація може доручити керування зовнішньому підряднику. Інфраструктура такого типу хмар може знаходитися в приміщеннях замовника (дата цетрах), або у зовнішнього оператора, також можливий варіант часткового знаходження у замовника та оператора. Найкращим варіантом знаходження інфраструктури для приватної хмари це розміщення на території організації, яка б обслуговувалась та керувалася її робітниками. Відомо, що моделям розгортання приватної хмари надають перевагу в більшості великі організації, та розгортає її інфраструктуру на своїй території. Часка використання приватних хмар складає близько 17%.

У таблиці нижче наведені основі переваги та недоліки приватної хмари

Таблиця 1.7 Переваги та недоліки приватної хмари

Переваги	Недоліки
Простота та ефективність у використанні	Контроль IT- інфраструктури сторонньою компанією (оператором)
Гнучкість як фінансова так і технологічна	
Перетворення капітальних витрат в операційні	
Економія на обслуговуючому персоналі	Залежність від стабільності доступу та швидкості Інтернету
Споживання IT-послуг в необхідному обсязі (відсутність переплат)	
Легкість масштабування	Постійна абонплата в незалежності від успіхів компанії
Швидка відповідь та реакція на пікові навантаження систем	
Надійність та відмовостійкість	Необхідність особливих підходів до організації кіберзахисту
Оновлення обладнання комплектуючих та ПЗ	

Отже, використовуючи приватну хмару, організація може контролювати рівень ізоляції, безпеки та конфіденційності даних.

Мульти-хмара - це така хмарна інфраструктура призначена для [14] використання певною спільнотою споживачів з організацій, які мають спільні потреби(занепокоєння) (наприклад, місія, вимоги безпеки, політика та міркування щодо дотримання). Такий тип хмар належить, керується та експлуатуватися однією або кількома організаціями громади, третьою стороною або деякою їх комбінацією. Інфраструктура мультихмар може розміщуватися в приміщеннях замовника чи поза ними [14] . Вартість громадської хмари є змінною. Вона залежить від тривалості зберігання даних. Коли збільшується час зберігання даних, то і відповідно збільшується і вартість. Такий тип хмар набагато більше підходить для динамічних даних. Загалом громадські хмари можуть бути економічно вигідними від приватних, через те, що користувачу не потрібно купувати ресурси заздалегідь.

Гібридна - це така хмарна інфраструктура яка складається з двох двох або більше різних хмарних інфраструктур (приватної, громадської або публічної), які залишаються унікальними, але пов'язані між собою стандартизованою або власною технологією, яка дозволяє передавати дані та застосовувати портативність (наприклад, розрив хмари для балансування навантаження між хмарами). Такий тип хмар досить часто використовується коли в організації бувають сезонні періоди активності. Наприклад, як тільки перестає справлятися внутрішня інфраструктура з даними задачами, тоді частина потужностей переноситься на публічну хмару. Зазвичай гібридні хмари використовуються для того, щоб отримати гнучкість від публічної хмари та контроль ресурсів та рівень безпеки від приватної хмари. Таким чином компанія розміщує важливу IT-інфраструктуру в своїх дата-цетрах, що знаходяться під їхнім контролем. А менш значущі додатки розгортають на публічних хмарах. Але при цьому вся хмарна інфраструктура має змогу функціонувати як єдина система, функціонує як єдина система, що, власне, і є особливістю гібридних хмар. Особливою актуальністю гібридна хмара користується у випадку великих підприємств, які за своїм фахом повинні активно взаємодіяти з великою кількістю зовнішніх користувачів. Наприклад: держструктури, банки, авіакомпанії та багато інших організацій.

1.3 Переваги хмарних обчислень

На сьогоднішній день, хмарні технології розвиваються як ніколи стрімко. Вони стають доступнішими. Цим хмарні обчислення все більше ваблять не лише великі підприємства але й стартапи. У більшості компаній з'являється альтернатива, яка не була доступною їм раніше. Тепер усі хто не міг через фінанси дозволити забезпечити свій бізнес необхідною IT інфраструктурою. Тепер ці компанії можуть вибрати потрібні характеристики хмарних технологій, які підійдуть для їхнього профілю, потреб та масштабу бізнесу [14]. Хмарні технології забезпечують швидку можливість реагування на збільшення попиту на обчислювальні потужності інформаційних мереж та систем, а також

гнучко та швидко реагувати на потреби ринку. У своєму звіті, опублікованому у 2011р., компанія Visiongain, розповідає, що більш ніж 30% підприємств у світі вже використовують хоча б одну, хмарну технологію.

На нашу думку, однією з основних переваг використання хмарних технологій є скорочення витрат на обладнання та обслуговування IT інфраструктури. Окрім цього, хмарні технології дають інші переваги такі як:

- цілодобовий доступ до інформації яка зберігається на хмарі, тобто користувач корпоративної IT структури може в будь-який момент отримати доступ до необхідної йому інформації;
- незалежність від апаратної платформи (можливість підключення до системи за допомогою будь-якого пристрою (ПК, планшет, телефон, та ін.));
- мобільність (можливість доступу в будь-яких точках світу);
- гнучкість (без обмежене використання обчислювальних ресурсів, таких, як пам'ять, процесор, диски; оплата за фактичне використання хмарних ресурсів);
- резервне копіювання та відновлення;
- автоматична інтеграція програмного забезпечення (через те, що у хмарі інтеграція ПЗ відбувається переважно автоматично, то не виникає потреба в самостійній інтеграції додатків, крім цього, є можливість налаштування параметрів та вибір сервісів і програмних додатків які найкраще підходять для компанії);
- надійність (надійність яку забезпечують сучасні хмарні провайдери є на рівень вищою ніж надійність яку забезпечують локальні ресурси)
- швидке розгортання (вибираючи хмарні сервіси необхідні для того чи іншого процесу, можна практично через декілька хвилин запустити систему, яка буде виконувати необхідні функції.

Окрім основних переваг хмарних технологій, можна виділити і деякі переваги для бізнес підрозділів. Ці переваги наведені в Таблиці

Таблиця 1.8 Переваги хмарних технологій для бізнес підрозділів

Корпоративний відділ	Переваги які він може отримати
Відділ продажу та маркетингу	вся необхідна інформація доступна фахівцям відділу продажів з будь-якого пристрою
	оптимізація рішень і продажів
	прогнозування поведінки клієнтів
	розробка маркетингової стратегії
Відділ керування персоналом	оптимізація документообігу і спільної роботи завдяки загальному доступу до інформації
	спрощення процесу найму, мотивації, звільнення, утримання співробітників
	професійне навчання персоналу, розвиток навичок і компетенцій в зручному форматі без відриву від роботи
Служба підтримки клієнтів	клієнтам доступно самообслуговування, це призводить до зниження навантаження на операторів
	централізація бази даних
	об'єднання всіх операцій взаємодій з клієнтом

Крім переваг наведених у Таблиці 1.8 є ще багато інших переваг хмарної корпоративної IT-системи, для інших відділів інших організацій.

Отже, використання хмарних обчислень істотно знижує капітальні витрати для: побудови центрів обробки даних, для побудови мережі передачі даних. Використовуючи хмарні обчислення у користувачів не виникає потреби вирішувати проблеми, щодо забезпечення надійності, доступності та захищеності. Оскільки ці витрати, та вирішення цих проблем поглинаються провайдером хмарних послуг. А щодо, безпеки хмарних сервісів варто

відмітити, що [14] надійність хмар, а особливо тих які знаходяться в спеціально обладнаних для цього центрів обробки даних, є дуже високою. Оскільки ці ЦОД мають резервні джерела живлення, регулярні резервування даних, охорону, високу пропускну здатність Інтернет каналу, висококваліфікованих працівників, а також стійкість до DDOS атак. Але всі ці заходи будуть ефективними тільки при відповідальному відношенню, тому що при халатному ставленню ефект може бути повністю протилежними.

1.4 Недоліки хмарних технологій.

Як і всіх технологій у хмарних теж є свої плюси та мінуси. Незважаючи на переваги які було розглянуто у попередньому пункті, хмарні технології мають свої мінуси (недоліки). Насамперед це стосується невеликих компаній які хочуть використовувати ці технології. Отже недоліки хмарних технологій:

- Технічні несправності. Не беручи до уваги те, що інформація та дані доступні у хмарі 24/7 та в будь-якому місці,[16] існують моменти, що в цій системі можуть виникнути серйозні дизфункції. Варто пам'ятати, що ці технології піддаються перебоям та іншим технічним проблемам. Навіть найкращі постачальники не можуть гарантувати 100% технічної надійності. З боку користувача необхідне дуже хороше підключення до мережі Інтернет з високою пропускною здатністю, для виходу на сервер в будь-який час;
- Конфіденційність даних та безпека. З питань безпеки є недоцільним надання сороній компанії(провайдеру) повного доступу не лише для зберігання, але й для обробки важливих даних. Ще одна небезпека ховається у використаннях систем віртуалізації, а саме використання ядер стандартних ОС в якості гіпервізора, що дозволяє використовувати віруси. Небезпека зберігання даних в хмарі полягає ща в тому, що вони знаходяться у вільному доступі для програмних розробників сервісу та для правоохоронних органів, які за запитом, можуть отримати доступ до даних користувача, при цьому користувач не завжди знатиме про це. Окрім того на сьогоднішній день немає технології яка б

гарантувала 100% конфіденційність даних. Хоч і сама хмара є досить надійною системою, але якщо відбудеться несанкціонований доступ, то зловмисник зможе отримати доступ до великого сховища даних;

- Користувач не завжди має можливість налаштувати послуги які він використовує під особисті потреби;
- Дороговизна створення власної хмарної IT інфраструктури та її підтримка;
- Відсутність стандартів які регулюють сферу хмарних технологій;
- Повільніша робота порівняно з локальним комп'ютером. Існує ймовірність, повільної роботи програм на хмарних сервісах ніж на локальному комп'ютері. За рахунок великої кількості передачі інформації в деяких програмах, може сповільнюватися робота через завантаженість віддалених серверів, а також проблем які можуть виникати на шляху між користувачем і "хмарою";
- Надійність. Щодо надійності зберігання інформації в хмарних сервісах то можна з упевненістю сказати що якщо інформація втрачається на хмарі то вона втрачається назавжди.

У підсумку можна сказати, що основні недоліки хмарних технологій стосуються в більшій мірі безпеки. Але на сьогоднішній день ніхто не може гарантувати 100% безпеки, оскільки як швидко б не розвивалися засоби захисту так само швидко і знаходяться нові способи несанкціонованого доступу.

РОЗДІЛ 2

2.1 Вплив пандемії на неперервність бізнес-процесів

Найбільшим попитом хмарні сервіси користуються у ланках малого та середнього бізнесу. Це зумовлено тим, що малий та середній бізнес не може дозволити собі розгорнути повну IT-інфраструктуру та забезпечити її обслуговування та функціонування. Хмарні технології допомагають швидко розгорнути IT-інфраструктуру, пришвидшити вихід їхнього продукту на ринок, надають перевагу перед конкурентами, та забезпечують неперервність бізнес-процесів.

Через спалах Covid-19, велика кількість компаній які все ще знаходились в процесі покращення своєї хмарної безпеки, змушені були пришвидшити виконання своїх планів. Компанія DivvyCloud у своїй доповіді «2020 Cloud misconfigurations report» стверджує, [17] що порушення даних, які були спричинені неправильною конфігурацією хмари, коштували компаніям майже $ 3,18 трлн у 2019 році. Також у цій статті наводиться аналіз щодо витоків та зломів які стосуються сумнівних хмарних налаштувань. Аналіз показав що в 2018 році виявили 81 порушення, а в 2019 році було виявлено 115 [18]. У своїй офіційній статі компанія McAfee та CSIS (Центр стратегічних та міжнародних досліджень), показує, що через кіберзлочинність, глобальний бізнес втрачає майже 600 мільярдів доларів США (Lewis, 2018).

Спалах пандемії проілюстрував нам важливість та необхідність належного планування неперервності, тому, що пандемія фактично зупинила діяльність багатьох організацій. Через це, на [19] даний момент багато співробітників у всьому світі вимагають роботи вдома, криза зосередила увагу на безпеці хмарних сервісів та стійкості її інфраструктури, щоб протистояти загрозам хмарної безпеки. [20] В перші місяці карантину був зафіксований стрімкий ріст попиту на рішення щодо захищеної віддаленої роботи Cisco AnyConnect, також багаторазово збільшились запити на хмарні системи багаторазової автентифікації Cisco DUO, захисту від шкідливого коду Advanced

Malware Protection, та захисту інтернет трафіку Cisco Umbrella. Передумовою цього стрімкого попиту було надання компанією Cisco, безкоштовного доступу до продуктів для безпечної віддаленої роботи на 90 днів, що в свою чергу призвело до росту в 15% в тиждень, за перші місяці.

В умовах пандемії багато компанії не мали надійних рішень щодо кіберзахисту та забезпеченя безпеки віддалених процесів роботи. Для прикладу, деякі працівники могли використовувати власні пристрої для доступу до даних компанії та електронної пошти, або загальнодоступні сервіси для обміні файлами і відеоконференціями. Хоча хмарні технології є чудовим рішенням для узгодження інформаційних технологій із бізнес-стратегіями, але незважаючи на їхні переваги малі та середні підприємства неохоче застосовують ці технології, побоюючись за безпеку даних.

Щоб забезпечити неперервність бізнес-процесів[21], з гарантією високої доступності, компаніям потрібний план та інструменти, завдяки яким вони зможуть в разі потреби здійснити швидку аварійне відновлення, в разі недоступності основної інфраструктури. Але наявності для цього лише резервного ЦОД в хмарі чи на землі, недостатньо. Необхідний механізм для автоматизації відновлення. Цей механізм повинен за мінімальний період часу не лише відновити дані, але й гарантувати їхню цілісність.

2.2 Безпека хмарних технологій

Проблеми інформаційної безпеки - це активна область досліджень, яку потрібно вирішити належним чином, щоб запобігати загрозам безпеці та атакам, які можуть завдати серйозних збитків як для постачальників послуг, так і для споживачів послуг[22]. Вразливості кібербезпеки властиві хмарним сховищам, не є новизною. Багато компаній все ще перебувають у процесі поліпшення своєї хмарної безпеки. Якщо компанія хоче захистити свої хмарні активи, то вона потребує впровадження політики хмарної безпеки. Політика безпеки (ПБ) дає змогу швидко реагувати на загрози та виклики а також допомагає захистити хмарні дані.

У ПБ зазначається стратегія безпеки та керування усіма рішеннями щодо безпеки хмарних активів. В політиці хмарної безпеки визначають:

- які типи даних можуть і не можуть переміщатися в хмару;
- як команда розглядає ризики для кожного типу даних;
- ким повинне прийматися рішення про перенесення робочого навантаження на хмару;
- хто має право доступу або переміщення даних
- умови регулювання та поточний стан відповідності
- правильна реакція на загрози, спроби злому та порушення даних
- павила, що стосуються пріоритетності ризиків

Політика забезпечує цілісність та конфіденційність інформації та допомагає командам швидко приймати правильні рішення.

Політика забезпечує цілісність та конфіденційність інформації та допомагає командам швидко приймати правильні рішення. Міжнародною організацією зі стандартів (ISO) визначаються ключові вимоги безпеки хмарних технологій для ефективного та безпечного рішення, так як: конфіденційність, цілісність, доступність, аутентифікація, авторизація.

Конфіденційність- означає, збереження даних користувачів та надання доступу до них лише привілейованим суб'єктам.

Цілісність- гарантує відсутність змін даних, при зберіганні чи транспортуванні, і дозвіл на модифікацію, копіювання чи видалення лише уповноваженим користувачам.

Доступність - [23]гарантує, що дані які запитує користувач або потрібні йому послуги будуть доступними в будь-якому місці, та в будь-який час.

Аутентифікація - означає підтвердженняу особистосі користувача перед наданям доступу до даних. Підтвердження може відбуватися шляхом використання певних засобів захисту профілю (паролів).

Авторизація - [24] означає забезпечення того, щоб користувач, який запитав конкретну інформацію, мав права на доступ до неї.

В Таблиці нижче показані ключові вимоги безпеки хмарних сервісів відносно моделі розгортання та моделі обслуговування.

Таблиця 2.1 - Ключові вимоги до безпеки хмарних сервісів

	Моделі розгортання хмарних сервісів								
Ключові вимоги до безпеки хмарних сервісів	Приватна хмара/Суспільна хмара			Публічна хмара			Гібридна хмара		
Конфіденційність	+	+	-	-	+	-	+	-	-
Цілісність	+	+	-	+	-	+	+	+	+
Автентифікація	+	-	+	+	-	+	+	-	-
Доступність	+	+	+	-	+	+	-	-	-
Спостережність	+	-	-	+	+	+	+	-	-
Моделі обслуговування хмарних сховищ	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS

Обов'язкові вимоги в таблиці позначаються “+”, а додаткові “-”.

2.2.1 Загрози хмарних сервісів

Попри всі переваги хмарних обчислень існує також ряд загроз безпеці, які є перепоною для організацій, котрі хочуть використовувати хмарні технології.

Загроза - це обставини або події, які можуть спричинити порушення політики безпеки та нанести збитки ІКС. Користувачі хмар стикаються з двома типами загроз безпеці: зовнішніми та внутрішніми.

Контроль доступу це одна з основних загроз для систем хмарного зберігання даних. Ця загроза не є особливістю самих систем, а скоріше результат того, як компанії використовують їх. Кількість постачальників хмарних сервісів зростає, вони заохочують малі компанії перносити свої дані в

хмари, за рахунок безоплатних тарифних планів та зниження затрат. Тому в більшості випадків компанії переходять не обдумуючи ретельно про політику доступу. Захист від цієї загрози повинен включати строгу політику доступу та набір інструментів для аутентифікації та перевірки особистості. Що стосується політики доступу, то компанія повинна надавати доступ до певних файлів та систем в хмарному сховищі, лише тим співробітникам яким цей доступ потрібний для виконання їхньої роботи, а для інших обмежити. Також проводити регулярні перевірки рівнів доступу співробітників до хмарних систем компанії. Це потрібно для того щоб скасовувати непотрібні привілеї співробітників. Що стосується інструментів аутентифікації та підтвердження особи, то ці інструменти використовуються для того, щоб співробітники могли з інших пристроїв безпечно входити в системи компанії. Багато постачальників хмарних послуг для цього пропонують системи багатофакторної аутентифікації (MFA) як частину своїх стандартних пакетів.

Загроза порушення та витоку даних. [19] 91% кібератак направлені на спробу витоку даних, починаються з атак на електронну пошту організації. Порушення та витік даних в хмарних системах представляють більшу загрозу, ніж у тих, якими керують компанії власноруч. Це пов'язано з тим, що велика кількість інформації яка передається між співробітниками та хмарними системами, можу бути перехоплена зловмисниками, які шукають слабкі місця в системах організації. Щоб захистити організацію від цього типу загроз, потрібно використовувати безпечні комунікації та з'єднання, використовувати засоби захисту даних, під час передачі та зберігання. Засобами захисту може бути шифрування для поштового сервера, повідомлень, за допомогою використання цифрових сертифікатів (веб-сайтів SSL / TLS та сертифікати S / MIME (безпечне / багатоцільове розширення електронної пошти)). Також для безпечного доступу до хмар, працівники мають використовувати надійні VPN мережі.

Ще одна проблема з якою часто стикаються хмарні системи є втрата даних. Крім зловмисних атак, втрата даних може відбуватися по різному. Дані

можуть бути скомпрометовані через видалення, модифікацію, втрату ключа шифрування та іншими способами, такими як землетруси, повені та пожежі тощо. Щоб уникнути загрози повної або часткової втрати даних. [23] Компанія має застосовувати резервне копіювання та відновлення. Відсутність резервних копій даних можуть привести до того, що після попадання в систему програми-вимагача, всі дані будуть зашифровані та втрачені.

Загрози прикладних програмних інтерфейсів (Application Programming Interface(API)). API це основні інструменти які забезпечують взаємодію з хмарними сервісами. Переважно вони використовуються працівниками компанії які використовують API для доступу до даних, які зберігаються в хмарі, та персоналом постачальників хмарних послуг. [24] Найчастіші вразливості безпеки прикладних програмних інтерфейсів, це надання постачальникам хмарних сховищ надмірний рівень доступу до даних компанії. Щоб захистити свій бізнес від цієї загрози, потрібно ретельно вибирати постачальників хмарних сервісів. Постачальник повинен дотримуватися вказівок щодо безпеки API OWASP.

Ще однієї загрозою може бути неправильне налаштування хмарного сховища[25]. Неправильна конфігурація може залишити дані незахищеними. Неправильно налаштований хмарний додаток, може призвести до отримання або компрометації даних хмарних активів організації. Найгірші випадки відкритих даних часто пояснюються простою людською помилкою, а не злагодженою атакою. Щоб захиститися від цієї загрози потрібно постійно перевіряти настройки конфігурації.

В Додатку А наведені загальновизнані та узгоджені загрози безпеці хмарним сервісам, методи їх пом'якшення та хмарні сервіси на які вони впливають.

2.2.2 Атаки направлені на хмарні сервіси

Атакою можна назвати спробу реалізації загрози. Успішна атака призводить до порушення політики безпеки (компрометація даних). Для хмарних технологій успішна атака, може призвести до витоку великого об'єму

даних та призводить до численних збитків компанії. Все частіше стають помітними, атаки на зовнішні мережі у хмарі.

Зловмисники поза хмарою часто застосовує [26] DoS або DDoS-атаки, таким чином він має змогу впливати на доступність хмарних сервісів та ресурсів. Таким самим чином для отримання доступу до ресурсів хмар зловмисник використовує сканування портів, підміну IP-адресу, зараження DNS, а також фішинг. Зловмисний користувач може [27] захоплювати та аналізувати дані в пакетах, що надсилаються через цю мережу, за допомогою програм чи пристроїв перехоплення та аналізу мережевого трафіку. Підміна IP-адреси відбувається, коли зловмисник видає себе за IP-адрес законного користувача, по якому вони можуть отримати доступ до інформації, до якої інакше доступ отримати було б неможливо. Відсутність доступу до послуг, у тому разі коли вона потрібна, може стати катастрофою для будь-кого, особливо це стосується випадку відмови у наданні послуги. Така ситуація може статися, коли виснажений хост-сервер спричиняє відмову у запитах законних споживачів. Така відсутність доступу до послуги від якої залежить компанія, може коштувати їй великих грошей і часу.

Що стосується внутрішніх зловмисників, тобто авторизованих користувачів, то вони можуть з легкістю отримати доступ до ресурсів інших користувачів, і при цьому не бути виявленим. Внутрішні зловмисники [28] несуть більшу загрозу, оскільки вони мають більше привілеїв та знання, які пов'язуються з мережею, механізмами безпеки та ресурсами для атака, на відміну від зовнішніх зловмисників. Тому інсайдеру легко проникнути в атаку, ніж зовнішньому нападники. Відповідно внутрішньому зловмиснику набагато легше реалізувати атаку ніж зовнішньому.

Для здійснення атаки зловмисники використовують вразливості хмарних сервісів. Вразливість хмари це свого роду лазівка в архітектурі безпеки, яка використовується зловмисником для отримання доступу до мережі та інших інфраструктурних ресурсів.

Атака зомбі (Zombie Attack). Це атака за допомогою якої зловмисник через інтернет намагається флудити жертву (вести беззмістовний діалог, зметою відволікання уваги), надсилаючи запити від невинних хостів у мережі. Типи таких хостів [29] називаються зомбі. Через те, що в хмарі запити на VMs доступні кожному користувачу через Інтернет, то зловмисник може залити велику кількість запитів через зомбі-хости, і це призведе до перегруження хмари. Коли хмара переванатажена, та вичерпана для обслуговуання ряду запитів,[30] то це може спричинити відмову або розподілену відмову в обслуговуванні на сервері, іншими словами DoS та DDoS атаку. Через переповня запитами зловмисника, хмарний сервіс не може обслуговувати дійсні запити користувача. Забезпечити захист від такої атаки можна за допомогою покращення автентифікації, авторизації та IDS / IPS.

Атака SQL інєкцією. Це такий вид атаки коли стандартному коді SQL, зловмисник [31] вставляє шкідливий код для доступу до несанкціонованої бази даних, для отримання конфіденційних даних про користувача. У цьому випадку веб-сайт дозволяє через SQL Server отримати доступ до даних хакера, переглядаючи їх як дані користувача, це дозволяє зловмиснику отримати знання про те, як функціонує веб-сайт, і тому зловмисник може вносити у це зміни[32]. Для захисту від SQL інєкцій, використовують проксі-архітектуру для динамічного визначення вводу користувача із запиту, що генерується додатком, вона не вимагає доступу до бази даних або коду джерела веб-програми, а також має високий рівень виявлення.

Ін'єкція сервісів (Service Injection Attack). Оскільки хмарна система відповідвє за визначення та створення безплатного екземпляра запитуваної послуги, то адрес для доступу до цього нового екземпляру повинна передаватися користувачеві, що її запитує. Атака ін'єкції сервісів полягає в тому, що [33] зловмисник намагається ввести шкідливий сервіс або нову віртуальну машину в хмарну систему і може надавати шкідливу послугу користувачам. Хмарне програмне забезпечення впливає на хмарні служби, змінюючи (або блокуючи) функціональність хмари. Якщо зловмиснику вдасця

[34] створити шкідливі служби такі як SaaS, PaaS або IaaS, та додати їх до хмарної системи, то всі дійсні запити автоматично будуть перенаправлятися на шкідливі сервіси. Для захисту від цієї атаки слід реалізувати модуль перевірки цілісності служби. Сильна ізоляція між віртуальними машинами може завадити зловмисникові вводити шкідливий код у віртуальну машину сусіда.

Virtual machine escape. Ця атака реалізується коли програма зловмисника, що працює у віртуальній машині, [35] розбиває рівень ізоляції, щоб запускати кореневі привілеї гіпервізора, а не привілеї віртуальної машини. Це дозволяє зловмиснику взаємодіяти безпосередньо з гіпервізором. За допомгою цієї атаки , зловмисник [36] отримує доступ до головної ОС та інших віртуальних машин, що працюють на фізичній машині.

Rootkit in Hypervisor. Руткіти (програма для приховання слідів, що свідчать про наявність зловмисника або шкідливого ПЗ в системі) [37] на основі віртуальної машини запускають гіпервізор, який компроментує існуючу операційну систему хосту віртуальної машини. Таким чином, нова ОС (гостьова) працює в якості основної з відповідним контролем над ресурсам, але насправді цього хосту не існує. Також гіпервізором створюється прихований канал для виконання несанкціонованого коду в системі, що дозволяє зловмиснику контролювати будь-яку віртуальну машину, що працює на хост-машині, і маніпулює діями в системі. Загрози, що виникають через вразливості на рівні VM, можна пом'якшити шляхом моніторингу за допомогою IDS (система виявлення інструкцій) / IPS (система запобігання вторгненню) та впровадження брандмауера.

Атака "Людина посередині". Це такий тип атак, коли зловмисник вмішується в розмову між двома сторонами, видає себе за обидві сторони та отримує доступ до інформації, якою обмінювались між собою користувачі. Цю атаку можна реалізувати, [38] коли рівень захищених сокетів (SSL) налаштований неправильно. Атака людини посередині дозволяє зловмиснику отримати доступ до обміну даними між центрами обробки даних. Для виявлення цієї атаки потрібно [39] проводити аналіз мережевого трафіку. Для

зниження ризику атаки людина посередині потрібна правильна конфігурація SSL та тести передачі даних між уповноваженими сторонами.

Підміна метаданих. Ця атака означає, що зловмисник може [40] модифікувати чи змінювати файли мови опису веб-служби (WSDL), в якому зберігається опис екземплярів служби. Ця атака може бути реалізована, якщо зловмиснику вдастя перервати код виклику служби з файлу WSDL під час доставки. Для запобігання цій атаці, інформація про послуги та додатки повинна зберігатися в зашифрованому вигляді. Для доступу до цієї інформації потрібно застосовувати надійну автентифікацію (та авторизацію).

Фішинг атака. Ці атаки стали добре відомими через маніпуляції з веб-посиланнями та перенаправленням користувача на заражене посилання для отримання конфіденційних даних. В хмарах ця атака може застосовуватися для розміщення фішингових сайтів з метою захоплення облікових записів та служб інших користувачів в хмарі, використовуючи для цього хмарну службу.

Атака бекдор-каналу. Це вид пасивної атаки, яка [41] дозволяє хакеру отримати віддалений доступ до зламаної системи. За допомогою бекдор-каналів хакери можуть контролювати ресурси жертви і зробити його зомбі для спроби DDoS-атаки. Він також може бути [42] використаний для розголошення конфіденційних даних жертви. Для забезпечення захисту від таких атак необхідно забезпечити ізоляцію між віртуальними машинами.

Атаки отруєння файлами cookie. Коли відбувається така атака то [43] вміст файлу cookie змінюється, для того щоб можна було отримати доступ до до несанкціонованої програми або веб-сторінки. Оскільки у файлах cookie міститься конфіденційна інформація про дані користувача, то отримавши доступ до них зловмисник зможе виконувати незаконні дії.

CAPTCHA Breaking Attacks. CAPTCHA означає автоматизований загальнодоступний тест Тюринга, він [44] використовується для розпізнавання людини та комп'ютера, щоб визначити чи є користувач шкідливою програмою чи людиною. CAPTCHA використовує стандарті механізми захисту, які так

само використовують і для пошуку шкідливого прогрманого забезпечення такого як Троянські програми, черв'яки, ботнети та інші

У додатку Б ведена узагальнена Таблиця атак та методії їх попередження.

РОЗДІЛ 3 Дослідження впливу хмарних технологій на прикладі компанії

3.1. Опис компанії

Об'єктом дослідження було обрано компанію ТОВ “Яреш”. Причиною вибору цієї компанії, стало те, що вона відноситься до категорії малого бізнесу, та останнім часом починає нарощувати свої потужності. Оскільки компанія є не великою то її бюджет не дозволяє створювати та обслуговувати власну IT-інфраструктуру. Тому потребує впровадження деяких хмарних рішень.

Компанія “Яреш” вже більше 10 років займається оптовою та роздрібною торгівлею професійними лакофарбовими, деревообробними матеріалами у місті Тернополі та його регіонах. Також організація займається реставрацією дерев'яних будинків. Вона є дистрибутором таких компаній, як ELEMENT, Байріс, Янтар, Adler та Altax. В компанії налічується до 10 працівників. Компанія має 1 офіс-магазин та 1 складське приміщення.

В організації для роботи персоналу використовується клієнт-серверна архітектура. Це означає, що усі користувачі є клієнтами, які підключаються до сервера і працюють на ньому. Для стабільної роботи користувачів компанія має у власності 2 сервера, а також використовують блоки безперебійного живлення UPS. На одному сервері одночасно можуть працювати до 30 користувачів. Ресурси сервера розділяються між користувачами залежно від їхньої потреби. Типові характеристики сервера наведені в таблиці 3.1.

Компоненти	Комплектуючі
Процесор	Intel® Xeon® Processor E5-2620 24 ядра
Оперативна пам'ять	32 ГБ
Жорсткий диск	1 Тб
Відеокарта	Integrated
Пристрої введення	Мишка оптична, клавіатура qwerty
Пристрої виведення	Монітор LCD 22"

Таблиця 3.1. Характеристики сервера

Для належної роботи інформаційної системи підприємства на серверах компанії встановлене наступне програмне забезпечення:

- 1С Підприємство
- Microsoft Office 2016
- Mozilla Firefox
- Google Chrome
- ESET NOD32

На сьогоднішній день компанія "Яреш", що стосується хмарних технологій, використовує поштовий сервіс Gmail, та віртуальний хостинг. Так, як у компанії є свої сервери то варто розглядати таку модель хмари, як гібридну. Використовуючи таку модель розгортання хмари, компанія зможе підвищити рівень безпеки зберігаючи критично важливу інформацію на своєму сервер, а іншу на серверах постачальника. В плані послуг які потрібні для забезпечення неперервності бізнес-процесів компанія потребує: послуги з копіюванням та відновленням, послуги сховища, та послуги для віддаленої спільної роботи.

3.2 Хмарні послуги для забезпечення неперервності бізнес-процесів.

Одними з найпопулярніших та наймасштабніші компаній на світовому ринку які надають послуги хмарних сервісів є Google, Microsoft та Amazon. В Україні великою популярністю користуються De Nowo, Gigacloud, Ucloud.

У цьому розділі будуть наведені характеристики та порівняння хмарних сервісів вітчизняних та міжнародних компаній. Будуть розглянуті послуги

DRaaS,BaaS, DaaS, STaaS, таких компаній як Google, Microsoft, De Nowo, Ucloud.

3.2.1. DRaaS та BaaS

BaaS послуга резервного копіювання та відновлення, та послуга аварійного відновлення DRaaS. Ці дві послуги зосереджуються на [47] мінімізації втрати даних. Послуга BaaS спеціалізується виключно на довгостроковому зберіганні даних, коли DRaaS зосереджується на короткостроковому зберіганні даних, інфраструктури,стану системи та моделях безпеки, на яких працюють ці набори даних, і швидкості, з якою робочі навантаження можуть відновитись після інцидент. Послуга DRaaS є більш дорогим варіантом, оскільки вона крім даних охоплює охоплює інфраструктуру, модель безпеки, програми, системи та швидке відновлення.

Резервне копіювання та відновлення вирішують завдання збереження цілісності, доступності, та довгострокового зберігання даних.BaaS [46] захищає дані, шляхом створення резервних копій на локальному пристрої та хмарному середовищі. Якщо відбулася втрата даних, то їх можна відновити вибравши відповідний набір даних та скопіювавши його до початкового середовища. Оскільки BaaS більш спрямована на зменшення витрат та збереження даних на довгий період часу, то відновлення є більш тривалим процесом.

DRaaS фокусується на швидкості відновлення даних. Ця послуга [45] включає технологію «реплікації», при якій сторонній постачальник постійно копіює змінені дані середовища компанії у хмарне середовище зберігання, щоб компанія могла відновити до останньої ітерації для зменшення втрати даних, а також підтримувати безпеку та стан системи, як було налаштовано програми, що використовуються.

В таблиці наведено для яких типів організацій найкраще підходить DRaaS чи RaaS.

RaaS	DRaaS
IT-команда готова самостійно відновлювати інфраструктуру після катастрофи	Швидке повне відновлення як даних, так і інфраструктури є обов'язковим пунктом, як правило, продиктованим галузевими нормами чи вимогами клієнтів.
Розглянуті набори даних не часто змінюються.	Організацією та технічним обслуговуванням DR повинен керувати фахівець, щоб IT-команда могла зосередитись на основних бізнес-цілях
Резервне копіювання та довгострокове зберігання	Постійне тестування на DR та безперервність бізнесу складно та складно для бізнесу регулярно проводити через обмежені ресурси або зосередженість на стратегічному напрямку.
Бізнес може простоювати від кількох днів до тижнів	Поточні випробування для забезпечення безперервності DR і бізнесу є важким і складним для бізнесу, щоб виконувати на регулярній основі через обмежені ресурси або зосередитися на стратегічному напрямку.
Деякі втрати даних є прийнятними (зміни, внесені між останньою резервною копією та катастрофою, будуть втрачені)	Набори даних змінюються швидкими темпами, і найновіша копія має першорядне значення.
Бізнес має довгострокову хмарну стратегію.	Тривалий час простою шкодить репутації та прибутку торгової марки.
	Наявність останньої версії даних має важливе значення для ведення бізнесу.
	Бізнес має довгострокову хмарну стратегію.

Таблиця 3.2 Коли обирати RaaS, а коли DRaaS

Рішення BaaS часто може бути хорошим варіантом для найнижчого [47] рівня відновлення, оскільки воно дешевше, ніж рішення DRaaS Часто компанії використовують суміш як рішень BaaS, так і DRaaS, щоб отримати збалансоване покриття для свого бізнесу за ціною, яка відповідає їх цілям у бюджеті.

3.2.2 DaaS

«Робочий стіл як послуга» (DaaS) - це такаха схема пропонування послуги на хмарі, де кожному користувачу пропонується робочий сітл з набором необхідного прикладного програмного забезпечення. Віртуальна інфраструктура робочого столу (VDI), розміщується в хмарі та оплачується як послуга передплати. Рішення DaaS використовує [48] багатокористувацьку архітектуру, де один екземпляр програми доставляється декільком користувачам, або "орендарям". Сторонній постачальник послуг бере на себе відповідальність за управління інфраструктурою настільних ПК. DaaS дозволяє реалізувати максимально зручну, безпечну та просту взаємодію різних пристроїв в рамках однієї мережі, підвищуючи її мобільність а також робить ці пристрої незалежними від географічного розташування, що в свою чергу забезпечує неперервність процесів. Також сервіс «Робочий стіл як послуга» захищає важливу та конфіденційну інформацію для компанії, за допомогою того, що на пристроях працівників встановлюється лише те програмне забезпечення, яке здатне, перетворити пристрій в “тонкий” клієнт (з мінімальними вимогами, яких достатньо лише для того, щоб отримати зображення на дисплей, а також відправити команду на сервер, який буде їх вподальшому обробляти). На малюнку проілюстований доступ до хмари “тонкий” клієнт.

Всі інші важливі і конфіденційні дані зберігаються на сторонніх серверах. Використання DaaS передбачає застосування корпоративних стандартів в плані захисту інформації, що передбачає не тільки захист цієї інформації, але і її резервне копіювання, а також забезпечення безперервного функціонування бізнесу в цілому. Корпоративні дані будуть захищені не тільки від несанкціонованого доступу і крадіжки, але і від різних стихійних лих.

3.2.3 STaaS

Storage as a Service (STaaS) ця послуга надає сховище в користування і перекладається “сховище як послуга”. Це така модель хмарних технологій, в

якій користувач може отримати доступ за допомогою Інтернету. STaaS це керована послуга, [49] в якій постачальник надає доступ до платформи зберігання даних для кінцевого клієнта. Послуга може бути наданою з виділеної окремої клієнтської інфраструктури, або вона може надаватися із загальнодоступної хмари як спільна послуга, що надається підпискою та оплачується відповідно до однієї або декількох корисних показників. На малюнку наглядно проілюстрований процес використання STaaS

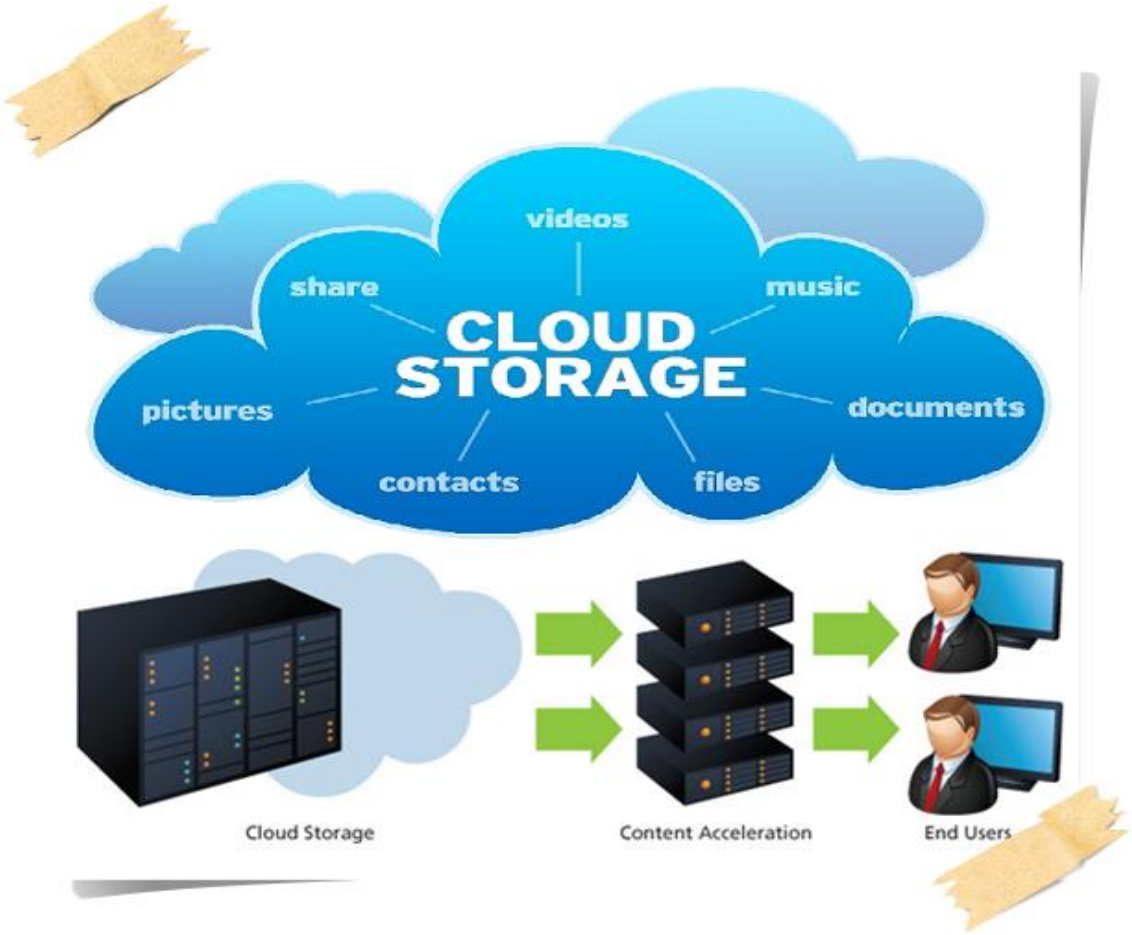

Рисунок 3.1 Модель передачі даних STaaS

За допомогою стандартних протоколів інтерфейсу пристрою або інтерфейсів прикладних програм (API) клієнти STaaS отримують доступ до окремих сховищ. Застосування “зберігання як послуга” це також і спосіб пом'якшення витрат на ліквідацію наслідків катастрофи, забезпечення довгострокового збереження записів та підвищення безперервності та доступності бізнесу. Для передавання даних та резервного зберігання та

відновлення будь-яких пошкоджених або відсутніх даних можна застосовувати STaaS. Вирізняють два типи віддаленого зберігання: зберігання об'єктів та блокове зберігання. В першому типі STaaS кінцевими клієнтами можуть зберігатися такі дані, як документи, тексти, PDF. Кожен блок функціонує як окремий жорсткий диск, і адміністратор сховища його налаштовує. В Другому типі STaaS він розділяє файл на окремі блоки даних, а потім зберігає блоки як єдину інформацію. Не маючи структури файлових папок, запам'ятовуючий пристрій може це зробити, оскільки кожен блок даних має унікальну адресу. Це дозволяє системі зберігання розподіляти окремі блоки даних там, де вона вважає найбільш корисним у системі зберігання. Кожного разу, коли до нього звертаються, програма системи зберігання збирає відповідні блоки назад, щоб зібрати файл.

3.3 Хмарні провайдери

У контексті дипломного проекту буде розглянуто вітчизняні та закордонні хмарні провайдери. Для аналізу та порівняння було обрано чотири провайдера Google, Microsoft, De Nowo, Ucloud.

Американська корпорація Google у 2008 році запропонувала свій перший хмарний сервіс, який став відомий широкому загалу в 2011 році. На сьогоднішній день, компанія пропонує більше як 50 послуг та 6 глобальних центрів обробки даних. Частка Google Cloud Platform на світовому ринку складає 5% . Компанією надаються такі послуги, як IaaS, SaaS, PaaS, FaaS (функція як сервіс, без серверні обчислення). На малюнку зображені популярні хмарні сервіси

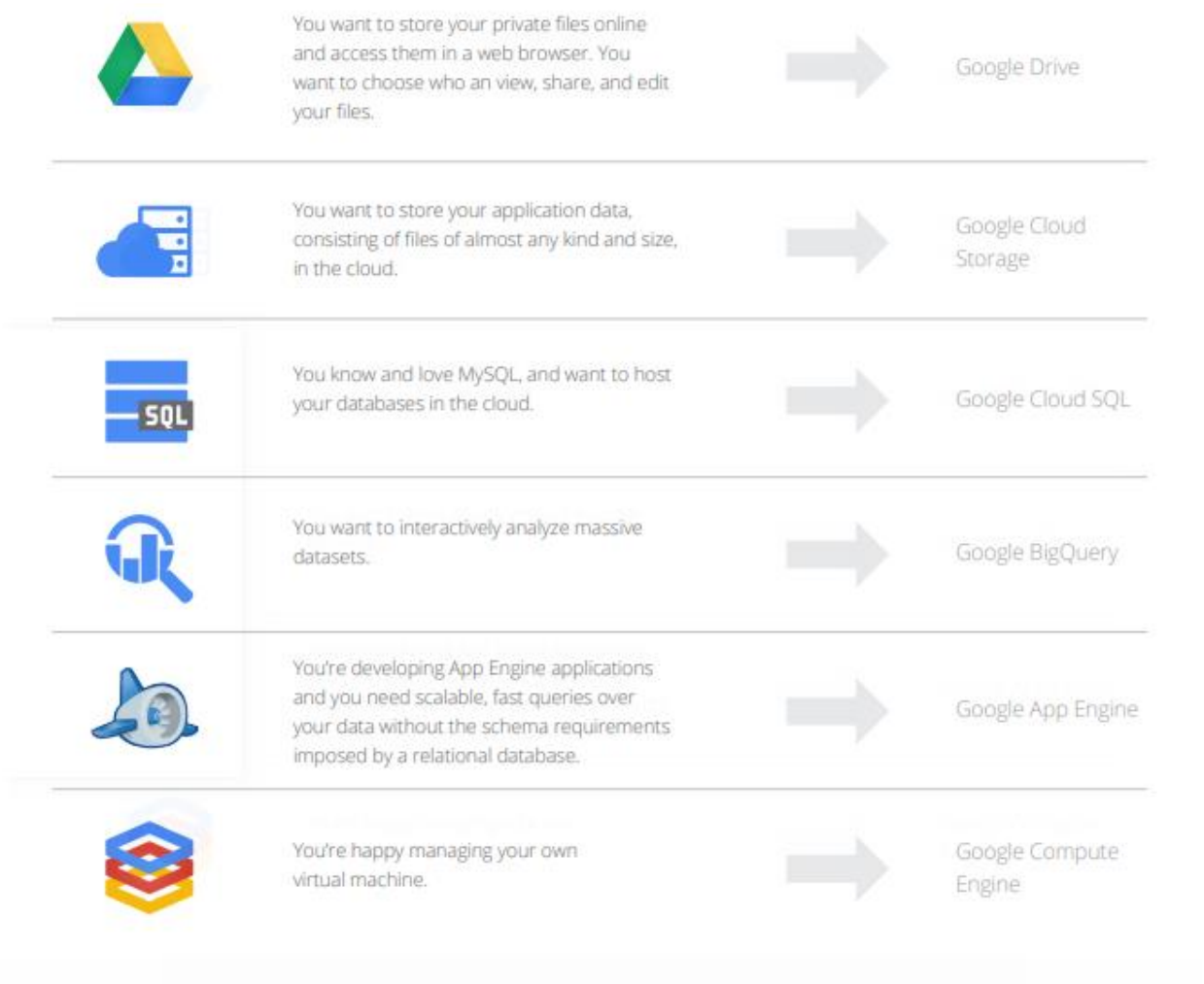

Рисунок 3.2 - Хмарні сервіси Гугл

Що стосується послуг для забезпечення неперервності бізнес-процесів то компанія пропонує такі сервіси: Google Storage, Google Chromebook, Google cloud platform.

Американська компанія Microsoft представила світу свої хмарні обчислювальні служби Microsoft Azure в 2010 році і не припиняв свого стрімкого розвитку. На сьогоднішній день Microsoft Azure є багатогранною складною системою, яка забезпечує підтимку багатьох різних послуг, мов програмування та фреймворків. Компанія налічує більш як 60 служб та ЦОД в 38 різних географічних регіонах, та займає 11% світового ринку. Компанія пропонує такі послуги як: IaaS, PaaS, SaaS, безсерверні обчислення. На рисунку зображені сервіси компанії Microsoft

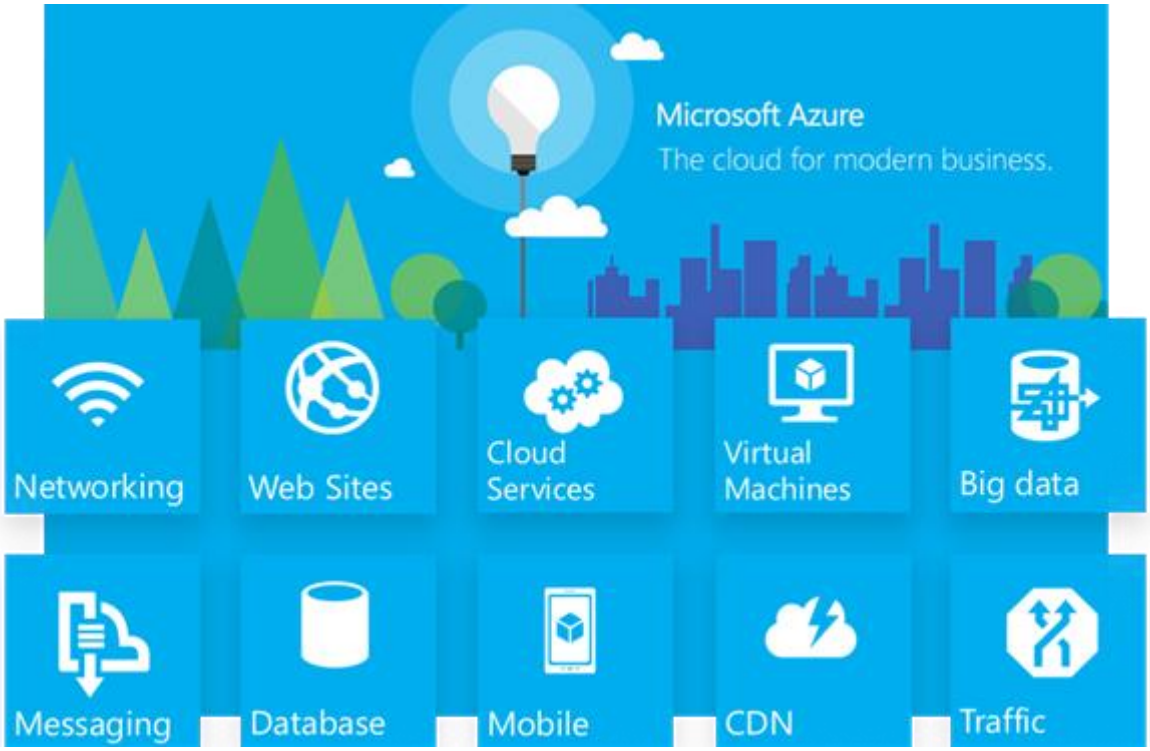

Рисунок 3.3 - Хмарні сервіси Mixrosoft

Що стосується послуг для забезпечення неперервності бізнес-процесів до розгляду будуть обрані послуги: Azure Storage, Windows Virtual Desktop, Azure Site Recovery/ Azure Backup.

Українська компанія De Nowo на ринку хмарних технологій вже більше 12 років. Компанія надає послуги IaaS та HPI((Hosted Private Infrastructure) приватни хмара як сервіс). Перший в Україні сертифікований провайдер. Для забезпечення неперервності бізнес-процесів компанія пропонує: De Nowo DRaaS/ De Nowo Backup.

Ucloud це українська компанія, яка надає хмарні послуги з 2011року. Компанія пропонує послуги інфраструктура як сервіс. На українському ринку Ucloud має восьмирічний досвід. Провайдер є партнером компанії Microsoft. Для забезпечення неперервності бізнес-процесів компанія пропонує: Ucloud DRaaS, Citrix Workspace.

3.4 Порівняльний аналіз хмарних провайдерів за послугами.

Для вибору хмарного провайдера та хмарних сервісів у таблиці наведена характеристика двох Українських та двох міжнародних компаній.

Таблиця 3.2 Порівняння хмарних провайдерів та сервісів

Назва компанії	Google	Microsoft	De Nowo	Ucloud
Країна походження	Америка	Америка	Україна	Україна
Розміщення ЦОД	США, Західна Європа, Східна Азія	Україна та ще 60 інших країнах	Україна, Німеччина.	Україна, Польща, Німечина
Сертифікація	ISO/IEC 27001	ISO/IEC 27001:2013	ISO/IEC 27001:2013	ISO/IEC 27001:2013
Рівень надійності (SLA)	99.99%	99.99%	99,95%	99,95%
Тестувальний період	90 днів (300 USD на рахунку)	30днів (200 USD на рахунку)	-	30 днів
Сервіс	Копіювання та відновлення			
Назва Послуги	Google Cloud DRaas	Azure Site Recovery/ Azure Backup.	De Nowo DRaaS/ De Nowo Backup	Ucloud DRaaS
Які послуги забезпечують	DRaas	DRaaS/BaaS	DRaaS/BaaS	DRaaS
Скрвіс	Робочий стіл як послуга			
Назва послуги	Google Workspace	Windows Virtual Desktop	-	Citrix Workspace

Ціна послуги	12 USD/місяць 1 користувач	14 USD/місяць 1 користувач		6 USD/місяць 1 користувач

Продовження таблиці 3.2

Назва компанії	Google	Microsoft	De Nowo	Ucloud
Сервіс	Сховище як послуга			
Назва послуги	Google Storage	Azure Storage	Enterprise Cloud Storage De Novo	Ucloud Storage
Ціна послуги	1TB 8,5 USD/міс	1TB 15USD/міс	1TB 7 USD/міс	1 TB 6USD/місяць

Аналізуючи дані наведені в таблиці можна сказати, що для забезпечення неперервності бізнес-процесів серед українських постачальників варто використовувати сервіс Ucloud. Оскільки ця компанія забезпечує надання таких важливих сервісів як DRaaS, також надає послуги DaaS. Компанія є партнером корпорації Microsoft, тому широких спектр сервісів цієї компанії доступний для Ucloud. Оскільки компанія українська то вартість її послуг є нижчою ніж у іноземних компаній. Вона є сертифікованою та рівень надійності SLA складає 99,95%. Центри обробки даних знаходяться не лише в Україні але і поза її межами. Компанія надає пробний безкоштовнй період для тестування свої сервісів, що є великою перевагою від інших постачальників. Перевагою українських провайдерів для української компанії є те, що вони мають мережеву близькість до українських компаній, що в свою чергу забезпечує високу швидкість та безпеку мережевого каналу

Що стосується іноземних компаній, то для малого бізнесу найкраще підійдуть сервіси які надає Google Cloud Platform. Тому, що компанія має світове ім'я та сформовану репутацію, та користується популярністю між

багатьма компаніями світу. Вона сертифікована, рівень надійності SLA складає 99,99%. Вартість її послуг є нижчою в порівнянні іншої іноземної компанії Microsoft. Ткаож компанія Google надає пробний період для тестування її сервісів та деякі сервіси безплатно (Google Drive до 5 ГБ, Gmail).

При виборі хмарних сервісів варто пам'ятати про те що обравши послуги іноземних провайдерів, час переказу коштів на рахунки іноземного провайдера, буде відрізнятися від вітчизняного. Оплата послуг буде тривати довше, а за несвоєчасну оплату надання послуг буде припинятися і це може нанести шкоди бізнесу. Також, вартість послуги яку надає іноземний провайдер прив'язується до курсу долара.

Тому при виборі між українським та іноземним хмарним сервісом варто надавати перевагу українським.

3.5 Рекомендації щодо вибору хмарного сервісу, постачальника та покращення рівня безпеки хмарних сервісів для компанії Хмарні провайдери

Вибираючи хмарну інфраструктуру для компанії “Яреш” рекомендується розгортати гібридну хмару. Компанія може дозволити розгорнути гібридну модель, так як має у власності сервера, використання гібридної хмари підвищить рівень безпеки компанії. Організація зможе такі важливі дані, як клієнтська база, фінансові звіти, дебіторська заборгованість зберігати на власному сервері. А не критичні дані, наприклад, роздрібні прайси на хмарі. Важливою перевагою використання гібридної хмари є те, що вона може розгортатися на серверах клієнта, що дає клієнту можливість фізичного доступу до сервера. Також можна використовувати деякі безкоштовні хмарні сервіси різних провайдерів разом з необхідними платними. Наприклад, використовувати послуги DRaaS для забезпечення неперервності бізнес-процесів, компанії Ucloud, та додатково для сховища деяких даних використовувати Google Docs, Nextcloud. В такому випадку компанія може

комбінувати патні послуги (DRaaS,BaaS), разом з безкоштовними Cloud Storage.

Для покращення захисту даних компанії рекомендується шифрувати дані за допомогою програм, перед тим як відправити їх на хмару , використовувати сервіси які забезпечують безпеку інформації, дотримуватися рекомендацій наведених у розділі 2. щодо захисту від загроз та атак. Вся інформація повинна передаватися по зашифрованих каналах зв'язку, а ключі шифрування повинні зберігатися тільки в клієнтів яким належить ця інформація. Для безпечної аутентифікації використовувати надійний пароль, який не менше ніж 1 раз в місяць потрібно змінювати і не зберігати його на паперових та електронних носіях з яких можна було б викрасти його.

Для захисту даних компанії потрібно прописати політику безпеки хмари. Для початку потрібно провести оцінку засобів керування безпекою постачальника хмарних послуг, так як у різних провайдерів різні рівні контролю безпеки. В ПБ необхідно вказати чіткі ролі для працівників компанії та відповідно до них встановити доступ до програм та даних., та встановити чіткі правила, що стосуються зв’язків із хмарою(рівні захищених сокетів (SSL), сканування мережевого трафіку та правила моніторингу), щоб уникнути порушення даних які може завдати зараження кінцевої точки хмари. Також потрібно задокументувати правила безпеки для внутрішнього та зовнішнього сховищ даних. Щоб запобігти втраті даних (DLP) та забезпечити шифруватии, потрібно використовувати API. У ПБ компанії, також потрібно прописати шляхи для команд для усунення порушень даних, окреслити процеси звітування та визначте криміналістичні функції. Цей крок допомагає, якщо встановлюються протоколи для аварійного відновлення. Ще для забезпечення безпеки необхідно проводити регулярні огляди та модернізувати компоненти, щоб не відставати від останніх загроз та виконувати планові перевірки SLA постачальника.

РОЗДІЛ 4. Охорона праці та безпека в надзвичайних ситуаціях

4.1 Охорона праці

На сьогоднішній більшість процесів стають автоматизованими. Практично всі організації у своїй роботі використовують комп'ютерні технології. А для компаній які хочуть застосовувати хмарні технології, для ведення бізнес-процесів, використання ЕОМ є невід'ємною для них складовою. Через те, що вся робота з використанням хмарних обчислень виконується робітникоми за допомогою комп’ютера, законодавством України є чіткі врегульовані норми та вимоги , щодо використання комп’ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп’ютером. Охорона праці це важлива частина будь-якого робочого процесу. В якій прописуються основні системи правил та заходів, для забезпечення збереження здоров'я і працездатності людини в процесі праці. Основне визначення охорони праці описується у статті 1 Закону України «Про охорону праці» від 14 жовтня 1992 року. Основні положення про охорону праці в Україні визначаються законодавчими актами.

Оскільки, робоче місце працівників в IT сфері це переважно комп'ютер з робочим столом, то роботодавець повинен забезпечити працівнику робоче місце так, щоб воно було добре пристосоване для трудової діяльності робітника, правильно та доцільно організоване, відносно простору, форми та розміру для забезпечення йому зручного положення при роботі і для високої продуктивність праці при найменшій фізичній і психічній напрузі. Але при правильній організації робочого місця продуктивність праці зростає з 8 до 20 відсотків.

Згідно охорони праці роботодавці повинні забезпечити дотримання державних санітарних правил та норм роботи. В контексті дипломного проекту до уваги береться забезпечення санітарно гігієнічних вимог при використанні електронно-обчислювальних машин колективного та

персонального використання (ЕОМ та ПЕОМ). Зокрема врахування санітарних норм освітлення, звукового шуму, вимог до температури, відносної вологості, вогнестійкості приміщення,та характеристик електромагнітних, інфрачервоних, та ультрафіолетових полів. Всі ці показники зазаначаються в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98. У пункті 2 цього документу описуються норми щодо розміщення, площі, освітлення робочого місця, а також вимоги до самого приміщення.

Згідно цих норм та правил забороняється встановлювати та відповідно використовувати комп’ютери в приміщеннях, які розташовуються у підвалах будинків. Для того, щоб уникнути можливих аварій та замикань. поряд з приміщеннями, де вестиметься робота з комп’ютером. Також забороняється, в приміщеннях де використовується комп'ютерна техніка, проведення робіт, які здійснення потребують надмірно вологих технологічних процесів. У відповідному приміщенні мають облаштовуватися системами опалення (центрального або індивідуального), також системами кондиціонування чи вентиляції повітря. Але всі ці системи та їхні комунікації повинні бути сховані під захисними щитками, для зменшення ризиків можливому потраплянню робітника під напругу. Також площа для одного робочого місця має становити не менше ніж 6,0 кв. м, а об'єм не менше ніж 20,0 куб. м. Конструкція робочого місця повина відповідати ДСТУ 8604:2015, а саме робоче місце для виконання робіт в положенні сидячи організовується відповідно до ДСТУ 8604:2015.

На умови праці великий вплив справляє мікроклімат, шум та освітлення. Основний принцип нормування мікроклімату - створення оптимальних умов для теплообміну тіла людини з довкіллям. У санітарних нормах СН- 245/71 встановлені величини параметрів мікроклімату (які залежать від пори року, характеру трудового процесу і характеру виробничого приміщення), що створюють комфортні умови.

Що стосується рівня шуму, то в нормативно правових актах також зазначається, що виробничі приміщення не повинні межувати з такими

приміщеннями, як виробничі цехи, майстерні тощо, оскільки рівні шуму і вібрації в таких приміщеннях перевищують допустимі значення за НАОП 3044-84. СН 3044-84 (ДНАОП 0.03-3.12-84). Оскільки відомо, що сильний тривалий шум може стати причиною функціональних змін серцево-судинної і нервової систем. Для захисту від шуму застосовують методи передбачені будівельними нормами і правилами (ДБН В.1.1-31:2013) . А для захисту від шуму (комп'ютеру, принтеру, вентиляційного устаткування) на робочому місці доситатньо використовувати звукопоглинання (властивість акустично оброблених поверхонь зменшувати інтенсивність відбитих ними хвиль за рахунок перетворення звукової енергії в теплову).

Всі комп'ютерні робочі місця за якими працюють робітники повинні мати природного та штучного освітлення. На вікна слід встановити регульовані пристрої (жалюзі, завіски, зовнішні козирки). Коефіцієнт природного освітленості в приміщенні (КПО) повинен бути не нижче ніж 1,5%. Також повинно відбуватися щоденне проведення вологого прибирання.

Для досягнення максимального рівня безпечності та охорони праці при роботі з комп'ютером, у виробничих приміщеннях необхідна наявність аптечок першої медичної допомоги, систем автоматичної пожежної сигналізації і вогнегасників. Для приміщень у яких працюють 5 або більше комп’ютерів разом, на видимому місці необхідно встановити службовий вимикач, який у разі потреби дозволить повністю відключити електричне живлення кімнати.

4.2 Безпека в надзвичайних ситуаціях

Термін “надзвичайна ситуація (НС)” означає, що коли відбуваються порушення нормальних умов життєдіяльності людини на територіях і об'єктах, спричинених небезпечною подією (катастрофою, епідемією, виликою пожежею, стихійним лихом, та ін.), яка призводить або може призвести до людських та матеріальних втрат, то така ситуація називається надзвичайною. За походженням НС поділяють на природні та антропогенні. Найбільш

поширеним видом надзвичайних ситуацій при експлуатації електронно обчислювальних машин є пожежа в приміщеннях та будівлях. В Україні загальні економічні, загально правові та соціальні основи для забезпечення пожежної безпеки, визначаються законом України «Про пожежну безпеку». Також цим законом регулюються відносини юридичних та фізичних осіб, державних органів. Поняття "пожежна безпека" означає такий стан об'єкта, при якому з регульованою імовірністю виключають можливість винекнення та розвиток пожежі а ще її впливу на людей, та її небезпечних факторів; а також забезпечення захисту матеріальних цінностей. Всі будівлі та приміщення, у яких експлуатують ВДТ і ЕОМ підпадають під категорію з вибухопожежної та пожежної безпеки згідно з НАПБ Б.03.002-2007. "Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою (32980)" від 03.12.2007, НАПБ В.01.053-2016/520 "Правила пожежної безпеки в галузі зв`язку" від 31.05.2016 та клас вибухонебезпепечних зон відповідно до НПАОП 0.00-1.32-01 «Правила будови електроустановок. Електрообладнання спеціальних установок» від 21.06.2001. Згідно цих документів необхідно наносити відповідні позначення на вхідні двері приміщення. Також, приміщення в яких знаходяться ВДТ, ЕОМ повинні оснащуватись системами пожежної сигналізації з димовими пожежними сповіщувачами, а також ручними CO2 вогнегасниками. Кількість вуглекислотних вогнегасників розраховується як 2 од. на кожні 20 м2 площі приміщення. Пожежна сигналізація потрібна для швидкого сповіщення про пожежу, за допомогою засобів світлового та звукового сповіщення. А також вона забезпечує автоматичне включення установок пожежегасіння й димовбирачів. Засоби пожежогасіння повинні знаходитись у вільно доступних місцях. Причинами виненекнення пожежі може бути вибух на підприємстві. Такий вибух, наприклад, можуть спричинити порушення правил і норм пожежної безпеки або нехтування Законом «Про пожежну безпеку» тощо. Ліквідувати пожежу силами персоналу можна на початковій стадії її розвитку за допомогою спеціальних засобів пожежогасіння. Пожежогасіння це такий

комплекс заходів, який спрямовується на усунення причин виникнення пожежі, а також створює умови, при яких подальше горіння буде неможливим. До засобів пожежогасіння відносять вогнегасники (у випадку гасіння електронних пристроїв використовують до 1000вт.- порошкові вогнегасники, до 10 000вт(10 кВт) вуглекислоті вогнегасники), пожежний інвентар, системи автоматичного пожежогасіння. Ці засоби, в залежності від категорії приміщень, можна розташовувати окремо, або в складі пожежних щитів. В залежності від їхнього агрегатного стану та особливості горіння різних горючих речовин і матеріалів пожежі за ДБН В.1.1-7:2016 “Пожежна безпека об`єктів будівництва. Загальні вимоги” від 01.06.2017 поділяються на відповідні класи. Основні способи гасіння пожежі засновуються на принципах зниження температури горючих речовин до рівня нижче температури її горіння, зупинки доступу парів і газів горючої речовини, та зниження концентрації кисню повітря в зоні горіння до 14 - 15%. Для забезпечення пожежної безпеки в організації необхідно проводити пожежну профілактику. Профілактичні заходи протипожежної безпеки включають в себе комплекс організаційних і технічних заходів, які спрямовуються для забезпечення безпеки людей, для запобігання пожежі та обмеження її поширення, для створення умов для успішного гасіння пожежі. Державна служба України з надзвичайних ситуацій завжди моніторить дотримання норм протипожежної безпеки. Цей моніторинг включає в себе контролювання навчання персоналу який відповідає за запобігання загоряння та усуненню наслідків пожежі, регулярну перевірку об'єктів нерухомості. Також в цей моніторинг входить розроблення, впровадження та контроль технічних способів забезпечення безпеки. Варто зазначити, що вся відповідальність за забезпечення пожежної безпеки підприємств, установ та організацій покладається на їх керівників і уповноважених ними осіб, окрім моментів які не передбачаються відповідним договором.

ВИСНОВКИ

Хмарні технології вже досить давно стали частиною нашого життя, Багато людей, не знають що вони користуються хмарними сервісами. Наприклад перевіряючи свою пошту, людина вже використовує хмарний сервіс. Завдяки своїм характеристикам, хмарні технології значно полегшують життя, бізнесу. Найбільшу свою популярність вони здобули серед малого та середнього бізнесу. Хмарні обчислення забезпечують це найцінніші критерії для бізнесу, такі як швидке реагування на потреби та зміну ринку, адаптацію та швидкий вихід бізнес продуктів. Хмарні технології представляють собою один з сучасних засобів для забезпечення неперервності бізнес-процесів, швидкого нарощення та масштабування бізнесу, що в свою чергу, сприяє швидкій окупності інвестицій, ефективного перерозподілу ресурсів, та економічного підйому.

В першому розділі кваліфікаційної роботи були описані характеристики та моделі хмарних послуг. Наведені переваги щодо застосування хмарних сервісів, такі як, швидке розгортання, гнучкість, мобільність, цілодобовий доступ та недоліки основним з яких є забезпечення безпеки в хмарних сервісах. Також у цьому розділі описується історія та ключові факти у розвитку хмарних технологій.

У другому розділі роботи, були проаналізовані можливі атаки та загрози хмарних обчислень (найбільшу загрозу становлять інсайдерські атаки), а також наведені способи їх усунення. Також у другому розділі описується вплив пандемії на хмарні технології та піднімається питання безпеки хмарних сервісів в цілому.

У третьому розділі вирішуються поставлені питання та завдання для дипломного проекту. А саме вибір хмарних сервісів для забезпечення неперервності бізнес- процесів компанії. Порівняння українських та іноземних

провайдерів які надають хмарні сервіси. Також були надані рекомендації, щодо підвищення рівня безпеки компанії яка використовує хмарні обчислення.

На основі проведеного дослідження можна сказати, що для обраної організації “Яреш” згідно з її потребами, для забезпечення неперервності бізнес-процесів, варто використовувати такі хмарні сервіси, як DRaaS/BaaS (Аварійне відновлення та копіювання/ Копіювання та відновлення), Daas (робочий стіл як сервіс, для зручної роботи віддалено (забезпечуючи непеерерність)), STaaS (сервіс сховища). Серед постачальників варто надавати перевагу українським, зокрема (Ucloud) та розгортати гібридну хмарну інфраструктуру для забезпечення вищого рівня захисту. Що стосується рекомендацій, в 3 розділі було запропоновано різні варіанти захисту (шифрування даних перед відправкою в мережу та на хмару, використання надіцних паролів, створення політики безпеки, дотримання всіх заходів щодо пом'якшення атак та загроз.

У четвертому розділі наводяться санітарні норми праці, та описується безпека при надзвичайні ситуації яка може виникнути. У цьому розділі розглянута безпека при виникненні пожежі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. N. Zagorodna, I. Kramar Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty & Co., Ashok Rajpath,. 446 p.

2. О.Кареліна, В.Дудикевич «Класифікація методів визначення захищеності інформаційних систем» VII науково-технічна конференція "Інформаційні моделі, системи та технології" Тернопільського національного технічного університету імені Івана Пулюя.- 12.2019р/

3. О.Карнаухов, Т.Лобур, М.Митник «Підвищення ефективності роботи центрів обробки даних засобами віртуалізації» Тернопільський національний технічний університет ім. Івана Пулюя.2011р

4. I. Strutynska, H.Kozbur, L.Dmytrotsa, I.Bodnarchuk, O.Hlado «Small and Medium Business Structures Clustering Method Based on Their Digital Maturity» 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T) 278-282pp/ 08.10.2019

5. V.Martsenyuk, Z.Mayhruk, M.Karpinski, N. Milian, I.Andrushchak, O.Veselskawe “ On implementation of decision tree induction in cloud platforms” 2019 Advances in Science and Engineering Technology International Conferences (ASET)/ IEEE/1-6pp/26.03.2019р

6.A history of cloud computing [Електронний ресурс] // Режим доступу: http://www.computerweekly.com/feature/A-history-of-cloud-computing

7. Douglas F. Parkhill. The Challenge of the Computer Utility. - Addison-Wesley Publishing Company, 1966 –246pp.

8. «The NIST Definition of Cloud Computing». [Електронний ресурс]:Режим доступу: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 145

9. A.Javaid. “Top Threats to Cloud Computing Security”. SSRN Electronic Journal January 2013.10p

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

10 Программное обеспечение как услуга. [Електронний ресурс]:Режим доступу: https://datapark.com.ua/ua/services/cloud/platforms-as-a-service-paas/

12 P.Mell and T.Grance.: “C O M P U T E R S E C U R I T Y” Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, September 2011. 7p.

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

14 Недашківський О.Л Сучасний захист інформації “ХМАРНІ ТЕХНОЛОГІЇ ТИПУ «IaaS» ЯК ЗАСІБ ОПТИМІЗАЦІЇ ПОТОКІВ ІНФОРМАЦІЇ В МЕРЕЖАХ ПЕРЕДАЧІ ТА ОБРОБКИ ДАНИХ” 2017

15 А. А. Каменщиков “ОБЛАЧНЫЕ ТЕХНОЛОГИИ И ИНТЕРОПЕРАБЕЛЬНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ В ЗДРАВООХРАНЕНИИ” Институт радиотехники и электроники им. В.А. Котельникова РАН 19 февраля 2013 г.

16 “2020 Cloud Misconfigurations Report”.Divvycloud/02.2020/15p

17 Lewis J. (2018). Economic Impact Of Cybercrime, No Slowing Down. Report supported by McAFee and CSIS, 28p.

18 G.Stevens. “Cloud Security: 5 Serious Emerging Cloud Computing Threats to Avoid”/-May 26, 2020

19 Е.Куликов “Что стимулирует спрос на облачные сервисы информационной безопасности?” КО IT для бизнеса - 2 червня 2020р.

21 N.Amara, H. Zhiqui, A.Ali//IEEE Cloud Computing Security Threats and Attacks with Their Mitigation Techniques-2017

22 Rev.B «Cloud Computing-ENISA-Benefits» risks, and recommendations for information security," ENISA. – December 2012

23. “6 insecure apis application programming interfaces”[Електронний ресурс]:Режим доступу:https://www.coursehero.com/file/p7ql64lm/6-Insecure-APIs-Application-Programming-Interfaces-API-give-users-the/

24 J.Vijaya “Authentication and Authorization Mechanism for Cloud Security”. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019

25 Douligeris C, Mitrokotsa A. DDoS attacks and de-fense mechanisms: classification and state-of-the-art.Computer Networks 2004; 44(5): 643–666.

26. Singh S. Cloud computing attacks: a discussion with solutions. Open Journal Of Mobile Computing AndCloud Computing 2014

27 Misconfigured Cloud Services Pose High Security Risks for Organizations/ Virtualization & Cloud - 27 червня 2018 https://www.researchgate.net/figure/The-Inside-and-Outside-attack_fig7_266885027

28 Shaw, E., Ruby, K., Post, J.: The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin 2, 1–10 (1988)

29 S.Choudhary, G.Pundir, Y.Singh “Detection and Isolation of Zombie Attack under Cloud Computing” International Research Journal of Engineering and Technology (IRJET)/- Jan 2020

30 Y. Hebbal, S. Laniepce, and J.-M. Menaud, “Virtual machine intro-spection: Techniques and applications,” in 2015 10th InternationalConference on Availability, Reliability and Security. IEEE, 2015, pp.676–685.

31 Y. Y. D. W. Anyi Liu, "SQLProb: A Proxy-based Architecture towards Preventing," in Proceedings of the 2009 ACM Symposium on Applied Computing, 2009 Schultz, E.: A framework for understanding and predicting insider attacks. Computers & Security 21(6), 526–531

32 Xuan S, Yang W, Dong H, Zhang J. Performance evaluation model for application layer firewalls. PLoS One.

33 Ian MuscatW “hat Are Injection Attacks?” Security Zone - Apr. 26,2017

34 Types of Injection attacks [Електронний ресурс] //Режим доступу: https://www.ibm.com/support/knowledgecenter/en/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_injection_attacks.htm

35 B.Plankers “What is VM Escape?” The lone sysadmin rounding technology outlaws up sine 2005.- September 22, 2007

36 Griffin “Virtual Machines: Virtualization vs. Emulation” Generalh.- August 16, 2006

37 Bunkar RK, Rai PK. Study on security model in cloud computing. International Journal of Advanced Research in Computer Science.

38 Injection attacks [Електронний ресурс] //Режим доступу: https://www.researchgate.net/publication/336793622_EECDH_to_prevent_MITM_attack_in_cloud_computing

39 D.Swinhoe "What is a man-in-the-middle attack? How MitM attacks work and how to prevent them"/CSO-FEB 13, 2019

40 Habiba UM. Cloud identity management security issues & solutions: A taxonomy. Complex Adaptive Systems Modeling. 2014:1-37

41.Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk-Based Criticality Analysis. In: Palmer, C., Shenoi, S. (eds.) Critical Infrastructure Protection III. IFIP AICT, vol. 311, pp. 35–49.

42 "What is a backdoor?" [Електронний ресурс] //Режим доступу: https://www.malwarebytes.com/backdoor/

43 "Backdoor Attack" [Електронний ресурс] //Режим доступу: https://www.imperva.com/learn/application-security/backdoor-shell-attack/

44. I.Dacosta, S.Chakradeo, M.Ahamad, P.Traynor "One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens" Attacks with Stateless Authentication Tokens. ACM Transactions on Internet Technology 12(1) - June 2012

45 N. Roshanbin and J. Miller, "A survey and analysis of current CAPTCHA approaches," Journal of Web Engineering, vol. 12, no. 1-2, pp.

46.What is DRaaS and why is it useful [Електронний ресурс] //Режим доступу: https://www.rackwareinc.com/draas

47 What is BaaS? Backend-as-a-service-vs serverless [Електронний ресурс] //Режим доступу: https://www.cloudflare.com/learning/serverless/glossary/backend-as-a-service-baas/

48 Baas vs draas 3 key differences know [Електронний ресурс]//Режим доступу: https://intervision.com/baas-vs-draas-3-key-differences-know/

49. Desktop as a service [Електронний ресурс]//Режим доступу: https://itglobal.com/ru-ru/company/glossary/desktop-as-a-service/

50. Сервис Storage as a Service(STaaS)[Електронний ресурс] // Режим доступу: https://cloud.softline.ru/manual-staas/

ДОДАТКИ

Додаток А.

Узагальнена таблиця загроз та методів їх запобігання

Загрози безпеці	Ураження хмарного сервісу	Методи пом'якшення наслідків (попередження наслідків)
Втрата даних	IaaS, PaaS, SaaS	• Регулярні резервні копії. • Використання правильних методів шифрування. • Захист даних під час передачі. • Впровадження надійної генерації, зберігання та управління ключами. • Юридично вказані методи посилення та підтримки технічного обслуговування постачальника.
Порушення цілісності даних	IaaS, PaaS, SaaS	• Захист даних під час передачі. • Використання правильних методів шифрування. • Для захисту даних їх слід аналізувати як під час проектування, так і під час виконання. • Впровадження надійної генерації, зберігання та управління ключами. • Юридичне затвердження, про те що постачальник повинен витирати стійкі носії до того, як їх випустять у пул. • Юридичне затвердження стратегії резервного копіювання та відновлення. • Реалізація надійних інтерфейсів пртикладного програмування (API).
Викрадення облікового запису чи послуги	IaaS, PaaS, SaaS	•Правильне розуміння політики безпеки та угоди про рівень обслуговування (SLA). • Використання багатофакторних методів аутентифікації. • Суворий моніторинг для виявлення несанкціонованих дій. • Унеможливити обмін обліковими даними між споживачами та послугами.

Продовження Додатоку А

Загрози безпеці	Ураження хмарного сервісу	Методи пом'якшення наслідків (попередження наслідків)
Небезпечні інтерфейси та API	IaaS, PaaS, SaaS	• Надійні механізми аутентифікації та контролю доступу. • Використання шифрування для передачі даних. • Аналіз інтерфейсів хмарного провайдера. • Правильне розуміння ланцюжка залежностей, пов'язаних з API.
Шкідливі інсайдери	IaaS, PaaS, SaaS	• Зробити управління людськими ресурсами частиною юридичної домовленості. • Суворе застосування процедури управління ланцюгами поставок. • Надання належної ясності безпеці та адміністративному процесу.
Недостатня перевірка	IaaS, PaaS, SaaS	• Використання галузевих стандартів для впровадження хмарних додатків та послуг. • Оцінка ризику за допомогою якісних та кількісних методів. • Розкриття відповідних журналів, даних та деталей інфраструктури.
Зловживання хмарними послугами	IaaS, PaaS	• Використання надійної авторизації та автентифікації. • Правильний аудит мережевого трафіку. • Покращений моніторинг кредитних карток.

Продовження Додатоку А

Загрози безпеці	Ураження хмарного сервісу	Методи пом'якшення наслідків (попередження наслідків)
Спільні технологічні проблеми	IaaS	• Використання кращих механізмів автентифікації та контролю доступу. • Перевірка вразливостей та конфігурації. • Моніторинг середовища на предмет несанкціонованих змін / діяльності. • Використання SLA для виправлення та усунення вразливостей.
Невідомий профіль ризику	IaaS, PaaS, SaaS	• Розкриття відповідних журналів, даних та деталей інфраструктури. • Аудиторська система оповіщення про порушення даних
Крадіжки особистих даних	IaaS, PaaS, SaaS	• Надійний пароль, механізми аутентифікації та контролю доступу
Зміни в бізнес-моделі	IaaS, PaaS, SaaS	• Забезпечення системи контролю та моніторингу пропонованих послуг.
Умова блокування	IaaS, PaaS, SaaS	• Моніторинг через систему виявлення інструкцій (IDS), вторгнень в систему запобігання (IPS) та впровадження брандмауера.

Додаток Б.

Узагальнена таблиця атак та методів їх запобіганню

Атака	Рівень безпеки	Методи захисту
SQL Injection	Базовий рівень/ програмний рівень	• Уникикання використання динамічно генерування SQL у коді. • Використання відповідних фільтрацій, для очищення введених користувачем даних. • Використання архітектури на основі проксі-сервера для динамічного виявлення та вилучення введених даних користувача.
Атаки міжсайтових сценаріїв (XSS)	Базовий рівень/ програмний рівень	• Використання фільтрації активного вмісту. • Використання браузерної співпраці. • Використання технології запобігання витоку даних на основі вмісту. • Використання технології виявлення вразливостей веб-додатків. • Підхід на основі проекту для мінімізації залежності від Інтернету браузер. • Правильна конфігурація захищеного шару сокету (SSL). • Використання антивірусного програмного забезпечення.
Фішингова атака	Базовий рівень	• Виявлення спаму.
DNS-атаки	Мережевий рівень	• Використання заходів безпеки DNS, наприклад розширення системи безпеки доменних імен (DNSSEC)
MITM Attacks (людина по середині)	Базовий рівень	• Правильна конфігурація захищеного шару сокету (SSL). • Використання інструментів шифрування, напр. Dsniff, Ettercap, Wsniff, Airjack тощо.
DOS/DDOS Attacks	Програмний рівень	• Використання кращих схем автентифікації та авторизації. • Використання системи виявлення вторгнень (IDS) / системи запобігання проникненню (IPS)

Продовження Додатку Б

Атака	Рівень безпеки	Методи захисту
Повторного використаня IP-адреса	Мережевий рівень	• Використання кращих схем автентифікації та авторизації. • Використання системи виявлення вторгнень (IDS) / системи запобігання проникненню (IPS)
Zombie Attacks	Мережевий рівень ВМ рівень	• Використання кращих схем автентифікації та авторизації. • Використання системи виявлення вторгнень (IDS) / системи запобігання проникненню (IPS)
Sniffer Attacks	Мережевий рівень	• Використання техніки розпізнавання знімків на основі протоколу розрішення адрес (ARP). • Використання техніки розпізнавання знімків, заснованої на часу зворотного проїзду (RTT).
Wrapping Attacks	Програмний рівень	• Використання належного механізму підпису. • Використання належної конфігурації захищеного сокетного рівня (SSL).
Cookie Poisoning	Програмний рівень	• Впровадження кращих схем шифрування. • Регулярне очищення даних cookie. • Використання політики безпеки браузера. • Використання інші механізми автентифікації перед створенням сеансів
CAPTCHA Breaking	Програмний рівень	• Збільшення довжини рядка. • Використання пертурбативного фону. • Використання накладання літер, щоб уникнути атак вертикальної сегментації. • Використання різних розмірів шрифту.
Хакерські атаки Google	Програмний рівень	• Використання стандартних заходів безпеки для Інтернет вразливостей. • Використання кращих схем автентифікації та авторизації. • Впровадження політики резервного копіювання, щоб уникнути проблем із відновленням даних, наприклад Постійний захист даних (CDP).

Додаток В

УДК 004.056.5

М.М. Фершлядин – гр. СБмз-61.
(Тернопільський національний технічний університет імені Івана Пулюя)

БЕЗПЕКА ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У БІЗНЕС ПРОЦЕСАХ

UDC 004.056.5

M. Fershliadyn

SECURITY OF CLOUD TECHNOLOGIES USAGE IN BUSINESS PROCESSES

В сучасному світі хмарні технології відіграють одну з важливих ролей для бізнесу. Вони допомагають забезпечити неперервність бізнес-процесів. За допомогою хмар організації можуть значно скоротити витрати на побудову центрів обробки даних, розробку мереж передачі даних, вирішення проблем безпеки забезпечення надійності, доступності та захищеності інформації, оскільки ці витрати поглинаються провайдером хмарних послуг, а компанія сплачує лише за оренду необхідних ресурсів,. За допомогою хмарних технологій забезпечується швидка можливість реагування на збільшення попиту на обчислювальні потужності інформаційних мереж та систем. [1]

Згідно з документом IEEE1 [2], який був опублікований у 2008 році, термін "Хмарні обчислення" висвітлюється, як парадигма, в рамках якої дані у мережі постійно зберігаються на серверах і тимчасово кешуються на клієнтській стороні (ноутбуках, смартфонах, персональних комп'ютерах). Хмари бувають 4 типів: публічні, приватні, громадські(спільні) та гібридні. Вони у свою чергу дають можливість обрати потрібну модель для забезпечення необхідних процесів.

У звіті [3], представленому Центром дослідження економіки і бізнесу (CEBR) йдеться про те, що економіка європейських країн буде отримувати додатково 177,3 млрд. євро щорічно завдяки хмарним обчисленням. Під час свого дослідження CEBR підсумував, що використання хмарних обчислень стане важливим фактором економічного росту, конкурентоспроможності і створення нових підприємств.

Отже, хмарні обчислення – це один з основних сучасних засобів для забезпечення максимальної ефективності ведення бізнесу, які допомагають компаніям нарощувати свою перевагу, досягати значної економії витрат, що, в свою чергу, сприяє швидкій окупності інвестицій і ефективного перерозподілу ресурсів та економічному підйому підприємства.

Але хмарні обчислення, як і всі технології, мають також свої мінуси. Основним значним недоліком у хмарних технологіях є ризики, пов'язані з безпекою. Оскільки, хмарні технології передбачають передачу свої даних для обробки, зберігання, то виникає питання в захищеності цих технологій. Актуальною задачею є аналіз порівняльний аналіз декількох хмарних сервісів на предмет їхньої надійності, безпеки, та конфіденційності даних з метою вибору найкращого для ведення бізнес-процесів.

Література.

1. A history of cloud computing [Електронний ресурс] // Режим доступу: http://www.computerweekly.com/feature/A-history-of-cloud-computing.
2. "IEEE COMPUTER SOCIETY DIGITAL LIBRARY" (англ.). [Електронний ресурс]: Режим доступу: https://www.computer.org/csdl/magazine/ic/2008/05/mic2008050096/13rRUwhpBHv. 3. Centre for Economics and Business Research [Електронний ресурс] // Режим доступу: https://www.cebr.com/.