Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студентки *Павлової Валерії Олександрівни*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення рівня захищеності інформації при роботі з системами хмарних обчислень*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Мацюк С.М.			
розділів:				
спеціальний	к.т.н., доц. Мацюк С.М.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Павловій Валерії Олександрівні* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Підвищення рівня захищеності інформації при роботі з системами хмарних обчислень***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Провести аналіз основних типів та моделей застосування хмарних сервісів та дослідити основні методи забезпечення неперервності бізнесу.	20.10.2022
Розділ 2	Визначити основні загрози систем хмарних обчислень, розробити політику забезпечення неперервності бізнесу центрів обробки даних та сформулювати рекомендації щодо забезпечення їх інформаційної безпеки.	16.11.2022
Розділ 3	Виконати розрахунок вартості проєктування та інтеграції політики у типовому центрі обробки даних, що входить до складу системи хмарних обчислень.	05.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 115 с., 5 рис., 6 табл., 4 додатка, 25 джерел.

Об’єкт дослідження: типовий центр обробки даних.

Мета роботи: розробка рекомендацій забезпечення готовності інформаційно-комунікаційних систем, у яких використовуються хмарні обчислення, до неперервності ведення бізнесу.

У першому розділі проведено аналіз основних типів та моделей застосування хмарних сервісів та досліджено основні методи забезпечення неперервності бізнесу.

У спеціальній частині виявлено основні загрози систем хмарних обчислень, створена політика забезпечення неперервності бізнесу центрів обробки даних та сформульовані рекомендації щодо забезпечення їх інформаційної безпеки.

В економічному розділі проведено розрахунок вартості проєктування та інтеграції політики у типовому центрі обробки даних, що входить до складу системи хмарних обчислень.

Новизна полягає у аналізі загроз та розробці загальних рекомендацій по захисту інформації для інноваційного типу інформаційно-комунікаційних систем хмарних обчислень. Розроблені рекомендації можуть бути застосовані для найбільш поширених видів хмарних сервісів.

ПОЛІТИКА НЕПЕРЕРВНОСТІ ВЕДЕННЯ БІЗНЕСУ, ІНФОРМАЦІЙНА БЕЗПЕКА, ХМАРНІ ОБЧИСЛЕННЯ, ВІДМОВОСТІЙКІСТЬ, ЗАГРОЗА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

Explanatory note: 115 p., 5 pic., 6 tabl., 4 app., 25 sources.

Object of study: a typical data center.

Purpose: to develop recommendations for ensuring the readiness of information and communication systems that use cloud computing for business continuity.

The first section analyzes the main types and models of cloud services and investigates the main methods of ensuring business continuity.

In the special part, the main threats to cloud computing systems are identified, a business continuity policy for data centers is created and recommendations for ensuring their information security are formulated.

The economic section calculates the cost of designing and integrating the policy in a typical data center, which is part of the cloud computing system.

The novelty lies in the analysis of threats and the development of general recommendations for information security for an innovative type of information and communication systems of cloud computing. The developed recommendations can be applied to the most common types of cloud services.

BUSINESS CONTINUITY POLICY, INFORMATION SECURITY, CLOUD COMPUTING, FAULT TOLERANCE, INFORMATION SECURITY THREAT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

БІ – безпека інформації;

ВМ – віртуальна машина;

ГІКТЗНБ – готовність ІКТ до забезпечення неперервності бізнесу;

ЗІ – захист інформації;

ЗТВ – задана точка відновлення;

ЗЧВ – заданий час відновлення;

ІКТ – інформаційно-комунікаційні технології;

ІС – інформаційна система;

ІСХТ – інформаційна система, з використанням хмарних технологій;

ІТ – інформаційні технології;

ММНБ – мінімальна мета забезпечення безперервності бізнесу

МНБ – менеджмент неперервності бізнесу;

НСД – несанкціонований доступ;

ОС – операційна система;

ПЗ – програмне забезпечення;

СЗІ – система захисту інформації;

ТЗІ – технічний захист інформації;

УНБ – управління неперервністю бізнесу;

ЦОД – центр обробки даних;

IaaS – Infrastracture as a service – інфраструктура як послуга;

PaaS – Platform as a service – платформа як послуга;

RAID – надлишковий масив незалежних дисків;

SaaS – Softwareas a service – програмне забезпечення як послуга;

SPOF – single point of failure – єдина точка відмови;

UPS – Uninterruptable Power Supply – джерело безперебійного живлення.

ЗМІСТ

с.

ВСТУП 9
1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 10
1.1 Аналіз хмарних систем 10
1.1.1 Класи хмарних систем 11
1.1.1.1 Закриті комерційні «хмари» 12
1.1.1.2 Платформи для розподілених обчислень 12
1.2 Основні характеристики хмарних сервісів 13
1.2.1 Масштабованість 13
1.2.2 Еластичність 13
1.2.3 Мультітенантність 14
1.3 Аналіз особливостей системам хмарних обчислень 14
1.3.1 Переваги хмарних систем 14
1.3.2 Види хмарних сервісів 17
1.3.2.1 Інфраструктура як сервіс (IaaS) 17
1.3.2.2 Платформа як сервіс (PaaS) 18
1.3.2.3 Програмне забезпечення як сервіс (SaaS) 20
1.3.3 Компоненти системи хмарних обчислень 22
1.3.3.1 Апаратні компоненти центру обробки даних 22
1.3.3.2 Телекомунікаційна складова доступу до ресурсів 22
1.3.3.3 Користувачі та їх програмно-апаратне забезпечення 23
1.3.3.4 Середня (middleware) частина центру обробки даних 23
1.3.3.5 Прикладні сервіси 24
1.3.4 Загальні вимоги до безпеки хмарних обчислень 24
1.3.5 Джерела загроз в системах хмарних обчислень 29
1.4 Центри обробки даних сервісів розподілених обчислень 31
1.4.1 Забезпечення відмовостійкості ЦОД 33
1.4.1.1 Резервні оглядові люки і зовнішні кабельні канали 33

1.4.1.2 Резервні сервіси провайдерів доступу 34
1.4.1.3 Резервування кімнат введення 35
1.4.1.4 Резервна головна розподільна зона 35
1.4.1.5 Резервна магістральна розводка 36
1.4.1.6 Резервна горизонтальна розводка 36
1.5 Вразливості хмарних систем 37
1.6 Загальні відомості про захист даних при їх обробці хмарними сервісами 39
1.7 Управління неперервністю бізнесу 42
1.8 Висновок. Постановка задачі 53
2 СПЕЦІАЛЬНА ЧАСТИНА 55
2.1 Вимоги до ГІКТЗНБ в менеджменті неперервності бізнесу 56
2.2 Аналіз сценаріїв відмови компонентів системи 67
2.3 Характеристика об'єкта інформаційної діяльності 70
2.4 Політика забезпечення неперервності бізнесу центрів обробки даних провайдера хмарних обчислень 71
2.4.1 Призначення документа 71
2.4.2 Позначення та скорочення 72
2.4.3 Терміни та визначення 73
2.4.4 Завдання і цілі ЗНБ 75
2.4.5 Оновлення Політики 77
2.4.6 Ролі та відповідальність 78
2.4.7 Порядок ознайомлення та навчання в області ЗНБ 82
2.4.8 План управління НС 82
2.4.9 Оголошення / дія / скасування режиму НС 83
2.4.10 Управління в режимі НС 84
2.4.11 Резервні офіси, переміщення працівників у резервні офіси 84
2.4.12 Розподіл навантажень між іншими ЦОД 85
2.5 Рекомендації щодо захисту інформації, що обробляється з використанням технології хмарних обчислень 85

2.5.1 Об'єкти, що підлягають захисту при використанні технологій хмарних обчислень 85
2.5.2 Загрози безпеці інформації, що обробляється з використанням технологій хмарних обчислень..... 87
2.5.2.1 Загрози, пов'язані з невизначеністю при розподілі відповідальності..... 88
2.5.2.2 Загрози БІ, пов'язані з неузгодженістю політик безпеки 89
2.5.2.3 Загрози БІ, пов'язані з безперервною модернізацією 89
2.5.2.4 Загрози БІ, пов'язані з призупиненням надання послуг внаслідок технічних збоїв 89
2.5.2.5 Загрози БІ, пов'язані з неможливістю міграції образів віртуальних машин 90
2.5.2.6 Загрози БІ, пов'язані з ліцензійними політиками..... 90
2.5.2.7 Загрози БІ, пов'язані з конфліктом юрисдикцій різних країн..... 90
2.5.2.8 Загрози БІ, пов'язані з неякісним перенесенням інфраструктури в хмару..... 91
2.5.2.9 Загрози БІ, пов'язані із здійсненням незахищеного адміністрування хмарних послуг..... 91
2.5.2.10 Загрози БІ, пов'язані з загальнодоступністю інфраструктури..... 91
2.5.2.11 Загрози БІ, пов'язані з використанням технологій віртуалізації..... 92
2.5.2.12 Загрози БІ, пов'язані з порушенням доступності хмарного сервера..... 92
2.5.2.13 Загрози БІ, пов'язані зі зловживаннями з боку споживачів хмарних послуг..... 92
2.5.3 Захист інформації при наданні хмарних послуг 92
2.7 Висновок 100
3 ЕКОНОМІЧНИЙ РОЗДІЛ 101
3.1 Розрахунок капітальних (фіксованих) витрат 101
3.2 Розрахунок річних поточних (експлуатаційних) витрат..... 104
3.3 Збитки підприємства..... 105
3.4 Висновок 107
ВИСНОВКИ..... 108

ПЕРЕЛІК ПОСИЛАНЬ 109
ДОДАТОК А 112
ДОДАТОК Б 113
ДОДАТОК В 114
ДОДАТОК Г 115

ВСТУП

Робочий процес на більшості сучасних підприємств характеризується високим рівнем автоматизації. Це, в свою чергу, значно підвищує продуктивність праці фахівців різних підрозділів компанії, а значить, є однією з гарантій успішного розвитку бізнесу в цілому. Але навіть короткочасна втрата доступу до стратегічно важливих бізнес-процесам і додатків стає дуже критичною і призводить до зупинки всього виробництва, а отже, і до фінансових збитків.

Забезпечення безперервності бізнесу є одним з ключових аспектів успішного функціонування будь-якої сучасної компанії. Даному питанню приділяється значна увага, в тому числі і при створенні системи інформаційної безпеки компанії.

Планування безперервності бізнесу (Business Continuity Planning або BCP) – це діяльність, спрямована на зниження ризиків переривання бізнесу і негативних наслідків таких збоїв, відновлення бізнесу до прийнятного рівня в певній послідовності і встановлені терміни, починаючи з моменту переривання.

Процедура планування безперервності бізнесу передбачає оцінку ризиків різноманітних організаційних процесів, створення політик, планів і процедур для мінімізації цих ризиків. Головна мета BCP – підтримання основних бізнес-функцій компанії.

Кінцева мета робіт зі створення системи забезпечення безперервності бізнесу - максимально швидке відновлення доступу до критичних IT-ресурсів і додатків, а також мінімізація ризиків і збитків для бізнесу в період виходу підприємства з надзвичайної ситуації. Передбачити всі можливі сценарії і підготуватися до них неможливо; однак чим більше глибина і масштаб планування подій та підготовчих заходів, тим ефективніше організація зможе відреагувати на непередбачені інциденти.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз хмарних систем

Хмарні обчислення – це модель забезпечення доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера. Як правило, сучасна хмарна система складається з великої кількості високопродуктивних серверів, на яких запущені віртуальні машини (сервери), свої для кожного користувача.

Одна з головних переваг хмарних систем, крім незалежності кожного користувача від інших, це можливість плавно регулювати обсяг використовуваних ресурсів і, відповідно, оплачувати тільки ті ресурси, які дійсно потрібні для вирішення завдання.

По суті, перехід до хмарних обчислень означає аутсорсинг традиційних процесів управління IT-інфраструктурою зовнішніми постачальниками. Більшість сучасних постачальників рішень сфери хмарних обчислень надають можливість не тільки використовувати існуючі хмарні платформи, але і створювати власні, що відповідають технологічним вимогам замовників.

Концепція хмарних обчислень стала результатом еволюційного розвитку інформаційних технологій за останні кілька років і відповіддю на виклики сучасного бізнесу. Аналітики Гартнер груп називають хмарні обчислення - найперспективнішою стратегічною технологією майбутнього, прогнозуючи переміщення більшої частини інформаційних структур в хмарні системи протягом 5-7 років. За їх оцінками, до 2023 року обсяг ринку хмарних обчислень досягне 350 мільярдів доларів[1].

1.1.1 Класи хмарних систем

На даний момент існує безліч продуктів і технологій, що пропонують ті чи інші рішення в області хмарних обчислень. Серед них можна виділити наступні класи рішень:

– закриті комерційні;

– платформи для розподілених обчислень;

– спеціалізовані засоби для створення розподілених веб-сервісів[1].

Для специфічних завдань часто можна знайти спеціалізовані рішення, можливості яких зазвичай суворо обмежені під вирішення однієї або декількох конкретних завдань. У разі обчислювально-трудомістких завдань такі рішення часто надають свої власні способи для розподілення обчислень. Як приклад таких спеціалізованих продуктів в області обробки мультимедійних потоків можна назвати Adobe Media Server або його аналог з відкритим вихідним кодом - Red5 Media Server.

Навіть у випадку, коли завдання доступні для вирішення в хмарних сервісах загального призначення, помітна яскраво виражена тенденція до вузької спеціалізації окремих обчислювальних вузлів. Зокрема, в сервіс-орієнтованих системах сервіси зазвичай представлені відокремленими інстанціями, кожна з яких вирішує строго обмежену задачу і не є універсальною. Розподілення в такому випадку досягається шляхом запуску великої кількості примірників цих відокремлених сервісів, так чи інакше взаємодіють один з одним в рамках сервісів одного типу. При цьому організація взаємодії сервісів різних типів сильно ускладнена.

Також варто зазначити, що процес розгортання практично будь розподіленої хмарної системи не відрізняється простотою, а тому вимагає наявності кваліфікованого персоналу. Дана вимога часто є ключовим аргументом проти об'єднання ресурсів у єдині обчислювальні кластера, здатні вирішувати набагато складніші завдання, ніж будь-яка з одиночних машин. Далі наведені різні підходи до побудови розподілених обчислювальних мереж.

1.1.1.1 Закриті комерційні «хмари»

Найбільш популярними є величезні публічні «хмари» від таких представників IT-індустрії, як Google, Microsoft і Amazon. Ці продукти доступні кожному, хто готовий за них платити, і відрізняються дуже високою якістю, надійністю і швидкодією. Проте всі вони є закритими і не допускають розгортання за межами контрольованої їх власниками території. Не представляється ніякої можливості розгорнути подібне «хмара» на своєму власному обладнанні[2].

Продукти даного класу запущені в єдиному екземплярі у вигляді глобального сервісу, доступного користувачам з усього світу. У їх архітектурі особливу увагу приділено апаратним особливостям устаткування, ретельно контролюється інфраструктура обчислювальних вузлів, використовується численне низькорівневе програмне забезпечення, написане спеціально для даних систем (наприклад, специфічні операційні та файлові системи). Все це обумовлює якісно інший рівень надаваних послуг, у порівнянні з будь-якими іншими існуючими або створюваними продуктами.

Яскравими представниками цього класу рішень є наступні всесвітньо відомі продукти:

– Amazon Elastic Compute Cloud;

– Google App Engine;

– Microsoft Windows Azure.

1.1.1.2 Платформи для розподілених обчислень

Менш популярними, але також добре відомими є численні, в більшості своїй вільні (з відкритим вихідним кодом і вільною ліцензією), продукти для розгортання великих розподілених мереж на масових апаратних засобах. Такі обчислювальні мережі часто називають «приватними хмарами». Інша назва подібних продуктів - grid toolkit. Рішення даного класу дозволяють об'єднати безліч обчислювальних вузлів в єдину мережу для подальшого запуску завдань в ній. Більшість з них націлені на виконання пакетних завдань, складених з запуску різних додатків на вузлах і пересилання даних між ними, що обумовлює

можливість використання таких методів для вирішення широкого спектру завдань. Важливою особливістю подібних рішень є об'єднана захищена середовище, в якому опиняються виконувані завдання. Доступ до даних і результатів обчислень суворо обмежується відповідно до настройками системи. Однак такі системи не підтримують роботу з потоковими даними і не зручні для вирішення одного з найпоширеніших нині класу задач, а саме надання різних повсякденних і не дуже послуг численним користувачам. Для таких завдань найбільше підходять сервіс-орієнтовані рішення, в той час як розглядаються платформи не дозволяють організувати поверх себе подібну архітектуру[2].

1.2 Основні характеристики хмарних сервісів

1.2.1 Масштабованість

Введення нових продуктів і сервісів, розширення каналу продажів і кількості замовників вимагають від інформаційних систем організації витримувати зростаючі навантаження і обробляти великі обсяги даних. Швидка і надійна робота, що виключає відмови в обслуговуванні, затримки у відповідях від системи і збої дозволяє підвищити лояльність і задоволеність замовників. Масштабовані додатки дозволяють витримувати велике навантаження, за рахунок збільшення кількості одночасно запущених екземплярів. Як правило, для одночасного запуску безлічі екземплярів використовується типове обладнання, що знижує загальну вартість володіння і спрощує супровід інфраструктури[3].

1.2.2 Еластичність

Гнучка реакція на мінливі умови ведення бізнесу є однією з характеристик успішного бізнесу. Наприклад, ситуація, що ринкова кон'юнктура і дії конкурентів можуть зажадати швидко впровадити новий продукт або послугу, провівши при цьому повний цикл планування, проєктування та розробки інформаційної системи. Еластичність дозволяє швидко наростити потужність інфраструктури, без необхідності проведення початкових інвестицій в

устаткування і програмне забезпечення. Еластичність пов'язана з масштабністю додатків, так як вирішує завдання моментального зміни кількості обчислювальних ресурсів, що виділяються для роботи інформаційної системи[3].

1.2.3 Мультітенантність

Мультітенантність - це один із способів зниження витрат за рахунок максимального використання загальних ресурсів для обслуговування різних груп користувачів, різних організацій, різних категорій споживачів і т.п. Мультітенантність може бути особливо приваблива для компаній-розробників додатків, оскільки дозволяє знизити власні витрати на оплату ресурсів хмарної платформи і максимально використовувати доступні обчислювальні ресурси.

1.3 Аналіз особливостей системам хмарних обчислень

1.3.1 Переваги хмарних систем

Згідно зі статистикою середній рівень завантаження процесорних потужностей у серверів під управлінням Windows не перевищує 10%, у Unix-систем цей показник краще, але тим не менше в середньому не перевищує 20%. Низька ефективність використання серверів пояснюється широко застосовуваним з початку 2000-х років підходом "один додаток - один сервер". Кожен раз для розгортання нової програми компанія набуває новий сервер. Очевидно, що на практиці це означає швидке збільшення серверного парку і як наслідок - зростання витрат на його адміністрування, енергоспоживання та охолодження, а також потреба в додаткових приміщеннях для установки все нових серверів і придбанні ліцензій на серверну ОС[4].

Віртуалізація ресурсів фізичного сервера дозволяє гнучко розподіляти їх між додатками, кожне з яких при цьому має доступ тільки до призначених йому ресурсів. В даному випадку реалізується підхід "один сервер - кілька додатків", але без зниження продуктивності, доступності та безпеки серверних додатків. Крім того, рішення віртуалізації дають можливість запускати в розділах різні

ОС за допомогою емуляції їх системних викликів до апаратних ресурсів сервера.

В основі віртуалізації лежить можливість одного комп'ютера виконувати роботу декількох комп'ютерів завдяки розподілу його ресурсів за кількома середах. За допомогою віртуальних серверів і віртуальних настільних комп'ютерів можна розмістити кілька ОС і кілька додатків в єдиному місці розташування. Таким чином, фізичні та географічні обмеження перестають мати якесь значення. Крім енергозбереження та скорочення витрат завдяки більш ефективному використанню апаратних ресурсів, віртуальна інфраструктура забезпечує високий рівень доступності ресурсів, більш ефективну систему управління, підвищену безпеку і вдосконалену систему відновлення в критичних ситуаціях.

Віртуальною машиною називають програмне або апаратне середовище, яке приховує справжню реалізацію будь-якого процесу або об'єкта від його видимого уявлення[5].

Віртуальна машина - це повністю ізольований програмний контейнер, який працює з власною ОС і додатками, як фізичний комп'ютер. Віртуальна машина діє так само, як фізичний комп'ютер, і містить власні віртуальні (тобто програмні) ОЗУ, жорсткий диск і мережевий адаптер[5].

ОС не може розрізнити віртуальну і фізичну машини. Те ж саме можна сказати про додатки та інших комп'ютерах в мережі. Але незважаючи на це віртуальні машини складаються виключно з програмних компонентів і не включають обладнання. Це дає їм ряд унікальних переваг над фізичним обладнанням.

Основні особливості віртуальних машин:

1 Сумісність. Віртуальні машини, як правило, сумісні з усіма стандартними комп'ютерами. Як і фізичний комп'ютер, віртуальна машина працює під управлінням власної гостьовий оперативної системи і виконує власні програми. Вона також містить усі компоненти, стандартні для фізичного комп'ютера (материнську плату, відеокарту, мережевий контролер і т.д.). Тому

віртуальні машини повністю сумісні з усіма стандартними операційними системами, програмами та драйверами пристроїв. Віртуальну машину можна використовувати для виконання будь-якого програмного забезпечення, придатного для відповідного фізичного комп'ютера;

2 Ізольованість. Віртуальні машини повністю ізольовані один від одного, як якщо б вони були фізичними комп'ютерами Віртуальні машини можуть використовувати загальні фізичні ресурси одного комп'ютера і при цьому залишатися повністю ізольованими один від одного, як якщо б вони були окремими фізичними машинами. Наприклад, якщо на одному фізичному сервері запущено чотири віртуальних машини, і одна з них дає збій, це не впливає на доступність решти трьох машин. Ізольованість - важлива причина набагато більш високої доступності та безпеки додатків, виконуваних у віртуальному середовищі, в порівнянні з додатками, виконуваними в стандартній, невіртуалізірованной системі;

3 Інкапсуляція. Віртуальні машини повністю інкапсулюють обчислювальну середу. Віртуальна машина являє собою програмний контейнер, що зв'язує, або «інкапсулює» повний комплект віртуальних апаратних ресурсів, а також ОС і всі її додатки в програмному пакеті. Завдяки інкапсуляції віртуальні машини стають неймовірно мобільними і зручними в управлінні. Наприклад, віртуальну машину можна перемістити або скопіювати з одного пункту до іншого так само, як будь-який інший програмний файл. Крім того, віртуальну машину можна зберегти на будь-якому стандартному носієві даних: від компактної карти Flash-пам'яті USB до корпоративних мереж зберігання даних;

4 Незалежність від устаткування. Віртуальні машини повністю незалежні від базового фізичного обладнання, на якому вони працюють. Наприклад, для віртуальної машини з віртуальними компонентами (ЦП, мережевою картою, контролером SCSI) можна задати налаштування, абсолютно не збігаються з фізичними характеристиками базового апаратного забезпечення. Віртуальні машини можуть навіть виконувати різні операційні системи (Windows, Linux та

ін.) На одному і тому ж фізичному сервері. У поєднанні з властивостями інкапсуляції і сумісності, апаратна незалежність забезпечує можливість вільно переміщувати віртуальні машини з одного комп'ютера на базі x86 на інший, не змінюючи драйвери пристроїв, ОС або програми. Незалежність від обладнання також дає можливість запускати в поєднанні абсолютно різні ОС і додатки на одному фізичному комп'ютері.

До основних різновидів віртуалізації відносять:

– віртуалізація серверів (повна віртуалізація і паравіртуалізація);

– віртуалізація на рівні операційних систем;

– віртуалізація додатків;

– віртуалізація подань.

1.3.2 Види хмарних сервісів

Хмарна обробка даних як концепція включає в себе поняття IaaS (Infrastructure as a service), PaaS (Platform as a service) і SaaS (Software as a service).

1.3.2.1 Інфраструктура як сервіс (IaaS)

IaaS - це надання комп'ютерної інфраструктури як послуги на основі концепції хмарних обчислень.

IaaS складається з трьох основних компонентів:

– апаратні засоби (сервери, системи зберігання даних, клієнтські системи, мережеве обладнання);

– операційні системи та системне ПЗ (засоби віртуалізації, автоматизації, основні засоби управління ресурсами);

– сполучне ПО (наприклад, для управління системами).[6]

IaaS заснована на технології віртуалізації, що дозволяє користувачеві обладнання ділити його на частини, які відповідають поточним потребам бізнесу, тим самим збільшуючи ефективність використання наявних обчислювальних потужностей. Користувач (компанія або розробник ПЗ)

повинен буде оплачувати лише реально необхідні йому для роботи серверний час, дисковий простір, мережеву пропускну спроможність та інші ресурси. Крім того, IaaS надає в розпорядження клієнта весь набір функцій управління в одній інтегрованій платформі.

IaaS позбавляє підприємства від необхідності підтримки складних інфраструктур центрів обробки даних, клієнтських і мережевих інфраструктур, а також дозволяє зменшити пов'язані з цим капітальні витрати і поточні витрати. Крім того, можна отримати додаткову економію, при наданні послуги в рамках інфраструктури спільного використання.

Першопрохідцями в IaaS вважається компанія Amazon, які на сьогоднішній день пропонують два основних IaaS-продукту: EC2 (Elastic Compute Cloud) і S3 (Simple Storage Service). EC2 являє собою Xen-хостинг зі статичними VPS-характеристиками, що не розширюються на льоту (хоча багато подібні сервіси вже надають т.зв. auto scaling). Сховище S3 має інтерфейс WebDAV і підтримує роботу з багатьма відомими мовами програмування.[6]

1.3.2.2 Платформа як сервіс (PaaS)

PaaS - це надання інтегрованої платформи для розробки, тестування, розгортання та підтримки веб-додатків як послуги.[6]

Для розгортання веб-додатків розробнику не потрібно купувати обладнання та програмне забезпечення, немає необхідності організовувати їх підтримку. Доступ для клієнта може бути організований на умовах оренди.

Такий підхід має такі переваги:

– масштабованість;

– відмовостійкість;

– віртуалізація;

– оперативність;

– безпека.

Масштабованість PaaS передбачає автоматичне виділення і звільнення необхідних ресурсів залежно від кількості обслуговуваних додатком користувачів.

PaaS як інтегрована платформа для розробки, тестування, розгортання та підтримки веб-додатків дозволить весь перелік операцій з розробки, тестування та розгортання веб-додатків виконувати в одній інтегрованому середовищі, виключаючи тим самим витрати на підтримку окремих середовищ для окремих етапів.

Здатність створювати вихідний код і надавати його в загальний доступ всередині команди розробки значно підвищує продуктивність по створенню додатків на основі PaaS.

Найвідомішим прикладом такої платформи є AppEngine від Google, яка пропонує хостинг для веб-додатків з можливістю купувати додаткові обчислювальні ресурси (наприклад, для тестування високих навантажень). Для запуску додатків Google AppEngine на віртуальних кластерних системах була розроблена платформа AppScale, яка не має, проте, ніякого відношення до Google.

У системах веб-пошуку і контекстної реклами компанії Yahoo використовується платформа Hadoop, орієнтована на передачу великих обсягів даних між мережевими серверами. На базі Hadoop побудовані HBase (аналог бази даних Google BigTable), а також HDFS (Hadoop Distributed File System, аналог Google File System).

Найбільшим постачальником хмарних платформ є підрозділ Microsoft - операційна система Windows Azure. Windows Azure створює єдине середовище, що включає хмарні аналоги серверних продуктів Microsoft (реляційна база даних SQL Azure, що є аналогом SQL Server, а також Exchange Online, SharePoint Online і Microsoft Dynamics CRM Online) і інструменти розробки (.NET Framework і Visual Studio, оснащена набором Windows Azure Tools). Так, наприклад, програміст, який створює сайт в Visual Studio, може не виходячи з програми розмістити свій сайт в Windows Azure.

1.3.2.3 Програмне забезпечення як сервіс (SaaS)

SaaS - модель розгортання програми, яка передбачає надання додатки кінцевому користувачеві як послуги на вимогу (on demand). Доступ до такого додатку здійснюється за допомогою мережі, а найчастіше за допомогою Інтернет-браузера.[6]

В даному випадку, основна перевага моделі SaaS для клієнта полягає у відсутності витрат, пов'язаних з установкою, оновленням і підтримкою працездатності обладнання та програмного забезпечення, що працює на ньому. Цільова аудиторія - кінцеві споживачі.

У моделі SaaS:

– додаток пристосоване для віддаленого використання;

– одним додатком можуть користуватися декілька клієнтів;

– оплата за послугу стягується або як щомісячна абонентська плата, або на основі сумарного обсягу транзакцій;

– підтримка додатки входить вже до складу оплати;

– модернізація програми може проводитися обслуговуючим персоналом плавно і прозоро для клієнтів.

З точки зору розробників програмного забезпечення, модель SaaS дозволить ефективно боротися з неліцензійним програмним забезпеченням, завдяки тому, що клієнт не може зберігати, копіювати та інсталювати програмне забезпечення.

По-суті, програмне забезпечення в рамках SaaS можна розглядати в якості більш зручної і вигідної альтернативи внутрішнім інформаційним системам.

Розвитком логіки SaaS є концепція WaaS (Workplace as a Service - робоче місце як послуга). Тобто клієнт отримує в своє розпорядження повністю оснащене всім необхідним для роботи ПО віртуальне робоче місце.

За нещодавно опублікованими даними SoftCloud попитом користуються наступні SaaS додатки (у порядку убування популярності):

– пошта;

– комунікації (VoIP);

– антиспам і антивірус;

– helpdesk;

– управління проєктами;

– дистанційне навчання;

– CRM;

– зберігання і резервування даних.[7]

Також, схожими є продукти MobileMe (Apple), Azure (Microsoft) і LotusLive (IBM). Суть даних сервісів в тому, що вони надають користувачам доступ до зберігання своїх даних (контакти, пошта, файли), а також для спільної роботи декількох користувачів з документами.

Питаннями зберігання призначених для користувача даних в Інтернет займається і компанія Google, яка розробляє проєкт GDrive, що представлятиме собою віртуальний жорсткий диск, який буде визначатися ОС як локальну. Також заявлено, що можна буде зберігати необмежену кількість даних, що звучить досить заманливо.

Ще одним цікавим представником виду SaaS є продукт iCloud, що представляє собою операційну систему, працювати з якою можна безпосередньо через браузер. Інтерфейс операційної системи виконаний в стилі Windows 10. На сьогоднішній день проєкт знаходиться у стадії бети і в самій ОС реалізований мінімум додатків.

Також до SaaS відносяться послуги Online backup, або, простіше кажучи - резервного копіювання даних. Користувач просто платить абонентську плату, а сервіси самі автоматично в певний час шифрують дані з комп'ютера або іншого пристрою і відправляють їх на віддалений сервер, тим самим дані можуть бути доступні з будь-якої точки земної кулі. Дану послугу зараз надають безліч компаній, у тому числі, такі як Nero і Symantec.

Таким чином, ці технології при спільному використанні дозволяють користувачам хмарних обчислень скористатися обчислювальними

потужностями і сховищами даних, які за допомогою певних технологій віртуалізації і високого рівня абстракції надаються їм як послуги.

1.3.3 Компоненти системи хмарних обчислень

Систему обчислень в «хмарі» розбивають на п’ять основних частин.

1.3.3.1 Апаратні компоненти центру обробки даних

Основні принципи вибору апаратних засобів, з подальшою їх атестацією, для обробки конфіденційної інформації в корпоративних мережах є стандартними, відносно інших систем. Вибір ґрунтується на гарантії якості, що відрізняється надійністю і стійкістю в роботі. Гарантію надають виробники апаратних компонентів. Також необхідно відзначити ряд необхідних організаційних і технічних заходів щодо запобігання несанкціонованого доступу до апаратної частини центрів обробки даних. Бувають ситуації, коли хакер намагається порушити режим інформаційної безпеки. Тому постійно ведеться контроль на визначення побічних сигналів або електромагнітних впливів. У таких випадках певними методами проводиться дослідження сигналів і захист від зовнішнього впливу. Подібні дії при аналогічній ситуації проводяться для систем хмарних обчислень з публічним доступом.[8]

1.3.3.2 Телекомунікаційна складова доступу до ресурсів

Принцип роботи зав'язаний на двох основних методах: шифрування IP-пакетів за допомогою апаратних і програмних засобів, або просто на відкритому трафіку. Практично завжди в корпоративних мережах компаній необхідно зберігати конфіденційність оброблюваних персональних даних для того, щоб була можливість доступу через IP-мережі. Тому, як правило, телекомунікаційна складова ґрунтується на шифруванні IP-пакетів. Всі кодування пакетів займає у системи значну частину ресурсів і може розтягуватися в часі. Зниження рівня шифрування призводить до збільшення відкритого трафіку, що сприяє падінню рівня захисту конфіденційної інформації. У деяких сферах діяльності людини дана ситуація неприпустима. Тому, актуальним завданням є підвищення швидкості IP-шифрування.[8]

1.3.3.3 Користувачі та їх програмно-апаратне забезпечення

В даний час не становить жодних проблем, з точки зору програмних і апаратних засобів, щодо шифрування IP-потоку по SSL протоколу на користувальницькому робочому місці. Швидкість обробки без проблем може досягати 10 Мбіт/с. На даний момент є досить сертифікованих фірм, що надають відповідні послуги. Набагато складніше забезпечити інформаційну безпеку по захисту ключів користувача, його операційної системи та особистої інформації в корпоративному хмарі. На персональні комп'ютери співробітника встановлюються електронні замки. Дану блокування може контролювати не тільки користувач заблокованого робочого місця, а й служба інформаційної безпеки компанії. Але це все стосується приватних систем, все більш складно складається для публічних хмар. Отримати легальні права доступу до системи може будь-який користувач. Тут порушникам, за допомогою спеціальних програмних і технічних засобів, які встановлюються безпосередньо на робочому місці, набагато легше подолати захист системи безпеки. Неможливо проконтролювати всіх користувачів мережі Інтернет на склад робочого місця і передбачити їх наміри. Тому в ЦОД публічних мереж повинні бути максимально ефективні засоби захисту, які постійно перебували б під жорстким контролем.[8]

1.3.3.4 Середня (middleware) частина центру обробки даних

Центр обробки даних за своєю структурою - це віртуальна машина. Відповідно, в ролі гіпервізора і набору різних гостьових операційних систем в даній машині можна вважати «середній» шар ЦОД. До віртуальним машинам також відноситься і керуюча система. Відомий факт, що при створенні та подальшій експлуатації віртуальних машин, гіпервізор відіграє ключову роль, як основний елемент системи інформаційної безпеки. Будучи, в свою чергу, операційною системою, гіпервізор працює з апаратним програмним забезпеченням, має можливість розподіляти функції від базової системи гостьовим. Тому, гіпервізор можна сміливо порівнювати зі стандартною операційною системою. Таким чином, для забезпечення нормального

функціонування системи в режимі інформаційної безпеки, необхідно застосовувати до гіпервізором вимоги, які використовуються для класичних операційних систем.

1.3.3.5 Прикладні сервіси

Прикладні сервіси можна порівнювати з прикладним програмним забезпеченням операційних систем, які проходять сертифіковану атестацію у сфері інформаційної безпеки. Період перевірки всіх вимог до програмного забезпечення під час етапів сертифікації операційних систем займав не більше кварталу. Для великих сервісів хмарних обчислень, таких як Microsoft Word або Explorer, витратили близько року на первинну перевірку відповідності системи сертифікованим стандартам. При вторинних перевірках, звичайно, цей період скоротився. Основним напрямком у вирішенні даної задачі є розробка найменшого необхідної кількості вимог до ПЗ при процесі атестації операційних систем. Аналогічно можна розглянути дані дії до гіпервізором.

1.3.4 Загальні вимоги до безпеки хмарних обчислень

Вимоги до безпеки хмарних обчислень здаються схожими з вимогами до звичайних ЦОД - застосування засобів мережевої безпеки та авторизації. [9] Проте, як було зазначено вище, фізичне розділення та апаратні засоби мережевого захисту не можуть захистити від атак на ВМ всередині одного сервера. Компанії, що надають послуги хмарних обчислень, для підвищення ефективності віртуалізації змушені розміщувати ВМ різних організацій на одних і тих же фізичних ресурсах. Детальний розгляд перерахованих нижче аспектів є першочерговим при плануванні переходу на будь-які види хмарних обчислень.

Однією з найважливіших характеристик хмарних обчислень є "самообслуговування", тобто доступ через Інтернет до управління обчислювальною потужністю. Така можливість істотно відрізняється від роботи в традиційних ЦОД, де доступ інженерів до серверів строго контролюється на фізичному рівні. У хмарних обчисленнях доступ інженерів відбувається через

Інтернет, що призводить до появи відповідних загроз. Відповідно, критично важливим є строгий контроль доступу для адміністраторів, а також забезпечення контролю і прозорість змін на системній рівні.[10]

Віртуальні машини динамічні. Вони можуть бути оперативно повернуті в попередній стан, а також легко припинені і перезавантажені. Крім цього, ВМ можуть бути клоновані, а також переміщені між фізичними серверами.

Подібна мінливість ВМ дуже сильно ускладнює створення і підтримку цілісної системи безпеки. Уразливості і помилки в налаштуваннях можуть безконтрольно поширюватися. Крім цього, досить непросто зафіксувати для подальшого аудиту стан захисту в якийсь певний момент часу. У середовищах хмарних обчислень потрібно мати можливість надійно зафіксувати стан захисту системи, безвідносно від її місця розташування та стану [9].

Сервери хмарних обчислень використовують ті ж ОС і ті ж веб-додатки, що і локальні віртуальні та фізичні сервера. Відповідно, для хмарних систем загроза віддаленого злому або зараження шкідливим кодом через уразливості точно так само висока. Насправді, ризик для віртуальних систем навіть вище, так як паралельне існування безлічі ВМ істотно збільшує площу атаки. Крім того, з'являється загроза злому або зараження всередині однієї фізичної системи, коли одна ВМ заражає або атакує іншу. Система виявлення та запобігання вторгнень повинна бути здатною помітити шкідливу активність на рівні ВМ, незалежно від розташування ВМ в хмарному середовищі.[10]

На відміну від фізичної машини, коли ВМ вимкнена, все ще є можливість її компрометації або зараження. [11] Для цього достатньо якого-небудь доступу до сховища образів ВМ через мережу. З іншого боку, виключена ВМ не має абсолютно ніякої можливості запустити якесь ПЗ для захисту від шкідливого коду. У середовищах хмарних обчислень відповідальність за захист і сканування бездіяльних ВМ лежить на провайдера. Підприємства, які використовують сервіси хмарних обчислень, повинні переконатися в тому, що провайдер використовує подібні засоби безпеки у своєму середовищі віртуалізації.

Існуючі рішення з безпеки створювалися до появи технології віртуалізації систем x86 і, відповідно, вони спроєктовані без обліку роботи у віртуальному середовищі. У хмарної середовищі, де ВМ різних користувачів поділяють єдині апаратні ресурси, одноразова сканування у всіх віртуальних системах призведе до катастрофічного зниження продуктивності всієї віртуальної середовища. Провайдери хмарних послуг, що надають базові функції безпеки своїм клієнтам, в змозі уникнути цієї проблеми, здійснюючи ресурсомісткі сканування на рівні гіпервізора, уникаючи, таким чином, конкуренції за обчислювальні ресурси на рівні кожної ВМ.

Згідно зі звітом "Data Breach Investigations Report", опублікованому Verizon Business Risk Team [12], 59% витоків даних були результатом злому хакерами. Треба думати, що спеціалізовані ресурси є більш захищеними, ніж ресурси розділяються. Відповідно, атакують поверхню повністю або частково розділяється хмарної середовища повинна бути більше і перебуває під більшою загрозою. Підприємства повинні мати можливість перевірити особисто і довести зовнішнім аудиторам, що ресурс не завдано шкоди і що системи не скомпрометовані, особливо в ситуації, коли вони розміщуються в розділяється фізичному середовищі. Цілісність операційної системи і файлів додатків, а також внутрішня активність повинні контролюватися.

Багато закони та стандарти, такі як PCI DSS і HIPAA, включають в себе вимоги використання криптографічних засобів для захисту важливої інформації, такої як інформація про власника кредитної картки і інформація, що ідентифікує людини. Криптографічний захист подібних даних є "тихою гаванню", тобто захищає компанію від санкцій закону, у разі, якщо дані будуть втрачені. Використання багатокористувацьких хмарних сервісів ускладнює слідування вимогам стандартів і законів, що породжує непросту задачу забезпечення надійного захисту і безпечного доступу до важливих даних.

Послуги хмарних обчислень припускають самообслуговування, що може породити плутанину в управлінні оновленнями. Як тільки компанія підписалася на хмарний сервіс, наприклад, створення веб-сервера з шаблонів, управління

установкою оновлень на платформу і веб-сервер вже не перебувають у віданні провайдера. З цього моменту за оновлення відповідає клієнт. Для 90% відомих вразливостей, які на практиці використовувалися зловмисниками, оновлення були випущені більше ніж за 6 місяців до інциденту. Отже, організації, що використовують хмарні обчислення, повинні бути пильні і намагатися забезпечити всі програми, що працюють в хмарі, новітніми оновленнями. Якщо оперативна установка оновлень неможлива або непрактична, то необхідно розглянути альтернативний підхід - використання "віртуальних латок". Технологія "віртуальних латок" припускає блокування націлених на уразливості атак безпосередньо на мережевому рівні, що не дозволяє шкідливому коду або зловмисникам яким-небудь способом скористатися не усуненою вразливістю.[13]

Підприємства прикладають істотні зусилля для відповідності різним законам і проходженню всіляким стандартам, таким як PCI, HIPAA і GLBA, а крім цього, проводять аудити у відповідності з різноманітними рекомендаціями (SAS70 і ISO). Необхідно забезпечити компанії можливістю довести дотримання законів і стандартів безпеки, незалежно від розташування використовуваних систем, які є об'єктом регулювання (фізичні сервери, віртуальні сервери, розміщені в хмарних середовищах).[14]

При використанні хмарних обчислень, периметр корпоративної мережі зникає, і захист найменш захищеною складової мережі визначає загальний рівень захищеності. Корпоративний брандмауер, основний компонент для впровадження політик безпеки і розмежування сегментів мережі, не в змозі вплинути на сервери, розміщені в хмарних середовищах. Його політики не в змозі вплинути на доступ до тих чи інших ресурсів - тепер це відповідальність провайдера хмарних обчислень. Для розмежування сегментів з різним рівнем довіри в хмарі ВМ повинні самі забезпечувати себе захистом, фактично переміщує мережевий периметр до самої ВМ.

Віртуалізація - це підготовка технології до використання в хмарних обчисленнях. Організації, які не використовують хмарні обчислення сьогодні,

найчастіше розглядають перехід на них у майбутньому. Центри обробки даних, які вже консолідували свої фізичні сервери у вигляді ВМ, можуть вже зараз зробити кроки для підвищення рівня захисту свого віртуалізованого середовища, а також підготувати ВМ до міграції в хмарні середовища, коли така необхідність виникне. [15]

Раніше віртуальну машину визначали як «ефективну ізольовану копію реальної машини». Проте сучасні віртуальні машини можуть не мати прямого апаратного аналогу. Наприклад, в залежності від способу моделювання набору інструкцій віртуального центрального процесора, віртуальна машина може моделювати реальну або абстрактну обчислювальні машини. При моделюванні реальної обчислювальної машини набір інструкцій процесора віртуальної машини збігається з набором інструкцій обраного для моделювання центрального процесора.

З погляду технічної реалізації для систем хмарних обчислень характерне використання засобів віртуалізації, що забезпечують можливість самообслуговування споживачів і динамічної масштабованості обчислювальних ресурсів. Використання засобів віртуалізації призводить до появи додаткових осіб і факторів, що впливають на системи хмарних обчислень і є джерелами загроз інформаційній безпеці, специфічними для технології хмарних обчислень. Так, збої в роботі засобів віртуалізації можуть призвести до порушення ізоляції і втрати оброблюваної інформації, а уразливості системи управління віртуальним середовищем створюють можливість для несанкціонованого доступу до обчислювальних ресурсів або даними з боку інших споживачів системи хмарних обчислень.

Універсальність доступу до інформаційних сервісів по каналах інформаційно-телекомунікаційних мереж розширює коло можливих сценаріїв реалізації загроз інформаційної безпеки з боку користувачів мереж. У той же час дана особливість систем хмарних обчислень дає можливість перенесення процесів обробки інформації в захищені та відмовостійкі центри [13].

1.3.5 Джерела загроз в системах хмарних обчислень

У зв'язку з використовуваної в системах хмарних обчислень моделлю надання інформаційних сервісів персонал провайдера володіє потенційно необмеженим доступом до інформації споживачів. На відміну від традиційних інформаційних систем, персонал провайдера не є представником споживача, а значить, знаходиться поза зоною його контролю. З урахуванням високої консолідації обчислювальних ресурсів в системах хмарних обчислень дана обставина значно розширює можливості реалізації загроз інформаційної безпеки з боку персоналу провайдера. При цьому залежно від функціональних завдань персоналу загрози можуть бути реалізовані шляхом фізичного доступу до компонентів системи хмарних обчислень, а також з використанням системного та прикладного програмного забезпечення.[16]

Крім того, в число можливих джерел загроз інформаційній безпеці в системах хмарних обчислень може входити оператор зв'язку, що надає послуги підключення між провайдером і споживачами та надає безпосередній вплив на забезпечення доступності інформаційних сервісів і захист переданих даних.

Традиційна модель управління доступом побудована на контурах комп'ютера, тому це призводить до слабкого контролю за читанням і зміною даних в розподілених обчислювальних системах. Ясно те, що традиційний контроль доступу не підходить для середовища хмарних обчислень. У середовищі хмарних обчислень традиційний механізм контролю за доступом володіє серйозними дефектами.

Узагальнені результати проведеного аналізу джерел загроз інформаційній безпеці для систем, у яких використовуються хмарні обчислення наведені в таблиці 1.1.

Таблиця 1.1 - Джерела загроз інформаційній безпеці в системах хмарних обчислень

Джерело загроз	Опис джерела загроз	Особливості джерела загроз в системах хмарних обчислень
Технічні засоби обробки інформації, програмне забезпечення, система електроживлення	Технічні засоби і технології, збої в роботі яких можуть призвести до реалізації загроз інформаційної безпеки	Вплив даних джерел загроз на інформаційну безпеку систем хмарних обчислень аналогічно традиційним інформаційним системам
Засоби віртуалізації	Уразливості і помилки в роботі засобів віртуалізації можуть призвести до несанкціонованого використання обчислювальних ресурсів і доступу до інформації споживачів систем хмарних обчислень, а також втрати даних	Поява даного джерела загроз пов'язане з використанням засобів віртуалізації для забезпечення можливості самообслуговування споживачів, високою консолідації та динамічної масштабованості ресурсів
Природні явища, стихійні лиха	Природні явища та стихійні лиха можуть призвести до реалізації загроз інформаційній безпеці, пов'язаних із фізичним ушкодженням або знищенням компонентів системи хмарних обчислень	У зв'язку із здійсненням обробки інформації в центрах обробки даних провайдера ймовірність реалізації загроз інформаційній безпеці, обумовлених наявністю даного джерела загроз, в системах хмарних обчислень знижується
Користувачі інформаційно-телекомунікаційних мереж	Користувач інформаційно-телекомунікаційних мереж може реалізувати загрози інформаційній безпеці з використанням інформаційно-телекомунікаційних мереж	У зв'язку з наданням доступу до інформаційних сервісів системи хмарних обчислень можливості реалізації загроз розширюються
Оператор зв'язку	Оператор зв'язку може реалізувати загрози доступності інформаційних сервісів системи	Універсальність доступу зумовлює залежність системи хмарних обчислень від оператора

Продовження таблиці 1.1

Джерело загроз	Опис джерела загроз	Особливості джерела загроз в системах хмарних обчислень
Персонал провайдера	Помилкові дії персоналу провайдера, що володіє необмеженим доступом до інформації споживачів і компонентам системи хмарних обчислень, можуть призвести до реалізації загроз інформаційної безпеки	Вплив даних джерел загроз на інформаційну безпеку систем хмарних обчислень аналогічно традиційним інформаційним системам
Недобросовісний персонал провайдера	Недобросовісний персонал провайдера, володіючи необмеженим доступом до інформації споживачів і компонентам системи хмарних обчислень, може реалізовувати загрози інформаційній безпеці, пов'язані з несанкціонованим доступом до інформації	У зв'язку з консолідацією обчислювальних ресурсів для обробки інформації споживачів, а також зі зниженням контрольованості процесів обробки інформації, можливості і реалізації загроз розширюються
Недобросовісні споживачі систем хмарних обчислень	Недобросовісні споживачі системи хмарних обчислень можуть реалізовувати загрози інформаційній безпеці по відношенню до інформації та обчислювальних ресурсів інших споживачів системи хмарних обчислень	Наявність даного джерела загроз інформаційній безпеці обумовлено динамічної масштабованість і консолідацією обчислювальних ресурсів.

1.4 Центри обробки даних сервісів розподілених обчислень

Хмарні обчислення пов'язані з новими завданнями для центрів обробки даних та їх мережної архітектури (рисунок 1.1).

ЦОД, або центр обробки даних, є виділеної мережею, яка відокремлена від локальних і глобальних мереж. Він зазвичай служить для взаємодії між собою пристроїв зберігання даних, підключених до одного або більше серверів. ЦОД часто характеризується високими швидкостями передачі даних між

зовнішніми пристроями зберігання і своєї високо масштабованої архітектурою. Також відмітною особливістю ЦОД є наявність спеціалізованого програмного забезпечення для управління, контролю і налаштування.[20]

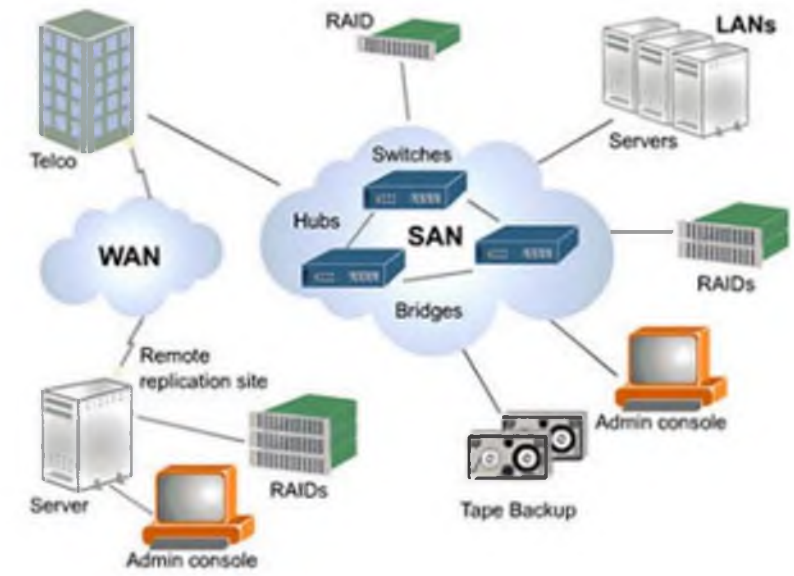

Рисунок 1.1 – Загальна структура ЦОД

В даний час питання захисту центрів обробки даних (ЦОД) - є одними з ключових для виробників і споживачів послуг інформаційної безпеки.

При створенні сучасних центрів обробки даних одним з найважливіших питань є забезпечення захисту оброблюваної інформації.

Продуктивність, надійність і керованість серверів стають вирішальними факторами для успішних операцій з використанням хмарних обчислень. Для забезпечення ефективної роботи ЦОД широко застосовуються технології віртуалізації, що дозволяють створювати на одному фізичному комп'ютері кілька віртуальних машин. Методи і засоби віртуалізації дозволяють створювати й ефективно використовувати керовану, надійну, безпечну інформаційну інфраструктуру. Віртуальні машини, будучи незалежними від конкретного обладнання одиницями, можуть поширюватися як шаблони, які можуть бути запущені на будь-якій апаратній платформі підтримуваної архітектури. За рахунок віртуалізації істотно підвищується гнучкість інформаційної інфраструктури, спрощуються процедури резервного копіювання та відновлення після збоїв.[20]

Очевидно, що проєктування, встановлення, налагодження та експлуатація компонентів хмарної інфраструктури являють собою комплекс складних завдань, ефективне вирішення яких вимагає високої кваліфікації відповідних фахівців: адміністраторів, системних інтеграторів, фахівців з проєктування, створенню та обслуговування ЦОД, розробників програмного забезпечення розподілених систем і т.д.

1.4.1 Забезпечення відмовостійкості ЦОД

Дата-центри, обладнані різнотипними телекомунікаційними пристроями, можуть виявитися здатними продовжувати роботу навіть в умовах катастрофи, яка в іншому випадку перервала б телекомунікаційний сервіс дата-центру.

Відповідно до TIA/EIA-942 структура ЦОД складається з трьох основних підсистем[20]:

MDA /Main Distribution Area – головна розподільна підсистема, забезпечує інтерфейс доступу до ЦОД і розподіляє трафік головної магістралі по внутрішніх магістралях. Вона включає кінцеве обладнання операторів зв'язку, маршрутизатори, магістральні комутатори тощо Тут MC – головний розподільний вузол, HC – комутаційний вузол, що розподіляє магістральний трафік по локальних лініях;

HDA /Horizontal Distribution Area – горизонтальна розподільча підсистема, направляє трафік внутрішніх магістралей по локальних лініях (довжиною не більше 100 м), що виходять в апаратні зони (стійки). Крім пасивного обладнання в ній використовуються комутатори ЛВС, тощо;

EDA/Equipment Distribution Area – підсистема розводки по обладнанню, що доставляє трафік в робочі області до серверів, дискових масивів тощо. Для обслуговування областей, де потрібні часті переконфігурації можуть використовуватися зонові сегменти з вузлами консолідації (ZDA).

1.4.1.1 Резервні оглядові люки і зовнішні кабельні канали

Наявність декількох зовнішніх кабельних каналів від власної лінії провайдера до кімнаті введення виключає єдину точку відмови для сервісів

провайдерів, входять у будинок. Ці кабельні канали повинні мати доступні для користувача оглядові люки в тих випадках, коли жорсткі металеві кабельні канали (Кабельні трубопроводи) провайдера не закінчуються біля стіни будівлі. Оглядові люки і зовнішні кабельні канали повинні перебувати з протилежних сторін стіни будівлі і повинні бути віддалені один від одного принаймні на 20 м (66 футів). У дата-центрах з двома кімнатами введення і двома оглядовими люками немає необхідності встановлювати кабельні трубопроводи від кожної кімнати введення до кожного з двох оглядових люків. При такій конфігурації від кожного провайдера доступу зазвичай вимагають встановити два зовнішніх кабелю, один до головній кімнаті введення через головний оглядовий люк, і один до допоміжної кімнаті введення через допоміжний оглядовий люк. Кабельні трубопроводи від головного оглядового люка до допоміжної кімнаті введення і від допоміжного оглядового люка до головній кімнаті введення забезпечують гнучкість, але не є обов'язковими[20].

У дата-центрах з двома кімнатами введення допускається встановлювати кабельні трубопроводи між двома кімнатами введення, з метою забезпечення прямого шляху для кабелів провайдера доступу між цими двома кімнатами, наприклад щоб виконати кільце для мережі SONET або SDH.

1.4.1.2 Резервні сервіси провайдерів доступу

З метою забезпечення неперервності послуг зв'язку, що поставляються дата-центру провайдерами доступу, можна залучити кілька провайдерів, використовувати кілька центральних офісів провайдерів, а також передбачити кілька різних кабельних трас від провайдерів доступу до дата-центру.

Наявність декількох провайдерів забезпечить неперервність зв'язку у разі масштабної аварії у провайдера або в разі його фінансового краху, здатного вплинути на сервіс.

Але все ж одне лише використання декількох провайдерів доступу не гарантує неперервності сервісу, оскільки провайдери часто спільно займають площу в центральних офісах і спільно використовують трубопровідні траси.

Користувачеві слід забезпечити таке становище, при якому сервіси надаються з різних центральних офісів і кабельні траси до цих установ йдуть по різним маршрутам. Ці траси повинні бути фізично віддалені один від одного на відстань не менше 20 м (66 футів) у всіх точках по всій довжині цих трас. [20]

1.4.1.3 Резервування кімнат введення

Кілька кімнат введення можна влаштувати з метою резервування, а не тільки для того, щоб обійти обмеження на максимальну довжину лінії. Наявність декількох кімнат введення підвищують ступінь резервування, але ускладнює організаційне управління. Слід уважно розподілити лінії між кімнатами введення. Провайдери доступу повинні встановити своє обладнання в обох кімнатах введення таким чином, щоб лінії всіх необхідних типів можна було підготувати до роботи (ініціювати) з кожної кімнати. Ініціювання обладнання провайдера в одній кімнаті введення не повинно бути підлеглим по відношенню до обладнання в іншій кімнаті введення. Обладнання провайдера в кожній з кімнат введення повинно бути спроможне працювати в разі відмови в іншій кімнаті введення. Дві кімнати введення слід відсунути один від одного на відстань не менше 20 м (66 футів) і розмістити в роздільних вогнезахисних зонах. [20]

1.4.1.4 Резервна головна розподільна зона

Другорядна розподільна зона забезпечить додаткове резервування, але при цьому ускладниться організаційне управління. Основні маршрутизатори та комутатори слід розподілити між головною розподільної зоною і додатковою розподільної зоною. Лінії також слід розподілити між двома цими зонами.

Влаштовувати другорядну розподільну зону не має сенсу, якщо машинний зал являє собою єдиний простір, оскільки пожежа в одній частині дата-центру потребують, ймовірно, відключення всього дата-центру цілком. Другорядну розподільну зону і головну розподільну зону слід розміщувати в роздільних вогнезахисних зонах, забезпечувати енергією від різних

розподільних щитів харчування і оснащувати окремими системами кондиціонування повітря. [20]

1.4.1.5 Резервна магістральна розводка

Резервна магістраль захищає від загального виходу з ладу внаслідок відмови магістральної кабельної розводки. Резервна магістраль може бути влаштована по-різному, залежно від бажаного ступеня захисту.

Магістральна розводка між двома зонами, наприклад, між горизонтальною розподільчою зоною і головною розподільної зоною, може бути виконана шляхом укладання двох кабелів між цими зонами, переважно за двома різними маршрутами. Якщо дата-центр має головну розподільну зону і другорядну розподільну зону, то укладати резервується магістральну розводку до горизонтальної розподільчої зоні немає необхідності, однак кабелі до головної розподільної зоні і другорядною розподільної зоні слід прокласти по різних маршрутах.

Деяку ступінь резервування можна також забезпечити шляхом установки магістрального кабелю між горизонтальними розподільними зонами. Якщо магістральна розводка від головної розподільчої зони до горизонтальної розподільчої зоні буде пошкоджена, можна буде перемикати з'єднання через іншу горизонтальну розподільну зону. [20]

1.4.1.6 Резервна горизонтальна розводка

Горизонтальну кабельну розводку до критично важливих систем можна прокласти по різних маршрутах, щоб підвищити ступінь резервування. При виборі маршрутів слід дотримуватися обережності, щоб не перевищити максимально можливу довжину горизонтального кабелю. [20]

Для критично важливих систем можна передбачити дві різні горизонтальні розподільні зони, якщо тільки не перевищувати обмежень на максимальну довжину кабелів. Але така ступінь резервування, можливо, не забезпечить набагато більш надійний захист, ніж укладання горизонтальної

розводки за різними маршрутами, якщо дві ці горизонтальні розподільні зони знаходяться в одній і тій же вогнезахисної зоні.

1.5 Вразливості хмарних систем

Концепція хмарних обчислень побудована на новій конфігурації. Нова конфігурація складається з розмаїття нових технологій, таких як Hadoop, Hbase, що підвищує продуктивність системи хмарних обчислень, але в той же час може призвести до ризику. Фактично завдання захисту хмарних систем можна розділити на дві складові: забезпечення безпеки функціонування обладнання та забезпечення безпеки даних. Провайдер повинен реалізувати захист свого апаратно-програмного комплексу від несанкціонованого вторгнення, модифікації коду, злому IT-системи, щоб забезпечити захист даних клієнта. Клієнт, у свою чергу, при необхідності розміщення будь-яких важливих і секретних даних, може використовувати технології шифрування для захисту цінної інформації від несанкціонованого доступу. [21]

У процесі організації системи безпеки провайдер і клієнт повинні враховувати наступні основні вразливості хмарних систем:

1 Складність контролю та управління хмарами

Необхідно упевнитися, що всі ресурси хмари інвентаризовані і в ньому немає неконтрольованих віртуальних машин, що не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари. Це високорівнева тип вразливостей, тому він пов'язаний з керованістю хмарою, як єдиною інформаційною системою і для нього загальну захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

2 Труднощі при переміщенні звичайних серверів в віртуальне середовище

Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Однак віртуалізація систем хмарних обчислень і перехід до хмарних середовищ призводять до появи нових загроз і вразливостей.

Доступ через Інтернет до управління обчислювальною потужністю - одна з ключових характеристик хмарних обчислень. У більшості традиційних систем хмарних обчислень доступ інженерів до серверів контролюється на фізичному рівні, в хмарних середовищах вони працюють через Інтернет. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одним з головних критеріїв захисту.

3. Динамічність віртуальних машин [21]

Високошвидкісна мінливість внутрішньої інфраструктури сильно ускладнює розробку цілісної системи безпеки. Уразливості операційної системи або додатків у віртуальному середовищі поширюються безконтрольно і часто виявляються не відразу, а через певний проміжок часу (наприклад, при відновленні з резервної копії). У середовищах хмарних обчисленнях важливо надійно зафіксувати певний рівень захисту системи. При цьому він не повинен залежати від поточного стану використовуваних сегментів.

4. Уразливості всередині віртуального середовища

Сервери хмарних обчислень і локальні сервери використовують одні й ті ж операційні системи та програми. Для хмарних систем загроза віддаленого злому або зараження шкідливим програмним забезпеченням висока. Ризик для віртуальних систем також високий. Паралельні віртуальні машини збільшує «площу атаки». Система виявлення та запобігання вторгнень повинна бути здатна виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарному середовищі.

5. Непрацюючі віртуальні машини

Коли віртуальна машина вимкнена, вона наражається на небезпеку зараження. Для здійснення атаки достатньо доступу до сховища образів віртуальних машин через мережу. На виключеною віртуальній машині абсолютно неможливо запустити захисне програмне забезпечення. В даному випадку повинна бути реалізована захист не тільки всередині кожної віртуальної машини, але і на рівні гіпервізора.

6. Відсутність периметра і розмежування мережі

При використанні хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що захист менш захищеної частини мережі визначає загальний рівень захищеності. Для розмежування сегментів з різними рівнями довіри в хмарі віртуальні машини повинні самі забезпечувати себе захистом, переміщаючи мережевий периметр до самої віртуальній машині. Корпоративний брандмауер як основний компонент для впровадження політики інформаційної безпеки та розмежування сегментів мережі не в змозі вплинути на сервери, розміщені в хмарних системах. [22]

1.6 Загальні відомості про захист даних при їх обробці хмарними сервісами

Доступ до хмарних ресурсів відбувається з клієнтських машин, на яких встановлено спеціальне програмне забезпечення для доступу або універсальний клієнт - браузер. На робочому місці можуть бути встановлені й інші програми, які можуть втручатися в роботу клієнта, перехоплюючи передачу інформації або нав'язуючи власну поведінку браузеру (наприклад, за допомогою сценаріїв JavaScript). Таким чином, першим вразливим місцем хмарної інфраструктури, як це не дивно, є клієнт.

Слід зазначити, що атаки на клієнтські програми вже добре відпрацьовані в веб-середовищі, але вони актуальні і для хмари, оскільки клієнти підключаються до хмари, як правило, за допомогою браузера. До цього класу атак можна віднести такі атаки, як троянські програми, міжсайтовий скриптинг, перехоплення веб-сесій, крадіжка паролів та ін. Власне, до цих типів атак відносяться також вірусні епідемії, які завантажили троянців, експлуатація вразливостей клієнтської операційної системи і додатків, впровадження стороннього коду у веб-додаток або в операційну систему.

Збереження даних. Оптимальною захистом конфіденційних даних, що знаходяться в сховищі, є використання різних технологій шифрування. Щоб запобігти спробам несанкціонованого доступу, провайдери повинні шифрувати дані від клієнтів, що зберігаються на їхніх серверах. Якщо ж дані стають непотрібними, провайдери повинні забезпечувати їх безповоротне видалення.

Захист інформації в процесі її передачі. Зашифрована повинна бути і передана інформація, доступ до якої можна отримати лише після процедури аутентифікації. Подібні заходи виступають гарантією того, що дані не будуть змінені або прочитані неуповноваженими на те особами. У цій сфері існує маса розроблених протоколів і алгоритмів з високим ступенем надійності, тому провайдерам немає необхідності винаходити щось своє.

Аутентифікація. Найпоширеніший спосіб аутентифікації - парольний захист. Однак з метою забезпечення більш високої надійності багато провайдерів пропонують скористатися токенами або сертифікатами. Також доцільним буде забезпечити взаємодію провайдера з системою аутентифікації користувачів клієнта, щоб інформація про список авторизованих користувачів із зазначенням їх повноважень оновлювалася в онлайн режимі.

Ізоляція користувачів. Для відділення додатків і даних одного клієнта від інших, оптимальним буде використання кожним клієнтом своєї віртуальної машини і своєї віртуальної мережі. Варіант, коли дані всіх клієнтів розміщуються в єдиній програмному середовищі і ізолюються одна від одної шляхом змін в коді, не забезпечує належного рівня надійності, оскільки код може містити помилку або пролом, в результаті чого дані одного клієнта зможуть побачити інші.

Оформлення нормативно-правових питань. Провайдери повинні строго слідувати прописаним правилами і дотримуватися чіткої стратегії у правовій сфері. Особливо це відноситься до питань експорту даних та забезпечення їх безпеки, збереження, а також до питань розкриття інформації.[23]

Реакція на інциденти. У разі виникнення непередбачених обставин провайдери повинні дотримуватися апріорі задокументованих правил, виявляючи інциденти, мінімізуючи їхні наслідки і повідомляючи користувачів про поточний стан справ.

Контроль цілісності - відстеження змін у файлах, системі і реєстрі.

Контроль цілісності операційної системи і додатків дозволяє виявити небезпечні зміни, які є наслідком компрометації системи. Ця підсистема включає в себе:

– перевірку за запитом або розкладом;

– всебічний контроль властивостей файлів, включаючи атрибути;

– контроль на рівні директорій;

– гранульовану настройку об'єктів контролю;

– звіти для аудиту.

Аналіз журналів - виявлення істотних подій з точки зору інформаційної безпеки в файлах журналів. Аналіз журналів збирає та аналізує журнали роботи операційної системи і додатків на предмет подій безпеки. Правила аналізу журналів дозволяють виявити значущі події у величезному масиві записів. Це:

– виявлення підозрілої поведінки;

– збір дій адміністратора, що мають відношення до безпеки;

– наскрізний збір подій з усього ЦОД.[24]

Захист від шкідливих програм, що враховує віртуалізацію - антивірус, адаптований для використання у віртуальному середовищі.

Захист від шкідливих програм, що враховує віртуалізацію, використовує спеціальні програмні інтерфейси, які надає гіпервізор, такі як VMsafe компанії VMware, [25] для захисту як активних, так і бездіяльних ВМ. Захист включає в себе як рівень перевірки самих віртуальних машин, так і агента всередині кожної ВМ, що забезпечують перевірку в реальному часі. Такий підхід гарантує, що ВМ очищена, навіть якщо була неактивна, а також актуальність її захисту при подальшому запуску. Не менш важливою властивістю захисту, спеціалізованої для захисту ВМ є дбайливе ставлення до обчислювальних ресурсів при перевірці всієї системи. Це:

– запобігання загрозам з боку шкідливого коду для активних і бездіяльних машин;

– захист від шкідливих програм, який деінсталює або блокують роботу антивіруса;

– інтеграція з панеллю керування системою;

– автоматичне налаштування захисту нових ВМ.[26]

1.7 Управління неперервністю бізнесу

Управління неперервністю бізнесу (Business Continuity Management або УНБ) - бізнес-процес, що відповідає за управління ризиками, які можуть серйозно вплинути на бізнес. [27] УНБ захищає інтереси ключових зацікавлених сторін, репутацію, бренд і діяльність по створенню цінності. Процес УНБ включає в себе зниження ризиків до прийнятного рівня і планування способів відновлення бізнес-процесів у разі порушення бізнесу. УНБ встановлює цілі, охоплення і вимоги по відношенню до Управління неперервності IT-послуг.

Управління безперервністю бізнесу є важливим стратегічним завданням. Будь-яка нештатна ситуація може призвести до тимчасового припинення діяльності компанії, а, отже, до серйозних фінансових збитків і втрати довіри з боку партнерів і клієнтів.

Особливу нішу серед систем управління безперервністю бізнесу займають катастрофостійкі рішення, які дають можливість прогнозувати і запобігати серйозним втратам у випадку надзвичайних ситуацій: пожеж, повеней та ін.

План забезпечення неперервності бізнесу (Business Continuity Plan або BCP) – план, який визначає кроки, необхідні для відновлення бізнес-процесів у разі порушення їх функціонування. План також повинен містити інформацію про події, які є підставою для його ініціювання; людей, які мають бути задіяні в реалізації плану; засобах комунікацій тощо.

Корпоративна програма управління неперервністю бізнесу повинна включати в себе наступні етапи:

– аналіз бізнес-процесів предметної області (Business Environment Analysis, BEA) - виділення та ранжування значущих для бізнесу процесів і визначення вимог до них по неперервності;

– аналіз ризиків (Risk Analysis, RA) - оцінка і ранжування значущих загроз і вразливостей неперервності бізнес-процесів, а також оцінка достатності існуючих організаційних і технічних заходів попередження переривань бізнесу;

– оцінка впливу на бізнес (Business Impact Analysis, BIA) - аналіз впливу бізнес-процесів на весь бізнес в цілому і визначення цілей відновлення кожного бізнес-процесу разом з підтримуючою його інфраструктурою;

– визначення стратегії неперервності бізнесу (Business Continuity Strategy definition) - фіксація цільового часу відновлення (recovery time objective, RTO) і цільової точки відновлення (recovery point objective, RPO) для кожного бізнес-процесу, вибір відповідних організаційних і технічних рішень;

– Розробка та супровід планів неперервності бізнесу (Business Continuity Plan, BCP) і відновлення інфраструктури в надзвичайних ситуаціях (Disaster Recovery Plan, DRP) для документального оформлення належних рішень;

– створення технічної та організаційної систем управління неперервністю бізнесу;

– формування адекватної програми супроводу та експлуатації корпоративної програми УНБ, зокрема, визначення програми обізнаності з питань забезпечення неперервності бізнесу.

У тому чи іншому вигляді всі ці етапи описуються в стандартах УНБ, прийнятих в різних країнах: практики неперервності бізнесу британського інституту BCI (Business Continuity Institute), американських інститутів DRI (Disaster Recovery Institute) і SANS (SysAdmin, Audit, Network, Security Institute); стандарти і специфікації Британського інституту стандартів (British Standard Institute, BSI); керівництва Австралійської національної агенції аудиту (ANAO); розділ міжнародного стандарту з інформаційної безпеки ISO / IEC 27001; стандарти і бібліотеки COBIT, ITIL, MOF в частині неперервності бізнесу та ін.

Управління неперервністю фокусується на значущих негативних подіях, так званими "катастрофами" для бізнесу. Менш значимі події розглядаються в рамках процесу управління інцидентами. Те, чи є якесь конкретне подія катастрофою, залежить від організації, в якій воно відбулося. Розмір і значимість негативного впливу події на бізнес, наприклад, фінансові втрати або втрата репутації, вимірюється в рамках аналізу впливу на бізнес. Аналіз впливу на бізнес визначає мінімальні вимоги до критичності, конкретні вимоги до технологій і послуг визначаються в рамках управління неперервністю.

Аналіз впливу на бізнес (Business Impact Analysis або BIA) - діяльність у рамках процесу Управління неперервністю бізнесу, яка визначає критичні бізнес-функції і їх залежність від чинників оточення. Цими факторами можуть бути постачальники, люди, інші бізнес-процеси, послуги тощо [28]. BIA визначає наслідки втрати послуг для бізнесу. Втрати можуть бути значними, наприклад, великі фінансові втрати, і "м'якими" - моральні втрати, втрата репутації, конкурентної переваги і т.п.

Аналіз впливу на бізнес визначає форму, яку може набувати руйнування або втрата, наприклад:

– втрачений дохід;

– додаткові витрати;

– шкоди репутації;

– втрата прихильності клієнтів;

– втрата конкурентної переваги;

– пошкодження і порушення здоров'я, законності та безпеки;

– ризик безпеки персоналу;

– втрата ринку збуту в короткостроковому і довгостроковому періодах;

– втрата операційних можливостей, наприклад, контролю.

Аналіз впливу на бізнес визначає, як будуть збільшуватися негативні наслідки руйнування або втрати після несприятливої події, а також час доби, тижня, місяця, коли вони будуть найбільш серйозними; кадрове забезпечення, навички, апаратура та послуги, які необхідні для підтримки мінімальних рівнів

неперервності критичних бізнес-процесів; часові рамки, в межах яких необхідно забезпечити мінімальний рівень відновлення кадрового забезпечення, апаратури, послуг та інших можливостей; часові рамки, в межах яких необхідно повністю відновити критичні бізнес-процеси і підтримують їх кадрове забезпечення, апаратуру, послуги та інші можливості; пріоритети відновлення для послуг.

Результати аналізу впливу на бізнес і оцінки ризиків є основою для побудови стратегії неперервності послуг відповідно до потреб бізнесу. Більшість організацій повинні дотримуватися балансу зменшення ризиків і формування механізмів відновлення. Як би добре не проводилися дії щодо зменшення ризиків, неможливо виключити їх усі. Тому завжди необхідно впроваджувати механізми відновлення в інтеграції з процесом управління доступністю, оскільки саме доступність послуг постраждає в першу чергу при виникненні неприємних для бізнесу подій. Типові заходи зменшення ризиків включають в себе:

– інсталяція UPS і резервного живлення для комп'ютерів;

– забезпечення відмовостійкості систем з критичними додатками, для яких неприйнятний будь-який простий (наприклад, банківська система);

– використання RAID і дзеркальних дисків для серверів для уникнення втрати інформації та забезпечення неперервності роботи;

– наявність запасних компонентів / устаткування, які будуть використані у разі збою основних. Наприклад, запасний сервер з мінімально необхідною конфігурацією, який буде задіяний в найкоротший час у разі відмови основного сервера;

– усунення SPOFов, наприклад, єдиної точки доступу в мережу або єдиної точки електроживлення;

– використання надійних IT-систем і мереж;

– аутсорсинг послуг декільком постачальникам послуг;

– збільшення контролю над безпекою;

– збільшення контролю над виявленням порушень в роботі послуг;

– всеосяжна стратегія відновлення і резервного копіювання, що включає в себе зовнішнє зберігання. Зовнішнє зберігання передбачає регулярне (найчастіше щоденне) копіювання критичної інформації у зовнішнє сховище.

Перераховані вище заходи не вирішать всі проблеми, але їх використання дозволить сильно скоротити ризик втрат для бізнесу в разі виникнення непередбачених обставин.

Опції відновлення, які повинні бути враховані при формуванні стратегії:

– перехід на ручну роботу. Для деяких типів послуг може стати гарною альтернативою на короткий період до відновлення послуги. Наприклад, Сервіс-деск може працювати якийсь час з паперовими заявками і журналами;

– взаємні угоди. Припускають укладання угод між організаціями, які використовують схожі технології. В даний час є неприйнятними для більшості IT-систем, але можуть використовуватися в окремих випадках - наприклад, для зовнішнього резервного копіювання або використання принтерів;

– поступове відновлення (Gradual Recovery). Передбачається відновлення послуги протягом більш ніж 72 годин. При поступовому відновленні зазвичай задіяний мобільний або стаціонарний резервний центр, оснащений елементами життєзабезпечення і мережевий розводкою, без комп'ютерних систем. Ця опція відновлення рекомендована для некритичних послуг, надання яких може бути затримано на дні і тижні без значного впливу на бізнес;

– проміжне відновлення (Intermediate Recovery). Передбачається відновлення послуги протягом 24-72 годин. При проміжному відновленні зазвичай використовується загальний мобільний або стаціонарний резервний центр, оснащений комп'ютерними системами і мережевими компонентами. Конфігурування апаратного та програмного забезпечення, а також відновлення даних виконуються в рамках Плану забезпечення неперервності послуг. Дана опція відновлення зазвичай пропонується третіми сторонами, які мають для цього все необхідне обладнання та кваліфікований персонал. Вартість цієї опції відновлення залежить від ресурсів третьої сторони, які мають бути задіяні для відновлення, а також від часу, протягом якого потрібно відновити послугу.

Перевагою даного методу є його прозорість для користувачів. Недоліком - те, що інформація (в тому числі конфіденційна) буде зберігатися у сторонньої організації. Останнє робить неприйнятним даний спосіб відновлення для багатьох організацій;

– швидке відновлення (Fast Recovery). Передбачається відновлення послуги за короткий проміжок часу, зазвичай менше 24 годин. При швидкому відновленні зазвичай використовується виділений стаціонарний резервний центр з комп'ютерними системами і ПЗ, сконфігурованими для роботи послуг. Негайне відновлення може займати до 24 годин, якщо потрібне відновлення даних резервного копіювання;

– негайне відновлення (Immediate recovery). Передбачається відновлення послуги без переривання послуги. Негайне відновлення зазвичай використовує технології зеркалирования, балансування завантаження і поділу майданчиків встановлення обладнання. Цей спосіб найчастіше передбачає "подвійну локацію" компонентів системи, тобто повне дублювання. Він є найдорожчим і застосовується тільки для критичних бізнес-процесів, простий яких може мати значний негативний вплив на бізнес. Копії повинні бути розташовані на максимальному видаленні від оригіналів, щоб не бути зачепленим руйнуючим подією. [29]

Стратегія забезпечення неперервності повинна включати в себе всі розглянуті вище способи відновлення. Різні послуги, що використовуються організацією, вимагають різних підходів до відновлення і зменшення ризиків збою. Яка б опція ні вибиралася, вона повинна бути економічно ефективною. Головне правило - чим довше бізнес може обходитися без послуги, тим дешевше має бути рішення щодо забезпечення її неперервності.

Одним з найбільш важливих джерел інформації для формування планів є Аналіз впливу на бізнес. Інші області також повинні бути проаналізовані: SLA, вимоги безпеки, інструкції експлуатації, процедури, зовнішні контракти.

Управління неперервністю бізнесу ґрунтується на наступних ключових принципах:

– попередження інцидентів - захист послуг ІКТ від таких загроз, як несприятливий вплив зовнішнього середовища і апаратні збої, операційні помилки, зловмисні атаки і природні лиха, є вкрай важливою для підтримки бажаних рівнів доступності систем в організації;

– виявлення інцидентів - найшвидше виявлення інцидентів буде зводити до мінімуму їх вплив на послуги, скорочувати роботи з відновлення та зберігати якість послуг;

– реагування - реагування на інцидент найбільш підходящим способом призведе до більш ефективному відновленню і зменшить будь простої. Невдале реагування може призвести до переростання незначного інциденту в щось більш серйозне;

– відновлення - визначення та реалізація відповідної стратегії відновлення буде забезпечувати впевненість у своєчасному відновленні послуг та підтримки цілісності даних. Розуміння пріоритетів відновлення дозволить відновлювати в першу чергу найбільш критичні послуги. Послуги, що носять менш критичний характер, можуть відновлюватися пізніше або, за деяких умов, взагалі не відновлюватися;

– вдосконалення - уроки, засвоєні з реагування на дрібні і великі інциденти, повинні документуватися, аналізуватися і переглядатися. Розуміння цих уроків дасть можливість організації краще готуватися, контролювати і уникати інцидентів і порушенні.

Менеджмент неперервності бізнесу (МНБ) - це цілісний управлінський процес, що ідентифікує потенційні впливу, які загрожують неперервності бізнес діяльності організації, і забезпечує основу для створення стійкості та можливості ефективного реагування, що забезпечує захист інтересів організації від порушень (Рисунок 1.2).

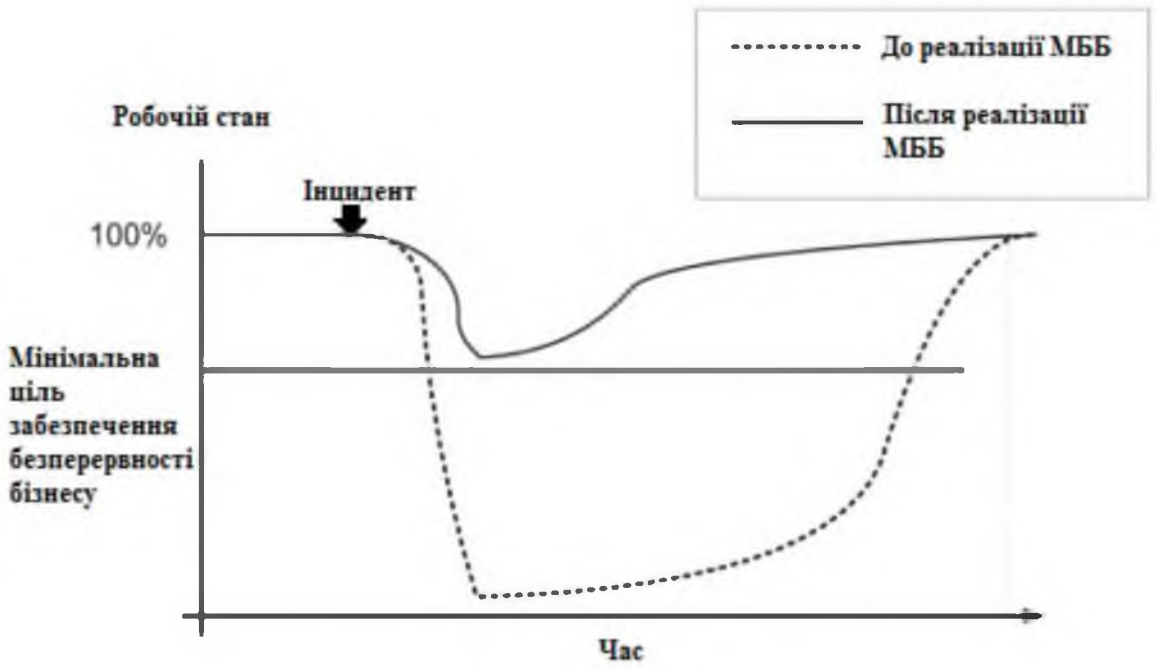

Рисунок 1.2 – Концепція готовності інформаційної системи до забезпечення безперервності бізнесу

Готовність інформаційно-комунікаційних технологій до забезпечення неперервності бізнесу (ГІКТЗНБ) відноситься до системи менеджменту, яка доповнює і підтримує програму МНБ і (або) СМІБ організації для підвищення готовності організації до:

– реагування на постійно змінюється середу ризику;

– забезпечення впевненості в продовженні критичних операцій бізнесу, підтримуваних пов'язаними з ними послугами ІКТ;

– реагуванню при виявленні одного або серії взаємопов'язаних подій, які стають інцидентами, до виникнення порушень послуг ІКТ;

– реагування на інциденти / лиха і відмови, а також до відновлення після них.

Рисунок 1.3 ілюструє, яким чином відповідний елемент ГІКТЗНБ підтримує типову тимчасову послідовність відновлення роботи після лиха і, в свою чергу, підтримує діяльність щодо забезпечення неперервності бізнесу. Реалізація ГІКТЗНБ дає можливість організації ефективно реагувати на нові і

виникаючі загрози, а також реагувати на порушення і відновлюватися після них.

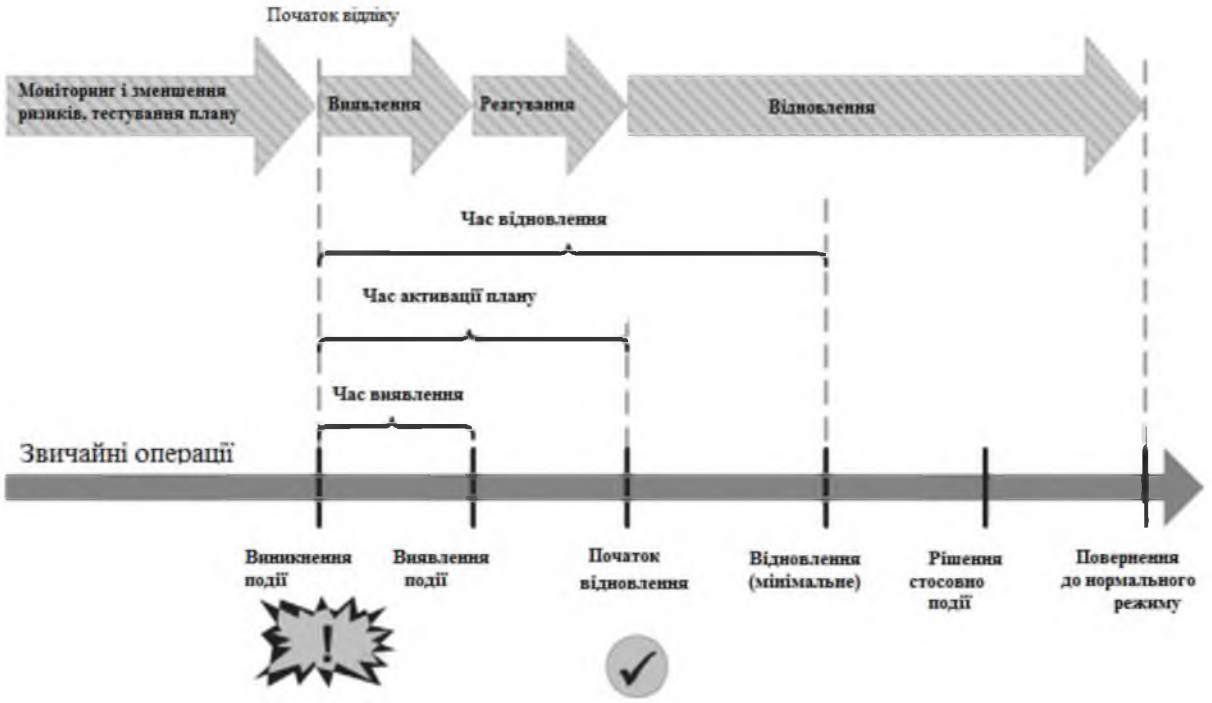

Рисунок 1.3 – Принципи забезпечення неперервності ведення бізнесу на типовій шкалі відновлення після події

Ключові елементи ГІКТЗНБ можна узагальнити наступним чином:

– кадри: фахівці, що володіють відповідними навичками і знаннями, і компетентний резервний персонал;

– споруди: фізичне середовище, в якій розташовані ресурси ІКТ;

– технічне оснащення:

– апаратні засоби (включаючи стійки, сервери, дискові масиви, накопичувачі на магнітній стрічці й прилади);

– мережі (включаючи послуги передачі даних і голосу), комутатори і маршрутизатори;

– програмні засоби, включаючи операційну систему і прикладні програми, зв'язок або інтерфейси між прикладними програмами і підпрограми пакетної обробки даних;

– дані: дані прикладних програм, голосові дані та інші види даних;

– процеси: відновлення і підтримки послуг ІКТ, включаючи підтримуючу документацію для опису конфігурації ресурсів ІКТ та створення можливості ефективного функціонування;

– постачальники: компоненти ланцюга постачання послуг, де надання послуг ІКТ залежить від зовнішнього постачальника послуг або другої організації, що беруть участь в ланцюгу поставок, наприклад, постачальник даних з фінансових ринків, постачальник телекомунікаційних послуг або постачальник послуг Інтернету.

Вигоди ефективної ГІКТЗНБ для організації полягають у тому, що організація:

– розуміє ризики по відношенню до неперервності послуг ІКТ та їх вразливості;

– визначає потенційний вплив порушення послуг ІКТ;

– сприяє поліпшенню співпраці між керівниками бізнесу та постачальниками її послуг ІКТ (внутрішніми і зовнішніми);

– розвиває і підвищує компетентність персоналу ІКТ шляхом демонстрації реагування допомогою проведення тренувань за планами забезпечення неперервності бізнесу, тестування механізмів ГІКТЗНБ;

– забезпечує вищому керівництву впевненість у тому, що воно може розраховувати на заздалегідь певні рівні послуг ІКТ та отримувати адекватну підтримку і засоби повідомлення у випадку аварії;

– забезпечує вищому керівництву впевненість у належному збереженні рівня інформаційної безпеки (конфіденційність, цілісність і доступність) при забезпеченні строгого проходження політикам інформаційної безпеки;

– надає додаткову впевненість у стратегії забезпечення неперервності бізнесу, пов'язуючи інвестиції в інформаційні технології до потреб бізнесу і забезпечуючи захист послуг ІКТ на відповідному рівні з урахуванням їх значимості для організації;

– використовує рентабельні послуги ІКТ, а не послуги з недостатнім або надмірним фінансуванням, завдяки розумінню рівня залежності організації від цих послуг ІКТ та характеру, місця розташування, взаємозалежність і використання компонентів, що складають послуги ІКТ;

– може покращувати свою репутацію щодо передбачливості та ефективності;

– потенційно отримує конкурентну перевагу завдяки продемонстрованої здатності забезпечувати неперервність бізнесу і підтримувати надання послуг і продуктів під час порушення; і розуміє і документує очікування причетних сторін, їх зв'язок з послугами ІКТ та їх використання.

Рисунок 1.4 – Застосування циклу «планування - здійснення - перевірка - дія» (PDCA)

Щоб організація досягла ГІКТЗНБ, їй необхідно ввести систематичний процес попередження, прогнозування та менеджменту порушень ІКТ та інцидентів, що володіють можливістю порушення послуг ІКТ. Найкраще цього можна досягти шляхом застосування фаз циклу «Планування - Здійснення - Перевірка – Дія» (PDCA - Plan-Do-Check-Act) як частини системи менеджменту

в ГІКТЗНБ (Рис. 1.4). Таким способом ГІКТЗНБ буде підтримувати менеджмент неперервності бізнесу, забезпечуючи впевненість у відповідній стійкості послуг ІКТ та можливості їх відновлення до заздалегідь визначених рівнів в рамках тимчасових термінів, необхідних і узгоджених організацій.[28]

1.8 Висновок. Постановка задачі

За результатами аналізу технологій роботи систем хмарних обчислень та загальних принципів та задач забезпечення неперервності ведення бізнесу можна зробити ряд висновків:

1) готовність інформаційно-комунікаційних технологій до забезпечення неперервності бізнесу є критично важливим фактором для систем розподілених обчислень;

2) для реалізації ефективного менеджменту неперервності бізнесу (МНБ) слід врахувати наступні важливі фактори:

– усвідомлення потреби у забезпеченні неперервності бізнесу і потреби у встановленні політики та цілей у сфері неперервності бізнесу;

– впровадження та здійснення засобів і заходів з управління сукупним ризиком при забезпеченні неперервності бізнесу організації;

– проведення моніторингу та аналізу ефективності МНБ;

– постійне поліпшення, засноване на достовірних і об'єктивних вимірах;

3) в рамках програми МНБ організація повинна визначити категорію своїх видів діяльності відповідно до їх пріоритетів для забезпечення неперервності (як визначено аналізом впливу на бізнес) і визначити мінімальний рівень, на якому повинна виконуватися кожна критична діяльність при її поновленні;

4) організація повинна визначити потребу в програмі ГІКТЗНБ, виходячи із загальних цілей менеджменту неперервності бізнесу, а також визначити та забезпечити ресурси, необхідні для встановлення, реалізації, функціонування та підтримки такої програми.

Враховуючи результати аналізу особливостей функціонування хмарних систем та вимоги до забезпечення безпеки систем хмарних обчислень в даній роботі необхідно виконати наступні задачі:

– розробити політику забезпечення неперервності бізнесу центрів обробки даних провайдера хмарних обчислень;

– виявити загрози безпеці інформації, що обробляється з використанням технологій;

– розробити рекомендації, направлені на удосконалення готовності інформаційно-комунікаційних технологій до забезпечення неперервності бізнесу надання послуг розподілених обчислень.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Щоб готовність ІКТ до забезпечення неперервності бізнесу (ГІКТЗНБ) була ефективною, вона повинна бути повністю інтегрована з управлінською діяльністю верхньої ланки організації, схваленим і підтриманим вищим керівництвом. Для підтримки та менеджменту програми ГІКТЗНБ може знадобитися ряд фахівців з практичним досвідом в області ГІКТЗНБ і персонал інших провідних напрямків діяльності та служб. Кількість ресурсів, необхідних для підтримки такої програми, буде залежати від величини і складності організації.

Організація повинна мати документально оформлену політику МНБ. Спочатку це може бути високорівневий документ, що уточнюється і розширюється при досягненні зрілості всього процесу ГІКТЗНБ. Політика повинна регулярно перевірятися і оновлюватися відповідно до потреб організації і повинна узгоджуватися з більш великими цілями менеджменту неперервності бізнесу організації.

Політика ГІКТЗНБ повинна надавати організації документально оформлені принципи, до виконання яких вона прагнутиме і за якими може вимірюватися ефективність ГІКТЗНБ. Політика має:

– встановлювати і демонструвати зацікавленість вищого керівництва в програмі ГІКТЗНБ;

– включати цілі ГІКТЗНБ організації або посилатися на них;

– визначати область застосування ГІКТЗНБ, включаючи обмеження і виключення;

– затверджуватися і схвалюватися вищим керівництвом;

– доводитися до відома відповідних внутрішніх і зовнішніх причетних сторін;

– визначити та забезпечити для відповідних структур доступність ресурсів, таких як бюджетні кошти; персонал, необхідний для здійснення діяльностей у відповідності з політикою ГІКТЗНБ;

– піддаватися перевірці через заплановані інтервали часу і в разі виникнення значних змін, таких як зміни зовнішнього середовища, зміни бізнесу і структури організації.

2.1 Вимоги до ГІКТЗНБ в менеджменті неперервності бізнесу

Організація повинна визначити область застосування МНБ і встановити цілі в області неперервності бізнесу, з урахуванням:

– вимог до забезпечення неперервності бізнесу;

– цілей і зобов'язань організації;

– прийнятного рівня ризику;

– встановлених законодавчих, обов'язкових і договірних вимог;

– інтересів її ключових причетних сторін.

Вище керівництво повинно встановити політику в області неперервності бізнесу і демонструвати виконання прийнятих зобов'язань по відношенню до неї.

Вхідні в МНБ діяльності включають забезпечення готовності до інцидентів, менеджмент неперервності операцій, планування відновлення після лиха (DRP - disaster recovery planning) і зменшення ризику, які зосереджені на підвищенні стійкості організації та її підготовці до ефективного реагування на інциденти, а також на відновленні після них в рамках заздалегідь певних часових шкал.

Таким чином, організація чітко розставляє свої пріоритети щодо МНБ , і саме ними керуються в діяльності ГІКТЗНБ. У свою чергу, МНБ залежить від ГІКТЗНБ в забезпеченні впевненості в тому, що організація може досягти своїх загальних цілей щодо забезпечення неперервності в будь-який час, особливо під час порушення.

ГІКТЗНБ, ймовірно, буде більш ефективною і рентабельною, коли вона спроектована і вбудована в послуги ІКТ з самого початку, як частина стратегії ГІКТЗНБ, що підтримує цілі забезпечення неперервності бізнесу організації. Це забезпечить впевненість у тому, що послуги ІКТ будуть краще створені, краще зрозумілі і більш стійкі. Зміна ГІКТЗНБ може бути складною, зухвало порушення й дорого коштують завдання.

Організація повинна розробляти, реалізовувати, підтримувати і постійно вдосконалювати сукупність документально оформлених процесів, які будуть підтримувати ГІКТЗНБ.

Ці процеси повинні забезпечувати впевненість у тому, що цілі ГІКТЗНБ чітко викладені, зрозумілі і доведені до відома, а також демонструвати зацікавленість вищого керівництва в ГІКТЗНБ.

Ці процеси повинні забезпечувати впевненість у тому, що цілі ГІКТЗНБ чітко викладені, зрозумілі і доведені до відома, а також демонструвати зацікавленість вищого керівництва в ГІКТЗНБ.

Щоб програма ГІКТЗНБ була ефективною, вона повинна бути процесом, повністю інтегрованим з управлінською діяльністю верхньої ланки організації, схваленим і підтриманим вищим керівництвом. Для підтримки та менеджменту програми ГІКТЗНБ може знадобитися ряд фахівців з практичним досвідом в області ГІКТЗНБ і персонал інших провідних напрямків діяльності та служб. Кількість ресурсів, необхідних для підтримки такої програми, буде залежати від величини і складності організації.

Основним завданням етапу планування є встановлення вимог готовності ІКТ організації, включаючи:

– стратегія і план ГІКТЗНБ, необхідні для підтримки бізнесу, законні (засновані на законі) нормативно-правові вимоги, пов'язані з певною сферою діяльності та досягненням цілей і завдань неперервності бізнесу організації;

– критерії ефективності, необхідні організації для моніторингу ступеня готовності ІКТ, яка потрібна для досягнення цих завдань і цілей.

В рамках політики організація повинна визначити потребу в програмі ГІКТЗНБ, виходячи із загальних цілей менеджменту неперервності бізнесу, а також визначити та забезпечити ресурси, необхідні для встановлення, реалізації, функціонування та підтримки такої програми ГІКТЗНБ.

Повинні визначатися і документуватися пов'язані з ГІКТЗНБ ролі, обов'язки, компетентність і повноваження.

В рамках програми МНБ організація повинна визначити категорію своїх видів діяльності відповідно до їх пріоритетів для забезпечення неперервності (як визначено аналізом впливу на бізнес) і визначити мінімальний рівень, на якому повинна виконуватися кожна критична діяльність при її поновленні. Вище керівництво повинно узгодити вимоги неперервності бізнесу організації, виходячи з яких буде задано час відновлення (ЗЧВ) і задана точка відновлення (ЗТВ) для мінімальної мети забезпечення неперервності бізнесу (ММНБ) на продукт, послугу або вид діяльності. Це ЗЧВ починається з моменту виникнення порушення до відновлення продукту, послуги або діяльності.

Існує цілий ряд послуг ІКТ, які можуть вважатися критичними і необхідними для забезпечення відновлення. Для кожної з цих критичних послуг ІКТ повинні бути задані і документально оформлені заданий час відновлення (ЗЧВ) і задані точки відновлення (ЗТВ) для мінімальної мети забезпечення неперервності бізнесу (ММНБ) послугами ІКТ. (Це може включати такі аспекти наданих послуг ІКТ, як служба технічної підтримки.) ЗЧВ критичних послуг ІКТ незмінно буде значно менше, ніж ЗЧВ неперервності бізнесу.

Організація повинна визначити і документально оформити свої критичні послуги ІКТ, включаючи короткі описи і назви, значимі для організації на рівні користувача послуг. Це забезпечить загальне розуміння послуг ІКТ персоналом, що має відношення до бізнесу та ІКТ, так як для однієї і тієї ж послуги ІКТ можуть використовуватися різні назви. Для кожної перерахованої критичної послуги ІКТ необхідно визначити підтримуваний нею продукт або послугу організації, і вище керівництво має погодити послуги ІКТ та пов'язані з ними вимоги ГІКТЗНБ.

Для кожної визначеної і узгодженої критичної послуги ІКТ повинні бути описані і задокументовані всі компоненти ІКТ в ланцюжку поставки послуги, показуючи, яким чином вони конфігуруються або зв'язуються для надання кожної послуги. Повинні бути документально оформлені зміни як звичайного середовища поставки послуг ІКТ, так і середовища поставки послуг забезпечення неперервності ІКТ.

Для кожної критичної послуги ІКТ поточні можливості забезпечення неперервності (наприклад, існування єдиної точки відмови) слід переглядати з профілактичною точки зору, щоб оцінити ризики переривання або погіршення послуг (оцінка може бути зроблена як частина загальної оцінки ризику в МНБ). Слід також шукати можливості підвищення стійкості послуг ІКТ і, таким чином, зниження ймовірності та (або) впливу порушення послуг. Це також може надати більше значення можливості раннього виявлення порушень послуг ІКТ та реагування на них. Організація може прийняти рішення, якщо існує бізнес-обґрунтування щодо вкладання коштів у встановлені можливості для підвищення стійкості послуг. Така оцінка ризику послуг (яка може стати частиною загальної структури менеджменту ризику організації) може також призвести до уточнення бізнес-обґрунтування для розширення можливостей відновлення послуг ІКТ.

Для кожної критичної послуги ІКТ слід порівнювати використовувані механізми забезпечення готовності ІКТ, такі як попередження, моніторинг, виявлення, реагування та відновлення, з вимогами неперервності бізнесу і документувати будь-які розбіжності.

Вище керівництво повинно бути проінформоване про будь-які розбіжності між критичними можливостями ГІКТЗНБ та вимогами неперервності бізнесу. Такі розбіжності можуть вказувати на ризики та потребу в додаткових ресурсах для забезпечення стійкості і відновлення, таких як:

– персонал, включаючи кількість, навички та знання;

– приміщення для розміщення засобів ІКТ, наприклад, машинний зал;

– підтримуюча технологія, апаратура, обладнання та мережі (технологія);

– інформаційні прикладні програми і бази даних;

– розподіл фінансових або бюджетних коштів;

– зовнішні послуги та постачальники (поставки).

Стратегії ГІКТЗНБ повинні визначати підходи до реалізації необхідної стійкості, щоб вводилися принципи попередження інцидентів, виявлення, реагування, відновлення та поновлення.

Необхідно оцінювати повний спектр варіантів стратегій ГІКТЗНБ. Обрані стратегії повинні бути здатні підтримувати вимоги забезпечення неперервності бізнесу організації.

При розробці стратегії організація повинна враховувати реалізацію і поточну потребу в ресурсах. Може бути укладений договір із зовнішніми постачальниками про надання послуг фахівців та передачі досвіду, що відіграє важливу роль у підтримці стратегії.

Стратегія ГІКТЗНБ повинна бути достатньо гнучкою, щоб задовольняти різним стратегіям бізнесу в умовах ринкових відносин. Крім того, стратегія повинна враховувати такі внутрішні обмеження і фактори, як:

– бюджет;

– доступність ресурсів;

– потенційні витрати і вигоди;

– технологічні обмеження;

– готовність організації ризикувати;

– існуюча стратегія ГІКТЗНБ організації;

– нормативні зобов'язання.

Організація повинна розглянути спектр варіантів для забезпечення готовності до інцидентів своїх критичних послуг ІКТ. Варіанти повинні враховувати посилення захисту і стійкості, а також забезпечення відновлення і відновлення після незапланованого порушення і можуть включати внутрішні механізми, послуги, що надаються організацією, та послуги, що надаються ззовні одне або кількома третіми сторонами.

Варіанти повинні враховувати різні компоненти, необхідні для забезпечення впевненості в неперервності та відновленні критичних послуг ІКТ.

Організація повинна визначити відповідні стратегії для підтримки основних знань і навичок щодо ІКТ. Це може також поширюватися на персонал підрядчиків та інших причетних сторін, що володіють великими спеціальними навичками і знаннями, пов'язаними з ІКТ. Стратегії захисту або забезпечення таких навичок можуть включати:

– документування способу виконання критичних послуг ІКТ;

– різнобічну підготовку персоналу ІКТ та підрядників для підвищення надмірності навичок;

– поділ основних навичок для зниження концентрації ризику (це може привести до фізичного поділу персоналу, що володіє основними навичками, або до забезпечення впевненості в тому, що необхідними основними навичками володіє не одна особа);

– збереження знань та управління знаннями.

Відповідно до ідентифікованими ризиками організація повинна розробляти стратегії, спрямовані на зменшення впливу непридатності звичайних приміщень ІКТ. Це може включати один або декілька наступних факторів:

– альтернативні приміщення в рамках організації, включаючи переміщення інших видів діяльності;

– альтернативні приміщення, що надаються іншими організаціями;

– альтернативні послуги, що надаються фахівцями третьої сторони;

– робота вдома або на інших віддалених об’єктах;

– інші узгоджені відповідні робочі місця;

– використання альтернативної робочої сили на встановленій території і альтернативні засоби, які можуть бути транспортовані на об’єкт, де відбулося порушення, і використані для забезпечення прямої заміни деяких з порушених фізичних активів.

Послуги ІКТ, від яких залежить критична діяльність бізнесу, повинні стати доступними до відновлення залежної від них критичної діяльності бізнесу. Таким чином, потрібні рішення, що забезпечують впевненість в доступності прикладних програм не пізніше певних часових термінів, наприклад, заданого часу відновлення, що визначається в межах аналізу впливу на бізнес. Технологічні платформи і прикладне програмне забезпечення повинні бути встановлені в терміни, необхідні організацією в цілому.

Технологіям, що підтримує критичні послуги ІКТ, часто потрібні складні механізми забезпечення неперервності, так що при виборі стратегій ГІКТЗНБ потрібно враховувати наступне:

– заданий час відновлення (ЗЧВ) для критичних послуг ІКТ, що підтримують критичні види діяльності, ідентифіковані МНБ ;

– місце розташування і відстань між технологічними об’єктами; кількість технологічних об’єктів;

– віддалений доступ до систем;

– вимоги охолодження;

– вимоги енергопостачання;

– використання необслуговуваних (темних) об’єктів на відміну від об’єктів з персоналом;

– активації альтернативних засобів ІКТ або це має відбуватися автоматично);

– рівень необхідної автоматизації;

– застарівання технології;

– можливість зв'язку з залученими постачальником послуг та інші зовнішні канали зв'язку.

Критична діяльність бізнесу може, крім того, залежатиме від надання новітніх або майже новітніх даних. Повинні бути розроблені пов'язані з критичною діяльністю бізнесу рішення щодо забезпечення неперервності даних для досягнення заданої точки відновлення (ЗТВ) кожної критичної діяльності бізнесу організації.

Обрані варіанти ГІКТЗНБ повинні забезпечувати впевненість у постійній конфіденційності, цілісності та доступності критичних даних, що підтримують критичні види діяльності (див. ISO / IEC 27001 та ISO / IEC 27002).

Стратегії ГІКТЗНБ і зберігання даних повинні задовольняти вимогам забезпечення неперервності бізнесу організації і враховувати наступні фактори:

– вимоги ЗТВ;

– як забезпечується безпечне зберігання даних, наприклад, диска, магнітної стрічки або оптичного носія даних; повинні існувати відповідні механізми резервного копіювання і відновлення для забезпечення впевненості в безпеці даних і в безпеці середовища;

– де зберігається і куди транспортується або передається інформація, відстань, мережеві з'єднання і т. д. (на об’єкту, поза об’єктом або у третьої сторони) та очікувані тимчасові, е терміни для пошуку резервних носіїв-даних;

– часові терміни відновлення, що визначаються обсягом даних, способом їх зберігання і складністю технічного процесу відновлення, поряд з вимогами користувача послуг і потребами в забезпеченні організаційної неперервності.

Домовленість про використання даних вкрай важлива. Це може включати передачу і надходження інформації від третіх сторін. Слід пам'ятати про те, що характер, актуальність і цінність даних можуть бути дуже різноманітними в межах організації.

ЗТВ пов'язана з кількістю даних, втрачених або невідновних в результаті порушення. Вона представлена на часовій шкалі у вигляді проміжку часу між останнім надійним резервним копіюванням і виникненням порушення. Задана точка відновлення залежить від використовуваної стратегії відновлення послуги ІКТ, особливо від плану резервування.

Початком відліку часу є вторгнення хакера в критичну систему ІКТ та порушення послуги. Першою контрольною точкою після виникнення порушення послуг ІКТ є безпосереднє виявлення інциденту безпеки (Подія, вторгнення) або непряме виявлення втрати (або погіршення) послуги, до сповіщення про який проходить якийсь час; наприклад, в деяких випадках

повідомлення може здійснюватися через дзвінок користувача до служби технічної підтримки.

Поки порушення послуг ІКТ розслідується, аналізується, про нього повідомляється і приймається рішення активізувати ГІКТЗНБ, може пройти додатковий час. Від початку порушення послуг ІКТ до прийняття рішення про активізацію ГІКТЗНБ може пройти кілька годин, з урахуванням часу на інформування і на прийняття рішення. У деяких ситуаціях рішення про активізацію може вимагати ретельного розгляду, наприклад, коли послуга не повністю втрачена або здається, що існують серйозні передумови швидкого відновлення послуги, тому що активізація ГІКТЗНБ часто впливає на звичайні операції бізнесу.

Після активізації може починатися відновлення послуг ІКТ. Воно може підрозділятися на відновлення інфраструктури (мережа, апаратні засоби, операційна система, програмні засоби резервного копіювання і т. д.) і відновлення прикладних програм (бази даних, прикладні завдання, процеси пакетної обробки, інтерфейси і т. д.). (Детальніше див. В ISO / IEC 24762).

Коли послуга ІКТ відновлена і персоналом ІКТ проведено тестування системи, послуга може бути надана на тестування прийнятності для користувача, перш ніж буде передана персоналу для використання в операціях із забезпечення неперервності бізнесу.

З метою забезпечення неперервності бізнесу, існує (ЗЧВ) на продукт, послугу або вид діяльності, починаючи з моменту виникнення порушення і до моменту відновлення продукту, послуги або виду діяльності, але для забезпечення такої можливості може знадобитися ряд послуг ІКТ, і кожна з цих послуг ІКТ може містити кілька систем або прикладних програм ІКТ. Кожна з цих складових систем або прикладних програм ІКТ буде мати своє власне заданий час відновлення, як складова частина загального заданого часу відновлення послуги ІКТ яке має бути менше, ніж заданий час відновлення неперервності бізнесу, враховує час виявлення та прийняття рішення і час проведення користувальницької перевірки застосування (якщо тільки продукт,

послуга чи діяльність із забезпечення неперервності бізнесу можуть підтримуватися без ІКТ протягом якогось періоду, наприклад, використовуючи ручні процедури).

Відновлені послуги ІКТ зазвичай функціонують протягом якогось періоду часу, підтримуючи діяльність із забезпечення неперервності бізнесу, і, якщо це тривалий період, то відновлені послуги ІКТ можуть зажадати розширення для підтримки зростаючого обсягу діяльності, можливо до моменту повного відновлення продукту, послуги або діяльності до звичайних обсягів операцій.

При виборі своєї стратегії ГІКТЗНБ організація повинна враховувати процеси, необхідні для забезпечення впевненості в життєздатності цієї стратегії, включаючи ті, що необхідні для запобігання інцидентів, виявлення інцидентів, реагування на інциденти і відновлення після лиха. Організація також має встановлювати будь-які фактори, необхідні для ефективної реалізації цих окремих процесів, наприклад, сукупність основних навичок, критичні дані, основні ефективні технології або критичне обладнання та засоби.

Загальна обізнаність про готовність елементів послуг ІКТ-кадрів, приміщень, технології, даних, процесів і постачальників, а також їх критичних компонентів - є вирішальним елементом забезпечення впевненості в необхідної підтримки системи менеджменту та управління неперервністю бізнесу, включаючи готовність ІКТ. Отже, організація повинна:

– підвищувати, покращувати і підтримувати обізнаність з допомогою неперервного навчання та інформаційних програм для відповідного персоналу і встановити процес оцінки ефективності забезпечення інформованості;

– забезпечити впевненість у поінформованості персоналу про те, який внесок він вносить у досягнення цілей ГІКТЗНБ.

Системи відновлення ІКТ та критичні дані, по можливості, повинні бути фізично відокремлені від робочого об’єкта, щоб запобігти впливу на них одного і того ж інциденту.

При реалізації стратегії слід звернути увагу на місцезнаходження всього

обладнання ІКТ. Повинні бути вивчені загальні характеристики масштабованості, керованості, підтримки, ефективності та вартості для різних стратегій реалізації, щоб визначити найбільш підходящі методи для обраних стратегій, що підтримують спільні цілі і завдання забезпечення неперервності бізнесу.

Організації повинна мати документи (плани) для управління при можливих порушеннях, щоб забезпечити неперервність послуг ІКТ та відновлення критичної діяльності.

Плани організації з менеджменту інцидентів ІКТ, забезпечення неперервності бізнесу та технічного відновленню можуть бути швидко активовані послідовно або одночасно.

Організація може розробити спеціальні документи планів відновлення або повернення послуг ІКТ в нормальний стан (плани відновлення). Проте визначити, що таке нормальний стан іноді можна тільки через деякий час після інциденту, тому негайна реалізація планів відновлення може бути неприпустимою. У цьому зв'язку організація повинна забезпечити впевненість у тому, що механізми неперервності здатні до додаткових дій з підтримки в більш великому плані неперервності бізнесу, надаючи час на приведення в дію планів. У невеликої організації може бути єдиний документ - план, що охоплює всі заходи щодо відновлення послуг ІКТ для всієї її діяльності. У дуже великій організації може бути багато документів плану відновлення, кожен з яких детально визначає відновлення конкретного елемента послуг ІКТ.

Плани реагування та відновлення ІКТ повинні бути лаконічними і доступними для осіб, чиї обов'язки визначені в планах.

Організація повинна вживати заходів щодо виправлення будь-яких фактичних відмов послуг ІКТ та елементів ГІКТЗНБ. Документально оформлена процедура для коригувальних заходів повинна визначати вимоги для:

– ідентифікації відмов;

– визначення причин відмов;

– оцінювання потреби в діях для забезпечення впевненості в тому, що невідповідності не повторяться;

– визначення та реалізації необхідних коригувальних заходів;

– фіксування результатів вжитих заходів;

– перевірки прийнятих коригувальних заходів.

В інформаційно-комунікаційних технологіях «висока доступність» відноситься до систем або компонентів, які неперервно функціонують протягом бажаного тривалого періоду часу. Доступність може вимірюватися по відношенню до «100% працездатності» або «Повної відсутності відмов». Існує широко поширений, але важкодосяжний еталон доступності систем чи продуктів (99,999%) доступності.

Резервування та доступність даних можуть бути досягнуті при використанні різноманітних технологій зберігання, таких як надлишкові дискові масиви (RAID - redundant array of disks), мережа зберігання даних (SAN - storage area network) і т. д.

Доступність прикладних програм теж вимагає розгляду і часто досягається за допомогою кластеризації.

Такі технології можуть бути реально ефективними в забезпеченні високої доступності лише за одночасної реалізації більш ніж в одному місці. Наприклад, просто наявність відмовостійкого сервера на тому ж об’єкті, що і основний або «робочий» сервер, не забезпечить необхідного рівня стійкості, у разі значних порушень безпеки. Це порушення вплине на обидва сервери. Щоб могли бути досягнуті необхідні рівні доступності, «відмовостійкий» сервер або інші підтримуючі технології повинні розміщуватися на іншому об’єкту.

2.2 Аналіз сценаріїв відмови компонентів системи

Існує цілий ряд можливих методів менеджменту ризику, які можуть допомогти в оцінці готовності ІКТ до забезпечення неперервності бізнесу та розробці відповідної структури для постійного розвитку і вдосконалення стійкості ІКТ.

Стандарт ISO 31010: 2009 «Керування ризиком. Методи загального оцінювання ризику» (ISO/IEC 31010: 2009 Risk management - Risk assessment techniques) призначений для відображення сучасних кращих практичних прийомів вибору і використання методів оцінки ризику. До цього стандарту слід звертатися з метою визначення найбільш відповідного методу для використання в організації.

Оцінка сценаріїв відмов є одним з методів, який може бути корисним для підвищення ефективності ГІКТЗНБ.

У період між оцінками можуть виникати проблеми невідомого ризику, як результат змін у внутрішній і зовнішній середовищі організації, які можуть перешкоджати забезпеченню неперервності бізнесу і стійкості. Метою оцінки сценаріїв відмов є визначення прийнятних індикаторів подій і забезпечення впевненості в тому, що плани ГІКТЗНБ надають можливість виявляти такі виникають аспекти ризику і зможуть підготувати організацію до забезпечення прийняття відповідних заходів перш, ніж відбудеться відмова.

Для цієї мети доступний ряд спеціальних методик, включаючи аналіз виду відмов та їх впливу (FMEA - Failure Mode Effect Analysis) та аналіз впливу відмови компонентів (CFIA - Component Failure lmpact Analysis). З демонстраційною метою в цьому додатку детально опрацьовується методика FMEA, в той же час організації слід вибирати методику, яка відповідає її середовищі та структурою.

Аналіз виду відмов та їх впливу (FMEA) - це процес визначення та аналізу можливих видів відмов системи з метою їх класифікації за ступенем серйозності або визначення впливу відмов на систему. У контексті цього стандарту FMEA може застосовуватися для визначення індикаторів критичних подій, які слід піддавати моніторингу з метою виявлення серйозних видів відмов у системі ІКТ організації. Процес, заснований на підході FMEA, може застосовуватися до кожного критичного компоненту послуг ІКТ.

Для кожного критичного компонента визначається:

– можливий вид відмови;

– можливий вплив на послугу ІКТ, серйозність кожного виду відмови та наслідки, які він матиме;

– раніше випробовувана організацією частота виникнення виду відмови, а також простота його моніторингу та виявлення;

– індикатори, які будуть сигналізувати або інформувати про відмову компонента;

– прямі і непрямі події, які пов'язані між собою і будуть змінювати стан кожного індикатора;

– існуючі заходи і засоби контролю і управління, які запобігають відмові критичних компонентів або можуть виявляти виникнення таких відмов;

– визначаються взаємопов'язані джерела даних і можливі методи моніторингу для виявлення змін значення індикатора; індикатори подій групуються по доступності методів і простоті моніторингу;

– визначається можливість застосування відповідних заходів і засобів контролю та управління для зниження або усунення ризику, щоб запобігти його повторне появу.

Вихідні дані FMEA включають список можливих видів відмов та їх впливу, взаємопов'язані події які можуть використовуватися для визначення індикаторів подій, що вимагають моніторингу.

Види відмов, визначені за допомогою процесу FMEA, можуть бути розставлені відповідно до пріоритетів відповідно до оціненої серйозністю, частотою виникнення і простотою моніторингу та виявлення.

FMEA також документує поточні знання і заходи стосовно ризиків відмов для використання в процесі постійного вдосконалення. Якщо FMEA використовується на етапі проектування, щоб уникнути майбутніх відмов, то він може використовуватися для управління до і під час поточного функціонування процесу. В ідеалі FMEA починається на самому ранньому (концептуальному) етапі проектування і триває протягом життєвого циклу продукту або послуги.

2.3 Характеристика об’єкта інформаційної діяльності

У роботі об’єктом дослідження є типовий центр обробки даних провайдера хмарних сервісів.

Об’єкт інформаційної діяльності – центр обробки даних, що працює в сегментах хостингу інфраструктурних послуг, створення і підтримки IT-інфраструктур і системній інтеграції.

Загальна площа центру - 570 квадратних метрів, площа машинного залу - 300 квадратних метрів. Приміщення розраховане на 70 серверних стійок. Середня електрична потужність однієї стійки - 6 кВт. Загальна потужність електропостачання ЦОД - 1 МВт.

Неперервне і автономне енергопостачання здійснюється за допомогою двох ліній електроживлення від роздільних трансформаторів, двох груп джерел безперебійного живлення (ІБП), двох електрощитів в ЦОД. Розподільні щити забезпечують захист від перевантажень і коротких замикань. В системі енергозабезпечення ЦОД вжиті всі заходи безпеки: виконано захисне заземлення, обладнані спеціалізовані фальшполи з антистатичним покриттям.

У разі зникнення зовнішнього електропостачання власна дизель-генераторна установка (ДГУ) виробництва компанії Cummins потужністю 1,4 МВт бере на себе 100% навантаження менш ніж за 20 секунд.

Резерву палива у вбудованому баку ДГУ достатньо для 10 годин роботи ЦОД і офісу, існує налагоджений механізм постачання палива. Процес запуску ДГУ повністю автоматизований.

Сигнали про відхилення від штатного режиму роботи будь-яких систем миттєво поступають в диспетчерський центр, що працює в режимі 24 * 7 * 365.

Для запобігання несанкціонованого доступу в приміщеннях ведеться цілодобове відеоспостереження, використовується єдина система контролю і управління доступом. Двері в приміщення серверної і супутні технологічні приміщення обладнані електронними дзвінками і зчитувачами карт.

За бажанням замовників встановлюються огороджувальні конструкції, усередині яких орендарі можуть розташувати власні системи контролю

доступу, відеоспостереження, лазерні системи виявлення вторгнень і інші елементи безпеки. Всі додаткові системи безпеки можуть бути надані замовникові як послуга.

Постійний контроль роботи обладнання в диспетчерській забезпечує неперервність функціонування ЦОД, захист від втрати даних, від виходу з ладу ІТК та інженерних або коммунікаційних систем. Сигнали про відхилення від штатного режиму роботи будь-яких систем миттєво поступають в диспетчерський центр.

У ЦОД використовується єдина система охоронного телебачення, управління якою ведеться з центрального поста охорони будівлі. Єдина система контролю і управління доступом забезпечує функції контрольно-пропускного пункту, відеоверіфікацію осіб, що проходять через турнікети, графічне відображення стану системи (наявність тривог, нештатних ситуацій, оперативної інформації з висновком поверхових планів), створення архіву всіх фактів відвідування об'єкта. Двері всіх приміщень ЦОД обладнані електронними замками і зчитувачами карт.

У будівлі організована єдина система охоронної і протипожежної сигналізації, що контролює зовнішній периметр дата-центру, всі технологічні приміщення, кришки приладових шаф, слабкострумових ніш.

2.4 Політика забезпечення неперервності бізнесу центрів обробки даних провайдера хмарних обчислень

2.4.1 Призначення документа

Політика забезпечення неперервності бізнесу в ЦОД провайдера хмарних обчислень (далі по тексту - Політика) спрямована на зниження впливу надзвичайної ситуації на життя і здоров'я працівників ЦОД, мінімізацію впливу на клієнтів, збереження активів, оцінку впливу надзвичайної ситуації на операційну діяльність ЦОД з метою її якнайшвидшого відновлення .

Справжня Політика описує метод побудови процесів забезпечення неперервності бізнесу ЦОД провайдера хмарних обчислень і визначає базову

сукупність правил, вимог і керівних принципів у галузі забезпечення неперервності бізнесу, спрямованих на:

– аналіз і моніторинг ризиків, вплив яких може частково або повністю призупинити критичні бізнес-процеси ЦОД провайдера хмарних сервісів;

– організацію оцінки критичності бізнес-процесів ЦОД провайдера хмарних сервісів;

– забезпечення неперервності критичних бізнес-процесів;

– мінімізацію збитку, що наноситься діяльності ЦОД провайдера хмарних сервісів виникненням надзвичайних ситуацій;

– забезпечення відповідності заходів, що вживаються в галузі забезпечення неперервності бізнесу ЦОД провайдера хмарних сервісів;

– надання працівникам рекомендацій та сприяння в галузі забезпечення неперервності бізнесу.

Справжня Політика забезпечення неперервності бізнесу в ЦОД провайдера хмарних сервісів застосована відносно до всіх працівників ЦОД.

Даний документ повинен розглядатися строго у відповідності з іншими внутрішніми документами ЦОД провайдера хмарних сервісів. У разі виникнення суперечностей між даним документом та іншими внутрішніми документами ЦОД провайдера хмарних сервісів, що зачіпають питання політики забезпечення неперервності бізнесу ЦОД провайдера хмарних сервісів, даний документ має більш високий пріоритет в частині процесів забезпечення неперервності бізнесу, за винятком Статуту ЦОД провайдера хмарних сервісів.

2.4.2 Позначення та скорочення

ЦОД – центр обробки даних провайдера хмарних сервісів;

ІБ - інформаційна безпека;

ІС - інформаційна система;

ІТ - інформаційні технології;

КУНС - команда управління надзвичайною ситуацією;

ЗНБ - забезпечення неперервності бізнесу;

План ЗНіВД - План забезпечення неперервності та відновлення діяльності;

НС - Надзвичайна Ситуація.

2.4.3 Терміни та визначення

Глобальна відмова інформаційної системи (далі - «ІС») - стан ІС, при якому всі користувачі ІС не можуть виконувати посадові обов'язки, використовуючи функціональні можливості ІС, та/або не виконуються функції ІС, які не потребують участі користувачів. Глобальний відмова ІС може призводити до повної або часткової втрати функціональності взаємопов'язаних ІС, з якими здійснюється інформаційна взаємодія.

Команда відновлення - команда, відповідальна за технічний і майновий аналіз НС та вжиття заходів до якнайшвидшого відновлення інфраструктури та/або бізнесу.

Команда управління надзвичайною ситуацією (КУНС) - колегіальний орган, уповноважений на координацію дій підрозділів і окремих працівників в умовах НС, в рамках наданих йому повноважень відповідно до їх посадовими інструкціями та положеннями цієї Політики.

Командний центр - це приміщення, де збирається КУНС для обговорення подальших кроків з усунення впливів НС на, тобто проводиться оперативне управління ЦОД при настанні НС.

Критичний процес - бізнес-процес, який підлягає відновленню при виникненні НС.

Куратор ЗНБ - працівник, в обов'язки якого входить менеджмент питань ЗНБ.

Неперервність бізнесу - стратегічна і тактична здатність організації планувати свої дії і реагувати на інциденти та порушення нормального ходу діяльності з метою продовження виконання операцій на певному прийнятному рівні.

Керівник напрямку ЗНБ - працівник ЦОД, на якого покладені завдання з оперативного управління процесами ЗНБ, включаючи контроль виконання політики, процедур, вирішення конфліктів, залучення ресурсів, надання звітності за ключовими показниками.

План ЗНіВД - внутрішній документ або комплект документів, що визначає цілі, завдання, порядок, способи і терміни здійснення комплексу заходів щодо запобігання або своєчасної ліквідації наслідків можливого порушення режиму повсякденного функціонування ЦОД, викликаного непередбаченими обставинами (виникненням НС) або іншою подією, настання, якого можливо, але важко передбачувано і пов'язане із загрозою істотних матеріальних втрат чи інших наслідків, що перешкоджають виконанню ЦОД прийнятих на себе зобов'язань.

Планування заходів на випадок виникнення НС - розробка та підтримка узгоджених процедур щодо попередження, зменшення масштабів, контролю, пом'якшення наслідків і прийняття інших заходів у разі настання НС.

Працівники - працівники ЦОД, що виконують на ЦОД роботу за трудовим договором; громадяни, які виконують на ЦОД роботу за цивільно-правовим договором.

Тестування - діяльність, в ході якої повністю або частково відпрацьовуються дії відповідно до Стратегії ЗНБ та/або Планом ЗНіВД , щоб переконатися, що План(и) ЗНіВД містять інформацію, що дозволяє при їх введенні в дію отримати бажаний результат.

Резервний офіс - приміщення, обладнане певними технічними засобами, в кількості, що дозволяє організувати відновлення і підтримку діяльності ЦОД у разі настання НС, що тягнуть неможливість здійснення діяльності ЦОД в цілому, або її частини, з використанням приміщень та/або технічної інфраструктури основного офісу.

Процеси ЗНБ - сукупність організаційних заходів, процесів і ресурсів, в завдання яких входить здійснення заходів, спрямованих на ЗНБ.

Управління ЗНБ-процес, в ході якого виявляються потенційні загрози для організації і визначаються можливі наслідки в разі здійснення цих загроз, а також створюється основа забезпечення здатності ЦОД відновлюватися і ефективно реагувати на виникнення НС. Управління ЗНБ включає в себе управління відновленням і продовженням бізнесу ЦОД в разі порушення нормального ходу діяльності, а також управління спільною програмою дій і заходів працівників, структурних підрозділів та органів управління ЦОД за допомогою проведення навчання, навчань та аналізу з метою підтримки Плану (-ів) ЗНіВД в актуальному стані.

НС - подія, здатна частково або повністю призупинити діяльність ЦОД несе за собою:

– порушення нормального функціонування основних автоматизованих систем, що реалізують бізнес-процеси ЦОД;

– непрацездатність (недоступність) основних каналів зв'язку, мережі інтернет, інших каналів зв'язку з взаємодіючими організаціями;

– відсутність фізичної можливості знаходження працівників ЦОД на робочих місцях внаслідок пожежі, повені, аварій, актів терору, диверсій, саботажу, стихійних лих та інших обставин непереборної сили;

– інші випадки, що спричинили порушення нормальної роботи ЦОД.

2.4.4 Завдання і цілі ЗНБ

Основними цілями ЗНБ є:

– підтримання здатності ЦОД виконувати прийняті на себе зобов'язання перед клієнтами та партнерами, попередження та запобігання можливого порушення режиму повсякденного функціонування ЦОД;

– забезпечення відповідності всіх механізмів ЗНБ вимогам державних органів України, а також вимогам нормативно-правових актів та прийнятим на ЦОД політикам, процедурам і планам;

– зниження тяжкості наслідків порушення режиму повсякденного функціонування ЦОД (у тому числі розміру матеріальних втрат, втрат інформації, втрати ділової репутації);

– збереження рівня управління ЦОД, що дозволяє забезпечити умови для прийняття обґрунтованих і оптимальних управлінських рішень, їх своєчасну і повну реалізацію;

– забезпечення сприятливих умов праці та безпеки працівників, безпеки відвідувачів, які перебувають у приміщеннях ЦОД;

– визначення переліку Критичних процесів ЦОД та переліку сценаріїв негативного розвитку подій, здатних призвести до зупинки бізнес-процесів ЦОД;

– забезпечення неперервності діяльності критичних бізнес-процесів ЦОД за рахунок визначення, впровадження та документування механізмів контролю, включаючи План(и) ЗНіВД розроблені для кожного структурного підрозділу та/або робочої групи. Кожен План ЗНіВД описує потреби структурної одиниці в ресурсах, необхідних для реалізації плану в частині продовження і відновлення діяльності від моменту оголошення НС до її завершення і перехід в режим повсякденного функціонування.

На ЦОД можуть встановлюватися додаткові вимоги, процедури, регламенти ЗНБ. Вони можуть бути більш деталізовані, передбачати додаткові обмеження, але не повинні суперечити цій Політиці.

ЗНБ включає в себе:

– визначення областей, в рамках яких організація може бути вразлива до ризиків неперервності;

– визначення ризиків, які можуть вплинути на функціонування організації;

– розгляд та аналіз ризику виникнення природних, техногенних катастроф, так само, як і інших непередбачених обставин, застосовних до офісів місцезнаходження ЦОД;

– розгляд ризиків, реалізація яких завдає істотної шкоди матеріальним і нематеріальним активам ЦОД;

– аналіз факторів, що впливають на ймовірність настання НС;

– аналіз ступеня впливу НС на: працівників; інфраструктуру інформаційні активи ЦОД.

З метою забезпечення повноцінного аналізу факторів впливу, аналіз повинен проводитися для кожного бізнес-процесу ЦОД у всіх структурних підрозділах ЦОД в рамках Плану ЗНіВД.

До завдань забезпечення нормальної діяльності в умовах НС ЦОД відноситься:

1) визначення процесів і операцій, що підлягають додатковому захисту;

2) забезпечення створення на щоденній основі резервних копій інформації про торги, а також іншої інформації в рамках процесів і операцій, що підлягають додатковому захисту;

3) забезпечення розміщення основного і резервного комплексів програмно технічних засобів на території України. У разі використання резервного комплексу програмно-технічних засобів ЦОД забезпечує виконання всіх процесів і операцій, що підлягають додаткового захисту, в тому числі забезпечення постачання комплексів альтернативними джерелами електроживлення, що дозволяють здійснювати діяльність ЦОД до закінчення робочого дня в умовах НС;

4) розробка і доведення до відома працівників ЦОД плану заходів на випадок виникнення НС (План ЗНіВД), а також проведення періодичного навчання працівників з питань їх дій в умовах НС;

5) доведення до відома учасників організованих торгів інформацію про порядок дій ЦОД в разі виникнення НС.

2.4.5 Оновлення Політики

Відповідальним за оновлення Політики є Куратор ЗНБ. Політика підлягає перегляду, в разі значних змін у діяльності ЦОД, таких як: відкриття нових видів

діяльності, розширення географії діяльності, зміна організаційної структури, поява або оновлення вимог регулюючих органів і т.д.

У разі перегляду Політики або її зміни, слід:

– внести відповідні зміни в структуру і текст Політики; затвердити Політику в установленому порядку;

– розіслати Політику в усі структурні підрозділи для виконання.

2.4.6 Ролі та відповідальність

Куратор ЗНБ:

– керує процесами ЗНБ. У рамках здійснення загального керівництва визначає основні напрямки ЗНБ, приймає рішення про скликання КУНС;

– на підставі документів, що подаються Керівником напрямку ЗНБ, приймає рішення щодо стратегічних поліпшень процесів ЗНБ;

– погоджує і виносить на затвердження Політику, а також інші процедури, інструкції, плани, регламенти та інші нормативні документи щодо ЗНБ.

Керівник напрямку ЗНБ:

– забезпечує розробку Політики, процедур, інструкцій, планів та інших документів, що регулюють процеси ЗНБ;

– організовує ознайомлення працівників з цією Політикою, а також координує процес підвищення обізнаності працівників у галузі ЗНБ;

– готує пропозиції щодо вибору методів і засобів ЗНБ, а також механізмів моніторингу процесів ЗНБ;

– забезпечує контроль виконання положень, викладених у цій Політиці та інших внутрішніх документах ЦОД, що регламентують процеси і встановлюють вимоги до ЗНБ;

– готує пропозиції щодо формування бюджету, спрямованого на ЗНБ;

– організовує роботи, спрямовані на розробку технічних, організаційних та адміністративних планів забезпечення реалізації Політики;

– бере участь в обробці і класифікації НС, з метою виявлення ризиків порушення неперервності бізнесу ЦОД;

– надає методологічну підтримку структурним підрозділам для складання та актуалізації Планів ЗНіВД;

– підтримує в актуальному стані зведений звіт до вимог структурних підрозділів ЦОД до ЗНБ (зведений План ЗНіВД);

– визначає програму Тестування;

– контролює процес реалізації програми Тестування;

– проводить аналіз результатів тестування, готує звіти та аналітичні матеріали, визначає необхідні коригувальні дії, і контролює їх виконання;

– приймає тактичні рішення по поліпшенню процесів ЗНБ та вносить пропозиції щодо стратегічних поліпшень цієї діяльності;

– оцінює стан процесів ЗНБ, ініціює перегляд Політики ЗНБ ЦОД.

Керівники структурних підрозділів ЦОД:

– у взаємодії з Керівником напрямку ЗНБ розробляють і узгоджують Плани ЗНіВД критичних бізнес-процесів, власниками яких вони є;

– забезпечують своєчасне надання Керівнику напрямки ЗНБ повної і достовірної інформації про Критичні процеси;

– беруть участь у тестуванні, складанні звітів за результатами тестування та проведенні аналізу цих результатів;

– контролюють повноту та актуальність Плану ЗНіВД;

– спільно з Керівником напрямку ЗНБ виробляють рішення щодо вдосконалення діяльності з ЗНБ;

– беруть участь у процесі забезпечення поінформованості працівників свого підрозділу в області ЗНБ;

– виконують вимоги по ЗНБ, викладені в цій Політиці та інших документах ЦОД по ЗНБ;

– забезпечують виконання працівниками своїх підрозділів Плану ЗНіВД і вимог інструкцій щодо дій у НС;

– забезпечують виконання вимог по ЗНБ, викладених у цій Політиці та інших внутрішніх документах ЦОД, працівниками свого структурного підрозділу та (якщо є) третіми особами, з якими вони взаємодіють в рамках своїх посадових обов'язків, у тому числі шляхом включення зазначених вимог до контрактів (угоди) , договорів з третіми особами.

Служба безпеки:

– при виникненні НС здійснює взаємодію зі штабами і службами по боротьбі з НС, сформованими муніципальними та (або) виконавчим державними органами;

– забезпечує умови для якнайшвидшої евакуації людей, що знаходяться в офісі (-ах) ЦОД, а також майна ЦОД, у разі такої необхідності;

– у разі евакуації людей і майна забезпечує охорону точки збору працівників ЦОД та складування майна ЦОД;

– забезпечує безперешкодний доступ до(в) офісу(-и) ЦОД муніципальним і (або) державним службам по боротьбі з НС у разі такої необхідності;

– забезпечує оперативний доступ працівників ЦОД, задіяних у реалізації Плану (-ів) ЗНіВД на резервних об’єктах.

Працівники ЦОД:

– виконують вимоги по ЗНБ, викладені в цій Політиці та інших внутрішніх документах ЦОД по ЗНБ;

– виконують Плани ЗНіВД відповідно до наділеними їм ролями; проходять щорічний обов'язковий навчальний курс з ЗНБ;

– беруть участь у проведенні тестувань ЗНБ (за наявності ролі у відновленні процесів);

– при виникненні НС діють відповідно до вимог інструкцій щодо дій у НС;

– забезпечують виконання вимог по ЗНБ, викладених у цій Політиці та інших внутрішніх документах ЦОД.

КУНС:

– визначає ступінь впливу НС на діяльність ЦОД, складає перелік втрат і оцінює розмір нанесеного збитку в результаті НС;

– оголошує режим НС;

– оголошує рішення про активацію Планів ЗНіВД та інформує зацікавлені сторони про це рішення;

– інформує органи управління ЦОД про хід виконання Планів ЗНіВД ;

– розглядає пропозиції щодо прийняття управлінських рішень та розміщення інформації в загальнодоступних джерелах;

– координує роботи з виконання Планів ЗНіВД ;

– інформує заінтересовані особи про хід відновлення діяльності ЦОД та заходи, вжиті для забезпечення її неперервності;

– організовує взаємодію з державними органами та іншими державними установами з метою координації спільних дій щодо забезпечення своєчасного проведення розрахунків за дорученнями клієнтів і за зобов'язаннями ЦОД, а також з іншими зацікавленими особами з питань ЗНБ;

– координує взаємодію з правоохоронними органами, аварійними та спеціалізованими службами (у тому числі з органами внутрішніх справ, пожежною охороною, аварійно-рятувальними службами, закладами охорони здоров'я, органами, які здійснюють державний санітарно-епідеміологічний нагляд);

– координує взаємодію з комунальними службами, в тому числі з питань забезпечення електро-, тепло- і водопостачання, з постачальниками послуг телефонного та інших видів зв'язку;

– координує процес організації необхідної допомоги працівникам ЦОД та членам їх сімей;

– протягом періоду дії НС здійснює інформаційну взаємодію з іншими підрозділами підприємства, ЦОД та клієнтами, нормальне функціонування яких порушується або може бути порушене в результаті настання НС на даному ЦОД.

2.4.7 Порядок ознайомлення та навчання в області ЗНБ

Процес ознайомлення та навчання працівників ЦОД в області ЗНБ включає в себе:

– вступний інструктаж з ЗНБ працівників ЦОД;

– ознайомлення з цією Політикою, розміщеної на внутрішньому корпоративному порталі ЦОД;

– ознайомлення з Планом ЗНіВД внутрішнього структурного підрозділу, що описує план заходів у разі виникнення НС;

– ознайомлення з іншими документами в галузі ЗНБ, у тому числі з питань дії працівників ЦОД в умовах НС;

– планове навчання (тренінг) працівників ЦОД основам ЗНБ;

– позапланове навчання працівників ЦОД, задіяних у процесах ЗНБ (за наявності унікальної ролі у відновленні Критичних процесів).

Відповідальні за проведення ознайомлення та навчання в області ЗНБ:

– поширення матеріалу для вступного інструктажу з ЗНБ здійснюється працівником ЦОД, відповідальним за проведення вступних семінарів, для нових працівників ЦОД;

– ознайомлення з іншими документами в галузі ЗНБ здійснюється керівниками відповідних структурних підрозділів (у тому числі ознайомлення з Планом ЗНіВД);

– планові та позапланові навчання, тренінги та тестування організовуються Керівником напрямку ЗНБ.

З метою підтримки кваліфікації на належному рівні відповідальні працівники за ЗНБ зобов'язані проходити регулярне навчання у профільних навчальних організаціях, які мають відповідні ліцензії.

2.4.8 План управління НС

Вихідною частиною Планування заходів на випадок виникнення НС, є визначення КУНС, Команди відновлення, а також вироблення Стратегії ЗНБ та умов оголошення НС.

Умовою початку дії Плану управління НС повинно бути рішення КУНС про введення режиму НС та про активацію планів ЗНіВД .

Якщо з якихось причин хтось із членів КУНС НЕ буде доступний в момент НС, то вони повинні бути заміщені працівниками зі складу членів Команди відновлення діяльності (відповідно до очолюваних ними напрямками діяльності).

У разі настання НС КУНС приймає рішення, спрямовані на зниження впливу НС на ЦОД і працівників ЦОД, незалежно від зовнішніх факторів НС.

План управління НС є робочим документом і містить необхідну інформацію для нормального функціонування команди:

– основна та резервна точки збору КУНС;

– склад КУНС;

– склад Команди відновлення;

– опис Командного центру;

– умови оголошення НС;

– стратегія на короткостроковий (до тижня), середньостроковий (до місяця) і довгостроковий (понад місяць) періоди дії НС;

– необхідні контактні дані.

План управління НС розробляється Керівником напрямку ЗНБ та узгоджується Куратором ЗНБ.

2.4.9 Оголошення / дія / скасування режиму НС

З метою координації дій усіх підрозділів ЦОД, активація Планів ЗНіВД допускається тільки після офіційного оголошення НС. Правом оголошення НС володіє тільки КУНС .

Дія режиму НС поділяється на наступні проміжки часу:

– негайно - найближчі години після оголошення НС;

– день 1й - перший повний робочий день, після оголошення НС;

– день 2-5-й - період з другого по п'ятий день;

– день 6-10-й - період з шостого по 10-й день дії НС;

– день 11-30-й - період з одинадцятого по 30-й день;

– більше місяця - в рамках даного періоду, розглядаються будуть проміжки часу більше одного місяця.

Рішенням КУНС режим дії пріоритетів будь-якого з проміжків часу може бути збільшений, з метою оптимізації використання ресурсів та оптимізації дій підрозділів в рамках обраної стратегії.

Рішення щодо скасування режиму дії НС приймає тільки КУНС .

2.4.10 Управління в режимі НС

У разі необхідності (при виникненні НС або ситуації, яка може перерости у НС), з метою забезпечення координації дій структурних підрозділів в умовах НС скликається КУНС .

Розпуск КУНС здійснюється за фактом повернення діяльності в режим повсякденного функціонування ЦОД.

Про скликання і розпуск КУНС Куратор ЗНБ негайно інформує відповідальних працівників ЦОД.

У КУНС призначаються такі працівники:

– Генеральний директор ЦОД (голова команди);

– члени Дирекції ЦОД;

– Куратор ЗНБ;

– Керівник напрямку ЗНБ (секретар команди);

– керівники структурних підрозділів, діяльність яких порушена або може бути порушена НС.

2.4.11 Резервні офіси, переміщення працівників у резервні офіси

Резервні офіси для структурних підрозділів визначаються в рамках реалізації Стратегії ЗНБ та підготовкою Планів ЗНіВД. У Планах ЗНіВД повинно бути вказано кількість резервних робочих місць, в кожен часовий проміжок, закріплених за структурним підрозділом ЦОД.

При складанні Плану (ів) ЗНіВД пріоритети повинні бути встановлені з урахуванням переміщення працівників в резервний офіс відразу після рішення

КУНС про оголошення режиму НС та активації резервного офісу. Переміщення від точки збору до резервного офісу проводиться відповідно опису, наведеному в плані ЗНіВД та/або ґрунтуючись на інформації, отриманої від КУНС.

2.4.12 Розподіл навантажень між іншими ЦОД

Всі ЦОД інформаційної системи підприємства зобов'язані виділити додаткові сервери, зарезервовані на випадок НС. При складанні Плану (ів) ЗНіВД пріоритети повинні бути встановлені з урахуванням оперативного розподілу навантажень між іншими ЦОД після рішення КУНС про оголошення режиму НС. Перенесення віртуальної інфраструктури до резервних серверів проводиться відповідно опису, наведеному в плані ЗНіВД та/або ґрунтуючись на інформації, отриманої від КУНС.

2.5 Рекомендації щодо захисту інформації, що обробляється з використанням технології хмарних обчислень

На базі представлених умов, міжнародного досвіду та аналітичних даних створені рекомендації щодо захисту інформації в для найбільш розповсюдженнях типів хмарних сервісів.

2.5.1 Об'єкти, що підлягають захисту при використанні технологій хмарних обчислень

До основних об'єктів, що підлягає захисту від НСД, відносяться:

– захищені інформаційні та обчислювальні ресурси (інформація конфіденційного характеру, що зберігається на машинних носіях, атрибути безпеки (мітки безпеки), пов'язані з інформацією, мережевий трафік, що містить інформацію конфіденційного характеру, образи віртуальних машин);

– фізичні та віртуальні пристрої обробки даних (хмарні клієнти, віртуальні машини, апаратне забезпечення ІСХТ, машинні носії інформації);

– службова інформація фізичних і віртуальних пристроїв обробки і передачі даних (тимчасові файли, тимчасові дані, створювані в процесі міграції

віртуальних машин, після її завершення, в процесі сеансу зв'язку хмарного клієнта з хмарним сервером, мережеві адреси, мережеві імена);

– канали передачі даних, мережеві потоки (інформаційні потоки між компонентами інфраструктури, сегментами ІСХТ, між різними ІСХТ при взаємодії між хмарними системами, мережеві з'єднання (сеанси зв'язку), маршрути передачі мережевих пакетів);

– системи обробки інформації, їх компоненти (обчислювальні мережі, системи та мережі реплікації; системи резервного копіювання; вузли, на яких функціонують: ПЗ управління хмарним сервером, ПЗ, яке здійснює мережеву взаємодію за протоколом http, ПЗ гіпервізорів; вузли, орендовані споживачами хмарних послуг) ;

– службова інформація віртуального і фізичного мережевого обладнання;

– вбудоване програмне забезпечення віртуальних і фізичних пристроїв обробки даних мережевого обладнання, системне і прикладне ПЗ, мережеві служби;

– службова інформація системного і прикладного ПЗ;

– об'єкти файлової системи віртуальних і фізичних дисків, дані на машинних носіях інформації;

– процеси і потоки, запущені в оперативній пам'яті;

– резервні копії даних (еталонні образи віртуальних машин, резервні копії журналів реєстрації подій БІ, конфігураційних файлів, ключів системного реєстру, записів баз даних засобів ЗІ, що входять до складу ІСХТ);

– бази даних, структурні елементи баз даних (облікові записи і ідентифікатори користувачів, автентифікаційна інформація суб'єктів доступу, бази даних ознак шкідливих комп'ютерних програм (вірусів), бази вирішальних правил засобів ЗІ);

– службова інформація стосовно засобів ЗІ (обов'язки, повноваження (ролі) суб'єктів доступу, параметри автентифікаційної інформації суб'єктів доступу, методи, типи і правила розмежування доступу, число паралельних сеансів доступу для кожної облікового запису користувачів ІСХТ, склад і зміст

інформації про події безпеки, які підлягають реєстрації , журнали реєстрації подій безпеки, конфігураційні файли, ключі системного реєстру).

2.5.2 Загрози безпеці інформації, що обробляється з використанням технологій хмарних обчислень

Об'єднання хмарних ресурсів в єдиний пул постачальник хмарних послуг об'єднує хмарні ресурси для обслуговування великої кількості споживачів в єдиний пул для динамічного перерозподілу хмарних ресурсів між споживачами в умовах постійної зміни попиту на такі, при цьому споживачі контролюють тільки основні параметри хмарної послуги (наприклад, обсяг даних, швидкість доступу), але фактичний розподіл хмарних ресурсів, що надаються споживачеві, здійснює постачальник. хмарних обчислень.

Обсяг наданих споживачеві хмарних ресурсів може швидко і гнучко змінюватися (в деяких випадках - автоматично) - збільшуватися або зменшуватися. Для кінцевого споживача хмарні ресурси постачальника хмарних послуг представляються нескінченними і можуть бути придбані в будь-якій кількості в будь-який час.

Елементи інформаційних систем, побудованих з використанням технологій хмарних обчислень, виконують різні функції, розподілені за рівнями архітектури побудови ІСХТ, показаної на рисунку 2.1.

Рисунок 2.1 – Загальна структура ЦОД

Всі елементи системи мають свої вразливості через які можуть бути реалізовані певні загрози.

2.5.2.1 Загрози, пов'язані з невизначеністю при розподілі відповідальності

В хмарі можуть бути визначені такі ролі, як провайдер хмарних послуг, користувач хмарних послуг, адміністратор клієнтської інформаційної системи, власник інформації і т. д. При цьому існують загрози БІ, пов'язані з невизначеністю при розподілі відповідальності між різними ролями в частині володіння даними, контролю доступу, підтримки інфраструктури і т. п. Організація БІ від таких загроз ускладнена тим, що її реалізація здатна привести до істотних розбіжностей між постачальником і споживачем хмарних послуг з питань, пов'язаних з визначенням їх прав та обов'язків. Особливо це стосується використання постачальником хмарних послуг, що надаються іншим постачальником (схема надання хмарних послуг за участю безлічі

посередників) Наслідком загроз БІ, пов'язаних з невизначеністю при розподілі відповідальності, є порушення конфіденційності, цілісності та доступності інформації постачальників хмарних послуг.

2.5.2.2 Загрози БІ, пов'язані з неузгодженістю політик безпеки

Внаслідок децентралізованності архітектури хмарної інфраструктури в різних засобах захисту, розподілених по інфраструктурі ІСХТ, можуть бути реалізовані різні політики безпеки. Наприклад, один засіб захисту може відмовити в доступі, а інше - надати. Така неузгодженість політик безпеки різних засобів ІСХТ може бути використана зловмисником в інтересах порушення конфіденційності та цілісності інформації. Наслідком загроз БІ, пов'язаних з невизначеністю при розподілі відповідальності, є порушення конфіденційності, цілісності та доступності інформації постачальників хмарних послуг.

2.5.2.3 Загрози БІ, пов'язані з безперервною модернізацією

Однією з переваг використання хмарних послуг є можливість здійснення вибору і (або) зміни первісного складу ПЗ вже після введення ІСХТ в експлуатацію. Однак у цих умовах система, що розглядається як захищена на етапі проектування, після введення її в експлуатацію може володіти безліччю вразливостей, що містяться в новому ПЗ. Наслідком загроз БІ, пов'язаних з безперервною модернізацією, є порушення цілісності та доступності інформації постачальників хмарних послуг.

2.5.2.4 Загрози БІ, пов'язані з призупиненням надання послуг внаслідок технічних збоїв

Постачальник хмарних послуг має можливість надавати різні види хмарних послуг в рамках одного хмарного сервера. При цьому технічні збої хоча б у одного з постачальників хмарних послуг, а також затримки або втрати в каналі передачі даних, орендованих постачальником хмарних послуг, можуть призвести до зниження якості або навіть припинення надання хмарних послуг їх кінцевому споживачу. Наслідком загроз БІ, пов'язаних з припиненням

надання послуг внаслідок технічних збоїв, є порушення доступності інформації з вини постачальника хмарних послуг.

2.5.2.5 Загрози БІ, пов'язані з неможливістю міграції образів віртуальних машин

Постачальник хмарних послуг використовує для реалізації своєї діяльності апаратне і ПЗ різних виробників, частина якого може використовувати специфічні інструкції, протоколи, методи, схеми комутації та інші особливості реалізації свого функціоналу. Внаслідок цього виникають загрози БІ, пов'язані з ризиком недостатності стандартних програмних інтерфейсів обміну даними (API) для реалізації процедури міграції образів віртуальних машин між різними постачальниками хмарних послуг в одному або обох напрямках. Наслідками даних загроз БІ є обмеження можливості зміни виробників апаратного і програмного забезпечення, що призводить до порушення цілісності та доступності інформації з вини постачальника хмарних послуг.

2.5.2.6 Загрози БІ, пов'язані з ліцензійними політиками

Політики ліцензування використання ПЗ зазвичай заснована на обмеженні кількості його установок або числа його користувачів. Так як створені віртуальні машини можуть бути використані лише кілька разів, провайдеру може знадобитися куди більше ліцензій, ніж йому необхідно в конкретний момент часу. Недостатність опрацювання питання управління політиками ліцензування використання ПЗ в хмарах, може призвести до загроз втрати доступності ПЗ, і як наслідок, порушення доступності інформації з вини постачальника хмарних послуг.

2.5.2.7 Загрози БІ, пов'язані з конфліктом юрисдикцій різних країн

Залежно від законодавства різних країн, резиденти яких беруть участь у наданні хмарних послуг, при забезпеченні БІ можуть використовуватися правові заходи різних юрисдикцій. При цьому у транскордонній передачі інформації конфіденційного характеру може бути відмовлено відповідно до вимог відповідних нормативно-правових актів. Наслідком загроз БІ, пов'язаних

з конфліктом юрисдикцій різних країн, є порушення доступності інформації постачальників хмарних послуг.

2.5.2.8 Загрози БІ, пов'язані з неякісним перенесенням інфраструктури в хмару

Міграція навіть частини інфраструктури інформаційної системи в хмару часто вимагає проведення серйозних змін в такий інфраструктурі (наприклад, в політиках безпеки та організації мережевого обміну даними). Неякісне перенесення інфраструктури інформаційної системи в хмару внаслідок несумісності програмних і мережевих інтерфейсів або невідповідностей політик безпеки може призвести до інцидентів БІ.

2.5.2.9 Загрози БІ, пов'язані із здійсненням незахищеного адміністрування хмарних послуг

Використання засобів адміністрування, що лежать між хмарної інфраструктурою і користувачами хмарних послуг, може бути причиною погроз БІ внаслідок недостатності уваги, приділеною контролю вводяться користувачами хмарних послуг даними (у тому числі автентифікаційних даних).

Крім того, зловмисник може провести атаку на ICXT за рахунок експлуатації вразливостей небезпечних інтерфейсів обміну даними (API). Дана атака не є специфічною для хмар, однак, відповідно до сервіс-орієнтованим підходом стандартні інтерфейси обміну даними служать основою для побудови хмарної інфраструктури. Таким чином, захист стандартних інтерфейсів обміну даними є пріоритетним завданням забезпечення БІ в хмарах з метою запобігання порушення конфіденційності, цілісності та доступності інформації з вини постачальника хмарних послуг.

2.5.2.10 Загрози БІ, пов'язані з загальнодоступністю інфраструктури

Оскільки користувачі хмарних послуг (у тому числі конкуруючі між собою) ділять одну й ту ж саму інфраструктуру, то виникають загрози порушення конфіденційності або цілісності даних шляхом здійснення прямого доступу до захищається даними користувачів.

2.5.2.11 Загрози БІ, пов'язані з використанням технологій віртуалізації

У більшості випадків основою для створення хмарної інфраструктури є технології віртуалізації. При цьому один фізичний сервер, його обчислювальні ресурси і ресурси пам'яті діляться між безліччю віртуальних машин. Існують різні загрози технологій віртуалізації (наприклад, загроза виходу програмного процесу за межі гіпервізора), що призводять до інцидентів БІ.

2.5.2.12 Загрози БІ, пов'язані з порушенням доступності хмарного сервера

Забезпечення доступності не є специфічним вимогою БІ для технологій хмарних обчислень, проте, відповідно до сервіс-орієнтованим підходом, реалізованим у хмарах, у разі порушення доступності хмарної інфраструктури буде припинено надання хмарних послуг усім споживачам. Більше того, здатність динамічно змінювати обсяг наданих споживачам хмарних послуг може бути використана зловмисником для проведення атаки. При цьому успішна атака щодо всього одного хмарного сервісу дозволить порушити доступність всього хмари.

2.5.2.13 Загрози БІ, пов'язані зі зловживаннями з боку споживачів хмарних послуг

У зв'язку з тим, що споживач хмарних послуг може встановлювати власне ПЗ на хмарний сервер, то для досягнення своїх неправомірних цілей споживач хмарних послуг може встановити шкідливе ПЗ, за допомогою якого здійснювати розсилку спаму, НСД до віртуальних машин інших клієнтів або інші комп'ютерні атаки, що може негативно вплинути на репутацію постачальника хмарних послуг. Дані загрози безпеки інформації можуть призвести як до порушення конфіденційності інформації обмеженого користування споживачів хмарних послуг, так і до порушення цілісності, а також доступності.

2.5.3 Захист інформації при наданні хмарних послуг

Забезпечення БІ при наданні інфраструктури як послуги вимагає приділити особливу увагу захисту апаратних і віртуальних пристроїв обробки

даних, а також каналів зв'язку.

При наданні платформи як послуги виникають загрози БІ, пов'язані з відсутністю у споживачів хмарних послуг контролю над використовуваним апаратним забезпеченням (у тому числі ОС), а також особливостями розробки хмарного ПЗ. Забезпечення БІ при наданні платформи як послуги вимагає забезпечення захисту системних і прикладних програм хмарного сервера.

При наданні ПЗ як послуги виникають загрози БІ, пов'язані з відсутністю у споживачів хмарних послуг контролю над використовуваним програмним і апаратним забезпеченням (у тому числі ОС). Забезпечення ЗІ при наданні програмного забезпечення як послуги вимагає приділяти особливу увагу захисту усіх об’єктів ІСХТ.

Заходи з ідентифікації і автентифікації суб'єктів доступу і об'єктів доступу повинні забезпечувати:

– ідентифікацію та автентифікацію користувачів, які є працівниками постачальника хмарних послуг;

– ідентифікацію та автентифікацію хмарних клієнтів, у тому числі стаціонарних, мобільних і портативних;

– управління ідентифікаторами в ході взаємодії між хмарами, у тому числі передача, трансляція, перетворення формату ідентифікаторів;

– захист зворотного зв'язку в ході автентифікації хмарного клієнта на хмарному сервері;

– ідентифікацію та автентифікацію користувачів, які є споживачами хмарних послуг;

– реалізацію в хмарному клієнті механізму перевірки відповідності параметрів автентификаційної інформації, що вводиться користувачами при реєстрації або зміну свого облікового запису, політиці безпеки, яка визначається постачальником хмарних послуг;

– взаємну ідентифікацію та автентифікацію хмарних сервера і клієнтів при їх мережевій взаємодії.

Заходи з управління доступом суб'єктів доступу до об'єктів доступу повинні забезпечувати:

– реалізацію механізмів управління (передачі відомостей про облікові записи, створення їх дублікатів та ін.) обліковими записами користувачів в ході взаємодії між хмарами;

– реалізацію необхідних методів, типів і правил розмежування доступу в ході взаємодії між хмарами;

– управління інформаційними потоками (фільтрація, маршрутизація, контроль з'єднань, односпрямована передача, створення і використання кластерів гіпервізорів і пулів хмарних ресурсів, а також інші способи управління) між компонентами, сегментами хмарної інфраструктури, а також при взаємодії між хмарами;

– поділ обов'язків, повноважень (ролей) адміністраторів та осіб, які забезпечують функціонування хмарних серверів і хмарних клієнтів;

– призначення мінімально необхідних прав і привілеїв користувачам, адміністраторам і особам, які забезпечують функціонування хмарного сервера;

– обмеження числа неуспішних спроб підключення хмарних клієнтів до хмарного сервера;

– попередження споживача хмарних послуг при його підключенні до хмарного серверу про реалізовані заходи ЗІ, а також про необхідність дотримання ним встановлених постачальником хмарних послуг правил обробки інформації;

– оповіщення користувача після успішного підключення до хмарного серверу про дату і час його попереднього підключення;

– блокування сеансу доступу до хмарного сервера після встановленого часу бездіяльності споживача хмарних послуг або за його запитом;

– дозвіл (заборона) дій споживачів хмарних послуг, дозволених до його ідентифікації і автентифікації в хмарному сервері;

– підтримку і збереження атрибутів безпеки (міток безпеки), пов'язаних з інформацією в ході взаємодії між хмарами;

– управління взаємодією між хмарами.

Заходи з обмеження програмного середовища повинні забезпечувати:

– контроль номенклатури ПЗ, що встановлюється та запускається;

– заборона встановлення і запуску забороненого до використання в ІС ПЗ.

Заходи щодо захисту машинних носіїв інформації повинні забезпечувати контроль доступу до інформації з обмеженим доступом, що зберігається на машинних носіях належить споживачам хмарних послуг.

Заходи з видалення залишкової інформації повинні забезпечувати:

– видалення невикористовуваних даних про споживачів хмарних послуг;

– видалення невикористовуваних образів віртуальних машин;

– видалення тимчасових даних, що створюються в процесі міграції віртуальних машин, по його завершенні;

– видалення тимчасових даних, що створюються в процесі сеансу зв'язку хмарного клієнта з хмарним сервером.

Заходи щодо реєстрації подій безпеки повинні забезпечувати:

– реалізацію в хмарному клієнті механізму збору та передачі на хмарний сервер інформації про зареєстровані події безпеки;

– реалізацію механізмів збору, запису, зберігання та обміну інформацією про реєстровані в ході взаємодії між хмарами події безпеки;

– синхронізація системного часу для хмарних клієнтів, а також фізичних і віртуальних вузлів, що беруть участь у наданні хмарних послуг (у тому числі при взаємодії між хмарами);

– забезпечення можливості порівняння інформації про події безпеки, зареєстровані хмарним клієнтом, з інформацією, зареєстровану хмарним сервером і (або) в ході взаємодії між хмарами;

– прогнозування вичерпання обчислювальних ресурсів ІС.

Заходи з криптографічного захисту інформації, що зберігається і передається повинні забезпечувати:

– шифрування мережевого трафіку, в процесі передачі інформації з обмеженим доступом:

– взаємодії між хмарами;

– взаємодії хмарного клієнта і хмарного сервера;

– адмініструванні хмарного сервера;

– міграції ВМ;

– шифрування інформації конфіденційного характеру, що зберігається на хмарних серверах.

Заходи з антивірусного захисту повинні забезпечувати: реалізацію антивірусного захисту (з використанням стандартних антивірусних засобів; антивірусних засобів, що функціонують під управлінням власного гіпервізора; антивірусних засобів, які використовують службову віртуальну машину-аналізатор і агентів на кожній користувальницької віртуальній машині та ін.) для наступних компонентів інфраструктури хмарного сервера:

– вузлів, на яких функціонує ПЗ управління хмарним сервером;

– вузлів, на яких функціонують гіпервізори;

– вузлів, орендованих споживачами хмарних послуг;

– вузлів, що функціонують в інтересах забезпечення безпеки хмарного сервера.

Заходи з виявлення (запобігання) вторгнень повинні забезпечувати виявлення і (або) блокування НСД або спеціального впливу на компоненти інфраструктури хмарного сервера і (або) оброблювану в них інформацію (носії інформації) з боку зовнішніх і внутрішніх порушників щодо наступних суб'єктів мережевої взаємодії:

– вузлів, на яких функціонує ПЗ управління хмарним сервером;

– вузлів, на яких функціонує ПЗ, яке здійснює мережеву взаємодію за протоколом http;

– вузлів, на яких функціонують гіпервізором;

– вузлів, орендованих споживачами хмарних послуг;

– вузлів, що функціонують в інтересах забезпечення безпеки хмарного сервера;

– віртуального і фізичного мережевого обладнання, його програмного забезпечення.

Заходи з контролю (аналізу) захищеності інформації повинні забезпечувати:

– автоматизований контроль дій хмарних клієнтів з метою виявлення деструктивного використання хмарних послуг.

– виявлення, аналіз вразливостей у ПЗ, що встановлюється на хмарному сервері (в тому числі на віртуальні машини споживачів хмарних послуг) та їх оперативне усунення;

– тестування відмовостійкості хмарного серверу, встановлення періоду автоматичного планового тестування.

Заходи щодо забезпечення цілісності ПЗ ІСХТ та інформації повинні забезпечувати:

– контроль цілісності інформації, що міститься в базах даних хмарного сервера;

– контроль помилкових дій споживачів хмарних послуг по вводу і (або) передачі інформації та попередження споживачів хмарних послуг про помилкові дії;

– контроль цілісності сеансу зв'язку між хмарним клієнтом і хмарним сервером, а також між хмарними серверами при взаємодії між хмарами;

– контроль цілісності хмарних клієнтів;

– контроль цілісності ПЗ, що входить до складу хмарних серверів;

– контроль цілісності еталонних образів віртуальних машин;

– резервне копіювання захищається інформації, що зберігається на хмарному сервері;

– резервне копіювання еталонних образів віртуальних машин, настановних пакетів (дистрибутивів) програм.

Заходи щодо забезпечення доступності інформації повинні забезпечувати:

– використання взаємодії між хмарами в інтересах резервування хмарних ресурсів;

– запуск міграції віртуальних машин на основі результатів прогнозування вичерпання обчислювальних ресурсів хмарного сервера;

– періодичне резервне копіювання даних про надані хмарних послугах, а також інформації обмеженого доступу, що належить споживачам хмарних послуг;

– об'єднання гіпервізорів в кластери, хмарних ресурсів в пули;

– управління якістю наданих хмарних послуг (об'ємом, часом доступу, та ін.) за рахунок контролю поточної пропускної здатності каналу зв'язку, часу затримки при передачі мережевих пакетів, кількості втрачених мережевих пакетів та ін;

– своєчасне виявлення відмов вузлів хмарної інфраструктури, а також недопустимого зниження якості наданих хмарних послуг;

– автоматичну зміну маршрутів передачі мережевих пакетів між вузлами хмарної інфраструктури при відмові в обслуговуванні мережевих запитів, що проходять по основних маршрутах;

– резервування пропускної здатності каналу передачі даних для пріоритетних хмарних послуг і найбільш значущих їх споживачів;

– управління коштами відновлення попереднього працездатного стану засобів ЗІ хмарного сервера в разі збоїв при здійсненні санкціонованого зміни їх стану;

– балансування мережевого навантаження між дублюючими фізичними та віртуальними каналами передачі даних між хмарним клієнтом і хмарним сервером, а також між хмарними серверами при взаємодії між хмарами.

Заходи щодо захисту хмарного серверу, його засобів і систем зв'язку та передачі даних повинні забезпечувати:

– поділ повноважень з управління (адміністрування) хмарним сервером, засобами ЗІ, каналами зв'язку, хмарними клієнтами, хмарними послугами між різними категоріями адміністраторів;

– підтвердження походження джерела інформації, одержуваної в процесі визначення мережевого адресу з мережевих імен, у тому числі при взаємодії між хмарами;

– забезпечення достовірності мережевих з'єднань (сеансів зв'язку) при взаємодії між хмарами;

– виключення можливості заперечення користувачем факту надання йому хмарної послуги.

Заходи щодо мережевого екранування повинні забезпечувати:

– реалізацію єдиних політик розмежування доступу між усіма суб'єктами та об'єктами мережевої взаємодії, у тому числі розподіл функцій міжмережевого екранування і завдання єдиних правил фільтрації для всіх фізичних і віртуальних мережевих екранів, що входять до складу ІС на всіх рівнях архітектури її побудови;

– фільтрацію мережевого трафіку відносно наступних компонентів інфраструктури хмарного сервера:

– вузлів, на яких функціонує ПЗ управління хмарним сервером;

– вузлів, на яких функціонує ПЗ, яке здійснює мережеву взаємодію за протоколом http;

– вузлів, на яких функціонують гіпервізором;

– вузлів, орендованих споживачами хмарних послуг;

– вузлів, що функціонують в інтересах забезпечення БІ хмарного сервера.

Заходи з централізованого управління повинні забезпечувати:

– централізоване оновлення баз сигнатур засобів ЗІ;

– централізоване управління журналами безпеки, що ведуться всіма засобами ЗІ, які входять до складу хмарного сервера, а також їх узагальнення у вигляді єдиного журналу подій БІ;

– централізоване управління резервним копіюванням журналів реєстрації подій БІ, параметрів налаштувань (конфігураційних файлів, ключів системного реєстру, записів баз даних та ін.) засобів ЗІ, що входять до складу хмарного сервера.

2.7 Висновок

Запропоновані варіанти забезпечення неперервності ведення бізнесу є універсальними для більшості ситуацій, можливих для даного об'єкта. Мета розробленої в даному розділі політики – максимально знизити рівень ризиків припинення роботи критичних бізнес-активів. При цьому модернізацію політики треба робити систематично, аби не випустити момент, коли вона втрачає актуальність. На базі представлених умов, міжнародного досвіду та аналітичних даних створені рекомендації щодо захисту інформації для найбільш розповсюдженнях типів хмарних сервісів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У даному розділі наведені наступні розрахунки:

1) розрахунок капітальних витрат;
2) розрахунок поточних витрат;
3) визначена величина можливого збитку.

На підставі отриманих результатів було зроблено висновок щодо економічної ефективності створення рекомендацій захисту інформації.

3.1 Розрахунок капітальних (фіксованих) витрат

При розробці політики безперервності ведення бізнесу капітальні витрати розраховуються за формулою (3.1):

$$К = К_{рп} + К_{пз} + К_{ic}, \quad (3.1)$$

де $К_{рп}$ – вартість розробки політики безперервності ведення бізнесу, грн.;

$К_{пз}$ – вартість додаткового програмного забезпечення, грн.;

$К_{ic}$ – витрати інтеграцію розробленої політики безперервності ведення бізнесу в існуючу систему, грн.

Витрати на розробку політики безперервності ведення бізнесу визначаються за формулою (3.2):

$$К_{рп} = З_в \cdot t, \quad (3.2)$$

де $З_в$ – мінімальна заробітна плата з нарахуваннями за годину, грн/годину і дорівнює 40,46 грн/годину;

t – трудомісткість створення та впровадження політики безперервності ведення бізнесу, годин.

Трудомісткість створення політики безперервності ведення бізнесу визначається тривалістю кожної робочої операції.

Формула для розрахунку трудомісткості (3.3) має наступний вигляд:

$$t = t_{тз} + t_{в} + t_{рс} + t_{впр} + t_{сі} + t_{д}, \text{ годин}, \quad (3.3)$$

де $t_{тз}$ – тривалість складання технічного завдання, годин;

$t_{в}$ – тривалість аналізу існуючої інформаційної системи, літературних джерел за темою тощо;

$t_{рс}$ – тривалість розробки політики безперервності ведення бізнесу, годин;

$t_{впр}$ – впровадження політики безперервності ведення бізнесу в існуючій інформаційній системі, годин;

$t_{сі}$ – тривалість створення інструкцій для навчання персоналу, годин;

$t_{д}$ – тривалість оформлення документації.

Складові трудомісткості визначаються на підставі умовної кількості оперантів Q, яка розраховується за формулою (3.4):

$$Q = q \cdot c\,(1 + p) \quad \text{штук}, \quad (3.4)$$

де q – очікувана кількість оперантів, q=20;

c – коефіцієнт складності рекомендацій, c=1,5;

p – коефіцієнт корекції методів в процесі їх опрацювання дорівнює 0,05.

$$Q=20*1,5*(1+0,05) \approx 32 \text{ штук}.$$

Тривалість складання технічного завдання становить 5 годин.

Тривалість аналізу існуючої інформаційної системи, літературних джерел за темою 30 годин.

Тривалість розробки політики безперервності ведення бізнесу 60 години.

Тривалість оформлення документації 10 годин.

Тривалість впровадження політики безперервності ведення бізнесу в існуючій інформаційній системі (3.5):

$$t_{в} = \frac{1,5Q}{(4...5) \cdot k} \text{ годин}, \quad (3.5)$$

$$t_в = \frac{1,5*32}{(5*0.8)} = 12 \text{ години.}$$

Тривалість розробки інструкцій з виконання політики безперервності ведення бізнесу:

$$t_{сі} = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)} \cdot 0,75 \text{ години,} \quad (3.6)$$

$$t_{сі} = \frac{32}{15\cdot 0.8} + \frac{32}{15} \cdot 0,75 = 4.27 \text{ години.}$$

Трудомісткість створення політики безперервності ведення бізнесу, згідно формули (3.3), складає:

$$t=5+30+60+12+4,27+10 = 121,27 \text{ годин.}$$

Витрати на створення політики безперервності ведення бізнесу розраховуються за формулою (3.7):

$$К_{пз} = t*(З_{зп} + З_{мч}), \quad (3.7)$$

де Ззп заробітна плата виконавця, дорівнює 40,46 грн/годину;

Змч – вартість машинного часу для налагодження програм на ПК.

$$З_{мч} = \frac{Впк + Впз}{2} \div T + 0,5\cdot 1,1948, \quad (3.8)$$

де Впк – вартість персонального комп'ютеру, дорівнює 32000 грн.;

Впз – витрати на додаткове програмне забезпечення;

Витрати на додаткове програмне забезпечення, що необхідне для створення політики безперервності ведення бізнесу, представлені в таблиці 3.1.

Таблиця 3.1 – Вартість додаткового програмного забезпечення, призначеного для створення політики безперервності ведення бізнесу

Найменування	Кількість, шт.	Ціна за 1 шт., грн.
Microsoft Office 2021	1	6305
Visio Standard 2021	1	5710
Загалом		12015

Т – трудомісткість і дорівнює (365-110-10)*8=1960 годин,

$$З_{мч} = \frac{32000+12015}{2} \div 1960 + 0{,}5 \cdot 1{,}1948 = 11{,}83 \text{грн./год.}$$

Витрати на створення політики безперервності ведення бізнесу:

К=121,27*(11,83+ 40,46)= 6341,21 грн.

Таблиця 3.2 – Вартість додаткового програмного забезпечення, призначеного для впровадження політики безперервності ведення бізнесу

Найменування	Кількість, шт.	Ціна за 1 шт., грн.
BMC BladeLogic Decision Support for Network Automation	1	105000
Загалом		105000

Сумарні капітальні витрати становлять:

К=105000+6341,21=111341,21

3.2 Розрахунок річних поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (рік), що виражені у грошовій формі. Річні поточні (експлуатаційні) витрати на функціонування політики безперервності ведення бізнесу розраховуються за формулою (3.9):

$$С = Са + Сз + Спз, \quad (3.9)$$

Са - річний фонд амортизаційних відрахувань, грн.;

Сз - річний фонд заробітної плати інженерно-технічного персоналу, грн;

Спз – річний витрати на ліцензійне програмне забезпечення.

Згідно з Податковим кодексом України строк корисного використання нематеріальних активів четвертої групи складає не менше як 5 років.

Са = (111341,21) (1/5) = 22268,24 грн.

Річний фонд заробітної плати адміністратора системи з врахуванням

ЄСВ у розмірі 22%, визначається за формулою (3.10):

$$Сз = Зосн, * 1,22, \quad (3.10)$$

$$Зосн = 6700 * 12 = 80400 \text{ грн.}$$

$$Сз = 80400 * 1,22 = 98088 \text{ грн.}$$

Витрати на функціонування політики безперервності ведення бізнесу:

$$Ск = 22268,24 + 98088 = 120356,24 \text{ грн.}$$

3.3 Збитки підприємства

Щоб одержати оцінку очікуваних збитків використовують таблицю потенційних загроз інформаційній безпеці.

Можливий збиток розраховується шляхом множення частоти виникнення потенційної загрози на величину збитку.

Показник очікуваних збитків можна визначити за формулою (3.11):

$$D = F * P, \quad (3.11)$$

де F – частота виникнення потенційної загрози в рік;

P – величина збитку у гривнях.

Оскільки основною діяльністю підприємства є надання послуг хмарних обчислень, оплата послуг клієнтами проходить з урахуванням часу використання (погодинно). Мінімальна ціна використання одного сервера протягом однієї години 7,63 грн./год. Всього на підприємстві - 90 серверних стійок, які працюють у режимі 24/7/365. У разі припинення роботи сервера, клієнт не оплачує час, який проходить до відновлення роботи. Враховуючи статистичні дані використання серверів в центрах обробки даних, причини і частоту припинення роботи та розрахунковий час, необхідний для відновлення роботи, залежно від причини, розраховано мінімальні загальні збитки підприємства за один рік для всіх 90 серверних стійок.

Таблиця 3.3 Збитки на підприємстві, у разі припинення роботи сервера, до впровадження політики безперервності ведення бізнесу

№ п/п	Клас потенційних загроз	Час необхідний для поновлення роботи	Частота виникнення, F	Втрати, Р грн./год	Показник очікуваних втрат, грн./рік
1	Повна втрата даних	8	30	7,63	1831,20
2	Часткова втрата даних	4	265	7,63	8087,80
3	Мережева атака	2	30	7,63	457,80
4	Помилка користувача	1	245	7,63	1869,35
5	Програмна помилка	3	50	7,63	1144,50
Загальні збитки для однієї стійки					13391,65
Загальні збитки для всіх серверів підприємства (90шт)					1205248,50

Таблиця 3.4 Збитки на підприємстві, у разі припинення роботи сервера, після впровадження політики безперервності ведення бізнесу

№ п/п	Клас потенційних загроз	Час необхідний для поновлення роботи	Частота виникнення, F	Втрати, Р грн./год	Показник очікуваних втрат, грн./рік
1	Повна втрата даних	2	30	7,63	457,80
2	Часткова втрата даних	0,5	265	7,63	1010,98
3	Мережеві атаки	1	30	7,63	465,43
4	Помилки користувача	1	245	7,63	1869,35
5	Програмні помилки	1	50	7,63	381,50
Загальні збитки для однієї стійки					4185,06
Загальні збитки для всіх серверів підприємства					376655,40

Економічна ефективність розраховується за формулою (3.12):

$$E = Вт1 – Вт2 – В, \quad (3.12)$$

де

$Вт_1$ – втрати від реалізації загроз до впровадження заходів захисту;

$Вт_2$ – втрати від реалізацій загроз після впровадження заходів захисту;

В – капітальні і експлуатаційні витрати за розрахунковий період.

$$E = 1205248,50 – 376655,40 – 120356,24 – 111341,21 = 596895,65 \text{ грн.}$$

3.4 Висновок

При виконанні роботи були прораховані капітальні 111341,21 грн і поточні витрати 120356,24 грн., та визначено вартість витрат на проєктування та впровадження політики безперервності ведення бізнесу в існуючу інформаційну систему. Розроблена політика дозволяє знизити час відновлення функціонування головних бізнес-процесів підприємства та знизити втрати від припинення їх роботи з 1205248,50 до 376655,40 грн. Впровадження розроблених рішень є економічно доцільним і значно підвищить рівень захищеності інформаційних ресурсів підприємства.

ВИСНОВКИ

При виконанні роботи було проаналізовано міжнародні стандарти, нормативно-правові документи, навчальні та дослідницькі матеріали у сфері управління неперервністю ведення бізнесу та створення програм готовності інформаційно-комунікаційних технологій до неперервності ведення бізнесу.

За результатами аналізу була розроблена політика управління неперервністю ведення бізнесу для типового центру обробки даних провайдера хмарних обчислень.

З урахуванням положень розробленої політики та особливостей інфраструктури інформаційних систем, створених із застосуванням хмарних обчислень було сформовано узагальнені практичні рекомендації щодо основних видів загроз та методів забезпечення інформаційної безпеки при реалізації наступних моделей використання хмарних обчислень: інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга.

Здійснено розрахунок економічної доцільності впровадження створеної політики неперервності бізнесу на типовому об’єкті інформаційної діяльності. Проведені розрахунки підтвердили позитивний економічний ефект. Завдяки впровадженню правил з реагування на події інформаційної безпеки буде скорочено час, необхідний для відновлення роботи основних бізнес-процесів об’єкта інформаційної діяльності.

Розроблені рекомендації щодо забезпечення захисту інформації що обробляється з використанням хмарних обчислень, базуються на міжнародних практичних рішеннях і можуть бути використані як основа для забезпечення інформаційної безпеки провайдерами хмарних послуг з різними технічними можливостями та типами сервісів.

ПЕРЕЛІК ПОСИЛАНЬ

1 The Gartner Group Research: Strategic Predictions for 2015 and Beyond / Спосіб доступу: http://www.gartner.com - Загол. з екрану.;

2 Ponemon Institute Research Report. Security of Cloud Computing Providers Study - /Спосіб доступу: http://www.ca.com/~/media/Files/IndustryResearch - Загол. з екрану.;

3 Amazon Web Services: Overview of Security Processes /Спосіб доступу: URL: http://aws.**amazon**.com - Загол. з екрану.;

4 Using Amazon Web Services for Disaster Recovery . - Glen Robinson, Attila Narin, and Chris Elleman. - October 2014 /Спосіб доступу: URL: http://aws.amazon.com - Загол. з екрану.;

5 НД ТЗІ 1.1-002-1999. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

6 Best Practices for Security and Compliance with Amazon Web Services. - A Trend Micro White Paper. - April 2013. /Спосіб доступу: URL: http://aws.amazon.com - Загол. з екрану.;

7 FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGYSIT Technical Reports SIT-TR-2012-001: On the Security of Cloud Storage Services;

8 Security guidance for critical areas of focus in cloud computing V3.0 /

Cloud Security Alliance /Спосіб доступу: URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf - Загол. з екрану.;

9 Міжнародний стандарт ISO/IEC 27005. Менеджмент ризиків інформаційної безпеки.;

10 Руководство по управлению рисками безопасности. Microsoft security center of excellence. – URL:http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk - Загол. з екрану.;

11 ДСТУ ISO/IEC 27001. Система управління інформаційною безпекою.;

12 TIA/EIA-942 (TIA-942) «Telecommunications Infrastructure Standard for Data Center»;

13 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

14 НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

15 НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

16 НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення;

17 Microsoft Azure Security and Audit Log Management /Спосіб доступу: URL: http://www.microsoft.com/windowsazure/ - Загол. з екрану.;

18 ISO 22301 Societal security - Business continuity management systems – Requirements;

19 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

20 НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи;

21 НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;

22 НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

23 НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

24 Міжнародний стандарт ISO/IEC 31000:2009. Ризик менеджмент – Принципи та керівництва.;

25 ISO/IEC 27017 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (DRAFT).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	4	
4	А4	Вступ	1	
5	А4	1 Розділ	45	
6	А4	2 Розділ	46	
7	А4	3 Розділ	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Підвищення рівня захищеності інформації при роботі з системами хмарних обчислень
Павлової Валерії Олександрівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 115 сторінках та містить 5 рисунків, 6 таблиць, 25 джерел та 4 додатка.

Об'єкт дослідження: типовий центр обробки даних.

У першому розділі проведено аналіз основних типів та моделей застосування хмарних сервісів та досліджено основні методи забезпечення неперервності бізнесу.

У спеціальній частині виявлено основні загрози систем хмарних обчислень, створена політика забезпечення неперервності бізнесу центрів обробки даних та сформульовані рекомендації щодо забезпечення їх інформаційної безпеки.

В економічному розділі проведено розрахунок вартості проектування та інтеграції політики у типовому центрі обробки даних, що входить до складу системи хмарних обчислень.

Студентка показала достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник