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 магістра

студента *Заворіна Івана Дмитровича*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення інформаційної безпеки*

при використанні хмарних технологій для учбових закладів

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер				

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Заворін І.Д.* **академічної групи** *125м-20-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення інформаційної безпеки при використанні хмарних технологій для учбових закладів*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	*Хмарні обчислення*	31.10.2021
Розділ 2	*Дослідження захисту інформації у хмарі*	24.12.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності впровадження запропонованих у проекті рішень*	4.01.2022

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.10.21р.

Дата подання до екзаменаційної комісії: 14.01.22р.

Прийнято до виконання _____ Заворін І.Д
(підпис студента)

РЕФЕРАТ

Пояснювальна записка: 103 с., 8 рис., 7 табл., 4 додатка, 43 джерела.

Об'єкт досліджень: хмарні технології що використовуються у навчальних закладах

Мета роботи: розробити рекомендації для підвищення рівня захисту інформації при використанні хмарних сервісів в навчальних закладах.

У спеціальній частині наводиться аналіз основних загроз в системах хмарних обчислень, а також розробка рекомендацій для можливості їх нейтралізації.

У роботі наведено аналіз хмарних технологій та їх ролі в сучасному світі ІТ технологій; аналіз архітектури побудови систем хмарних обчислень; аналіз основних загроз інформації, яка зберігається, оброблюється і передається в системі хмарних обчислень; аналіз проблем забезпечення доступності, цілісності та конфіденційності даних у системах хмарних обчислень; розроблені рекомендації для підвищення рівня захисту інформації при використанні хмарних сервісів в навчальних закладах..

В економічному розділі визначена економічна ефективність та обґрунтована економічна доцільність впровадження систем хмарних обчислень на приватних підприємствах.

Наукова новизна роботи полягає у розробленні та обґрунтуванні рекомендацій щодо вирішення проблеми захисту інформації при використанні хмарних сервісів в навчальних закладах.

ХМАРНІ ТЕХНОЛОГІЇ, КОНФІДЕНЦІЙНІСТЬ, ЦІЛІСНІТЬ, ДОСТУПНІСТЬ, ХМАРНІ ОБЧИСЛЕННЯ, АРХІТЕКТУРА СИСТЕМ НА ОСНОВІ ХМАРНИХ ОБЧИСЛЕНЬ

РЕФЕРАТ

Пояснительная записка: 103 с., 8 рис., 7 табл., 4 приложения, 43 источника.

Объект исследований: облачные технологии, используемые в учебных заведениях.

Цель работы: разработать рекомендации для повышения уровня защиты информации при использовании облачных сервисов в учебных заведениях.

В специальной части приводится анализ основных угроз в системах облачных вычислений, а также разработка рекомендаций для возможности их нейтрализации.

В работе приведен анализ облачных технологий и их роль в современном мире ИТ технологий; анализ архитектуры построения систем облачных вычислений; анализ основных угроз информации, которая хранится, обрабатывается и передается в системе облачных вычислений; анализ проблем обеспечения доступности, целостности и конфиденциальности данных в системах облачных вычислений; разработанные рекомендации для повышения уровня защиты информации при использовании облачных сервисов в учебных заведениях.

В экономическом разделе определена экономическая эффективность и обоснована экономическая целесообразность внедрения облачных сервисов в учебных заведениях.

Научная новизна работы заключается в разработке и обосновании рекомендаций по решению проблемы защиты информации при использовании облачных сервисов в учебных заведениях.

ОБЛАЧНЫЕ ТЕХНОЛОГИИ, КОНФИДЕНЦИАЛЬНОСТЬ, ЦЕЛОСТНОСТЬ, ДОСТУПНОСТЬ, ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, АРХИТЕКТУРА СИСТЕМ НА ОСНОВЕ ОБЛАЧНЫХ СЕРВИСОВ

THE ABSTRACT

Explanatory note: 103 p., 8 fig., 7 table ; 4 applications, 43 of the sources.

Object of research: cloud technologies used in educational institutions.

Objective: to develop recommendations for improving the level of information protection when using cloud services in educational institutions.

The special part provides an analysis of the main threats in cloud computing systems, as well as the development of recommendations for the possibility of neutralizing them.

The paper presents an analysis of cloud technologies and their role in the modern world of IT technologies; analysis of the architecture of building cloud computing systems; analysis of the main threats to information stored, processed and transmitted in the cloud computing system; analysis of the problems of ensuring the availability, integrity and confidentiality of data in cloud computing systems; developed recommendations for improving the level of information protection when using cloud services in educational institutions.

The economic section defines the economic efficiency and justifies the economic feasibility of the introduction of cloud services in educational institutions.

The scientific novelty of the work lies in the development and justification of recommendations for solving the problem of protecting information when using cloud services in educational institutions.

CLOUD TECHNOLOGIES, CONFIDENTIALITY, INTEGRITY, ACCESSIBILITY, CLOUD CALCULATIONS, ARCHITECTURE OF SYSTEMS BASED ON CLOUD SERVICES

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API – Application Programming Interfaces;

AWS – Amazon Web Services;

BaaS – бізнес-процеси як послуга (Business processes-as-a-service);

CD – Compact Disc;

CPU – Central Processing Unit;

DaaS – дані як послуга (Data-as-a-Service);

DNS – Domain Name System;

DVD – Digital Versatile Disc;

HaaS – устаткування як послуга;

IaaS – інфраструктура як послуга (Infrastructure-as-a-Service);

IEEE – Institute of Electrical and Electronics Engineers;

IP – Internet Protocol;

IDS – Intrusion Detection System;

MSP – Managed Service Providers;

NAS – Network Attached Storage;

NIDS – Network intrusion detection system;

NIST – національний інститут стандартів та технологій (National Institute of Standards and Technology);

PaaS – платформа як послуга (Platform-as-a-Service);

RAID – Redundant Array of Independent Disks;

RMA – Return Merchandise Authorization;

RPO – Recovery Point Objective;

RTO – Recovery Time Objective;

SAN – Storage Area Network;

SaaS – програмне забезпечення як послуга (Software-as-a-Service);

SAS – Statement on Auditing Standards;

SLA – Service Level Agreement;

VLAN – Virtual Local Area Network;

АС – автоматизована система;

ЕОТ – електроніка й обчислювальна техніка;

ЗІ – захист інформації;

ІР – інформаційні ресурси;

ІС – інформаційна система;

ІТ – інформаційні технології;

КЗЗ – комплекс засобів захисту;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

КМ – комп'ютерна мережа;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ОС – операційна система;

ПБ – політика безпеки;

ПБІ – політика безпеки інформації;

ПЕОМ – персональна електронно-обчислювальна машина;

ПК – персональний комп'ютер;

ПРД – правила розмежування доступу;

ТЗІ – технічний захист інформації;

ЦОД – центр обробки даних.

ЗМІСТ

ВСТУП 12

РОЗДІЛ 1. ХМАРНІ ОБЧИСЛЕННЯ 14

1.1 Моделі розгортання та обслуговування хмарного сервісу 16

1.2 Хмарне сховище та апаратна віртуалізація 22

1.3 Хмарні обчислення — переваги і недоліки 23

1.3.1 Переваги хмарних обчислень 23

1.3.2 Недоліки хмарних обчислень 27

1.4 Оцінка ефективності хмарних сервісів 28

1.4.1 Продуктивність хмарних сервісів 28

1.4.2 Швидкість масштабування 29

1.4.3 Узгодженість зберігання 29

1.4.4 Вимірювання параметрів 30

1.4.5 Прогнозування продуктивності на основі трасування 31

1.5 Доступність 34

1.6 Надійність 37

1.7 Продуктивність 38

1.8 Безпека хмарного сервісу 39

1.9 Впровадження хмарних технологій 40

1.10 Компанії, що займаються наданням «хмарних» сервісів 41

1.11 Висновок 43

РОЗДІЛ 2. ДОСЛІДЖЕННЯХ ЗАХИСТУ ІНФОРМАЦІЇ У ХМАРІ 45

2.1 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 46

2.2 Класи загроз систем на основі хмарних технологій 52

2.2.1 Традиційні атаки на ПЗ 52
2.2.2 Функціональні атаки на елементи хмари 52
2.2.3 Атаки на клієнта 53
2.3.4 Загрози віртуалізації 53
2.2.5 Атаки на гіпервізор 54
2.2.6 Атака на диск віртуальної машини 55
2.2.7 Втрата віртуальних машин 56
2.2.8 Атаки на системи управління 57
2.2.9 Атака на мережу реплікації віртуальних машин 58
2.2.10 Проблема управління даними 58
2.2.11 Комплексні загрози 59
2.2.12 Зупинка діяльності хмарного провайдера 60
2.2.13 Проблема забезпечення безпеки в хмарних середовищах 60
2.3 Модель загроз для хмарних технологій 62
2.4 Рекомендації щодо забезпечення інформаційної безпеки в хмарному середовищі 63
2.4.1 Захист мережі віртуальних машин 63
2.4.2 Шифрування файлових систем 69
2.4.3 Рекомендації по нейтралізація уразливості API 70
2.4.4 Запобігання загрози інсайдерів 70
2.4.5 Захист від втрати даних 71
2.4.6 Захист від крадіжки облікових даних 72
2.4.7 Захист від невідомих ризиків 72
2.4.8 Налаштування безпеки на рівні користувача 72
2.4.9 Створення «приватних хмар» 73

2.5 Висновок 74

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА 76

3.1 Мета техніко-економічного обґрунтування дипломного проекту 76

3.2 Визначення витрат на розробку політики безпеки інформації 76

3.2.1 Розрахунок капітальних (фіксованих) витрат 76

3.2.2 Розрахунок експлуатаційних (поточних) витрат 79

3.3 Оцінка величини збитку у разі реалізації загроз 81

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень 89

3.5 Висновок економічного розділу 91

ВИСНОВКИ 92

ПЕРЕЛІК ПОСИЛАНЬ 93

ДОДАТОК А. ПЕРЕЛІК МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ 98

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ 99

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ 100

ДОДАТОК Г. ВІДГУК НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА 101

ВСТУП

Хмарні обчислення – це нова модель, яка зменшує складність IT-інфраструктури за рахунок ефективного об′єднання ресурсів в самокеровану віртуальну інфраструктуру та їх надання на вимогу в якості послуг.

Хмарні обчислення – технологія розподіленого опрацювання даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс. Суть концепції хмарних обчислень полягає в наданні кінцевим користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків (включаючи операційні системи та інфраструктуру) через Інтернет. Розвиток сфери хмарних обчислень було обумовлено потребою, що виникла в програмному забезпеченні і цифрових послугах, якими можна було б керувати зсередини, але які були б при цьому більш економічними і ефективними за рахунок економії на масштабі.

Ринок програмного забезпечення мав до недавнього часу достатньо простий вектор розвитку. Програмісти розробляли програми, які потім поширювалися традиційним чином на носіях і встановлювалися на комп'ютер. Щоб програма працювала, до ПК пред'являлися певні системні вимоги: вказувалися необхідні продуктивність процесора, обсяг оперативної пам'яті, кількість вільного місця на жорсткому диску і т. д. Паралельно з цим розвивався Інтернет. Серверне обладнання, яке обслуговувало роботу сайтів, також удосконалювалося.

Але в якийсь момент виявилося, що можна об'єднати обчислювальні потужності для підтримки програмних сервісів, аналогічних тим, які задіюються звичайними користувачами. Так почалася історія «хмарних обчислень». Сьогодні цей термін можна застосувати для будь-яких сервісів, що надаються через мережу Інтернет.

Хмарні обчислення – це потужний підхід до проведення ресурсоємних обчислень. Кожен користувач хоч раз звертався до послуг сервісів, що надають можливість працювати з додатками, не встановлюючи їх на комп'ютер. Хмари складаються з тисяч серверів, розміщених в дата центрах,

що забезпечують роботу десятків тисяч додатків, які одночасно використовують мільйони користувачів. Неодмінною умовою ефективного управління такою масштабною інфраструктурою є повна автоматизація.

Хмарні обчислення дозволяють організувати динамічне надання послуг, коли користувачі можуть здійснювати оплату за фактом і регулювати обсяг своїх ресурсів залежно від реальних потреб без довгострокових зобов'язань.

У середовищі хмарних обчислень зберігання і перенесення даних виконується іншим способом, що знаходяться поза традиційних уявлень про захист, що створює нові виклики для систем забезпечення безпеки. Для багатьох перенесення даних в хмарну середу на комп'ютери, де не можна їх контролювати, здається неприйнятним. Крім того, цей підхід дійсно вимагає розгляду питань відповідності стандартам та обліку різних нормативно-правових аспектів. Втім, насправді хмарне середовище може бути захищене не гірше, а може бути, навіть і краще, ніж традиційний центр обробки даних. Однак у випадку роботи з хмарним середовищем підхід до інформаційної безпеки теж буде радикально відрізнятися від підходу в традиційному середовищі.

У роботі буде розглянуто концепцію хмарних обчислень, механізми забезпечення цілісності, доступності та конфіденційності інформації при її передачі від користувача безпосередньо до хмари та при зберіганні у хмарі, основні загрози, які виникають в процесі використання хмарних технологій. Також у роботі буде проаналізовано та виявлено переваги та недоліки хмарних технологій.

На основі отриманої інформації буде сформовано рекомендації стосовно забезпечення інформаційної безпеки при використанні хмарних технологій на підприємствах приватної форми власності.

РОЗДІЛ 1. ХМАРНІ ОБЧИСЛЕННЯ

Хмарні обчислення – технологія обробки даних, в якій програмне забезпечення надається користувачеві як Інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему і власне програмне забезпечення, з яким він працює. [1,2]

Згідно документу IEEE, опублікованому в 2008 році, «Хмарні обчислення – це парадигма, в рамках якої інформація постійно зберігається на серверах в мережі Інтернет і тимчасово кешується на клієнтській стороні, наприклад на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах тощо». Отже у користувача є можливість отримати доступ до даних або обчислювальних ресурсів з будь-якого пристрою.[3]

Хмарні обчислення – це модель забезпечення повсюдного та зручного мереживного доступу на вимогу до загального пулу конфігурованих обчислювальних ресурсів (наприклад, мережам передачі даних, серверам, пристроям зберігання даних, додаткам і сервісам – як разом, так і окремо), які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними витратами та/або зверненням до провайдера.[4-6]

Хмарні обчислення – це потужний підхід до проведення ресурсоємних обчислень.[5]

Хмарні обчислення – це використання Інтернет-з′єднань високої пропускної здатності для отримання сервісів, які надаються централізовано, зазвичай третіми сторонами, і тим самим зводять до мінімуму витрати на адміністрування та супроводження IT для організацій, які споживають ці сервіси.[8]

Використовуваний сьогодні термін «хмарні обчислення» можна застосувати для будь-яких сервісів, що надаються через мережу Інтернет.

Хмарна модель дуже схожа на декілька попередніх поколінь сервісних моделей: розділення машинного часу 60-70-х років, клієнт-серверні архітектури 80-90-х років і постачання додатків у вигляді сервісів недавніх

років.[8]

Різниця в тому, що технічні можливості еволюціонували в такій мірі, щоб ідея, так давно існуюча, нарешті, змогла втілитися в життя. До появлення сучасних високошвидкісних каналів передачі даних централізована доставка більшості сервісів була можлива лише з пунктів, які знаходяться в безпосередній географічній близькості від одержувача.[11]

Сучасні ж мережі дозволяють централізувати адміністрування та об′єднати продуктивність географічно розподілених серверів.

Споживачі хмарних обчислень можуть значно зменшити витрати на інфраструктуру інформаційних технологій (в короткостроковому і середньостроковому планах) і гнучко реагувати на зміни обчислювальних потреб, використовуючи властивості обчислювальної еластичності хмарних послуг.[10]

Як це передбачається у визначенні хмарних обчислень NIST (National Institute of Standards and Technology), хмарна система є набором ресурсів, доступних через мережу для замовників-користувачів (тобто хмарних передплатників – хмарних споживачів).[7, 12]

У загальному випадку, хмарна система використовує модель клієнт-сервер і її передплатники застосовують модель клієнт-сервер, яка передбачає, що передплатники відправляють по мережі повідомлення серверним комп'ютерам, які у відповідь на отримані повідомлення виконують відповідну роботу.[9]

На рисунку 1.1 показана загальна схема взаємодії хмари та її клієнтів: хмарні обчислювальні ресурси являють собою комплекс взаємопов'язаних комп'ютерних систем, доступ до яких клієнти здійснюють по мережі.[7, 12]

Як показано на рисунку, можуть з'являтися нові клієнти, старі клієнти можуть йти, в різні моменти часу кількість клієнтів буде різною. Подібним чином і хмара підтримує пул апаратного забезпечення, яким управляє для максимізації (збільшення продуктивності і рівня) сервісу і мінімізації витрат.[12]

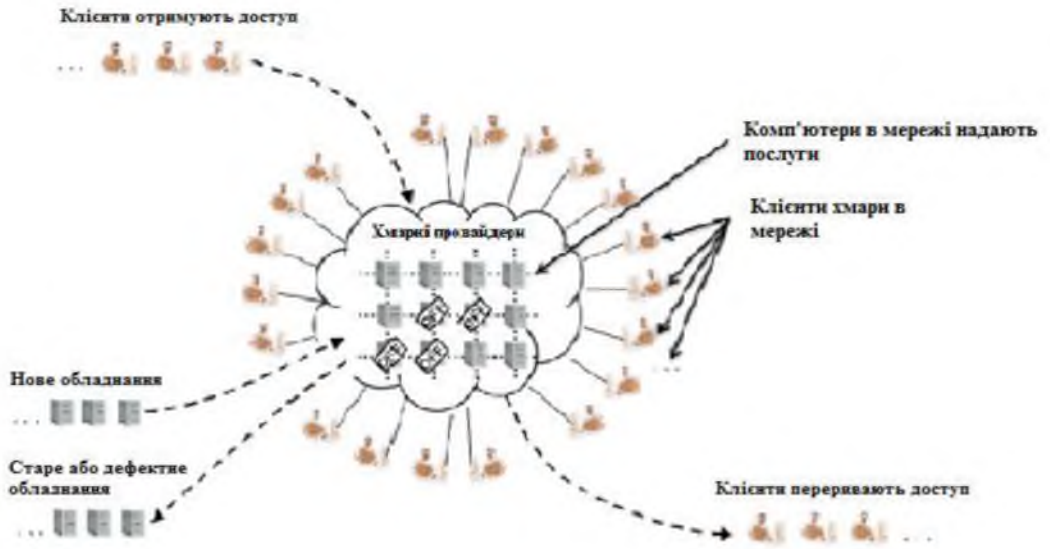

Рисунок 1.1 – Загальна схема «хмара» та передплатники

Для підтримки високої доступності сервісів, незважаючи на очікувані відмови і закінчення терміну життя компонент, хмара, по мірі виникнення необхідності, підключає нові і виводить з експлуатації старі апаратні компоненти або ті, що відмовили. Хмара ефективно управляє пулом апаратних ресурсів для оптимального, з точки зору витрат, надання сервісів.

Одна зі стратегій такого управління полягає в тому, що хмарний провайдер відключає невикористовуванні компоненти на період скорочення потреб абонентів. З позицій чи управління споживаної потужністю або поновлення апаратного забезпечення, міграція робочих навантажень замовників з одного фізичного комп'ютера на інший є ключовою стратегією, що дозволяє провайдеру оновлювати апаратне забезпечення і консолідувати робочі навантаження без заподіяння незручностей передплатникам.[7, 12]

1.1 Моделі розгортання та обслуговування хмарного сервісу

Модель розгортання (модель охоплення, модель розміщення) характеризує базу користувачів, яким надаються ресурси. На рисунку 1.2 показані моделі розгортання «хмари».[2,9]

Рисунок 1.2 – Моделі розгортання «хмари»

Приватна хмара – інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), можливо також клієнтами та підрядниками даної організації. Приватна хмара може перебувати у власності, управлінні та експлуатації, як самої організації, так і третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.[2,9,17]

Публічна хмара – інфраструктура, призначена для вільного використання широкою публікою. Публічна хмара може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будь-якої їх комбінації). Публічна хмара фізично існує в юрисдикції власника — постачальника послуг. [2,9,17]

Гібридна хмара – це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних), що залишаються унікальними об'єктами, але пов'язаних між собою стандартизованими чи приватними технологіями передачі даних та програм (наприклад, короткочасне використання ресурсів публічних хмар для балансування навантаження між хмарами). [2,9,17]

Громадська хмара – вид інфраструктури, призначений для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання (наприклад, місії, вимоги безпеки, політики, та відповідності різним вимогам). Громадська хмара може перебувати в кооперативній (спільній) власності,

управлінні та експлуатації однієї або більше з організацій спільноти або третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника. [2,9,17].

Модель обслуговування співвідноситься з рівнем або типом сервісів, що надаються хмарної системою. На рисунку 1.3 показана архітектура хмарних обчислень.[2,9,13]

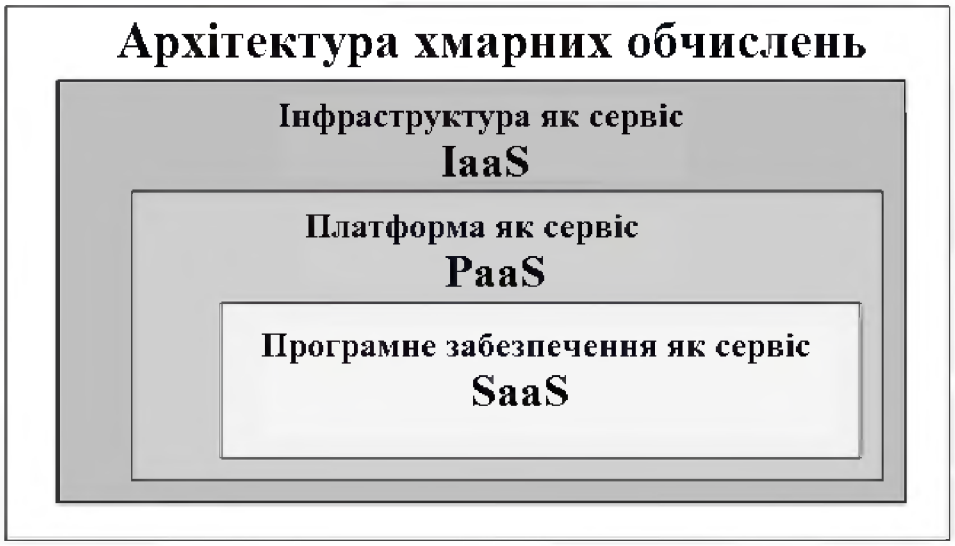

Рисунок 1.3 – Архітектурні компоненти «хмар»

Програмне забезпечення як послуга (SaaS, англ. Software-as-a-Service) – модель, в якій споживачеві надається можливість використання прикладного програмного забезпечення провайдера, який працює в хмарній інфраструктурі і доступний з різних клієнтських пристроїв або за допомогою тонкого клієнта, наприклад, з браузера (наприклад, веб-пошта) або інтерфейс програми. Контроль і керування основною фізичною і віртуальною інфраструктурою хмари, в тому числі мереж, серверів, операційних систем, зберігання або навіть індивідуальних можливостей програми (за винятком обмеженого набору налаштувань конфігурації програми) здійснюється хмарним провайдером. [2,9]

Платформа як послуга (PaaS, англ. Platform-as-a-Service) – модель, яка надає споживачеві можливість використання хмарної інфраструктури для розміщення базового програмного забезпечення для подальшого розміщення на ньому нових або існуючих додатків (власних, розроблених на замовлення

або придбаних тиражованих додатків). До складу таких платформ входять інструментальні засоби створення, тестування та виконання прикладного програмного забезпечення, системи управління базами даних, сполучне програмне забезпечення, середовища виконання мов програмування – надаються хмарним провайдером. [2,9]

Контроль і керування основною фізичною і віртуальною інфраструктурою хмари, в тому числі мереж, серверів, операційних систем, зберігання здійснюється хмарним провайдером, за винятком розроблених або встановлених додатків, а також, по можливості, параметрів конфігурації середовища (платформи). [2,9]

Інфраструктура як послуга (IaaS, англ. Infrastructure-as-a-Service) надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки, зберігання, мереж та іншими фундаментальними обчислювальними ресурсами, наприклад, споживач може встановлювати і запускати довільне програмне забезпечення, яке може включати в себе операційні системи, платформенне і прикладне програмне забезпечення. [2,9]

Споживач може контролювати операційні системи, віртуальні системи зберігання даних і встановлені програми, а також обмежений контроль набору доступних сервісів (наприклад, міжмережевий екран, DNS). Контроль і керування основною фізичною і віртуальною інфраструктурою хмари, в тому числі мереж, серверів, типів використовуваних операційних систем, систем зберігання здійснюється хмарним провайдером. [2,9]

Якщо у користувача у власності є апаратні засоби і необхідно забезпечувати їх роботу, то необхідно враховувати такі фактори, як недостатня потужність серверів, вирішення надзвичайних ситуацій, динамічне виділення ресурсів та можливі проблеми з електропостачанням.

Переваги «хмарного» ЦОД (рисунок 1.4) полягають в тому, що гнучкість надання ресурсів може забезпечити безпрецедентну економію – мінімум невикористаних ресурсів.[17]

Рисунок 1.4 – Переваги «хмарного» ЦОД

Планування необхідної потужності і забезпечення ресурсами завжди грає важливу роль. Хмарні обчислення спрощують рішення деяких проблем, які необхідно вирішувати в тому випадку, якщо апаратні засоби перебувають у власності користувача. Наприклад, якщо у користувача немає фінансових можливостей для розширення бізнесу на той момент, коли постає проблема купівлі нового обладнання. Якщо користувач керує власною інфраструктурою, то йому будуть потрібні чималі кошти на кожну нову мережу пристроїв зберігання даних (Storage Area Network, SAN) або кожен придбаний сервер. Крім того, буде потрібен досить значний час на введення в експлуатацію – від моменту прийняття рішення до розміщення замовлення, оплати, фізичної доставки, приймання, монтажу, інсталяції ПЗ, тестування і, нарешті, введення в експлуатацію.[2,17]

Природно, що будь-який високоякісний сервер має деякий резерв, що дозволяє безболісно вирішити деякі типові апаратні проблеми. Але, навіть якщо є, наприклад, резервний жорсткий диск, призначений на заміну диска в складі масиву RAID, який відмовив, все одно хтось має замінити відмовивший диск, управляти процедурою RMA, а потім встановити новий диск на сервер. Для цього потрібно не тільки час, а і висока кваліфікація, і при цьому необхідно провести всі ці роботи в стислі терміни, щоб уникнути повного виходу сервера з ладу.[21,21]

Якщо сервер остаточно вийде з ладу, то, якщо тільки користувач не має інфраструктури з високим ступенем відмово стійкості, він зіштовхнетеся з проблемами, і всі співробітники повинні будуть діяти в умовах форс-мажорних обставин, роблячи всі зусилля для усунення наслідків виниклої аварійної ситуації. У таких випадках залишається тільки сподіватися на те, що є якісна і актуальна резервна копія, а план аварійного відновлення опрацьовано досить добре, щоб провести відновлення в найкоротші можливі терміни. Відновлення – це майже завжди ручний процес.

Цілком можливо, що потужності обладнання, яке ви використовуєте, з часом зміняться. Крім того, цілком можливо, що необхідно буде вивести з експлуатації застарілий і знецінений сервер. Навіть якщо користувач хоче повністю списати застарілий сервер, все одно хтось повинен буде цим займатися. [21,22]

При управлінні власною інфраструктурою, може знадобитися оплачувати нерухомість або електроенергію, не використовуючи при цьому велику частину оплачуваних ресурсів, що являє собою зовсім непродуктивну витрату грошей.

При використанні хмарної інфраструктури жоден з наступних аспектів не викликає особливих проблем, тому що:

- потужності у хмарну інфраструктуру додаються тільки на той момент, коли вони дійсно потрібні. Немає ніяких витрат, асоційованих з виділенням ресурсів, тому немає необхідності турбуватися про синхронізацію потреб у потужностях та бюджетні потреби. Можна наростити потужність за лічені хвилини;
- немає необхідності турбуватися про апаратні засоби, на яких працюють сервіси;
- можна взагалі не дізнатися про те, що фізичний сервер, на якому фактично виконувалася робота, повністю відмовив. Якщо правильно підібрано інструментарій, то можна добитися автоматичного відновлення після найскладніших аварійних ситуацій;

- якщо потреби в потужностях змінюються, то може знадобитися інша віртуальна апаратна конфігурація. У цьому випадку користувач просто відмовляється від свого віртуального сервера і отримує інший;
- немає необхідності платити за нерухомість і електроенергію. Оскільки використовується лише частина апаратних потужностей, підвищується ефективність використання фізичного простору, необхідного для забезпечення потреб в обробці інформації.[23]

1.2 Хмарне сховище та апаратна віртуалізація

Апаратна віртуалізація являє собою технологію, яка дозволяє більшості постачальників послуг хмарних обчислень пропонувати свої послуги. Якщо у користувача є комп'ютер, на якому він запускає Windows або Linux в таких емуляторах, як Parallels або Fusion, то він використовує технологію віртуалізації, аналогічну тій, що застосовується для реалізації хмарних обчислень. Завдяки віртуалізації адміністратор IT може підрозділити фізичний сервер на будь-яку кількість віртуальних серверів, кожен з яких працює під управлінням власної операційної системи і кожному з яких виділяються такі ресурси, як пам'ять, CPU, ділянки дискового простору. Деякі технології віртуалізації навіть дозволяють переміщати працюючі екземпляри віртуальних серверів з одного фізичного сервера на інший. З точки зору користувача або програми, які працюють на віртуальному сервері, не існує ніяких можливостей визначити, чи є сервер, на якому вони працюють, віртуальним або фізичним.[24,26]

Ряд віртуалізаційних технологій, доступних на ринку, використовують різні підходи до проблеми віртуалізації. Xen представляє собою розширення популярної системи віртуалізації на основі відкритого коду. Xen надає компоненти так званих гіпервізорів, на яких можуть працювати одна або декілька операційних систем. Гипервізор створює рівень апаратних абстракцій, який дозволяє операційним системам спільно використовувати ресурси фізичного сервера. [26]

Абстрагування від апаратних засобів в хмарі здійснюється не тільки завдяки заміні фізичних серверів віртуальними. Віртуалізації підлягають і системи фізичного зберігання даних.

Хмарне сховище дозволяє переміщувати дані в хмару, і при цьому не турбуватися про те, як саме вони зберігаються, і не замислюватися про їх резервне копіювання. Коли дані, переміщені в хмару, знадобляться знову, достатньо буде просто звернутися в хмару і отримати їх. При цьому можна не знати, як зберігаються ці дані, де вони зберігаються, і що відбувається з тим чи іншим обладнанням, коли вони періодично переміщаються в хмару і навпаки.

Як і у випадку з іншими елементами хмарних обчислень, на ринку пропонується кілька підходів до хмарного сховища. Всі вони пов'язані з розбивкою даних на невеликі ланцюжки та зберігання їх на безлічі серверів. Ланцюжки даних забезпечуються індивідуально обчисленими контрольними сумами, так, щоб дані можна було швидко відновити, незалежно від того, що могло б відбутися протягом часу зберігання з накопичувачами, що фізично зберігають дані, і скомпрометувати хмару.[19]

З точки зору принципу роботи, хмарне сховище принципово відрізняється від традиційних мережевих накопичувачів, і слугує принципово іншим цілям. Хмарне сховище може працювати повільніше, адже має велику ступінь структурованості, внаслідок чого його використання в якості оперативного сховища даних непрактично, незалежно від того, чи працює програма, що використовує ці дані, у хмарі або ще десь.[22]

1.3 Хмарні обчислення — переваги і недоліки

1.3.1 Переваги хмарних обчислень

Концепція хмарних обчислень значно змінила традиційний підхід до доставки, управління та інтеграції додатків. У порівнянні з традиційним підходом, хмарні обчислення дозволяють управляти більшими інфраструктурами, обслуговувати різні групи користувачів у межах однієї

хмари. Далі буде розглянуто переваги хмарних обчислень більш детально.[17]

- Недорогі комп'ютери для користувачів.

Користувачам немає необхідності купувати дорогі комп'ютери, з великим об'ємом пам'яті і дисків, щоб використовувати програми через веб-інтерфейс. Також немає необхідності в CD і DVD приводах, так як вся інформація і програми залишаються в «хмарі». Користувачі можуть перейти зі звичайних комп'ютерів і ноутбуків на більш компактні і зручні нетбуки.[17]

- Збільшена продуктивність комп'ютерів користувачів.

Оскільки велика частина програм і служб запускаються віддалено в мережі Інтернет, комп'ютери користувачів з меншим числом програм швидше запускаються і працюють.

- Зменшення витрат і збільшення ефективності IT інфраструктури.

Звичайні сервера середньої компанії завантажені на 10–15%. В одні періоди часу є потреба в додаткових обчислювальних ресурсах, в інших ці дорогі ресурси простоюють. Використовуючи необхідну кількість обчислювальних ресурсів в «хмарі» в будь-який момент часу, компанії скорочують витрати на обладнання та його обслуговування до 50%. При цьому багато разів збільшується гнучкість виробництва в постійно мінливій економічній обстановці.

- Менше проблем з обслуговуванням.

Так як фізичних серверів з впровадженням хмарних технологій стає менше, їх стає легше і швидше обслуговувати. Що стосується програмного забезпечення, то воно вже встановлене, налаштоване і постійно оновлюється в «хмарі».

- Зменшення витрат на придбане програмне забезпечення.

Замість придбання пакетів програм для кожного локального користувача, компанії купують потрібні програми в «хмарі». Дані програми будуть використовуватися тільки тими користувачами, яким ці програми необхідні в роботі. Більше того, вартість програм, орієнтованих на доступ через Інтернет, значно нижче, ніж їх аналогів для персональних комп'ютерів.

Якщо програми використовуються не часто, то їх можна просто орендувати з погодинною оплатою. [17]

- Постійне оновлення програм.

Коли користувач запускає віддалену програму в будь-який час, він може бути впевнений, що ця програма має останню версію – без необхідності щось встановлювати заново або платити за оновлення.

- Збільшення доступних обчислювальних потужностей.

У порівнянні з персональним комп'ютером обчислювальна потужність, доступна користувачу «хмарних» комп'ютерів, практично обмежена лише розміром "хмари", тобто загальною кількістю вилучених серверів. Користувачі можуть запускати більш складні завдання, з великою кількістю необхідної пам'яті, місця для зберігання даних, тоді, коли це необхідно. [22]

- Необмежений обсяг збережених даних.

У порівнянні з доступним місцем для зберігання інформації на персональних компьютерах, обсяг сховища в «хмарі» може гнучко і автоматично підлаштовуватися під потреби користувача. При зберіганні інформації в «хмарі» користувачі можуть забути про обмеження, що накладаються звичайними дисками, «хмарні» розміри обчислюються мільярдами Гб доступного місця.[17]

- Сумісність з більшістю операційних систем.

В хмарних технологіях операційні системи не грають ніякої ролі. Користувачі Unix можуть обмінюватися документами з користувачами Microsoft Windows і навпаки без жодних проблем. Доступ до програм і віртуальним комп'ютерам відбувається за допомогою веб-браузера або іншими засобами доступу, що встановлюються на будь-який персональний комп'ютер з будь-якою операційною системою.[22]

- Покращена сумісність форматів документів.

Якщо користувачі користуються однією «хмарною» програмою для створення і редагування документів, у них просто немає несумісності версій і форматів, на відміну від тих, хто, наприклад, отримає документ Word 2007 і не

зможе прочитати його на локальному комп'ютері з Word 2003 або OpenOffice.

- Простота спільної роботи групи користувачів.

При роботі з документами в «хмарі» немає необхідності пересилати один одному їх версії або послідовно редагувати їх. Тепер користувачі можуть бути впевненими, що перед ними остання версія документа і будь-яка зміна, внесена одним користувачем, миттєво відбивається в іншого. [17]

- Повсюдний доступ до документів.

Якщо документи зберігаються в «хмарі», вони можуть бути доступні користувачам у будь-який час і в будь-якому місці. Більше немає такого поняття як забуті файли: якщо є Інтернет – вони завжди поруч.[22]

- Завжди сама остання і свіжа версія.

В «хмарі» завжди знаходиться сама остання і найсвіжіша версія програми або документа.

- Доступність з різних пристроїв.

Користувачі хмарних технологій мають набагато більш широкий вибір пристроїв доступу до документів і програм. Тепер можна вибирати між звичайним персональним комп'ютером, ноутбуком, Інтернет-планшетом, смартфоном або нетбуком.[17]

- Стійкість даних до втрати або крадіжки обладнання.

Якщо дані зберігаються в «хмарі», їх копії автоматично розподіляються по декільком серверам, які можливо знаходяться на різних континентах. При крадіжці або поломці персональних комп'ютерів користувач не втрачає цінну інформацію, яку він до того ж може отримати з будь-якого іншого комп'ютера. Хтось може заперечити, що резервне копіювання на інший персональний комп'ютер або на інші носії інформації, наприклад, DVD диски або флеш-накопичувачі, також убезпечить дані. Але в останньому випадку треба врахувати два моменти. По-перше, за резервним копіюванням треба стежити і регулярно його виконувати. По-друге, дані методи не забезпечують фізичної безпеки, наприклад, від пожежі або крадіжки. [22]

1.3.2 Недоліки хмарних обчислень

Недоліків хмарних обчислень значно менше, але все ж таки вони є суттєвими для організацій, які планують перехід на використання цієї технології.

- Постійне з'єднання з мережею Інтернет. [22]

Хмарні технології завжди вимагають з'єднання з мережею Інтернет. Або майже завжди. Деякі «хмарні» програми завантажуються на локальний комп'ютер і використовуються в той час, коли Інтернет недоступний. В інших випадках, якщо немає доступу до Інтернету – немає роботи, програм, документів. Це напевно найсильніший аргумент проти хмарних технологій. Але сучасній людині не обійтися без послуг, доступних в мережі Інтернет так само, як і без мобільного телефону, платіжних карт і багато чого іншого. Багато хто вже ні дня не може обійтися без електронної пошти. Тому, враховуючи розвиток сучасного світу, Інтернет буде доступний завжди і скрізь, де ви знаходитесь, як, наприклад, електрика і вода.[17]

- Погано працює з повільним Інтернет-доступом.

Багато «хмарних» програм вимагають гарного Інтернет-з'єднання з великою пропускною здатністю. Сьогодні все рідше і рідше зустрічаються старі неоптоволоконні магістралі для мережі Інтернет, швидкості доступу постійно ростуть, а ціни – знижуються.

- Програми можуть працювати повільніше ніж на локальному комп'ютері.

Деякі програми, в яких потрібна передача значної кількості інформації, працюватимуть на локальному комп'ютері швидше не тільки через обмеження швидкості доступу в Інтернет, але і через завантаженість віддалених серверів і проблем на шляху між користувачем і «хмарою». [22]

- Не всі програми або їх властивості доступні віддалено.

Якщо порівнювати програми для локального використання та їх «хмарні» аналоги, останні поки програють у функціональності.

- Безпека даних може бути під загрозою. Тут ключовим є слово «може».

Все залежить від того, хто надає «хмарні» послуги. Якщо провайдер

постійно робить резервні копії ваших даних, вже не один рік працює на ринку подібних послуг і має хорошу репутацію, то загрози безпеки даних може ніколи не статися. Як сказав відомий фахівець з криптографії та комп'ютерної безпеки Брюс Шнайєр, все питання в довірі. [22]

Якщо Ваші дані в «хмарі» втрачені, вони втрачені назавжди. Це факт. Але втратити дані в «хмарі» набагато складніше, ніж на локальному комп'ютері. Незважаючи на те, що кількість плюсів перевершує мінуси, в кожній конкретній ситуації вони мають велику важливість або, навпаки, не мають ніякого значення.

1.4 Оцінка ефективності хмарних сервісів

1.4.1 Продуктивність хмарних сервісів

Для того щоб порівняти хмари, потрібно вибрати параметри їх оцінки.По-перше, параметри оцінки мають бути безпосередньо пов'язані з продуктивністю додатків, повинні бути зрозумілі і безпосередньо відображати різні аспекти продуктивності. Наприклад, параметри зберігання повинні відображати ефективність вводу/виводу для додатків, що інтенсивно використовують системи зберігання. По-друге, параметри повинні бути застосовні до самих різних провайдерів, незалежно від того, як вони реалізують сервіси. Наприклад, одні провайдери використовують віртуальні машини Xen, а інші Hyper-V або інші внутрішні технології віртуалізації. Ці параметри повинні бути абстраговані від деталей реалізації та відображати вплив на продуктивність сервісів від початку до кінця. [21]

При користування більшістю сервісів, клієнти повинні платити за спожиті ресурси. Користувачі, для яких вартість має важливе значення, можуть відмовитися від послуг провайдера хмари, що пропонує кращу продуктивність, але за високими цінами. Зробити вибір користувачам допоможуть два параметри визначення рентабельності платних сервісів хмари: вартість виконання еталонного тесту для оцінки рентабельності

примірника віртуальної машини та рентабельність різних сервісів зберігання на основі вартості кожної операції зберігання.[21]

1.4.2 Швидкість масштабування

Унікальна особливість хмари – масштабований обчислювальний кластер. Швидкість масштабування може виявитися критичною і для продуктивності, і для вартості додатків, що працюють з мінливим навантаженням. При збільшенні навантаження швидкість масштабування повинна бути такою, щоб якість сервісу не знижувався. Навіть коли робоче навантаження низьке, споживачеві все одно доводиться мати кілька запасних копій на випадок його різкого зростання, тому чим швидше може масштабуватися кластер, тим менше резервних примірників потрібно споживачам, що в свою чергу знижує витрати.

Для порівняння швидкості масштабування обчислювальних кластерів можна використовувати параметр «затримки при масштабуванні» – час, необхідний для отримання нового примірника віртуальної машини, від моменту видачі запиту до моменту, коли машина буде готова обслуговувати додаток.[20]

1.4.3 Узгодженість зберігання

Хмарні провайдери, як правило, виконують послуги зі зберігання даних розподілено. Це підвищує готовність і масштабованість. Однак це не гарантує узгодженості зберігання, тому можливі ситуації, коли операції читання повертають застарілі дані. Для порівняння узгодженості даних у сервісів зберігання різних провайдерів можна, наприклад, вибрати параметр «час повернення в узгоджений стан» – час, через який елемент даних (рядок у таблиці, бінарний об'єкт або повідомлення черги) стає доступним сервісу.[21]

Продуктивність глобальної мережі визначається мінімальною затримкою від деякої середньої точки до центрів обробки даних провайдера.

Припустимо, що провайдер має ЦОД в США і в Європі. Для середньої точки в США мережна затримка при отриманні сервісу для споживача з цієї країни зазвичай менше.

Затримка для середньої точки відповідає реальній затримки при використанні досить гарного алгоритму балансування навантаження, завжди робить запит в найближчий центр обробки даних. У даному дослідженні ця затримка вимірювалася від декількох географічно рознесених середніх точок у PlanetLab.[21]

1.4.4 Вимірювання параметрів

Вимірювання параметрів використовується для того, щоб оцінити продуктивність хмар, які пропонують провайдери хмарних технологій. Було проведено дослідження, в результаті якого було розроблено набір інструментів для вимірювання параметрів послуги від чотирьох провідних провайдерів: Amazon Web Services, GoGrid, CloudSigma, AppEngine, Azure та Cloud Servers. Крім того, деякі сторонні компанії можуть використовувати цей інструментарій для того, щоб запропонувати сервіси порівняння продуктивності хмар в режимі реального часу. Користувачам необхідно лише підписатися на такі сервіси та завантажити дані порівняльного аналізу за певний період часу і для конкретного провайдера.

У кінцевому рахунку порівняння продуктивності хмар робиться для того, щоб можна було швидко і точно вибрати провайдера: користувачів перш за все хвилює продуктивність при виконанні їх застосування у різних провайдерів.

Користувачі можуть прямо застосовувати результати порівняння по одному або декільком параметрам, щоб припустити, якою буде продуктивність програми при роботі з різними провайдерами хмари. Наприклад, для програми інтенсивної обробки документів можна використовувати параметр «час виконання еталонного тесту», щоб визначити, в якій хмарі додаток буде працювати найбільш ефективно.

Аналогічно для програми, що активно використовує системи зберігання, такі як сайт електронної комерції, можна використовувати параметри «затримка сервісу зберігання» і «пропускна здатність сервісу зберігання», щоб визначити провайдера з найбільш придатним сервісом.[22]

1.4.5 Прогнозування продуктивності на основі трасування

Попередній підхід, який передбачає використання набору інструментів для вимірювання параметрів послуги і порівняння продуктивності хмар, дуже простий, але може виявитися обмеженим, оскільки в деяких випадках не зрозуміло, як об'єднувати результати по декільком значним параметрами. Наприклад, складна задача, така як обробка відео, може передбачати й інтенсивні обчислення, і інтенсивне використання систем зберігання. Об'єднання результатів порівняння, що стосуються обчислень і зберігання, є достатньо складним завданням.[20]

Один із способів його вирішення – збір даних про локальне виконання програми та об'єднання локального трасування з результатами вимірювань і прогнозування загальної продуктивності при роботі в мережі.

Трасування показує, як локально виконується додаток і які ресурси використовуються. Можна використовувати результати вимірювання для прогнозування часу, необхідного кожному компоненту хмари. Для серверного компонента можна помножити час центрального процесора, споживане локально, на різницю у швидкості між локальним примірником та екземпляром у хмарі. Що стосується часу, витраченого на запити до бази даних, то можна безпосередньо використовувати параметр «операційна затримка» сервісів зберігання. Після чого можна скласти всі прогнозовані періоди часу. Отримане значення дозволить оцінити реальний час виконання даної програми в хмарі. [20]

Однак при реалізації такого підходу виникають проблеми, і одна з них полягає в складності автоматичного отримання трасування виконання програми, враховуючи, що такі трасування можуть суттєво відрізнятися в

залежності від типу програми.

Ще одна проблема полягає у неможливості точно передбачити час, який буде витрачено віртуальною машиною, оскільки в деяких випадках просте множення на коефіцієнт може внести суттєву помилку. Досі явно не вирішене питання полягає в тому, як спроектувати платформу прогнозування продуктивності в хмарі, що забезпечує високу точність і вимагає мінімального втручання користувачів.[21]

Продуктивність може стати не єдиним критерієм вибору провайдера – керованість, готовність і надмірність даних також є критичними.

У даному випадку найбільш критичним є забезпечення захисту інформації, що знаходиться у хмарі або взаємодіє з нею.

Також до уваги приймалося забезпечення доступності, надійності та відказостійкості хмарного сервісу.

У таблицях 1.1, 1.2, 1.3 приведено основні та додаткові сервіси, що надають найбільші провайдери хмарних сервісів Microsoft Azure, GoGrid, CloudSigma.

При порівнянні даних із таблиць 1.1, 1.2, 1.3 видно, що найбільш повний пакет послуг серед компаній, які є провайдерами хмарних сервісів, надає компанія Microsoft Azure.

Таблиця 1.1 – Сервіси, що надаються провайдерами. Функціональні можливості

Функціональні можливості	Microsoft Azure	GoGrid	CloudSigma
Вільний вибір операційної системи	Так	Ні	Ні
Гнучкий ресурс вибору розмірів «хмари»	Так	Ні	Ні
Широкий діапазон вибору розмірів «хмари»	Так	Ні	Ні
Контроль використання кількості ядер процесора	Так	Ні	Ні
Наявність стійких серверів	Так	Так	Ні
Постійне зберігання інформації	Так	Так	Ні
Можливість серверного клонування	Так	Ні	Ні
AES шифрування	Так	Ні	Ні
Автоматичне резервування та відновлення системи	Так	Так	Ні

Таблиця 1.2 – Сервіси, що надаються провайдерами. Можливості доступу

Можливості доступу	Microsoft Azure	GoGrid	CloudSigma
FTP – доступ панелі керування	Так	Ні	Ні
Контроль API	Так	Не повністю запропоновано	Не повністю запропоновано
Повний браузерний контроль	Так	Так	Так

Таблиця 1.3 – Сервіси, що надаються провайдерами. Можливості мережі

Можливості мережі	Microsoft Azure	GoGrid	CloudSigma
Європейська зона доступності	Так	Ні	Ні
Безкоштовний вхідний трафік	Так	Ні	Не повністю запропоновано
Повністю ізольований мережевий трафік	Так	Так	Ні
Доступність статичного IP та DHCP	Так	Так	Ні
Розміщення власних IP – адрес	Так	Так	Ні
Стандартна функціональність VLAN	Так	Так	Ні
Додаткова функціональність VLAN	Так	Ні	Ні

Ці сервіси бажано, а в деяких випадках і необхідно (в залежності від роду діяльності підприємства), використовувати для виконання тих чи інших функцій, якими займаються приватні підприємства.

1.5 Доступність

Коли підприємство надає клієнтам якийсь сервіс – не важливо, який саме, хмарний чи традиційний на основі власного центру обробки даних – то ця компанія, як правило, надає клієнтам угоду про рівень сервісу (SLA), де вказуються ключові параметри (рівні сервісу), яких клієнт має право очікувати від даного сервісу.

Перш, ніж прийняти рішення про перехід на хмарні технології, необхідно зрозуміти, що представляють собою доступність, надійність і продуктивність хмарних сервісів. [22]

Доступність – властивість ресурсу системи, яка полягає в тому, що користувач або процес, який володіє відповідними повноваженнями, може

використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.[21,22]

Тобто, це показник, який вказує, наскільки часто може використовуватися сервіс протягом визначеного періоду часу. Наприклад, якщо Web-сайт доступний протягом 710 годин з 720-годинного періоду (1 місяць), то можна сказати, що протягом цього місяця доступність сервера становила 98,6%.

Хоча показник 98,6% на перший погляд здається дуже гарним, прийнятність цього значення в дійсності сильно залежить від того, для якого застосування заміряється цей показник, а іноді і від того, які окремі функції програми були доступними.

Більшість вважають, що система має високу доступність, якщо оголошене очікуване значення показника доступності становить від 99,99 до 99,999%. При доступності 99,999% система може виявитися недоступною тільки 5 хвилин 15 секунд на рік. [21,22]

Більшість перебоїв в роботі сервісів представляють собою результат неполадок в роботі устаткування. Ці перерви в роботі можуть виявитися тривалими, якщо адміністратори сервісу неправильно діагностують причину збою або допустять інші помилки в усуненні проблеми. Таким чином, для оцінки очікуваної доступності повинні використовуватися дві змінні:

- ймовірність виникнення збоїв або неполадок системи протягом оціночного періоду;
- очікуваний час простою у разі виникнення збоїв і неполадок.

Очікувана доступність компонента виражається наступною математичною формулою:

$$a = (p-(c * d)) / p, \quad (1.1)$$

де:

a – очікувана доступність;

c – ймовірність (%) відмови сервера протягом заданого періоду;

d – очікуваний час простою внаслідок відмови сервера;

p – оцінюваний період.

Щоб отримати надійну оцінку доступності, необхідно оцінити всі можливі компоненти, відмова яких може призвести до перебоїв у роботі, і підсумувати їх. Доступність системи оцінюється як різниця загальної тривалості оціночного періоду мінус сума тривалості всіх простоїв протягом цього періоду, поділена на загальну тривалість оціночного періоду:

$$a = (p - SUM (cl * dl / cn * dn)) / p. \quad (1.2)$$

Наприклад, якщо ваш провайдер зазвичай відчуває технічні проблеми два рази на рік, причому час простою зазвичай становить дві години, то доступність Інтернет-з'єднання оцінюється так:

$$(8760 - (200\% * 2)) / 8760 = 99,95\%. \quad (1.3)$$

Таким чином, загальний показник доступності системи буде таким:

$$(8760 - ((40\% * 24) + (200\% * 2))) / 8760 = 99,84\%. \quad (1.4)$$

Чим більше точок відмови, які являють собою компоненти, відмова яких призведе до простою системи, тим нижче її рейтинг доступності. Далі, тривалість часу простою робить ще більш сильний вплив на ймовірність того, що сервіс буде недоступний.[21,22]

Побічно вирішити проблему допомагає надмірність. Якщо є два або більше фізичних компонентів, що представляють логічні компоненти, то очікуваний час простою логічного компонента являє собою очікувану тривалість періоду часу в разі події, коли всі ці фізичні компоненти відмовлять одночасно. Іншими словами, формула (c * d), використовувана для обчислення часу простою, дещо ускладняється і приймає наступний вигляд:

$$(c * d^{n)} / (p^{(n-1)}). \quad (1.5)$$

У цій формулі n представляє собою рівень надлишковості системи. У випадку, коли n = 1, формула, як і очікувалося, спрощується:

$$(c * d^{n}) / (p^{(n-1)}) = (c * d) / (p^{0}) = c * d. \quad (1.6)$$

Якщо в розглянутому прикладі в систему додати ще один надлишковий компонент – ще один сервер, то це дозволить швидко переходити на інший ресурс при збої, і в даному випадку оцінка доступності вашого Web-сервера буде набагато покращена:

$$(8760 - ((40\% * 24^{2})) / (8760^{(2-1)})) / 8760 = 99{,}999\%. \quad (1.7)$$

Більшість відмов, які в традиційних центрах обробки відбуваються рідко, в хмарній інфраструктурі трапляються часто. Цей уявний недолік надійності компенсується тим фактом, що більшість відмов, які в звичайному центрі обробки даних вважаються катастрофічними, у хмарі є буденністю.

Такі події, як втрата фізичного сервера без будь-яких попереджень, трапляються вкрай рідко. Навпаки, коли один з компонентів відмовляє (або видає попередження про високу ймовірність відмови), він замінюється надлишковим компонентом, що дозволяє уникнути простою системи.

У фізичній інфраструктурі втрата сервера – це катастрофа. Фактично в хмарному середовищі можна втратити цілу зону доступності і вважати це дрібним інцидентом. Навпаки, при роботі у фізичному середовищі, раптова втрата всього центру обробки даних буде великою катастрофою. [23]

1.6 Надійність

Надійність часто пов'язана з доступністю, хоча в дійсності надійність представляє собою дещо іншу концепцію. Зокрема, надійність зводиться до того, наскільки можна покладатися на здатність системи захищати цілісність даних і виконувати транзакції. Нестабільність, асоційована з низькою доступністю дуже часто викликає питання, в результаті якого користувачі не відчувають впевненості в тому, що їхній останній запит дійсно був виконаний, що часто може призвести до пошкодження даних в системах управління реляційними базами даних.

Очевидно, що система, яка часто недоступна, не може вважатися і

надійною. Система з високим рівнем доступності, тим не менш, теж може бути ненадійною, якщо є недовіра до даних, які вона надає. Таке може статися, наприклад, у разі, коли один з процесів або компонентів несподівано зупиняється, ніяк про це не повідомляючи.[23]

У значній мірі надійність вашої системи залежить від того, як написаний код, керуючий її роботою. Хмарна структура має ще ряд аспектів, що виходять за рамки написання коду вашої програми, які, тим не менш, теж можуть вплинути на надійність вашої системи. У хмарному середовищі найбільш серйозним серед цих аспектів є те, як керувати постійними даними.

Оскільки віртуальні екземпляри мають тенденцію мати більш низьку доступність в порівнянні з їх фізичними аналогами, шанс на те, що дані виявляться пошкодженими, в хмарному середовищі підвищується в порівнянні з фізичною центром обробки даних. Зокрема, кожен раз, коли відбувається втрата сервера, істотний вплив можуть надати такі чинники:

- втрачаються будь-які дані, які зберігаються в цьому екземплярі і ніколи не резервувалися;
- пристрої блокового зберігання піддаються ризику пошкодження (в точності так само, як це може статися і в традиційному центрі обробки даних).

Слід пам'ятати два правила, які дозволять підвищити надійність додатків, розгорнутих в хмарному середовищі.

- Не слід зберігати постійні дані в ефемерних сховищах примірника.
- Треба регулярно створювати моментальні знімки блокових томів.[23]

1.7 Продуктивність

Всі питання, про які треба потурбуватись при розгортанні високопродуктивних трансакційних програм у фізичному центрі даних, відносяться і до розгортання додатків в хмарному середовищі.

Рекомендації:

- плануйте використання хмар таким чином, щоб логічні операції могли бути розподілені по безлічі серверів;

- якщо не створюються кластери серверів баз даних, треба сегментувати доступ до бази даних таким чином, щоб операції читання могли виконуватися на підлеглих серверах, а операції запису – на головному;
- застосовуйте такі механізми, як багатопоточність і / або розгалуження процесів, щоб якомога ефективніше реалізувати потенціал кожного окремого процесорного ядра.[22]

1.8 Безпека хмарного сервісу

Хмарні послуги є одним із способів передачі даних з пункту А в пункт Б, їх зберігання та обробки. У цей момент виникає багато питань, пов'язаних з цим процесом, наприклад, можлива втрата даних, яка відповідальність у разі втрати даних.[16, 29]

З хмарними послугами пов'язані такі важливі для кожного підприємства питання, як:

- конфіденційність даних;
- права власності на дані;
- правові вимоги щодо збереження даних;
- вимоги державного законодавства до обробки даних та місця їх знаходження;
- вимоги зарубіжних законодавств до обробки даних та місцем їх знаходження.

Крім аспектів відповідності законам, стандартам і специфікаціям, хмарна середа піднімає ще одне питання: юридичні проблеми, пов'язані з тим, де саме зберігаються дані:

- Дані можуть представлятися для розгляду в судових інстанціях за повістками із судів або можуть бути використані в інших судових діях, в яких бере участь провайдер і які можуть вимагати інших процедур.
- В деяких країнах (наприклад, в станах Євросоюзу) законодавство пред'являє досить жорсткі вимоги, які вказують де і як повинні зберігатися конфіденційні дані.[16, 29]

За даними Forrester Research, половина організацій, не впроваджують хмарні технології, виправдовує свою поведінку побоюваннями за безпеку. У сфері безпеки організації найбільше стурбовані такими факторами, як захист даних, правильне функціонування систем та їх доступність. При цьому все більшого значення набувають завдання захисту додатків, оптимального моніторингу та аудиту, а також дотримання законодавчих та нормативних вимог.

1.9 Впровадження хмарних технологій

На сьогоднішній день хмарні технології, а також супутні їм продукти, пропонують нові можливості для ведення бізнесу і скорочення поточних витрат. Хмари пропонують IT-продукти та послуги за дуже низької вартості, завдяки тому, що вони розраховані на масове споживання. Довіра споживачів до хмар поступово зростає. Ще кілька років тому високотехнологічні рішення не були так доступні малому бізнесу, як зараз.[10]

Проводиться безліч досліджень, присвячених сприйняттю замовниками технології хмарних обчислень, але всі вони дають подібні результати. Незважаючи на те, що проблеми безпеки та інтеграції остаточно не вирішені, компанії все одно схиляються на користь впровадження хмарних технологій. А ті, хто вже використовує хмарні обчислення деякий час, дуже задоволені результатом. Сімдесят відсотків компаній, які в даний час використовують хмарну платформу, планують перенести на неї додаткові додатки протягом найближчих 12 місяців. Іншими словами, хмарні обчислення стають невід'ємним компонентом IT-стратегії.[30, 36]

Головним аргументом на користь впровадження хмарних технологій є кілька факторів, які представлені на рисунку 1.5). Найважливішими з них є масштабованість і економія коштів.

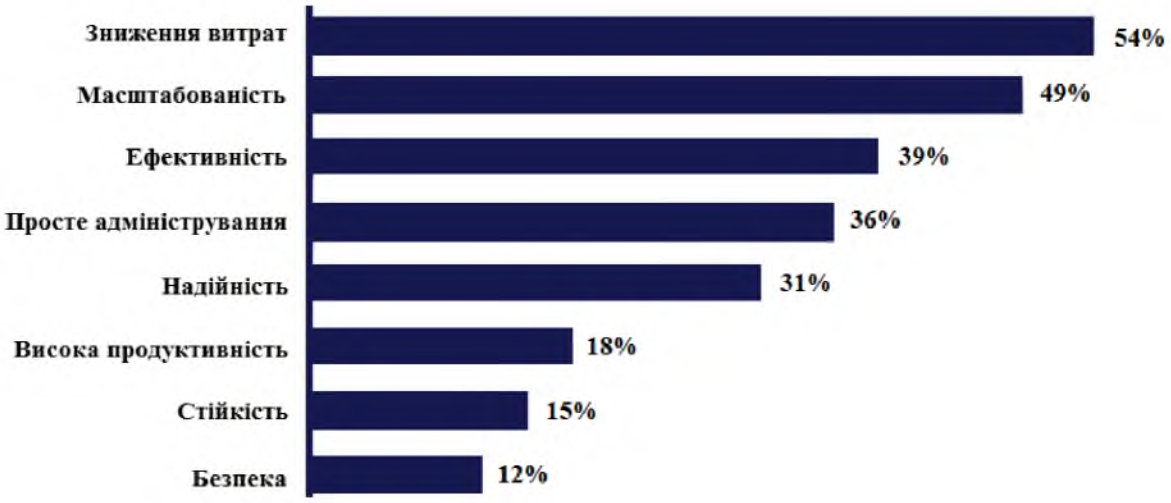

Рисунок 1.5 – Причини переходу компаній на хмарні обчислення

Модель оплати на основі реального використання та зниження капітальних витрат – це основні причини, за якими компанії переходять на хмарні обчислення. Крім того, багато компаній розгортають відразу кілька категорій бізнес-додатків, що призводить до швидкого зростання обсягів даних.

У зв'язку з цим виникає потреба в більш динамічною інфраструктурі зберігання. Вона повинна легко адаптуватися до постійно змінюваних умов бізнесу.

Таким чином, хмарні технології, які забезпечують гнучке надання IT-ресурсів, дозволяють своєчасно реалізовувати нові програми та ініціативи. Серед найбільш значущих інструментів, які переносяться на хмарну платформу, електронна пошта, системи архівування, управління взаємозв'язками з замовниками, зберігання даних.[30]

Темпи переходу на хмарні обчислення в різних галузях різні. У числі перших трьох – технологічні компанії, сектор фінансових послуг, а також сектор юридичних і професійних послуг.

1.10 Компанії, що займаються наданням «хмарних» сервісів

Ринок хмарних обчислень постійно зростає і на сьогодні багато компаній

надають послуги хмарних провайдерів. Це такі компанії, як:

- Amazon LCC
- Microsoft
- Google
- IBM
- Salesforce, Inc.
- Rackspace US, Inc
- GoGrid / ServePath LLC
- Akamai Technologies

Дослідницька компанія Evans Data Corp у 2016 році проводила опитування серед користувачів на тему, продукти яких компаній вони використовують або планують використовувати для впровадження хмарних технологій. На рисунку 1.6 в системі координат розташовані постачальники хмарних сервісів відповідно до того, як їх сприймають користувачі. Вісь абсцис показує, наскільки високо замовники оцінюють здатність постачальника реалізувати стратегію хмарних обчислень. По осі ординат розташовані оцінки повноти рішень. Кругові маркери демонструють ступінь освоєння рішень постачальника замовниками, при цьому внутрішній червоний круг показує поточну кількість впроваджень, а зовнішня чорна окружність – кількість впроваджень, що плануються в найближчі 12 місяців. [26]

Рисунок 1.6 – Рейтинг постачальників хмарних сервісів відповідно до того, як їх сприймають користувачі

Як видно з рисунку три компании є лідерами серед провайдерів. На думку опитаних респондентів, вони мають найвищий потенціал для реалізації технології хмарних обчислень.[26, 27]

1.11 Висновок

На сьогоднішній день сфера використання хмарних обчислень дуже стрімко розвивається, але поки залишається барьер, який більшість організацій невзмозі подолати. Ймовірні користувачі бояться самого факту, що інформацію зберігатимуть сторонні люди. І, хоча, майже неможливість втрати або крадіжки даних вже доведена, деякі не готові довіритися подібним сервісам. Інший істотний недолік на даний період часу – це якість, стабільність і швидкість Інтернет-з'єднань, що створює відчутні труднощі.

Однак, незважаючи на суттєві недоліки, переваг від впровадження даної технології набагато більше, особливо для організацій, які тільки розпочинають свою діяльність. Адже це економія для споживачів, боротьба з піратством для розробників, мінімізація витрат в IT сфері для учбових закладів, уніфікація мережевих стандартів для всіх користувачів.

Таким чином формувалися завдання для подальших досліджень:

– на основі проаналізованих в першому розділі даних, провести аналіз загроз для систем на основі хмарних обчислень;

– виділити загрози, реалізація яких може бути критичною для інформації, яка оброблюється в системах на основі хмарних обчислень;

- розробити рекомендації щодо забезпечення інформаційної безпеки при переході на хмарні сервіси учбових закладів.

РОЗДІЛ 2. ДОСЛІДЖЕННЯХ ЗАХИСТУ ІНФОРМАЦІЇ У ХМАРІ

Об'єкт досліджень – хмарні те технології що використовуються у навчальних закладах.

Предмет досліджень – рівень захисту інформації при доступі до хмарних технологій в учбових закладах.

Мета – розробити рекомендацій по підвищенню інформаційної безпеки в інформаційно-комунікаційних системах навчальних закладів, що використовують хмарні технології.

Вихідні дані для проведення роботи:

- державні стандарти України в галузі інформаційної безпеки, нормативні документи з технічного захисту інформації та закони України;
- міжнародні стандарти в галузі інформаційної безпеки.

Наукова новизна роботи полягає в розробці рекомендацій по підвищенню безпеки використання хмарних технологій в інформаційно-комунікаційних системах навчальних закладів.

Практична цінність - отримані результати можуть бути використані для подальшого та поглибленого питань безпеки інформаційних систем учбових закладів що використовують хмарні технології.

Результати повинні відповідати вимогам Закону України «Про інформацію», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99, НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», «Про вищу освіту», Закону України «Про освіту», «Положення

про організацію навчального процесу у вищих навчальних закладах», що затверджено наказом Міністерства освіти України від 2 червня 1993 р. №161, нормативних документів з технічного захисту інформації, державних стандартів України в галузі інформаційної безпеки та інших законів України, що стосуються забезпечення безпеки інформації.

Результати досліджень мають бути подано у вигляді, що дозволяє безпосереднє використання для створення засобів захисту інформації в гібридних або повністю системах хмарних обчислень.

Економічний ефект від реалізації результатів роботи очікується за рахунок підвищення рівня захищеності інформації в учбових закладах що використовують хмарні технології.

Соціальний ефект від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей працівникам навчальних закладів підвищити продуктивність праці та її комфортність.

2.1 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

Відповідно до документу: «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» встановимо критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу при використанні систем хмарних обчислювань.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об’єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об’єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об’єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об’єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

Запити на зміну прав доступу до об’єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об’єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного

об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об’єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об’єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту та імпорту.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів і інтерфейсних процесів, до яких вона відноситься.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається.

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності

інформації, що міститься в об'єкті, який передається.

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен аутентифікувати цього користувача з використанням захищеного механізму.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Розподіл обов’язків адміністраторів

Політика розподілу обов’язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов’язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і аутентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

В ідеальному випадку вище перераховані критерії оцінки захищеності інформації, при використанні систем хмарних обчислювань, мають допомогти визначити вимоги з захисту інформації в комп'ютерних системах від несанкціонованого доступу, створити захищені комп'ютерні системи, оцінити придатність комп'ютерних систем для обробки критичної інформації при використанні хмарних технологій. Але, враховуючи особливості функціонування систем на основі хмарних обчислень, можна передчасно

зробити висновок, що забезпечити деякі критерії буде досить складно, а іноді неможливо.

В подальшій роботі буде проаналізовано основні класи атак на системи, які побудовані на основі хмарних технологій. З урахуванням критеріїв, що пред'являються до захисту інформації в комп'ютерних системах від несанкціонованого доступу буде розроблено рекомендації для захисту від проаналізованих загроз та їх обґрунтування. [39,40]

2.2 Класи загроз систем на основі хмарних технологій

2.2.1 Традиційні атаки на ПЗ

Традиційні атаки на ПЗ – це атаки, пов'язані з уразливістю мережевих протоколів, операційних систем, модульних компонент та інших. Це традиційні загрози, для захисту від яких досить встановити антивірус, міжмережевий екран, IPS та інші потрібні компоненти.

Важливо тільки, щоб ці засоби захисту були адаптовані до хмарної інфраструктури і ефективно працювали в умовах віртуалізації. Тому що, наприклад, міжмережеві екрани призначені на захисту периметра, проте в хмарі непросто виділити периметр для окремого клієнта, що значно ускладнює захист. Тому технологію міжмережевого екранування потрібно адаптувати до хмарної інфраструктури.[33,37]

2.2.2 Функціональні атаки на елементи хмари

Функціональні атаки на елементи хмари пов'язані з багатошаровістю хмари, загальним принципом безпеки, що загальний захист системи дорівнює захисту найслабшої ланки. Так успішна DoS-атака на зворотний проксі, встановлений перед хмарою, заблокує доступ до всієї хмари, не дивлячись на те, що всередині хмари всі зв'язки будуть працювати без перешкод. Аналогічно SQL-ін'єкція, яка пройшла через сервер додатків дасть доступ до

даних системи, не залежно від правил доступу в прошарку зберігання даних.

Для захисту від функціональних атак для кожного шару хмари потрібно використовувати специфічні для нього засоби захисту:

- для проксі - захист від DoS-атак;
- для веб-сервера - контроль цілісності сторінок;
- для сервера додатків - екран рівня додатків;
- для шару СУБД - захист від SQL -ін'єкцій;
- для системи зберігання - резервне копіювання і розмежування доступу.

2.2.3 Атаки на клієнта

Атаки на клієнта відпрацьовані у веб-середовищі, але вони також актуальні і для хмари, оскільки клієнти підключаються до хмари, як правило, за допомогою браузера. В нього потрапляють такі атаки як Cross Site Scripting (XSS), перехоплення веб-сесій, крадіжка паролів, "людина посередині" та інші. Захистом від цих атак традиційно є сувора аутентифікації і використання шифрованого з'єднання з взаємною аутентифікацією, однак не всі творці «хмар» можуть собі дозволити настільки марнотратні і, як правило, не дуже зручні засоби захисту.

2.3.4 Загрози віртуалізації

Оскільки платформою для компонентів хмари традиційно є віртуальні середовища, то атаки на систему віртуалізації також загрожують і всій хмарі вцілому. Віртуальним серверам притаманні рівно ті ж уразливості, що і фізичним.

Однією з ключових проблем використання технологій віртуалізації є легітимність захисту інформації, яка обробляється в віртуальному середовищі.

Згідно з українським законодавством організації зобов'язані забезпечити належний захист конфіденційної інформації, з якою вони працюють, у тому

числі із застосуванням сертифікованих засобів захисту.

Ці проблема стосуються як інформації, яка містить відомості, що становлять державну таємницю, так і конфіденційної інформації - комерційної таємниці або персональних даних.

Проблема впровадження технологій віртуалізації пов'язані з тим, що з одного боку, традиційні засоби захисту інформації не завжди сумісні з середовищем віртуалізації, так як спочатку розроблялися для використання у фізичному середовищі. З іншого боку, вони не захищають від нових загроз безпеці інформації, специфічних для віртуальної інфраструктури. Це основні недоліки традиційних засобів захисту.

Якщо порушник отримує доступ до середовища віртуалізації, операційне середовище традиційних систем захисту інформації виявляється повністю скомпрометованим.[24,25]

Цей тип загроз унікальний для хмарних обчислень. Справа в тому, що при використанні цієї технології в системі з'являються додаткові елементи, які можуть бути піддані атаці. До них можна віднести гіпервізор, систему перенесення віртуальних машин з одного вузла на інший і систему управління віртуальними машинами. Перераховані елементи можуть піддатися наступним атакам:

- атака на гіпервізор з віртуальної машини;
- атака на гіпервізор з фізичної мережі;
- атака на диск віртуальної машини;
- атака на засоби адміністрування віртуальної інфраструктури;
- атака на віртуальну машину з іншої віртуальної машини;
- атака на мережу реплікації віртуальних машин.

2.2.5 Атаки на гіпервізор

Ключовим елементом віртуальної системи є гіпервізор, який забезпечує

поділ ресурсів фізичного комп'ютера між віртуальними машинами. Втручання в роботу гіпервізора може привести до того, що одна віртуальна машина може отримати доступ до пам'яті і ресурсів іншої, перехоплювати її мережевий трафік, відбирати її фізичні ресурси і навіть зовсім витіснити віртуальну машину з сервера.

З середовища гіпервізора порушник може непомітно для традиційних систем захисту інформації, що працюють у віртуальних машинах:

- здійснити НСД до сервера віртуалізації та гіпервізора;
- копіювати і блокувати весь потік даних, що йде на всі пристрої (HDD, принтер, USB, мережу);
- читати і змінювати дані на дисках віртуальних машин, навіть коли вони вимкнені, без участі програмного забезпечення цих віртуальних машин.

Сервер віртуалізації може містити помилки чи вразливості.[27]

Поки мало хто з хакерів розуміє, як саме працює гіпервізор, тому атак подібного типу практично немає, проте це ще не гарантує, що вони не з'являться в майбутньому.

Рекомендовані заходи захисту:

- Розмежування доступу до сервера віртуалізації.
- Своєчасне встановлення оновлень ПЗ середовища віртуалізації.
- Обмеження запуску програм.

2.2.6 Атака на диск віртуальної машини

Віртуальна машина зазвичай виконується на сервері віртуалізації, а її диск зберігається в мережі зберігання даних SAN/NAS.

Для підвищення продуктивності систем зберігання даних (і комп'ютерних мереж, в цілому) використовуэться архітектура SAN (Storage Area Network). При застосуванні SAN архітектури встановлюється пряме з'єднання між пристроями зберігання даних і серверами, і, внаслідок цього,

реалізується високошвидкісне переміщення даних між пулом пристроїв зберігання даних і користувачами. SAN архітектура забезпечує виділення мережі зберігання даних, роз'єднуючи зв'язок між сервером додатків і пристроями зберігання даних.

Кінцевою метою використання SAN архітектури є зменшення складності адміністрування системами зберігання даних як в одній мережі, так і в разі приєднання гетерогенної мережі комп'ютерів. Крім того, максимально зменшується втручання людини в роботу систем зберігання даних (без збитку їх продуктивності або доступності).[26]

SAN-пам'ять не є єдиним шляхом розвитку систем зберігання даних. Вона дійсно з'явилася як перше рішення для зберігання великих обсягів даних на рівні підприємства. NAS-пам'ять забезпечує часткове вирішення проблеми прискорення доступу до даних. До складу цього рішення входять пристрої, які іноді називають тонкими серверами. Вони призначені для забезпечення доступу і керування пристроями зберігання даних за дорученням інших серверів або безпосередньо кінцевих користувачів.

NAS-пам'ять знімає функції здійснення доступу та управління доступом до даних з серверів додатків. Крім того, NAS-пам'ять незалежна від ОС, тому через неї може здійснюватися хостинг даних за дорученням всіх користувачів мережі.

Рекомендовані заходи захисту:

- Захист даних віртуальних машин шляхом розмежування доступу до дисків віртуальних машин. Це може бути реалізоване шляхом сертифікованих систем захисту інформації від НСД.

- Використання міжмережевих екранів, які контролюють протоколи і файлові формати віртуальної інфраструктури.

2.2.7 Втрата віртуальних машин

Слід зазначити, що віртуальна машина являє собою файл, який може бути запущений на виконання в різних вузлах хмари. У системах управління

віртуальними машинами передбачені механізми перенесення віртуальних машин з одного вузла на інший. Однак файл віртуальної машини можна і взагалі вкрасти і спробувати запустити її за межами хмари.

Винести фізичний сервер з ЦОДа неможливо, а ось віртуальну машину можна вкрасти по мережі, не маючи фізичного доступу до серверів. Правда, окрема віртуальна машина за межами хмари не має практичної цінності – красти треба як мінімум по одній віртуальній машині з кожного шару, а також дані з системи зберігання для відновлення аналогічної хмари, тим не менш, віртуалізація цілком допускає викрадення частини або всієї хмари цілком.

2.2.8 Атаки на системи управління

Величезна кількість віртуальних машин, які використовуються в хмарах, особливо в публічних хмарах, вимагає таких систем управління, які могли б надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в системи управління може привести до появи віртуальних машин невидимок, блокування одних машин і підстановка в шари хмари неавторизованих елементів. Все це дозволяє зловмисникам одержувати інформацію з хмари або захоплювати її частини чи всю хмару цілком.

Рекомендовані заходи захисту:

- Захист периметру мережі адміністрування шляхом розмежування доступу до серверів віртуальних машин і засобів управління інфраструктурою.

Віртуальні машини одного фізичного рівня можуть обмінюватися трафіком напряму без участі фізичних мережив комутаторів. Таким чином використання фізичних міжмережевих екранів не буде ефективним. [24]

Рекомендовані заходи захисту:

- Модернізація існуючих сертифікованих міжмережевих екранів, їх перенесення у віртуальне середовище.

- Створення спеціалізованих систем захисту інформації від несанкціонованого доступу та міжмережевого екрана, який би контролював

трафік всередині сервера віртуалізації.

2.2.9 Атака на мережу реплікації віртуальних машин

По мережі реплікації віртуальних машин передаються сегменти їх оперативної пам'яті. Можливість перехвату цих даних – пряма загроза безпеці.

Рекомендовані заходи захисту:

- Мережа реплікації даних має бути ізольована від усіх інших мереж або потребується обов'язково використовувати сертифікованих захищених каналів для реплікації.

Простота створення і введення в експлуатацію віртуальних машин може створити проблеми для безпеки, якщо до них не застосовується політика безпеки.

Рекомендовані заходи захисту:

- Організація централізованого процесу управління життєвим циклом віртуальних машин, який чітко прописаний в політиці безпеки організації.

2.2.10 Проблема управління даними

Принципова відмінність між традиційними центрами обробки даних і хмарним середовищем криється в тому, що дані фізично розташовуються на серверах, що належать сторонній компанії. Ті підприємства та організації, які вдалися до послуг аутсорсингу і довірили свої дані провайдерам керованих послуг, частково подолали цю проблему між власною фізичною інфраструктурою IT та хмарним середовищем. Хмарні ж сервіси додають до цього фізичну неможливість навіть побачити сервери, на яких розміщені ваші дані. Основною практичною проблемою є те, що деякі сторонні фактори, що не мають ніякого відношення до вашого бізнесу, можуть, тим не менш, поставити під питання безпеку ваших даних.

Наприклад, створити проблеми у інфраструктурі можуть наступні події.

- Компанія, яка надає хмарні сервіси, оголошується банкрутом, її майно (в тому числі сервери) конфіскується, і провайдер перестає надавати послуги.

- Нездатність хмарного провайдера належним чином захистити компоненти своєї інфраструктури – особливо в тому, що стосується управління фізичним доступом, що може скомпрометувати системи.

Рекомендовані заходи захисту:

- Рекомендується виконувати віддалену копію всієї інформації.

- Рекомендується зашифровувати всі конфіденційні дані у базі даних і в пам'яті. Розшифровувати цю інформацію слід тільки в пам'яті і лише на той час, поки існує потреба в цих даних. Крім того, слід шифрувати резервні копії і всі мережеві комунікації.

- Слід підібрати ще одного хмарного провайдера і регулярно здійснювати автоматизовані процедури резервного копіювання (для цієї мети існують як комерційні рішення, так і рішення на основі відкритого коду). Це дозволить гарантувати можливість відновлення як поточних даних, так і історичної інформації, причому відновлення буде можливо навіть в тому випадку, якщо хмарний провайдер припинить свою діяльність.[27]

2.2.11 Комплексні загрози

Контроль хмар і управління ними також є проблемою безпеки.

Як гарантувати, що всі ресурси хмари пораховані і в ній немає непідконтрольних віртуальних машин, не запущено зайвих бізнес-процесів і не порушена взаємна конфігурація шарів та елементів хмари.

Комплексні загрози «хмарам» пов'язані з керованістю хмарою як єдиною інформаційною системою та пошуком зловживань або інших порушень в роботі хмари, які можуть призвести до зайвих витрат на підтримку працездатності інформаційної системи. Цей тип загроз найбільш високорівневий і для нього неможливо створити універсального засобу захисту – для кожної хмари її загальний захист потрібно будувати індивідуально.[23]

2.2.12 Зупинка діяльності хмарного провайдера

Можливі різні варіанти для зупинки діяльності хмарного провайдера:

- банкрутство;
- згортання бізнесу для переорієнтації на іншу сферу діяльності;
- тривалий простій внаслідок масштабного і тривалого збою в подачі електроенергії.

Що б не відбувалося, є ризик втратити доступ до виробничих систем внаслідок дій іншої компанії. Крім того, користувач ризикує і тим, що організація, що управляє його даними, може не захистити їх відповідно до раніше укладених угод про рівень сервісу.

Найбільш важливий аспект у даному випадку – це регулярне здійснення віддаленого резервного копіювання та зберігання резервних копій за межами виробничого середовища. Ця міра повинна захистити від негативних наслідків, викликаних припиненням роботи хмарного провайдера. Ще краще користуватися послугами ще одного хмарного провайдера, за допомогою якого можна запустити іншу інфраструктуру.[28]

2.2.13 Проблема забезпечення безпеки в хмарних середовищах

У середовищі хмарних обчислень зберігання і перенесення даних виконується іншим способом, що знаходяться поза традиційних уявлень про захист, що створює нові виклики для систем забезпечення безпеки. Для багатьох людей перенесення їх даних в хмарне середовище, де вони не можуть їх контролювати, здається неприйнятним. Крім того, цей підхід дійсно вимагає розгляду питань відповідності стандартам та обліку різних нормативно-правових аспектів. Однак у випадку роботи з хмарним середовищем підхід до інформаційної безпеки теж буде радикально відрізнятися від підходу в традиційному середовищі.[19]

Приймаючи рішення про перехід на хмарну обробку даних, слід розглянути цілу низку критичних аспектів, що стосуються інформаційної

безпеки, в тому числі:

- організаційно-правові аспекти, питання відповідності з місцевим законодавством і стандартами в хмарній інфраструктурі будуть принципово іншими;

- на сьогодні не опубліковано експлойтів, спрямованих на компрометацію системи безпеки хмарної інфраструктури;

- у хмарному сховищі даних слід дотримуватися профілю захищеності, який характеризується високим рівнем безпеки;

- технології віртуалізації, такі як Xen, можуть мати власні вразливості, що може призвести до появи нових напрямків атаки.

Незважаючи на те, що питання безпеки хвилює всіх без винятку користувачів, які тільки починають знайомитися з хмарною обробкою даних і розглядають можливості переходу на хмарну інфраструктуру, насправді в ній існують інші, і набагато більш серйозні питання, пов'язані, перш за все з безпекою.

- Багато законів та стандартів, керуючих інфраструктурою IT, розроблялися без урахування віртуалізації.

- Сама ідея захисту периметра в мережі в хмарному середовищі втрачає сенс, тому що в хмарі немає такого поняття, як «периметр».

- Управління реєстраційною інформацією користувачів виходить за рамки стандартних процедур управління ідентифікаційною інформацією.

Як і в багатьох інших аспектах хмарного середовища, безпека тут теж може бути забезпечена, і навіть на більш високому рівні, ніж у звичайному внутрішньому центрі обробки даних. Ефемерна природа віртуальних примірників вимагає, щоб бралися до уваги надійні процедури забезпечення безпеки, без яких традиційні середовища хостингу можуть обходитися.

Таким чином, перехід на хмарні обчислення може призвести до створення комп'ютерної інфраструктури підвищеної захищеності.

2.3 Модель загроз для хмарних технологій

Загрози для хмарних технологій можна класифікувати за ймовірністю їх втілення та рівнем впливу на ресурси. Ймовірність загроз та їх оцінка наведені у таблиці 2.2.

Таблиця 2.1 – Модель загроз для хмарних технологій

Загроза	Ймовірність втілення	Рівень впливу на ресурс
Атаки на ПЗ	Б	значний
Атаки на клієнта	Б	середній
Комплексні загрози «хмарам»	Б	значний
Зупинка діяльності хмарного провайдера	А	критичний
Загрози віртуалізації	В	критичний
Атаки на гіпервізор	А	критичний
Атака на диск віртуальної машини	В	значний
Перенесення віртуальних машин	А	значний
Атаки на системи управління	Б	значний
Атака на віртуальну машину з іншої віртуальної машини	Б	значний
Атака на мережу реплікації віртуальних машин	А	середній
Неконтрольоване збільшення числа віртуальних машин	В	значний
Проблема управління даними	Б	середній

Ймовірність здійснення атаки використовуючи загрози та вразливості:

А – низька;

Б – середня;

В – висока.

Рівні впливу на ресурс:

- критичний – інформація/ресурс/мережа може бути знищена, змінена без можливості відновлення. В даному випадку втрати підприємства є значними;
- значний – інформація/ресурс/мережа може втратити деякі свої властивості, але може бути відновлена. В даному випадку втрати підприємства є меншими, ніж внаслідок повної втрати і неможливості відновити інформацію;
- середній – інформація/ресурс/мережа втрачає деякі властивості, але може бути відновлена в прийнятні терміни і з мінімальними втратами;
- незначний – інформація/ресурс/мережа може зазнати невеликих змін, які можливо відновити в найкоротший термін.

2.4 Рекомендації щодо забезпечення інформаційної безпеки в хмарному середовищі

Неправомірне використання хмарних сервісів пов'язано з недосконалістю механізмів реєстрації і аутентифікації користувачів, що дає можливість як використання відповідних ресурсів без оплати послуг, так і можливість використання їх для протиправної діяльності (розміщення керуючих центрів зомбі-мереж, розсилання спаму, атаки, розміщення шкідливого коду, обходу механізмів захисту). Найбільш уразливими сервісами є IaaS і PaaS. Як заходи протидії рекомендується вводити суворі правила початкової реєстрації, використовувати засоби моніторингу та аналізу мережевого трафіку клієнтів.

На основі проаналізованих загроз, моделі загроз і даних, які приведені в розділі спеціальної частини при переході на хмарні технології слід враховувати наступні розроблені рекомендації.

2.4.1 Захист мережі віртуальних машин

Як правило, міжмережевий екран захищає периметр одного або декількох мережевих сегментів. Захист периметру мережі за допомогою міжмережевого

екрану показана на рисунку 2.1.[22]

Основний брандмауер захищає зовнішній периметр, пропускаючи тільки трафік HTTP, HTTPS, FTP. Не слід пропускати у свою мережу трафік FTP. FTP – це небезпечний протокол, і в різних реалізаціях було знайдено безліч вразливостей. Замість FTP слід користуватися протоколом SCP - протоколом копіювання файлів, що використовують в якості транспорту не RSH (Remote Shell), а SSH (Secure Shell).

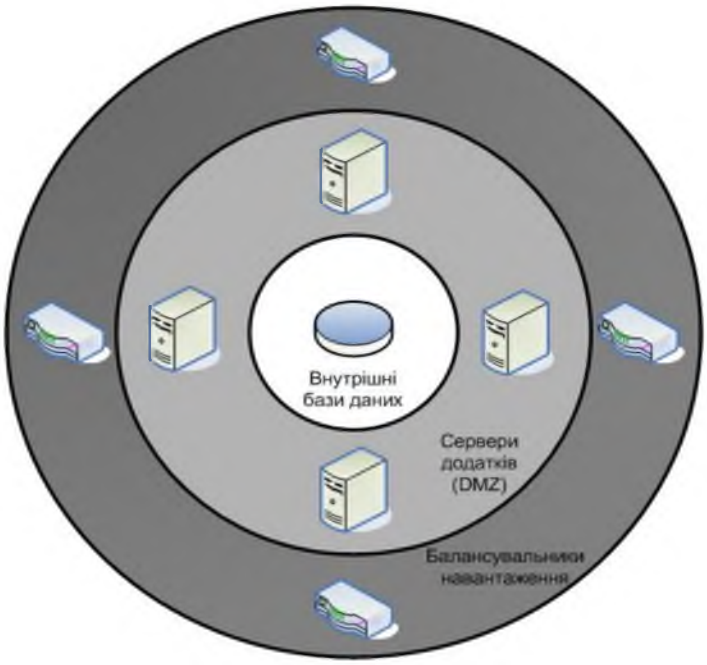

Рисунок 2.1 – Захист периметра мережі за допомогою брандмауера

Між захищеним мережевим сегментом і зовнішнім периметром знаходяться прикордонні системи, наприклад балансувальники навантаження, які направляють трафік в так звану "демілітаризовану зону" (DMZ), захищену іншим брандмауером. У цій зоні розташовуються сервери додатків, які направляють запити до баз даних через третій брандмауер у внутрішню захищену мережу, де знаходяться внутрішні бази даних, що зберігають конфіденційну інформацію.

У такій структурі для отримання доступу до даних за зростанням рівня секретності організовуються кілька рівнів (або периметрів) мережевого захисту за допомогою брандмауерів. Основною перевагою такої архітектури є те, що навіть якщо правила брандмауера, що захищає внутрішню мережу,

сформульовані погано, вони не обов'язково відкривають її для доступу ззовні, за винятком тих випадків, коли демілітаризована зона теж вже скомпрометована. На додаток, загальна тенденція полягає в тому, що зовнішні сервіси сильніше захищені від вразливостей Інтернету, у той час як внутрішні сервіси менш орієнтовані на Інтернет. Слабкість же цієї інфраструктури полягає в тому, що компрометація будь-якого з внутрішніх серверів в межах конкретного сегмента автоматично надає повний доступ і до інших серверів в цьому мережевому сегменті.

На рисунку 2.2 наведено візуальне подання концепції правил брандмауерів в хмарному середовищі. Ця концепція хмарної інфраструктури сильно відрізняється від концепції, прийнятої в традиційних центрах обробки даних.[21]

Всі віртуальні сервери знаходяться в мережі на одному рівні, а управління трафіком здійснюється за допомогою визначення груп безпеки. Немає ні мережевих сегментів, ні периметра. Членство в одній і тій же групі безпеки не надає привілейованого доступу до інших серверів, що належать до тієї ж групи безпеки, за винятком того випадку, коли явно визначені правила надають привілейований доступ. Нарешті, окремий сервер може бути членом кількох різних груп безпеки. Правила, визначені для конкретного сервера, являють собою об'єднання правил для всіх груп, до яких цей сервер належить.

Можна визначити групи безпеки таким чином, щоб імітувати традиційний захист мережевого периметра. Наприклад, можна створити таку конфігурацію:

- створити прикордонну групу безпеки, яка б прослуховувала весь трафік через порти 80 і 443;

- створити групу безпеки DMZ, яка б прослуховувала трафік, що виходить з прикордонної групи, через порти 80 і 443;

- створити внутрішню групу безпеки, яка б прослуховувала трафік, що виходить з групи DMZ, через порт 3306.

Якщо система безпеки не дозволяє обмежувати доступ через порти при визначенні правил доступу з однієї групи безпеки в іншу, можна імітувати цю можливість за рахунок визначення правил на основі вихідного IP-адреси для кожного сервера у вихідній групі.

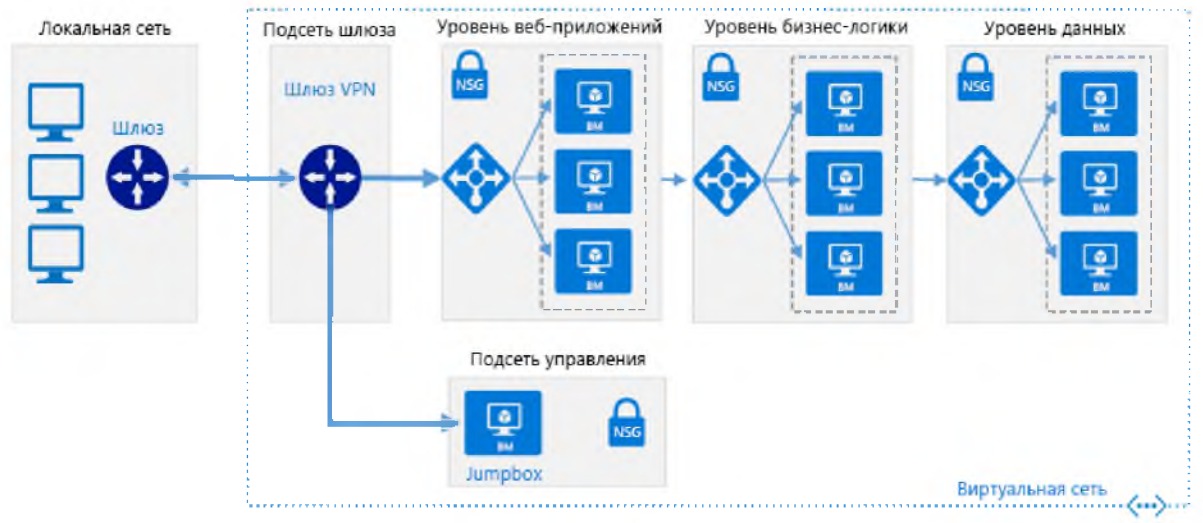

Рисунок. 2.2 – Відсутність периметра і мережевих сегментів у сучасному хмарному середовищі.

Як і у випадку з традиційним захистом периметра, доступ до серверів, що належать до вашої внутрішньої групі безпеки, можна отримати лише тоді, коли попередньо буде скомпрометована спочатку прикордонна група, потім - DMZ, і, нарешті - один з внутрішніх серверів. На відміну від традиційного захисту периметра, тут існує можливість того, що випадково буде надано глобального доступу до внутрішньої зони і, таким чином, вона буде відкрита для вторгнень. Але в хмарному середовищі, якщо атакуючий і скомпрометує один з серверів внутрішньої зони, не отримає автоматичного доступу до інших серверів з цієї зони, якщо тільки не скористається оригінальним експлоітом. Іншими словами, доступ до одного з серверів у внутрішній зоні не обов'язково означає доступ до інших серверів в межах цієї зони.

Така архітектура системи безпеки надає дві основні переваги.

– Оскільки можна віддалено керувати правилами брандмауера, атакуючий не має єдиної мішені для своєї атаки, як у випадку з фізичним

брандмауером.

– Відсутність можливості випадково зруйнувати правила захисту мережі і таким чином назавжди блокувати будь-який доступ в даний мережевий сегмент.

Рекомендується скористатися підходом, який імітує традиційний захист мережевого периметра, тому що цей підхід до управління мережевим трафіком добре вивчений і простий для розуміння. Якщо скористатися цим підходом, важливо розуміти, що створюються тільки віртуальні еквіваленти фізичних мережевих сегментів традиційної фізичної інфраструктури. Справжніх рівнів мережевої безпеки, які є у традиційній конфігурації, немає.

Рекомендації по найбільш ефективної організації мережевої системи безпеки в хмарі:

– На кожному віртуальному сервері слід запускати тільки один мережевий сервіс (плюс всі сервіси, необхідні для адміністрування). Кожен новий мережевий сервіс, присутній в системі, являє собою вектор атаки. Якщо зосередити на одному сервері безліч сервісів, то створиться безліч векторів атаки, які потенційно дозволяють отримати доступ до даних, що зберігаються на цьому сервері або для використання цього сервера для отримання прав доступу до іншої мережі.

– Не слід надавати відкритого доступу до даних, які мають вищий рівень секретності. Якщо отримання несанкціонованого доступу до клієнтської бази даних вимагає компрометації балансувальника навантаження, сервера додатків і сервера бази даних (і при цьому ви впроваджуєте рекомендації запускати тільки один сервіс на кожному з серверів), зловмисникові потрібно реалізувати цілих три різних вектора атаки перш, ніж він зможе дістатися до цих даних.

– Слід відкривати тільки ті порти, які є абсолютно необхідними для підтримки сервісу, що надається конкретним сервером, і не більше того. Зрозуміло, захист кожного з серверів повинен бути посилений таким чином, щоб на ньому працював тільки один сервіс - той, який спочатку був

призначений для роботи на ньому. Іноді буває й так, що на сервері запускаються ті сервіси, які спочатку не призначалися для роботи на даному сервері. Також може бути, коли в складі сервісу виявляється експлоїт, що не вимагає доступу від імені root (nonroot exploit), але дозволяє атакуючому запустити ще один сервіс за допомогою експлойтів, що вимагають доступ від імені root. Блокуючи доступ до всього, за винятком цільового сервісу, можна запобігти використанню цих типів експлойтів.

– Слід обмежити доступ до сервісів, надаючи його тільки тим клієнтам, які дійсно їх потребують. Природно, що балансувальники навантаження повинні відкривати Web-порти 80 і 443 для всього трафіку. У відкритому доступі потребують тільки ці два протоколи і конкретний сервер. Для будь-якого іншого сервісу трафік повинен бути обмежений конкретними вихідними адресами.

– Слід використовувати зворотний проксі. Зворотний проксі – це проксі-сервер, який, на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або декілька серверів, логічно розташованих у внутрішній мережі. Зазвичай зворотні проксі-сервери встановлюються перед Web-серверами. Часто використовується для балансування мережного навантаження між декількома Web-серверами і підвищення їх безпеки, граючи при цьому роль брандмауера на прикладному рівні. Як правило, зворотний проксі представляє собою Web-сервер, наприклад Apache, який маршрутизує трафік від клієнта до сервера. За рахунок використання проксі-сервера можна ускладнити для зловмисника атаку на вашу інфраструктуру. По-перше, Apache і IIS набагато краще справляються з завданнями щодо відображення мережевих атак, ніж будь-який з серверів додатків, які ви можете використовувати. У результаті ймовірність проникнення експлоїта буде значно знижена, а ймовірність його знешкодження та швидкість випуску поліпшення істотно підвищяться. По-друге, при використанні експлоїта на проксі-сервер атакує не отримає доступ, йому в будь-якому випадку доведеться шукати додаткову уразливість на самому вашому сервері додатків.

– Слід використовувати динамічну природу хмарної середовища для автоматизації усунення проблем з мережевою безпекою. В будь якому випадку, потрібно відкривати порти на брандмауері, для вирішення деяких бізнес-завдань. Можливо, було відкрито порт FTP на Web-сервері, бо в одного з ключових замовників з'явилася нагальна необхідність використовувати анонімний доступ через FTP для пакетного закачування файлів. Замість того, щоб тримати цей порт постійно відкритим, ви можете відкривати його у заздалегідь визначений час доби і тримати відкритим протягом обумовленого з клієнтом проміжку часу, а потім знову закривати. Можливо, навіть буде вирішено створювати тимчасовий сервер, що виконує роль FTP-сервера для пакетного завантаження, обробляти закачаний файл, а потім знову зупиняти цей сервер.

2.4.2 Шифрування файлових систем

Кожен використовуваний віртуальний сервер буде монтувати ефемерні пристрої зберігання даних або пристрої блочного зберігання даних.

Найбільш безпечний підхід до обох сценаріїв полягає в монтуванні ефемерних пристроїв і пристроїв блочного зберігання з використанням зашифрованої файлової системи. У хмарному середовищі управління запуском віртуального сервера з використанням зашифрованих файлових систем виявляється простіше й пропонує більш високий рівень захищеності.

Основна проблема, пов'язана з використанням зашифрованих файлових систем на серверах, полягає в тому, яким чином буде реалізоване керування паролем для розшифрування. Конкретному серверу необхідно отримати пароль для розшифрування перш, ніж він зможе змонтувати зашифровану файлову систему. Найбільш загальний підхід до вирішення цієї проблеми полягає в зберіганні пароля в незашифрованій кореневій файловій системі. Оскільки метою шифрування файлової системи є захист від фізичного доступу до образу диска, зберігання пароля на окремій, незашифрованій

файловій системі не настільки проблематично, але, тим не менше, воно все-таки є проблемою.

У хмарному середовищі не потрібно зберігати в хмарі пароль для розшифрування. Замість цього можна передати пароль для розшифрування нового віртуального примірника при його запуску. Сервер може зберегти ключ для розшифрування з одного з параметрів запуску сервера, а потім змонтувати блоковий пристрій, використовуючи зашифровану файлову систему.

Рекомендовані заходи захисту:

-Можна використовувати додатковий рівень безпеки, зашифрувавши пароль і зберігши ключ для його розшифрування в образі машини.

2.4.3 Рекомендації по нейтралізація уразливості API

Уразливості в API зазвичай пов'язані з їх доопрацюванням постачальниками послуг. Це робиться для того, щоб надавати додаткові сервіси, але побічним ефектом є підвищення складності API та іншим ризикам. Цей ризик стосується всіх типів сервісів, включаючи SaaS, IaaS і PaaS.

Рекомендовані заходи захисту:

- застосовувати такі засоби як аналіз підходів забезпечення безпеки програмних інтерфейсів, забезпечення строгої аутентифікації і контролю доступу, застосування засобів шифрування трафіку, а також аналіз ланцюжків залежностей, пов'язаних з API.

2.4.4 Запобігання загрози інсайдерів

Діяльність співробітників компанії-постачальника послуг також може представляти загрозу. Це пов'язано із зосередженням в одному місці безлічі IT-сервісів, що працюють під єдиним управлінням в інтересах різних замовників, причому процеси і процедури постачальника часто непрозорі для його замовників. При цьому персонал має повний доступ до даних і інших

ресурсів постачальника, що створює ризик несанкціонованого доступу, причому виявити його може бути дуже складно або навіть зовсім неможливо. Даний ризик також стосується всіх типів сервісів, включаючи SaaS, IaaS і PaaS.

В якості рекомендованих заходів захисту рекомендується:

- провести детальну оцінку рівня забезпечення безпеки в компанії-постачальника в контексті питань, пов'язаних з персоналом, ввести вимоги до персоналу в договір обслуговування,
- вимагати від постачальника надання всієї актуальної інформації про підходи і практики корпоративного управління та відповідності всім вимогам.

2.4.5 Захист від втрати даних

Втрата даних може бути пов'язана з помилками персоналу (як замовника, так і постачальника), використанням ненадійних накопичувачів і носіїв, внаслідок втрати ключа шифрування, а також внаслідок ненадійності обладнання ЦОД або відсутності процедур аварійного відновлення. Найбільш імовірною причиною витоку даних є несанкціонований доступ, в результаті порушення порядку виведення з експлуатації носіїв інформації, а також внаслідок політичних ризиків. Дані уразливості характерні для всіх класів сервісів.

В якості рекомендованих заходів захисту рекомендується:

- контролювати доступ до API, шифрувати дані і контролювати їх цілісність при передачі, аналізувати засоби захисту даних як на етапі проектування, так і в ході експлуатації,
- вимагати від постачальника неухильного дотримання регламентів знищення інформації при виведенні обладнання з експлуатації, а також визначити порядок резервного копіювання даних,
- установити в корпоративній мережі шлюзовий шифрувальний пристрой,
- дозволить здійснювати шифрування всіх корпоративних даних,

що завантажуються з хмари і вивантажуються в неї.

Справа в тому, що повністю зашифровані з урахуванням ідентифікації дані набагато важче піддаються хитрощам хакерів.

2.4.6 Захист від крадіжки облікових даних

Крадіжка облікових даних може статися внаслідок шахрайства, з використанням фішингу, шкідливого ПО, а також при реалізації вразливостей в обладнанні і ПО.

В якості рекомендованих заходів захисту рекомендується:

- не допускати використання загальних облікових записів,
- використовувати засоби багатофакторної аутентифікації,
- вести моніторинг несанкціонованої активності,
- аналізувати політики безпеки постачальника.

2.4.7 Захист від невідомих ризиків

Невідомі ризики пов'язані з тим, що клієнт не має повної інформації про хмарне середовище, і, отже, не володіє всією повнотою інформації про ризики інформаційної безпеки.

В якості рекомендованих заходів захисту рекомендується:

- вимагати від постачальника інформації про інфраструктуру, включаючи версії ПЗ, наявність засобів захисту, даних журналів, впровадження засобів моніторингу подій та управління інцидентами.

2.4.8 Налаштування безпеки на рівні користувача

Деякі компанії для забезпечення хмарної безпеки дозволяють організаціям створювати складні налаштування безпеки на рівні користувача. Мається на увазі те, що компанія може, приміром, розробити таку політику: «віце-президент з продажу вправі отримувати доступ до глобальних прогнозів продажів, але якщо він спробує отримати такі дані через смартфон з території

однієї країни за допомогою невідомого протоколу та при цьому двома годинами раніше він виходив у мережу з повною аутентифікацією з зовсім іншої країни, запит повинен бути відхилений».

2.4.9 Створення «приватних хмар»

Навчальний заклад, який все ж таки не переконали і він залишається не впевненою в надійності публічних хмар, може скористатися «віртуальною приватною хмарою». Це досягається шляхом використання провайдером публічної хмарної інфраструктури для організації приватної хмари. При такій організаційній структурі, частина даних клієнта зберігається і обробляється за рахунок ресурсів власної інфраструктури, а частина – за рахунок ресурсів зовнішнього провайдера. Як приклад віртуальної приватної хмари можна привести сервіс компанії Microsoft під назвою Azure Virtual Private Cloud (Azure VPC). [36]

«Хмара» – це набір технологій, які відповідають певним вимогам.

Побудова «приватної хмари» – це процес впровадження спеціального програмного і апаратного забезпечення для центрів обробки даних, а також розробки IT-регламентів, що дозволяють надати компанії прозору і просту процедуру надання інформаційно-технічних ресурсів бізнес-підрозділам компанії. [36]

Послуги зі створення «приватної хмари» включають в себе:

1. Обстеження поточного фізичного обладнання та організації віртуального середовища замовника.
2. Вироблення технічних рішень з організації або модернізації віртуальної інфраструктури замовника.
3. Розробка технічних рішень з моніторингу та управління віртуальною інфраструктурою.
4. Розробка технічних рішень з автоматизації надання інформаційно-технічних ресурсів користувачам.

5. Установку і настройку систем віртуалізації та автоматизованого надання ресурсів.
6. Розробку регламентів надання ресурсів.
7. Інтеграцію систем зі сторонніми засобами резервного копіювання.

Потреба в даних послугах виникає тоді, коли:

- У замовника є декілька підрозділів, які керують великою кількістю фізичних серверів. Сервери виділені під конкретний сервіс і управляються підрозділом, що супроводжує цей сервіс. Як результат у кожного підрозділу в штаті знаходяться адміністратори серверів і систем зберігання даних. У департаменту IT є бажання консолідувати адміністраторів інфраструктури в рамках одного підрозділу, стандартизувати та регламентувати їх роботу. А також розвантажити фахівців підрозділів, що відповідають за бізнес-додатки.
- У замовника в наявності велика структура віртуалізації. Замовник має проблеми із стандартизацією, керованістю і надійністю віртуалізованих сервісів.
- У замовника є підрозділи, яким потрібно регулярне надання інформаційно-технічних ресурсів і є необхідність зниження витрат IT-підрозділу на супровід цих ресурсів без втрати контролю за їх виділенням.

В якості основи для побудови приватних хмар використовуються системи комплексної віртуалізації та управління IT-інфраструктурою на основі продуктів Microsoft, HP, IBM, Dell, VMware,. Продукти, на основі яких будуються «приватні хмари», - Microsoft Azure, HP CloudSystem Matrix, VMware vCloud, IBM SmartCloud Enterprise. [36]

2.5 Висновок

Багато навчальних закладів, які все ще не наважуються впроваджувати у себе системи на основі хмарних технологій, виправдовують таку свою

поведінку побоюваннями за безпеку своїх даних. У сфері безпеки найбільше стурбовані такими факторами, як захист даних, правильне функціонування систем та їх доступність. При цьому все більшого значення набувають завдання захисту додатків, оптимального моніторингу та аудиту, а також захисту від загроз інформаційної безпеки.

При переході на хмарні технології будь-якій навчальний заклад повинен замислитися над дотриманням вимог забезпечення інформаційної безпеки даних. Рекомендації, які розроблені і обґрунтовані в даній дипломній роботі, допоможуть швидко і легко зорієнтуватися на що потрібно перш за все звернути увагу:

1. Які існують загрози для систем на основі хмарних обчислень.
2. Які елементи варто захищати в першу чергу.
3. Які є унікальні елементи для хмарної архітектури.
4. Які вимоги слід ставити перед провайдерами хмарних технологій.
5. Як обирати хмарного провайдера і яку інформацію потрібно вимагати від нього.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є визначення економічної доцільності використання запропонованих засобів та заходів інформаційної безпеки.

Для визначення цього необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити обсяги відвернених втрат, та, на основі цього, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі розрахованих показників можна буде визначити, наскільки прибутковим або збитковим є запропонований проект.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.[6]

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної;

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Відповідно до специфіки розробленої ПБ та конкретних рішень, обраних у цій політиці, актуальними капітальними витратами можна вважати наступні:

– вартість розробки проекту інформаційної безпеки;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Трудомісткість у даному випадку буде розраховуватися за формулою 3.1:

$$t = t_{об} + t_{а} + t_{вз} + t_{озб} + t_{д\ год}, \qquad (3.1)$$

де $t_{об}$ – тривалість проведення обстеження АС підприємства;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Показники часу, витраченого на розробку політики інформаційної безпеки наведені у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	Значення, год
$t_{об}$	65
$t_{а}$	16
$t_{вз}$	10
$t_{озб}$	16
$t_{д}$	16

Згідно з формулою 3.1 трудомісткість розробки ПБ становить:

$$t = 65\ год + 16\ год + 10\ год + 16\ год + 16\ год,$$

і, таким чином,

$$t = 123\ год.$$

Надалі потрібно розрахувати витрати на створення ПБ ($К_{рп}$), використовуючи наступні показники – витрати на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) та вартість витрат машинного часу ($З_{мч}$). Розрахунок проводиться за формулою 3.2:

$$К_{рп} = З_{зп}\ грн. \qquad (3.2)$$

У свою чергу, витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб},\ грн, \qquad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, в загальному випадку, становить – 72 грн/год.

Згідно з формулою 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 123\ год \cdot 72\ грн/год,$$

і, таким чином,

$$З_{зп} = 8856 \text{ грн.}$$

Тож, витрати на створення ПБ за формулою 3.2 становлять:

$$К_{рп} = 8856 \text{ грн.}$$

У результаті розрахунків, маємо вартість розробки ПБ – 8856 гривень.

У даному конкретному випадку повна вартість капітальних витрат розраховується за формулою 3.4:

$$К = К_{рп} + К_{навч} \text{ грн.} \quad (3.4)$$

Під $К_{навч}$, мається на увазі одноразовий кваліфікаційний захід для співробітників, з питань ознайомлення з новою редакцією політики безпеки. Даний захід проводиться спеціалістом ІБ, тому додатково йому виплачується сума у розмірі 500 грн, окрім виплати за розробку нової редакції ПБ.

Тож, згідно до формули 3.4, повна вартість капітальних витрат становить:

$$К = 8856 \text{ грн} + 500 \text{ грн},$$

і, таким чином,

$$К = 9356 \text{ грн.}$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.[6]

Для даного підприємства актуальними будуть наступні витрати:

– заробітна плата обслуговуючого персоналу;

– кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки;

– технічне й організаційне адміністрування й сервіс.

Оскільки методи захисту, передбачені політикою безпеки, мають більш організаційний характер, поточними витратами можна вважати заробітну платню системного адміністратора, витрати на опечатування зовнішніх інтерфейсів робочих станцій та витрати пов'язані з діяльністю користувачів, тож поточні витрати розраховуються за формулою 3.5:

$$C = C_{за} + C_{оп} + C_{дк}\ грн, \qquad (3.5)$$

де $C_{за}$ – витрати на заробітну плату системного адміністратора;

$C_{оп}$ – витрати на опечатування зовнішніх інтерфейсів робочих станцій;

$C_{дк}$ – витрати, пов'язані з діяльністю користувачів.

У свою чергу, витрати на заробітну плату системного адміністратора розраховуються за формулою 3.6:

$$C_{зпад} = З_{дод1} + З_{дод2}\ грн, \qquad (3.6)$$

Де $З_{дод1}$ – додаткова заробітна плата системного адміністратора за проведення кваліфікаційних заходів та перевірку знать та навичок персоналу стосовно правил, регламентованих політикою безпеки;

$З_{дод1}$ – додаткова заробітна плата системного адміністратора за додаткові обов'язки – відповідальність за виконання деяких розділів політики безпеки інформації.

Додаткова заробітна платня №1 складає 500 грн за проведення одного кваліфікаційного заходу. Такі заходи планується проводити раз на 2 місяці, тож фактично за місяць системний адміністратор отримуватиме 250 грн додаткової заробітної платні №1 на місяць. Додаткова платня №2 враховуватиме обсяг відповідальності, що покладатиметься на системного адміністратора політикою безпеки. Таким чином, розмір додаткової заробітної платні №2 становитиме – 1000 грн/місяць.

За формулою 3.6, можна розрахувати:

$$C_{зпад} = (250\ грн + 1000\ грн) \cdot 12\ місяців,$$

і, таким чином,

$$C_{знад} = 15000 \text{ грн.}$$

Поточні витрати за опечатування зовнішніх інтерфейсів на рік включатимуть у себе вартість 2 журналів (200 грн) опечатування та 150 пломб-наліпок (450 грн). Тож:

$$C_{оп} = 200 \text{ грн} + 450 \text{ грн},$$

і, таким чином,

$$C_{оп} = 650 \text{ грн.}$$

Витрати, пов'язані з діяльністю користувачів мають під собою на увазі витрати, що спричинені професійною діяльністю. Такою діяльністю вважається перенавантаження серверу і частий перезапис інформації на жорстких дисках серверу у процесі роботи, що приведе сервер у неробочий стан. Такі витрати включають у себе вартість полагодження серверу, профілактична заміна компонентів. За рік, вартість таких витрат сягатиме 1500 грн. Тож:

$$C_{дк} = 1500 \text{ грн.}$$

Розрахунок повної вартості експлуатаційних витрат за формулою 3.5:

$$C = 15000 \text{ грн} + 650 \text{ грн} + 1500 \text{ грн},$$

і, таким чином,

$$C = 17150 \text{ грн.}$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Далі буде вказано загрози з можливим економічним впливом на підприємство:

1) Злам мережі, порушення нормального функціонування системи призводить до простою на підприємстві;

2) Несанкціоноване ознайомлення з інформацією (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

3) Несанкціонована модифікація/видалення інформації (співробітниками) призведе до порушення робочого процесу, що у свою чергу призведе до втрати частини запланованого заробітку;

4) Несанкціоноване копіювання інформації на знімні носії (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

5) Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи мають схожий ефект зі зламом мережі;

6) Несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками має схожий ефект з несанкціонованим ознайомленням з інформацією працівниками;

7) Несанкціонована модифікація/видалення інформації конкурентами та зловмисниками має схожий ефект з несанкціонованою модифікацією/видаленням інформації співробітниками;

8) Крадіжка/псування матеріальних цінностей (об’єктів ІТС) конкурентами та зловмисниками призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

9) Використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами має схожий ефект зі зламом мережі;

10) Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди має схожий ефект зі зламом мережі;

11) Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює, у свою чергу це призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

12) Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи, що в свою чергу призведе до втрати частини запланованого заробітку.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V \, грн, \tag{3.7}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ і V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс}{F} \cdot t_п \; грн, \tag{3.8}$$

де F – місячний фонд робочого часу;

$Зс$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_в = П_{ви} + П_{пв} + П_{зч}\ грн, \quad (3.9)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{O}{F} \cdot (t_п + t_в + t_{ви})\ грн, \quad (3.10)$$

де F – місячний фонд робочого часу;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}\ грн, \quad (3.11)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в\ грн, \quad (3.12)$$

де F – місячний фонд робочого часу;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

Відповідно до пронумерованого вище списку загроз, можна розрахувати ймовірні збитки. Враховуючи той факт, що деякі загрози мають схожі наслідки, розрахунки будуть проводитись для одного випадку з групи подібних, але надалі буде враховуватись кількість можливих подій на рік та ймовірність їх виникнення.

Відповідно до переліку загроз, вказаного вище, для загроз №1, №5, №9, №10 збитки від реалізації однієї з цих загроз розраховуються за формулами 3.7–3.11:

$$П_п = 13000\ грн \cdot 14\ чол/212\ год \cdot 3\ год,$$

$$П_п = 2575{,}47\ грн.$$

$$П_{ви} = 0\ грн.$$

$$П_{зч} = 0\ грн.$$

$$П_{пв} = 14000\ грн/212\ год \cdot 1\ год,$$

$$П_в = 66{,}03\ грн.$$

$$П_в = 0\ грн + 66{,}03\ грн + 0\ грн,$$

$$П_в = 66{,}03\ грн.$$

$$V = 3001065\ грн/212\ год \cdot (3\ год + 1\ год + 0\ год),$$

$$V = 56623{,}86\ грн.$$

І таким чином,

$$U = 2575{,}47\ грн + 66{,}03\ грн + 56623{,}86\ грн,$$

$$U = 59264{,}5 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз №1, №5, №9 або №10 становитиме – 59264 грн 50 копійок.

Для загроз №2, №4, №6 потрібно враховувати не збитки, а розмір не одержаної вигоди від реалізації однієї з цих загроз. Експертним висновком розмір неодержаної вигоди визначені у розмірі – 90031,95 грн/місяць (3% від планового місячного прибутку підприємство не буде отримувати).

Оскільки загрози №8 та №12 мають схожі наслідки, розмір збитку від реалізації однієї з загроз буде таким самим і для іншої і буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн}/212 \text{ год} \cdot 24 \text{ год},$$

$$П_п = 1471{,}70 \text{ грн.}$$

$$П_{ви} = 0 \text{ грн.}$$

Враховуючи специфіку роботи підприємства, одним з найцінніших ресурсів компанії є робочі станції (ноутбуки), тому в якості показника $П_{зч}$ враховується вартість заміни ноутбука.

$$П_{зч} = 8000 \text{ грн.}$$

$$П_{пв} = 14000 \text{ грн}/212 \text{ год} \cdot 120 \text{ год},$$

$$П_в = 7924{,}52 \text{ грн.}$$

$$П_в = 0 \text{ грн} + 7924{,}52 \text{ грн} + 8000 \text{ грн},$$

$$П_в = 15924{,}52 \text{ грн.}$$

$$V = 1478 \text{ грн}/212 \text{ год} \cdot (120 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 823{,}58 \text{ грн.}$$

І таким чином,

$$U = 1471{,}70 \text{ грн} + 15924{,}52 \text{ грн} + 823{,}58 \text{ грн},$$

$$U = 18219{,}8 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загрози №8 становитиме – 18219 грн 80 копійок.

Оскільки загроз № 3, № 7 та №11 мають подібні наслідки, збиток від їх реалізації буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн} \cdot 14 \text{ чол}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_п = 2575{,}47 \text{ грн.}$$

$$П_{ви} = 14000 \text{ грн}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_{ви} = 198{,}11 \text{ грн.}$$

$$П_{зч} = 0 \text{ грн.}$$

$$П_{пв} = 0 \text{ грн.}$$

$$П_в = 198{,}11 \text{ грн} + 0 \text{ грн} + 0 \text{ грн},$$

$$П_в = 198{,}11 \text{ грн.}$$

$$V = 3001065 \text{ грн}/212 \text{ год} \cdot (3 \text{ год} + 3 \text{ год} + 0 \text{ год}),$$

$$V = 84935{,}80 \text{ грн.}$$

І таким чином,

$$U = 2575{,}47 \text{ грн} + 198{,}11 \text{ грн} + 84935{,}80 \text{ грн},$$

$$U = 87709{,}30 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз № 3, № 7 або №11 становитиме – 87709 грн 30 копійок.

Таким чином, маючи дані про можливі збитки від реалізації загроз можна провести розрахунок збитків на рік від реалізації даних загроз. Зводні дані та кінцева величина збитку зазначені у таблиці 3.2:

Таблиця 3.2 – Розрахунок річних обсягів збитків від реалізації загроз

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Злам мережі, порушення нормального функціонування системи	59264,5	1	0,54	32002,83
Несанкціоноване ознайомлення з інформацією (співробітниками)	90031,95	1	0,3	27009,59
Несанкціонована модифікація/видалення інформації (співробітниками)	87709,30	2	0,3	52625,58
Несанкціоноване копіювання інформації на знімні носії (співробітниками)	90031,95	1	0,32	28810,22
Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи	59264,5	1	0,70	41485,15
Несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками	90031,95	1	0,5	45015,98
Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди	59264,5	1	0,72	42670,44

Продовження таблиці 3.2

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює	87709,30	1	0,36	31575,35
Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи	18219,8	1	0,36	6559,13
ЗАГАЛОМ				372581.72

Для розрахунку коефіцієнтів вірогідності були використані дані з таблиць 1.8 і 1.9, а саме – коефіцієнти К2, що відповідають за мотивацію джерела загрози і зручність використання вразливості відповідно. Рівні коефіцієнта К2 були відповідно змінені на часткову шкалу (1 – 0,2; 2 – 0,4; 3 – 0,6; 4 – 0,8; 5 – 1). На підставі коефіцієнтів К2 джерела і коефіцієнтів К2 вразливості експертним шляхом були визначені коефіцієнти вірогідності реалізації зазначених вище загроз.

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою :

$$E = B \cdot R - C \text{ грн}, \tag{3.13}$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі,

частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Тож, економічний ефект становить:

$$E = 372581{,}72 \text{ грн} - 17150 \text{ грн},$$

$$E = 355431 \text{ грн}.$$

В загальному вигляді, оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій $T_о$.

У даному випадку ТСО не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.14:

$$ROSI = E / K, \qquad (3.14)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Тож,

$$ROSI = 372581{,}72 \text{ грн} / 9356 \text{ грн},$$

$$ROSI = 39{,}8.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $Е_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма

прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.15:

$$ROSI > (N_{деп} - N_{інф}) / 100 \qquad (3.15)$$

де $N_{деп}$ = 19 – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф}$ = 8 – річний рівень інфляції, %.

39,8 > 0,11, отже проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.16:

$$T_o = E / K = 1 / ROSI = 0,025 \text{ року.} \qquad (3.16)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки капітальних та поточних витрат на введення та експлуатацію засобів захисту, що рекомендовані політикою безпеки.

В ході розрахунків було з’ясовано що введення в експлуатацію засобів та заходів захисту є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (0,025 року), а коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта (39,8 > 0,11). Тож, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВКИ

Використання хмарних обчислень дозволяє значно скоротити витрати на IT-послуги, інакше оцінити весь процес автоматизації діяльності компаній і створення програмного забезпечення, відмовитися від високих вхідних інвестицій в інфраструктуру та її подальшу підтримку.

В даній дипломній роботі було проаналізовано архітектуру побудови системи хмарних обчислень, а також було зроблено аналіз основних механізмів захисту інформації, яка зберігається, оброблюється і передається в системі хмарних обчислень.

Так як інформація користувача розміщується на віддалених серверах, то є дуже актуальною проблема забезпечення доступності, цілісності, а головне конфіденційності даних у системах хмарних обчислень. В дипломній роботі були розроблені рекомендації, за допомогою яких можна спробувати вирішити ці проблеми на підприємствах приватної форми власності.

Рекомендовано в якості платформи для хмарного сервісу використовувати платформу Microsoft Azure та обрати Office 365 в якості провайдера SaaS для корпоративних додатків учбового закладу.

На основі аналізу загроз, було зроблено висновок, що розроблені рекомендації забезпечують вибрані критерії оцінки захищеності інформації.

В економічному розділи було проведено аналіз економічної ефективності впровадження систем на основі хмарних обчислень на підприємствах приватної форми власності. Було розраховано капітальні витрати, експлуатаційні витрати на утримання та обслуговування програмного забезпечення, передбачувані збитки від атак. Обґрунтована економічна доцільність.

ПЕРЕЛІК ПОСИЛАНЬ

1. Матеріал "Хмарні технології: реальність нашого життя" з першого молодіжного порталу (Електрон. ресурс) / Спосіб доступу: URL: http://relax.dviger.com/gallery/work/c_22335.html – Хмарні технології: реальність нашого життя

2. Матеріал з Вікіпедії – вільної енциклопедії (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/Облачные_вычисления – Стаття «Хмарні обчислення»

3. Спеціалізований сайт КПІ, присвячений GRID в дослідницькому університеті (Електрон. ресурс) / Спосіб доступу: URL: http://grid.kpi.ua/index.php/uk/base-of-foreign-sources/38-2011-03-22-13-20-00.html – Інформація про клауд технології

4. Спеціалізований сайт, присвячений хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://russia.emc.com/collateral/emc-perspective/h6870-consulting-cloud-ep.pdf — Перевага приватної «хмари» для бізнесу: скорочення витрат та підвищення гнучкості ведення бізнесу.

5. Розділ онлайнового журналу Softkey.info (Електрон. ресурс) / Спосіб доступу: URL: http://www.softkey.info/reviews/review10196.php – Хмарні технології в ПЗ – тенденція минулого року

6. Ресурс, присвячений хмарним обчисленням і віртуалізації (Електрон. ресурс)/Спосіб доступу: URL: http://www.ixbt.com/news/soft/index.shtml?15/26/17 — Хмарні обчислення дають скорочення IT-витрат та спрощення технологічних задач

7. Ресурс, присвячений хмарним обчисленням і віртуалізації (Електрон. ресурс) / Спосіб доступу: URL: http://www.smart-cloud.org/ — Сайт присвячений хмарним обчисленням.

8. Професійний блог, який містить інформацію про хмарні обчислення (Електрон. ресурс) / Спосіб доступу: URL: http://habrahabr.ru/company/scalaxy/blog/65228/ — Стаття «Cloud computing: хто і як літає в хмарах?»

9. Спеціалізований сайт, присвячений хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://www.cloudzone.ru/. — У світі хмарних технологій.

10. Спеціалізований сайт, присвячений хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://www.microsoft.com/uk-UA/businessproductivity/why/CloudOnYourTerms.aspx — Стаття «Хмара на власних умовах».

11. Професійний блог, який містить інформацію про хмарні обчислення (Електрон. ресурс) / Спосіб доступу: URL: http://habrahabr.ru/post/85957/ — Стаття «Скільки коштує Amazon CloudFront»

12. Спеціалізований сайт, присвячений хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://cloud.sorlik.ru/synopsis-4.html — Основи хмарних обчислень (по рекомендаціям NIST).

13. Спеціалізований сайт, присвячений хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://www.cloudzone.ru/. — У світі хмарних технологій.

14. Російськомовна версія порталу GoGrid (Електрон. ресурс) / Спосіб доступу: URL: http://gogrid.ru/. — GoGrid :: Масштабований хостинг Windows і Linux серверів.

15. Сайт компанії SecureIT (Електрон. ресурс) / Спосіб доступу: URL: http://www.securit.ru/solutions/laws/ — Законодавство та стандарти інформаційної безпеки.

16. Спеціалізований мікросайт Intelligent enterprise, присвячений хмарним обчислюванням (Електрон. ресурс) / Спосіб доступу: URL: http://www.iemag.ru/clouds/opinions/detail.php?ID=25286— Як зробити хмару безпечною. Рекомендації Cloud Security Alliance.

17. Сайт Інтернет Університет Інформаційних технологій (Електрон. ресурс) / Спосіб доступу: URL: http://www.intuit.ru/department/se/incloudc/3/3.html — Вступ в хмарні обчислення. Переваги хмарних очислень.

18. Сайт PCWeek.ua – Корпоративні інформаційні технології та рішення (Електрон. ресурс) / Спосіб доступу: URL: http://www.pcweek.ua/ themes/detail.php?ID=137661 — Amazon передрікає захід ери ЦОДів.

19. Спеціалізований сайт Anti-Malware (Електрон. ресурс) / Спосіб доступу: URL: http://www.anti-malware.ru/news/2012-01-26/5173— Стаття «NIST випустив рекомендації по безпеці даних в “хмарі”»

20. Edvard L. Haletky. "VMware vSphere and Virtual Infrastructure Security: Securing the Virtual Environment". — Prentice Hall, 2009, ISBN-10: 0137158009.

21. Ronald L. Krutz, Russel Dean Vines. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing". Wiley, 2010. ISBN-10: 0470589876.

22. John Rhoton. "Cloud Computing Explained: Implementation Handbook for Enterprises". Recursive Press, 2009. ISBN-10: 0956355609 | ISBN-13: 978-0956355607.

23. Стаття "Технологія хмарних обчислень як ефективний інструмент підтримки бізнесу"з російськомовного Web-сайту IBM (Електрон. ресурс) / Спосіб доступу: URL: http://tinyurl.com/32p27pp — Що таке хмарні обчислення і як їх можна використовувати.

24. Інформаційний ресурс, присвячений віртуалізації з використанням VMware, Xen, MS Hyper-V та інших продуктів і технологій (Електрон. ресурс) / Спосіб доступу: URL: http://www.vm4.ru/ — Віртуалізація. VMware vSphere & Co.

25. Інформаційний ресурс, присвячений системній інтеграції та IT-сервісам (Електрон. ресурс) / Спосіб доступу: URL: http://www.hbc.ru/services/itdevelop/oblako/— Стаття «Побудова приватної хмари»

26. Розділ журналу BYTE-Росія, присвячений віртуалізації і хмарним технологіям (Електрон. ресурс) / Спосіб доступу: URL: http://tinyurl.com/39v92jg — Технології віртуалізації.

27. Сайт компанії IBM (Електрон. ресурс) / Спосіб доступу: URL: http://www.ibm.com/ru/cloud/ — Хмарні обчислення. Скорочення витрат.

Покращення процесу надання послуг. Підтримка інновацій в бізнесі.

28. Розділ журналу Information Security, присвячений проблемам довіри хмарним сервісам (Електрон. ресурс) / Спосіб доступу: URL: http://www.itsec.ru/imag/insec-1-2012/ — Хмарні сервіси

29. Як зробити хмару безпечною. Рекомендації Cloud Security Alliance (Електрон. ресурс) / Спосіб доступу: URL: http://www.iemag.ru/clouds/opinions/detail.php?ID=25286

30. John Allspaw. "The Art of Capacity Planning: Scaling Web Resources". — O'Reilly Media, 2008. ISBN-10: 0596518579 | ISBN-13: 978-0596518578.

31. John Rittinghouse, James Ransome. "Cloud Computing: Cloud Computing: Implementation, Management, and Security".—CRC Press, 2009.

32. Професійний блог, який містить інформацію про хмарні обчислення (Електрон. ресурс) / Спосіб доступу: URL: http://grigorkin.ru/2010/03/probuem-elastic-compute-cloud-ec2/Elastic-Compute- Cloud- Amazon-EC2. — Amazon Web Services.

33. Блог Олексія Бокова, що містить багато інформації про Amazon Web Services (Електрон. ресурс) / Спосіб доступу: URL: http://bokov.net/blog/ — Блог Бокова

34. Інтернет - портал, присвячений стандартам безпеки в області платіжних карт (Електрон. ресурс) / Спосіб доступу: URL: http://www.pcidss.ru/about/pcidss/ — PCI DSS.

35.Розділ журналу «Security Focus» присвячений віртуалізації і хмарним технологіям (Электронный ресурс) / URL: http://www.secfocus.ru/articles/16783.htm

36. Стаття «Побудова приватної хмари» (Электронный ресурс) / URL: http://www.hbc.ru/services/itdevelop/oblako/

37. Портал, присвячений інформаційній безпеці, орієнтований на менеджерів та експертів (Електрон. ресурс) / Спосіб доступу: URL: http://www.iso27000.ru — Захист інформації, управління інформаційною безпекою та ризиками.

38. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

39. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»

40. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»

41. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»

42. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94, ВВР, 1994// (Електрон. ресурс) / Спосіб доступу: URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр

43. «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99

ДОДАТОК А. ПЕРЕЛІК МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	РЕФЕРАТ	3	
2	А4	СПИСОК УМОВНИХ СКОРОЧЕНЬ	2	
3	А4	ЗМІСТ	3	
4	А4	ВСТУП	2	
5	А4	РОЗДІЛ 1. СТАН ПИТАННЯ	30	
6	А4	РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА	31	
7	А4	РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА	17	
8	А4	ВИСНОВКИ	1	
9	А4	ПЕРЕЛІК ПОСИЛАНЬ	5	
10	А4	ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	ДОДАТОК Б. Перелік документів на оптичному носії	1	
12	А4	ДОДАТОК В. Відгук керівника економічного розділу	1	
13	А4	ДОДАТОК Г. Відгук керівника кваліфікаційної роботи	1	

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

- Пояснювальна записка Заворін І.Д. 125м-20-1.docx
- Презентація Заворін І.Д. 125м-20-1.docx

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник економічного розділу
к.е.н., доц. Пілова Д.П Підпис: _____

ДОДАТОК Г. ВІДГУК НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

на тему: «Забезпечення інформаційної безпеки при використанні хмарних технологій для учбових закладів» студента групи 125м-20-1 Заворіна Івана Дмитровича

Кваліфікаційна робота за спеціальністю 125 «Кібербезпека» Заворіна І.Д. представлена пояснювальною запискою на 103 стор., містить 8 рис., 7 табл., 4 додатка, 43 джерела.

Об'єкт досліджень – технологія хмарних обчислень.

Предмет досліджень – система безпеки інформації при використанні хмарних технології для учбових закладів.

Мета – розробити рекомендації для підвищення рівня захисту інформації при використанні систем хмарних обчислень для учбових закладів. У спеціальній частині наводиться аналіз основних загроз в системах хмарних обчислень, а також розробка рекомендацій для можливості їх нейтралізації.

Наукова новизна роботи полягає у розробленні та обґрунтуванні рекомендацій щодо вирішення проблеми захисту інформації при використанні хмарних сервісів в навчальних закладах.

В економічному розділі виконаний розрахунок економічної ефективності запропонованих рішень.

В якості недоліків слід відзначити наступне: недотримання графіка проведення розробки, нечіткість окремих висновків і визначень.

В цілому дипломна робота виконано у відповідності до вимог, які пред'являються до дипломних робіт магістра і заслуговує оцінки "добре", а Заворін Івана Дмитрович присвоєння йому кваліфікації магістра з кібербезпеки за освітньою програмою "Кібербезпека".

Керівник роботи к.т.н., доц. Флоров С.В.