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

студентки *Марченко Валерії Тарасівни*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення інформаційної безпеки хмарних сервісів на основі розподілу рівнів захищеності та оптимізації ресурсів*

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

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студентки *Марченко Валерії Тарасівни* **академічної групи** *125м-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Підвищення інформаційної безпеки хмарних сервісів на основі розподілу рівнів захищеності та оптимізації ресурсів***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 №1036-е

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз технології хмарних обчислень. Порівняльна характеристика фізичних дата центрів там хмарних платформ. Моделі розгортання хмарних сервісів. Аналіз нормативно-правового забезпечення.	30.10.2021
Розділ 2	Ризики. Методи аналізу ризиків. Модель загроз хмарної ІТКС. Метод розподілу рівнів захищеності ресурсів хмарної ІТКС. Методика оптимізації ризиків хмарної ІТКС.	15.11.2021
Розділ 3	Розрахунок витрат на розробку методики розподілу рівнів захищеності та оптимізації ресурсів. Економічне обґрунтування доцільності впровадження розробленої методики.	20.12.2021

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2021р.

Дата подання до екзаменаційної комісії: 11.01.2022р.

Прийнято до виконання _____ Марченко В.Т.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 61 с., 7 рис., 7 табл., 4 додатки, 38 джерела.

Об’єкт дослідження: системи захисту інформації в ІТКС, що побудовані з використанням технологій хмарних обчислень.

Предмет дослідження: методи зниження ризиків у хмарних ІТКС.

Мета кваліфікаційної роботи: зниження ризиків інформаційної безпеки в хмарних ІТКС при обробці інформації різного ступеня конфіденційності.

У першому розділі кваліфікаційної роботи розглянуто технології хмарних обчислень та хмарні провайдери, описані моделі розгортання хмарних сервісів, а також переваги і недоліки використання хмарних ІТКС. Проведено аналіз нормативно-правової бази та стандартів у сфері інформаційної безпеки.

У спеціальній частині кваліфікаційної роботи описано поняття ризиків, їх невизначеності та чутливості. Проаналізовано існуючі методи аналізу ризиків та визначено складність оцінки даними існуючими методиками. Побудовано модель загроз хмарної ІТКС. Запропоновано новий метод розподілу рівнів захищеності ресурсів хмарної ІТКС, а також методику оптимізації ризиків з використанням лінійного програмування.

У третьому розділі кваліфікаційної роботи було обґрунтовано економічну ефективність запропонованої методики.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ХМАРНА ІНФРАСТРУКТУРА, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ

ABSTRACT

Explanatory note: 61 pages, 7 figures, 7 tables, 4 applications, 38 sources.

Object of study: information protection systems of information and telecommunication systems that are built with cloud computing technologies

Research subject: methods of reducing risks in cloud information and telecommunication systems

The purpose of the work: to reduce information security risks in cloud ITCs when processing information of varying degrees of confidentiality

The first section of the qualification work considers cloud computing technologies and cloud providers, describes the models of cloud services deployment, as well as the advantages and disadvantages of using cloud information and communication system. An analysis of the regulatory framework and standards in the field of information security is provided.

The special part of the qualification work describes the concepts of risk, its uncertainty and sensitivity. The existing methods of risk analysis are analyzed and the complexity of the assessment by these existing methods is determined. The model of threats of cloud information and communication system is constructed. A new method of allocating the levels of protection of cloud information and communication system resources as well as a method of risk optimization using linear programming are proposed.

In the third section of the qualification work the economic efficiency of the proposed method is calculated.

INFORMATION AND COMMUNICATION SYSTEM, COMPLEX INFORMATION SECURITY SYSTEM, CLOUD INFRASTRUCTURE, RISKS ASSESSMENT, THREAT MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AaaS – модель хмарного сервісу «Автентифікація як сервіс»

BYOD – політика використання користувачами персональних пристроїв

CSA – некомерційна організація «Альянс хмарної безпеки»

DBaaS – модель хмарного сервісу «База даних як сервіс»

DDos – атака типу «Розподілена відмова в обслуговуванні»

Dos – атака типу «Відмова в обслуговуванні»

EDos – атака типу «Економічна відмова в стійкості»

IaaS – модель хмарного сервісу «Інфраструктура як сервіс»

IDS – система розпізнавання вторгнень

IPS – система запобігання вторгнень

MitM – атака типу «Людина посередині»

PaaS – модель хмарного сервісу «Платформа як сервіс»

SaaS – модель хмарного сервісу «Програмне забезпечення як сервіс»

SLA – взаємна домовленість про рівень якості надання послуг

ЗЗІ – засоби захисту інформації

ІБ – інформаційна безпека

ІТКС – інформаційно-телекомунікаційна система

НСД – несанкціонований доступ

ОС – операційна система

ПЗ – програмне забезпечення

СМІБ – система менеджменту інформаційної безпеки

ЗМІСТ

ВСТУП……...……..1
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ……2
1.1. Стан питання……..2
1.2. Фізичні дата центри ……..2
1.3. Аналіз технології хмарних обчислень..……..3
1.4. Хмарні провайдери……5
1.5. Моделі розгортання хмарних сервісів……6
1.6. Переваги і недоліки використання хмарних ІТКС……9
1.7. Аналіз стандартів інформаційної безпеки……10
1.8. Висновки до розділу 1. Постановка задачі……...13
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА……15
2.1. Модель системи захисту інформації……..15
2.2. Ризики. Невизначеність ризику. Чутливість ризику……...16
2.3. Існуючі методи аналізу ризиків……18
2.4. Аналіз моделей оцінки ризиків в ІТКС……21
2.5. Складність аналізу ризиків існуючими методиками ……26
2.6. Класифікація порушників хмарної ІТКС……28
2.7. Модель загроз хмарної ІТКС……30
2.8. Метод розподілу рівнів захищеності ресурсів хмарної ІТКС……32
2.9. Лінійне програмування……....36
2.10. Методика оптимізації ризиків хмарної ІТКС……..37
2.11. Практичне застосування методики розподілу рівнів захищеності та оптимізації ризиків……..……....40
2.12. Висновки до розділу 2……...49
РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА……50
3.1. Обґрунтування витрат на створення методики розподілу рівнів захищеності хмарних ресурсів та оптимізації ризиків ……51
3.2. Визначення витрат на розробку методики ……...51

3.3. Оцінка можливого збитку від атаки на вузол чи сегмент корпоративної мережі……..55
3.4. Загальний ефект від впровадження методики аналізу та оптимізації ризиків ……58
3.5. Визначення та аналіз показників економічної ефективності розробленої методики……58
3.6. Висновки до розділу 3……59
ВИСНОВКИ……..61
ПЕРЕЛІК ПОСИЛАНЬ…….....63
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи
ДОДАТОК Б. Перелік документів на оптичному носії
ДОДАТОК В. Відгук керівника кваліфікаційної роботи
ДОДАТОК Г. Відгуки керівників розділів

ВСТУП

В інформаційно-телекомунікаційних системах, а саме в тих, що є відносно традиційними у плані використовуваних обчислювальних ресурсів та проектуванні, поняття інформаційної безпеки часто не є пріоритетним завданням у розумінні керівництва організації. Однак, якщо дана проблема має бути вирішена, існує цілком відпрацьований алгоритм побудови комплексної системи захисту інформації, що забезпечує стан захищеності як системи, так і інформації, що обробляється у цій системі.

Багато підприємств все частіше замислюються про міграцію локальних ІТКС у хмару, що має свої переваги та недоліки. Найбільш поширеним аргументом за міграцію ресурсів є вигідність даного рішення. Безпека інформації у разі забезпечується як із боку користувача, і із боку постачальника хмарних сервісів. Проте, у плані створення КСЗІ немає універсального підходу, який описує особливості побудови даних систем захисту для хмарних ІТКС. Також актуальною проблемою є обробка інформації різного ступеня конфіденційності, що потребує виділення ресурсів відповідних рівнів захищеності.

Існує необхідність розробки методики побудови хмарних ІТКС та її супровід на всіх етапах життєвого циклу, з використанням якої стає можливою оптимізація ризиків інформаційної безпеки при обробці інформації різної конфіденційності. Всі ресурси підлягають категоріюванню, і при цьому має враховуватись тип моделі надання хмарних сервісів – SaaS, PaaS та IaaS. Для успішної розробки методики допоміжними інформаційними ресурсами виступають нормативно-правові акти та стандарти в сфері інформаційної безпеки, а також порівняльні характеристики існуючих методів для локалізованих ІТКС для вироблення основних вимог до майбутньої методики побудови систем захисту ІТКС та оптимізації ризиків.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Питання інформаційної безпеки займає не останнє місце в процесі побудови будь-якої інфраструктури, а в більшості випадків є пріоритетом. Як відомо, останнім часом підприємства мігрують свої значні обчислювальні потужності з фізичних дата центрів до хмарних публічних хмар з урахуванням їх переваг та недоліків.

Складність забезпечення безпеки інформаційно-телекомунікаційної системи в хмарі зумовлена неможливістю впливу клієнта на процеси в дата центрі хмарного провайдера. Налаштування фаєрволу, розподілу доступу користувачів – особиста відповідальність клієнта, однак при достатній конфігурації цілісність, доступність та конфіденційність даних гарантується хмарним провайдером. Обробка інформації з різним ступенем конфіденційності та критичності може включати ризики для клієнта, так як обчислювальні хмарні сервіси мають різний рівень захищеності та вразливості. Отже, всі можливі ризики повинні бути проаналізовані, а на основі даного аналізу необхідно застосувати методику оптимізації ризиків.

1.2 Фізичні дата центри

Деякий час тому більшість інфраструктурних рішень включала в себе використання фізичних дата центрів на території підприємств, що мало низку обмежень.

Перш за все, це відносно статична інфраструктура, а її ріст можливий в більшості випадків за рахунок горизонтального розширення. Як відомо, горизонтальне розширення (horizontal scaling) – це процес додавання до кластеру нових обчислювальних ресурсів для розподілу завантаження на систему. В той же час вертикальне розширення (vertical scaling) реалізується за рахунок

нарощування обчислювальної потужності серверу, що вже знаходиться у використанні. Також це означає, що в момент пікової активності або її спаду неможливо налаштувати динамічне масштабування (Autoscaling), в результаті чого маємо або додаткові витрати на придбання нового апаратного чи програмного забезпечення, або мінімальне завантаження вже існуючих ресурсів [1].

Обслуговування такої інфраструктури повністю покладене на підприємство-власника, і, хоча, це дає перевагу з точки зору фізичної безпеки, даний процес вимагає залучення більшої кількості спеціалістів з певними навичками. Слід зазначити складність реалізації автоматизації обслуговування, тому всі дії персоналу відбуваються ітераційно на постійній основі. Оновлення інфраструктури супроводжується простоями - це часте явище для великих середовищ.

Безперечно, в використання фізичних дата центрів є і свої переваги. Найбільш суттєвим є контроль за обробкою та зберіганням даних, процесом розгортання програмного забезпечення, мережевими конфігураціями [2] – тобто повна самостійність та незалежність від постачальників віртуальних обчислювальних ресурсів як у випадку з хмарними провайдерами.

1.3 Аналіз технології хмарних обчислень

Хмарні обчислення – це модель мережевого доступу за потребою до деякої спільної множини обчислювальних ресурсів, що можуть бути оперативно виділені для користування або звільнені з мінімальними експлуатаційними витратами чи зверненнями до провайдера [2]. Характеризується динамічним масштабуванням та балансуванням обчислювальної потужності, а також включає неоднорідні ресурси з різним рівнем захищеності, що впливає на застосування існуючих методів захисту конфіденційної інформації. Поняття «контрольована зона» для даного типу інфраструктури не є актуальним, адже доступ до консолі управління інфраструктури можливий з будь-яких девайсів.

Принцип роботи побудований на основі технології віртуалізації [3], тобто концепції створення декількох ресурсів з одиночної фізичної апаратної системи. В процесі виділення ресурсів відбувається сегментація апаратних компонентів деякого комп'ютеру, таких як процесор, оперативна пам'ять та сховище даних, на декілька віртуальних елементів за рахунок розгортання спеціалізованого програмного забезпечення. Наприклад, у випадку віртуалізації оперативної системи отримуємо хостову машину та віртуальну, що характеризуються повною ізоляцією між середовищами, але в той же час можливі мережеві з'єднання, а також сконфігуровані спільні директорії для роботи з файлами.

В основному можлива віртуалізація оперативної системи, систем зберігання даних, програмного забезпечення та баз даних.

Технологія реалізується за допомогою гіпервізора, який може бути двох типів: автономний та на основі базової ОС [4]. Перший тип працює безпосередньо на апаратному забезпеченні хоста та представляє собою обмежену версію ОС, натомість другий функціонує як прикладне програмне забезпечення з використанням існуючої операційної системи. Автономний гіпервізор відрізняється підвищеною безпекою через відсутність необхідності операційної системи для його роботи, адже існує ймовірність атаки на ОС. Інша перевага – краща продуктивність та відсутність затримок знову ж таки через відсутність додаткого рівня ОС. Гібридні гіпервізори поєднують характеристики першого і другого типів.

На рисунку 1.1 зображені описані типи гіпервізорів.

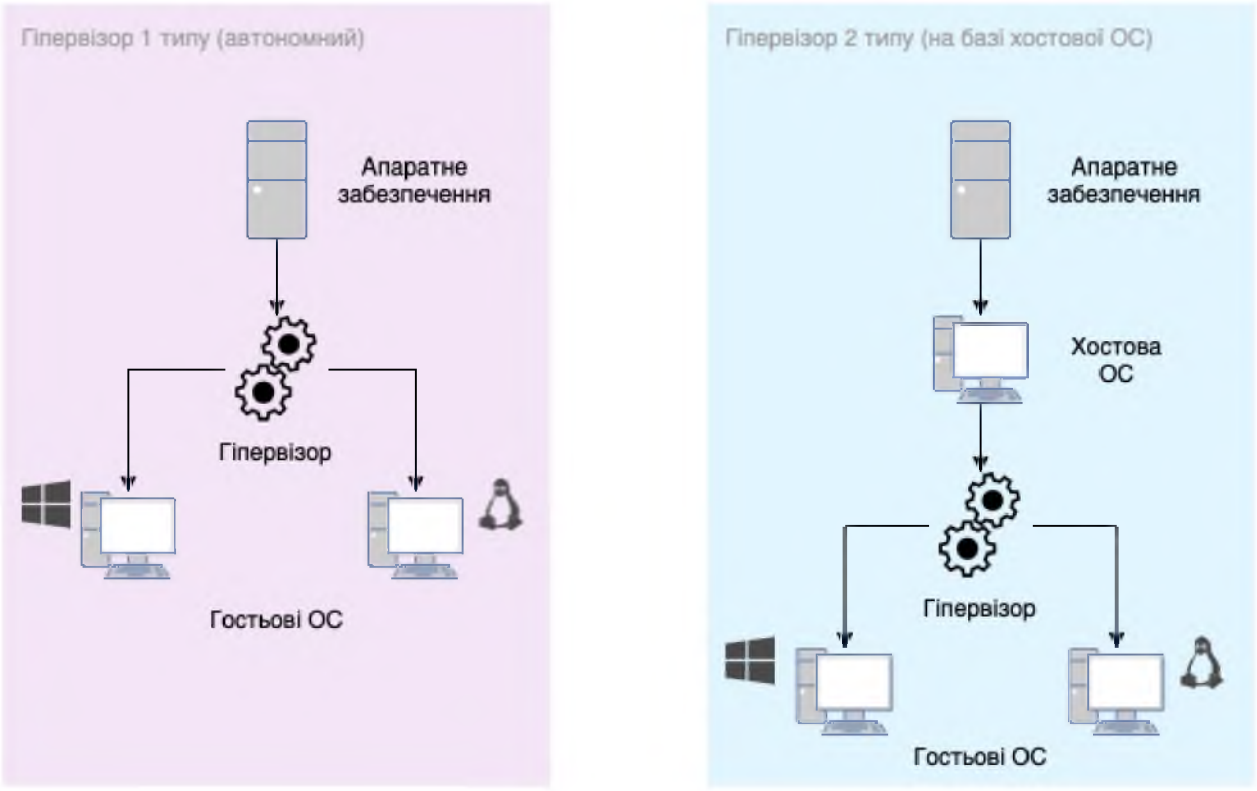

Рисунок 1.1 - Гіпервізори двох типів

В хмарних обчисленнях набули розповсюдження гіпервізори Xen, KVM, Hyper-V [5, 6], що використовуються в трьох найпопулярніших хмарних провайдерах: Amazon Web Services, Google Cloud Platform, Microsoft Azure.

1.4 Хмарні провайдери

Хмарні провайдери, або постачальники хмарних послуг – це компанії, що створюють публічні хмари, керують приватними хмарами та забезпечують виділення компонентів хмарних обчислень за вимогою [7]. Зазвичай, такі загальнодоступні хмари використовуються як частина гібридної хмарної інфраструктури, тобто локальна інфраструктура комбінується з хмарною.

Зручність послуг постачальника полягає в отриманні швидкого доступу до обчислювальних сервісів, які не потребують значного втручання в налаштування. Це стосується мережі, баз даних, хмарного сховища та серверів. Операційні системи, такі як Windows OS, Linux тощо за замовчуванням встановлюються на

створені сервери користувачем в залежності від його вибору та доступні для використання за лічені хвилини. Інше спеціалізоване інфраструктурне ПЗ, таке як Apache Kafka або Kubernetes не потрібно розгортати самостійно на серверах, адже дані сервіси є окремим продуктом в хмарі, а їх конфігурація на нижчих рівнях забезпечується провайдером.

Найпопулярнішими сертифікованими постачальниками хмарних послуг є Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure. Даний список не обмежений трьома гігантами в сфері хмарних технології, а в залежності від потреб користувача та його бізнесу можуть бути використані інші платформи.

1.5 Моделі розгортання хмарних сервісів

В цілому існує декілька моделей розгортання хмарних сервісів: загальнодоступна (публічна), гібридна або приватна хмара [8].

Публічні хмари – найпоширеніший тип розгортання хмарних обчислень. В даному випадку ресурси належать стороннім постачальникам хмарних послуг і керуються ними, доступ користувачеві надається через мережу Інтернет. Особливістю є розгортання ресурсів кожного користувача поряд з іншими «орендарями» з точки зору апаратного забезпечення хмарного постачальника, але програмно ресурси є ізольованими, а доступ реалізується з використанням облікових записів та веб-браузера. Сплата лише за те, що використовується, - основний принцип загальнодоступних хмар, масштабованість інфраструктури майже необмежена (окрім виділених квот на деякі ресурси), а широка мережа серверів постачальника забезпечує високу доступність. З точки зору безпеки – найбільш не захищений вид розгортання.

У випадку гібридної інфраструктури, користувачу надається більша гнучкість у поєднанні з більшою захищеністю. Фізична інфраструктура (on-premise) підприємства може бути поєднана з хмарною, при цьому ресурси хмарної інфраструктури є додатковим, що означає їх зупинку чи видалення у разі

відсутності потреби в масштабованості. Конфіденційна інформація може циркулювати лише в локальній інфраструктурі, що означає контроль користувача за даними. Однак, потенційною проблемою може бути складність налаштування з'єднання локальної та хмарної інфраструктури.

В приватній хмарі розгортаються ресурси лише одного підприємства, вона може бути фізично розташована в центрі обробки даних організації або розміщуватися за допомогою стороннього постачальника послуг. Програмне забезпечення призначене виключно для потреб підприємства, те ж саме стосується і обладнання. Такі хмари часто використовуються фінансовими або державними установами з критично важливими операціями або даними для посилення контролю над своєю інфраструктурою. Масштабованість є більшою порівняно з локальною інфраструктурою.

Важливо розглянути основні моделі надання послуг хмарних провайдерів - IaaS, PaaS, SaaS [9].

Модель Інфраструктури як сервісу (IaaS) полягає в оренді підприємством серверів та сховищ даних в хмарі для розгортання свого ПЗ чи зберігання даних. Користувачі можуть запускати будь-яку ОС на орендованих серверах без витрат на обслуговування та експлуатацію. Провайдер контролює фізичну інфраструктуру, а за встановлення та підтримку клієнтського ПЗ не несе відповідальності. За такою моделлю надаються ресурси Google Compute Engine, AWS EC2 тощо.

Платформа як сервіс (PaaS) – надання конкретного програмного забезпечення, що розгорнуте в обраній хмарній платформі самим провайдером і керується також ним. До ПЗ, наданого за такою моделлю, можуть відноситися: операційна система, система управління базами даних, засоби розробки ПЗ чи тестування, сервіси контейнерізації. Прикладами можуть слугувати Google App Engine, Heroku, AWS Elastic Beanstalk.

Програмне забезпечення як (SaaS) включає надання споживачам продуктів, що обслуговуються, розгортаються в хмарі самим провайдером. Доступ надається через браузер чи додаток на ПК. Споживач лише повинен сплачувати

за використання цього програмного забезпечення згідно з умовами надання послуг. Це найрозповсюдженіша модель, за якої клієнти отримують доступ до Microsoft Office 365, Google Doc, Dropbox тощо. На рисунку 1.2 перелічені приклади сервісів хмарних провайдерів, що відповідають переліченим моделям надання послуг.

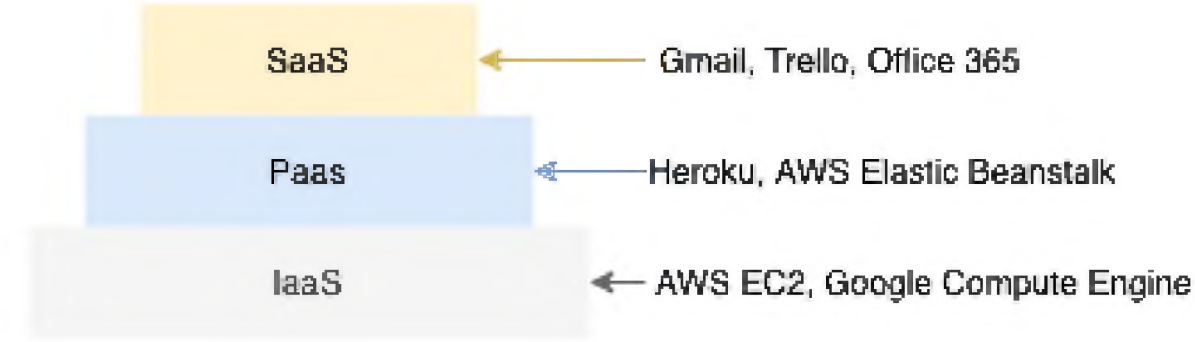

Рисунок 1.2 – Сервіси, що відповідають моделям надання послуг

На рисунку 1.3 зображені рівні управління користувачем та хмарним провайдером.

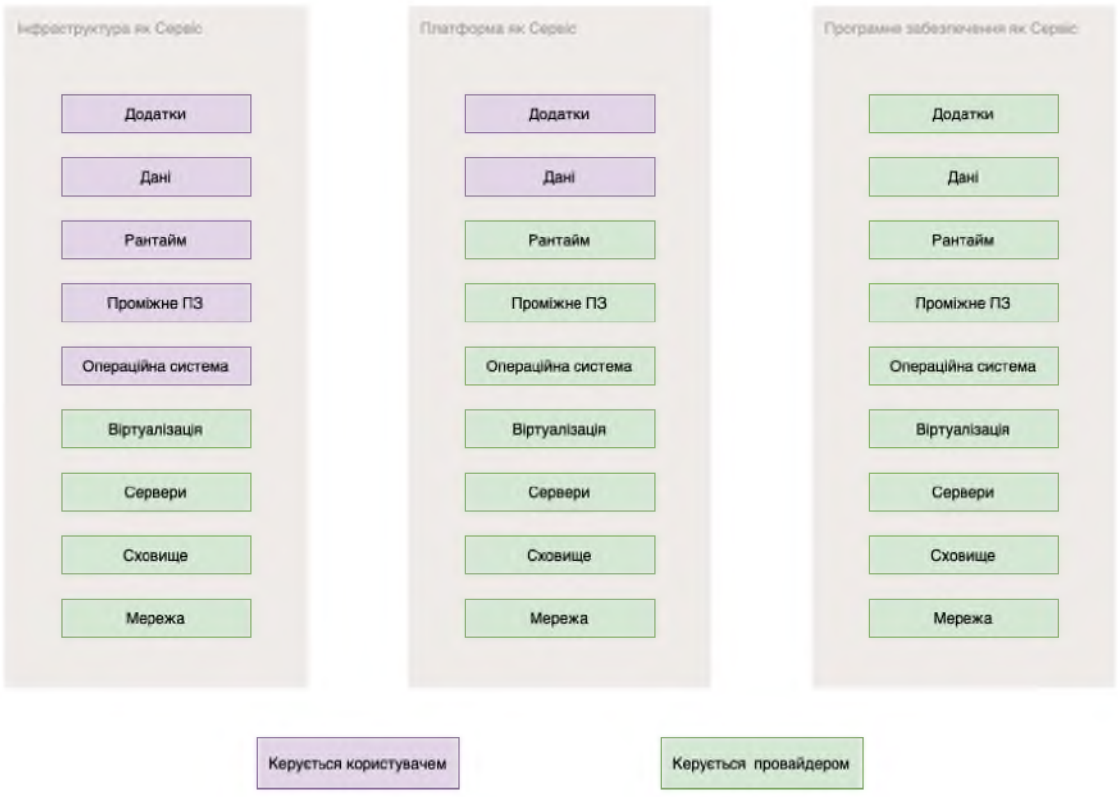

Рисунок 1.3 – Рівні управління моделей розгортання

Додатковими моделями є:

- Автентифікація як сервіс (AaaS), за якої надаються такі сервіси як мультифакторна автентифікація, Single Sign-On та менеджмент паролів [].
- База даних як сервіс (DBaaS) – керований сервіс хмарним провайдером, управління якого забезпечує провайдер, користувач лише опікується даними [].

1.6 Переваги і недоліки використання хмарних ІТКС

Використання хмарних ІТКС має ряд переваг та недоліків у порівнянні з локальної інфраструктурою, що можуть бути ключовими в процесі вибору інфраструктурного рішення. Аргументами «за» є наступні твердження.

Зменшення витрат. Немає необхідності витрачати значні кошти на закупівлю апаратного забезпечення для внутрішнього зберігання, а також на обслуговування та навчання обслуговуючого персоналу [12].

Відсутність єдиної точки збою. Всі дані реплікуються між декількома серверами, тому, якщо один сервер з даними виходить з ладу, інший все ще зберігає той самий набір даних [12].

Можливість віддаленої роботи з ресурсами. За допомогою веб консолі хмарного провайдеру робота з необхідними компонентами інфраструктури стає надзвичайно ефективною. В той же час кожен користувач може бути впевнений, що працює з актуальною версією документів, ресурсів тощо [12].

Масштабованість. За умови стрімкого розвитку підприємства, може виникнути необхідність в додатковій обчислювальній потужності чи в розширеному сховищі даних, при цьому досягти цього можна в мінімальні строки. В інший ситуації, коли кількість запитів клієнтів підприємства зростає або спадає на певний час під впливом деяких подій, конфігурація інфраструктури

дає змогу автоматично нарощувати додаткові обчислювальні ресурси або скорочувати непотрібні після спаду активності [12].

Автоматизація. Резервне копіювання, налаштування серверу під час його старту, доставка оновленої версії створеного ПЗ на сервери – це лише не повний список можливих дій, що не потребують втручання персоналу, а можуть виконуватися механізмами ресурсів хмарних платформ [12].

Регуляція нормативними актами роботи хмарних провайдерів також є перевагою, адже можна бути впевненим в дотриманні кращих практик.

Однак, недоліки роботи з хмарними ІТКС стосуються в більшості безпеки інформації, а саме забезпечення конфіденційності, цілісності та доступності оброблюваної інформації [12].

Питання про безпеку хостів, мереж та програмних інтерфейсів залишається відкритим, що ставить під сумнів дотримання конфіденційності.

Доступність може бути порушена навіть відсутністю Інтернету з боку користувача, що унеможливлює доступ до ресурсів хмарної інфраструктури за необхідності.

Існує поняття «прив'язка до постачальника (vendor lock)» – залежність користувача від одного постачальника, що визиває складність міграції з однієї платформи до іншої в плані коштів або технічних можливостей. Тобто, перехід з однієї хмарної платформи до іншої потребуватиме значних зусиль. Але варто зазначити, що надані сервіси поступово стають більш гнучкими та підтримують багатохмарну (multicloud) модель.

1.7 Аналіз стандартів інформаційної безпеки

Для повного аналізу нормативно-правових актів в сфері інформаційної безпеки стосовно даної теми, необхідно розглянути стандарти як для аналізу ризиків, так і для регламенту безпеки хмарних платформ [13].

Серія стандартів ISO/IEC 27000 включає стандарти, що можуть бути застосовані для вирішення задачі оптимізації ризиків:

- ISO/IEC 27001:2013 “Information technology – Security techniques – Information security management systems – Requirements”. Встановлює вимоги до створення, впровадження СМІБ організації, а також її підтримки та покращення. Включає вимоги до оцінки ризиків ІБ. Положення стандарту є загальними для всіх без винятків організацій.
- ISO-IEC 27002:2005 “Information technology – Security techniques – Code of practice for information security management”. Містить поради з менеджменту ІБ для спеціалістів зі створення СМІБ та її супроводження. Серед основних розділів: політика безпеки, організація ІБ, фізична безпека, управління доступом, а також інцидентами.
- ISO/IEC 27004:2016 “Information technoloty. Security techniques. Information security management. Measurement”. Містить рекомендації для допомоги організаціям в оцінці ефективності ІБ та СМІБ з метою виконання вимог ISO/IEC 27001:2013.
- ISO/IEC 27005:2011 “Information technology – Security techniques – Information security risk management”. Надає рекомендації для реалізації достатнього рівня ІБ, заснованого на менеджменті ризиків. Стандарт описує критерії та підходи до оцінки ризиків, а також оптимізацію чи мінімізацію ризиків. Цей процес проводиться за декількох етапів:
    - Ідентифікація активів постачальника послуг та порушників ІБ
    - Ідентифікація існуючих нормативних вимог ІБ
    - Ідентифікація загроз ІБ
    - Оцінка ймовірності реалізації загроз ІБ за допомогою якісного підходу
    - Оцінка вразливостей ІБ ІТКС
    - Оцінка вартості активів
    - Розрахунок ризиків ІБ кількісним методом

Стандарт ISO/IEC 31010:2009 “Risk management – Risk assessment techniques” також містить принципи, що стосуються вибору та застосування систематичних методик оцінки ризику.

Що стосується ІБ в хмарних сервісах, для регуляції існує стандарт ISO/IEC 27017:2015 “Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services”. Провайдери хмарних сервісів, а також їх користувачі, повинні дотримуватися додаткових вказівок щодо реалізації засобів управління ІБ в хмарній платформі. При цьому для постачальників щорічно проводяться атестації акредитованими агентствами, однак результати не розповсюджуються на інфраструктуру користувача, а лише на сервіси, що пропонуються провайдером [14].

Стандарти організації National Institute of Standards and Technology (NIST) формують фреймворк управління ризиками, серед основних є наступні:

- NIST SP 800-30 “Guide for Conducting Risk Assessments”
- NIST SP 800-39 “Managing Information Security Risk”
- NIST SP 800-53A “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans”
- NIST SP 800-55 “Performance Measurement Guide for Information Security”
- NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing”. Наразі є основним нормативно-методичним документом в області розгортання, експлуатації та забезпечення ІБ хмарних сервісів
- NIST SP 800-145 “The NIST Definition of Cloud Computing”. Містить основні поняття в сфері хмарних обчислень
- NIST SP 800-146 “Cloud Computing Synopsis and Recommendations”. Включає інформацію про хмарні технології, рекомендації з експлуатації, а також питання оцінки ризиків у разі застосування хмарних сервісів

Приватна організація Cloud Security Alliance створила нормативно-методичний документ CSA “Security Guidance for critical areas of focus in cloud computing” для рекомендації щодо побудови КСЗІ хмарного сервісу.

Найбільш розповсюдженим документом для регуляції обов’язків сторін в сфері хмарних ІТКС є “Service Level Agreement (SLA)” [15]. Це формальний договір між клієнтом та постачальником, що містить опис наданої моделі

обслуговування, права та обов'язки сторін, а також рівень якості надання сервісу. Згідно з цим документом, хмарні провайдери надають інформацію, наприклад, про рівень забезпечення щомісячного відсотку безвідмовної роботи в залежності від використаного сервісу.

В залежності від типу оброблюваних даних, хмарні сервіси проходять щорічні аудити для сертифікації їх продуктів на відповідність стандартам в індустрії платіжних карток (PCI DSS) [16], медичного страхування (HIPAA) [17] тощо.

Регуляція процесу збору, обробки та зберігання персональних даних клієнтів відбувається згідно з документом General Data Protection Regulation (GDPR), що стосується безпосередньо хмарних провайдерів [18].

Допомогти побудувати безпечну інфраструктуру в залежності від обраного інструменту покликаний Center for Internet Security (CIS) Benchmark. Містить зрозумілий список рекомендацій щодо використання кожного компоненту хмарної інфраструктури згідно з кращими практиками забезпечення ІБ, причому для кожного хмарного провайдеру існує окремий набір практик з урахуванням особливостей їх сервісів [19].

1.8 Висновки до розділу 1. Постановка задачі

В даному розділі було проаналізовано роботу фізичних дата центрів, функціонування хмарних ІТКС, були описані моделі розгортання. Визначено переваги і недоліки використання як хмарних провайдерів, так і локальної інфраструктури. Для забезпечення процесу оцінки ризиків при використанні хмарних платформ необхідною нормативно-правовою базою були приведені основні стандарти в сфері інформаційної безпеки.

Задачею даної роботи є оцінити існуючі моделі аналізу ризиків, побудувати модель загроз та модель порушника хмарної ІТКС, провести аналіз ризиків, пов'язаних з особливостями використання хмарних технологій, а також на основі отриманих результатів шляхом використання методики розподілу

рівнів захищеності ресурсів оптимізувати їх склад за допомогою методів лінійного програмування.

РОЗДІЛ 2.

2.1 Модель системи захисту інформації

Існуюча модель взаємозв'язку між компонентами інформаційної безпеки розглянута на рисунку 2.1.

Рисунок 2.1 - Взаємодія між компонентами ІБ

Всі компоненти пов'язані між собою та безпосередньо впливають на стан захищеності інформації, тому слід зазначити основні з них у контексті використання хмарної інфраструктури.

Ресурсом, або активом є інформація чи компонент, що становить важливість для власника. Власник має на меті забезпечення стану захищеності свого активу. Завдати шкоди ресурсу може порушник, тобто особа, що може отримати несанкціонований доступ за рахунок експлуатації відомої вразливості.

Загроза – сукупність умов та факторів, що можуть створювати потенційну чи вже існуючу небезпеку, в даному випадку для хмарної ІТКС.

Захисні заходи, або контрзаходи - впроваджені заходи для зниження рівня потенційного ризику.

Вразливість – недолік в програмному, апаратному забезпеченні або процедурі, що може бути експлуатований порушником з метою отримання доступу до компоненту інфраструктури і, як наслідок, до циркулюючої інформації (активу).

Ризик – ймовірність того, що конкретна загроза безпеці використовуватиме вразливості системи [20].

2.2 Ризики. Невизначеність ризику. Чутливість ризику

Аналіз ризиків будується на обробці вхідних даних та прийнятті рішень, що направлені на знаходження найбільш корисних стратегій для обробки цього ризику. Під час аналізу розглядаються причини та джерела ризику, їх наслідки та ймовірності виникнення цих наслідків.

Дуже часто можна стикнутися з поняттям невизначеності ризику, що означає хоча б часткову недостатність інформації, розуміння чи знання щодо події, її наслідків чи ймовірності [21]. Навіть ступінь невизначеності підлягає оцінці, що базується на розумінні, кількості, якості та цілісності метрик й доступної інформації, пов'язаної з ризиком. Поряд з аналізом невизначеності існує аналіз чутливості ризику, тобто яке значення величина ризику має відносно змін в окремих параметрах вхідних даних. Даний аналіз застосовується для визначення тих даних, які повинні бути точними, і тих, що мають менший вплив на точність оцінки. Тобто, можна сказати, що до другого типу даних ризик має меншу чутливість.

Отже, необхідно виявляти джерело невизначеності для всебічного та повного аналізу ризиків, а також встановлювати параметри, до яких є чутливим аналіз, і ступінь його чутливості.

Згідно з принципами інформаційної безпеки хмарних ІТКС, ризики можуть бути класифіковані як:

- Ризик порушення конфіденційності. Перш за все, конфіденційність – забезпечення недоступності інформації для неавторизованих користувачів в кожній точці обробки інформації. Конфіденційність повинна забезпечуватися в процесі обробки, збереження та передачі даних. Порушення даної властивості інформації можливе за рахунок перехвату мережевого трафіку, викрадення снапшотів віртуальної машини або з власної помилки користувачів хмарної ІТКС чи за наявності певного наміру.
- Ризик порушення цілісності. Гарантія незмінності, точності та повноти інформації, що обробляється в хмарному сервісі, забезпечується цілісністю. Жодна інформація не повинна бути змінена або знищена внаслідок НСД.
- Ризик порушення доступності. Можливість отримати авторизований доступ до необхідної інформації своєчасно забезпечується доступністю. На цю властивість може вплинути збій, наприклад, динамічного балансування або масштабування ресурсів хмарної інфраструктури, зі сторони порушників можливі DDoS, EDoS атаки.

Загальновідомі ризики перераховуються в документі CSA “Security Guidance for critical areas of focus in cloud computing”, до їх списку можна включити викрадення облікових записів, атаки на гіпервізор, атаки на хмарну інфраструктуру, викрадення обчислювальних ресурсів хмарної ІТКС та порушення механізму динамічного балансування.

2.3 Існуючі методи аналізу ризиків

Існують два типи підходів до аналізу ризиків.

Перший з них базується на перевірці захищеності ІТКС згідно з вимогами стандартів та нормативно-правових документів в сфері ІБ. Забезпечення безпеки підтверджується повною відповідністю вимогам з метою запобігання шкоди внаслідок інцидентів. Ефективність, в свою чергу, спостерігається при однакових значеннях рівню витрат на зменшення ймовірності ризику та очікуваних втрат у разі відсутності запобіжних дій або у випадку, коли витрати на систему захисту менші за можливі втрати.

За іншого підходу також має місце збалансованість витрат та отриманої ефективності, а вартість засобів захисту не повинна бути більшою за вартість інформації, що підлягає захисту. Можна стверджувати, що в даному випаду використовуються принципи кількісної оцінки та управління ризиками.

Стандарт ISO/IEC 27000 визначає ризик як комбінацію ймовірності реалізації загрози та наслідки. Ключовими показниками є SLE (Single Loss Expectancy) та ALE (Annualized loss expectancy) [22]. Тобто, розрахунок одиночного випадку втрати та знаходження очікуваних річних втрат.

SLE = цінність активу * фактор впливу

Фактор впливу – відсоток від цінності активу, який буде втрачено в разі реалізації загрози.

ALE = SLE * річна частота реалізації

Якщо цінність активу – 1000$, а втрачено було ¼ частину внаслідок інциденту, в такому випадку фактор впливу – 25%. SLE буде дорівнювати 250$. ALE в даному прикладі при частоті реалізації 5 разів на рік буде мати значення 1250$.

Втрати можуть бути більшими за початкову вартість активу, наприклад, у випадку масштабного позову до відповідальності після інциденту, відповідно, фактор впливу буде сягати більше 100%.

Річна частота реалізації може бути меншою, ніж 1, якщо інцидент очікується раз в декілька років. В такому випадку його значення розраховується як 1/n, де n – кількість років.

Впевненість в ризику можлива за наявності історичних даних, але якщо призначення значень компонентам для розрахунку відбувалося без підгрунтя, маємо невизначеність ризику і в кількісному підході. Для розрахунку допоможе модифікація вже зазначеної вище формули ALE:

ALE = SLE * річна частота реалізації * невизначеність,

де невизначеність коливається від 1 (абсолютно визначеного) до чисел більших, ніж 1 (невизначених). Невизначеність в значенні 1.5 означає, що показник ALE може бути на 50% більшим, ніж при абсолютній визначеності ризику.

Згідно зі стандартом ISO/IEC 27005 оцінка ризику відбувається шляхом множення ймовірності реалізації загрози (P) та значення величини втрат (C).

$$R = P_i \times C_i \qquad (2.1)$$

В подальшому необхідно обрати запобіжний захід, що може бути одним з наступних [20]:

- Зниження ризику. Означає вибір заходів та засобів управління, що дозволяють оцінити ризик як залишковий зі значенням, нижчим за пороговий.
- Збереження ризику. Якщо величина є допустимою, запобіжні заходи не застосовуються.
- Запобігання ризику. Повна відмова від умов, що викликають оцінений ризик.
- Переніс ризику. Залучення третьої сторони для побудови ефективного процесу управління ризиком.

Методи аналізу ризиків інформаційної безпеки можуть бути якісними, кількісними та напівкількісними. Вони визначають сукупність певних послідовних дій для оцінки ризиків та можуть включати спеціалізоване програмне забезпечення для цієї мети [23].

Кількісний метод. Використані дані є об'єктивними та вимірювальними, а розрахунки базуються таких змінних як вартість активу, ймовірність реалізації загрози та втрата даного активу. Дозволяє розрахувати коефіцієнт повернення інвестицій (ROI) на запроваджені рішення. Безперечною перевагою є зростаюча точність аналізу з урахуванням збільшення даних про попередні оцінки. Однак, даний метод все ще має суб'єктивне бачення учасників процесу аналізу, на трудомісткі розрахунки необхідно чимало часу та необхідних знань персоналу. Прикладами такого методу слугують програмні продукти RiskWatch, ГРИФ 2006 і методологія ISAMM [24].

Якісний метод. Ризик подається прозоро та його класифікація зрозуміла, а вартість активу з фінансової точки зору немає необхідності визначати. Залучення персоналу відбувається легше, адже відсутні специфічні розрахунки в залежності від використаного методу кількісного аналізу. Проте, знайдені ризики можуть недостатньо відрізнятися за ступенем важливості, а інвестування в запобіжні заходи складно аргументувати. Прикладом є методика Octave, що має допоміжні програмні засоби [25].

Змішані методи комбінують раніше перелічені особливості, при цьому застосовується числова оцінка для подальшого розрахунку рівню ризику за формулою з використанням змінних ймовірності та наслідків. На основі даного методу побудовані методики Mehari, Magerit та CRAMM [26], що також мають допоміжні програмні інструменти [25].

Оцінені ризики можуть бути розподілені по групах в залежності від необхідності запобіжних заходів.

Універсальний алгоритм процесу оцінки інформаційних ризиків стандарту ISO 27005 зображений на рис. 2.2.

Рисунок 2.2 - Алгоритм оцінки інформаційних ризиків ISO 27005

2.4 Аналіз моделей оцінки ризиків в ІТКС

Для повного аналізу існуючих моделей аналізу ризиків необхідно охопити якісні, змішані та кількісні методи оцінки.

Аналіз небезпеки процесу (PHA). Відноситься до змішаних методик оцінки та є певним набором організованих і систематичних оцінок потенційних небезпек. Використовується через ефективність на ранніх стадіях проектування системи захисту інформації в умовах недостатніх даних про функціонування ІТКС для ідентифікації вразливостей, загроз, інцидентів та потенційних втрат. В процесі аналізу приймаються до уваги географічне розташування об’єкту,

обладнання, програмно-апаратні інтерфейси компонентів ІТКС та середовище функціонування. Класифікація ризиків відбувається за оцінкою від високого (червоний рівень), середнього (жовтий рівень) до низького (зелений рівень). Оцінюється категорія частоти інциденту та його тяжкість [28]. Етапи аналізу методом PHA наведені на рис. 2.3.

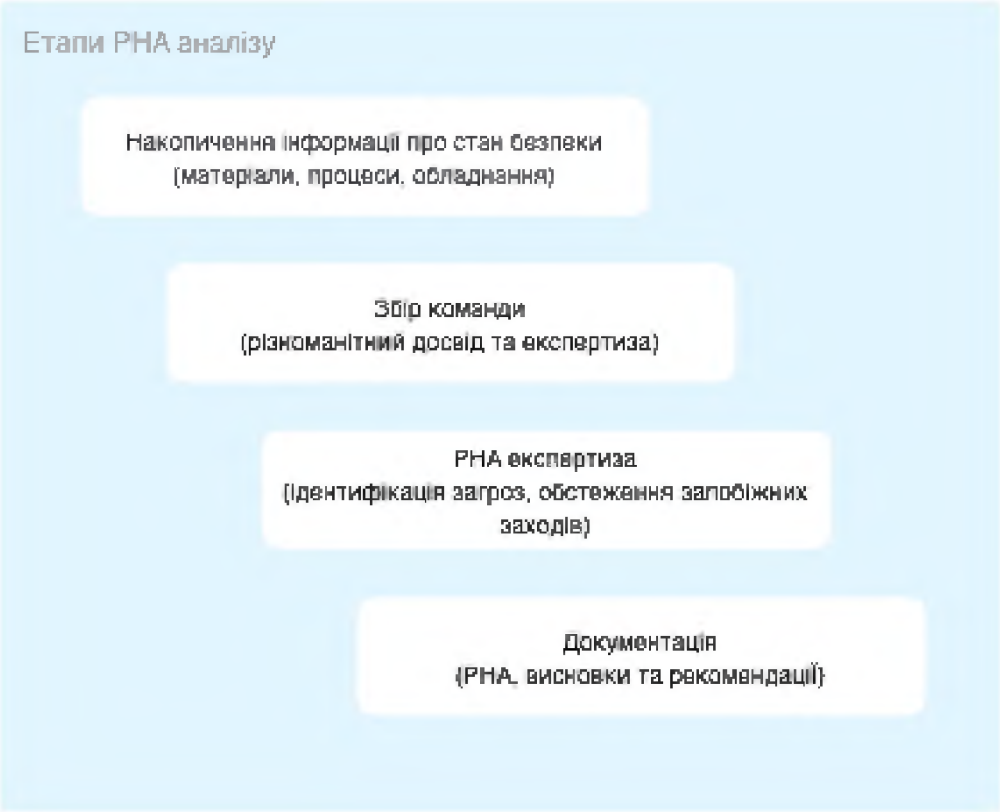

Рисунок 2.3 – Етапи аналізу методом PHA

Дослідження небезпеки та працездатності (HAZOP). Якісний метод аналізу ризиків, представляє собою процес деталізації та ідентифікації проблем небезпеки та працездатності систем, аналіз виконується групою спеціалістів [29]. Метою створення даного методу була ідентифікація відхилень від планів проекту, відмов, їх причин та наслідків. Ідея методу – в систематизованій перевірці. Основною проблемою є комбінація даного методу з іншими, так як дослідження складної системи потребує використання декількох методів аналізу.

Процес оцінки ризиків може бути побудованим наступним чином:

- Призначення особи з відповідними повноваженнями для проведення дослідження

- Визначення мети та області дослідження
- Встановлення ряду «управляючих слів»
- Формування експертної групи та сбір документації
- Безпосередньо в процесі аналізу дана експертна група розділяє процес інформаційної безпеки на складові та підсистеми, щоб конкретизувати аналіз. Мета встановлюється для кожного компоненту окремо, як і причини та наслідки в кожному випадку виявлення негативного результату
- Розробка запобіжних заходів для мінімізації ризиків

Етапи аналізу методом HAZOP представлені на рис. 2.4.

Рисунок 2.4 – Етапи аналізу методом HAZOP

Аналіз рівнів надійності засобів захисту (LOPA). Змішаний метод аналізу ризиків, дозволяє аналізувати наявність достатніх заходів щодо мінімізації ризиків. В ході використання методу відбуваються пошуки рівнів захисту, що унеможливлюють причину, яка призводить до небажаних наслідків. Розраховується величина наслідків для визначення актуальності запобіжних заходів щодо зменшення ризику до довільного рівня. Спосіб може використовуватися для підвищення точності раніше описаних методик PHA та HAZOP. LOPA забезпечує знаходження незалежних рівнів захисту (IPL) та рівнів безпеки (SIL).

Вхідними даними є:

- Інформація щодо ризиків, вразливостей, загроз та наслідків, що може бути отримана в рамках попереднього аналізу небезпек або за допомогою іншої методики
- Інформація щодо існуючих заходів менеджменту ризиків
- Частота інцидентів та ймовірність відмови засобів захисту інформації, величина наслідків та визначення довільного ризику

В ході дослідження відбувається встановлення причин небажаного результату, знаходження пар «причина – наслідок», визначення рівнів захисту, що перешкоджають небажаним наслідкам, та їх ефективності. Порівняння розрахованого рівню ризику з довільним для визначення необхідності додаткових засобів захисту.

Для кількісного розрахунку ризиків може використовуватися дана формула ймовірності несанкціонованого отримання інформації:

$$P = 1 - \prod_i \left[1 - P_{ijk}^{(б)}\right] \prod_j \left[1 - P_{ijk}^{(б)}\right] \prod_k \left[1 - P_{ijk}^{(б)}\right], \qquad (2.2)$$

де i – структурний компонент системи;

j – канал несанкціонованого отримання інформації;

k – категорія порушника.

Загальна формула для визначення ризику реалізації загрози щодо активу:

$$R = R_{\text{загр}} R_n C \frac{K_0 + K_i}{2} 100\%, \quad (2.3)$$

де R – числова величина ризику реалізації загрози,

$R_{\text{загр}}$ – ймовірність реалізації загрози;

R_n – ризик невідповідності вимогам нормативно-технічної документації;

C – цінність активу;

K_0 – ймовірність експлуатації організаційних вразливостей;

K_1 – ймовірність експлуатації технічних вразливостей.

Найзагальнішою моделлю захисту АС є модель системи безпеки з повним перекриттям [30]. Вона базується на принципі існування хоча б одного засобу забезпечення безпеки потенційного каналу витоку інформації. Загалом включає декілька послідовних кроків. Перелік всіх об'єктів системи, що підлягають захисту від впливу порушника:

$$R = \{r_i\} \quad (2.4)$$

Перелік всіх можливих варіантів його дій (визначення потенційних загроз):

$$S = \{s_{ij}\} \quad (2.5)$$

Розрахунок кількісного виразу «загроза – об'єкт», що представлені дводольним графом $\{S, R\}$, при цьому одна загроза не обмежується одним об'єктом і навпаки.

Наступним кроком є формування множини ЗЗІ:

$$I = \{i_n\}, \quad (2.6)$$

останній етап включає оцінювання кількісної міри можливості протидії – {S, R, I}.

Дана модель може бути розширена за допомогою п'ятикортежного набору {S, R, I, Q, T}, де додається інформація про множину вразливостей ІТКС (Q) та множину бар'єрів (T), що перекривають шляхи реалізації загроз ІБ та розглядаються як $\{P_i, L_i, R_i\}$ - ймовірність реалізації загрози, величина шкоди в

разі інциденту та ступінь супротиву механізмів захисту відповідно. Залишковий ризик характеризує надійність бар'єру та визначається за формулою:

$$Risk_i = P_i L_i (1 - R_i) \quad (2.7)$$

2.5 Складність аналізу ризиків існуючими методиками

Як було зазначено раніше, існує велика кількість найрізноманітніших методик аналізу ризиків. Однак, при подальшому аналізі даних методів, з'ясовуються їхні недоліки та деякі обставини, за яких методику можна назвати непридатною для повноцінного аналізу ризиків. У випадку з хмарними обчисленнями, існуючі методики можуть не покривати всі критерії оцінки, що також не дає повної картини для вживання превентивних заходів. І хоча це лише питання часу, слід навести аргументи проти використання існуючих методик. Здебільшого це стосується фактору невизначеності під час розробки та запровадження інфраструктурних рішень.

Контрольована зона, яка раніше досліджувалась при створенні комплексної системи захисту інформації інформаційно-телекомунікаційних систем підприємств, для хмарних платформ стає неактуальним поняттям. Все інформаційне середовище може бути розділене на зони [31]. Зона публічного доступу - це незахищене середовище, що може бути за межами підприємства. Забезпечується обмежений контроль доступу до інформації та фізичних активів, де будь-яка втрата призведе до низького та середнього впливу на бізнес. Прикладом може слугувати периметр будівлі підприємства, громадське фойє, зона прийому клієнтів або навіть кафе, де можлива позаофісна робота. Не рекомендується зберігати фізичні активи чи інформацію в зоні публічного доступу. Натомість контрольованою зоною є робоче середовище, середовище з обмеженим доступом та середовища зберігання таємної інформації. Відрізняється забезпеченням додаткових заходів безпеки, адже тут збирається, обробляється, зберігається інформація з відповідним маркуванням ступеню секретності. Для робочої зони, де може не циркулювати інформація з обмеженим

доступом, можуть бути запроваджені слабші методи захисту інформації, однак оцінити переваги від впровадження механізмів захисту допомагає саме аналіз ризиків.

Повертаючись до поняття неактуальності контрольованої зони, аргументувати це можна тим, що доступ до ресурсів хмарної інфраструктури надається за допомогою веб інтерфейсу з будь-якого авторизованого девайсу, однак в більшості випадків авторизація стосується облікових записів, а не самого апаратного забезпечення. Менеджмент ресурсів хмарної платформи гарантує зручність та ефективність з погляду бізнесу, проте дотримання безпечних заходів поставлено під сумнів.

Концепція Bring Your Own Device (BYOD) [32] набула широкого розповсюдження, і якщо робочі комп'ютери персоналу оснащені необхідним програмним забезпеченням захисту системи, то персональні девайси цілком можуть бути невідповідними для використання в подібних цілях. Впроваджуються політики інформаційної безпеки, що розповсюджуються на персональні пристрої та зменшують перелік можливих загроз, однак не гарантують повного їх перекриття.

Існує деяка складність в оцінці наявності вразливостей хмарної інфраструктури та можливих загроз щодо неї у зв'язку з реплікуванням ресурсів, керованим самою хмарною платформою. Компоненти можуть бути розподілені по кількох регіонах, проте реалізація цієї функції прихована від кінцевого користувача. У той час як за наявності фізичного датацентру це зводить нанівець ризики, пов'язані з географією. І тут ми маємо справу з загрозами фізичного простору, що знову ж таки пов’язано з поняттям вже відомої контрольованої зони.

Сервіси, що надаються хмарною платформою, будь це сховище даних або віртуальні машини, безсумнівно можуть містити вразливості, у тому числі і zero day, проте через невідомість ймовірності реалізації загрози щодо вразливості проведення аналізу ризиків може бути ускладнено. А беручи до уваги той факт, що одну знайдену вразливість можуть містити тисячі однакових

ресурсів різних користувачів, стає зрозумілим, що даний ризик повинен бути обов'язково оцінений для ефективності аналізу.

Загрози хмарної інфраструктури можуть бути нетиповими для традиційних обчислювальних мереж, а тому може бути не достатньо статистичних даних щодо ймовірності реалізації, наслідків інцидентів тощо.

Крім того, моделі надання послуг є різними, їх рівні абстракції відрізняються між собою і тому є специфічні для кожної моделі вразливості та механізми їх експлуатації. Наприклад, IaaS надає більше повноважень кінцевому користувачеві з управління власною інфраструктурою, проте PaaS приховує деталі реалізації, даючи лише необхідну функціональність для досягнення поставленої мети клієнта. Тому стає зрозуміло, що від обраної моделі залежить перелік загроз і вразливостей.

2.6 Класифікація порушників хмарної ІТКС

Щоб визначити найімовірніші атаки на хмарну ІТКС, необхідно скласти модель порушника. Моделлю порушника є аналіз можливих портретів порушників, їх інформованості про компоненти системи та наявність технічної підготовки.

Порушники можуть належати до двох типів в залежності від наявності прав доступу:

- Зовнішні порушники. Не мають доступу до ІТКС, тому реалізують загрози з зовнішніх мереж.
- Внутрішні порушники. Мають доступ до ІТКС та її ресурсів, можуть діяти безпосередньо в ІТКС. Можуть належати до привілейованих чи непривілейованих користувачів, що може впливати на широту їх повноважень для реалізації загроз.

З огляду на особливості хмарних ІТКС, можна виділити наступні категорії порушників.

Особи, які не мають санкціонованого доступу до хмарної ІТКС (зовнішні порушники). Підключення до внутрішньої мережі можливе за допомогою зовнішніх каналів зв'язку. Отримання доступу можливе з використанням шкідливого ПЗ.

Користувачі, які мають санкціонований доступ до хмарної ІТКС, але не мають доступу до інформації, що обробляється в рамках ІТКС (внутрішні порушники). Взаємодія з хмарною ІТКС в даному випадку може включати використання програмно-апаратних закладок, знімання інформації, модифікацію хмарної інфраструктури, при цьому виконання подібних дій не ускладнено, оскільки використовується безпосереднє підключення.

Користувачі хмарної ІТКС мають обмежені повноваження для взаємодії з ІТКС з робочого місця (внутрішні порушники). Ця категорія порушників, як і наступні дві категорії, має необхідні привілеї для отримання доступу до цільової інформації. Також їм відомі дані про топологію та інфраструктуру загалом, оскільки порушники мають безпосередній доступ до її компонентів.

Користувачі, які мають віддалений доступ до певної інформації та компонентів ІТКС (внутрішні порушники).

Привілейовані користувачі, що виконують роль адміністратора безпеки повної частини ІТКС (внутрішні порушники).

Обслуговуючий персонал ресурсів ІТКС, у тому числі постачальники сервісів та підрядники (внутрішні порушники).

Аудитори ІТКС, а також співробітники спецслужб, уповноважені щодо контролю та аналізу безпеки (внутрішні порушники). Адміністратори, обслуговуючий персонал та аудитори мають інформацію про вразливість ПЗ, помилки, а також програмні закладки на різних життєвих стадіях як ПЗ, так і самої ІТКС. Відомо про типи оброблюваної інформації, її цінність.

2.7 Модель загроз хмарної ІТКС

Модель загроз ІТКС представляє собою описове представлення характеристик загроз безпеки інформації, що обробляється в ІТКС. У процесі складання даної моделі необхідно ідентифікувати всі можливі джерела загроз ІБ та об'єкти, які можуть бути підвладні даним загрозам. Описати способи реалізації загроз та вразливості, що експлуатуються. Окрім цього, оцінюється масштаб втрат. Залежно від результатів побудови моделі загроз, виявляються слабкі сторони ІБ, що дає можливість вплинути на них і підвищити рівень захищеності.

Існує загроза фізичного характеру, за якої може спостерігатися порушення працездатності апаратного забезпечення віртуалізації хмарної платформи. Джерелом цієї загрози можуть бути як зовнішні порушники, так і порушники, що мають санкціонований доступ до устаткування. У першому випадку в більшості ситуацій існує певний намір, однак у другому можлива помилка співробітника. Реалізація можлива шляхом завдання фізичної шкоди компонентам у тому випадку, якщо механізми організаційно-технічного захисту інформації мають недоліки, пов'язані з можливістю здійснення збоїв та модифікації конфігурації.

Помилки персоналу при конфігурації гіпервізорів, віртуальних машин та інших апаратних засобів віртуалізації також несуть загрозу, при цьому завдати шкоди можуть лише порушники з правами системного адміністратора або адміністратора безпеки, відповідальні за експлуатацію та функціонування ІТКС. Наслідки подібної помилки можуть виражатися в порушенні ІБ гіпервізора та інших компонентів технології віртуалізації, що спричинить можливість НСД до ресурсів та порушення конфіденційності або цілісності інформації.

Помилки в роботі ПЗ щодо забезпечення технології віртуалізації ресурсів може бути небезпечною загрозою з погляду НСД до інфраструктури внаслідок використання відомих порушнику вразливостей. Зрештою, реалізація загрози призведе до несанкціонованого розкрадання, втрати, модифікації інформації

різного ступеня конфіденційності. Внутрішніми порушниками можуть виступати користувачі з повноваженнями адміністратора, персонал з обслуговування ПЗ або персонал з супроводу хмарної ІТКС, що захищається. Не виключено задіяння представників спецслужб.

Внутрішні порушники, що є користувачами хмарної ІТКС і використовують робоче місце або віддалений доступ для підключення до ресурсів, можуть зробити атаку переповнення буфера по відношенню до хмарної інфраструктури. Внаслідок цього можливий НСД до програмно-технічних засобів. Вразливістю для реалізації загрози є недоліки засобів захисту. Серед негативних наслідків – порушення доступності сервісів та вимог SLA.

Порушення масштабування та працездатності загалом хмарних віртуальних машин та інших обчислювальних ресурсів можливе внаслідок атак на інфраструктуру типу Dos, DDos, EDos. Джерелами цієї загрози виступають мотивовані зовнішні та внутрішні порушники з наявністю необхідних технічних знань для реалізації подібних атак. Вразливостями, що експлуатуються, можуть бути помилки в ПЗ, невірні параметри гіпервізора і недоліки в роботі СЗІ. Насамперед порушується доступність ресурсів хмарної ІТКС, внаслідок чого порушується й домовлений рівень надання послуг сервісів хмарної платформи.

Існує загроза отримання доступу до засобів управління інфраструктурою зовнішніми та внутрішніми порушниками внаслідок неправильного розмежування доступу та налаштування програмних засобів захисту. Крім зміни конфігурацій ресурсів, існує можливість отримання доступу до інформації різного ступеня конфіденційності, включаючи і персональні дані, і комерційну таємницю з метою подальшого її читання, зміни та крадіжки.

Оскільки інформація різного ступеня конфіденційності підлягає категоріюванню, порушення цього правила може стати наступною загрозою ІБ. Для різної інформації необхідно використовувати різні набори ресурсів для ізоляції, проте політика безпеки може містити недоліки щодо процесу розміщення інформації, що обробляється.

Наслідком може бути помилкове одержання доступу до конфіденційної інформації з рівнем захищеності вище, ніж цільова інформація, шляхом отримання доступу до ресурсу нижчого рівня захищеності.

Найнебезпечнішими загрозами можуть виступати мережеві атаки, реалізовані як зовнішніми, так і внутрішніми зловмисниками. До подібних атак можуть належати MitM, SQL-injection, XML-injection, XSS та інші [33], перелічені в щорічному рейтингу OWASP Top 10. Серед наслідків варто очікувати взлам ресурсу, отримання адміністративних повноважень та отримання доступу до конфіденційної інформації з метою її крадіжки або модифікації. Не виключені мережеві атаки між сегментами однієї ІТКС, що становить ще більшу загрозу безпеці.

Важливим компонентом хмарної ІТКС є зняття знімків образу віртуальної машини. Як правило, знімок містить дані, що зберігаються на віртуальній машині, включаючи певну конфіденційну інформацію користувача. Можливість увімкнення функції збереження знімків є у системних адміністраторів, а їх перегляд доступний і системному адміністратору, і постачальнику послуг. При цьому несанкціоноване зняття може стосуватися підсистеми зберігання, а також оперативної пам'яті серверів.

Інформація різного ступеня конфіденційності може бути розкрита, що спричинено недоліками СЗІ.

2.8 Метод розподілу рівнів захищеності ресурсів хмарної ІТКС

Для забезпечення ефективного рівня захищеності внаслідок аналізу ризиків можна запропонувати один із способів досягнення поставленого завдання, а саме квантифікування параметрів. У цьому контексті квантифікування передбачає зведення якісних параметрів захищеності до кількісних [34]. Також є необхідні умови, які обов'язково повинні бути реалізовані для забезпечення даного процесу. Серед них - побудова моделей порушника та загроз хмарної ІТКС, обчислення поточного рівня захищеності,

накопичення статистичних даних про ресурси інфраструктури та заключний етап зіставлення отриманих результатів із якісною шкалою оцінки ризику.

Накопичення статистичних даних про ресурси ІТКС можливе за допомогою експлуатації хмарної мережі, тобто регулярної взаємодії з аналізованою системою. Встановлені програмні засоби захисту інформації в цій інфраструктурі роблять можливим відстеження всіх дій на момент аналізу, які можуть бути пов'язані з порушенням політик безпеки, підозрілою мережевою активністю, спробами отримання несанкціонованого доступу та іншими забороненими діями. Особливо корисними можуть бути логування, налаштоване на віртуальних машинах, а також спеціальні сервіси хмарних платформ, що відстежують дії рівнів аудиту, отримання доступу до ресурсів, зчитування даних зі сховищ та зміни конфігурацій компонентів інфраструктури. За допомогою доступної інформації стає можливим виявлення та класифікація інцидентів, аналіз причини та оцінка впливу на кожен із ресурсів ІТКС.

В основі даного методу квантифікування використовується теорема Байєса, що має низку переваг для виконання поставленого завдання. Ця методика елементарної теорії ймовірності дозволяє визначити ймовірність настання події за умови наявності статистичних даних. Є можливість відстеження оновлень вхідних даних, виявлення залежності факторів інформаційної безпеки, а результати цього підходу аргументовані і можуть бути змінені у разі зміни структури відносин між значеннями завдання. Розглядається ступінь довіри до отриманих даних, гіпотез, також надаються їх ймовірності [34].

У контексті аналізу ризиків інформаційної безпеки ризик представляється як розподіл ймовірності, що належить безлічі результатів R [34]:

$$S \times D \to R, \tag{2.8}$$

де S – множина станів хмарної ІТКС;

D – множина можливих рішень.

Застосовуючи формулу Байєса, в контексті аналізу ризиків можна уявити її таким чином:

$$P(\theta|y) = \frac{P(y|\theta)P(\theta)}{P(y)} \quad (2.9)$$

$P(\theta)$ у цьому випадку є апріорним розподілом ймовірностей можливих значень θ, а $P(\theta|y)$ – апостеріорним розподілом, що залежить від умови, що дані y спостерігалися. θ є гіпотезою, а y – свідченням цієї гіпотези.

Специфіка аналізу ризиків хмарних обчислень полягає в обліку розподілу ресурсів. Іншими словами, у типовій хмарній інфраструктурі існує безліч вузлів різних типів. У такому випадку зіставляється оцінка *k*-го вузла мережі *n*-го типу, схильного до впливу *i*-тої загрози з використанням *j*-го каналу несанкціонованої передачі інформації.

Модель загроз для хмарних ІТКС може бути побудована з уточненнями за допомогою накопичення статистичних даних про схожі вузли з точки зору показників ІБ, проте для цього потрібне виконання деяких умов. Насамперед повинні застосовуватися аналогічні засоби захисту інформації, такі як антивірусне ПЗ, IDS, IPS та інші. Ресурси можна порівняти у межах використовуваної моделі надання послуг, що стосується і загроз по відношенню до цих ресурсів.

В цілому алгоритм створення моделі загроз для подальшого використання відповідно до методу квантифікування може складатися з наступних етапів [34]:

- Збір даних про загрози та вплив загроз;
- Отримання даних про порушення таких властивостей як цілісність, доступність та конфіденційність реалізацією загрози;
- Розрахунок апостеріорної ймовірності гіпотез при забезпеченні перелічених вище властивостей;
- Розрахунок у разі порушення показників захищеності;
- Розподіл ресурсів за рівнем захищеності;
- Формулювання висновків щодо розрахунків.

Результатом стане можливість порівняння рівня інформаційної безпеки з цільовим показником, а також отримання кількісної оцінки рівня захищеності, що надає перевагу у подальшому процесі мінімізації ризиків.

Ресурси можуть бути розділені за трьома категоріями з точки зору захищеності:

- Категорія А – захищені системи;
- Категорія В – системи з високим рівнем захищеності;
- Категорія С – системи з низьким рівнем захищеності.

Далі визначаються гіпотези щодо належності ресурсу до однієї з цих категорій - θ_1, θ_2, и θ_3. Апріорні ймовірності даних гіпотез - $P(\theta_1)$, $P(\theta_2)$ і $P(\theta_3)$ відповідно.

Додавши до розрахунків дані про показники конфіденційності (С), цілісності (I) та доступності (А), можна визначити їх умовні ймовірності, оскільки вплив загроз на ресурси хмарної ІТКС забезпечувався в різній кількості випадків.

Показники забезпечення конфіденційності інформації з урахуванням розподілу ресурсів за категоріями безпеки – $P(C|\theta_1)$, $P(C|\theta_2)$, $P(C|\theta_3)$. Для першої групи захищеності ресурсів забезпечення цілісності матиме вигляд $P(I|\theta_1)$, другої та третьої груп - $P(I|\theta_2)$, $P(I|\theta_3)$ відповідно. Аналогічно і з властивістю доступності показники захищеності ресурсів хмарної ІТКС при впливі загрози Y: $P(A|\theta_1)$, $P(A|\theta_2)$, $P(A|\theta_3)$ [34].

Апостеріорні ймовірності гіпотез для одного свідчення на прикладі показника конфіденційності:

$$P(\theta_1|C) = \frac{P(C|\theta_1)P(\theta_1)}{\sum_{i=1}^{3} P(C|\theta_i)P(\theta_i)}$$

$$P(\theta_2|C) = \frac{P(C|\theta_2)P(\theta_2)}{\sum_{i=1}^{3} P(C|\theta_i)P(\theta_i)} \qquad (2.10)$$

$$P(\theta_3|C) = \frac{P(C|\theta_3)P(\theta_3)}{\sum_{i=1}^{3} P(C|\theta_i)P(\theta_i)}$$

Якщо в результаті відомий факт недотримання конфіденційності, цілісності та доступності після впливу загрози на ресурс, розглядається протилежна подія:

$$P(\overline{C,I,A}|\theta_i) = 1 - P(C,I,A|\theta_i) \quad (2.11)$$

У разі наявності одразу трьох показників, використовується наступна формула:

$$P(\theta_i|C,I,A) = \frac{P(C|\theta_i)P(I|\theta_i)P(A|\theta_i)P(\theta_i)}{\sum_{i=1}^{3} P(C|\theta_i)P(I|\theta_i)P(A|\theta_i)P(\theta_i)} \quad (2.12)$$

При цьому ймовірності гіпотез або підвищуватимуться, або знижуватимуться при їх підтвердженні або спростуванні.

В результаті знайдені ймовірності приналежності ресурсу до однієї з трьох груп матимуть вигляд $P(\theta_1|C,I,A)$, $P(\theta_2|C,I,A)$, $P(\theta_3|C,I,A)$.

Надалі цей розрахунок допомагає проводити оцінку рівня забезпечення безпеки і рівня ресурсів, і загалом хмарної інфраструктури із запланованими показниками ІБ, а також стосовно конкретної загрози. Процес мінімізації ризиків буде побудований більш ефективно у зв'язку з точнішими результатами аналізу ризиків даним методом, а розподіл ресурсів за рівнями захищеності дозволить застосовувати СЗІ до певної групи, де це необхідно з міркувань захисту.

2.9 Лінійне програмування

Для вирішення задачі мінімізації ризиків задіяний метод лінійного програмування, тобто метод із строго лінійними функціями та обмеженнями. Завдання, які вирішуються в такий спосіб, носять екстремальний характер. Частими ситуаціями застосування лінійного програмування є виробничо-господарські дослідження з метою знаходження оптимального використання ресурсів. Метод досить вивчений для його застосування, що є безумовною

перевагою у використанні. Нелінійні завдання можуть бути приведені до лінійного виду для подальшого вирішення.

Основними поняттями в лінійному програмуванні є набір змінних та цільова функція. Змінні представлені як $x = (x_1, x_2, \dots x_n)$, їх функція має вигляд $f(x) = f(x_1, x_2, \dots x_n)$. У процесі вирішення необхідно знайти естремум цієї цільової функції за належністю змінних до певної області - $G \subset R^n$. Область може відрізнятися залежно від розділу математичного програмування, а саме може відноситися до квадратичного, опуклого і цілісного програмування, однак лінійне програмування характеризується тим, що цільова функція є лінійною по відношенню до змінних, а область значень визначається системою лінійних нерівностей або рівностей. При цьому існує вимога цілісності та невід'ємності величин, що обумовлено фізичним змістом.

Розв'язання задач оптимізації реалізовано за допомогою методу гілок і меж та методом Гоморі [34]. У першому випадку виконується перебір всіх значень з можливістю відкинути ті, які є оптимальними [35]. Метод Гоморі застосовується в задачах з цілими значеннями, де знаходження такого значення є критерієм оцінки розв’язання завдання [36].

2.10 Методика оптимізації ризиків хмарної ІТКС

У хмарній ІТКС може оброблятись інформація різного ступеня секретності. Класифікація таких типів інформації необхідна для знаходження необхідного рівня забезпечення конфіденційності, цілісності та доступності, що, у свою чергу, означає знаходження оптимальних ресурсів хмарної інфраструктури для обробки та зберігання інформації.

Існують наступні типи конфіденційності інформації [34]:

- Відкрита інформація, доступ до якої не контролюється, те саме стосується і використання та знищення.

- Конфіденційна інформація, доступ до якої отримують лише авторизовані особи відповідно до політики безпеки та розмежування доступу.
- Критична інформація, яка за будь-яких обставин не повинна бути розкрита, інакше подібний інцидент загрожує репутаційними втратами хмарних провайдерів.

Кожному суб'єкту присвоюється рівень доступу до необхідного ступеня конфіденційності інформації. При цьому розмежування доступу виконується з наступним правилом: якщо рівень захищеності ресурсу нижче ступеня конфіденційності інформації, що запитується, йому буде відмовлено в обробці даних цього рівня конфіденційності. Усі права доступу встановлюються з урахуванням матриці доступу.

Описане правило можна подати у такому вигляді:

$$s \leq k, \tag{2.13}$$

де s – ступінь конфіденційності інформації;

k – рівень захищеності ресурсу.

Розрахунок ризику проводиться за формулою комбінації ймовірності події та її наслідків:

$$R = \sum_l P_l C_l^y, \tag{2.14}$$

де P_l – ймовірність успішної реалізації i-тої загрози;

C_l^y – оцінка вартості збитків при успішній реалізації l-тої загрози;

l – 1…n – кількість ймовірних загроз.

Для вимірювання рівня ризиків складається матриця ризиків, у рядках якої розташовані ризикові події, а в стовпцях – їх ймовірності та наслідки.

Побудована матриця з урахуванням однієї загрози матиме наступний вигляд:

$$\begin{bmatrix} r_{11} & \cdots & r_{1s} \\ \vdots & \ddots & \vdots \\ r_{\lambda 1} & \cdots & r_{\lambda s} \end{bmatrix},$$

де $r_{\lambda s}$ – ризик ІБ у разі впливу загрози.

Отримані ризики оцінюються за шкалою нормативно-правових документів, а також можуть бути поділені за декількома рівнями:

- Високий рівень. Вимагає якнайшвидшого реагування на ризик та прийняття контрзаходів проти прояву негативного впливу.
- Середній рівень. Контрзаходи можуть бути створені як частина всього плану зниження ризиків з реалізацією в певні строки, ризики середнього ступеню небезпеки не вимагають миттєвого вирішення.
- Низький рівень. Необхідно визначити наскільки потреба мінімізації ризиків даної групи є актуальною. У разі відсутності такої необхідності, слід забезпечити спостереження за ризиками низького рівня небезпеки.

Щоб оптимізувати використання ресурсів, необхідно визначити кількість одиниць ресурсів певних рівнів захищеності, які можуть використовуватися в хмарній інфраструктурі для досягнення мінімального рівня ризику. З урахуванням наведеної матриці ризиків та правила розмежування доступу можна надати цільову функцію оптимізаційної задачі:

$$x_1 r_{11} + x_2 r_{21} + x_2 r_{22} + x_3 x_{31} + x_3 x_{32} + x_3 x_{33} + .. + x_m x_{mm} \rightarrow min \qquad (2.15)$$

При цьому забезпечення виконання вимог користувачів, пов'язаних з обробкою та зберіганням конфіденційної інформації, має бути виконане відповідно до SLA.

Рішення щодо використання оптимальних ресурсів має бути обґрунтовано економічно.

В результаті за допомогою даного методу оптимізації ризиків на основі лінійного програмування вирішуються завдання з ідентифікації вразливостей та загроз хмарної ІТКС, класифікується оброблювана інформація за ступенем конфіденційності, проводиться кількісна оцінка ймовірності реалізації загроз та наслідків разом із розподілом ресурсів за рівнем захищеності залежно від виявлених загроз.

2.11 Практичне застосування методики розподілу рівнів захищеності та оптимізації ризиків

Для демонстрації роботи запропонованого методу необхідно виконати розрахунок ймовірностей, оцінити ризики та провести їх оптимізацію. Оцінити отримані результати можна порівнявши їх із результатами методики A Figure of Merit Model. Дана методика застосовується на всіх етапах життєвого циклу хмарної ІТКС та впровадження засобів захисту інформації, критеріями оцінки яких є простота використання, продуктивність та вартість [37]. Вартість включає витрати на встановлення та обслуговування хмарних обчислювальних ресурсів. Обрані засоби захисту при цьому не повинні ускладнювати роботу з хмарною інфраструктурою. Оцінка може проводитись за загальними чи окремими показниками якості роботи.

Хмарні ІТКС або їх компоненти можуть бути позначені як $A_1 A_2 \dots A_n$. Для визначення математичної функції необхідно визначити показник A_i ІТКС з урахуванням її ресурсів та управлінням безпекою на них.

Разом розрахункова формула для визначення показника якості матиме вигляд [34]:

$$F(A_i) = W_1 s(A_i) + W_2 e(A_i) + W_3 p(A_i) + W_4 c(A_i), \qquad (2.16)$$

де $s(A_i)$ – показник безпеки A_i;

$e(A_i)$ – показник легкості використання A_i;

$p(A_i)$ – показник продуктивності A_i;

$c(A_i)$ – показник вартості A_i.

W_i є коефіцієнтом кожного фактору, що означає його рівень важливості щодо інших факторів.

В даному випадку будуть використані показники безпеки $s(A_i)$ та вартості $c(A_i)$. Перший показник є сумою метрик найефективніших засобів захисту інформації та частин суми інших, не перевищуючи значення 1. Число

ресурсів складових ІТКС – n, рівень захищеності n-го ресурсу - S_i. Подібний розрахунок можливий у разі застосування множини засобів захисту інформації до одного ресурсу ІТКС.

Найбільш ефективні ЗЗІ - s_1, s_2, s_3, з урахуванням цього розрахунок показника безпеки буде наступним:

$$s = min\{max(s_1 s_2 s_3) + 20\%[\sum s_i - max(s_1 s_2 s_3)], 1.0\} \quad (2.17)$$

Зазначені 20% не є принциповими і можуть бути замінені на необхідну розмірність.

Захищеність хмарної інфраструктури загалом є сумою показників S_i, які визначаються експертами та можуть бути призначені для різних типів ЗЗІ. Це буде мати такий вигляд:

$$S(A_i) = \sum S_i \quad (2.18)$$

Наступний показник означає вартість володіння, експлуатації та обслуговування ЗЗІ обчислювальних ресурсів та може бути знайдений за допомогою цієї формули:

$$C(A_i) = \sum C_j, \quad (2.19)$$

де $j = 1,2, \ldots n$ – кількість обчислювальних ресурсів.

Для знаходження сумарної вартості необхідно провести розрахунок витрат на встановлення СЗІ систем віртуалізації, навчання персоналу роботі та подальше обслуговування ІТКС із коефіцієнтами витрат даних категорій:

$$C_j = (W_{c1} C_1 + W_{c2} C_2 + W_{c3} C_3 / W_{c1} + W_{c2} + W_{c3}) \quad (2.20)$$

де $C_1 C_2 C_3$ – витрати на перераховані категорії;

$W_{c1} W_{c2} W_{c3}$ – коефіцієнти витрат.

Як приклад інфраструктури для практичного застосування використовуваного методу була обрана хмарна ІТКС CLAVIRE (Cloud

Applications Virtual Environment). Це багатопрофільне інструментально-технологічне середовище другого покоління, яке реалізує перспективну модель хмарних обчислень Application as a Service [38].

Реалізація SaaS, AaaS відбувається у публічній хмарі, створюваної з урахуванням Grid.

Серед функціональності даного рішення можливість динамічного моніторингу системи, запуску додатків та розподілу навантаження на серверах, тобто в цілому управління певним набором ресурсів. Ресурси розподіленого середовища підлягають квотуванню та тарифікації за використання, що відображається в білінгу. Доступ до обчислювальних ресурсів уніфікований на основі інтерфейсів відомих програмно-апаратних архітектур. З погляду прав доступу до ресурсів середовища регулюються багаторівневою політикою доступу, при цьому права адміністраторів є диференційованими. У разі необхідності скасування змін існує функція їх відкату, а щоб уникнути інцидентів втрати даних, може бути налаштовано резервування у віддалене сховище, яке також є компонентом даного розподіленого середовища.

Для розгортання компонентів хмарної ІТКС сумісними операційними системами можуть бути [38]:

- Microsoft Windows Server
- Linux
- Необхідні залежності для встановлення та коректної роботи:
- Silverlight
- Mono Framework
- .NET
- Веб-сервер з підтримкою ASP .NET WebServices, WCF, Silverlight
- Інструмент віддаленого розгортання з технологією WebDeploy.

Можна припустити, що до складу хмарної ІТКС входять такі ресурси:

Таблиця 2.1 – Ресурси хмарної ІТКС

Ресурс	Кількість
Користувачі	200
Веб-інтерфейс	2
Ресурси ЦОД	10
Грід-інфраструктура	100
Хмарна інфраструктура	50
Сховище даних	6
Грід-гейт	1
Сервер авторизації	1

Наступним етапом є оцінка ймовірності інциденту ІБ, що передує розрахунку захищеності ресурсів за допомогою методу квантифікування. Для отримання ймовірностей необхідно врахувати статистичні дані відкритих інтернет ресурсів, таких як Open Security Foundation, Data Loss Statics та Cloud Incidents Statics [34]. Наприклад, наступна таблиця містить дані за попередні роки.

Таблиця 2.2 – Статистика ризиків ІТКС

Ризик	Ймовірність реалізації
Втрата/виток даних	0,265
Експлуатація ресурсів порушником	0,194
Використання вразливих програмних інтерфейсів	0,142
Взлам акаунтів	0,123

Продовження таблиці 2.2

Інші загрози	0,084
Вразливості віртуалізації	0,065

Маючи необхідні дані, знайти результуючу ймовірність загроз можна, використовуючи таку формулу [34]:

$$P_s = 1 - \overline{P} = 1 - (1 - P_1)(1 - P_2)(1 - P_n) = 0{,}618 \quad (2.21)$$

Приблизні коефіцієнти стійкості ЗЗІ, отримані емпіричним методом методики A Figure of Merit та необхідні для подальших розрахунків:

1. IDS/IPS – 0,45
2. DLP – 0,4
3. Антивірусне ПЗ – 0,3
4. Токен – 0,3
5. Цифровий сертифікат – 0,2
6. Пароль – 0,1

Однак слід пам'ятати, що отримані коефіцієнти є суб'єктивними і можуть бути недостовірними в деяких випадках.

Наступним кроком є розрахунок рівня захищеності ресурсів, щоб надалі розділити всі наявні ресурси за групами ступеня захищеності - A, B і C. Визначення даного значення в даному випадку ґрунтується на співвідношення вартості оброблюваної інформації до сумарного неприйнятного збитку.

Для початку необхідно визначити вартість ЗЗІ ресурсів, призначених для обробки відкритої, конфіденційної та критичної інформації [34]:

$$C_{\Sigma} = \sum_S (C_1^3 + C_2^3 + C_3^3), \quad (2.22)$$

де C_1^3 – вартість ЗЗІ ресурсу для обробки відкритої інформації;

C_2^3 – вартість ЗЗІ ресурсу для обробки конфіденційної інформації;

C_3^3 – вартість ЗЗІ ресурсу для обробки критичної інформації;

S – кількість ресурсів.

Отриманий в результат показник вартості використовується у безпосередньому розрахунку рівня захищеності самого компонента ІТКС:

$$\alpha = 1 - \overline{R} = 1 - \frac{C_S}{C_\Sigma} \times P_S,$$

(2.23)

де C_S – вартість інформації, що захищається;

C_Σ - вартість всіх ЗЗІ;

P_S – результуюча ймовірність.

У свою чергу вартість всіх ЗЗІ знаходиться із суми значень вартості ЗЗІ ресурсів для обробки трьох типів інформації таким чином:

$$C_\Sigma = \sum_S (C_1^3 + C_2^3 + C_3^3) \qquad (2.24)$$

Знаходження значення захищеності $F(A_\iota)$, s з використанням методики A Figure of Merit можливе за допомогою перерахованих вище формул.

Після проведених розрахунків отримано такі результати, що подані у таблиці.

Таблиця 2.3 – Результати розрахунку значення захищеності

Ресурс	A Figure of Merit	Запропонований метод
Користувачі	37%	43%
Веб-інтерфейс	51%	72%
Ресурси ЦОД	58%	72%
Грід-інфраструктура	64%	58%
Хмарна інфраструктура	58%	52%
Сховище даних	59%	61%
Грід-гейт	59%	81%
Сервер-авторизації	58%	86%

На основі цієї таблиці можна розподілити всі перелічені ресурси за трьома групами захищеності. Як згадувалося раніше, це групи: А – захищені ресурси, В – ресурси високого рівня захищеності від потенційних атак, С – ресурси з слабким захистом.

Відомо, що ЗЗІ забезпечує три властивості інформації: конфіденційність (С), цілісність (І) та доступність (А). У цьому випадку це кортеж можливих показників захищеності хмарної інфраструктури.

Для аналізу реального прикладу ІТКС необхідно точно знати ступінь забезпечення цих трьох критеріїв, проте для демонстрації практичного застосування запропонованого в даній роботі методу можна визначити такі ступені.

Таблиця 2.4 – Показники забезпечення властивостей інформації

Група ресурсу	Конфіденційність	Цілісність	Доступність
С	60%	70%	90%
В	80%	50%	80%
А	20%	12%	30%

Варто наголосити, що методика A Figure of Merit не дає можливості визначити кількісні значення рівня захищеності.

На основі таблиці вище, можна скласти таблицю умовного входження ресурсу до групи певного ступеня захищеності.

Таблиця 2.5 – Ймовірності входження ресурсу до певної групи

Конфіденційність		Цілісність		Доступність	
$P(C\|\theta_1)$	0,6	$P(I\|\theta_1)$	0,7	$P(A\|\theta_1)$	0,9
$P(C\|\theta_2)$	0,8	$P(I\|\theta_2)$	0,5	$P(A\|\theta_2)$	0,8
$P(C\|\theta_3)$	0,2	$P(I\|\theta_3)$	0,12	$P(A\|\theta_3)$	0,2

При цьому апріорні ймовірності:

- $P(\theta_1) = 0{,}125$
- $P(\theta_2) = 0{,}375$
- $P(\theta_3) = 0{,}5$

У разі одночасного отримання показників конфіденційності та цілісності, ймовірність розраховуватиметься наступним чином:

$$P(\theta_i|C,I) = \frac{P(C|\theta_i)P(I|\theta_i)P(\theta_i)}{\sum_{i=1}^{3} P(C|\theta_i)P(I|\theta_i)P(\theta_i)}$$

(2.25)

Отримані результати:

$P(\theta_1|C,I) = 0{,}25$

$P(\theta_2|C,I) = 0{,}71$

$P(\theta_3|C,I) = 0{,}06$

Найбільше значення спостерігається у другому випадку, отже, це свідчить про належність ресурсу до групи В.

Тепер, після визначення групи захищеності, можна провести оптимізацію ризиків ІТКС методом лінійного програмування. Цей метод знову можна порівняти з методом A Figure of Merit, однак другий відрізняється неможливістю оптимізації ризиків ІБ за його допомогою, але пропонується до використання для розрахунку економічної ефективності [34].

Наступна таблиця надає вихідні дані для оптимізації ризиків.

Таблиця 2.6 – Вхідні дані для задачі оптимізації ресурсів

Критерій	Ресурс групи А	Ресурс групи В	Ресурс групи С
Витрати на утримання (C_λ^3)	1	3	8
Вартість обробки інформації (C_s^0)	2	5	10
Масштабування ресурсів до кількості (I)	200	80	40

Значення ймовірності (P_t)	1	0,5	0,1

Продовження таблиці 2.6

Значення збитків (C_t^y)	2	5	10
Кількість оптимізованих заявок (I_n)	200	280	40

Витрати на утримання одиниці ресурсу залежить від рівня його захищеності та ступеня конфіденційності інформації.

Масштабування передбачає забезпечення необхідною кількістю одиниць необхідних ресурсів для обробки інформації певного ступеня конфіденційності.

Значення ймовірності реалізації загрози залежить від рівня захищеності ресурсу, але не ступеня конфіденційності інформації, що обробляється.

Отримавши значення ймовірностей та значення збитків, можна створити матрицю ризиків r_{ij}.

Таблиця 2.7 – Результати матриці на основі значень ймовірностей та збитків

	Відкрита інформація	Конфіденційна інформація	Критична інформація
Ресурс А	2	5	10
Ресурс В	5	2,5	5
Ресурс С	0,2	0,5	1

Кількість оптимізованих заявок означає розподіл ресурсів та їх виділення під тип оброблюваної інформації після проведених розрахунків, і в даному випадку для ресурсів групи А – 200 заявок (відкрита інформація), групи В – 280 (відкрита інформація та конфіденційна), групи С – 40 (критична інформація). Усього 320 можливих заявок на обробку інформації.

За допомогою методу Гоморі лінійного програмування результат буде наступним. Кількість ресурсів рівня захищеності А: x1 = 40; кількість ресурсів рівня захищеності В: x2 = 180; кількість ресурсів рівня С: x3 = 100.

Таким чином, слабо захищені ресурси можуть бути зменшені в кількості, що може захистити оброблювану інформацію від потенційних загроз з більшою ймовірністю.

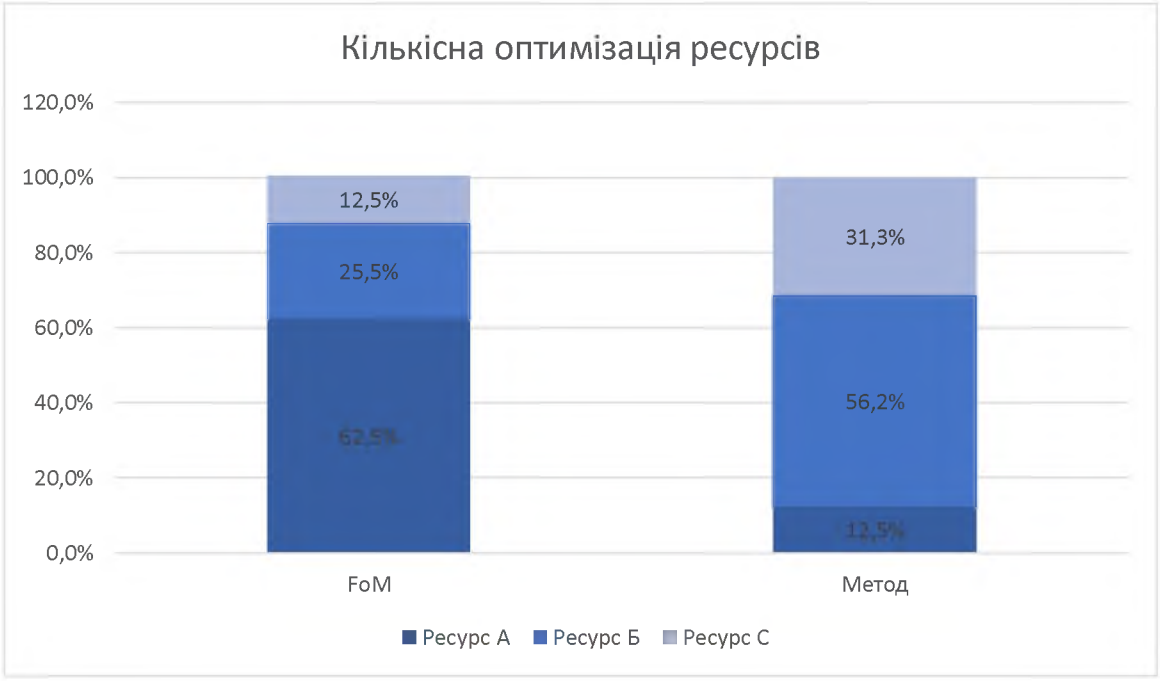

Рисунок 2.5 – Кількісна оптимізація ресурсів хмарної ІТКС

2.12 Висновки до розділу 2

У другому розділі було розглянуто поняття ризику, його невизначеності та чутливості. Існуючі кількісні, якісні, та напівкількісні методи аналізу ризиків були проаналізовані для визначення їх слабких та сильних сторін. Побудована модель загроз хмарної ІТКС та модель порушника. На основі проведеного аналізу було визначено складність використання існуючих методик для оцінки ризику в хмарних ІТКС. Для вирішення проблеми запропоновано методику розподілу рівнів захищеності хмарних сервісів, що побудована з використанням формули Байєса з урахуванням апріорної та апостеріорної ймовірності приналежності ресурсу до одного з трьох рівнів захищеності – A, B та C. Оптимізація ризиків настання інциденту, або реалізації загрози щодо ресурсу, проведена за рахунок використання лінійного програмування – методів Гоморі та методу меж і гілок. Для демонстрації результатів роботи запропонованої

методики було проведено розрахунки та приведена порівняльна характеристика з методом A Figure of Merit.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на створення методики розподілу рівнів захищеності хмарних ресурсів та оптимізації ризиків

Для визначення показників економічної ефективності розробки методики оптимізації ризиків необхідно провести розрахунок витрат на розробку методики(експлуатаційні та капітальні витрати), можливих збитків від атаки(величина збитків) та загальний ефект від впровадження системи ІБ.

У результаті з'являється можливість проаналізувати доцільність запропонованих рішень інформаційної безпеки. Очікується, що впроваджені рішення є доцільними та економічно ефективними для підприємства.

3.2 Визначення витрат на розробку методики

- Розрахунок капітальних(фіксованих) витрат

Капітальні витрати включають вартість розробки безпосередньо методики, вартість покупки необхідного ліцензійного ПЗ або апаратного забезпечення як основного, так і додаткового. Окрім цього, до цієї категорії входять ще й інтеграція в систему та витрати на навчання технічних спеціалістів і обслуговуючого персоналу.

За наступною формулою визначається трудомісткість розробки методики:

$$t = t_{\text{тз}} + t_{\text{в}} + t_{a} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{ годин} \qquad (3.1)$$

де $t_{\text{тз}}$ - тривалість складання технічного завдання на розробку методики;

$t_{\text{в}}$ - тривалість розробки концепції безпеки інформації у організації;

$t_{\text{а}}$ - тривалість процесу існуючих методик;

$t_{\text{озб}}$ - тривалість визначення вимог до розробки;

$t_{\text{вз}}$ - тривалість вибору основних рішень, використаних для розрахунку ризиків;

$t_{овр}$ - тривалість збору статистичних даних;

$t_д$ - тривалість документального оформлення;

Згідно з підрахунками та проведеною роботою, було витрачено 6 годин на складання технічного завдання для розробки комплексної системи захисту інформації, а тривалість розробки концепції безпеки інформації саме в організації зайняла також 6 годин. При цьому 4 години було витрачено на аналіз ризиків, 5 годин на визначення вимог до методів та засобів захисту та також 5 годин на документування. Організація відновлювальних робіт, також забезпечення безперервного функціонування організації потребували 5 годин.

Отримуємо наступний результат:

$$t = 6 + 6 + 10 + 4 + 5 + 7 + 5 = 43 \text{ годин}$$

Розрахунок витрат на створення методики $К_{рп}$ можна виконати за наступною формулою.

$$К_{рп} = З_{зп} + З_{мч}, \qquad (3.2)$$

$З_{зп}$ та $З_{мч}$ в даному випадку визначають заробітну плату спеціаліста з інформаційної безпеки та вартість машинного часу, що необхідний для розробки, відповідно. Розраховуються ці значення за наступними формулами.

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

де $З_{іб}$ - заробітна плата спеціаліста з інформаційної безпеки, грн/година;

$$З_{зп} = 43 \cdot 38 = 1634 \text{ грн}$$

$$З_{мч} = t \cdot С_{мч}, \text{ грн} \qquad (3.4)$$

де $С_{мч}$ - вартість машинного часу;

Для розрахунку вартості машинного часу використовується формула, що потребує визначення тарифу на електричну енергію, встановлену потужність, тощо.

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{ грн} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт*година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації ПК, частки одиниці;

$F_р$ – річний фонд робочого часу, 1920 для 8-годинного робочого дня;

$К_{лпз}$ – вартість ліцензійного ПЗ, грн;

$Н_{апз}$ – річна норма амортизації на ліцензійне ПЗ, частки одиниці;

Для техніки, що використовується в середньому, встановлена потужність 0,4, а тариф дорівнює 1,68 кВт на годину.

$$С_{мч} = 0{,}4 \cdot 3 \cdot 1{,}68 + \frac{12000 \cdot 0{,}6}{1920 \cdot 2} + \frac{5000 \cdot 0{,}6}{1920 \cdot 2} = 3{,}79 \text{ грн} \quad (3.6)$$

Тобто, година роботи машинного часу становить 3,79 грн.

$$З_{мч} = 43 \cdot 3{,}79 = 163$$

$$К_{рп} = 1634 + 163 = 1797$$

Далі необхідно розрахувати капітальні витрати на розробку методики за наступною формулою:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н, \quad (3.7)$$

де $К_{пр}$ – вартість розробки проекту та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного та додаткового програмного забезпечення, тис. грн;

$К_{рп}$ – вартість розробки методики безпосередньо, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців та обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на тестування працездатності розробленої методики, тис. грн;

Для даного випадку створення методики відсутні вартість закупівлі апаратного забезпечення та допоміжних матеріалів. Згідно з цими обставинами, всі капітальні витрати становлять наступну суму:

$$К = 20000 + 2000 + 5000 + 2000 + 1000 = 30000 \text{ грн.} \quad (3.8)$$

- Розрахунок експлуатаційних(поточних) витрат

Експлуатаційні витрати розраховуються як річні.

$$С = С_{ел} + С_{а} + С_{єв} + С_{з} + С_{тос} + С_{н} + С_{о}, \text{ грн} \quad (3.9)$$

де $С_{ел}$ – вартість електроенергії, грн;

$С_{а}$ – річний фонд амортизаційних відрахувань;

$С_{з}$ – річний фонд заробітної плати технічно-інженерного персоналу;

$С_{тос}$ – витрати на технічне та організаційне адміністрування;

$С_{н}$ – витрати на навчання адміністративного персоналу;

$С_{о}$ – витрати на залучення сторонніх організацій;

Вартість електроенергії, що використовується апаратним забезпеченням інформаційної безпеки протягом року:

$$С_{ел} = Р \cdot F_{р} \cdot Ц_{е} = 0{,}4 \cdot 1{,}68 \cdot 1920 \cdot 3 = 3870{,}72 \text{ грн} \quad (3.10)$$

Витрати на технічне і організаційне адміністрування та сервіс систем інформаційної безпеки, що становлять 1-3% від вартості капітальних витрат:

$$С_{тос} = К \cdot 0,02 = 30000 \cdot 0,02 = 600 \text{ грн} \quad (3.11)$$

Повні експлуатаційні щорічні витрати, враховуючи можливу додаткову заробітну плату обслуговуючого персоналу, витрати на адміністрування та сервіс, вартість електроенергії та щорічні витрати на навчання працівників підприємства:

$$С = С_{ел} + С_{тос} + С_{о} + С_{з} = 3870,72 + 5000 + 25000 + 25000 = 58871 \text{ грн}$$

Під витратами на залучення сторонніх організацій мається на увазі навчання працівників підприємствам на зовнішніх тренінгах для загальної орієнтації в сфері ІБ. Навчання проводиться раз на рік та коштує 1000 грн.

Заробітна плата обслуговуючого персоналу складає 10000 грн з урахування єдиного соціального внеску та річної заробітної плати, оскільки вимоги до повного робочого дня та тижня немає.

3.3 Оцінка можливого збитку від атаки на вузол чи сегмент корпоративної мережі

Необхідні дані для розрахунку упущеної вигоди від простою атакованого вузла або сегменту хмарної ІТКС та інших значень, що описуються у кожній відповідній формулі, представлені нижче:

$З_о = 10000$ грн

$З_с = 4000$ грн

$Ч_с = 25$ людини

$Ч_о = 2$ людини

$t_{ви} = 4$ години

$t_в = 10$ години

$t_п = 5$ годин

$О = 250000$ грн

$П_{зч} = 0$ грн

$I = 50$ штук

$N = 1$ раз

Визначення упущеної вигоди:

$$U = П_п + П_в + V, \quad (3.12)$$

де $П_п$ – оплачувані витрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн;

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

Оплачувані витрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі:

$$П_п = \frac{\sum З_с}{F} \cdot t_п, \quad (3.13)$$

$$П_п = \frac{100000}{176} \cdot 5 = 2841$$

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

F – місячний фонд робочого часу(176 год из 40-годинному робочому тижні),

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

Вартість відновлення працездатності вузла або сегмента корпоративної мережі:

$$П_в = П_{ви} + П_{пв} + З_ч, \quad (3.14)$$

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

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

$З_ч$ – вартість заміни устаткування або запасних частин, грн;

Витрати на повторне введення інформації працівниками:

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви}, \quad (3.15)$$

$$П_{ви} = \frac{100000}{176} \cdot 4 = 2273,$$

де $t_{ви}$ – час повторного введення інформації співробітниками атакованого вузла чи сегмента корпоративної мережі, грн;

Витрати на повне відновлення вузла або сегмента корпоративної мережі:

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в, \quad (3.16)$$

$$П_{пв} = \frac{20000}{176} \cdot 10 = 1136$$

Де $З_о$ – заробітна плата обслуговуючого персоналу, грн на місяць;

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

Після отриманих складових можна визначити відновлення працездатності вузла:

$$П_в = 2273 + 1136 + 0 = 3409$$

Витрати від зниження очікуваного обсягу продажів за час простою:

$$V = \frac{О}{F_r} \cdot (t_п + t_{ви} + t_в), \quad (3.17)$$

$$V = \frac{250000}{2080} \cdot (5 + 10 + 4) = 2284,$$

де $F_г$ – річний фонд часу роботи організації(2080 годин)

Підсумкова оцінка збитків як упущеної вигоди від простою та неможливості роботи:

$$U = 2841 + 3409 + 2284 = 8534$$

Для повного розрахунку необхідно упущену вигоду від простою помножити на кількість атак за рік та вузлів, що постраждають та будуть простоювати внаслідок атаки:

$$B = \sum i \sum n \cdot U, \quad (3.18)$$

$$B = 1 \cdot 50 \cdot 8534 = 426700$$

3.4 Загальний ефект від впровадження методики аналізу та оптимізації ризиків

Визначається за формулою:

$$E = B \cdot R - C, \quad (3.19)$$

$$E = 426700 \cdot 0{,}2 - 58871 = 26469$$

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

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі;

C – щорічні витрати на експлуатацію, тис грн;

3.5 Визначення та аналіз показників економічної ефективності розробленої методики

Для розрахунку цього пункту використовується коефіцієнт ROSI, що означає коефіцієнт повернення інвестицій. У контексті інформаційної безпеки мається на увазі більше збереження коштів та уникнення збитків у разі впровадження розробленої методики аналізу та оптимізації ризиків та наскільки це є ефективним.

$$ROSI = \frac{E}{K}, \quad (3.20)$$

де Е – загальний ефект від впровадження методики, тис. грн;

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

$$ROSI = \frac{26469}{30000} = 0{,}88$$

Термін окупності розробленої та впровадженої методики можна визначити за наступною формулою:

$$T_o = \frac{K}{E} = \frac{1}{ROSI}, \quad (3.21)$$

$$T_o = \frac{K}{E} = \frac{1}{0{,}88} = 1{,}2 \text{ роки}$$

Отже, саме за таких час всі витрати на покращення інформаційної безпеки можуть окупитись.

3.6 Висновки до розділу

В даному розділі бути проведені розрахунки щодо доцільності впровадження розробленого рішення. Для визначення цього факту бути використані такі показники як експлуатаційні щорічні витрати – 25594,82 тисяч грн, капітальні витрати – 10205,23 грн та ефективність після впровадження – 9735,58 тисяч грн. Розмір збитків становить 98140 тисяч грн.

Після розрахунків можна зробити висновок, що розробка методики була доцільною тому, що витрати на забезпечення безпеки інформації виявилися меншими, ніж розмір збитків внаслідок атаки та витрати на поновлення функціонування корпоративної мережі, а також роботи працівників.

Завдяки розрахунку коефіцієнту повернення інвестицій визначено час повернення коштів, що бути витрачені на весь процес розробки та впровадження

методики аналізу ризиків та оптимізації. Орієнтований час – 1,2 рік, що є досить позитивним результатом.

ВИСНОВКИ

У кваліфікаційній роботі містяться 3 розділи:

1. Стан питання. Постановка задачі
2. Спеціальна частина
3. Економічна частина

Під час виконання кожного з розділу були проведені наступні етапи:

- Огляд хмарних обчислювальних технологій та моделей розгортання хмарних сервісів. Огляд хмарних провайдерів. Визначення переваг та недоліків використання як хмарних ІТКС, так і фізичної інфраструктури.
- Аналіз нормативно-правової бази та стандартів в сфері забезпечення інформаційної безпеки, в тому числі і в хмарних ІТКС.
- Визначення поняття ризиків, їх невизначеності та чутливості. Огляд існуючих методик аналізу ризиків, визначення складності оцінки ризиків в хмарних ІТКС існуючими методами.
- Побудова моделі порушників та моделі загроз.
- Огляд методики розподілу рівнів захищеності ресурсів хмарної ІТКС з використанням підходу Байєса.
- Огляд методики оптимізації ризиків в хмарних ІТКС з використанням лінійного програмування.
- Демонстрація практичного застосування запропонованої методики підвищення інформаційної безпеки ресурсів хмарної ІТКС.

Для визначення доцільності розробки даної методики, спрямованої на підвищення безпеки інформації хмарних ІТКС, в ході виконання роботи було проведено економічні розрахунки. Було визначено експлуатаційній та капітальні витрати, а також можливих збитків у разі реалізації загроз. На основі цих розрахунків було визначено економічну доцільність. Даним значенням було

підтверджено доцільність даного рішення. Знайдений коефіцієнт повернення інвестицій підтверджує економічну ефективність розробленої методики підвищення захищеності ресурсів хмарної ІТКС.

ПЕРЕЛІК ПОСИЛАНЬ

1. A virtual data center versus a physical data center [Електроний ресурс] - Режим доступу до ресурсу: https://subscription.packtpub.com/book/virtualization-and-cloud/9781783551682/1/ch01lvl1sec13/a-virtual-data-center-versus-a-physical-data-center.
2. The Pros and Cons of On-Prem vs. Colocation vs. Cloud vs. Edge [Електроний ресурс] – Режим доступу до ресурсу: https://www.vxchnge.com/blog/pros-cons-on-prem-colocation-cloud.
3. Google Cloud Platform: Google Cloud Platform: What it is, how to use it, and how it compares [Електроний ресурс] – Режим доступу до ресурсу: https://www.acronis.com/en-us/articles/google-cloud-platform/.
4. What is hypervisor? [Електроний ресурс] – Режим доступу до ресурсу: https://www.vmware.com/topics/glossary/content/hypervisor.
5. What is Virtualization in Cloud Computing? - Characteristics & Benefits [Електроний ресурс] – Режим доступу до ресурсу: https://www.analyticssteps.com/blogs/what-virtualization-cloud-computing-characteristics-benefits.
6. What is Cloud Hypervisor? [Електроний ресурс] – Режим доступу до ресурсу: https://www.vmware.com/topics/glossary/content/cloud-hypervisor.
7. What are cloud service providers? [Електроний ресурс] – Режим доступу до ресурсу: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-providers.
8. What are public, private, and hybrid clouds? [Електроний ресурс] – Режим доступу до ресурсу: https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/#overview.

9. Облачная пирамида: IaaS, PaaS, SaaS [Електроний ресурс] – Режим доступу до ресурсу: https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-i-saas.
10. Database as a Service (DBaaS) Explained [Електроний ресурс] – Режим доступу до ресурсу: https://www.mongodb.com/database-as-a-service.
11. Authentication As a Service: Architecture, Technologies and Solutions [Електроний ресурс] – Режим доступу до ресурсу: https://www.apriorit.com/dev-blog/549-authentication-as-a-service.
12. Pros and Cons of Cloud Computing [Електроний ресурс] – Режим доступу до ресурсу: https://www.morefield.com/blog/pros-and-cons-of-cloud-computing/.
13. Cloud Security Standards: What to Expect & What to Negotiate Version 2.0 [Електроний ресурс] – Режим доступу до ресурсу: https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf.
14. Google App Security and Compliance Whitepaper [Електроний ресурс] – Режим доступу до ресурсу: https://static.googleusercontent.com/media/gsuite.google.com/ru//files/google-apps-security-and-compliance-whitepaper.pdf.
15. Cloud Storage Service Level Agreement [Електроний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/storage/sla.
16. PCI DSS [Електроний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/security/compliance/pci-dss.
17. HIPAA [Електроний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/security/compliance/hipaa.
18. Google Cloud & the General Data Protection Regulation (GDPR) [Електроний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/privacy/gdpr

19. CIS Benchmark [Електроний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark.
20. Risk Term [Електроний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/glossary/term/risk.
21. Как справиться с неопределенностью при оценке рисков ИБ [Електроний ресурс] – Режим доступу до ресурсу: https://www.jetinfo.ru/kak-spravitsya-s-neopredelennostyu-pri-oczenke-riskov-ib/.
22. Risk Based Approach to Security [Електроний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/B9781597499491000048.
23. Information Security Risk Assessment Methods, Frameworks and Guidelines [Електроний ресурс] – Режим доступу до ресурсу: http://www.infosecwriters.com/Papers/MHaythorn_Risk_Frameworks_guidelines.pdf.
24. Quantitative Risk Assessment with ISAMM on ESA's Operations Data Systems [Електроний ресурс] – Режим доступу до ресурсу: https://www.itrust.lu/wp-content/uploads/2007/09/publications_TTC_2007_abstract_risk_assessment_with_ISAMM.pdf.
25. Оцінка інформаційних ризиків [Електроний ресурс] – Режим доступу до ресурсу: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm.
26. A Qualitative Risk Analysis and Management Tool - CRAMM [Електроний ресурс] – Режим доступу до ресурсу: https://www.sans.org/white-papers/83/
27. Основные подходы к анализу и оценке рисков информационной безопасности [Електроний ресурс] – Режим доступу до ресурсу: http://nirit.org/wp-content/uploads/2017/09/42-48.pdf.

28. What is PHA, what is it for and how is it constructed? [Електроний ресурс] – Режим доступу до ресурсу: https://www.leedeo.es/l/preliminary-hazard-analysis-how-constructed/.
29. HAZOP [Електроний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/HAZOP.
30. Модель системи безпеки з повним перекриттям [Електроний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Модель_системи_безпеки_з_повним_перекриттям.
31. Security Zones [Електроний ресурс] – Режим доступу до ресурсу: https://protectivesecurity.govt.nz/physical-security/lifecycle/design/apply-good-practices/security/.
32. Bring Your Own Device [Електроний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Bring_your_own_device.
33. OWASP Top Ten [Електроний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-project-top-ten/.
34. Методика снижения рисков информационной безопасности облачных сервисов на основе квантифицирования уровней защищенности и оптимизации состава ресурсов [Електроний ресурс] – Режим доступу до ресурсу: http://www.dslib.net/zaw-informacia/metodika-snizhenija-riskov-informacionnoj-bezopasnosti-oblachnyh-servisov-na-osnove.html.
35. Метод ветвей и границ [Електроний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Метод_ветвей_и_границ.
36. Алгоритм Гомори [Електроний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Алгоритм_Гомори.
37. A Figure of Merit [Електроний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/topics/chemistry/figure-of-merit.
38. Облачные вычисления второго поколения: Система CLAVIRE [Електроний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/spbifmo/blog/319688/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	14	
6	А4	Спеціальна частина	35	
7	А4	Економічний розділ	10	
8	А4	Висновки	2	
9	А4	Список літератури	4	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

№	Найменування
1	Кваліфікаційна_Робота_Марченко_В_Т_125м_20_1.docx
2	Презентація_Марченко_В_Т_125м_20_1.pptx

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студентки групи 125м-20-1

Марченко Валерії Тарасівни

на тему: «Підвищення інформаційної безпеки хмарних сервісів на основі розподілу рівнів захищеності та оптимізації ресурсів»

Пояснювальна записка складається за вступу, трьох розділів і висновків, викладених на 60 сторінках.

Метою кваліфікаційної роботи є зниження ризиків інформаційної безпеки в хмарних ІТКС при обробці інформації різного ступеня конфіденційності.

Практичне значення результатів кваліфікаційної роботи полягає у дослідження методики розподілу рівнів захищеності та оптимізації ризиків для досягнення поставленої мети. В кваліфікаційній роботі вирішуються наступні задачі: аналіз хмарних технологій, аналіз нормативно-правового забезпечення у сфері інформаційної безпеки, аналіз моделей загроз та порушника, дослідження моделей аналізу ризиків, обґрунтування використання методу мінімізації ризиків інформаційної безпеки у хмарних ІТКС. За результатами досліджень було розроблено та оцінено результати застосування методики розподілу рівнів захищеності та оптимізації ризиків, розраховано ефективність застосування та визначено доцільність.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначним відхиленням від стандартів.

За час дипломування Марченко В.Т. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» , а кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи,
д.т.н., професор **В.І. Корнієнко**

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)