ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)

Освітній рівень

Галузь знань 17 Електроніка та телекомунікації

Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка

Шифр і назва спеціальності

на тему Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж

ДРТР. 022222.01.02. ПЗ

Виконав: студент 2 курсу, група $ТР_м$-22-1 _____ Максим СЛОБОДЯН
підпис Ім'я, прізвище

Керівник: д-р техн. наук, проф. _____ Сергій ПІДЧЕНКО
підпис Ім'я, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ Сергій ПІДЧЕНКО
підпис Ім'я, прізвище

20 12 2023 р.

Хмельницький, 2023

Хмельницький національний університет

Факультет *інформаційних технологій*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність *172 – Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою Сергій ПІДЧЕНКО
«1» 09 2023р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Слободяну Максиму Олеговичу

1 Тема роботи: *Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж*
керівник роботи Підченко Сергій Костянтинович, д-р техн. наук, професор
Затверджено наказом по університету від «15» серпня 2023р. № 30
2 Строк подання студентом роботи на кафедру: 1.12 2023р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи: підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.
Об'єкт дослідження: процес забезпечення надійності та відмовостійкості корпоративної безпроводової мережі.
Предмет дослідження: метод підвищення відмовостійкості корпоративної мережі шляхом резервування серверного устаткування як найбільш критичної ланки системи, реалізації механізму резервного копіювання та відмово стійкого каналу доступу до Інтернет.
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити):
1. Огляд методів підвищення відмовостійкості безпроводових мереж, а також відомих вразливостей таких мереж
2. Розробка математична модель відмовостійкої корпоративної безпроводової мережі
3. Розробка відмовостійкої системи резервування серверного забезпечення на базі засобів віртуалізації
4. Розробка відмовостійкої корпоративної мережі

Завдання отримав _____
Науковий керівник _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз завдання на магістерську роботу	15.09 .2023р.	Виконано
2	Написання вступу та 1-го розділу роботи	15.10 .2023р.	Виконано
3	Написання 2-го розділу роботи	25.10 .2023р.	Виконано
4	Написання 3-го розділу роботи	5.11, .2023р.	Виконано
5	Написання 4-го розділу роботи	10.11 .2023р.	Виконано
6	Виправлення помилок відповідно до зауважень керівника роботи	15.11 .2023р.	Виконано
7	Підготовка доповіді та презентаційних матеріалів	1.12 .2023р.	Виконано

Студент _____ Максим СЛОБОДЯН
Підпис Ім'я, прізвище

Керівник роботи _____ Сергій ПІДЧЕНКО
Підпис Ім'я, прізвище

АНОТАЦІЯ

Тема дипломної роботи: «Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж»

Автор роботи: *Слободян Максим Олегович*

Керівник роботи: *д-р техн. наук, проф. Підченко Сергій Костянтинович*

Пояснювальна записка: 72 сторінки (без додатків), 23 рисунки, 4 таблиці, 40 джерел посилання, 2 додатки.

Графічна частина: 40 презентаційних слайдів.

КЛЮЧОВІ СЛОВА: корпоративна мережа, безпроводовий зв’язок, телекомунікації, кібербезпека, відмовостійкість

Мета роботи: підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.

Об'єкт дослідження: процес забезпечення надійності та відмовостійкості корпоративної безпроводової мережі.

Предмет дослідження: метод підвищення відмовостійкості корпоративної мережі шляхом резервування серверного устаткування як найбільш критичної ланки системи, реалізації механізму резервного копіювання та відмово стійкого каналу доступу до Інтернет.

В першому розділі магістерського дослідження було виконано аналіз літературних джерел та науково-практичних публікацій згідно теми роботи, а саме:

- дано характеристику корпоративної мережі підприємства як базу для розгортання на її базі інфраструктури підприємства та розглянуто типові топології таких мереж, а саме зіркоподібну топологію та змішану топологію на прикладі реального технологічного рішення;

- проведено детальний аналіз можливих відмов та несправностей корпоративних мереж, які спричинені як власними відмова, так і зловмисними

діями, спрямованими на кібератак на вразливості системи; також дана класифікація таких вразливостей;

В другому розділі магістерського дослідження було виконано наступне:

- розроблена узагальнена математична модель надійності вузла корпоративної мережі;
- дано характеристики моделі корпоративної мережі;
- розроблено формальну модель станів корпоративної мережі;
- розглянуто корпоративну мережу, що складається з елементів з відомими розподілами часу безвідмовної роботи та часу відновлення. Функціонування мережі відбувається згідно з визначеною схемою розрахунку надійності, де всі елементи поділені на робочі та резервні;

В третьому розділі магістерської роботи було виконано наступне:

- розроблено модель ковзного резервування для серверів корпоративної мережі, побудовано граф стані моделі
- розраховано стаціонарні показники надійності системи: стаціонарні ймовірності системи, стаціонарний коефіцієнт готовності та середній час відновлення
- розраховано перехідні характеристики: перехідні ймовірності системи, функція готовності та функція ймовірності безвідмовної роботи

В четвертому розділі магістерської роботи було виконано наступне:

- розгорнуто та налаштовано серверних гіпервізора VMware ESXi для побудови на його базі відмово стійкого ядра корпоративної інфраструктури підприємства
- встановлено та налаштовано віртуальну машину від управлінням операційної системи Windows;
- налаштовано резервний канал доступу до мережі Інтернет на базі технології Dual WAN.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – База даних

ПЗ – Програмне забезпечення

ЦП – Центральний процесор

CPU – Central processing unit

DNS – Domain name system

DHCP – Dynamic host configuration protocol

LAN – Local area network

MAC – Medium access control

NIC – Network interface card

PMKID – Pairwise master key identifier

RAID – Redundant array of independent disks

SSH – Secure shell

WAN – Wide Area Network

WPA – Wi-Fi protected access

WPS – Wi-Fi protected setup

WEP – Wired equivalent privacy

ВСТУП

Корпоративні мережі, що використовуються для підтримки функціонування на їхній базі інфраструктури підприємства, характеризуються підвищеними вимогами щодо безвідмовної роботи із забезпечення підтримки усіх бізнес-процесів.

Корпоративна мережа призначена для підтримки діяльності підприємства, і її користувачами є лише співробітники цього підприємства (гостьовий сегмент може бути передбачено для зони очікування, або безпосередньо для надання доступу клієнтам, якщо дана компанія веде роботу із клієнтами). На відміну від мереж операторів зв'язку, корпоративні мережі, як правило, не надають послуг стороннім організаціям та користувачам . Корпоративна мережа працює за протоколом TCP/IP і використовує стандарти Інтернету, разом з сервісними додатками, які забезпечують доставку даних користувачам мережі.

Актуальність роботи обумовлена проблемою забезпечення належного рівня надійності та відмовостійкості корпоративних мереж із безпроводових доступом, а також забезпечення належного рівня інформаційної безпеки та кібербезпеки в таких системах.

Мета і задачі дослідження. Метою роботи є підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі **задачі**:

- аналіз базової архітектури корпоративної телекомунікаційної мережі з позиції відмовостійкості та вразливостей до кібератак;
- удосконалення базової архітектури корпоративної телекомунікаційної мережі шляхом введення в систему елементів надлишковості та механізмів живучості;
- імітаційне моделювання відмовостійкої корпоративної мережі;

- проектування відмовостійкої корпоративної інфраструктури на базі мережі із захищеними безпровоовими каналами доступу, надійними механізмами резервного копіювання та резервним каналом доступу до мережі Інтернет.

Об'єктом дослідження є процес забезпечення надійності та відмовостійкості корпоративної безпроводової мережі.

Предметом дослідження є метод підвищення відмовостійкості корпоративної мережі шляхом резервування серверного устаткування як найбільш критичної ланки системи, реалізації механізму резервного копіювання та відмово стійкого каналу доступу до Інтернет.

Для вирішення поставлених задач були використані такі **методи дослідження:** методи математичного аналізу, чисельні методи, методи теорії надійності, , методи алгоритмізації та програмування.

Науково-практична новизна отриманих результатів:

- набув подальшого розвитку метод підвищення надійності корпоративної мережі із безпроводових доступом шляхом забезпечення резервування серверного устаткування, яке побудоване на базі інфраструктури віртуалізації; а також впровадження механізму резервного каналу доступу до мережі Інтернет на базі технології Dual-Wan.

- встановлена та налаштовано серверне забезпечення корпоративної мережі та IT інфраструктури підприємства на базі гіпервізора VMware ESXI;

- запропонована схема резервування, яка дозволить забезпечити відмово стійку роботу системи шляхом введення ковзного резервного серверного вузла.

Апробацією результатів дослідження є стаття у фаховому виданні Слободян М.О. Модель хаотичної надширокосмугової системи передачі інформації для бездротових сенсорних мереж / М.О. Слободян // Вісник Хмельницького національного університету. Технічні науки. – 2023. – № 2. – С. 284–289.

1 ОГЛЯД МЕТОДІВ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ БЕЗПРОВОДОВИХ МЕРЕЖ, А ТАКОЖ ВІДОМИХ ВРАЗЛИВОСТЕЙ ТАКИХ МЕРЕЖ

1.1 Загальна характеристика корпоративних мереж

Корпоративні мережі, що використовуються для підтримки функціонування на їхній базі інфраструктури підприємства, характеризуються підвищеними вимогами щодо безвідмовної роботи [1-3].

Структура підприємства, яке відноситься до малого та середнього бізнесу, складається із взаємодіючих підрозділів, кожен з яких може мати свою власну структуру [1, 2]. Ці елементи функціонально пов'язані між собою та виконують конкретні види робіт в рамках єдиного процесу. Крім того, в ході протікання бізнес-процесів має місце постійний обмін інформацією, як в усному вигляді, так із залученням інформаційно-комунікаційних технологій, електронного документообігу тощо. Також забезпечується взаємодія окремих елементів із зовнішніми системами, як каналами інфокомунікацій. Такими рисами характеризуються більшість підприємств малого та середнього бізнесу, а також інші організації, наприклад, приватні медичні заклади, заклади вищої освіти, урядові установи, фінансові організації, промислові підприємства, комерційні фірми тощо [1-3].

Корпоративна мережа призначена для підтримки діяльності підприємства, і її користувачами є лише співробітники цього підприємства (гостьовий сегмент може бути передбачено для зони очікування, або безпосередньо для надання доступу клієнтам, якщо дана компанія веде роботу із клієнтами). На відміну від мереж операторів зв'язку, корпоративні мережі, як правило, не надають послуг стороннім організаціям та користувачам [1]. Корпоративна мережа працює за протоколом TCP/IP і використовує стандарти Інтернету, разом з сервісними додатками, які забезпечують доставку даних користувачам мережі [4].

Для корпоративних мереж характерним є територіальне розподілення її сегментів, які, об’єднуючи офіси, підрозділи та інші структури, які географічно віддалені один від одного [1, 2] . Ці мережі дозволяють забезпечити спільну обробку даних та обмін даними між кінцевими пристроями, що керовані операторами робочих станцій, а також спільне використання корпоративних додатків та офісних пристроїв із мережевими інтерфейсами. Використання обчислювальних мереж надає підприємству ряд переваг, таких як розподіл ресурсів, вдосконалення комунікацій, поліпшення доступу до інформації, швидке і якісне ухвалення рішень, а також свобода в територіальному розміщенні комп’ютерів [2, 5].

Також до характеристик корпоративних мереж відносять здатність таких мереж виконувати паралельні обчислення, що в свою чергу дозволяє досягти високої продуктивності, перевищуючи ефективність окремого процесора у системі з декількома обчислювальними вузлами. До ключових переваг розподілених систем належать підвищені показники відмовостійкість. Під відмовостійкістю розуміється можливість системи виконувати свої функції навіть при відмовах окремих елементів апаратури та частковій недоступності даних. З метою підвищення відмовостійкість в розподілених системах застосовуються принципі надлишковості, які дозволяють передавати виконання завдань на інші оброблювальні вузли у випадку відмови одного з поточних вузлів [1, 5].

Наступною важливою характеристикою корпоративної мережі є умова забезпечення співробітникам оперативного доступу до розгалуженої корпоративної інформації, що представлена інфраструктурою фірми. Корпоративна мережа сприяє поліпшенню та оптимізації комунікації між співробітниками підприємства, клієнтами та постачальниками, зменшуючи потребу у інших традиційних формах комунікації, таких як телефон чи пошта. Корпоративна мережа також може служити основою для організації аудіо- та відеоконференцій, а також для створення внутрішньої телефонної системи [1, 5].

Структурна характеристика корпоративної мережі залежить від цільового призначення, яке визначається бізнес процесами підприємства, структурою самого підприємства та кількістю співробітників, номенклатурою офісного обладнання та його характеристиками з позиції задоволення потреб персоналу [5-7].

На рисунку 1.1 зображена узагальнена схема характеристик корпоративної мережі невеликої фірми з позиції функціональних вимог.

Рисунок 1.1 – Узагальнені характеристики корпоративної мережі щодо її функціональних вимог

Відповідно до рисунку 1.1, корпоративна мережа включає в себе різні структурні елементи, які взаємодіють між собою для забезпечення ефективної роботи всього підприємства.

Основні структурні елементи корпоративної мережі такі [7]:

- сервери: це комп'ютери (серверні станції) чи комп'ютерні системи, які забезпечують різноманітні сервіси та ресурси, такі як зберігання даних, обробка запитань, електронна пошта тощо. Сервери можуть бути централізованими або розподіленими за різними вузлами мережі;

- клієнтські комп'ютери: це робочі станції чи персональні комп'ютери, які використовуються співробітниками для доступу до ресурсів мережі. Клієнтські комп'ютери можуть виконувати різноманітні завдання та служити для взаємодії з серверами;

- мережеве обладнання: маршрутизатори, комутатори, концентратори та інше обладнання, яке забезпечує фізичне з'єднання та передачу даних в мережі. Розташування цього обладнання може включати централізовані мережеві центри, а також розподілені вузли мережі;

- канали зв'язку: проводові та безпроводові засоби передачі даних, такі як оптичні волоконні лінії, мідні кабелі, без проводові канали зв'язку тощо. Вони забезпечують комунікацію між різними елементами мережі;

- програмне забезпечення мережі: це програми та операційні системи, які використовуються для управління та контролю мережевими ресурсами. До таких додатків належать операційні системи серверів, програми аутентифікації та авторизації, антивірусне програмне забезпечення тощо;

- безпека: елементи, пов'язані з забезпеченням безпеки мережі, наприклад, такі як файрволи, антивіруси, системи виявлення вторгнень та інші засоби захисту;

- інфраструктура додатків: це може включати бази даних, електронну пошту, програми для спільної роботи, корпоративні портали та інші додатки, які

використовуються співробітниками в контексті корпоративної діяльності для реалізації бізнес-процесів;

Усі перераховані елементи повинні взаємодіяти узгоджено, створюючи ефективну та добре організовану корпоративну мережу інфраструктури підприємства.

Розглянемо приклади топологій корпоративних мереж організації, яка складається із декількох філій та має складну ієрархічну структуру [7-9].

На рисунку 1.1 наведено приклад топології «Зірка», згідно якої кожну окрему філію організації обслуговує один сервер (Філія 1), декілька серверів (Філія 2) або один сервер для обслуговування кількох філій організації одночасно (Філія 3-4). Можливі змішані схеми, що включають всі описані випадки або їхні комбінації [9].

Топологія «Зірка» є рекомендованою для забезпечення ефективного керування та надійності функціонування мережі, враховуючи важливість того, щоб кожне відгалуження також буде організовано у вигляді зірки. Такий підхід сприяє зручному керуванню серверами нижчого рівня і підвищує надійність мережі. Крім того, це гарантує існування «третьої сторони» під час передачі повідомлень від користувача одного сервера до користувача іншого сервера. Це особливо важливо, наприклад, у банківських мережах чи мережах з високим рівнем відповідальності користувачів за передачу інформації [9].

Розглянемо приклад для даної організації, де електронне повідомлення від клієнта Філії 3 проходить через сервер Філії 1 для доставки клієнту Філії 2. Цей механізм забезпечує надійність та безпеку обміну інформацією, що особливо актуально у сферах, де важливий своєчасний обіг інформації, таких як банківська сфера та інші фінансові організації.

Топологія мережі, що характеризується наявністю багатьох вузлів може збільшити експлуатаційні витрати та ускладнити обслуговування, але в той же час воно також має свої переваги. Зокрема, це дозволяє розподіляти навантаження між серверами, зменшуючи навантаження на окремі елементи мережі та спрощуючи

адміністративну роботу. При цьому немає необхідності адмініструвати велику кількість користувачів на одному сервері, особливо якщо це стосується співробітників інших організацій.

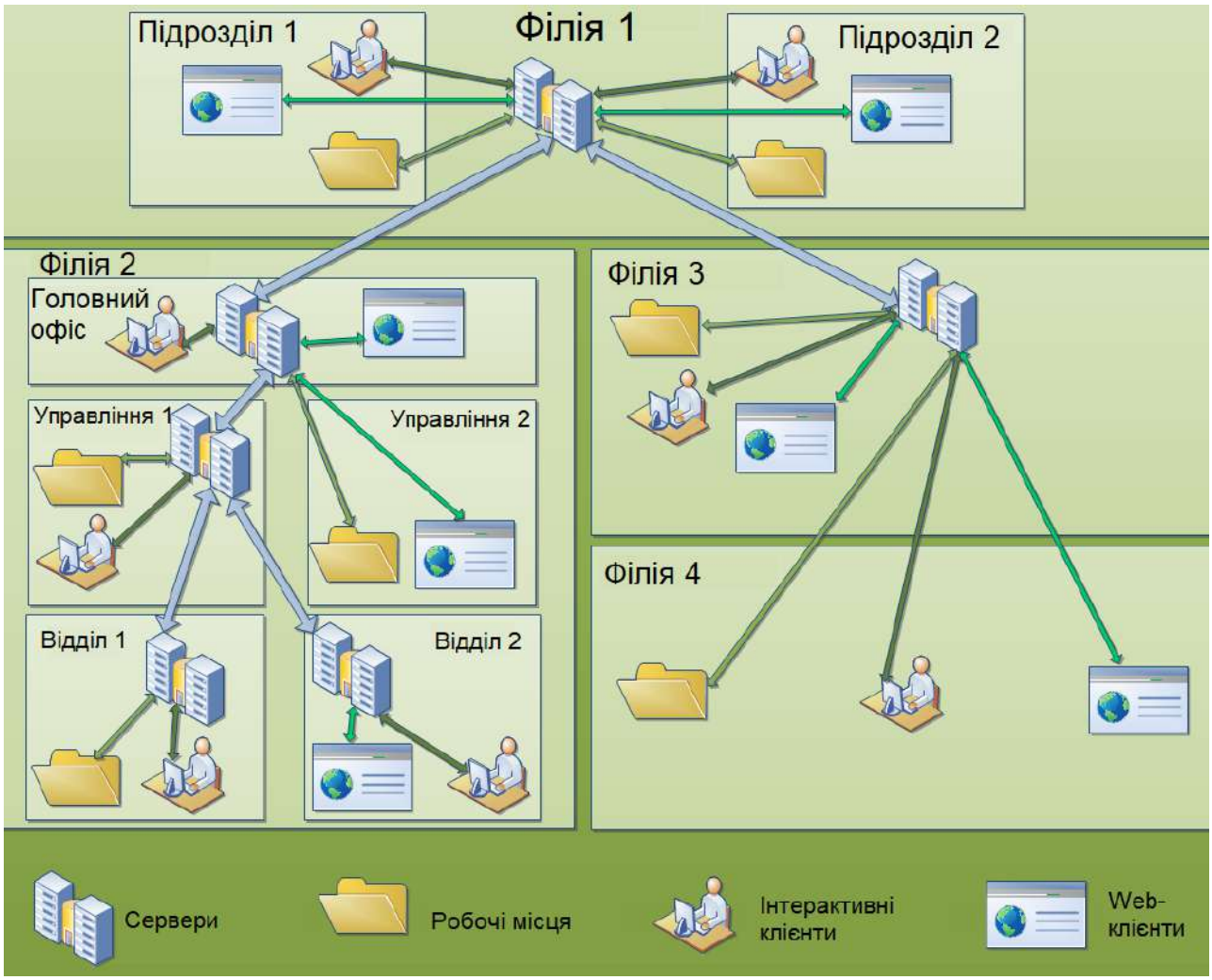


Рисунок 1.2 – Приклад топології корпоративної мережі «Зірка» [9]

Використання кількох серверів для обслуговування окремого підрозділу організації може бути доцільним у випадках, коли її підрозділи розташовані на великій

території та мають значну кількість персоналу, що використовує мережі загального доступу. Такий підхід дозволяє підвищити рівень захисту та надійності мережі.

Приклад змішаної топології корпоративної мережі наведено на рисунку 1.3.

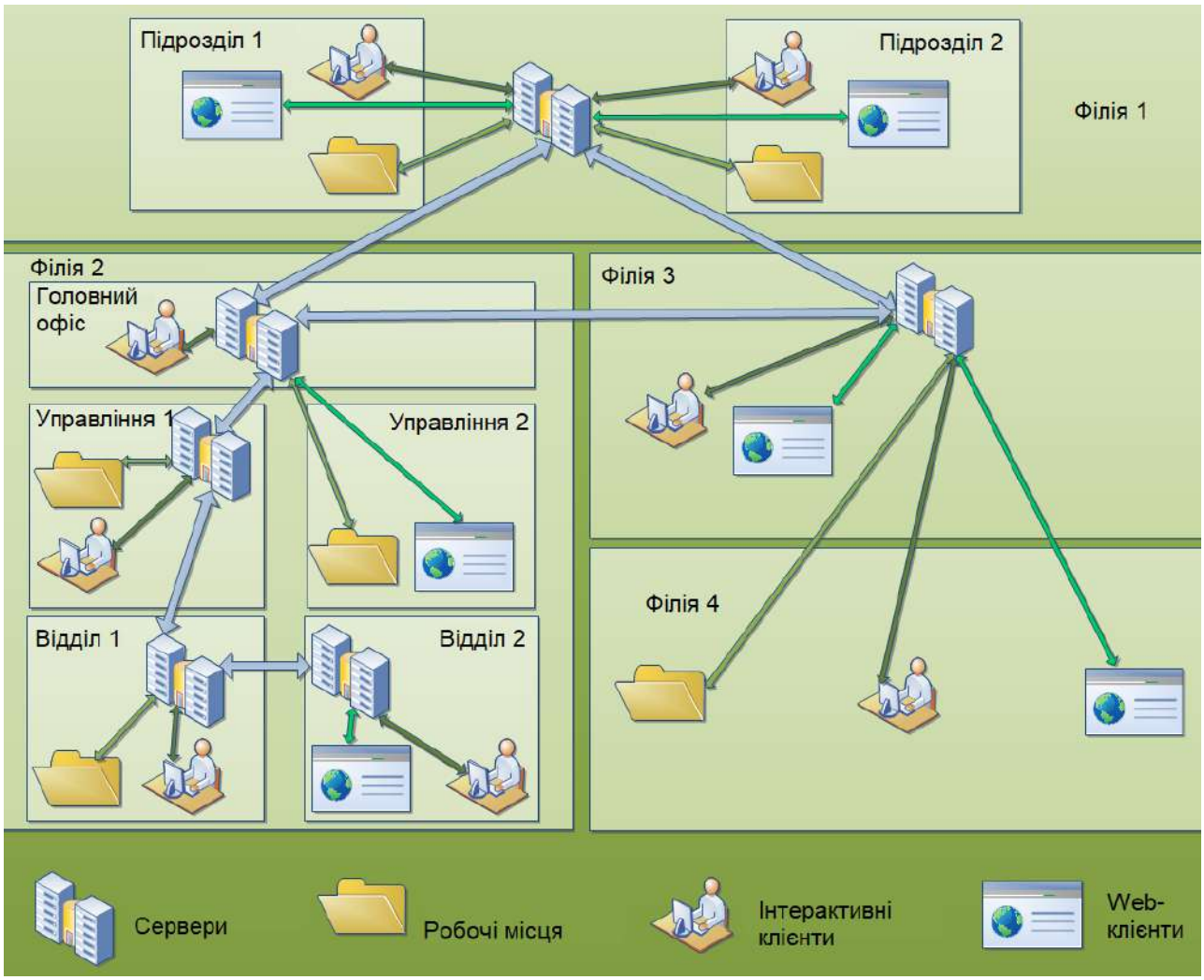


Рисунок 1.3 – Приклад змішаної топології корпоративної мережі [9]

Взаємна можливість передачі двосторонніх повідомлень між серверами, що розташовані на одному рівні, сприяє ефективному обміну даними безпосередньо між ними. Хоча такий підхід може зменшити навантаження на канали передачі даних, він

призводить до значного зменшення керованості мережі. Без визначеної «третьої сторони», яка могла б виступати арбітром у випадку конфліктних ситуацій між різними організаціями і їхніми підрозділами, може виникнути складність в управлінні та регулюванні.

Існують різні варіанти топології мережі, але вони, в основному, випливають із зазначених вище принципів. Зміна налаштувань маршрутних таблиць на вузлах мережі може впливати на форму топології, варіюючи її варіанти та структуру [9].

1.2 Огляд можливих відмов та вразливостей

1.2.1 Загальні відмови в корпоративних мережах та їхні причини

Відмови у функціонуванні комп'ютерних корпоративних мереж можуть виникати з різних причин і включати різноманітні проблеми. На рисунку 1.4 наведена класифікація типових відмов, які можуть виникати в процесі функціонування. До них можна віднести [11] :

- апаратні відмови: вихід з ладу обладнання – пошкодження або виходження з ладу мережевого обладнання, такого як маршрутизатори, комутатори, сервери або кабелі, може призвести до відмови в частині або всій мережі;
- програмні відмови: помилки програмного забезпечення [11] – програмні вразливості чи неправильна робота програм можуть призвести до відмов в роботі мережі. Це може включати помилки операційних систем, мережевих протоколів чи програмних додатків;
- спроби вторгнення та кібератаки [12]: 1) віруси та шкідливе програмне забезпечення: на мережеве програмне забезпечення можуть викликати відмови або порушити роботу мережі, інфікуючи комп'ютери чи сервери;
2) DDoS – атаки з переповненням [13]: кібератаки, спрямовані на перевантаження серверів або мережевих ресурсів, можуть призвести до відмови в обслуговуванні;

Рисунок 1.4 – Класифікація відмов у корпоративних мережах та їхніх причин

- помилки у конфігурації та управлінні: 1) Некоректна конфігурація – неправильна настройка параметрів мережевого обладнання чи програм може викликати проблеми в роботі мережі; 2) проблеми з управлінням ресурсами [8] – недостатня або неефективна управлінська політика може призвести до відмови через неспроможність вирішення конфліктів або неадекватну реакцію на події;
- проблеми з безпекою: неавторизований доступ [17] – неправомірний доступ до мережевих ресурсів може викликати проблеми з безпекою та викликати відмови у функціонуванні;
- проблеми з електропостачанням та фізична безпека [17]: 1) Перебої в електропостачанні – Відключення електропостачання або флуктуації можуть викликати відмови в роботі обладнання; 2) Фізична пошкодження – непередбачувані події, такі як природні катастрофи чи вандалізм, можуть завдати фізичних пошкоджень обладнанню і спричинити відмови;
- системні та організаційні проблеми [17]: 1) неадекватне масштабування мережі може призвести до перевантаження ресурсів та відмов у роботі; 2) некоректне планування архітектури та розміщення ресурсів може створити ситуації, при яких мережа неспроможна ефективно працювати.

Таким чином, для того щоб запобігти відмовам та мінімізувати їхні негативні наслідки, важливо розробляти та виконувати ефективні стратегії безпеки, проводити систематичне тестування та планування, а також впроваджувати ефективні практики управління мережами.

1.2.2 Можливі відмови, що спричинені вразливостями безпроводових мереж Wi-Fi

Як було зазначено, найбільш розповсюдженими безпроводовими локальними мережами є такі, що побудовані на протоколах сімейства IEEE 802.11 [17]. Ці протоколи не регламентують засоби безпеки, які б могли повністю забезпечити захист

мережі, тому можливими є виявлення та використання різного роду вразливостей у цих мережах. В результаті вразливостей мережі, до прикладу, можливі витоки конфіденційної інформації, розкриття персональних даних персоналу та клієнтів фірми, що може стати причиною значних збитків.

Вразливість Wi-Fi [18] обумовлена перш за все самим фактом використання безпроводового каналу зв'язку, що теоретично робить можливим несанкціоноване підключення з будь-якого місця, яке знаходиться в зоні покриття.

Так, наприклад, однієї із найбільш розповсюджених атак, що спрямована на Wi-Fi мережі, є так званий Wardriving [19]. В ході атаки цього типу зловмисник ставить за мету перехопити сигнал шляхом фізичного переміщення комп'ютера. Такий тип атаки може мати успіх із незахищеними або недостатньо захищеними Wi-Fi мережами. В переважній більшості користувачі користуються технологіями захисту WEP [20] та WPA [21], або взагалі не використовують захист мережі, що робіть їх вразливими до даного типу атак.

Також відомою вразливістю є критична вразливість стандарту WPA2 [22], яка називається KRACK [23]. Дана вразливість надає зловмиснику, який знаходиться в зоні покриття Wi-Fi об'єкту атаки, можливість виконувати повторне встановлення унікальних ключів шифрування і таким чином обходити захист WPA2. Усуненням вразливості є оновлення алгоритму роботи, згідно якого кожен ключ шифрування повинен використовуватись лише один раз [23].

В цілому найбільш розповсюдженими типами вразливостей Wi-Fi є помилки у конфігурації безпроводових пристроїв (Wi-Fi маршрутизаторів та точок доступу); використання вразливих технологій захисту WEP та WPA; витік даних з безпроводової мережі через вразливості інших (в т.ч. проводових) сегментів корпоративної мережі [18].

Безпроводові мережі Wi-Fi мають декілька відомих вразливостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу чи

виконання атак. Розглянемо детально відмови безпроводових Wi-Fi мереж, причинами яких є зловмисні дії пов’язані із хакерськими атаками (рисунок 1.5):

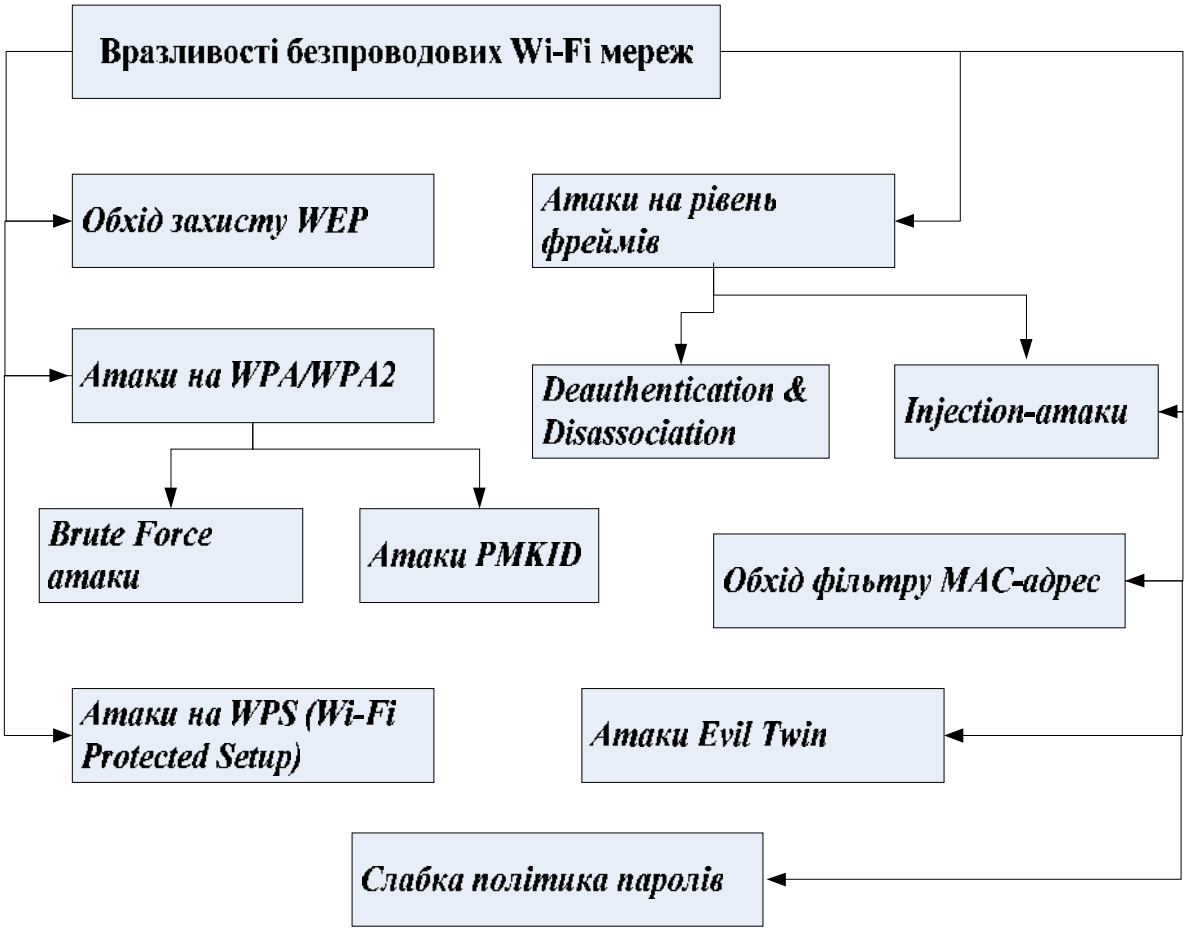


Рисунок 1.5 – Причини відмов Wi-Fi мереж, спричинені хакерськими атаками на відповідні вразливості мережі

- обхід захисту WEP (Wired Equivalent Privacy): WEP є одним з ранніх протоколів шифрування для Wi-Fi, що відомий своєю слабкістю. Його можна легко зламати шляхом збору та аналізу трафіку.

Рекомендується також використовувати більш сучасні протоколи шифрування, такі як, наприклад, протокол WPA (Wi-Fi Protected Access) або WPA2 [20-22];

- атаки на WPA/WPA2: 1) Brute Force атаки – атаки на паролі методом спроб і помилок можуть бути використані для вгадування паролів WPA або WPA2; 2) атаки з використанням PMKID – зловмисники можуть застосовувати атаки, які використовують PMKID (Pairwise Master Key Identifier) для взлому паролів WPA/WPA2 [23].

- атаки на WPS (Wi-Fi Protected Setup): WPS, який призначений для спрощення процесу підключення нових пристроїв до Wi-Fi, може бути вразливим до атак, таких як PIN-атаки, які спрямовані на вгадування PIN-коду;

- атаки Evil Twin [25]: зловмисники можуть створити фальшиву точку доступу, яка має ідентичний SSID (ім’я мережі) і може викликати підключення користувачів. Це може призвести до перехоплення трафіку та інших атак;

- атаки на рівень фреймів: 1) атаки Deauthentication або Disassociation [26]: зловмисники можуть використовувати спеціальні фрейми для відсилання сигналів відключення пристроїв від мережі; 2) Injection-атаки – введення шкідливих фреймів у трафік мережі для здійснення атак типу Man-in-the-Middle [27];

- обхід фільтру MAC-адрес [28]: фільтрація за MAC-адресами є однією з методів контролю доступу, вона може бути обійдена шляхом підробки або зламуванням MAC-адреси;

- спільне використання паролю та слабкі паролі: використання слабких паролів або використання одного пароля для декількох пристроїв може стати джерелом вразливостей [29].

Загальна стійкість безпроводової мережі може бути покращена за допомогою правильної конфігурації, ретельного планування, регулярного обслуговування та використання надійного обладнання.

1.3 Методи підвищення відмовостійкості корпоративних мереж

В ході аналізу літературних джерел згідно тематики дослідження [30-33] були виділена такі методи забезпечення відмовостійкості корпоративних мереж (рисунок 1.6).

Методи підвищення надійності та відмовостійкості (загальні механізми забезпечення живучості) поділяються на активні методи, що включають методи алгоритмізації та інтелектуального аналізу для контролю стану мережі та своєчасного реагування з метою компенсації негативного фактору відмов компонентів; пасивні методи передбачають ручне коригування архітектури та підтримку резервування критичних вузлів, наприклад, файловий серверів.

Загалом ці методи ґрунтуються на застосуванні відмово стійкої архітектури із введенням надлишковості в систему.

Надлишковість дисковий масивів представлена використанням дзеркальних (Mirror 1) RAID масивів для забезпечення відмовостійкості сховища даних [34].

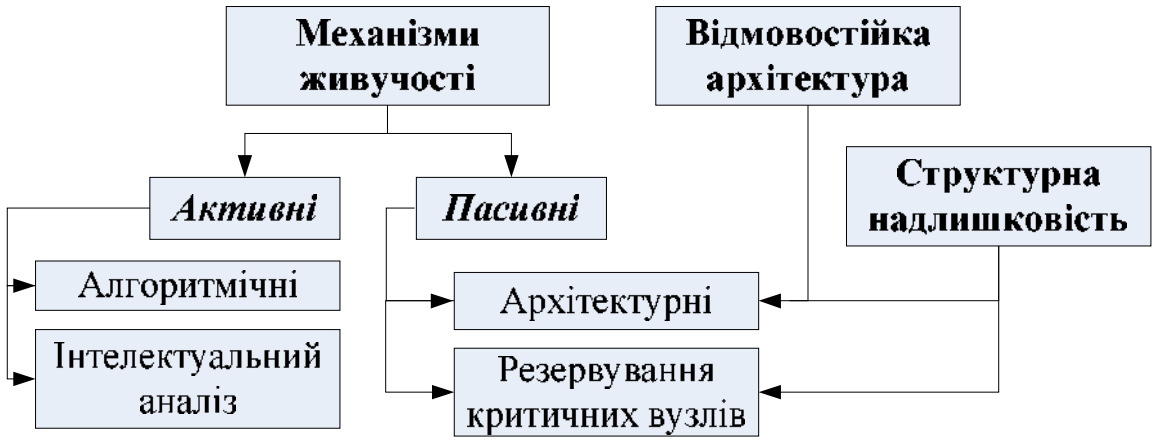


Рисунок 1.6 – Методи забезпечення відмовостікості

Механізм своєчасного резервного копіювання системних файлів, операційних систем та корпоративної бази даних. Ефективно це можна реалізувати засобами резервного копіювання Veeam Backup & Replication [35].

Забезпечення безвідмовного підключення шляхом застосування технологій Dual-WAN для резервного каналу доступу [36].

1.4 Постановка задачі дослідження

В результаті аналізу існуючих методів та засобів підвищення відмовостійкості та надійності корпоративних мереж, а також відомих вразливостей для кібератак на такі мережі, сформульовані наступні задачі до вирішення в даній роботі:

- формалізація завдання та розробка математичної моделі корпоративної телекомунікаційної мережі із сегментами, з'єднаними безпроводовими каналами;
- аналіз базової архітектури корпоративної телекомунікаційної мережі з позиції відмовостійкості та вразливостей до кібератак;
- удосконалення базової архітектури корпоративної телекомунікаційної мережі шляхом введення в систему елементів надлишковості та механізмів живучості;
- імітаційне моделювання відмовостійкої корпоративної мережі;
- проектування відмовостійкої корпоративної інфраструктури на базі мережі із захищеними безпровоовими каналами доступу, надійними механізмами резервного копіювання та резервним каналом доступу до мережі Інтернет.

Висновки до першого розділу

В першому розділі магістерського дослідження було виконано аналіз літературних джерел та науково-практичних публікацій згідно теми роботи, а саме:

- дано характеристику корпоративної мережі підприємства як базу для розгортання на її базі інфраструктури підприємства та розглянуто типові топології

таких мереж, а саме зіркоподібну топологію та змішану топологію на прикладі реального технологічного рішення;

- проведено детальний аналіз можливих відмов та несправностей корпоративних мереж, які спричинені як власними відмова, так і зловмисними діями, спрямованими на кібератак на вразливості системи; також дана класифікація таких вразливостей;

- проведено огляд відомих методів підвищення надійності та відмовостійкості корпоративних безпроводових мереж шляхом введення в структуру систему надлишкових елементів, використання алгоритмічних засобів живучості та резервування каналі доступу.

2 РОЗРОБКА МАТЕМАТИЧНА МОДЕЛЬ ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ

2.1 Узагальнена математична модель надійності вузла корпоративної мережі

Аналіз та розрахунок надійності корпоративної безпроводової мережі полягає у її декомпозиції з метою представлення складної системи у вигляді набору складових елементів з відновленням, які можуть перебувати в одному з двох станів: 0 – елемент працює та 1 – елемент відновлюється.

Позначимо через $Y_0\,(s,\,t)$ – ймовірність знаходження елементу в справному стані на проміжку $[t;\,t+s]$, а через $Y_1\,(\tau,\,t)$ – ймовірність того, що на проміжку $[t;\,t+\tau]$ даний елемент відновлюється.

Диференціюванням отримаємо відповідні щільності розподілу:

$$y_0(s,t) = -\frac{\P Y_0(s,t)}{\P s}$$
$$y_1(t,t) = -\frac{\P Y_1(t,t)}{\P t} \qquad (2.1)$$

де функція $y_0\,(s,\,t)$ – це щільність розподілу ймовірностей справної роботи елемента на проміжку $[t;\,t+s]$, $y_1\,(\tau,\,t)$ – щільність розподілу ймовірностей відновлення елемента на проміжку $[t;\,t+\tau]$.

Нехай в початковий момент часу $t = 0$ елемент знаходиться в справному стані, тоді

$$Y_0(s,0) = \bar{F}(s),\ Y_1(t,0) = 0 \qquad (2.2)$$

отже

$$y_0(s,0) = f(s),\ y_1(t,0) = 0 \qquad (2.3)$$

Введемо позначення: x - випадковий час справної роботи елементу;

h - випадковий час відновлення елементу;

t – момент часу за якого елемент справний;

x – довільний момент часу на проміжку від 0 до t;

t-x – момент завершення відновлення елементу, що відмовив;

s – час, протягом якого елемент справний.

Ймовірність справної роботи елемента протягом часу $x + s$ за умови, що в момент часу $t – x$ сталось відновлення, становить:

$$p = y_1(0, t - x) f(x + s) \qquad (2.4)$$

В результаті інтегрування на проміжку [0; t]отримуємо вираз:

$$y_0(s,t) = \int_0^t f(x+s) y_1(0, t - x)\, dx + f(t+s) \qquad (2.5)$$

де $f(t + s)$ відповідає початку процесу роботи та означає, що за відсутності відмови до моменту t елемент працює безвідмовно протягом часу $t + s$.

Аналогічне рівняння можна записати для функції $y_1(\tau, t)$ без вільного члена. Таким чином має місце наступна система інтегральних рівнянь відносно функцій y_0 та y_1:

$$\begin{cases} y_0(s,t) = \int_0^t f(x+s)\, y_1(0,t-x)\,dx + f(t+s) \\ y_1(t,t) = \int_0^t g(x+t)\, y_0(0,t-x)\,dx \end{cases} \qquad (2.6)$$

Система інтегральних рівнянь (2.6) пов'язує між собою дві функції, які містять у собі інформацію про попередні стани процесу елемента, що обумовлено наявністю в аргументах функцій y_0 та y_1 додаткових змінних s та τ, що відповідають залишковому часу роботи та відновлення.

У тому випадку, коли залишковий час роботи та відновлення рівний нулю, функціями $w(t) = y_0(0,t)$ та $w_B(t) = y_1(0,t)$ назвемо параметри потоку відмов та відновлення відповідно.

Введемо такі позначення: $j_s(t) = j(t+s)$. Тоді отримаємо:

$$\begin{aligned} y_0(s,t) &= w_B * f_s(t) + f_s(t) \\ y_1(t,t) &= w * g_t(t) \\ Y_0(s,t) &= w_B * \bar{F}_S(t) + \bar{F}_S(t) \\ Y_1(t,t) &= w * \bar{G}_t(t) \end{aligned} \qquad (2.7)$$

Із (2.7) можна виразити ймовірності Y_0 для малих s, а також Y_1 для малих τ через такі характеристики елемента як функція готовості та простоювання і параметри потоку відмов та відновлення:

$$\begin{aligned} Y_0(s,t) &= K_\Gamma(t) - w(t)s + o(s^2) \\ Y_1(t,t) &= K_\Pi(t) - w_B(t)t + o(t^2) \end{aligned} \qquad (2.8)$$

Тоді маємо:

$$K_Г(t) = Y_0(0,t) = \int_0^{\infty} y_0(s,t)\,ds$$
$$K_П(t) = Y_1(0,t) = \int_0^{\infty} y_1(t,t)\,dt \qquad (2.9)$$

Зробивши підстановку $s = 0$; $\tau = 0$ у вираз (2.7) отримаємо:

$$\begin{aligned} w(t) &= w_B * f(t) + f(t) \\ w_B(t) &= w * g(t) \end{aligned}, \qquad (2.10)$$

звідки слідує:

$$\begin{aligned} w(t) &= f(t) + f * f * g(t) + f * f * f * g * g(t) + \ldots \\ &= \sum_{k=0}^{\infty} f^{*(k+1)} * g^{*(k)}(t), \qquad (2.11) \\ w_B(t) &= f * f * g * g(t) + \ldots = \sum_{k=1}^{\infty} f^{*(k)} * g^{*(k)}(t) \end{aligned}$$

Очевидно, що функції готовності та простоювання співпадають із ймовірностями $p_0(t)$ та $p_1(t)$ – перебування елемента у справному стані та стані відмови. Ці ймовірності задовольняють рівнянням, які аналогічні до рівнянь Ерланга:

$$\begin{cases} p_0'(t) = -\lambda(t)\,p_0(t) + \mu(t)\,p_1(t) \\ p_1'(t) = \lambda(t)\,p_0(t) - \mu(t)\,p_1(t) \end{cases} \qquad (2.12)$$

де λ, μ – інтенсивність потоку відмов та відновлення.

Звідси слідує, що роботу елемента можна описати за допомогою найпростішого графу станів, із гілками якого співставлень функції λ та μ.

Система рівнянь (2.12) відповідає найпростішому такому графу, який з ображено на рисунку 2.1.

Рисунок 2.1 – Граф станів елементу, який підлягає відновленню

Функції p_0 та p_1 задовольняють початковим умовам $p_0(0) = 1$, $p_1(0) = 0$, що відповідає робочому стану елемента в момент $t = 0$.

Розв’язавши систему (2.6) можна знайти інтенсивності λ (t) та μ (t), або спочатку розв’язати систему (2.6) і вже на базі розв’язку обчислити відповідні інтенсивності.

Розглянута модель атомарного відновлювального елементу є масштабованою, що дозволяє розробити на її базі модель функціонування системи будь-якого рівня складності.

Нехай час безвідмовної роботи та час відновлення елементу мають експоненціальний розподіл з параметрами λ і μ відповідно. Аналітичні вирази для параметрів потоків відмов та відновлення, середньої кількості сумарних відмов та відновлень протягом часу [0; t], а також функцій готовності та простою, середнього напрацювання на відмову та часу відновлення в інтервалі [0; t] можна знайти наступним чином.

З виразу (2.10) для параметрів потоку відмов та відновлення зображення за Лапласом має вигляд:

$$\hat{w}(z)=\frac{\hat{f}(z)}{1-\hat{f}(z)\hat{g}(z)}=\frac{\lambda(z+\mu)}{z(z+\mu+\lambda)},$$
$$\hat{w}_B(z)=\frac{\hat{f}(z)\hat{g}(z)}{1-\hat{f}(z)\hat{g}(z)}=\frac{\lambda\mu}{z(z+\mu+\lambda)} \qquad (2.13)$$

звідки, повертаючись до оригіналу, отримуємо:

$$w(t)=\frac{\mu\lambda}{\mu+\lambda}+\frac{\lambda^2}{\mu+\lambda}e^{-(\mu+\lambda)t},$$
$$w_B(t)=\frac{\mu\lambda}{\mu+\lambda}-\frac{\mu\lambda}{\mu+\lambda}e^{-(\mu+\lambda)t} \qquad (2.14)$$

Середня сумарна кількість відмов та середня сумарна кількість відновлень протягом часу [0; t]:

$$M(t)=\int_0^t w(x)\,dx=\frac{\mu\lambda}{\mu+\lambda}t+\frac{\lambda^2}{(\mu+\lambda)^2}\left(1-e^{-(\mu+\lambda)t}\right),$$
$$M_B(t)=\int_0^t w_B(x)\,dx=\frac{\mu\lambda}{\mu+\lambda}t+\frac{\mu\lambda}{(\mu+\lambda)^2}\left(1-e^{-(\mu+\lambda)t}\right) \qquad (2.15)$$

Для функції готовності та функції простою зображення за Лапласом має вигляд:

$$\hat{K}_Г(z)=\frac{1-\hat{f}(z)}{z\left(1-\hat{f}(z)\hat{g}(z)\right)}=\frac{z+\mu}{z(z+\mu+\lambda)},$$
$$\hat{K}_П(z)=\frac{\hat{f}(z)\left(1-\hat{g}(z)\right)}{z\left(1-\hat{f}(z)\hat{g}(z)\right)}=\frac{\lambda}{z(z+\mu+\lambda)} \qquad (2.16)$$

Використовуючи обернене перетворення Лапласа, запишемо оригінали функцій:

$$K_{Г}(t)=\frac{m}{m+l}+\frac{l}{m+l}e^{-(m+l)t},$$
$$K_{П}(t)=\frac{l}{m+l}+\frac{l}{m+l}e^{-(m+l)t} \qquad (2.17)$$

Середній сумарний час безвідмовної роботи та середній сумарний час відновлення на проміжку часу [0; t]:

$$m(t)=\int_0^t K_{Г}(x)\,dx=\frac{m}{m+l}t+\frac{l}{(m+l)^2}\left(1-e^{-(m+l)t}\right),$$
$$m_{B}(t)=\int_0^t K_{П}(x)\,dx=\frac{l}{m+l}t+\frac{l}{(m+l)^2}\left(1-e^{-(m+l)t}\right) \qquad (2.18)$$

Співвідношення (2.18) справедливі для процесів із експоненціальним законом розподілу.

2.2 Характеристика моделі корпоративної мережі

Нехай, що дана корпоративна мережа складається з m елементів з відомими розподілами часу безвідмовної роботи та часу відновлення, а її функціонування відбувається відповідно до визначеної схеми розрахунку надійності. Усі елементи умовно поділяються на робочі та резервні. До першого класу віднесемо також всі елементи навантаженого та полегшеного резерву, а до другого – лише елементи, які перебувають у ненавантаженому стані. При відмові робочого елемента і наявності резервного він замінюється резервним, причому ця заміна виконується миттєво і

абсолютно надійним пристроєм. Обмеження щодо миттєвої заміни можна скасувати. При наявності кількох резервних елементів порядок заміни відмовленого робочого елемента резервним вважатиметься відомим. Контроль стану елементів є постійним, і відмова будь-якого елемента виявляється негайно після її виникнення. Однак ця умова також може бути скасована. Передбачається, що можливість засобів відновлення і порядок відновлення елементів відомі, тобто регламентованим вважається послідовність прийняті на обслуговування. Останній факт важливий у випадку обмеженого відновлення коли може виникнути черга на відновлення. Відновлення елемента розпочинається одразу після його відмови або після виявлення відмови контролюючим пристроєм при наявності вільного ресурсу засобу відновлення, відповідно до прийнятого пріоритету обслуговування. Під час ремонту елементів відбувається повне відновлення їхньої надійності.

На функціонування та обслуговування кожного елемента можуть впливати інші елементи системи. У зв’язку з цим кожен елемент може перебувати в кількох можливих станах: -у робочому стані, у стані відновлення або у стані простою. При цьому стан простою елемента може бути обумовлений наступними причинами:

- відбулося переривання роботи елемента, що може статися, якщо цей елемент знаходиться в складі вузла, який послідовно пов’язаний з елементом або вузлом, що відмовив;
- відбулося переривання відновлення елемента, що може статися, якщо у разі застосування регламенту відновлення з пріоритетами, що може передбачати переривання відновлення;
- елемент справний, але за умовами функціонування він знаходиться в черзі на роботу, що може статися, наприклад, у випадку ненавантаженого резервування;
- елемент перебуває в стані відмови, але за умовами обслуговування його не ремонтують і він перебуває в черзі на відновлення, що можливо, наприклад, у випадку обмеженого відновлення з прямим або визначеним пріоритетом.

Визначення можливих станів кожного елемента системи є важливим при описі її функціонування в цілому. Вважатимемо, що перехід кожного елемента з одного стану в інший відбувається миттєво внаслідок відмови або відновлення даного елемента чи будь-якого іншого елемента системи. Додатково припустимо, що відмова чи відновлення будь-якого елемента не впливає на закони розподілу інших елементів, і час простою елемента (якщо це не вказано окремо) не впливає на його характеристики надійності, тобто перебуваючи в стані простою, елемент зберігає ці характеристики такими ж, як у момент переривання роботи або відновлення.

2.3 Формальна модель станів корпоративної мережі

Представимо множину усіх станів деякої корпоративної телекомунікаційної мережі через *E*, а через *n* – кількість цих станів. Відповідно до визначення відмови елементу, розділимо стани системи на два класи станів: підмножину робочих елементів та підмножину елементів, які зазнали відмов:

$$E = \{E_+ \cup E_-\} \tag{2.19}$$

де E_+ - множина робочих станів;

E_- - множина станів відмов.

В кожен фіксований момент часу *t* для кожного *k*-го стану ($k = 1 \ldots n$) виділимо такі підмножини елементів:

$$E_k = \{R_k, W_k, R_k^{\cdot}, W_k^{\cdot}, R_k^0, W_k^0\} \tag{2.20}$$

R_k – множина номерів елементів, які працюють,

W_k – множина номерів елементів, які відновлюються в даний момент часу;

R_k' - множина номерів елементів, які простоюють в результаті переривання їхньої роботи;

W_k' - множина номерів елементів, які простоюють в результаті переривання їхнього відновлення;

R_k^0 – множина номерів елементів, які складають чергу на роботу;

W_k^0 – множина номерів елементів, які складають чергу на відновлення;

Для кожного k-го стану визначимо вектор, який характеризує стан усіх елементів в момент часу t:

$$A_k = \{a_{1k}, a_{2k}, ..., a_{mk}\} \tag{2.21}$$

з компонентами:

$$a_{ik} = \begin{cases} s_i, \text{якщо} \quad i \in R_k \\ t_i, \text{якщо} \quad i \in W_k \\ 0, \text{якщо} \quad i \in R_k^0 \cup W^0{}_k \end{cases} \tag{2.22}$$

Отже, функціонування будь-якої відновлювальної системи повністю описати матрицею станів S, розмірності $m \times n$, стовпцями якої є вектори A_k.

Висновки до другого розділу

В другому розділі магістерського дослідження було виконано наступне:

- розроблена узагальнена математична модель надійності вузла корпоративної мережі;
- дано характеристики моделі корпоративної мережі;

- розроблено формальну модель станів корпоративної мережі;
- розглянуто корпоративну мережу, що складається з елементів з відомими розподілами часу безвідмовної роботи та часу відновлення. Функціонування мережі відбувається згідно з визначеною схемою розрахунку надійності, де всі елементи поділені на робочі та резервні;
- розглянуто можливі стани елементів у системі, визначено їх можливі причини і формально представлено множину усіх станів корпоративної мережі. Для опису функціонування системи використано матрицю станів, де вектори характеризують стан усіх елементів в конкретний момент часу.

3 РОЗРОБКА ВІДМОВОСТІЙКОЇ СИСТЕМИ РЕЗЕРВУВАННЯ СЕРВЕРНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ ЗАСОБІВ ВІРТУАЛІЗАЦІЇ

3.1 Розробка моделі резервування серверного забезпечення корпоративної мережі

Представимо локальні сервери корпоративної мережі підприємства у вигляді відновлювальної системи із ковзним резервуванням елементів. Схема такої системи показана на рисунку 3.1. Вузли системи представлені фізичними серверами (кластер) на базі яких розгорнута інфраструктура віртуалізації VMware ESXI [37]. Кожен сервер керується гіпервізором, на якому запущені віртуальні машини різного призначення: умово розділені за функціональним призначенням на сервер бази даних (БД) та сервери прикладних додатків.

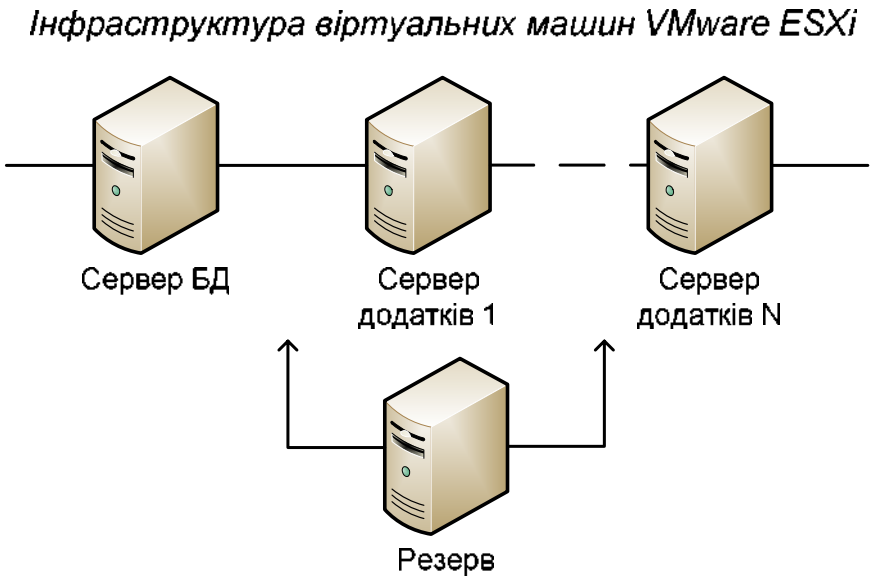


Рисунок 3.1 – Схема ковзного резервування серверів підприємства

Серед усіх компонентів сервера виділимо ключові компоненти – такі, вихід з ладу кожного з яких призводить до непрацездатності (відмови) сервера.

Нехай в даній конфігурації сервер БД, сервер додатків та резервний сервер є системою із ковзним резервуванням кратністю 0,5.

Середній час напрацювання на відмову та час відновлення для кожного із серверів подано в таблиці 3.1.

Таблиця 3.1 – Параметри надійності та відновлення серверів

№	1	2	3
Назва	Сервер БД	Сервер додатків	Резерв
Середній час напрацювання на відмову, год	8760	4380	2190
Середній час відновлення, год	1	1	1
Інтенсивність відмов λ, год$^{-1}$	$1{,}1416 \cdot 10^{-4}$	$2{,}2831 \cdot 10^{-4}$	$4{,}5662 \cdot 10^{-4}$
Інтенсивність відновлення μ, год$^{-1}$	1	1	1

Відновлення працездатності системи покладено на систему резервного копіювання та відновлення, яка реалізується відповідним спеціалізованим програмним забезпеченням.

Подамо процес функціонування системи у вигляді графу станів, який зображено на рисунку 3.2. Вершини графу відповідають стану системи від 0 до 11. Номери елементів, що відмовили показано поряд із вершинами 6-11. Наприклад, число «1»

відповідає відмові першого елементу і роботу другого та третього елементів. В такому разі після відновлення першого елементу система перейде у стан, коли усі елементи справні, однак працюватимуть лише елементи «2» та «3».

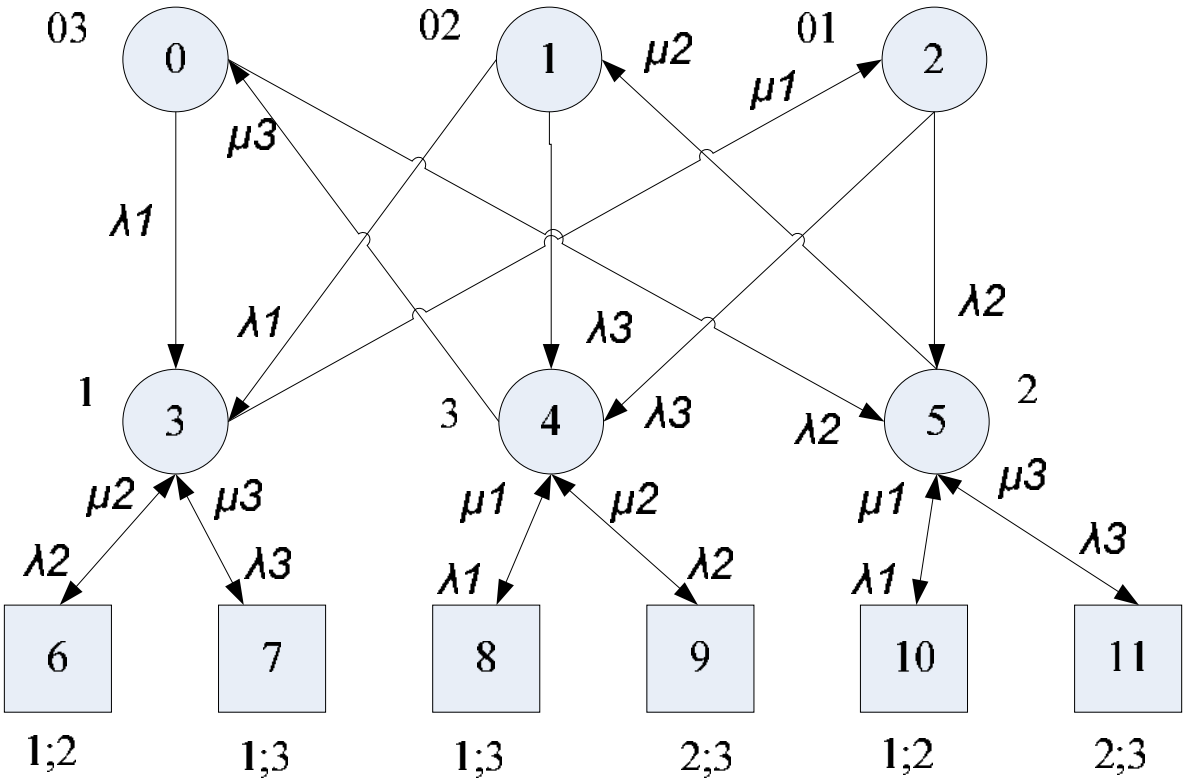


Рисунок 3.2 – Граф станів системи ковзного резервування серверів

Функціональні стани системи, які відповідають справній роботі усіх елементів розміщені на нульовому рівні моделі:

- стан 03: працює перший та другий елементи, третій елемент перебуває у резерві;

- стан 02: працює перший та третій елементи, другий елемент перебуває у резерві;

- стан 01: працює другий та третій елементи, перший елемент перебуває у резерві.

Стани найнижчого рівня моделі відповідають відмовам системи. Згідно прийнятої стратегії обслуговування перехід з даних станів можливий лише до станів рівнем вище.

Проведемо аналіз надійності системи та знайдемо стаціонарні показники надійності.

3.2 Розрахунок стаціонарних показників надійності системи резервування серверів корпоративної мережі

Для даної моделі система лінійних алгебраїчних рівнянь відносно стаціонарних ймовірностей p_i, (i = 0; 1; …11) має такий вигляд:

$$\begin{cases} -(\lambda_1+\lambda_2)p_0+\mu_3 p_4=0 \\ -(\lambda_1+\lambda_3)p_1+\mu_2 p_5=0 \\ -(\lambda_1+\lambda_3)p_2+\mu_1 p_3=0 \\ \lambda_1 p_0+\lambda_1 p_0-(\mu_1+\lambda_2+\lambda_3)p_3+\mu_2 p_6+\mu_3 p_7=0 \\ \lambda_3 p_1+\lambda_3 p_2-(\mu_3+\lambda_1+\lambda_2)p_4+\mu_1 p_8+\mu_2 p_9=0 \\ \lambda_2 p_0+\lambda_2 p_2-(\mu_2+\lambda_1+\lambda_3)p_5+\mu_1 p_{10}+\mu_3 p_{11}=0 \\ \lambda_2 p_3-\mu_2 p_6=0 \\ \lambda_3 p_3-\mu_3 p_7=0 \\ \lambda_1 p_4-\mu_1 p_8=0 \\ \lambda_2 p_4-\mu_2 p_9=0 \\ \lambda_1 p_5-\mu_2 p_{10}=0 \\ \lambda_3 p_5-\mu_3 p_{11}=0 \end{cases} \quad (3.1)$$

Умова нормування:

$$\sum_{i=0}^{11} p_i = 1 \qquad (3.2)$$

Розв’язавши систему (3.1) у урахуванням умови (3.2) отримуємо значення стаціонарних ймовірностей (таблиця 3.2).

Таблиця 3.2 – Стаціонарні ймовірності системи

p_0	0.5712	p_6	$2.2329 \cdot 10^{-8}$
p_1	0.2856	p_7	$4.4659 \cdot 10^{-8}$
p_2	0.1428	p_8	$2.2329 \cdot 10^{-8}$
p_3	$9.7803 \cdot 10^{-5}$	p_9	$4.4659 \cdot 10^{-8}$
p_4	$1.9561 \cdot 10^{-4}$	p_{10}	$1.8608 \cdot 10^{-8}$
p_5	$1.6300 \cdot 10^{-4}$	p_{11}	$7.4431 \cdot 10^{-8}$

Коефіцієнт готовності системи дорівнює сумі ймовірностей робочих станів системи (1-5):

$$K_Г = \sum_{i=0}^{5} p_i = 0{,}99999977 .$$

Параметр потоку відмов:

$$w = (\lambda_2 + \lambda_3) p_3 + (\lambda_1 + \lambda_2) p_4 + (\lambda_1 + \lambda_3) p_5 = 2{,}2702 \times 10^{-7} \text{ (год}^{-1}\text{)}$$

Час напрацювання на відмову:

$$T_{відмов} = \frac{K_Г}{w} = 4\ 404\ 988 \text{ (год).}$$

Середній час відновлення:

$$T_{відновлн.} = \frac{1 - K_Г}{w} = 0{,}99999999956 \text{ (год)}$$

3.3 Розрахунок перехідних характеристик надійності системи резервування серверів корпоративної мережі

Нижче наведено код на мові Matlab для розрахунку показників надійності системи резервування:

```
clear;

% A x P = E
global l  m;

%l = [0.04, 0.08, 0.1];
%m = [2, 1, 4];

L1 = 1.*365.*24;
L2 = 0.5.*365.*24;
L3 = 0.25.*365.*24;
M1 = 1;
M2 = 1;
M3 = 1;
```

```
l = [1./L1, 1./L2, 1./L3];
m = [1./M1, 1./M2, 1./M3];

E = zeros(12,1);
E(1,1) = 1;
A = zeros(12);


% eq. 1
%A(1,1) = -(l(1) + l(2));
%A(1,5) = m(3);

A(1,:) = 1;

% eq. 2
A(2,2) = -(l(1) + l(3));
A(2,6) = m(2);
% eq. 3
A(3,3) = -(l(2) + l(3));
A(3,4) = m(1);
% eq. 4
A(4,1) = l(1);
A(4,2) = l(1);
A(4,4) = -(m(1) + l(2) + l(3));
A(4,7) = m(2);
A(4,8) = m(3);
% eq. 5
```

```
A(5,2) = l(3);
A(5,3) = l(3);
A(5,5) = -(m(3) + l(1) + l(2));
A(5,9) = m(1);
A(5,10) = m(2);
% eq. 6
A(6,1) = l(2);
A(6,3) = l(2);
A(6,6) = -(m(2) + l(1) + l(3));
A(6,11) = m(1);
A(6,12) = m(3);
% eq. 7
A(7,4) = l(2);
A(7,7) = -m(2);
% eq. 8
A(8,4) = l(3);
A(8,8) = -m(3);
% eq. 9
A(9,5) = l(1);
A(9,9) = -m(1);
% eq. 10
A(10,5) = l(2);
A(10,10) = -m(2);
% eq. 11
A(11,6) = l(1);
A(11,11) = -m(1);
% eq. 12
A(12,6) = l(3);
```

```
A(12,12) = -m(3);


P = A^(-1) * E;

K = sum(P(1:6));
w = (l(2) + l(3)) .* P(4) + ...
(l(1) + l(2)) .* P(5) + ...
(l(1) + l(3)) .* P(6);

T = K ./ w;

Tv = (1 - K) ./ w;

tspan = [0:10000:L2.*10];
p0 = zeros(12,1);
p0(1) = 1;
[t,p] = ode45(@odefun1,tspan,p0);
figure;plot(t, p, LineWidth=2); grid on
xlabel('t, год.')
ylabel('Ймов.')
legend({'p_0(t)','p_1(t)','p_2(t)','p_3(t)','p_4(t)'})



Kg = sum(p(:,1:6),2);

p0 = zeros(6,1);
```

```
p0(1) = 1;
[t,p] = ode45(@odefun2,tspan,p0);
%figure;plot(t, p)
Pt = sum(p,2);

figure; plot(t,Kg,t,Pt,LineWidth=2);grid on
xlabel('t, год.')
ylabel('Ймов.')
legend({'K_г(t)','P(t)'})



H = zeros(6,1);
H(1,1) = -1;
B = zeros(6);

%eq.1
B(1,1) = -(l(1) + l(2));
B(1,5) = m(3);
%eq.2
B(2,2) = -(l(1) + l(3));
B(2,6) = m(2);
%eq.3
B(3,3) = -(l(2) + l(3));
B(3,4) = m(1);
%eq.4
B(4,1) = l(1);
B(4,2) = l(1);
```

```
    B(4,4) = -(m(1) + l(2) +l(3));
    %eq.5
    B(5,2) = l(3);
    B(5,3) = l(3);
    B(5,5) = -(m(3) + l(1) +l(2));
    %eq.6
    B(6,1) = l(2);
    B(6,3) = l(2);
    B(6,6) = -(m(2) + l(1) +l(3));

    tau = B^(-1) * H;
    T1 = sum(tau);

    function dpdt = odefun1(t,p)
    global l  m;

    dpdt(1,1) = -(l(1) + l(2)) .* p(1) + m(3) .* p(5);
    dpdt(2,1) = -(l(1) + l(3)) .* p(2) + m(2) .* p(6);
    dpdt(3,1) = -(l(2) + l(3)) .* p(3) + m(1) .* p(4);
    dpdt(4,1) = l(1) .* p(1) + l(1) .* p(2) - ...
    (m(1) + l(2) + l(3)) .* p(4) + m(2) .* p(7) + m(3) .*
p(8);
    dpdt(5,1) = l(3) .* p(2) + l(3) .* p(3) - ...
    (m(3) + l(1) + l(2)) .* p(5) + m(1) .* p(9) + m(2) .*
p(10);
    dpdt(6,1) = l(2) .* p(1) + l(2) .* p(3) - ...
    (m(2) + l(1) + l(3)) .* p(6) + m(1) .* p(11) + m(3) .*
p(12);
```

```
dpdt(7,1) = l(2) .* p(4) - m(2) .* p(7);
dpdt(8,1) = l(3) .* p(4) - m(3) .* p(8);
dpdt(9,1) = l(1) .* p(5) - m(1) .* p(9);
dpdt(10,1) = l(2) .* p(5) - m(2) .* p(10);
dpdt(11,1) = l(1) .* p(6) - m(1) .* p(11);
dpdt(12,1) = l(3) .* p(6) - m(3) .* p(12);
end

function dpdt = odefun2(t,p)
global l  m;

dpdt(1,1) = -(l(1) + l(2)) .* p(1) + m(3) .* p(5);
dpdt(2,1) = -(l(1) + l(3)) .* p(2) + m(2) .* p(6);
dpdt(3,1) = -(l(2) + l(3)) .* p(3) + m(1) .* p(4);
dpdt(4,1) = l(1) .* p(1) + l(1) .* p(2) - ...
(m(1) + l(2) + l(3)) .* p(4);
dpdt(5,1) = l(3) .* p(2) + l(3) .* p(3) - ...
(m(3) + l(1) + l(2)) .* p(5);
dpdt(6,1) = l(2) .* p(1) + l(2) .* p(3) - ...
(m(2) + l(1) + l(3)) .* p(6);

end
```

Для знаходження функції готовності системи $f = K_{\Gamma}(t)$ складемо систему лінійних диференціальних рівнянь відносно перехідних ймовірностей $p_i(t)$, $i = 0; 1…11$:

$$
\begin{cases}
\dfrac{dp_0}{dt} = -(\lambda_1 + \lambda_2)\, p_0 + \mu_3 p_4 \\
\dfrac{dp_1}{dt} = -(\lambda_1 + \lambda_3)\, p_1 + \mu_2 p_5 \\
\dfrac{dp_2}{dt} = -(\lambda_2 + \lambda_3)\, p_2 + \mu_1 p_3 \\
\dfrac{dp_3}{dt} = \lambda_1 p_0 + \lambda_1 p_1 - (\mu_1 + \lambda_2 + \lambda_3)\, p_3 + \mu_2 p_6 + \mu_3 p_7 \\
\dfrac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3 + \lambda_1 + \lambda_2)\, p_4 + \mu_1 p_8 + \mu_2 p_9 \\
\dfrac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3 + \lambda_1 + \lambda_2)\, p_4 + \mu_1 p_8 + \mu_2 p_9 \\
\dfrac{dp_5}{dt} = \lambda_2 p_0 + \lambda_2 p_2 - (\mu_2 + \lambda_1 + \lambda_3)\, p_5 + \mu_1 p_{10} + \mu_3 p_{11} \\
\dfrac{dp_6}{dt} = \lambda_2 p_3 + \mu_2 p_6 \\
\dfrac{dp_7}{dt} = \lambda_3 p_3 + \mu_3 p_7 \\
\dfrac{dp_8}{dt} = \lambda_1 p_4 + \mu_1 p_8 \\
\dfrac{dp_9}{dt} = \lambda_2 p_4 + \mu_2 p_9 \\
\dfrac{dp_{10}}{dt} = \lambda_1 p_5 + \mu_1 p_{10} \\
\dfrac{dp_{11}}{dt} = \lambda_3 p_5 + \mu_3 p_{11}
\end{cases}
\qquad (3.3)
$$

Розв’язок системи (3.3) – функції перехідних ймовірностей – зображено на рисунку 3.3.

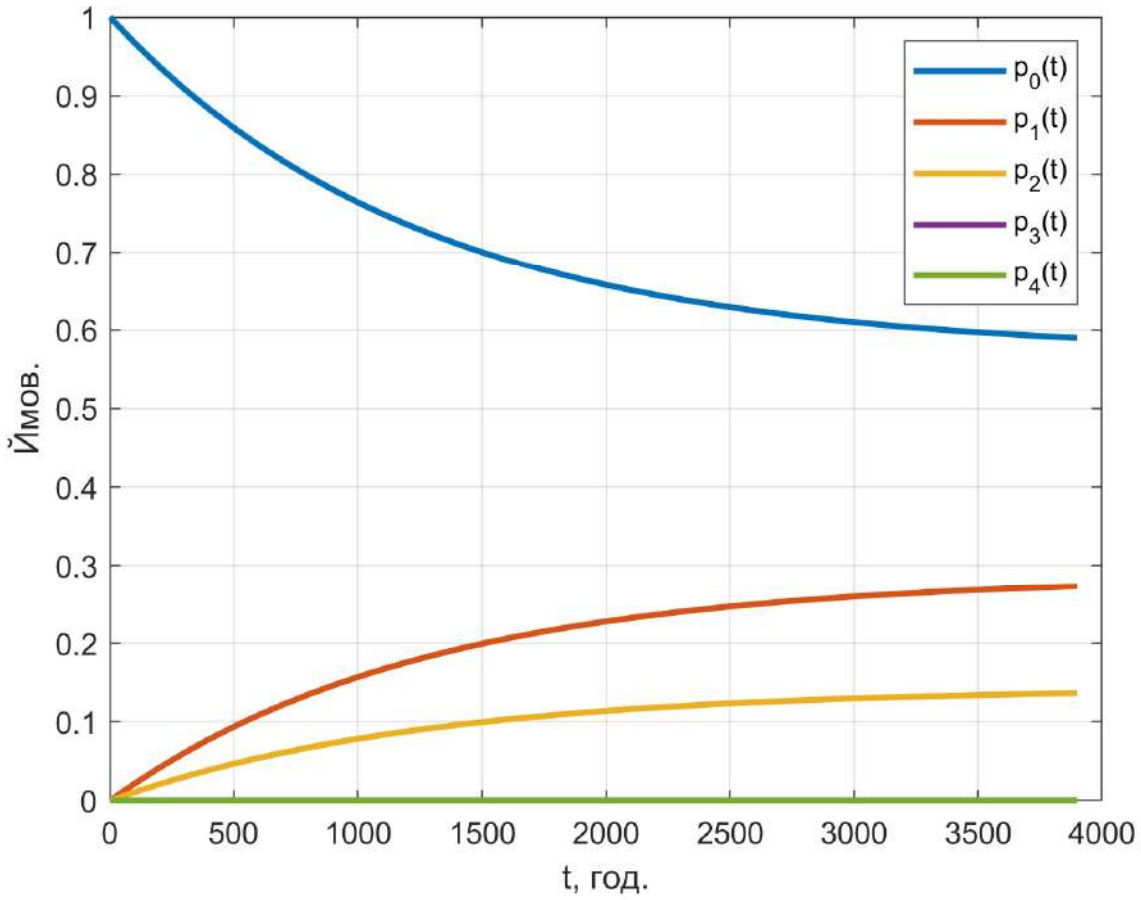


Рисунок 3.3 – Перехідні ймовірності станів системи

Як видно з рисунку 3.3, готовність системи визначається в переважній більшості лише функціями $p_{0\text{-}3}(t)$.

Визначимо функцію готовності системи як суму функцій перехідних ймовірностей, які відповідають справним станам системи:

$$K_Г(t) = \sum_{i=0}^{5} p_i(t) \qquad (3.4)$$

Ймовірність безвідмовної роботи знайдемо з перехідних ймовірностей, які розраховуються із відповідної системи диференціальних рівнянь, що були складені на основі вихідного графу станів (рисунок 3.2) для якого заборонені переходи зі станів відмов. Дана система диференціальних рівнянь має вигляд:

$$\begin{cases} \dfrac{dp_0}{dt} = -(\lambda_1+\lambda_2)p_0 + \mu_3 p_4 \\ \dfrac{dp_1}{dt} = -(\lambda_1+\lambda_3)p_1 + \mu_2 p_5 \\ \dfrac{dp_2}{dt} = -(\lambda_2+\lambda_3)p_2 + \mu_1 p_3 \\ \dfrac{dp_3}{dt} = \lambda_1 p_0 + \lambda_1 p_1 - (\mu_1+\lambda_2+\lambda_3)p_3 + \mu_2 p_6 + \mu_3 p_7 \\ \dfrac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3+\lambda_1+\lambda_2)p_3 \\ \dfrac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3+\lambda_1+\lambda_2)p_4 \\ \dfrac{dp_5}{dt} = \lambda_2 p_0 + \lambda_2 p_2 - (\mu_2+\lambda_1+\lambda_3)p_5 \end{cases} \qquad (3.5)$$

Розв’язком системи (3.5) є відповідні функції ймовірностей, підсумовуючи які функцію безвідмовної роботи системи:

$$P(t) = \sum_{i=0}^{5} p_i(t) \qquad (3.6)$$

Функція функцію готовності системи $K_\Gamma(t)$ та функція безвідмовної роботи $P(t)$ зображені на рисунку 3.4.

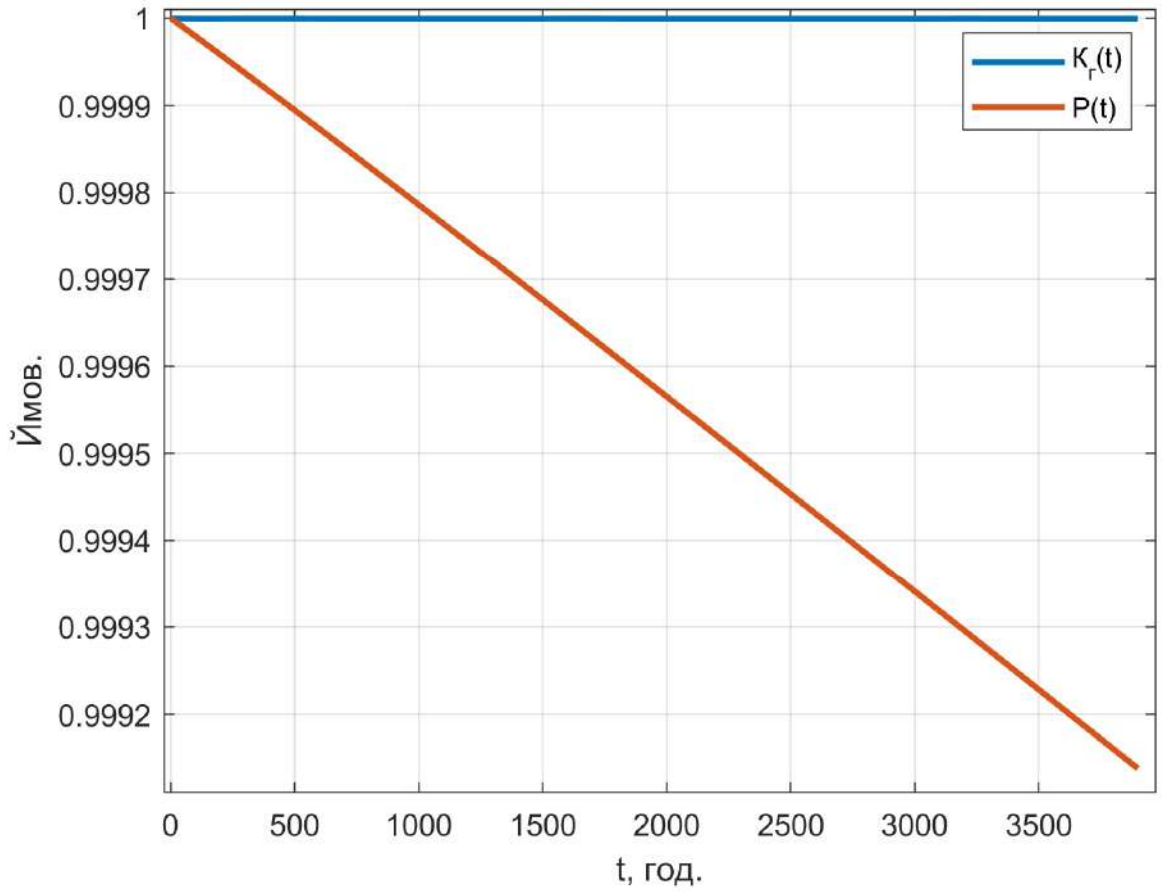


Рисунок 3.4 – Функція готовності системи $K_{\Gamma}(t)$ та функція безвідмовної роботи $P(t)$

Порівнюючи ймовірність безвідмовної роботи із функцією готовності , остання практично рівна одиниці, отже готовність системи може бути оцінена за допомогою коефіцієнту готовності.

Розрахуємо середній час безвідмовної роботи системи шляхом розв’язання системи лінійних алгебраїчних рівнянь відносно часу перебування у справному стані для системи, що відповідає виправленому графу станів (рисунок 3.2), для якого заборонені виходи із станів відмов. Система рівнянь має вигляд:

$$\begin{cases} -(\lambda_1+\lambda_2)t_0+\mu_3 p_4=-1 \\ -(\lambda_1+\lambda_3)t_1+\mu_2 p_5=0 \\ -(\lambda_2+\lambda_3)t_2+\mu_1 p_3=0 \\ \lambda_1 t_0+\lambda_1 t_1-(\mu_1+\lambda_2+\lambda_3)t_3=0 \\ \lambda_3 t_1+\lambda_3 t_2-(\mu_3+\lambda_1+\lambda_2)t_4=0 \\ \lambda_2 t_0+\lambda_2 t_2-(\mu_2+\lambda_1+\lambda_3)t_5=0 \end{cases} \quad (3.7)$$

Таблиця 3.3 – Середній час перебування системи в справних станах

τ_0	2518327 год	τ_3	431 год
τ_1	1258210 год	τ_4	861 год
τ_2	628992 год	τ_5	718 год

Отже, середній час безвідмовної роботи системи становить:

$$T_c=\sum_{i=0}^{5} t_i = 4\,407\,538 \text{ (год)} \quad (3.8)$$

Висновки до третього розділу

В третьому розділі магістерської роботи було виконано наступне:

- розроблено модель ковзного резервування для серверів корпоративної мережі, побудовано граф стані моделі

- розраховано стаціонарні показники надійності системи: стаціонарні ймовірності системи, стаціонарний коефіцієнт готовності та середній час відновлення

- розраховано перехідні характеристики: перехідні ймовірності системи, функція готовності та функція ймовірності безвідмовної роботи

4 РОЗРОБКА ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Встановлення та налаштування гіпервізора VMware ESXi

Програмне забезпечення VMware vSphere [37] – це платформа віртуалізації VMware, яка перетворює центри обробки даних на об'єднану обчислювальну інфраструктуру, яка включає центральний процесор (ЦП), сховище та мережеві ресурси. Середовище vSphere керує цими інфраструктурами як уніфікованим операційним середовищем і надає користувачеві інструменти для адміністрування центрів обробки даних, які беруть участь у цьому середовищі.

На рисунку 4.1 показана структурна схема екосистеми vSphere.

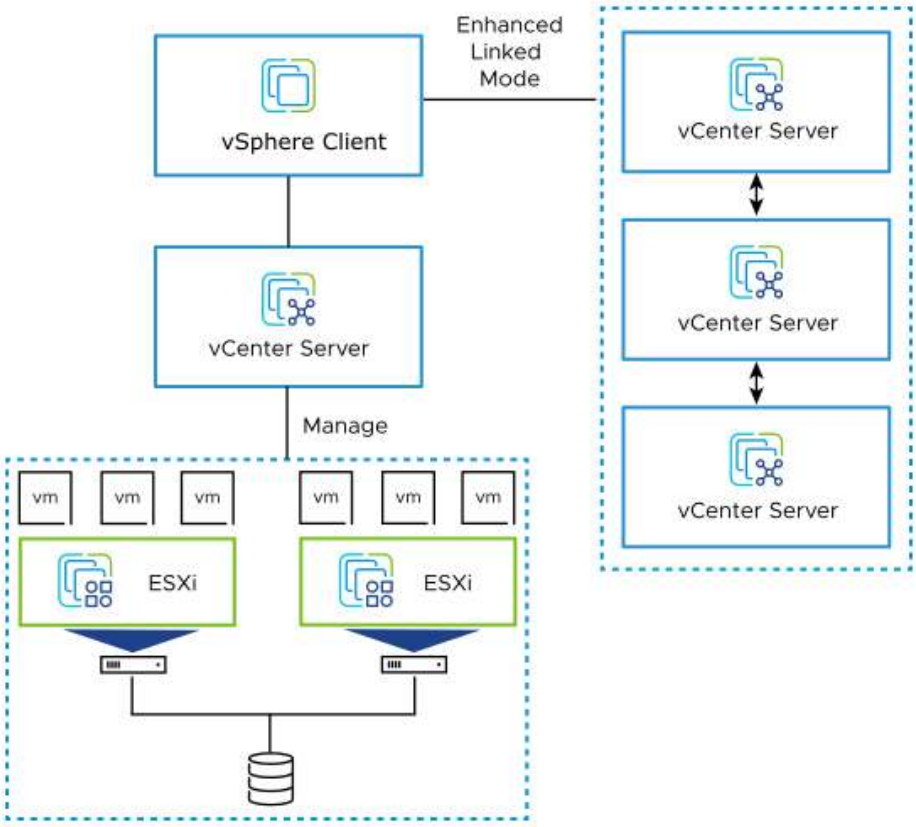


Рисунок 4.1 – Структурна схема екосистеми vSphere.

Двома основними компонентами vSphere є ESXi і vCenter Server . Система ESXi – це платформа віртуалізації, яка надає можливості створення та запуску віртуальних машин та віртуальних пристроїв. Сервер vCenter – це служба, за допомогою якої адміністратор системи керуєте кількома хостами, підключеними до мережі, і розподіляє ресурси машин-хостів [37].

В таблиці 4.1 наведені мінімальні та рекомендовані технічні вимоги для встановлення гіпервізора VMware vSphere.

Таблиця 3.1 – Технічні вимоги для встановлення гіпервізора VMware vSphere

	Мінімальні вимоги	Рекомендовані вимоги
процесор	1 процесор, 2 ядра	два процесори, чотири і більше ядер на ЦП
оперативна пам’ять	4 ГБ	8 Гбайт або більше
Мережа	один мережевий адаптер 1 Гбіт/с	два мережеві адаптери 1 Гбіт/с
Локальне сховище даних (SATA/SAS)	один диск ємністю 10 Гбайт	RAID 1 із 2=х дисків по 10 Гб.

Для встановлення гіпервізора необхідно завантажити ISO образ з офіційного вебсайту [38] . Даний ISO файл дистрибутива VMware vSphere Hypervisor має невеликий розмір (близько 630 МБ) і містить лише необхідні драйвери, в основному для серверів брендових виробників. Часто виробники серверів випускають власні дистрибутиви гіпервізора зі своїми драйверами.

Для встановлення гіпервізора необхідно записати ISO образ системи на файловий носій та завантажити робочу станцію з цього носія. Після завантаження користувач побачить вікно запрошення майстра встановлення (рисунок 4.2).

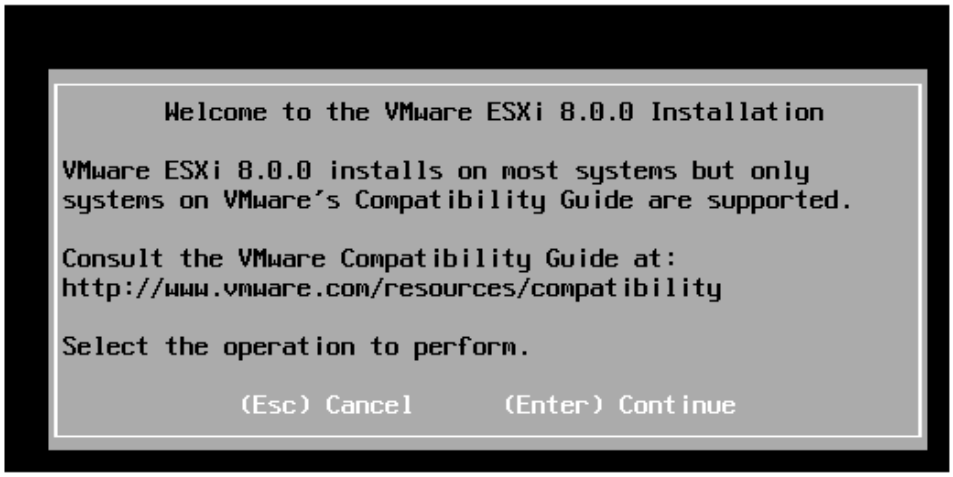


Рисунок 4.2 – Початок встановлення гіпервізора ESXi

Процес встановлення гіпервізора представлений послідовністю кроків:

1. Підтвердження початку інсталяції (див. рисунок 4.2).

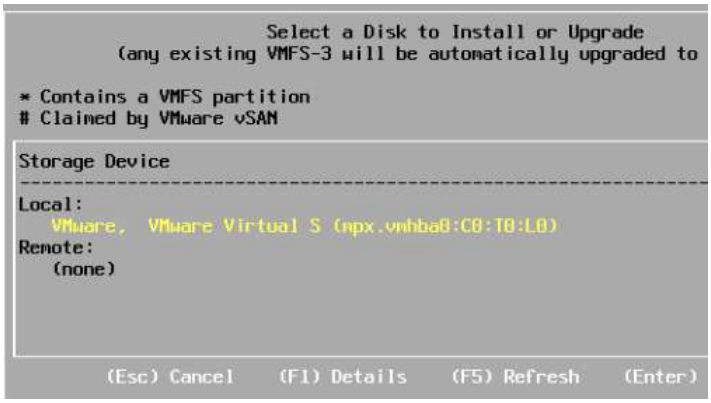
2. Вибір локального диску для встановлення на нього системи гіпервізора. Згідно рекомендацій розмір диску має бути щонайменше 10 Гб.

3. Далі система запропонує вибрати розкладку клавіатури та ввести надійний пароль адміністратора.

4. По завершенню інсталяції майстер встановлення запропонує витягти носій з образом ISO та перезавантажити систему.

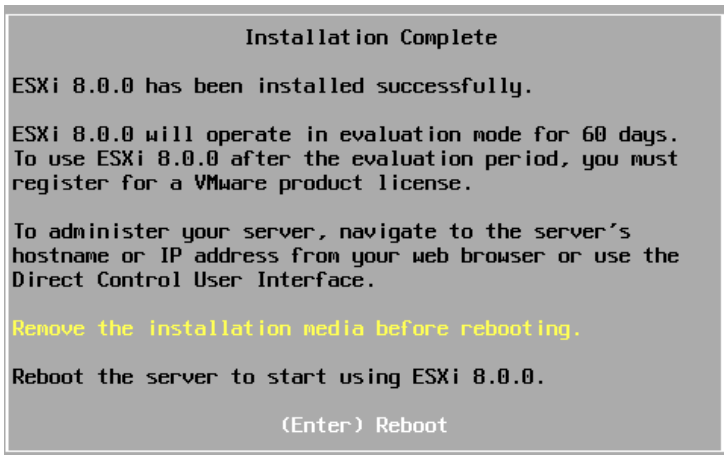
Варто зауважити, що для повноцінної роботи гіпервізора процесор має підтримувати апаратні інструкції віртуалізації. У разі несумісності процесора система видасть помилку: Unsupported CPU: CPU_SUPPORT_ERROR: CPU в цьому комп'ютері не підтримується ESXI 8.0.0.

У тестовому середовищі можна ігнорувати сумісність CPU за допомогою параметра allowLegacyCPU=true.



а)

б)



в)

Рисунок 4.3 – процес встановлення гіпервізора ESXi:
вибір локального диску для розміщення системи (а); введення надійного паролю адміністратора (б); завершення інсталяції (в)

Після успішного встановлення та перенавантаження системи гіпервізора готовий до роботи та подальших налаштувань. За замовчування ESXi сконфігурований на автоматичне отримання IP-адреси через DHCP. Для додаткових налаштувань необхідно перейти у відповідне конфігураційне меню за допомогою клавіші F2 та ввести облікові дані.

У розділі Troubleshooting Mode можна: увімкнути SSH доступ до хоста VMware , налаштувати таймаути, перезапустити агенти керування ESXi.

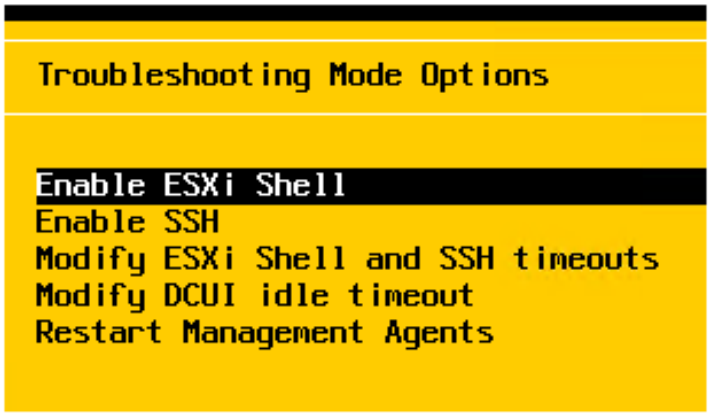


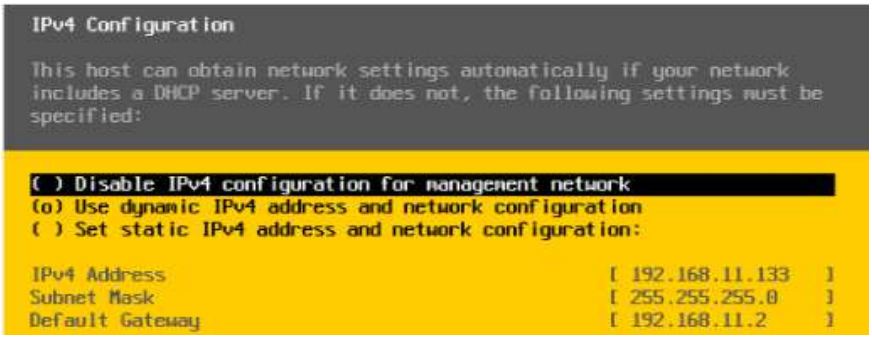
Рисунок 4.4 – Меню Troubleshooting Mode

В цьому меню, зокрема можна змінити мережеві налаштування, облікові дані користувачів системою та провести базове тестування працездатності мережі (рисунок 4.5).

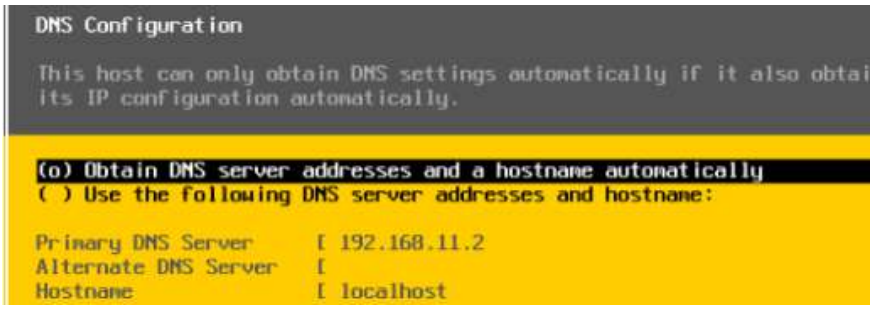
В меню DNS Configuration можна вказати primary та secondary DNS сервера та задати ім’я хоста (рисунок 4.5, в)

У меню Test Management Network можна перевірити роботу мережі (командою ping) та роботу DNS.

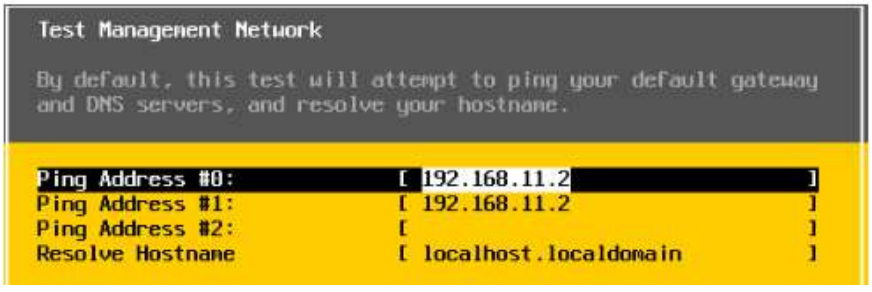
а)



б)



в)



г)

Рисунок 4.5 – Меню мережевих налаштувань інтерфейсі ESXi: налаштування мережі IPv4 (а, б); налаштування служби DNS (в); тестування мереж – ping (г)

Наступним кроком є підключення та подальше налаштування гіпервізора через Веб-інтерфейс Host Client – основний інтерфейс керування VMware Hypervisor. Для цього, відкрийте браузер на своєму комп'ютері та введіть в адресний рядок IP адресу вашого хоста ESXi та ввести облікові дані (рисунок 4.6).

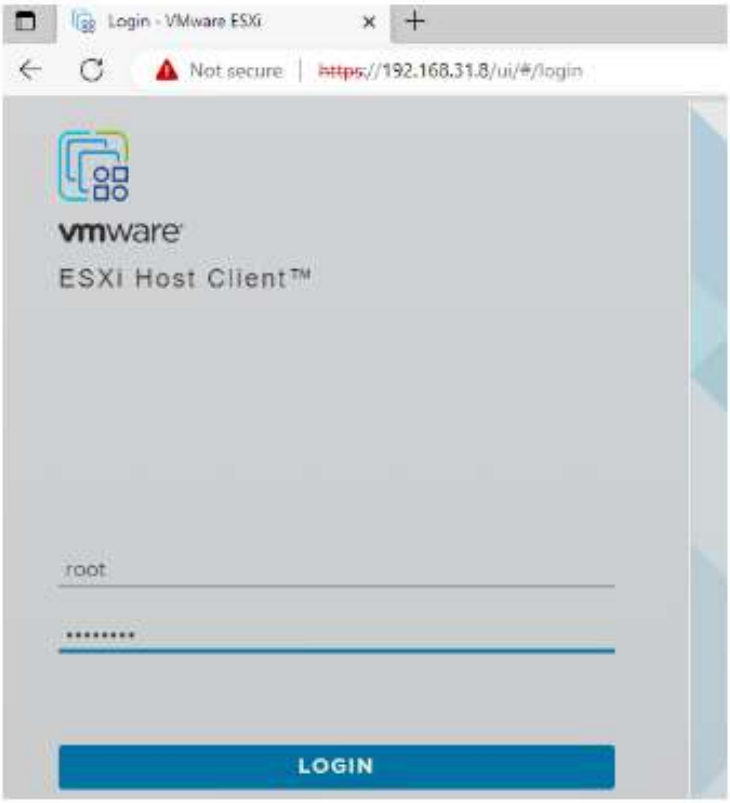


Рисунок 4.6 - Веб-інтерфейс керування VMware Hypervisor

У розділі Networking можна управляти віртуальними мережами. Одне з базових понять Hypervisor – віртуальний комутатор.

Віртуальний комутатор (vSphere Switch або vSwitch) – це віртуальний пристрій, який передає дані між віртуальними машинами всередині сервера та передає дані назовні через фізичний NIC. Є два види віртуальних комутаторів:

1) Standard Switches - простий віртуальний комутатор, що логічно знаходиться всередині фізичного сервера.

2) Distributed Switches – розподілений віртуальний комутатор, може бути поширений на кілька фізичних серверів (не доступний у безкоштовній версії VMWare Hypervisor, та й у платній редакції VMWare vSphere доступний лише в Enterprise Plus редакції) .

У ESXi за умовчанням вже створено один віртуальний комутатор vSwitch0 , який включає один фізичний адаптер vmnic0 і дві групи портів - службова (Management Network) для управління гіпервізором і мережа для передачі даних (VM Network). Інтерфейс керування гіпервізором vmk0 (vmkernel port) включений до групи Management Network.

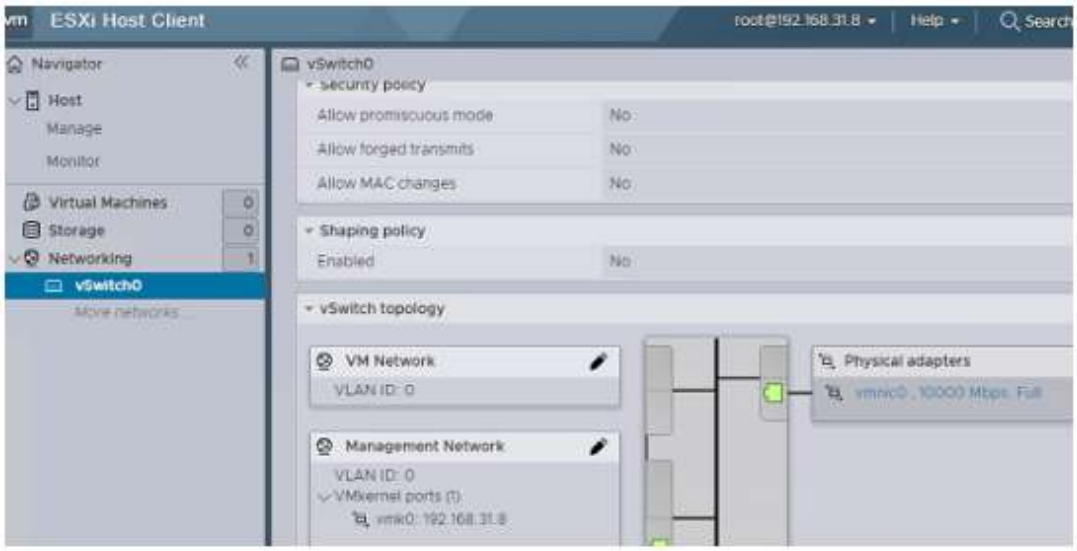


Рисунок 4.7 – Налаштування віртуального комутатора

У більшості випадків, зазвичай, одного віртуального комутатора на окремому гіпервізорі виявляється вже достатньо. Але, якщо ви бажаєте забезпечити ізоляцію

віртуальних машин один від одного та використовувати різні параметри VLAN для різних груп портів, то може знадобитися створення додаткових портів.

Важливо уникати непотрібних змін у Management Network або vmkernel port, оскільки це може призвести до втрати доступу до інтерфейсу управління гіпервізором. У випадку втрати доступу до гіпервізору, можна відновити налаштування мережі за допомогою опції "Restore Network Settings" у консолі DCUI.

Далі, важливим етапом є створення сховища для розміщення файлів віртуальних машин. ESXi дозволяє використовувати як локальні диски, так і зовнішні сховища, підключені по iSCSI, NFS або Fibre Channel. Однак у цьому випадку ми розглядатимемо використання локального диска в ролі сховища. Для цього слід перейти в розділ "Storage -> Devices" і перевірити доступні диски, можливо здійснивши Rescan для їх виявлення.

Рисунок 4.8 – Керування сховищем даних

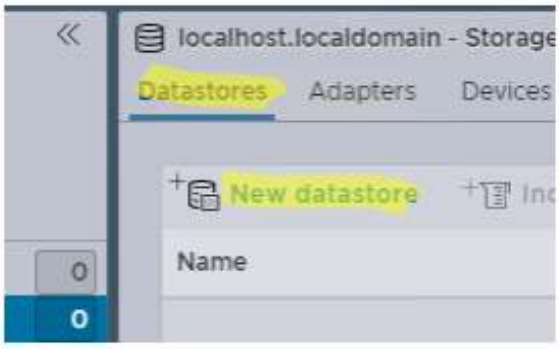


Рисунок 4.9 – Створення нового сховища

4.2 Створення та налаштування віртуальної машини

Для створення нової віртуальної машини необхідно У Web-інтерфейсі вибрати "Virtual Machines" -> "Create / Register VM" -> "Create a new virtual machine".

Далі слід ввести назву для віртуальної машини та обрати тип і версію гостьової операційної системи. Необхідно обрати сховище даних, де будуть зберігатися файли конфігурації та віртуальні диски віртуальної машини. Ці параметри можуть бути змінені пізніше. У випадку недостатнього місця на диску, система попередить про необхідність розширення розміру VMFS сховища.

Під час налаштування віртуальної машини слід вказати базові параметри, такі як кількість CPU, обсяг оперативної пам'яті, розмір жорсткого диска, адаптери мережі та інші. Файли віртуальних дисків (VMDk) та конфігурації віртуальної машини (VMX) зберігаються на сховищі. Це можуть бути локальні диски, флешки USB або зовнішні сховища, підключені по iSCSI, NFS або Fibre Channel.

Для підключення віртуальної машини до мережі визначте її віртуальний мережевий адаптер у групі портів VM Network на комутаторі vSwitch0.

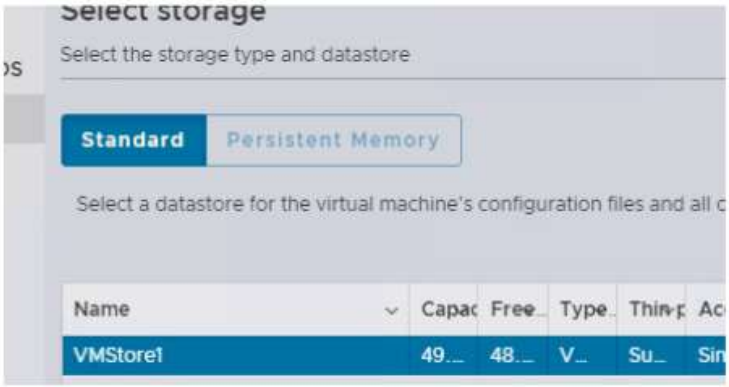
Варто зауважити, що обмеження ліцензії Free vSphere Hypervisor дозволяє призначити не більше 8 vCPU для віртуальної машини.

Для встановлення операційної системи віртуальної машини необхідно завантажити інсталяційний образ (ISO файл) в локальне сховище VMware та вказати образ для CD/DVD приводу в налаштуваннях віртуальної машини після чого запустити інсталяцію гостьової ОС. Після завершення інсталяції слід обов’язково встановіть пакет VMTools для додаткових драйверів та служб у віртуальній машині.

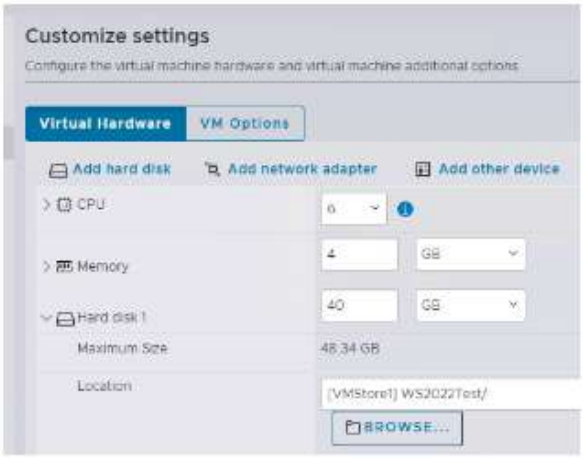
Якщо потрібно мігрувати віртуальну машину або конвертувати фізичний хост у віртуальну машину, скористайтеся утилітою VMware vSphere Converter.

Процес встановлення віртуальної машини під управлінням OS Windows показано на рисунках 4.10 – 4.12.

а)



б)



в)

Рисунок 4.10 – Створення нової віртуальної машини: введення назви (а), вибір сховища (б) та базова конфігурація (в)

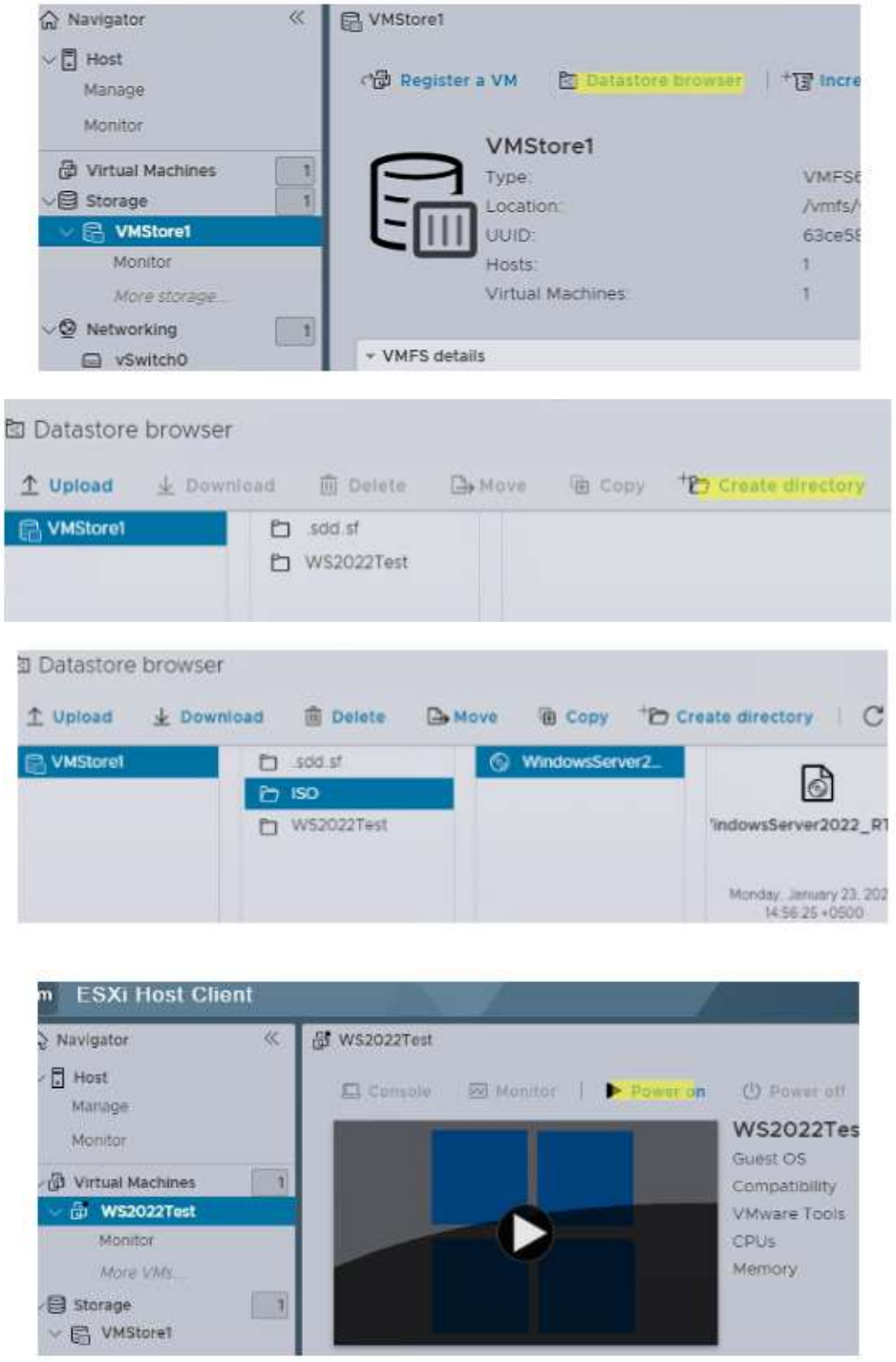


Рисунок 4.11 – Завантаження ISO образу для гостьової машини та запуст процесу встановлення

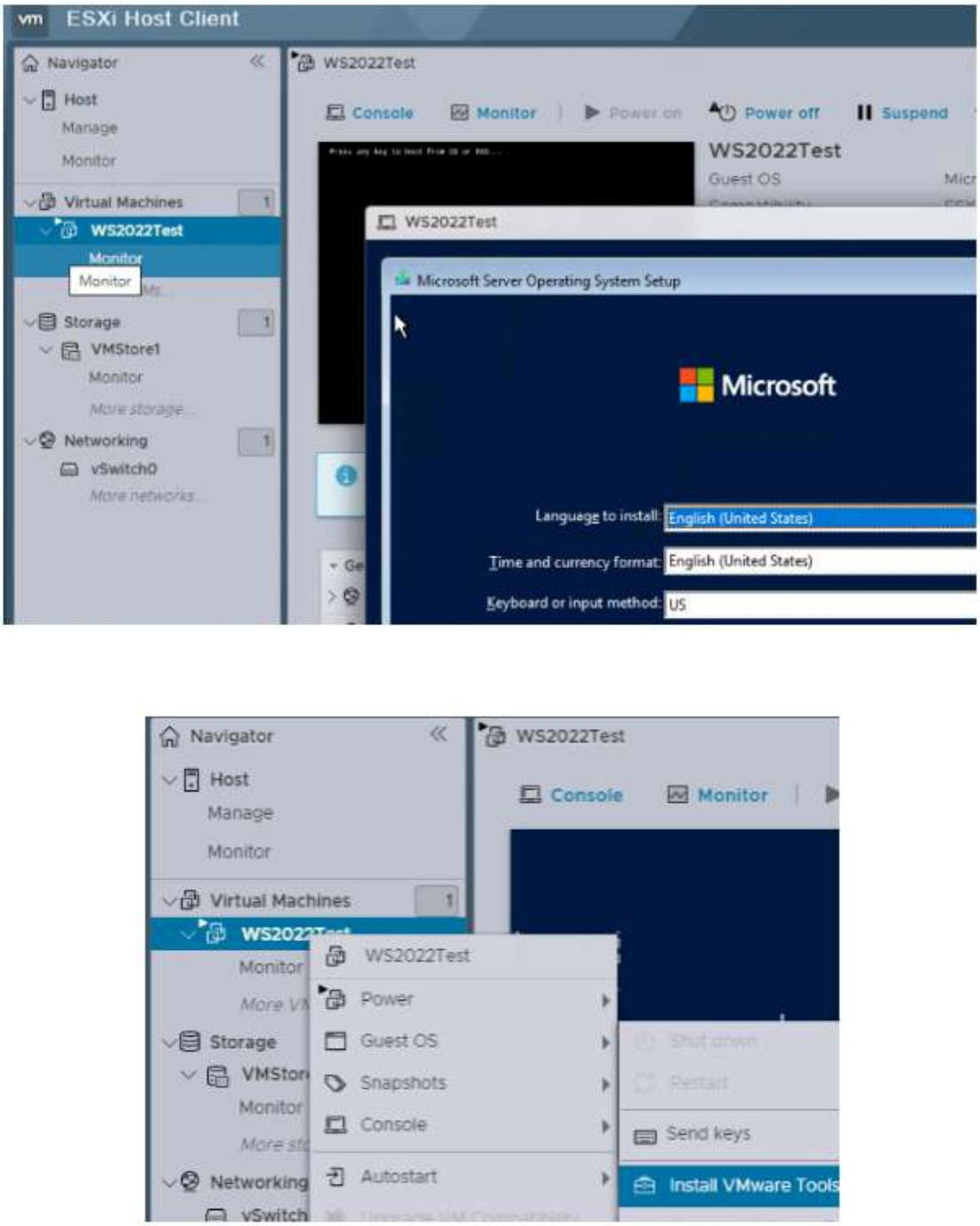


Рисунок 4.12 – Запуск гостьової ОС

4.3 Налаштування системи Dual-WAN

Для забезпечення відмово стійкого доступу до мережі Інтернет запропоновано використання системи Dual-WAN, яка дозволяє підключати до головного шлюза корпоративної мережі декілька провайдерів.

В якості шлюзу було обрано маршрутизатор сімейства EdgeRouter, усі моделі якого можуть підтримувати більше одного WAN-з'єднання. Для налаштування Dual-WAN спочатку необхідно увійдіть до системи налаштувань EdgeRouter та перейти у меню базових налаштувань пристрою (Рисунок 4.13). Далі слід обрати опцію «Балансування навантаження» та перейти у меню налаштування Dual -WAN. У нашому прикладі обидва будуть залишені на DHCP, але змініть їх для свого провайдера, якщо потрібно. Далі в розділі «Другий інтернет-порт» увімкніть прапорець «Тільки цей інтерфейс, якщо інший не працює», щоб функція відновлення після збою працювала. Переконавшись у правильності введених налаштувань, необхідно натиснути кнопку «Застосувати зміни». Та перезавантажити пристрій

Процес налаштування Dual-WAN показано на рисунку 4.13.

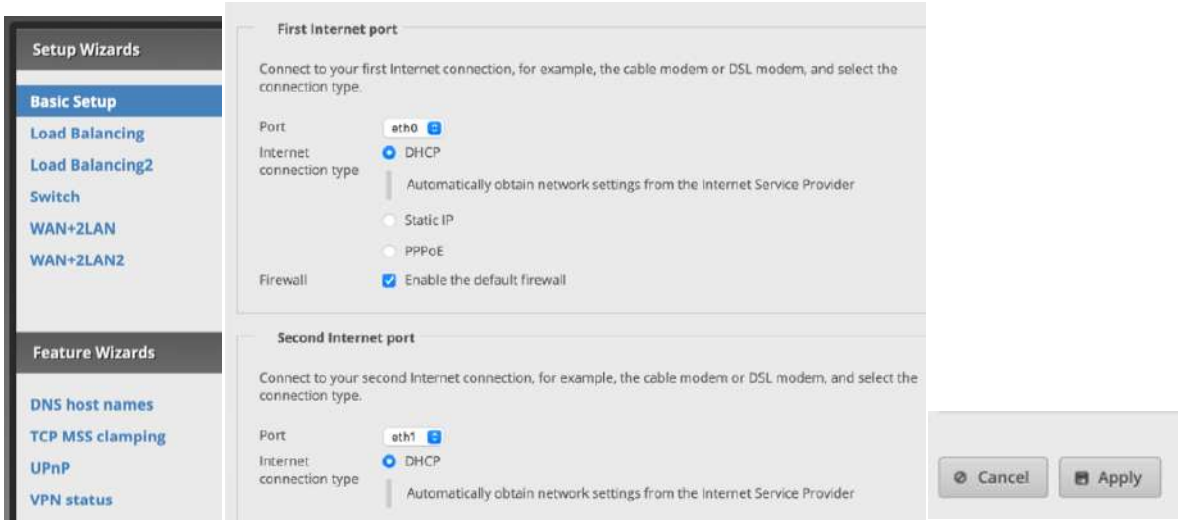


Рисунок 4.13 – Налаштування Dual-WAN

Після перенавантаження слід переконатись, що обом інтерфейсам WAN було призначено IP-адресу.

Тепер у разі відключення одного із WAN-з'єднань, а трафік спрямовуватиметься через інший інтерфейс WAN – рисунок 4.15.

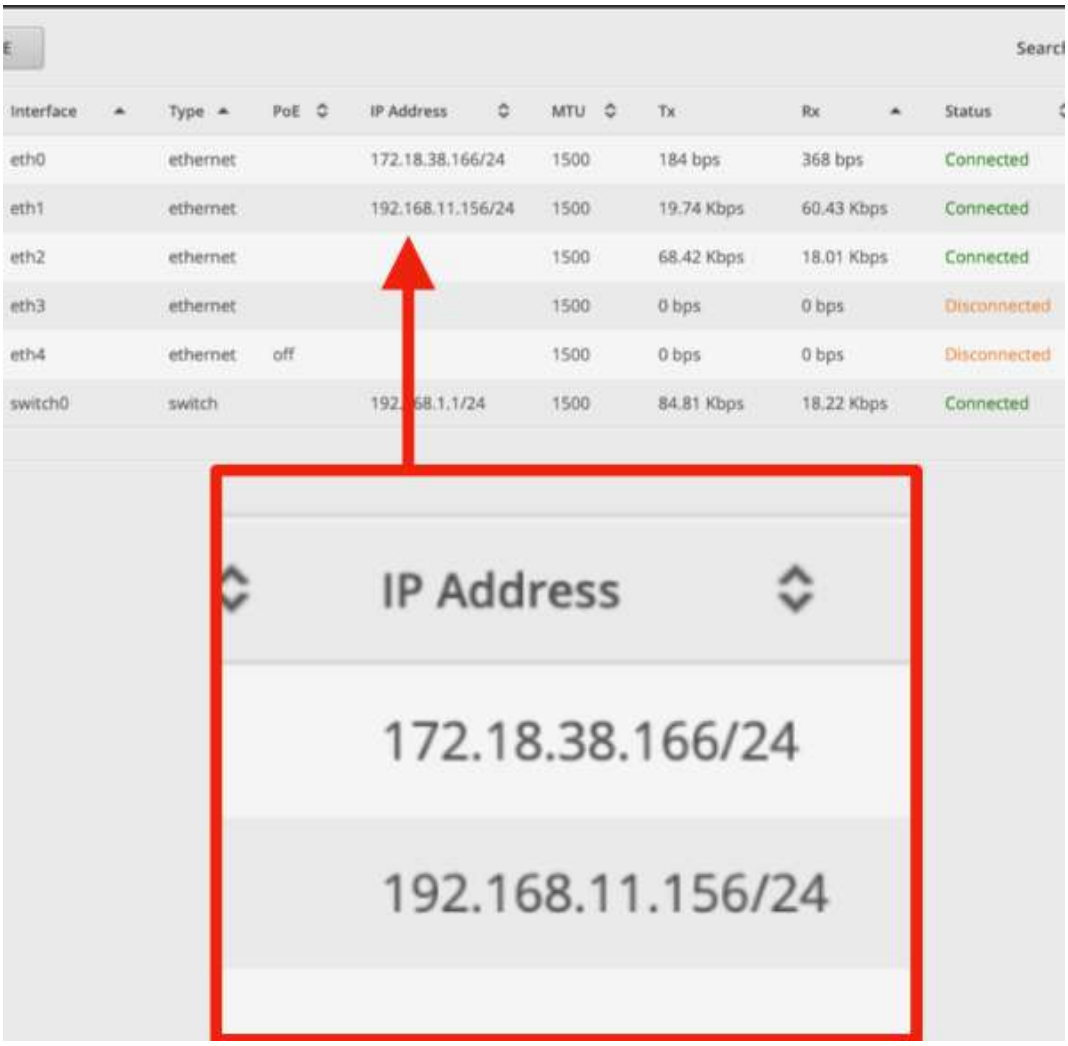


Рисунок 4.14 – Перевірка налаштування Dual-WAN

Висновки до четверного розділу

В четвертому розділі магістерської роботи було виконано наступне:

- розгорнуто та налаштовано серверних гіпервізора VMware ESXi для побудови на його базі відмово стійкого ядра корпоративної інфраструктури підприємства
- встановлено та налаштовано віртуальну машину від управлінням операційної системи Windows;
- налаштовано резервний канал доступу до мережі Інтернет на базі технології Dual WAN.

ВИСНОВКИ

Дослідження корпоративних мереж виявило важливі вимоги до їхньої надійності та відмовостійкості, які визначаються як підвищеними вимогами бізнес-процесів, так і зростанням кількості кіберзагроз. Забезпечення надійності мережі є стратегічно важливою задачею для підтримки функціонування підприємства та безпеки обміну даними.

Мета роботи була сформульована у підвищенні відмовостійкості корпоративної мережі із безпроводовим доступом. Досліджено базову архітектуру мережі, виявлено вразливості та можливі відмови. У результаті були сформульовані та вирішені важливі технологічні задачі щодо підвищення надійності та відмовостійкості корпоративних безпроводових мереж шляхом включаючи надлишковості за методом ковзного резервування серверного устаткування.

Методи математичного аналізу, чисельні методи та теорія надійності були використані для моделювання та аналізу системи. Створено узагальнену математичну модель та формальну модель станів корпоративної мережі.

Отримані результати включають подальший розвиток методів підвищення надійності, введення резервного серверного устаткування та резервного каналу доступу Інтернет за допомогою технології Dual WAN. Також було налаштовано серверне забезпечення на базі гіпервізора VMware ESXI та запропоновано схему резервування для досягнення відмовостійкості.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Лучкова А. В. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж [Електронний ресурс]. Режим доступу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17175/1935.pdf?sequence=3&isAllowed=y.

2. Мережеві технології. Типи мереж [Електронний ресурс]. Режим доступу: https://merezhevi-tekhnologiji.webnode.com.ua/tipi-merezh/.

3. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.

4. Коваль Ю. В. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський – Київ, 2021. – 84 с.

5. Корпоративні мережі та системи доступу. Робоча програма навчальної дисципліни. Національний технічний університет «Харківський політехнічний інститут» [Електронний ресурс]. Режим доступу: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/41b00438-b196-4123-85e1-037d64aba329/content.

6. Комп'ютерні мережі : навчальний посібник / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. – Вінниця : ВНТУ, 2013. – 371 с/

7. Організація комп'ютерних мереж : підручник: для студ. Спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

8. Комп'ютерні мережі: контроль та прогнозування перевантажень. Навчальний посібник / О.М. Ткаченко, Я.І. Торошанко, А.В. Лемешко, В.О. Сосновий, С.С. Коротков., К. : ДУТ, 2021, 77с

9. Структура корпоративної мережі [Електронний ресурс]. Режим доступу: https://fossdocmail.com/uk/network/.

10. Надійність комп'ютерних мереж [Електронний ресурс]. Режим доступу:https://wiki.cuspu.edu.ua/index.php/%D0%9D%D0%B0%D0%B4%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D1%85_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6.

11. Поняття відмови програмного забезпечення як помилки в ньому [Електронний ресурс]. Режим доступу: https://ua.waykun.com/articles/ponjattja-vidmovi-programnogo-zabezpechennja-jak.php.

12. Що таке кібератака? [Електронний ресурс]. Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack.

13. Ddos Attack Halts Heating In Finland Amidst Winter [Electronic resource]. Access: https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

14. Топ 5 помилок у конфігурації додатків [Електронний ресурс]. Режим доступу: https://corewin.ua/blog/top-5-application-security-misconfigurations/.

15. Система управління конфігураціями пристроїв в мережі підприємства [Електронний ресурс] / Гурін В.І. // Національний університет «Києво-Могилянська академія». Режим доступу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/6ed67546-7336-4b70-b6a6-5d945b0b6dfb/content.

16. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

17. IEEE 802.11™ Wireless Local Area Networks [Electronic resource]. Access: https://www.ieee802.org/11/.

18. Шовкута В. А. Аналіз механізмів захисту та вразливостей бездротових Wi-Fi мереж [Електронний ресурс] / ДВНЗ «Національний гірничий університет». Режим доступу: https://ir.nmu.org.ua/bitstream/handle/123456789/149268/18-20.pdf?sequence=1&isAllowed=y.

19. War Driving (Access Point Mapping) [Electronic resource]. Access: https://www.techtarget.com/searchmobilecomputing/definition/war-driving.

20. Wired Equivalent Privacy (WEP) [Electronic resource]. Access: https://www.techtarget.com/searchsecurity/definition/Wired-Equivalent-Privacy.

21. Wi-Fi Protected Access (WPA) [Electronic resource]. Access: https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access.

22. What are Wi-Fi security protocols and are they encryption tools? [Electronic resource]. Access: https://www.avast.com/c-wep-vs-wpa-or-wpa2#:~:text=WPA2%20(Wi%2DFi%20Protected%20Access,and%20protect%20Wi%2DFi%20networks.

23. Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse [Electronic resource] / M. Vanhoef. Access: https://www.krackattacks.com/.

24. How does Wi-Fi Protected Setup work? [Electronic resource]. Access: https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work.

25. What Is an Evil Twin Attack and How Does It Work? [Electronic resource]. Access: https://www.avast.com/c-evil-twin-attack.

26. Wireless Disassociation Attacks ? [Electronic resource]. Access: https://www.baeldung.com/cs/wireless-disassociation-attacks#:~:text=Wireless%20disassociation%20attacks%2C%20also%20known,to%20disconnect%20from%20the%20network.

27. Man in the middle (MITM) attack [Electronic resource]. Access: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.

28. HardReset.info: Як відфільтрувати MAC-адреси на Open Mesh OM5P-AC [Електронний ресурс]. Режим доступу: https://www.hardreset.info/uk/devices/open-mesh/open-mesh-om5p-ac/faq/mac-address-filter/mac-address-filter-router/#google_vignette.

29. Правила створення та використання надійних паролів – рекомендації кіберполіції [Електронний ресурс]. Режим доступу: https://cyberpolice.gov.ua/news/pravyla-stvorennya-ta-vykorystannya-nadijnyx-paroliv--rekomendacziyi-kiberpolicziyi-2070/.

30. Стецюк М. В., Стецюк В. М., Савенко О. С. Модель архітектури автоматизованих інформаційних систем супроводу фінансово-господарських процесів та підтримки управлінських рішень в закладах вищої освіти, 2019. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах», вип. 2, СС. 91-98.

31. Habibian H.; Patooghy A. Fault-tolerant routing methodology for hypercube and cube-connected cycles interconnection networks. The Journal of Supercomputing 2017, vol. 73, pp 4560–4579.

32. Ланде Д.В. Методи підвищення живучості інформаційної складової корпоративних інформаційно-аналітичних систем підтримки прийняття рішень. Реєстрація, зберігання і обробка даних 2012, том 14, №2, СС.48-58.

33. Wu J. Revelation of the Heterogeneous Redundancy Architecture. In: Cyberspace Mimic Defense. Wireless Networks. Springer Nature Switzerland AG. 2020, PP 207–271.

34. RAID [Electronic resource]. Access: https://www.prepressure.com/library/technology/raid.

35. Veeam Backup & Replication [Electronic resource]. Access: https://www.veeam.com/vm-backup-recovery-replication-software.html.

36. UISP – EdgeRouter Dual-WAN Setup [Electronic resource]. Access: https://support.hostifi.com/en/articles/7042510-uisp-edgerouter-dual-wan-setup.

37. VMWare ESXi [Electronic resource]. Access: https://www.vmware.com/products/esxi-and-esx.html

38. Product Evaluation Center for VMware vSphere Hypervisor 8 [Electronic resource]. Access: https://customerconnect.vmware.com/en/evalcenter?p=free-esxi8

39. Слободян М. Модель хаотичної надширокосмугової системи передачі інформації для бездротових сенсорних мереж // Вісник Хмельницького національного університету, Том 1, №2, 2023 (319), СС. 284-288.

40. Slobodian M. Cyber-physical system for express analysis of psychophysiological state based on pulse-wave examination // Actual problems of modern technologies: book of abstracts of the XII International scientific and practical conference of young researchers and students, (Ternopil, December, 6th-7th, 2023) / Ministry of Education and Science of Ukraine, Ternopil Ivan Puluj National Technical University [and other.]. – Ternopil: PE Palianytsia V.A., 2023. – 497p.

ДОДАТОК А

Матеріали апробації наукових результатів кваліфікаційної роботи

DOI: 10.31891/2307-5732-2023-319-1-284-288
УДК 621.398

Максим СЛОБОДЯН
Хмельницький національний університет
ORCID ID: 0000-0002-9277-565X
e-mail: mslobodian@khmnu.edu.ua

МОДЕЛЬ ХАОТИЧНОЇ НАДШИРОКОСМУГОВОЇ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ ДЛЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

У статті описано застосування моделі надширокосмугового зв'язку на основі хаотичної синхронізації як малопотужного та ефективного альтернативного рішення для побудови бездротових сенсорних мереж. Використання хаотичних сигналів як носіїв інформації в системах бездротового зв'язку має низку переваг, до яких відноситься широкий спектр сигналу, висока інформаційна ємність, кібербезпека та низьке енергоспоживання кіл-генераторів. Передача цифрового сигналу виконується за допомогою маніпуляції хаотичними радіоімпульсами, прийом і демодуляція яких реалізується на основі використання односпрямованої синхронізації нелінійних динамічних систем. На основі теорії хаотичної синхронізації, в програмному середовищі MATLAB/Simulink була побудована модель та проведено імітаційне моделювання хаотичної надширокосмугової системи передачі інформації. Розглянуто негативний впливи шуму в каналі зв'язку та проблему неідентичності параметрів систем. Запропоновані моделі можуть бути використані для проектування та розробки ефективних бездротових сенсорних мереж для застосування у сфері охорони здоров'я.

Ключові слова: бездротові сенсорні мережі, хаотичний зв'язок, надширокосмугові системи, динамічні системи, синхронізація

Maksym SLOBODIAN
Khmelnytskyi National University

MODEL OF A CHAOTIC ULTRA-WIDEBAND INFORMATION TRANSMISSION SYSTEM FOR WIRELESS SENSOR NETWORKS

Distributer measuring systems, consisting of interconnected wireless sensor nodes with autonomous supply, have plenty of applications in different areas of engineering end technology. Therefore, wireless sensor network design and optimization is a vital problem in informational technologies and computer engineering. Regardless of particular application and architecture, a wireless sensor network consists of several small sensor nodes somehow distributed in an area of inspection. Such a design ensures a distributed parameter measuring, according to which, each node performs preprocessing procedures for the data, which are to be aggregated by a so-called sink node and sent via other networks, e.g., wired or wireless local area network. For healthcare solutions, it is important to ensure a stable connection with the network and server back-end to provide a high-level analysis based on predicting methods of machine learning algorithms. This paper describes an application of an ultra-wideband communication model based on chaos synchronization as a low-power and efficient alternative solution for building wireless sensor networks. Thus,

using chaotic signals as information carriers in wireless communication has several advantages, including a wide smooth spectrum, high information capability, cybersecurity, and low power consumption. The synchronization problem is one of the most vital tasks to be solved to design a chaos application for ultra-wide-band communication. Being well-studied for periodic signals, modern synchronization theory contains plenty of solutions for classical telecommunication and radio engineering systems, however, it is not developed enough for chaotic systems. Hence, a one-directional dissipative synchronization between two Chen systems is studied in the first section. The second section is devoted to the computer simulation of the model, described in the previous section. All the models built and the simulations performed have been done using MATLAB/Simulink software. The negative impact of channel noise and inequality of system parameters is considered. The possible way how to improve technical characteristics is also provided. Proposed models are to be used to design and develop low-cost wireless sensor networks for multi-channel healthcare solutions.

Keywords: wireless sensor networks, chaos communication, ultra-wide-band systems, dynamic systems, synchronization

Постановка проблеми та аналіз літературних джерел згідно теми дослідження

Розподілені вимірювальні системи, що складаються із взаємопов'язаних бездротових сенсорних вузлів з автономним живленням, знаходять широке застосування в різних галузях інженерних технологій та сприяють вирішенню різноманітних наукових та інженерно-технічних задач. Тому проектування та оптимізація бездротових сенсорних мереж (БСМ), в т.ч. спеціалізованого програмного забезпечення (ПЗ) для їхніх компонентів, є актуальною проблемою в інформаційних технологіях та комп'ютерній інженерії. Незалежно від конкретного застосування та архітектури, БСМ складається з набору невеликих сенсорних вузлів, розподілених у зоні контролю, наприклад, випадковим чином або рівномірно у критичних місцях, і з’єднаних між собою бездротовим каналом зв’язку [1]. Така конструкція забезпечує вимірювання та контроль розподілених в просторі фізичних величин, наприклад, температури, тиску, вологості; або моніторинг параметрів людського тіла в системах охорони здоров’я, наприклад, пульсових сфігмографічних хвиль (ПСФГ) [2, 3]. Відповідно до структури компонентів БСМ, кожен вузол, який оснащений відповідним сенсором та вимірювальним перетворювачем, виконує процедури попередньої обробки даних та їхню передачу для подальшої агрегації головними вузлами і відправлення через шлюзи локальних мережі, наприклад, дротових або бездротових локальних мереж (LAN), персональних мереж (PAN), або одразу через мережі Інтернет до централізованого сервера обробки та збору даних [1].

Протоколи бездротового зв’язку, що використовуються в промислових і персональних мережах, включно з БСМ і бездротовим Інтернетом речей (IoT), базуються на декількох стандартах [4-6]: IEEE 802.11 (Wi-Fi, LAN), IEEE 802.15.1 (Bluetooth) та IEEE 802.15.4 (PAN). Ці стандарти, як і все сімейство стандартів IEEE 802, здебільшого визначають лише фізичний рівень (PHY) і частково канальний рівень (DLL). [5, 6]. Так, стандарт IEEE 802.15.4 має кілька варіацій базового протоколу, розроблених для задоволення конкретних технічних вимог [6]. Наприклад, технологія ZigBee реалізує базовий протокол IEEE 802.15.4, а також розширює його унікальною моделлю з’єднання вузлів [7].

Методи передачі інформації, що базуються на використанні хаотичних коливань в якості несучих сигналів, беруть свій початок з відкриття явища синхронізації нелінійних динамічних систем (НДС) [8-9]. Перші результати в цій області дослідження були отримані на початку 90-х років XX ст. і з того часу викликають інтерес у науковців та інженерів-дослідників, що підтверджується численними вітчизняними та зарубіжними публікаціями. Пояснюється це насамперед рядом переваг, яких теоретично можна досягти реалізувавши методи хаотичного прийому-передачі для побудови енергоефективних бездротових систем передачі інформації різного призначення. Так, будучи за своєю природою неперіодичними широкосмуговими сигналами, схожими за формою та спектром до комоподібних сигналів, хаотичні коливання характеризуються широкою смугою частот та стійкістю щодо поширення в багатопроменевому середовищі, у порівнянні із сигналами із обмеженим спектром [10]. Завдяки розвитку теорії та практичної реалізації нелінійних НДС у

вигляді простих електричних кіл-осциляторів, можливим є схемотехнічна реалізації генераторів хаотичних коливань, що є ефективним альтернативним рішенням щодо розширення спектру для побудови на їхній базі завадостійких багатоканальних систем передачі, що є особливо актуальним для безпровідних сенсорних мереж. Так, наприклад, стандартом IEEE 802.15.4a хаотичні системи прямої передачі визначаються як опціональне рішення для персональних безпровідних систем зв'язку [11, 12]. В таких системах прийому-передачі аналогова електронна схема генерує хаотичні коливання одразу в заданій смузі частот без перенесення частоти сигналу, аналогічно прийом та обробка такого сигналу на приймальній стороні виконується без проміжного перетворення частоти [11].

Для побудови систем цифрового зв'язку на базі детермінованого хаосу необхідно використовувати одну з декількох можливих стратегій прийому. Так, наприклад, когерентний метод прийому потребує синхронізації між приймачем і передавачем, в складі яких повинні бути відтворені майже ідентичні фрагменти деякої НДС генератора хаотичних коливань [8-10]. Задача синхронізації є однією з найголовніших, які необхідно вирішити для застосування хаотичних сигналів для надширокосмугових (НШС) систем зв'язку. Наприклад, в роботі [13] на основі хаотичної синхронізації спроектовано приймально-передавальний пристрій для кварцового перетворювача сенсора тиску. Будучи добре вивченою для періодичних сигналів, сучасна теорія синхронізації містить багато рішень для класичних телекомунікаційних і радіотехнічних систем, однак стосовно хаотичних систем вона залишається недостатньо розвиненою.

В якості альтернативи, представляючи меншу складність для практичної реалізації і не вимагаючи забезпечення синхронізації, деякі некогерентні методи також можуть бути використані, навіть якщо вони теоретично гірші за технічними характеристиками ніж когерентні методи [11].

Метою роботи є розробка та імітаційне моделювання хаотичної цифрової системи зв'язку на основі загальної синхронізації для передачі даних з хаотичною маніпуляцією (Chaos Shift Keying, CSK). Запропонована модель позиціонується як ефективний альтернативний метод хаотичної НШС бездротової передачі інформації для подальшої реалізації в системах БСМ.

Математична модель хаотичної системи передачі на базі синхронізації НДС

Розглянемо деяку неперервну НДС, що еволюціонує з часом згідно наступного векторного рівняння:

$$d\vec{u}(t)/dt = \vec{F}\left(\vec{u}(t), \vec{k}\right), \quad \vec{u}(t) \in \mathbb{R}^n, \quad \vec{k} \in \mathbb{R}^m \tag{1}$$

де $\vec{u}(t) = \left(u_1(t), u_2(t), \ldots, u_n(t)\right)$ – вектор стану системи, $\vec{k} = \left[k_1, k_2, \ldots, k_m\right]$ – вектор параметрів, $\vec{F}$ – нелінійна векторна функція, яка вважається відомою на передавальній та приймальній сторонах.

Згідно методу декомпозиції НДС, вихідна система (1) розглядається як така, що може бути представлена у вигляді двох підсистем:

$$\vec{F} = \left(\vec{G}, \vec{H}\right), \quad \vec{u} = \left(\vec{v}(t), \vec{w}(t)\right) \tag{2}$$

де $\vec{v}(t) = \left(u_1(t), u_2(t), \ldots, u_p(t)\right)$, $\vec{w}(t) = \left(u_{p+1}(t), u_{p+2}(t), \ldots, u_n(t)\right)$ – вектори стану, а $\vec{G} = \left(F_1(\vec{u}), F_2(\vec{u}), \ldots, F_p(\vec{u})\right)$, $\vec{H} = \left(F_{p+1}(\vec{u},\vec{k}), F_{p+2}(\vec{u},\vec{k}), \ldots, F_n(\vec{u},\vec{k})\right)$ – векторні функції для цих підсистем.

Тоді, вираз (1) можна переписати як:

$$\begin{cases} d\vec{v}(t)/dt = \vec{G}\left(\vec{v}(t), \vec{w}(t), \vec{k}\right) \\ d\vec{w}(t)/dt = \vec{H}\left(\vec{v}(t), \vec{w}(t), \vec{k}\right), \end{cases} \quad \left(\vec{v}(t), \vec{w}(t)\right) \in \mathbb{R}^n, \quad \vec{k} \in \mathbb{R}^m \tag{3}$$

де $\vec{v}(t)$ та $\vec{w}(t)$ – вектори стану для першої та другої системи відповідно.

Тепер розглянемо дві ідентичні НДС, що були піддані декомпозиції згідно правила (2) та позначимо їх *1* та *2* відповідно. Односторонній зв'язок між цими системами забезпечується вектором $\vec{v}_1(t)$ системи *1*, який в

свою чергу є керуючим, або «рушійним» сигналом для системи *2*.

Вважатимемо систему *1* головною, або «ведучою» системою – вона буде зберігати свою автономність залишаючись при цьому автоколивальною. На відміно від системи *1*, система *2* є розімкнутою в тому сенсі, що втрачає свою автономність за рахунок повної або часткової заміни власного вектору стану $\vec{v}_2(t)$ вектором $\vec{v}_1(t)$ системи 1, що надійшов каналом зв'язку.

Таким чином, повна синхронізації між НДС *1* та *2* описується наступною системою рівнянь:

$$\begin{cases} d\vec{v}_1(t)/dt = \vec{G}_1(\vec{v}_1(t), \vec{w}_1(t), \vec{k}_1), & d\vec{v}_2(t)/dt = \vec{G}_2((1-d)\times\vec{v}_1(t) + d\times\vec{v}_1(t), \vec{w}_2(t), \vec{k}_2), \\ d\vec{w}_1(t)/dt = \vec{H}_1(\vec{v}_1(t), \vec{w}_1(t), \vec{k}_1), & d\vec{w}_2(t)/dt = \vec{H}_2((1-d)\times\vec{v}_1(t) + d\times\vec{v}_1(t), \vec{w}_2(t), \vec{k}_2), \\ (\vec{w}_{1,2}(t), \vec{v}_{1,2}(t)) \in \mathbb{R}^n, & \vec{k}_{1,2} \in \mathbb{R}^m \end{cases} \quad (4)$$

де d – коефіцієнт, що визначає ступінь зв'язку між НДС *1* та *2*.

Похибка синхронізації обчислюється на основі різниці векторів $e(t) = \|\vec{w}_1(t) - \vec{w}_2(t)\|$, асимптотичне зменшення якої ($\varepsilon \to 0$ при $\tau \to \infty$) свідчить про встановлення режиму повної синхронізації.

Розглянемо в якості прикладу НДС систему Чена [14, 15], яка описується трьома нелінійними диференціальними рівняннями:

$$\begin{cases} dx_1/dt = a(x_2 - x_1) \\ dx_2/dt = (c - a)x_1 - x_1x_3 + cx_2 \\ dx_3/dt = x_1x_2 - bx_3 \end{cases}, \quad (5)$$

де a, b та c – дійсні параметри системи.

Виконаємо наступні підстановки:

$$\begin{aligned} &x_i = m_1V \quad (i = 1\ldots3), \quad t = m_2t, \quad p = a - c, \\ &k_1 = am_1m_2/m_1, \quad k_3 = pm_1m_1/m_2, \quad k_4 = m_1m_1m_3/m_2, \quad k_6 = m_1m_1m_2/m_3, \\ &k_2 = am_1, \quad k_5 = cm_1, \quad k_7 = bm_1 \end{aligned} \quad (6)$$

тоді система (5) може бути записана у вигляді:

$$\begin{cases} dV_1/dt = k_1V_2 - k_2V_1 \\ dV_2/dt = -k_3V_1 - k_4V_1V_3 + k_5V_2 \\ dV_3/dt = k_6V_1V_2 - k_7V_3 \end{cases}, \quad (7)$$

де $k_j = 1 / (R_jC_i)$ – розмірні коефіцієнти, що можуть бути виражені через деякі ємності та опори ($j = 1\ldots7$, $i = 1..3$).

Генератора хаосу, побудований на основі НДС, яка описана у вигляді рівнянь (7), може бути реалізований у вигляді електронної схеми, наприклад, на базі операційних підсилювачів та пасивних елементів.

Проведемо імітаційне моделювання процесу односпрямованої дисипативної синхронізація між двома системами Чена, математична модель якого була представлена вище.

Пакет імітаційних моделей було реалізовано в програмному середовищі MATLAB/Simulink відповідно до математичної моделі.

Імітаційне моделювання хаотичної системи передачі

Імітаційна модель «ведучої» НДС генератора, яка представляє собою частину передавального каскаду структури передавача, зображена на рис. 1,а. Інформаційний двійковий сигнал *s*, що вводиться в передавальний блок, керує сигналом *x*, який надсилається в канал зв'язку, за допомогою комутаційного елемента (Switch – 1/0). Таким чином, режими синхронізації та десинхронізації відповідають двійковим "1" та "0" відповідно. Модель НДС приймача аналогічна до моделі НДС передавача – обидві реалізовано згідно рівнянь системи Чена (7) – за винятком розмикання останньої за вектором стану V_2, який виступає в якості рушійного сигналу, а також схеми

оцінки похибки синхронізації, згідно якої виконується виділення цифрового сигналу s' на приймальній стороні (рис. 1,б). Загальна модель запропонованої цифрової системи зв'язку показана на рис. 1,в. Система складається з НДС передавача та НДС приймача, які з'єднаних каналом зв'язку з додаванням білого шуму – Add White Gaussian Noise (AWGN). Змінна стану V_2 використовується як носій сигналу. Пройшовши через канал зв'язку, зашумлений сигнал s' надходить на вхідний порт моделі НДС приймача. Вектори стану обох систем – $\vec{V}$ та $\vec{V}$¢ – контролюються і відслідковуються в процесі моделювання. Відповідні фазові портрети зображені на рис. 2,б,в та г.

Дисипативна синхронізація двох НДС вимагає майже повного співпадіння параметрів обох систем. Крім того, іншим дестабілізуючим фактором, що перешкоджає встановленню режиму синхронізації, є шуми в каналі зв'язку [10]. Одним з можливих методів зменшення негативного впливу цих двох факторів є керування ступенем зв'язку за рахунок підбору оптимального значення коефіцієнта підсилення в колі зворотного зв'язку на неавтономної НДС приймача [10]. Можливий варіант реалізації такої схеми показано у вигляді моделі на рис. 2,а – як видно, у приймальній НДС реалізовано коло зворотного зв'язку з коефіцієнтом підсилення d, а вхідний сигнал проходить через підсилювач, коефіцієнт підсилення якого дорівнює $1 - d$. Таким чином, сигнал, який надходить на підсистему G_2 приймальної НДС, є сумою вхідного сигналу та сигналу зворотного зв'язку у відповідності до (4). В результаті такої модифікації контур зворотного зв'язку покращує стійкість системи передачі до дестабілізуючих факторів, зменшуючи нестабільність її та запобігаючи небажаним зривам синхронізації [10]. Значення параметра d обирається за допомогою процедури оптимізації та комп'ютерного моделювання.

У режимі повної синхронізації, що відповідає рівню логічної "1" цифрової системи передачі, фазовий портрет на площині $V_{а,2}$–$V_{на,2}$ керуючого сигналу автономної НДС $x = V_{а,2}$ і сигналу $V_{на,2}$, виробленого неавтономною НДС приймача, має вигляд прямої лінії з кутом нахилу нахилом $\alpha = 45°$ (за однакових масштабах осей) – рис. 2,г. Будь-які спотворення фазового портрета спричинені нерівномірністю параметрів системи, впливом шумів або (у випадку комп'ютерного моделювання) похибками моделювання (рис. 6, в).

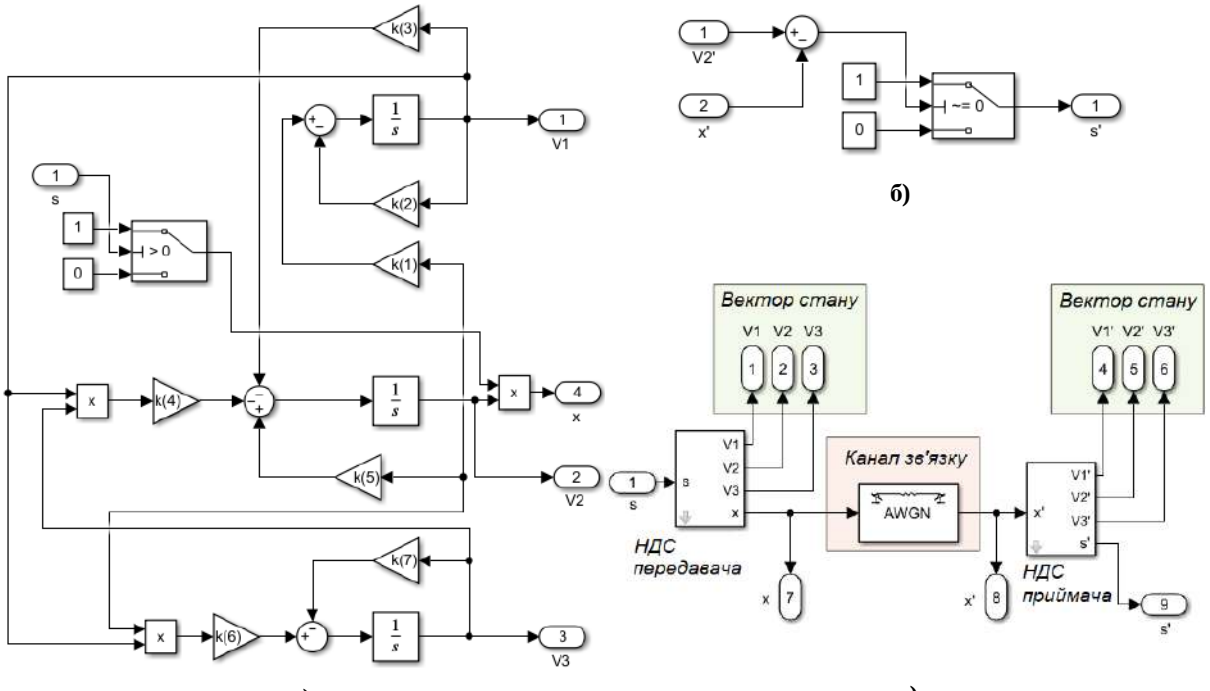


Рис. 1. Імітаційна модель хаотичної системи передачі: а) – НДС генератора з уведенням цифрового сигналу; б) – спрощена схема виділення інформаційного сигналу на основі оцінки похибки синхронізації; в) – узагальнена схема запропонованої системи цифрового зв'язку

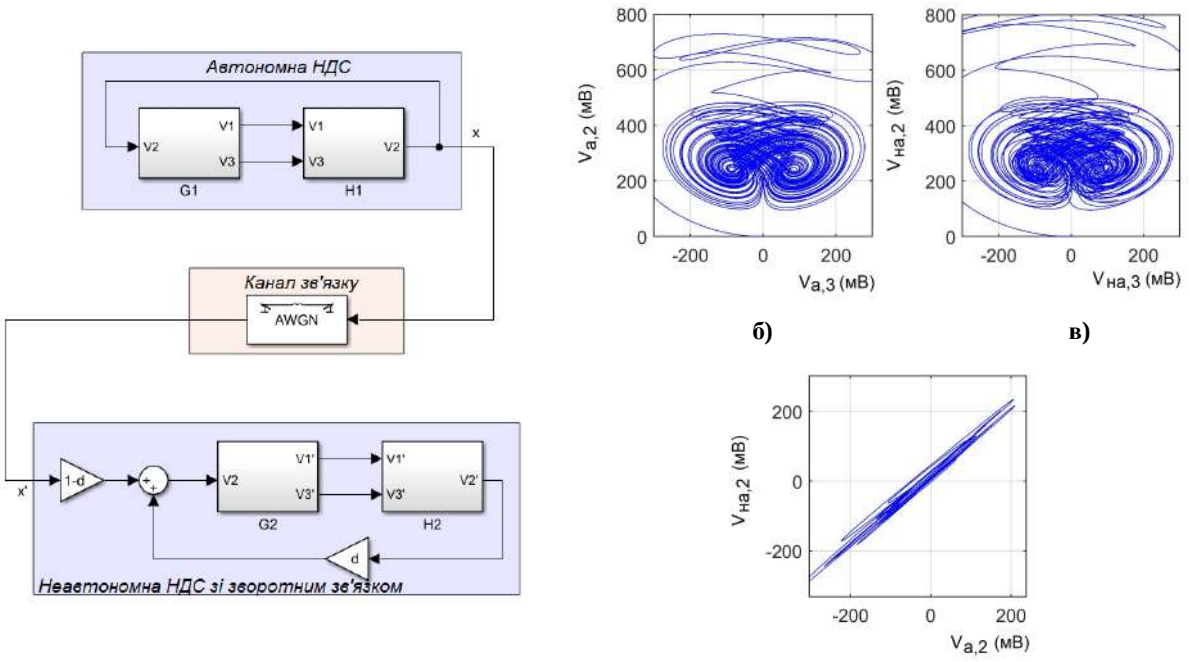


Рис. 2. Імітаційна модель хаотичної системи передачі із контуром зворотного зв'язку в НДС приймача: а) – структурна схема системи; б), в) – фазові портрети НДС генераторів передавача та приймача відповідно; г) оцінка синхронізації за фазовим портретом керуючого сигналу

Висновки

Системи бездротового зв'язку, які базуються на використанні хаотичних сигналів в якості несучих для передачі інформації, характеризуються низкою переваг у порівнянні із традиційними методами зв'язку, що використовують періодичні несучі сигнали. По-перше, хаотичні сигнали – це простий та ефективний спосіб розширення спектру, який дозволяє організувати багатоканальні системи зв'язку з низькою ймовірністю перекривання каналів. По-друге, завдяки низькому енергоспоживанню електричних кіл генераторів хаотичних коливань, які є фізичними реалізаціями моделяй НДС, пристрої, побудовані на їх основі, можуть працювати автономно протягом тривалого часу. Також варто відзначити, що хаотичні носії, будучи за формою та характеристиками шумоподібними і неперіодичними, забезпечують додатковий рівень кібербезпеки, приховуючи передану інформацію від третіх осіб. Останні два факти є ключовими щодо застосування в БСМ, тому в цьому дослідженні було обрано саме таку стратегію прийому-передачі для НШС систем, зокрема згідно до стандарту IEEE 802.15.4a.

Однак для створення прототипу такого передавача необхідно вирішити низку проблем, серед яких вибір стратегії прийому та демодуляції хаотичного сигналу між когерентним та некогерентним методами; оптимізація параметрів та підвищення стійкості до дестабілізуючих факторів, таких як шуми каналу, власні шуми приймача, розкид параметрів тощо.

Комплекс імітаційних моделей, розроблених і описаних у цій роботі, буде використано в подальших дослідженнях для вирішення задачі оптимізації когерентної схеми прийому хаотичних сигналів на основі повної синхронізації НДС з метою мінімізації дестабілізуючого впливу розкиду параметрів і шумів в каналі зв'язку.

Запропонована модель хаотичної НШС системи передачі інформації буде використана для проектування та розробки недорогих енергоефективних сенсорних вузлів БСМ з метою застосування їх у сфері охорони здоров'я.

Література

1. Fraisse, C. What is a wireless sensor network? [Electronic resource] / C. Fraisse, J. McNair, T. B. Onofre // UF/IFAS Extension. – Access mode: https://standards.ieee.org/ieee/802.15.4a/3571/. – 11.03.2023.

2. Taranchuk, A. Quartz pulse wave sensor with a capacitive control for healthcare solutions [Text] / A. Taranchuk, S. Pidchenko // IEEE Sensors Journal. – 2021. – Vol. 21, no. 6. – P. 8613-8620. DOI: 10.1109/JSEN.2020.3049065.

3. Taranchuk, A. Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems [Text] / A. Taranchuk // Telecommunications and Radio Engineering. – 2018. – Vol. 77, no. 3. – P. 269-281. DOI: 10.1615/TelecomRadEng.v77.i3.80.

4. IEEE 802.11 – Wireless local area networks [Electronic resource]. – Access mode: https://www.ieee802.org/11/. – 11.03.2023.

5. IEEE 802.15.1 Standard for information technology- Local and metropolitan area networks [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.1/3513/. – 11.03.2023.

6. IEEE 802.15.4 Standard for low-rate wireless networks [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.4/7029/. – 11.03.2023.

7. ZigBee – The full-stack solution for all smart devices [Electronic resource]. – Access mode: https://csa-iot.org/all-solutions/zigbee/. – 11.03.2023.

8. Eroglua, D. Synchronization of chaos and its applications [Text] / D. Eroglua, J.S.W. Lambb, T. Pereira // Contemporary Physics. – 2017. – Vol. 58, no. 3. – P. 207-243. DOI: 10.1080/00107514.2017.1345844.

9. Complete synchronization of two Chen-Lee systems [Text] / L.-J. Sheu, H.-K. Chen, J. H. Chen, L. M. Tam, W.-Ch. Chen, S-K. Lao, K. T. Lin // Journal of Physics Conference Series. – 2008. – Vol. 96, article no. 012138. DOI: 10.1088/1742-6596/96/1/012138.

10. Golevych, O. Synchronization of non-linear dynamic systems under the conditions of noise action in the channel [Text] / O. Golevych, O. Pyvovar, P. Dumenko // Latvian Journal of Physics and Technical Sciences. – 2018. – Vol. 5, no. 3. – P. 70-76. DOI: 10.2478/lpts-2018-0023.

11. Chaotic UWB communicatins for low rate WPAN applications [Text] / N. Rebhi, G. Zaibi, A. Kachouri, P. Charge, D. Fournier-Prunaret // 2008 2nd International Conference on Signals, Circuits and Systems, Nabeul, Tunisia. – 2008. – P. 1-7. DOI: 10.1109/ICSCS.2008.4746940.

12. IEEE 802.15.4a Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless medium access control and physical layer specifications for low-rate wireless personal area networks: Amendment 1: Add Alternate physical layers [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.4a/3571/. – 11.03.2023.

13. Pidchenko, S. Chen system-based chaotic transceiver for frequency output quartz transducers [Text] / S. Pidchenko; A. Taranchuk; M. Slobodian // Radioelectronic and Computer Systems. – 2022. – No. 2. – P. 178-190. DOI: 10.32620/reks.2022.2.14.

14. Chen, G. Yet another chaotic attractor [Text] / G. Chen, T. Ueta // International Journal of Bifurcation and Chaos. – 1999. - Vol. 9, no. 7. – P. 1465-1466. DOI: 10.1142/S0218127499001024.

15. Ueta, T. Bifurcation analysis of Chen's equation [Text] / T. Ueta, G. Chen // International Journal of Bifurcation and Chaos. – 1999. – Vol. 10, no. 8. – P. 1917-1931. DOI: 10.1142/S0218127400001183.

References

1. Fraisse, C. What is a wireless sensor network? [Electronic resource] / C. Fraisse, J. McNair, T. B. Onofre // UF/IFAS Extension. – Access mode: https://standards.ieee.org/ieee/802.15.4a/3571/. – 11.03.2023.

2. Taranchuk, A. Quartz pulse wave sensor with a capacitive control for healthcare solutions [Text] / A. Taranchuk, S. Pidchenko // IEEE Sensors Journal. – 2021. – Vol. 21, no. 6. – P. 8613-8620. DOI: 10.1109/JSEN.2020.3049065.

3. Taranchuk, A. Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems [Text] / A. Taranchuk // Telecommunications and Radio Engineering. – 2018. – Vol. 77, no. 3. – P. 269-281. DOI: 10.1615/TelecomRadEng.v77.i3.80.

4. IEEE 802.11 – Wireless local area networks [Electronic resource]. – Access mode: https://www.ieee802.org/11/. – 11.03.2023.

5. IEEE 802.15.1 Standard for information technology- Local and metropolitan area networks [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.1/3513/. – 11.03.2023.

6. IEEE 802.15.4 Standard for low-rate wireless networks [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.4/7029/. – 11.03.2023.

7. ZigBee – The full-stack solution for all smart devices [Electronic resource]. – Access mode: https://csa-iot.org/all-solutions/zigbee/. – 11.03.2023.

8. Eroglua, D. Synchronization of chaos and its applications [Text] / D. Eroglua, J.S.W. Lambb, T. Pereira // Contemporary Physics. – 2017. – Vol. 58, no. 3. – P. 207-243. DOI: 10.1080/00107514.2017.1345844.

9. Complete synchronization of two Chen-Lee systems [Text] / L.-J. Sheu, H.-K. Chen, J. H. Chen, L. M. Tam, W.-Ch. Chen, S-K. Lao, K. T. Lin // Journal of Physics Conference Series. – 2008. – Vol. 96, article no. 012138. DOI: 10.1088/1742-6596/96/1/012138.

10. Golevych, O. Synchronization of non-linear dynamic systems under the conditions of noise action in the channel [Text] / O. Golevych, O. Pyvovar, P. Dumenko // Latvian Journal of Physics and Technical Sciences. – 2018. – Vol. 5, no. 3. – P. 70-76. DOI: 10.2478/lpts-2018-0023.

11. Chaotic UWB communicatins for low rate WPAN applications [Text] / N. Rebhi, G. Zaibi, A. Kachouri, P. Charge, D. Fournier-Prunaret // 2008 2nd International Conference on Signals, Circuits and Systems, Nabeul, Tunisia. – 2008. – P. 1-7. DOI: 10.1109/ICSCS.2008.4746940.

12. IEEE 802.15.4a Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless medium access control and physical layer specifications for low-rate wireless personal area networks: Amendment 1: Add Alternate physical layers [Electronic resource]. – Access mode: https://standards.ieee.org/ieee/802.15.4a/3571/. – 11.03.2023.

13. Pidchenko, S. Chen system-based chaotic transceiver for frequency output quartz transducers [Text] / S. Pidchenko; A. Taranchuk; M. Slobodian // Radioelectronic and Computer Systems. – 2022. – No. 2. – P. 178-190. DOI: 10.32620/reks.2022.2.14.

14. Chen, G. Yet another chaotic attractor [Text] / G. Chen, T. Ueta // International Journal of Bifurcation and Chaos. – 1999. - Vol. 9, no. 7. – P. 1465-1466. DOI: 10.1142/S0218127499001024.

15. Ueta, T. Bifurcation analysis of Chen's equation [Text] / T. Ueta, G. Chen // International Journal of Bifurcation and Chaos. – 1999. – Vol. 10, no. 8. – P. 1917-1931. DOI: 10.1142/S0218127400001183.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів

6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University (Ukraine)
Pierre and Marie Curie University (The French Republic)
University of Maribor (The Republic of Slovenia)
Technical University of Kosice (The Slovak Republic)
Vilnius Gediminas Technical University (The Republic of Lithuania)
International Academy Mohammed VI of Civil Aviation (Morocco)
T. Shevchenko Scientific Society

CURRENT ISSUES IN MODERN TECHNOLOGIES

Book
of abstracts

of the XII International scientific and practical conference of young researchers and students
December, 6th-7th, 2023

UKRAINE
TERNOPIL – 2023

A43
Actual problems of modern technologies: book of abstracts of the XII International scientific and practical conference of young researchers and students, (Ternopil, December, 6th-7th, 2023) / Ministry of Education and Science of Ukraine, Ternopil Ivan Puluj National Technical University [and other.]. – Ternopil: PE Palianytsia V.A., 2023. – 497.
ISBN

PROGRAM COMMITTEE

Chairman: Mytnyk M.M. –Ph.D., Assoc. Prof., Rector of TNTU (Ukraine).

Co-Chairman: Maruschak P.O. – Dr., Prof. of TNTU (Ukraine).

Scientific secretary: Dovbush T.A. – Ph.D., Assoc. Prof. of TNTU (Ukraine)

Members of the program committee: Vyherer T. – Prof. of University of Maribor (The Republic of Slovenia); Vinash J. – Prof. of Technical University of Košice (Slovakia); Prentkovskis O. – Prof of Vilnius Gediminas Technical University (Lithuania); Stahovych P. – Dr., Prof of Ignacy Łukasiewicz Rzeszow University of Technology (The Republic of Poland); Menoy A. – Dr., Prof. of International Academy Mohammed VI of Civil Aviation (Morocco); Andreikiv O.Ye. – Dr., Prof. Ivan Franko National University of Lviv, Corresponding Member of National Academy of Sciences of Ukraine (Ukraine).

The address of the organization committee:
TNTU, Ruska str. 56, Ternopil, 46001,
tel. (0352) 519724, fax (0352) 254983
E-mail: **: tarasdowbush@gmail.com**
Editing, design, layout: Dovbush T.A.

TOPICS OF THE CONFERENCE

– Physical and Technical Fundamentals of New Technologies Development;
– New Materials, Strength and Durability of the Constructions Elements;
– Modern Technologies in Construction, Machine- and Instrument-Building;
– Modern Technologies in Transport Area;
– Electrical Engineering and Energy Efficiency;
– Fundamental Issues of Food, Bio and Nanotechnologies;
– Economic and Social Aspects of New Technologies;
– Computer and Information Technologies and Communication Systems.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів
6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

А43
Актуальні задачі сучасних технологій : зб. тез доповідей XII міжнар. наук.-практ. конф. Молодих учених та студентів, (Тернопіль, 6-7 грудня 2023) / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін.]. – Тернопіль: ФОП Паляниця В. А., 2023. – 497.
ISBN

ПРОГРАМНИЙ КОМІТЕТ

Голова: Митник Микола Мирославович – к.т.н., доцент, Ректор ТНТУ ім. І. Пулюя. (Україна)

Заступник голови: Марущак Павло Орестович – д.т.н., проф. ТНТУ ім. І. Пулюя. (Україна)

Вчений секретар: Довбуш Тарас Анатолійович – к.т.н., доц. ТНТУ ім. І. Пулюя. (Україна)

Члени: Вухерер Т. – професор факультету інженерної механіки Маріборського університету (Словенія); Вінаш Я. – професор кафедри технології металів Технічного університету у Кошице (Словаччина); Прентковскіс О. – декан факультету Вільнюського технічного університету ім. Гедимінаса (Литва); Стахович Ф. – завідувач кафедри обробки матеріалів тиском Жешувського політехнічного університету ім. Лукасевича (Польща); Меноу А. – д.т.н., професор Міжнародного університету цивільної авіації (Марокко); Андрейків О. – д.т.н., професор кафедри механіки Львівського національного університету ім. І. Франка, член-корр. НАН України.

Адреса оргкомітету:
ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. **0506689327**, факс (0352) 255798
E-mail: confmolstud@gmail.com
Редагування, оформлення, верстка: Довбуш Т.А.

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- фізико-технічні основи розвитку нових технологій;
- нові матеріали, міцність і довговічність елементів конструкцій;
- сучасні технології в будівництві, машино- та приладобудуванні;
- сучасні технології на транспорті;
- електротехніка та енергозбереження;
- фундаментальні проблеми харчових, біо- та нанотехнологій;
- економічні та соціальні аспекти нових технологій;
- комп’ютерно-інформаційні технології та системи зв’язку.

УДК 004.021

М. О. Слободян
(Хмельницький національний університет, Україна)

КІБЕРФІЗИЧНА СИСТЕМА ДЛЯ ЕКСПРЕС-АНАЛІЗУ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ НА ОСНОВІ ПУЛЬСОКСИМЕТРІЇ

M. Slobodian

CYBER-PHYSICAL SYSTEM FOR EXPRESS ANALYSIS OF PSYCHOPHYSIOLOGICAL STATE BASED ON PULSE-WAVE EXAMINATION

The paper presents the architecture of a cyber-physical system for express analysis of the human psychophysiological state based on pulse-wave (PW) studies of the central and peripheral pulse. The integration of sensor devices, a transmission channel, and a data processing and visualization unit is performed in the form of a single cyber-physical platform with elements of artificial intelligence.

Assessment of the psychophysiological state plays an important role in the methodology of studying the general condition of a person. Such studies, in particular, are relevant for athletes under conditions of increased physical and psychological stress, for example, during training and participation in competitions [1]. Such a dual nature of psychophysiological processes requires an integrated approach to building a research strategy that will combine psychophysical testing methods (for example, assessment of neurodynamic properties of higher nervous activity, the balance of nervous processes, state of basic mental functions, autonomic regulation of heart rate), as well as purely psychological testing methods (assessment of motivation, mood, well-being, activity, and anxiety) [1]. It is proposed to consider methods of assessing the psychophysiological state based on statistical analysis of heart rate variability (HRV) according to PW studies. These parameters include, in particular, the coefficient of variation of cardiac intervals, mode, standard deviation, and tension index [1].

The architecture of the levels of the cyber-physical system (Fug.1) is presented in the form of a 5-level platform, which includes the following components [2]:

1) means of interaction with the surrounding world (in this work, represented by high-precision pressure sensors based on piezo resonance transducers [3]);

2) means of data collection and delivery – the control unit and software of the sensor node, which is based on a small-sized, low-power microprocessor (MP) device and integrated with the electronic communication module;

3) primary data processing tools – a set of hardware and software designed to process the results of telemedicine measurements in real-time in order to prepare data for intelligent analysis (extraction of important information, increasing the level of protection, data compression, etc;)

4) decision support tools – intelligent software tools based on artificial intelligence models integrated into the cloud environment; the main task of such systems is the post-processing of data received from the lower levels of the cyber-physical system in order to make a technological decision in accordance with the user's request;

5) service tools – a set of end devices and software interfaces that implement human-machine interaction between the user and the system, including the use of neurolinguistic models of communication simulation, for example, ChatGPT [4].

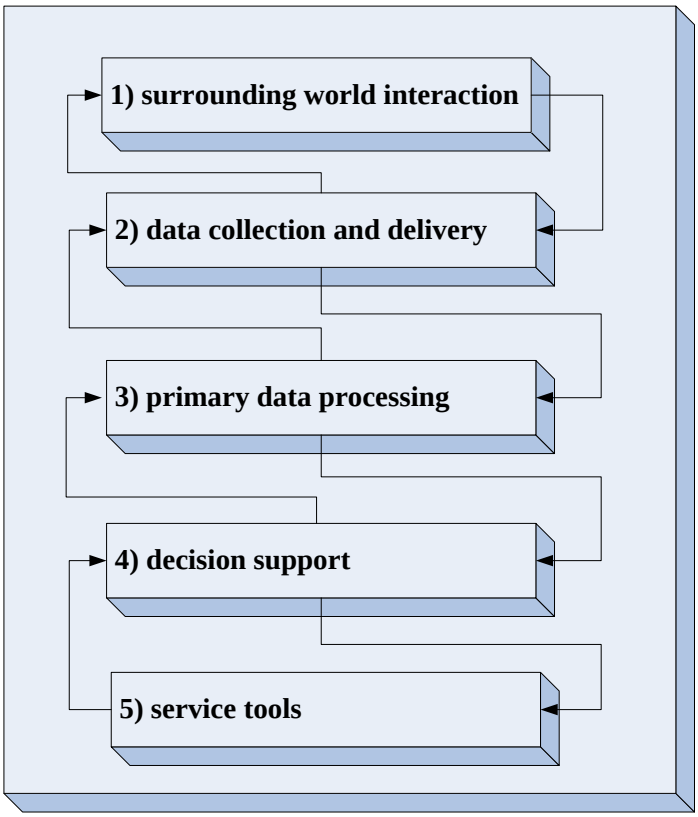


Figure 1. System architecture

The proposed architecture of the cyber-physical system can be used for further development of intelligent cyber-physical systems for rapid analysis of the psychophysiological state of people based on the analysis of HRV indicators.

References

1. Diahnostyka psykhofizychnoho stanu sportsmeniv: metodychnyi posibnyk / H.V. Korobeinikov ta in. Kyiv : 2008. 64 p.

2. Melnyk, A.O., Intehratsiia rivniv kiberfizychnoi systemy // Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Kompiuterni systemy ta merezhi. 2015. № 830. P. 61–67.

3. Taranchuk, A., Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems // Telecommunications and Radio Engineering. 2018. Vol. 77, № 3. P. 269-281.

4. Introducing ChatGPT [Electronic resource] / Access mode: https://openai.com/blog/chatgpt. 24.10.2023.

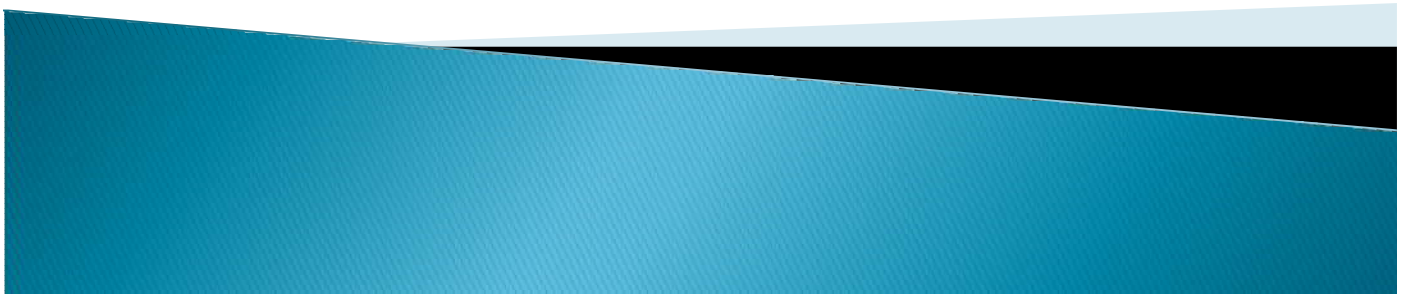
ДОДАТОК Б

Презентаційні матеріали за результатами виконання дипломної роботи

Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж

Слободян М.О.
ТРм-22-1

Керівник: д.т.н.,
проф. Підченко С.К.



Актуальність роботи

Корпоративні мережі, що використовуються для підтримки функціонування на їхній базі інфраструктури підприємства, характеризуються підвищеними вимогами щодо безвідмовної роботи із забезпечення підтримки усіх бізнес-процесів.

Корпоративна мережа призначена для підтримки діяльності підприємства, і її користувачами є лише співробітники цього підприємства (гостьовий сегмент може бути передбачено для зони очікування, або безпосередньо для надання доступу клієнтам, якщо дана компанія веде роботу із клієнтами). На відміну від мереж операторів зв'язку, корпоративні мережі, як правило, не надають послуг стороннім організаціям та користувачам . Корпоративна мережа працює за протоколом TCP/IP і використовує стандарти Інтернету, разом з сервісними додатками, які забезпечують доставку даних користувачам мережі.

Актуальність роботи обумовлена проблемою забезпечення належного рівня надійності та відмовостійкості корпоративних мереж із безпроводових доступом, а також забезпечення належного рівня інформаційної безпеки та кібербезпеки в таких системах.

Мета і задачі дослідження

Метою роботи є підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі **задачі**:

– аналіз базової архітектури корпоративної телекомунікаційної мережі з позиції відмовостійкості та вразливостей до кібератак;

– удосконалення базової архітектури корпоративної телекомунікаційної мережі шляхом введення в систему елементів надлишковості та механізмів живучості;

– імітаційне моделювання відмовостійкої корпоративної мережі;

– проектування відмовостійкої корпоративної інфраструктури на базі мережі із захищеними безпровоовими каналами доступу, надійними механізмами резервного копіювання та резервним каналом доступу до мережі Інтернет.

Об’єкт, предмет та методи дослідження

- **Об’єктом дослідження** є процес забезпечення надійності та відмовостійкості корпоративної безпроводової мережі.
- **Предметом дослідження** є метод підвищення відмовостійкості корпоративної мережі шляхом резервування серверного устаткування як найбільш критичної ланки системи, реалізації механізму резервного копіювання та відмово стійкого каналу доступу до Інтернет.
- Для вирішення поставлених задач були використані такі **методи дослідження:** методи математичного аналізу, чисельні методи, методи теорії надійності, , методи алгоритмізації та програмування.

Науково-практична новизна отриманих результатів

- набув подальшого розвитку метод підвищення надійності корпоративної мережі із безпроводових доступом шляхом забезпечення резервування серверного устаткування, яке побудоване на базі інфраструктури віртуалізації; а також впровадження механізму резервного каналу доступу до мережі Інтернет на базі технології Dual-Wan.
- встановлена та налаштовано серверне забезпечення корпоративної мережі та IT інфраструктури підприємства на базі гіпервізора VMware ESXI;
- запропонована схема резервування, яка дозволить забезпечити відмово стійку роботу системи шляхом введення ковзного резервного серверного вузла.

Апробація результатів

1) стаття у фаховому виданні – Слободян М.О. Модель хаотичної надширокосмугової системи передачі інформації для бездротових сенсорних мереж / М.О. Слободян // Вісник Хмельницького національного університету. Технічні науки. – 2023. – № 2. – С. 284–289.

2) тези доповіді - Slobodian M. Cyber-physical system for express analysis of psychophysiological state based on pulse-wave examination // Actual problems of modern technologies: book of abstracts of the XII International scientific and practical conference of young researchers and students, (Ternopil, December, 6th-7th, 2023) / Ministry of Education and Science of Ukraine, Ternopil Ivan Puluj National Technical University [and other.]. – Ternopil: PE Palianytsia V.A., 2023. – 497p.

Проходження професійної практики

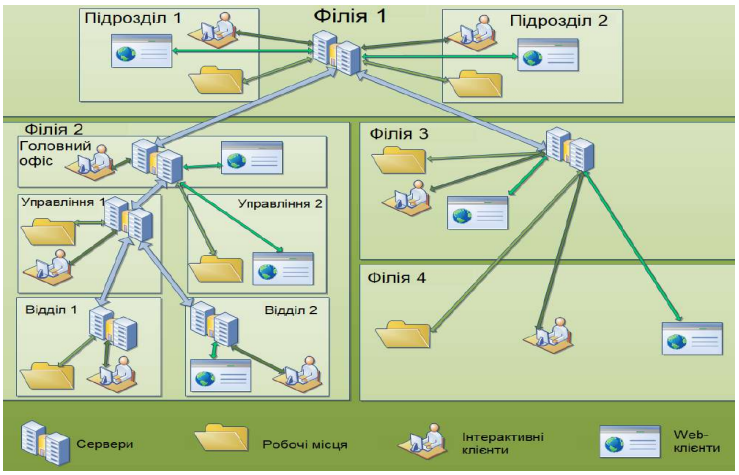
- База практики – ТОВ «ІТТ» - приватна ІТ компанія, яка займається діяльністю у сфері проводового електрозв’язку, видання комп’ютерних ігор та іншого програмного забезпечення, розробкою програмного забезпечення, управлінням комп’ютерним обладнанням, обробкою даних та розміщенням інформації на веб-сайтах.

1 ОГЛЯД МЕТОДІВ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ БЕЗПРОВОДОВИХ МЕРЕЖ, А ТАКОЖ ВІДОМИХ ВРАЗЛИВОСТЕЙ ТАКИХ МЕРЕЖ

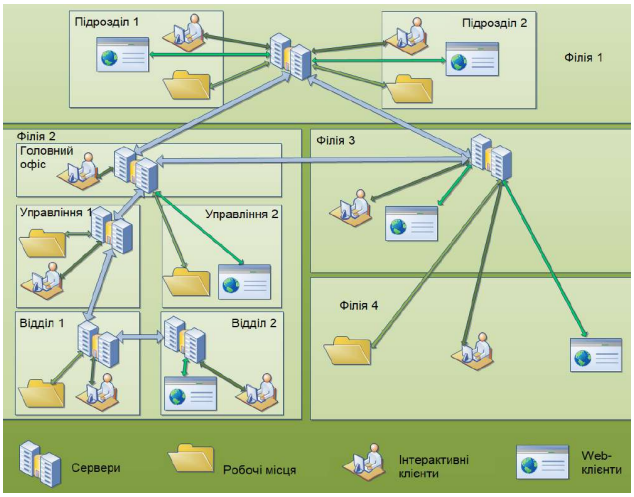
Структурні елементи	
Робочі станції	Клієнтська операційна система, Пакет прикладних програм (загального призначення та корпоративних), Апаратна частина (в т.ч. засоби безперебійного живлення)
Сервери	Серверна операційна система з підтримкою засобів віртуалізації Відмовостійка дискова система із системою резервного копіювання даних Резервне живлення
Мережеве обладнання	Маршрутизатори, комутатори та бездротові точки доступу,
Канали зв'язку	Проводові та оптичні канали зв'язку Бездротові канали зв'язку на основі стандартів IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth)
Програмне забезпечення мережі	Спеціалізовані програмні засоби для керування мережевими ресурсами,
Засоби безпеки	Антивірусне програмне забезпечення, мережеві екрани, засоби аутентифікації та авторизації
Інфраструктура корпоративних додатків	Системи керування базами даних, бекенди корпоративних додатків

Узагальнені характеристики корпоративної мережі щодо її функціональних вимог

1.1 Загальна характеристика корпоративних мереж



Приклад топології корпоративної мережі «Зірка»

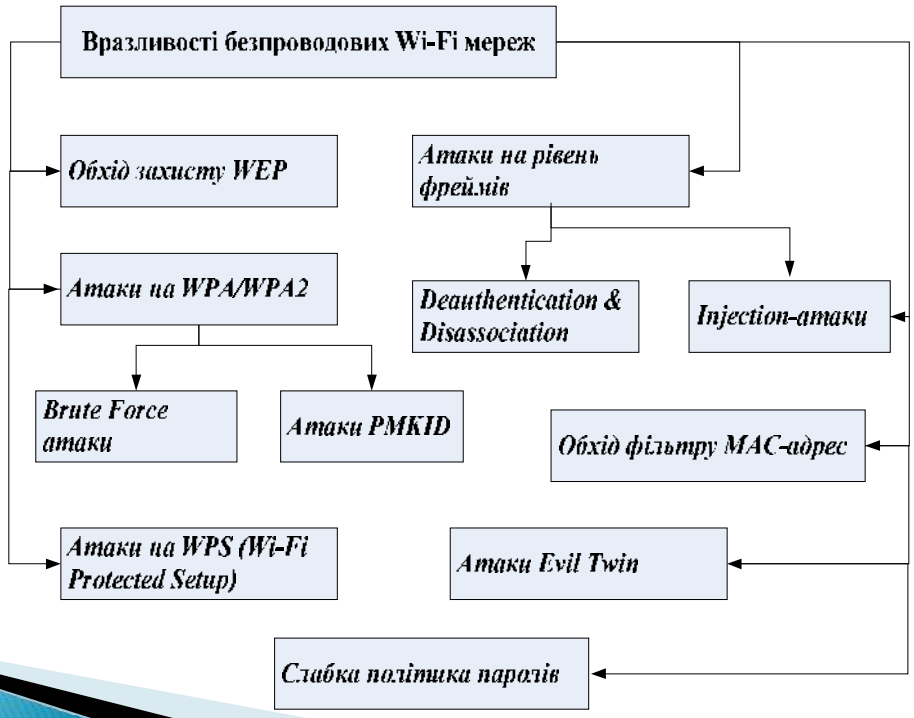


Приклад змішаної топології корпоративної мережі

1.2 Огляд можливих відмов та вразливостей

- помилки у конфігурації та управлінні: 1) Некоректна конфігурація – неправильна настройка параметрів мережевого обладнання чи програм може викликати проблеми в роботі мережі; 2) проблеми з управлінням ресурсами [8] – недостатня або неефективна управлінська політика може призвести до відмови через неспроможність вирішення конфліктів або неадекватну реакцію на події;
- проблеми з безпекою: неавторизований доступ [17] – неправомірний доступ до мережевих ресурсів може викликати проблеми з безпекою та викликати відмови у функціонуванні;
- проблеми з електропостачанням та фізична безпека [17]: 1) Перебої в електропостачанні – Відключення електропостачання або флуктуації можуть викликати відмови в роботі обладнання; 2) Фізична пошкодження – непередбачувані події, такі як природні катастрофи чи вандалізм, можуть завдати фізичних пошкоджень обладнанню і спричинити відмови;
- системні та організаційні проблеми [17]: 1) неадекватне масштабування мережі може призвести до перевантаження ресурсів та відмов у роботі; 2) некоректне планування архітектури та розміщення ресурсів може створити ситуації, при яких мережа неспроможна ефективно працювати

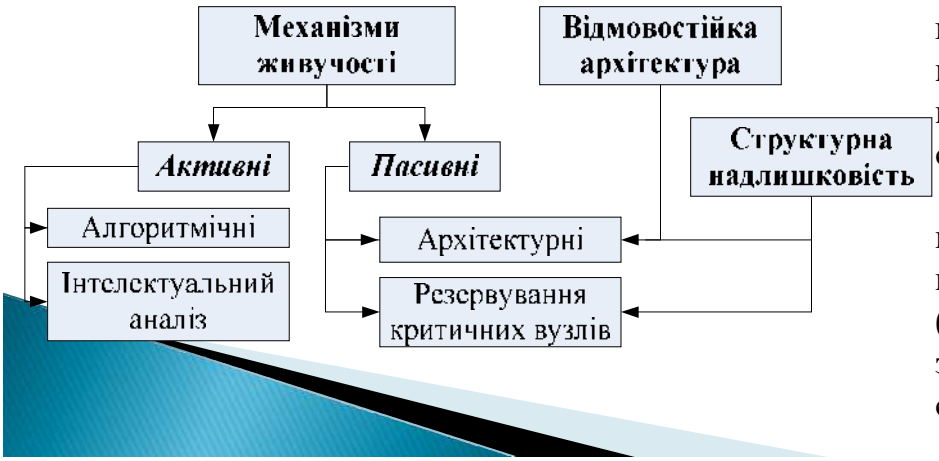
1.2.2 Можливі відмови, що спричинені вразливостями безпроводових мереж Wi-Fi



1.3 Методи підвищення відмовостійкості корпоративних мереж

В ході аналізу літературних джерел згідно тематики дослідження [30-33] були виділена такі методи забезпечення відмовостійкості корпоративних мереж.

Методи підвищення надійності та відмовостійкості (загальні механізми забезпечення живучості) поділяються на активні методи, що включають методи алгоритмізації та інтелектуального аналізу для контролю стану мережі та своєчасного реагування з метою компенсації негативного фактору відмов компонентів; пасивні методи передбачають ручне коригування архітектури та підтримку резервування критичних вузлів, наприклад, файловий серверів.



Загалом ці методи ґрунтуються на застосуванні відмово стійкої архітектури із введенням надлишковості в систему.

Надлишковість дисковий масивів представлена використанням дзеркальних (Mirror 1) RAID масивів для забезпечення відмовостійкості сховища даних [34].

Висновки до першого розділу

- В першому розділі магістерського дослідження було виконано аналіз літературних джерел та науково-практичних публікацій згідно теми роботи, а саме:
- дано характеристику корпоративної мережі підприємства як базу для розгортання на її базі інфраструктури підприємства та розглянуто типові топології таких мереж, а саме зіркоподібну топологію та змішану топологію на прикладі реального технологічного рішення;
- проведено детальний аналіз можливих відмов та несправностей корпоративних мереж, які спричинені як власними відмова, так і зловмисними діями, спрямованими на кібератак на вразливості системи; також дана класифікація таких вразливостей;
- проведено огляд відомих методів підвищення надійності та відмовостійкості корпоративних безпроводових мереж шляхом введення в структуру систему надлишкових елементів, використання алгоритмічних засобів живучості та резервування каналі доступу.

2 РОЗРОБКА МАТЕМАТИЧНА МОДЕЛЬ ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ

2.1 Узагальнена математична модель надійності вузла корпоративної мережі

Аналіз та розрахунок надійності корпоративної безпроводової мережі полягає у її декомпозиції з метою представлення складної системи у вигляді набору складових елементів з відновленням, які можуть перебувати в одному з двох станів: 0 – елемент працює та 1 – елемент відновлюється.

Позначимо через $Y_0(s, t)$ – ймовірність знаходження елементу в справному стані на проміжку $[t; t + s]$, а через $Y_1(\tau, t)$ – ймовірність того, що на проміжку $[t; t + \tau]$ даний елемент відновлюється.

Диференціюванням отримаємо відповідні щільності розподілу:

$$y_0(s,t) = -\frac{\P Y_0(s,t)}{\P s}$$
$$y_1(t,t) = -\frac{\P Y_1(t,t)}{\P t} \qquad (2.1)$$

де функція $y_0(s, t)$ – це щільність розподілу ймовірностей справної роботи елемента на проміжку $[t; t + s]$, $y_1(\tau, t)$ – щільність розподілу ймовірностей відновлення елемента на проміжку $[t; t + \tau]$.

Нехай в початковий момент часу $t = 0$ елемент знаходиться в справному стані, тоді

$$Y_0(s,0) = \bar{F}(s),\ Y_1(t,0) = 0 \qquad (2.2)$$

отже

$$y_0(s,0) = f(s),\ y_1(t,0) = 0 \qquad (2.3)$$

Введемо позначення: x - випадковий час справної роботи елементу;

h - випадковий час відновлення елементу;

t – момент часу за якого елемент справний;

x – довільний момент часу на проміжку від 0 до t;

t-x – момент завершення відновлення елементу, що відмовив;

s – час, протягом якого елемент справний.

Ймовірність справної роботи елемента протягом часу $x + s$ за умови, що в момент часу $t – x$ сталось відновлення, становить:

$$p = y_1(0, t - x)\, f(x + s) \tag{2.4}$$

В результаті інтегрування на проміжку [0; t]отримуємо вираз:

$$y_0(s,t) = \int_0^t f(x+s) y_1(0, t - x)\, dx + f(t+s) \tag{2.5}$$

де $f(t + s)$ відповідає початку процесу роботи та означає, що за відсутності відмови до моменту t елемент працює безвідмовно протягом часу $t + s$.

Аналогічне рівняння можна записати для функції $y_1(\tau, t)$ без вільного члена. Таким чином має місце наступна система інтегральних рівнянь відносно функцій y_0 та y_1:

$$\begin{cases} y_0(s,t) = \int_0^t f(x+s) y_1(0, t - x)\, dx + f(t+s) \\ y_1(t,t) = \int_0^t g(x+t) y_0(0, t - x)\, dx \end{cases} \tag{2.6}$$

Система інтегральних рівнянь (2.6) пов’язує між собою дві функції, які містять у собі інформацію про попередні стани процесу елемента, що обумовлено наявністю в аргументах функцій y_0 та y_1 додаткових змінних s та τ, що відповідають залишковому часу роботи та відновлення.

У тому випадку, коли залишковий час роботи та відновлення рівний нулю, функціями $w(t) = y_0(0,t)$ та $w_B(t) = y_1(0,t)$ назвемо параметри потоку відмов та відновлення відповідно.

Введемо такі позначення: $j_s(t) = j(t+s)$. Тоді отримаємо:

$$
\begin{aligned}
y_0(s,t) &= w_B * f_s(t) + f_s(t) \\
y_1(t,t) &= w * g_t(t) \\
Y_0(s,t) &= w_B * \bar{F}_S(t) + \bar{F}_S(t) \\
Y_1(t,t) &= w * \bar{G}_t(t)
\end{aligned}
\tag{2.7}
$$

Із (2.7) можна виразити ймовірності Y_0 для малих s, а також Y_1 для малих τ через такі характеристики елемента як функція готовості та простоювання і параметри потоку відмов та відновлення:

$$
\begin{aligned}
Y_0(s,t) &= K_\Gamma(t) - w(t)s + o(s^2) \\
Y_1(t,t) &= K_\Pi(t) - w_B(t)t + o(t^2)
\end{aligned}
\tag{2.8}
$$

Тоді маємо:

$$
\begin{aligned}
K_\Gamma(t) &= Y_0(0,t) = \int_0^\infty y_0(s,t)\,ds \\
K_\Pi(t) &= Y_1(0,t) = \int_0^\infty y_1(t,t)\,dt
\end{aligned}
\tag{2.9}
$$

Зробивши підстановку $s = 0$; $\tau = 0$ у вираз (2.7) отримаємо:

$$
\begin{aligned}
w(t) &= w_B * f(t) + f(t) \\
w_B(t) &= w * g(t)
\end{aligned}
\quad ,
\tag{2.10}
$$

звідки слідує:

$$
\begin{aligned}
w(t) &= f(t) + f * f * g(t) + f * f * f * g * g(t) + \ldots \\
&= \sum_{k=0}^{\infty} f^{*(k+1)} * g^{*(k)}(t), \\
w_B(t) &= f * f * g * g(t) + \ldots = \sum_{k=1}^{\infty} f^{*(k)} * g^{*(k)}(t)
\end{aligned}
\tag{2.11}
$$

Очевидно, що функції готовності та простоювання співпадають із ймовірностями $p_0(t)$ та $p_1(t)$ – перебування елемента у справному стані та стані відмови. Ці ймовірності задовольняють рівнянням, які аналогічні до рівнянь Ерланга:

$$\begin{cases} p_0'(t) = -\lambda(t)\, p_0(t) + \mu(t)\, p_1(t) \\ p_1'(t) = \lambda(t)\, p_0(t) - \mu(t)\, p_1(t) \end{cases} \qquad (2.12)$$

де λ, μ – інтенсивність потоку відмов та відновлення.

Звідси слідує, що роботу елемента можна описати за допомогою найпростішого графу станів, із гілками якого співставлень функції λ та μ.

Система рівнянь (2.12) відповідає найпростішому такому графу, який з ображено на рисунку 2.1.

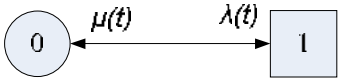


Рисунок 2.1 – Граф станів елементу, який підлягає відновленню

Функції p_0 та p_1 задовольняють початковим умовам $p_0(0) = 1$, $p_1(0) = 0$, що відповідає робочому стану елемента в момент $t = 0$.

Розв'язавши систему (2.6) можна знайти інтенсивності λ (t) та μ (t), або спочатку розв'язати систему (2.6) і вже на базі розв'язку обчислити відповідні інтенсивності.

Розглянута модель атомарного відновлювального елементу є масштабованою, що дозволяє розробити на її базі модель функціонування системи будь-якого рівня складності.

Нехай час безвідмовної роботи та час відновлення елементу мають експоненціальний розподіл з параметрами λ і μ відповідно. Аналітичні вирази для параметрів потоків відмов та відновлення, середньої кількості сумарних відмов та відновлень протягом часу [0; t], а також функцій готовності та простою, середнього напрацювання на відмову та часу відновлення в інтервалі [0; t] можна знайти наступним чином.

З виразу (2.10) для параметрів потоку відмов та відновлення зображення за Лапласом має вигляд:

$$\hat{w}(z)=\frac{\hat{f}(z)}{1-\hat{f}(z)\hat{g}(z)}=\frac{\lambda(z+\mu)}{z(z+\mu+\lambda)},$$
$$\hat{w}_B(z)=\frac{\hat{f}(z)\hat{g}(z)}{1-\hat{f}(z)\hat{g}(z)}=\frac{\lambda\mu}{z(z+\mu+\lambda)} \quad (2.13)$$

звідки, повертаючись до оригіналу, отримуємо:

$$w(t)=\frac{\mu\lambda}{\mu+\lambda}+\frac{\lambda^2}{\mu+\lambda}e^{-(\mu+\lambda)t},$$
$$w_B(t)=\frac{\mu\lambda}{\mu+\lambda}-\frac{\mu\lambda}{\mu+\lambda}e^{-(\mu+\lambda)t} \quad (2.14)$$

Середня сумарна кількість відмов та середня сумарна кількість відновлень протягом часу [0; t]:

$$M(t)=\int_0^t w(x)\,dx=\frac{\mu\lambda}{\mu+\lambda}t+\frac{\lambda^2}{(\mu+\lambda)^2}\left(1-e^{-(\mu+\lambda)t}\right),$$
$$M_B(t)=\int_0^t w_B(x)\,dx=\frac{\mu\lambda}{\mu+\lambda}t+\frac{\mu\lambda}{(\mu+\lambda)^2}\left(1-e^{-(\mu+\lambda)t}\right) \quad (2.15)$$

Для функції готовності та функції простою зображення за Лапласом має вигляд:

$$\hat{K}_Г(z)=\frac{1-\hat{f}(z)}{z\left(1-\hat{f}(z)\hat{g}(z)\right)}=\frac{z+\mu}{z(z+\mu+\lambda)},$$
$$\hat{K}_П(z)=\frac{\hat{f}(z)\left(1-\hat{g}(z)\right)}{z\left(1-\hat{f}(z)\hat{g}(z)\right)}=\frac{\lambda}{z(z+\mu+\lambda)} \quad (2.16)$$

Використовуючи обернене перетворення Лапласа, запишемо оригінали функцій:

$$K_{\Gamma}(t)=\frac{m}{m+l}+\frac{l}{m+l}e^{-(m+l)t},$$
$$K_{\Pi}(t)=\frac{l}{m+l}+\frac{l}{m+l}e^{-(m+l)t} \qquad (2.17)$$

Середній сумарний час безвідмовної роботи та середній сумарний час відновлення на проміжку часу [0; t]:

$$m(t)=\int_0^t K_{\Gamma}(x)dx=\frac{m}{m+l}t+\frac{l}{(m+l)^2}\left(1-e^{-(m+l)t}\right),$$
$$m_B(t)=\int_0^t K_{\Pi}(x)dx=\frac{l}{m+l}t+\frac{l}{(m+l)^2}\left(1-e^{-(m+l)t}\right) \qquad (2.18)$$

Співвідношення (2.18) справедливі для процесів із експоненціальним законом розподілу.

2.2 Характеристика моделі корпоративної мережі

Нехай, що дана корпоративна мережа складається з *m* елементів з відомими розподілами часу безвідмовної роботи та часу відновлення, а її функціонування відбувається відповідно до визначеної схеми розрахунку надійності. Усі елементи умовно поділяються на робочі та резервні. До першого класу віднесемо також всі елементи навантаженого та полегшеного резерву, а до другого – лише елементи, які перебувають у ненавантаженому стані. При відмові робочого елемента і наявності резервного він замінюється резервним, причому ця заміна виконується миттєво і абсолютно надійним пристроєм. Обмеження щодо миттєвої заміни можна скасувати. При наявності кількох резервних елементів порядок заміни відмовленого робочого елемента резервним вважатиметься відомим. Контроль стану елементів є постійним, і відмова будь-якого елемента виявляється негайно після її виникнення. Однак ця умова також може бути скасована. Передбачається, що можливість засобів відновлення і порядок відновлення елементів відомі, тобто регламентованим вважається послідовність прийняті на обслуговування. Останній факт важливий у випадку обмеженого відновлення коли може виникнути черга на відновлення. Відновлення елемента розпочинається одразу після його відмови або після виявлення відмови контролюючим пристроєм при наявності вільного ресурсу

засобу відновлення, відповідно до прийнятого пріоритету обслуговування. Під час ремонту елементів відбувається повне відновлення їхньої надійності.

На функціонування та обслуговування кожного елемента можуть впливати інші елементи системи. У зв'язку з цим кожен елемент може перебувати в кількох можливих станах: -у робочому стані, у стані відновлення або у стані простою. При цьому стан простою елемента може бути обумовлений наступними причинами:

- відбулося переривання роботи елемента, що може статися, якщо цей елемент знаходиться в складі вузла, який послідовно пов'язаний з елементом або вузлом, що відмовив;
- відбулося переривання відновлення елемента, що може статися, якщо у разі застосування регламенту відновлення з пріоритетами, що може передбачати переривання відновлення;
- елемент справний, але за умовами функціонування він знаходиться в черзі на роботу, що може статися, наприклад, у випадку ненавантаженого резервування;
- елемент перебуває в стані відмови, але за умовами обслуговування його не ремонтують і він перебуває в черзі на відновлення, що можливо, наприклад, у випадку обмеженого відновлення з прямим або визначеним пріоритетом.

Визначення можливих станів кожного елемента системи є важливим при описі її функціонування в цілому. Вважатимемо, що перехід кожного елемента з одного стану в інший відбувається миттєво внаслідок відмови або відновлення даного елемента чи будь-якого іншого елемента системи. Додатково припустимо, що відмова чи відновлення будь-якого елемента не впливає на закони розподілу інших елементів, і час простою елемента (якщо це не вказано окремо) не впливає на його характеристики надійності, тобто перебуваючи в стані простою, елемент зберігає ці характеристики такими ж, як у момент переривання роботи або відновлення.

2.3 Формальна модель станів корпоративної мережі

Представимо множину усіх станів деякої корпоративної телекомунікаційної мережі через E, а через n – кількість цих станів. Відповідно до визначення відмови елементу, розділимо стани системи на два класи станів: підмножину робочих елементів та підмножину елементів, які зазнали відмов:

$$E = \{E_+ \dot{E} E_-\} \qquad (2.19)$$

де E_+ - множина робочих станів;

E_- - множина станів відмов.

В кожен фіксований момент часу t для кожного k-го стану ($k = 1…n$) виділимо такі підмножини елементів:

$$E_k = \left\{ R_k, W_k, R_k', W_k', R_k^0, W_k^0 \right\} \quad (2.20)$$

R_k – множина номерів елементів, які працюють,
W_k – множина номерів елементів, які відновлюються в даний момент часу;
R_k' - множина номерів елементів, які простоюють в результаті переривання їхньої роботи;
W_k' - множина номерів елементів, які простоюють в результаті переривання їхнього відновлення;
R_k^0 – множина номерів елементів, які складають чергу на роботу;
W_k^0 – множина номерів елементів, які складають чергу на відновлення;
Для кожного *k*-го стану визначимо вектор, який характеризує стан усіх елементів в момент часу *t*:

$$A_k = \left\{ a_{1k}, a_{2k}, ..., a_{mk} \right\} \quad (2.21)$$

з компонентами:

$$a_{ik} = \begin{cases} s_i, \text{якщо} \quad i \in R_k \cup R_k' \\ t_i, \text{якщо} \quad i \in W_k \cup W_k' \\ 0, \text{якщо} \quad i \in R_k^0 \cup W^0{}_k \end{cases} \quad (2.22)$$

Отже, функціонування будь-якої відновлювальної системи повністю описати матрицею станів *S*, розмірності $m \times n$, стовпцями якої є вектори A_k.

Висновки до другого розділу

- В другому розділі магістерського дослідження було виконано наступне:
- розроблена узагальнена математична модель надійності вузла корпоративної мережі;
- дано характеристики моделі корпоративної мережі;
- розроблено формальну модель станів корпоративної мережі;
- розглянуто корпоративну мережу, що складається з елементів з відомими розподілами часу безвідмовної роботи та часу відновлення. Функціонування мережі відбувається згідно з визначеною схемою розрахунку надійності, де всі елементи поділені на робочі та резервні;
- розглянуто можливі стани елементів у системі, визначено їх можливі причини і формально представлено множину усіх станів корпоративної мережі. Для опису функціонування системи використано матрицю станів, де вектори характеризують стан усіх елементів в конкретний момент часу.

3 РОЗРОБКА ВІДМОВОСТІЙКОЇ СИСТЕМИ РЕЗЕРВУВАННЯ СЕРВЕРНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ ЗАСОБІВ ВІРТУАЛІЗАЦІЇ

3.1 Розробка моделі резервування серверного забезпечення корпоративної мережі

Представимо локальні сервери корпоративної мережі підприємства у вигляді відновлювальної системи із ковзним резервуванням елементів. Схема такої системи показана на рисунку 3.1. Вузли системи представлені фізичними серверами (кластер) на базі яких розгорнута інфраструктура віртуалізації VMware ESXI [37]. Кожен сервер керується гіпервізором, на якому запущені віртуальні машини різного призначення: умово розділені за функціональним призначенням на сервер бази даних (БД) та сервери прикладних додатків.

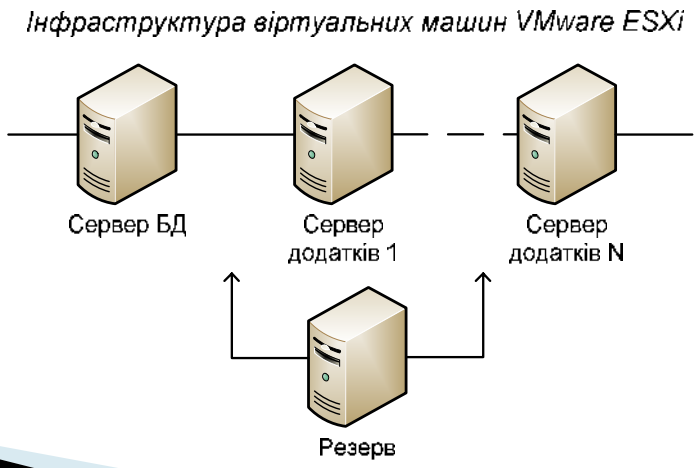


Рисунок 3.1 – Схема ковзного резервування серверів підприємства

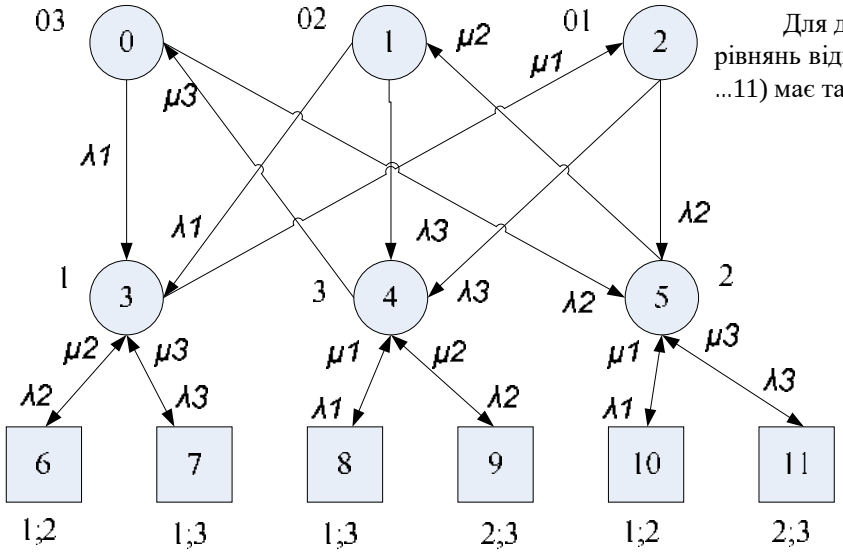


Рисунок 3.2 – Граф станів системи ковзного резервування серверів

Для даної моделі система лінійних алгебраїчних рівнянь відносно стаціонарних ймовірностей p_i, (i = 0; 1; ...11) має такий вигляд:

$$\begin{cases} -(\lambda_1+\lambda_2)p_0+\mu_3 p_4=0 \\ -(\lambda_1+\lambda_3)p_1+\mu_2 p_5=0 \\ -(\lambda_1+\lambda_3)p_2+\mu_1 p_3=0 \\ \lambda_1 p_0+\lambda_1 p_0-(\mu_1+\lambda_2+\lambda_3)p_3+\mu_2 p_6+\mu_3 p_7=0 \\ \lambda_3 p_1+\lambda_3 p_2-(\mu_3+\lambda_1+\lambda_2)p_4+\mu_1 p_8+\mu_2 p_9=0 \\ \lambda_2 p_0+\lambda_2 p_2-(\mu_2+\lambda_1+\lambda_3)p_5+\mu_1 p_{10}+\mu_3 p_{11}=0 \\ \lambda_2 p_3-\mu_2 p_6=0 \\ \lambda_3 p_3-\mu_3 p_7=0 \\ \lambda_1 p_4-\mu_1 p_8=0 \\ \lambda_2 p_4-\mu_2 p_9=0 \\ \lambda_1 p_5-\mu_2 p_{10}=0 \\ \lambda_3 p_5-\mu_3 p_{11}=0 \end{cases}$$

Розв'язавши систему (3.1) у урахуванням умови (3.2) отримуємо значення стаціонарних ймовірностей (таблиця 3.2).

Таблиця 3.2 – Стаціонарні ймовірності системи

p_0	0.5712	p_6	$2.2329\cdot10^{-8}$
p_1	0.2856	p_7	$4.4659\cdot10^{-8}$
p_2	0.1428	p_8	$2.2329\cdot10^{-8}$
p_3	$9.7803\cdot10^{-5}$	p_9	$4.4659\cdot10^{-8}$
p_4	[illegible]	p_{10}	$1.8608\cdot10^{-8}$
p_5	$1.6300\cdot10^{-4}$	[illegible]	$7.4431\cdot10^{-8}$

$$K_Г=\sum_{i=0}^{5} p_i = 0{,}99999977$$

$$T_{відмов}=\frac{K_Г}{\omega}=4\ 404\ 988 \text{ (год).}$$

$$T_{відновл.}=\frac{1-K_Г}{\omega}=0{,}99999999956 \text{ (год).}$$

3.3 Розрахунок перехідних характеристик надійності системи (MATLAB)

```
Clear;
% A x P = E
global l  m;
%l = [0.04, 0.08, 0.1];
%m = [2, 1, 4];
L1 = 1.*365.*24;
L2 = 0.5.*365.*24;
L3 = 0.25.*365.*24;
M1 = 1;
M2 = 1;
M3 = 1;
l = [1./L1, 1./L2, 1./L3];
m = [1./M1, 1./M2,
1./M3];
E = zeros(12,1);
E(1,1) = 1;
A = zeros(12);
% eq. 1
%A(1,1) = -(l(1) + l(2));
%A(1,5) = m(3);
 A(1,:) = 1;
 % eq. 2
A(2,2) = -(l(1) + l(3));
A(2,6) = m(2);
% eq. 3
A(3,3) = -(l(2) + l(3));
A(3,4) = m(1);
% eq. 4
A(4,1) = l(1);
A(4,2) = l(1);
A(4,4) = -(m(1) + l(2) +
l(3));
A(4,7) = m(2);
A(4,8) = m(3);
% eq. 5
A(5,2) = l(3);
A(5,3) = l(3);
A(5,5) = -(m(3) + l(1) +
l(2));
A(5,9) = m(1);
A(5,10) = m(2);
% eq. 6
A(6,1) = l(2);
A(6,3) = l(2);
A(6,6) = -(m(2) + l(1) +
l(3));
A(6,11) = m(1);
A(6,12) = m(3);
% eq. 7
A(7,4) = l(2);
A(7,7) = -m(2);
% eq. 8
A(8,4) = l(3);
A(8,8) = -m(3);
% eq. 9
A(9,5) = l(1);
A(9,9) = -m(1);
% eq. 10
A(10,5) = l(2);
A(10,10) = -m(2);
% eq. 11
A(11,6) = l(1);
A(11,11) = -m(1);
% eq. 12
A(12,6) = l(3);
A(12,12) = -m(3);

P = A^(-1) * E;

K = sum(P(1:6));
w = (l(2) + l(3)) .* P(4) +
...
(l(1) + l(2)) .* P(5) + ...
(l(1) + l(3)) .* P(6);

T = K ./ w;

Tv = (   K) ./ w;

tspan = [0:10000:2
p0 = zeros(12,1);
p0(1) = 1;
[t,p] =
ode45(@odefun1,tspan,p
0);
figure;plot(t, p,
LineWidth=2); grid on
xlabel('t, год.')
ylabel('Ймов.')
legend({'p_0(t)','p_1(t)','p_
2(t)','p_3(t)','p_4(t)'})

Kg = sum(p(:,1:6),2);
 p0 = zeros(6,1);
p0(1) = 1;
[t,p] =
ode45(@odefun2,tspan,p
0);
%figure;plot(t, p)
Pt = sum(p,2);

figure;
plot(t,Kg,t,Pt,LineWidth=2
);grid on
xlabel('t, год.')
ylabel('Ймов.')
legend({'K_г(t)','P(t)'})

H = zeros(6,1);
H(1,1) = -1;
B = zeros(6);

%eq.1
B(1,1) = -(l(1) + l(2));
B(1,5) = m(3);
%eq.2
B(2,2) = -(l(1) + l(3));
B(2,6) = m(2);
%eq.3
B(3,3) = -(l(2) + l(3));
B(3,4) = m(1);
%eq.4
B(4,1) = l(1);
B(4,2) = l(1);
B(4,4) = -(m(1) + l(2)
+l(3));
%eq.5
B(5,2) = l(3);
B(5,3) = l(3);
B(5,5) = -(m(3) + l(1)
+l(2));
%eq.6
B(6,1) = l(2);
B(6,3) = l(2);
B(6,6) = -(m(2) + l(1)
+l(3));

tau = B^(-1) * H;
T1 = sum(tau);

function dpdt =
odefun1(t,p)
global l  m;

dpdt(1,1) = -(l(1) + l(2))
.* p(1) + m(3) .* p(5);
dpdt(2,1) = -(l(1) + l(3))
.* p(2) + m(2) .* p(6);
dpdt(3,1) = -(l(2) + l(3))
.* p(3) + m(1) .* p(4);
dpdt(4,1) = l(1) .* p(1) +
l(1) .* p(2) - ...
(m(1) + l(2) + l(3)) .* p(4)
+ m(2) .* p(7) + m(3) .*
p(8);
dpdt(5,1) = l(3) .* p(2) +
l(3) .* p(3) - ...
(m(3) + l(1) + l(2)) .* p(5)
+ m(1) .* p(9) + m(2) .*
p(10);
dpdt(6,1) = l(2) .* p(1) +
l(2) .* p(3) - ...
(m(2) + l(1) + l(3)) .* p(6)
+ m(1) .* p(11) + m(3) .*
p(12);
dpdt(7,1) = l(2) .* p(4) -
m(2) .* p(7);
dpdt(8,1) = l(3) .* p(4) -
m(3) .* p(8);
dpdt(9,1) = l(1) .* p(5) -
m(1) .* p(9);
dpdt(10,1) = l(2) .* p(5) -
m(2) .* p(10);
dpdt(11,1) = l(1) .* p(6) -
m(1) .* p(11);
dpdt(12,1) = l(3) .* p(6) -
m(3) .* p(12);
end

function dpdt =
odefun2(t,p)
global l  m;

dpdt(1,1) = -(l(1) + l(2))
.* p(1) + m(3) .* p(5);
dpdt(2,1) = -(l(1) + l(3))
.* p(2) + m(2) .* p(6);
dpdt(3,1) = -(l(2) + l(3))
.* p(3) + m(1) .* p(4);
dpdt(4,1) = l(1) .* p(1) +
l(1) .* p(2) - ...
(m(1) + l(2) + l(3)) .* p(4);
dpdt(5,1) = l(3) .* p(2) +
l(3) .* p(3) - ...
(m(3) + l(1) + l(2)) .* p(5);
dpdt(6,1) = l(2) .* p(1) +
l(2) .* p(3) - ...
(m(2) + l(1) + l(3)) .* p(6);

end
```

Для знаходження функції готовності системи $f = K_Г\ (t)$ складемо систему лінійних диференціальних рівнянь відносно перехідних ймовірностей $p_i(t)$, $i = 0; 1...11$:

$$\begin{cases}
\frac{dp_0}{dt} = -(\lambda_1 + \lambda_2)\, p_0 + \mu_3 p_4 \\
\frac{dp_1}{dt} = -(\lambda_1 + \lambda_3)\, p_1 + \mu_2 p_5 \\
\frac{dp_2}{dt} = -(\lambda_2 + \lambda_3)\, p_2 + \mu_1 p_3 \\
\frac{dp_3}{dt} = \lambda_1 p_0 + \lambda_1 p_1 - (\mu_1 + \lambda_2 + \lambda_3) \\
\frac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3 + \lambda_1 + \lambda_2) \\
\frac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3 + \lambda_1 + \lambda_2) \\
\frac{dp_5}{dt} = \lambda_2 p_0 + \lambda_2 p_2 - (\mu_2 + \lambda_1 + \lambda_3) \\
\frac{dp_6}{dt} = \lambda_2 p_3 + \mu_2 p_6 \\
\frac{dp_7}{dt} = \lambda_3 p_3 + \mu_3 p_7 \\
\frac{dp_8}{dt} = \lambda_1 p_4 + \mu_1 p_8 \\
\frac{dp_9}{dt} = \lambda_2 p_4 + \mu_2 p_9 \\
\frac{dp_{10}}{dt} = \lambda_1 p_5 + \mu_1 p_{10} \\
\frac{dp_{11}}{dt} = \lambda_3 p_5 + \mu_3 p_{11}
\end{cases}$$

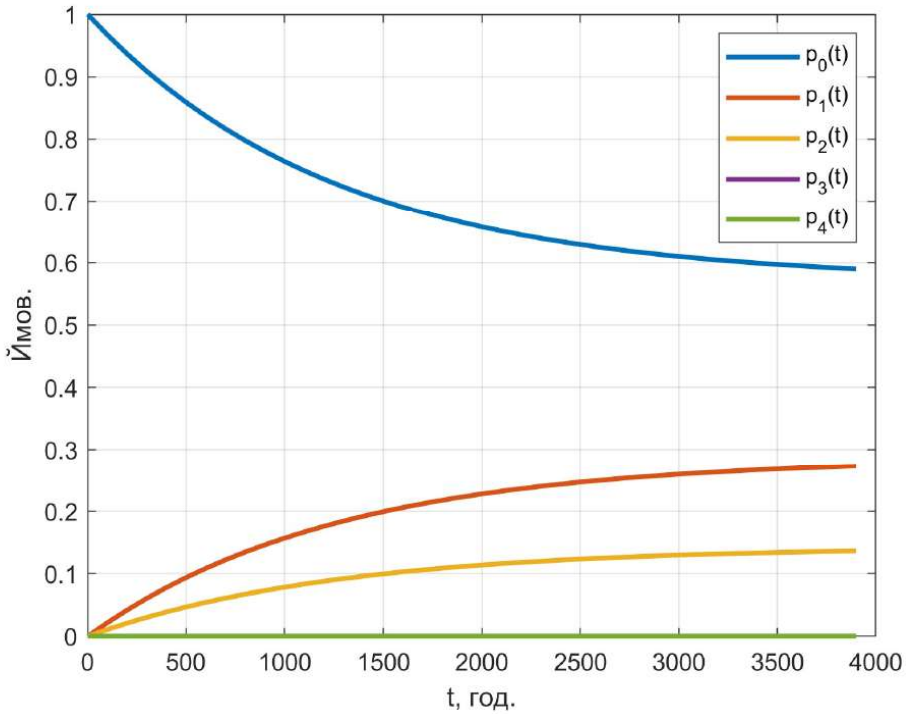


Рисунок 3.3 – Перехідні ймовірності станів системи

Ймовірність безвідмовної роботи знайдемо з перехідних ймовірностей, які розраховуються із відповідної системи диференціальних рівнянь, що були складені на основі вихідного графу станів (рисунок 3.2) для якого заборонені переходи зі станів відмов. Дана система диференціальних рівнянь має вигляд:

$$\begin{cases} \frac{dp_0}{dt} = -(\lambda_1+\lambda_2)p_0 + \mu_3 p_4 \\ \frac{dp_1}{dt} = -(\lambda_1+\lambda_3)p_1 + \mu_2 p_5 \\ \frac{dp_2}{dt} = -(\lambda_2+\lambda_3)p_2 + \mu_1 p_3 \\ \frac{dp_3}{dt} = \lambda_1 p_0 + \lambda_1 p_1 - (\mu_1+\lambda_2+\lambda_3) \\ \frac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3+\lambda_1+\lambda_2) \\ \frac{dp_4}{dt} = \lambda_1 p_1 + \lambda_3 p_2 - (\mu_3+\lambda_1+\lambda_2) \\ \frac{dp_5}{dt} = \lambda_2 p_0 + \lambda_2 p_2 - (\mu_2+\lambda_1+\lambda_3) \end{cases}$$

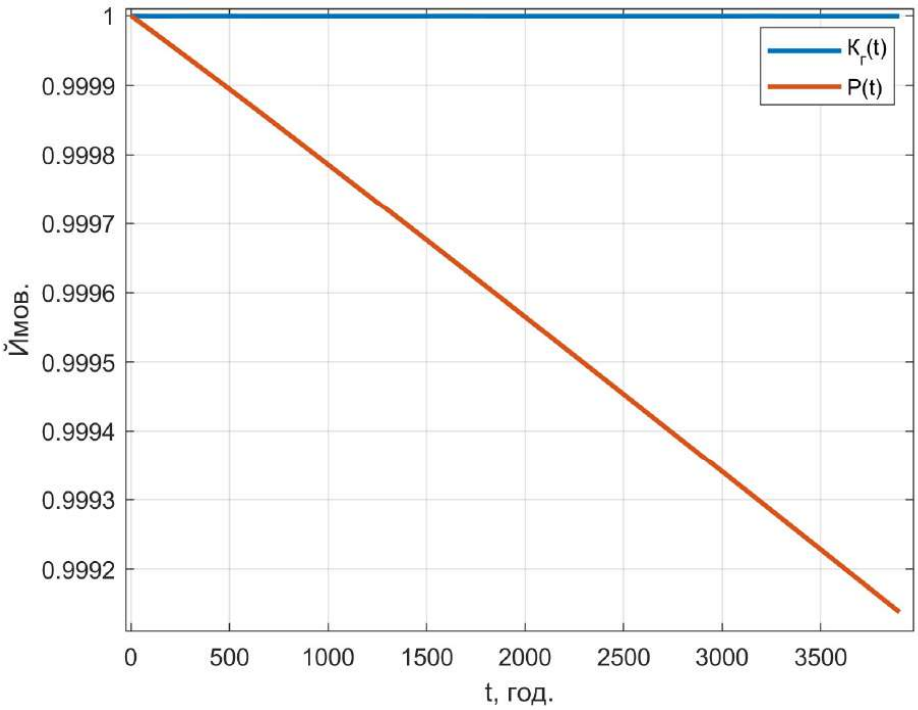


Рисунок 3.4 – Функція готовності системи $K_Г(t)$ та функція безвідмовної роботи $P(t)$

Порівнюючи ймовірність безвідмовної роботи із функцією готовності , остання практично рівна одиниці, отже готовність системи може бути оцінена за допомогою коефіцієнту готовності.

Розрахуємо середній час безвідмовної роботи системи шляхом розв'язання системи лінійних алгебраїчних рівнянь відносно часу перебування у справному стані для системи, що відповідає виправленому графу станів (рисунок 3.2), для якого заборонені виходи із станів відмов. Система рівнянь має вигляд:

(год) (3.8)

$$\begin{cases} -(\lambda_1+\lambda_2)t_0+\mu_3 p_4=-1 \\ -(\lambda_1+\lambda_3)t_1+\mu_2 p_5=0 \\ -(\lambda_2+\lambda_3)t_2+\mu_1 p_3=0 \\ \lambda_1 t_0+\lambda_1 t_1-(\mu_1+\lambda_2+\lambda_3)t_3=0 \\ \lambda_3 t_1+\lambda_3 t_2-(\mu_3+\lambda_1+\lambda_2)t_4=0 \\ \lambda_2 t_0+\lambda_2 t_2-(\mu_2+\lambda_1+\lambda_3)t_5=0 \end{cases}$$

Отже, середній час безвідмовної роботи системи становить:

$$T_c=\sum_{i=0}^{5} t_i = 4\,407\,538$$

Таблиця 3.3 – Середній час перебування системи в справних станах

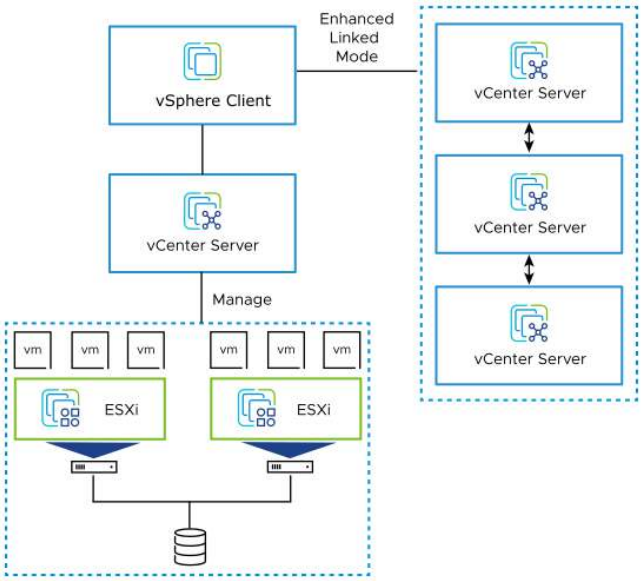
τ_0	2518327 год	τ_3	431 год
τ_1	1258210 год	τ_4	861 год
τ_2	628992 год	τ_5	718 год

Висновки до третього розділу

- В третьому розділі магістерської роботи було виконано наступне:
- розроблено модель ковзного резервування для серверів корпоративної мережі, побудовано граф стані моделі
- розраховано стаціонарні показники надійності системи: стаціонарні ймовірності системи, стаціонарний коефіцієнт готовності та середній час відновлення
- розраховано перехідні характеристики: перехідні ймовірності системи, функція готовності та функція ймовірності безвідмовної роботи

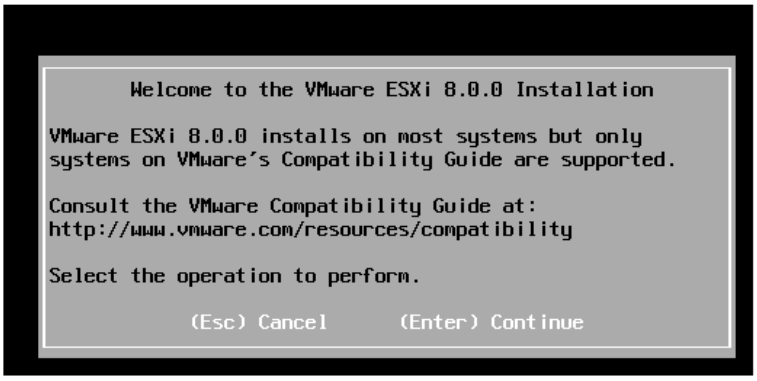
4 РОЗРОБКА ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Встановлення та налаштування гіпервізора VMware ESXi



	Мінімальні вимоги	Рекомендовані вимоги
процесор	1 процесор, 2 ядра	два процесори, чотири і більше ядер на ЦП
оперативна пам'ять	4 ГБ	8 Гбайт або більше
Мережа	один мережевий адаптер 1 Гбіт/с	два мережеві адаптери 1 Гбіт/с
Локальне сховище даних (SATA/SAS)	один диск ємністю 10 Гбайт	RAID 1 із 2=х дисків по 10 Гб.

Рисунок 4.1 – Структурна схема екосистеми vSphere.



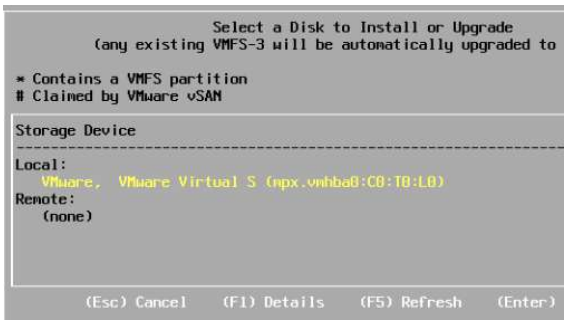


Рисунок 4.2 – Початок встановлення гіпервізора ESXi

Рисунок 4.3 – процес встановлення гіпервізора ESXi:
вибір локального диску для розміщення системи (а); введення надійного паролю адміністратора (б); завершення інсталяції (в)

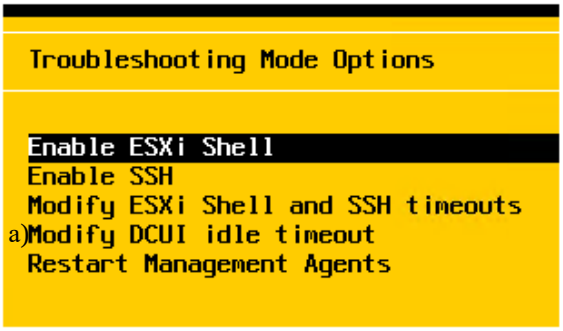
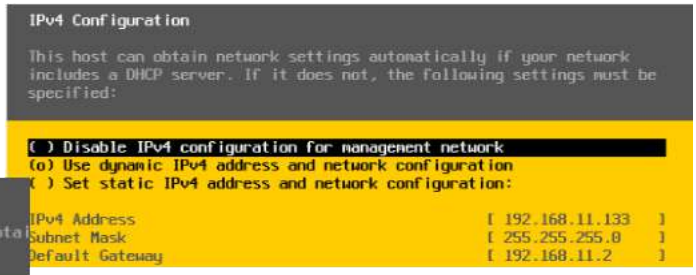
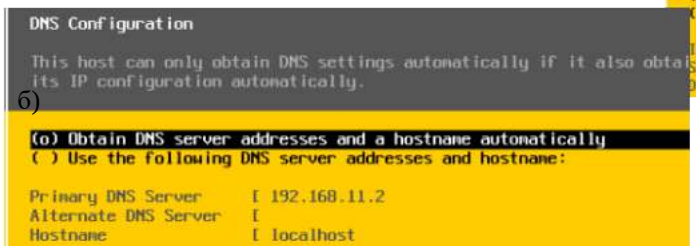


Рисунок 4.4 – Меню Troubleshooting Mode

а)



б)



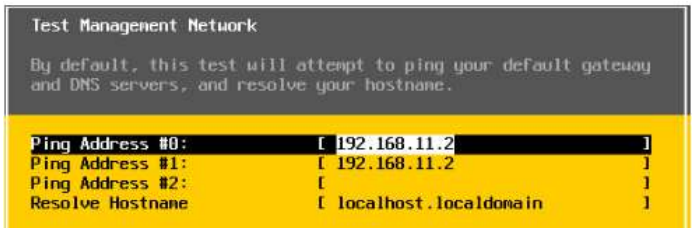
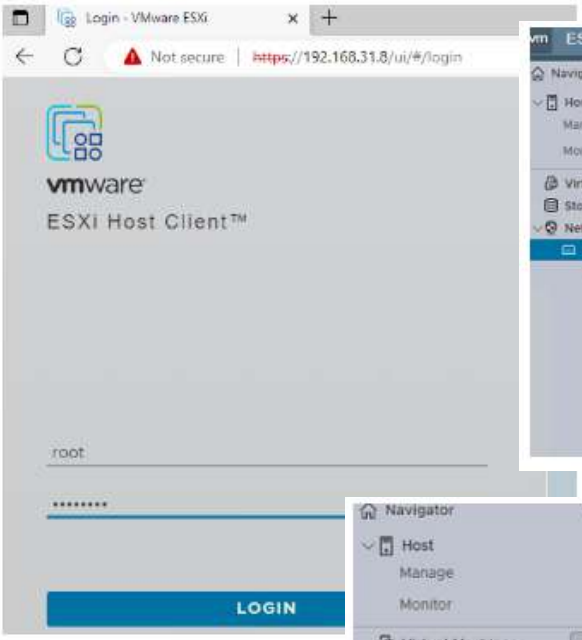


Рисунок 4.5 – Меню мережевих налаштувань інтерфейсі ESXi: налаштування мережі IPv4 (а, б); налаштування служби DNS (в); тестування мереж – ping (г)



Веб-інтерфейс керування VMware Hypervisor

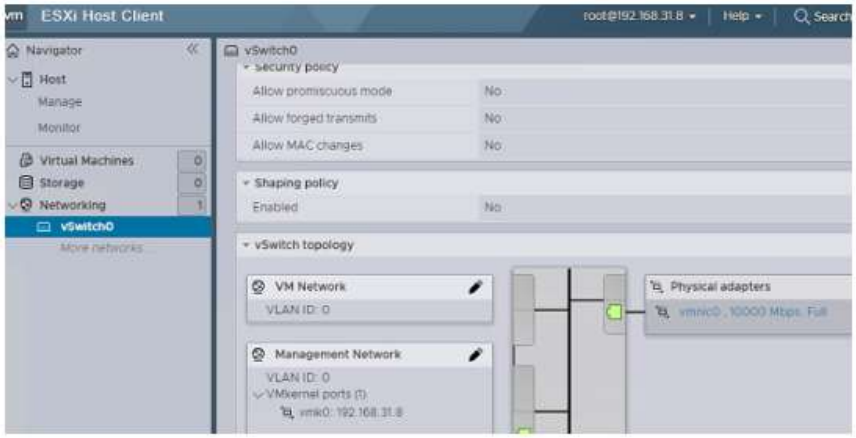


Рисунок 4.7 – Налаштування віртуального комутатора

Рисунок 4.8 – Керування сховищем даних

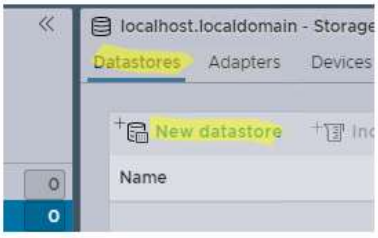
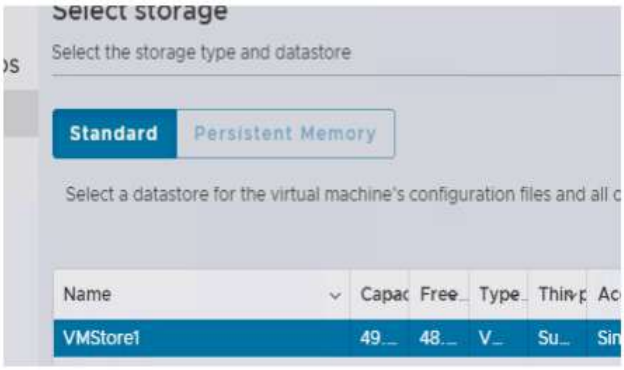


Рисунок 4.9 – Створення нового сховища



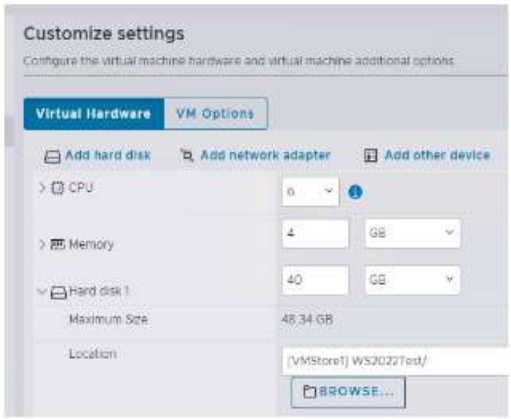


Рисунок 4.10 – Створення нової віртуальної машини: введення назви (а), вибір сховища (б) та базова конфігурація (в)

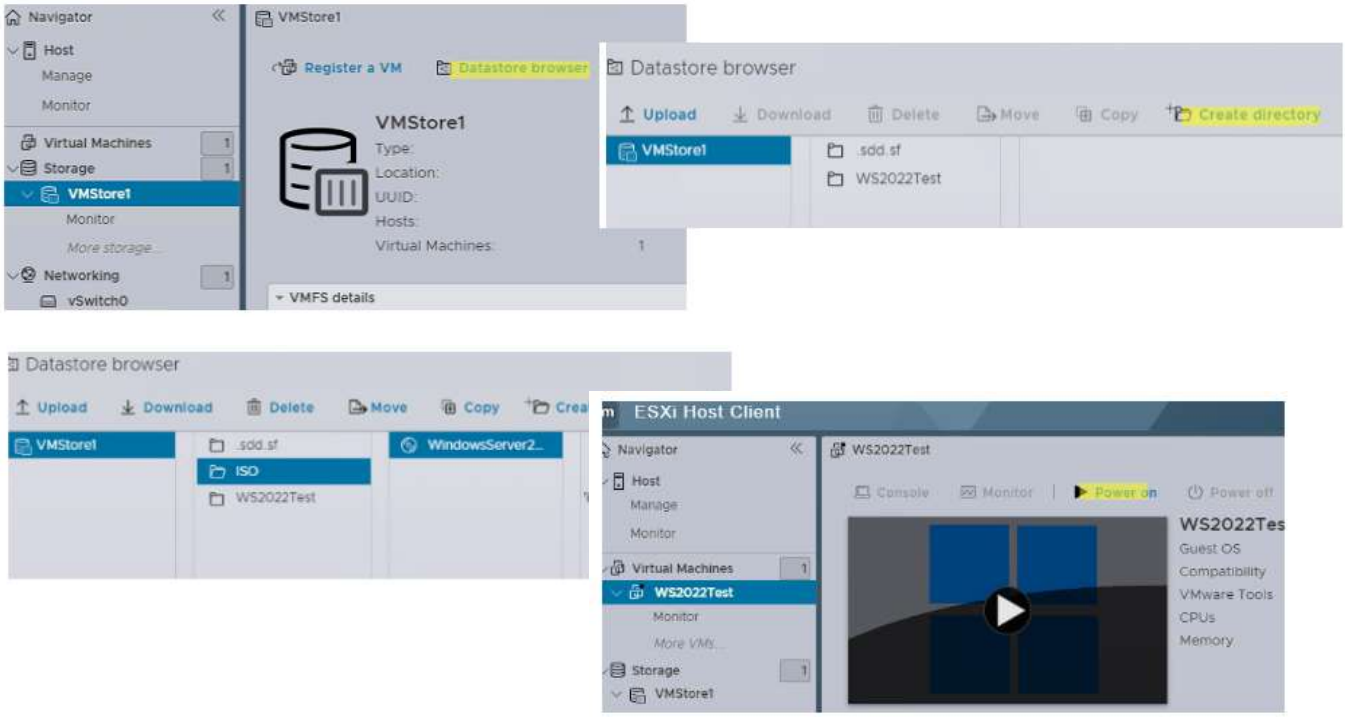


Рисунок 4.11 – Завантаження ISO образу для гостьової машини та запуст процесу встановлення

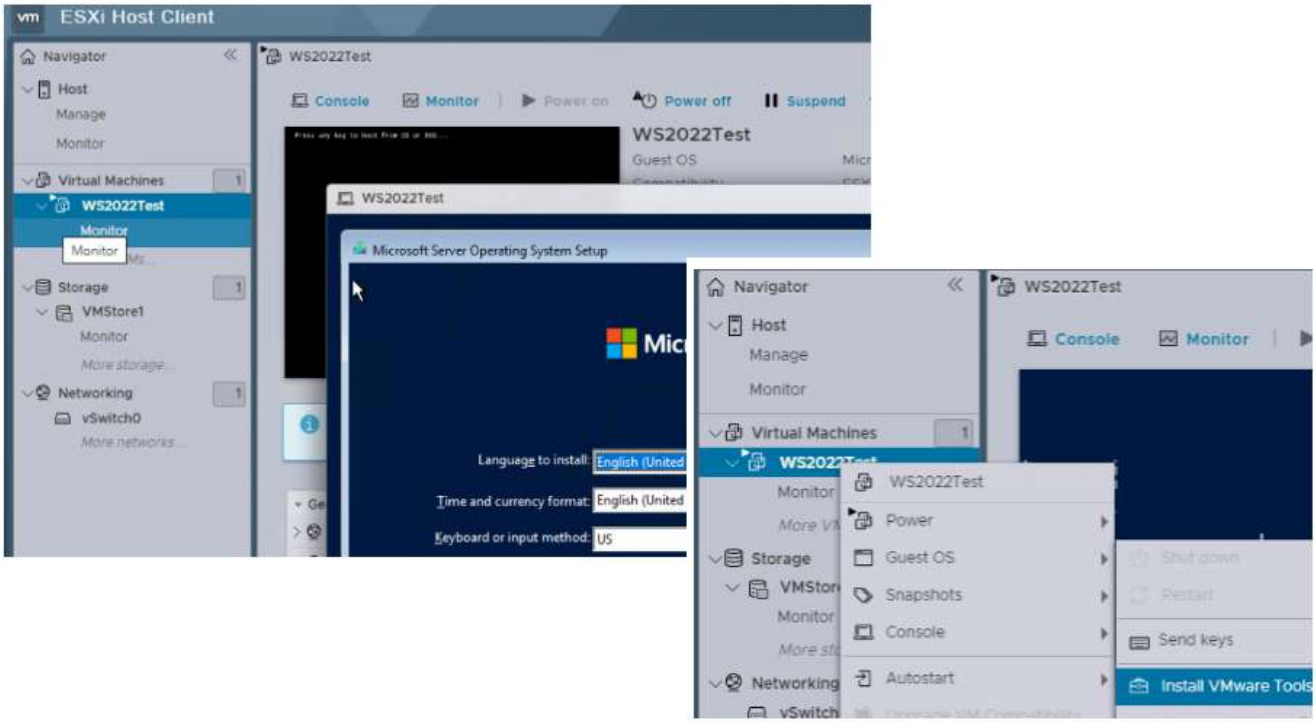
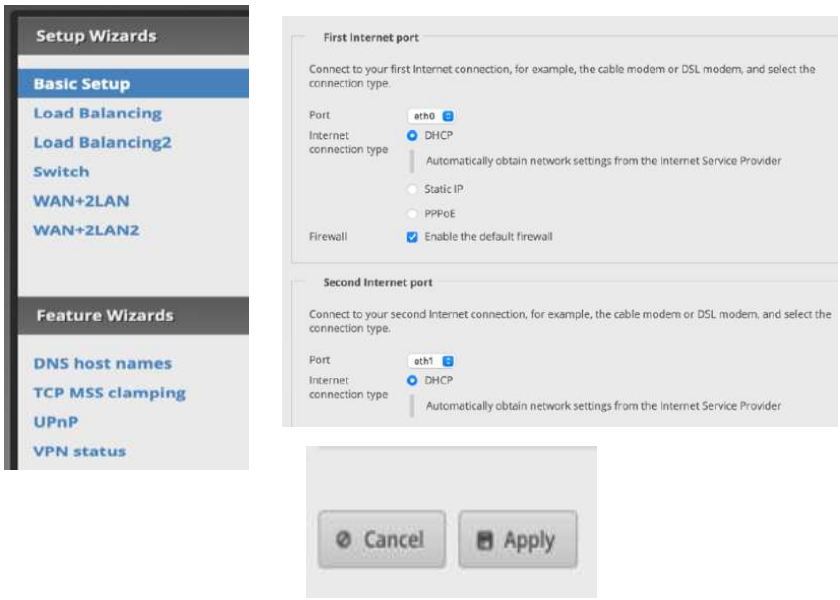


Рисунок 4.12 – Запуск гостьової ОС

4.3 Налаштування системи Dual-WAN



В якості шлюзу було обрано маршрутизатор сімейства EdgeRouter, усі моделі якого можуть підтримувати більше одного WAN-з'єднання. Для налаштування Dual-WAN спочатку необхідно увійдіть до системи налаштувань EdgeRouter та перейти у меню базових налаштувань пристрою (Рисунок 4.13).

Після перенавантаження слід переконатись, що обом інтерфейсам WAN було призначено IP-адресу.

Тепер у разі відключення одного із WAN-з'єднань, а трафік спрямовуватиметься через інший інтерфейс WAN – рисунок 4.15.

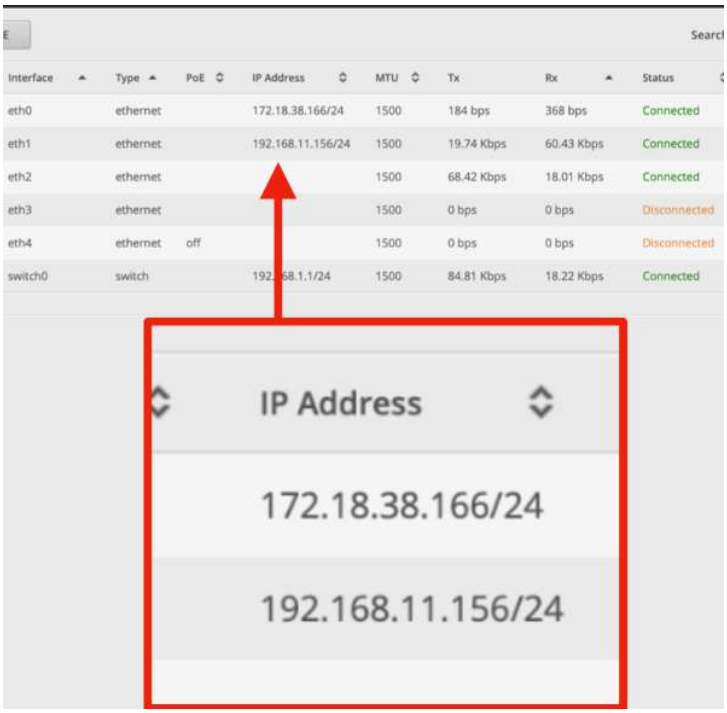


Рисунок 4.14 – Перевірка налаштування Dual-WAN

Висновки до четверного розділу

- В четвертому розділі магістерської роботи було виконано наступне:
- розгорнуто та налаштовано серверних гіпервізора VMware ESXi для побудови на його базі відмово стійкого ядра корпоративної інфраструктури підприємства
- встановлено та налаштовано віртуальну машину від управлінням операційної системи Windows;
- налаштовано резервний канал доступу до мережі Інтернет на базі технології Dual WAN.

ВИСНОВКИ

Дослідження корпоративних мереж виявило важливі вимоги до їхньої надійності та відмовостійкості, які визначаються як підвищеними вимогами бізнес-процесів, так і зростанням кількості кіберзагроз. Забезпечення надійності мережі є стратегічно важливою задачею для підтримки функціонування підприємства та безпеки обміну даними.

Мета роботи була сформульована у підвищенні відмовостійкості корпоративної мережі із безпроводовим доступом. Досліджено базову архітектуру мережі, виявлено вразливості та можливі відмови. У результаті були сформульовані та вирішені важливі технологічні задачі щодо підвищення надійності та відмовостійкості корпоративних безпроводових мереж шляхом включаючи надлишковості за методом ковзного резервування серверного устаткування.

Методи математичного аналізу, чисельні методи та теорія надійності були використані для моделювання та аналізу системи. Створено узагальнену математичну модель та формальну модель станів корпоративної мережі.

Отримані результати включають подальший розвиток методів підвищення надійності, введення резервного серверного устаткування та резервного каналу доступу Інтернет за допомогою технології Dual WAN. Також було налаштовано серверне забезпечення на базі гіпервізора VMware ESXI та запропоновано схему резервування для досягнення відмовостійкості.

Завідувачу кафедри
телекомунікацій, медійних та
інтелектуальних технологій (ТМІТ)
Сергію ПІДЧЕНКУ
студента 2 курсу, гр. ТРм-22-1
Максима СЛОБОДЯНА

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1.12.2023 _____ Слободян М. О.
дата підпис

Anti-Plagiarism v-15.257

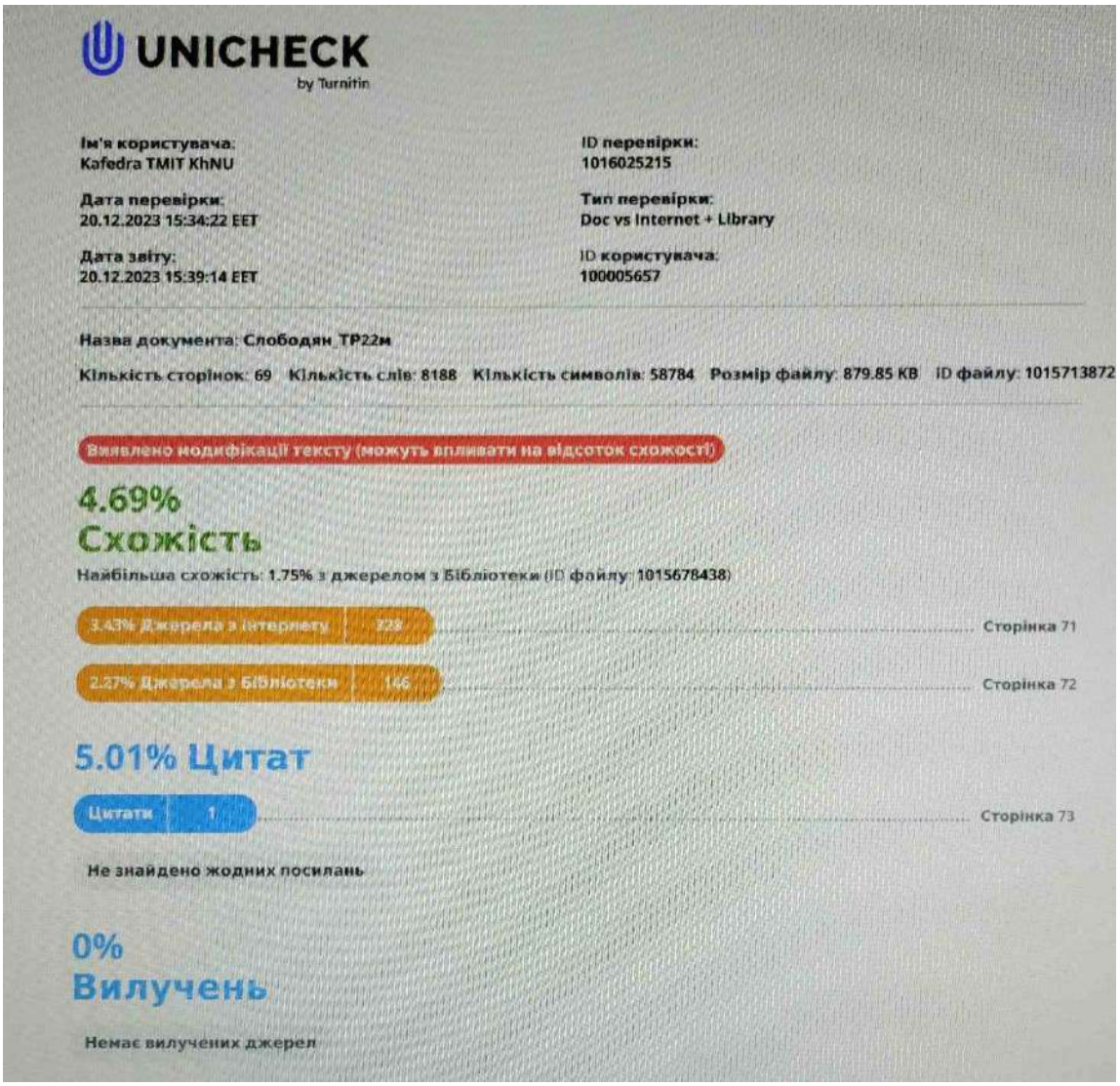
Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 124092 Название: Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж Добавлено в БД: 2023-12-20 Авторы: Слободян Максим Олегович Руководители: Підченко Сергій Костянтинович Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	43848	627	616 (1%)	9 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы



РІШЕННЯ КАФЕДРИ

ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: *Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж*

Автор: **Слободян Максим Олегович**

Спеціальність: **172 Телекомунікації та радіотехніка**

Освітня програма: **Телекомунікації та радіотехніка**

Науковий керівник: **д.т.н., проф. Підченко Сергій Костянтинович**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 4,69% відносяться до загальновживаних фраз та не є плагіатом. Найбільша схожість з одним джерелом – 1,75%

Відповідальний за контроль
плагіату за системою Unicheck та Anti-Plagiarism (ХНУ):

20.12.23р. Олег ПИВОВАР

Зав. каф. ТМІТ Сергій ПІДЧЕНКО

20.12.23р.

РЕЦЕНЗІЯ

на магістерську дипломну роботу
студента групи ТРм-22-1 Слободяна М.О.
«Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж»

Корпоративні мережі, що використовуються для підтримки функціонування на їхній базі інфраструктури підприємства, характеризуються підвищеними вимогами щодо безвідмовної роботи із забезпечення підтримки усіх бізнес-процесів. Корпоративна мережа призначена для підтримки діяльності підприємства, і її користувачами є лише співробітники цього підприємства (гостьовий сегмент може бути передбачено для зони очікування, або безпосередньо для надання доступу клієнтам, якщо дана компанія веде роботу із клієнтами). Метою даної роботи є підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі задачі: аналіз базової архітектури корпоративної телекомунікаційної мережі з позиції відмовостійкості та вразливостей до кібератак; удосконалення базової архітектури корпоративної телекомунікаційної мережі шляхом введення в систему елементів надлишковості та механізмів живучості; проведено імітаційне моделювання відмовостійкої корпоративної мережі; виконано проектування відмовостійкої корпоративної інфраструктури на базі мережі із захищеними безпроводовими каналами доступу, надійними механізмами резервного копіювання та резервним каналом доступу до мережі Інтернет.

В магістерській роботі набув подальшого розвитку метод підвищення надійності корпоративної мережі із безпроводових доступом шляхом забезпечення резервування серверного устаткування, яке побудоване на базі інфраструктури віртуалізації; а також впровадження механізму резервного каналу доступу до мережі Інтернет на базі технології Dual-Wan.

Позитивною стороною роботи є встановлене та налаштоване серверне забезпечення корпоративної мережі та IT інфраструктури підприємства на базі гіпервізора VMware ESXI та запропонована схема резервування, яка дозволить забезпечити відмовостійку роботу системи шляхом введення ковзного резервного серверного вузла.

Апробацією результатів дослідження є стаття у фаховому виданні Слободян М.О. Модель хаотичної надширокосмугової системи передачі інформації для бездротових сенсорних мереж / М.О. Слободян // Вісник Хмельницького національного університету. Технічні науки. – 2023. – № 2. – С. 284–289.

В цілому магістерська дипломна робота Максима Слободяна є актуальною в сфері сучасних технологій телекомунікацій та радіотехніки, виконана на високому науково-технічному рівні та заслуговує оцінки «відмінно».

Рецензент:
зав. кафедри кібербезпеки, к.т.н., доцент Юрій КЛЬОЦ

ВІДГУК

на магістерську дипломну роботу

студента групи ТРм-22-1 Слободяна М. О.

«Метод підвищення надійності та відмовостійкості корпоративних безпроводових мереж»

Метою роботи є підвищення надійності та відмовостійкості корпоративної мережі із безпроводових каналом доступу.

В роботі проведено детальний аналіз можливих відмов та несправностей корпоративних мереж, які спричинені як власними відмова, так і зловмисними діями, спрямованими на кібератак на вразливості системи; також дана класифікація таких вразливостей; дано характеристику корпоративної мережі підприємства як базу для розгортання на її базі інфраструктури підприємства та розглянуто типові топології таких мереж, а саме зіркоподібну топологію та змішану топологію на прикладі реального технологічного рішення; отримав подальшого розвитку метод підвищення надійності корпоративної мережі із безпроводовим доступом шляхом забезпечення резервування серверного устаткування, яке побудоване на базі інфраструктури віртуалізації; а також впровадження механізму резервного каналу доступу до мережі Інтернет на базі технології Dual-Wan; запропонована схема резервування, яка дозволить забезпечити відмовостійку роботу системи шляхом введення ковзного резервного серверного вузла.

Під час виконання дипломної роботи Максим Слободян проявив себе старанним, ініціативним фахівцем з високим рівнем знань та вмінням їх застосовувати для вирішення завдань в галузі електроніки та телекомунікацій.

В цілому магістерська дипломна робота виконана на високому науково-технічному рівні, а її автор Максим Слободян заслуговує на оцінку «відмінно».

Керівник:
д.т.н., професор Сергій ПІДЧЕНКО