Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі»

КвРКІП. 170151.23.14 ПЗ

Виконав: студентка 2 курсу, група КІ2м-21-1 _____ Сахнюк В.В.
Підпис Ініціали, прізвище

Керівник доктор техн. наук, професор _____ Лисенко С.М.
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
03 05 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітньо-наукова програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

" 01 " 09 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Сахнюк Віталіні Валентинівні

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

Керівник проекту (роботи) Говорущенко Т.О., д.т.н., професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 09.01.2023 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих методів виявлення кібер-загроз в комп'ютерних системах

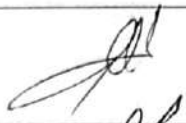
Моделювання динамік збоїв та забезпечення стійкості корпоративної комп'ютерної мережі

Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

Реалізація та дослідження методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

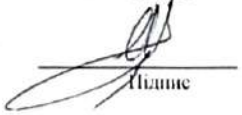
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_06_»_____09_____2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	05.09.2022	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2022	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2022	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2022	виконано
5	Робота над науковою статтею	05.01.2023	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2023	виконано
8	Оформлення пояснювальної записки згідно вимог	15.04.2023	виконано
9	Попередній захист	18.04.2023	виконано
10	Захист ДРМ на засіданні ЕК	До 10.05.2023	

Студент  Підпис В.В. Сахнюк Ініціали, прізвище

Керівник роботи  Підпис С.М. Лисенко Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

Автор роботи: Віталіна Сахнюк

Керівник роботи: Сергій Лисенко

Пояснювальна записка: 84 с., 16 рис., 2 табл., 4 дод., 85 джерел.

СТІЙКІСТЬ МЕРЕЖІ, АТАКИ, ПРОГРАМНО-АПАРТНІ ЗАСОБИ, ЛІНІЙНІ СТАЦІОНАРНІ СИСТЕМИ.

Об'єктом дослідження є процес забезпечення стійкості комп'ютерних мереж.

Предметом дослідження є метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі.

Метою кваліфікаційної роботи магістра є забезпечення стійкості комп'ютерних мереж в умовах здійснення загроз.

Для розв'язання поставлених задач використовувалися основні положення теорії комп'ютерних мереж та систем, системного аналізу, моделювання, методів аналізу даних, теорії математичної статистики, теорії дискретної математики.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі, який на відміну від відомих для забезпечення стійкості здійснює додаткову модифікації топології комп'ютерної мережі шляхом її віртуального розширення, та який здійснює виявлення впливових розповсюджувачів, а також передбачає знаходження найбільш критичних вузлів в комп'ютерній мережі, що її порушують стійкість;

− набули подальшого розвитку програмно-технічні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

Практична значимість отриманих результатів полягає у тому, що в результаті виконаного наукового дослідження буде розроблено апаратно-програмні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ 6

ВСТУП 7

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ВИЯВЛЕННЯ КІБЕР-ЗАГРОЗ В КОМП'ЮТЕРНИХ СИСТЕМАХ 9

1.1 Аналіз відомих методів забезпечення стійкості корпоративної комп'ютерної мережі стійкості комунікаційних мереж 9

1.2 Виклики мережі 11

1.3 Аспекти стійкості 15

1.4 Існуючі підходи до забезпечення стійкої маршрутизації 19

1.4.1 Еластична маршрутизація в сітчастих мережах 20

1.4.2 Схеми резервування ресурсів резервного шляху в мережевих мережах 21

1.5 Відновлення 23

1.6 Використання ресурсів відновлення 23

1.6.1 Область операцій відновлення 25

1.6.2 Рівень операцій відновлення 25

1.7 Висновки та постановка задачі 28

2 МОДЕЛЮВАННЯ ДИНАМІК ЗБОЇВ ТА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ 30

2.1 Здійснення моделювання комп'ютерних мереж 30

2.2 Методи дослідження стійкості комп'ютерної мережі 34

2.2.1 Методи моделювання 34

2.2.2 Методи аналізу 35

2.2.3 Застосування метаевристики для моделювання стійкості комп'ютерної мережі 36

2.2.4 Отримання ациклічних графів при моделювання стійкості комп’ютерних мереж 37

2.2.5 Методи проєктування стійких комп’ютерних мереж 39

2.2.6 Аналітичний підхід у моделюванні складних мереж 39

2.3 Моделювання епідемій у некерованій мережі за допомогою ланцюга Маркова 41

2.4 Моделювання епідемій в мережах з використанням системного підходу LTI 45

2.5 Чисельний підхід вирішення задачі моделювання стійкості комп’ютерної мережі 47

2.6 Висновок 48

3 МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ 49

3.1 Теорія лінійних стаціонарних систем та явища розповсюдження в мережах як основа методу синтезу апаратно-програмних засобів забезпечення стійкості 49

3.1 Представлення мереж як лінійної стаціонарної системи 49

3.2 Стійкість комп’ютерної мережі в умовах епідемій шляхом застосування віртуального розширення мережі 55

3.2.1 Дослідження стійкості комп’ютерної мережі в умовах невизначеної передачі даних та віртуального розширення мережі 60

3.2.2 Оброблення вхідних даних, отриманих зі змодельованої комп’ютерної мережі 64

3.3 Виявлення впливових розповсюджувачів, що порушують стійкість мережі 66

3.4 Знаходження найбільш критичних вузлів в комп’ютерній мережі 69

3.5 Знаходження множини k найбільш критичних вузлів мережі 72

3.6 Висновок 73

4 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ МЕТОДУ СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ 75

4.1 Експериментальні дослідження методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі 75

4.2 Мережеві дані для дослідження 81

4.3 Застосування методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі 83

4.4 Висновки 88

ВИСНОВКИ 89

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 91

ДОДАТОК А 3

ДОДАТОК Б 11

ДОДАТОК В 12

ДОДАТОК Г 14

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КМ – комп’ютерна мережа

ЛСС – лінійна стаціонарна система

БД - база даних

БПР - блок прийняття рішень

ГА - генетичний алгоритм

ОС - операційна система

ПЗ - програмне забезпечення

ВСТУП

Проблеми стійкості комп'ютерних мереж можуть виникати з різних причин і мати різні наслідки. Ось кілька загальних проблем, які можуть вплинути на стійкість комп'ютерних мереж:

Відмова мережевого обладнання, такого як маршрутизатори, комутатори, сервери або кабелі, може призвести до втрати зв'язку в мережі. Це може статися через фізичну поломку, електричні перешкоди, програмні помилки або злам.

Збільшення кількості користувачів в мережі може призвести до перевантаження мережевих ресурсів, таких як пропускна здатність, швидкість передачі даних, процесорні ресурси тощо, що може призвести до зниження стійкості мережі та погіршення її продуктивності.

Комп'ютерні мережі можуть бути піддаються кібератакам, таким як віруси, хакерські атаки, DDoS-атаки тощо. Ці атаки можуть призвести до втрати доступу до мережі, втрати даних або пошкодження мережевої інфраструктури.

Неправильна конфігурація мережевого обладнання або програмного забезпечення може призвести до проблем зі стійкістю мережі. Неправильні налаштування маршрутизації, фаєрволів, VLAN, VPN та інших мережевих параметрів можуть призвести до неправильної роботи мережі та втрати зв'язку.

Відсутність резервування або недостатня резервування мережевих ресурсів може призвести до втрати доступності мережі.

Актуальність роботи полягає в розробці удосконаленого метод синтезу апаратно-програмних засобів, який уможливить забезпечення стійкості корпоративної комп’ютерної мережі в умовах здійснення загроз.

Метою кваліфікаційної роботи магістра є забезпечення стійкості комп’ютерних мереж.

Поставлена мета досягається розв’язанням таких основних задач:

– дослідити методи забезпечення стійкості корпоративної комп’ютерної мережі;

– проаналізувати сучасні програмно-технічних засоби забезпечення стійкості корпоративної комп’ютерної мережі;

– дослідити та описати моделювання комп’ютерних мереж, описати методи моделювання, аналізу мереж в моменти здійснення негативних зовнішніх впливів на мережу, що впливає на її стійкість;

– розробити метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі;

– реалізувати метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі.

Об’єктом дослідження є процес забезпечення стійкості комп’ютерних мереж.

Предметом дослідження є метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі.

Наукова новизна отриманих результатів:

1. Набув подальшого розвитку метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі, який на відміну від відомих для забезпечення стійкості здійснює додаткову модифікації топології комп’ютерної мережі шляхом її віртуального розширення, та який здійснює виявлення впливових розповсюджувачів, а також передбачає знаходження k найбільш критичних вузлів в комп’ютерній мережі, що її порушують стійкість.

2. Набули подальшого розвитку програмно-технічні засоби забезпечення стійкості корпоративної комп’ютерної мережі.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження буде розроблено апаратно-програмні засоби забезпечення стійкості корпоративної комп’ютерної мережі.

Для розв’язання поставлених задач використовуються основні положення теорії комп’ютерних мереж та систем, системного аналізу, моделювання, методів аналізу даних, теорії математичної статистики, теорії дискретної математики.

За темою кваліфікаційної роботи магістра опублікована одна стаття у фаховому науковому виданні в фаховому журналі «Вісник Хмельницького національного університету» №2 за 2023 рік [1].

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ВИЯВЛЕННЯ КІБЕР-ЗАГРОЗ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Аналіз відомих методів забезпечення стійкості корпоративної комп'ютерної мережі стійкості комунікаційних мереж

Несправності елементів комунікаційної мережі неминучі. Вони можуть виникнути внаслідок різних викликів, у тому числі природних сил (наприклад, ураганів, землетрусів), людських помилок (наприклад, обрізання кабелю) або зловмисних атак, і це лише деякі з них. Незважаючи на очевидну різноманітність їхніх характеристик, їх об'єднує спільна риса: їх неможливо усунути.

Наші повсякденні справи, які стають все більш залежними від послуг комунікаційних мереж, відповідають за експоненціальне зростання обмінюваної інформації. Як наслідок, нові збої мережевих каналів (або вузлів) призводять до значних втрат даних і прибутку. З постійно спостережуваним розширенням охоплення комунікаційних мереж у напрямку підтримки майже всіх видів діяльності нашого суспільства очікується, що негативні наслідки збоїв лише посилюватимуться.

Більшість порушень маршрутизації в мережах зв'язку є результатом випадкових несправностей каналів/комутаційних пристроїв [1, 2], включаючи, наприклад, розрізання кабелю під час вуличних робіт (переважно розкопок), пошкодження підводного кабелю рибальськими суднами або збої в електропостачанні. Згідно [3], збої окремих каналів відіграють головну роль у глобальних мережах, охоплюючи близько 70 % усіх подій збоїв. У мережах дальнього зв'язку на кожні 10 км оптоволоконного зв'язку обрив кабелю відбувається раз на 12 років [4].

Збої в з'єднанні інколи можуть тривати кілька днів/тижнів і, таким чином, спричиняти значне зниження продуктивності мережі. Проблема ускладнюється в бездротових мережах через часову залежність характеристик зв'язку від різних факторів, включаючи погодні збої. Однак у локальних мережах із дротовими з'єднаннями частка відмов вузлів у порівнянні з усіма відмовами зазвичай більша

завдяки можливості забезпечити кращий фізичний захист коротших з'єднань. Локалізація несправностей із подальшим необхідним ремонтом з'єднань (або вузлів) може тривати від годин до днів, що означає серйозні збої в роботі мережевих служб.

Тому існує виправдана потреба у розробці мережевих механізмів автоматичної реконфігурації, зокрема відповідальності за відновлення мережевих послуг до моменту фізичного усунення несправностей елементів мережі. Без будь-якого вбудованого механізму відновлення пошкодженого трафіку значна частина мережі може незабаром стати марною з точки зору клієнтів.

Щоб боротися з несправностями елементів мережі, необхідно спочатку проаналізувати виклики, відповідальні за їх виникнення.

Однак різноманітність характеристик виклику робить завдання ідентифікації виклику в реальному часі досить складним і часто потребує багатоетапного підходу. Також важливо ідентифікувати проміжні події, що відбуваються перед будь-яким збоєм служби, тобто несправності та помилки, що стосуються елементів мережі, що є необхідним для забезпечення відповіді механізмів відновлення мережі в реальному часі.

Різноманітність комунікаційних мережевих технологій, а також викликів, що викликають диференційовані сценарії відмови, є причиною існування ряду дисциплін щодо стійкості мережі, посилаючись на підходи до проектування мережі для забезпечення безперервності обслуговування (зокрема, включаючи живучість, стійкість до відмов, стійкість до трафіку та механізми стійкості до збоїв). Аналіз стійкості комунікаційних мереж може, у свою чергу, виконуватися з використанням вимірюваних характеристик, тобто атрибутів надійності мережі (таких як надійність і доступність), безпеки або продуктивності – все це пов'язано з передбачуваною якістю обслуговування та включено до рекомендацій Міжнародної телекомунікації. Союз – Сектор стандартизації телекомунікацій (ITU-T) і Інженерна робоча група Інтернету (IETF).

Останні методи відновлення функціонування мережі були в основному розроблені для топологій сітчастих мереж і походять від відповідних методів,

запропонованих для кільцевих оптичних мереж. Незалежно від характеристик мережі, альтернативні шляхи, хоча й забезпечують автоматичне відновлення після збоїв, завжди вимагають додаткових мережевих ресурсів (зазвичай пов'язаних із пропускною здатністю зв'язку).

Класифікація механізмів резервування ресурсів альтернативних шляхів на основі численних критеріїв, найважливіші з яких включають: методи налаштування резервного шляху, обсяг процедури відновлення, а також використання мережевих ресурсів. Особлива увага приділяється представленню методів спільного використання ресурсів альтернативних шляхів для зменшення кількості пропускної здатності каналу, необхідної для встановлення альтернативних шляхів. Загалом можна спостерігати компроміс між отриманим співвідношенням додаткових ресурсів і часом, необхідним для активації альтернативних шляхів. Презентація основних методів обчислення альтернативних шляхів також розширена обговоренням результуючої обчислювальної складності.

Забезпечення стійкості наскрізної передачі часто передбачає проблеми, пов'язані з багатодомною маршрутизацією, тобто маршрутизацією між кількома доменами, кожен з яких визначається на основі географічного масштабу або власності, де через аспекти конфіденційності точна інформація про маршрутизацію не передається між доменами.

1.2 Виклики мережі

Комунікаційні мережі стикаються з великою групою проблем, усвідомлення яких має вирішальне значення для проектування та планування мережі. Згідно [5], виклик можна визначити як характеристику/умову, яка може статися як подія, що впливає на нормальну роботу мережі. Основні виклики для комунікаційних мереж:

1. масштабні катастрофи
2. соціально-політичні та економічні
3. залежні невдачі
4. людські помилки

5. зловмисних атак
6. незвичайний трафік
7. екологічні виклики

Масштабні катастрофи можуть бути викликані стихійними лихами (такими як стихійні лиха), включаючи землетруси (наприклад, землетрус у Тайвані 2006 року [6], землетрус у Веньчуані 2008 року [7], землетрус у Японії 2011 року [8] тощо), або урагани (наприклад, Катріна [9]) призводять до значних порушень зв'язку, а також комунікаційного обладнання (вузлів). Крім земних або метеорологічних причин, природні катаклізми можуть також бути результатом космологічних подій, включаючи, наприклад, геомагнітні бурі [10]. Іншим джерелом масштабних катастроф є людська діяльність. Такі антропогенні катастрофи можуть бути спричинені або зловмисними діями, або виникнути через ігнорування ранніх попереджень під час роботи системи.

Соціально-політичні та економічні виклики включають навмисну діяльність (також терористичні акти), спрямовану на порушення нормальної роботи мережі, наприклад, у відповідь на політичні рішення або просто для досягнення переваги на економічних ринках.

Залежні несправності стосуються викликів, які можуть призвести до каскаду збоїв, наприклад, після збою системи (або її частини), що пропонує послугу іншій системі [11]. Приклади включають електромережі, що забезпечують живлення для Інтернету.

Людські помилки мають на увазі незловмисну діяльність людини. Вони включають, наприклад, помилки неправильної конфігурації, що є результатом людської некомпетентності. Як наслідок, комунікаційні мережі можуть навіть зіткнутися з катастрофічними збоями.

Зловмисні атаки - це ще одна група викликів, які стосуються навмисних дій, спрямованих на те, щоб викликати якомога більше збоїв, як правило, спрямованих на найважливіші програмні/апаратні елементи мережевої інфраструктури.

Незвичайний трафік може бути проблемою, якщо його обсяг перевищує межі (тобто верхню межу), прийняті на етапі проектування мережі. Такий додатковий

трафік може бути вставлений у мережу, наприклад, після виникнення катастрофічної події, яка не обов’язково порушує саму мережеву інфраструктуру, але призводить до значного збільшення кількості одночасних запитів на отримання інформації.

Екологічні виклики у свою чергу залежать від характеристик середовища спілкування. Вони пов'язані, наприклад, з аспектами мобільності в бездротових ad-hoc мережах (і, зокрема, з залежними від часу характеристиками бездротових з'єднань).

Незалежно від проблеми, найважливіші аспекти стосуються характеристик, які можна виміряти в просторі та в часі. Вплив збою на продуктивність комунікаційної мережі може відрізнятися від початкового обсягу/тривалості виклику. Наприклад, атака, яка є проблемою, пов’язаною з одним вузлом, може вплинути на продуктивність усієї мережі.

Відповідно до [12, 13], будь-яку мережеву проблему можна класифікувати на основі детальних критеріїв, включаючи причину (природна, створена людиною або залежна від проблеми), межі (внутрішні чи зовнішні), ціль (пряма чи побічна), мета (незловмисна). корисливий або зловмисний), намір (ненавмисний або навмисний), здатність (випадкова чи некомпетентність), розмір (апаратне забезпечення, програмне забезпечення, протоколи чи трафік), домен (середовище, мобільність, затримка чи енергія), сфера (вузли, посилання або область), значимість

Виявлення проблем у режимі реального часу часто є складним завданням, особливо коли вони мають низку спільних симптомів. Наприклад, спостережуване збільшення трафіку може бути наслідком спроби атаки розподіленої відмови в обслуговуванні (DDoS) або просто законного перевантаження, спричиненого спалахом натовпу.

Для правильного розпізнавання викликів необхідний багатоетапний підхід часто необхідно [14]. Він включає виявлення симптомів виклику (тобто, які можуть призвести до розпізнавання початку виклику), визначення першопричини виклику та визначення потенційного впливу на систему. Однак, щоб бути економічно ефективним, будь-яким діям з відновлення має передувати оцінка впливу виклику

порівняно з вартістю відновлення [15]. Механізми виявлення викликів, які зазвичай викликаються розподіленим способом, повинні бути якомога меншими, щоб не використовувати ресурси без потреби (що є ключовою вимогою для мереж з обмеженими ресурсами) і не порушувати нормальну роботу мережі [16].

Якщо мережа не забезпечена вбудованими механізмами захисту від викликів (якщо відповідні механізми не застосовуються, наприклад, через високу вартість), а також перед лицем нових/невідомих викликів, будь-який такий виклик може згодом ініціювати помилку, тобто недолік є або випадковим недоліком конструкції (наприклад, помилка програмного забезпечення), або навмисним недоліком, який не було усунено, наприклад, через обмеження вартості системи.

Помилка має бути виявлена в режимі реального часу або на фізичному рівні (наприклад, через втрату сигналу, втрату модуляції або втрату тактового сигналу) за допомогою розпізнавання погіршення сигналу (наприклад, збільшення частоти бітових помилок – BER), або погіршення якості обслуговування (вказується зниженням пропускної здатності або збільшенням затримки передачі). Після виявлення несправності важливо локалізувати точку несправності, щоб поширювати сповіщення про несправності, необхідні для усунення негативного впливу несправності на продуктивність мережі [17, 18]. Повне повернення мережі зв'язку до нормального робочого стану може бути досягнуто пізніше, лише якщо усунути основні причини несправності.

Для будь-якого виклику, окрім оцінки його впливу на продуктивність комунікаційної мережі, важливо визначити ймовірність виникнення виклику (challenge_prob), а також ймовірність fail_prob того, що конкретний виклик призведе до збою (оскільки не всі виклики обов’язково призводять до до несправностей). Ці два показники в поєднанні з інформацією про вплив виклику можуть бути використані для визначення міри впливу мережевих ресурсів на збої від [19].

Проблеми, що призводять до збоїв мережевих каналів/вузлів, часто означають серйозні збої в маршрутизації запитів. Виникаюча проблема недоступності шляхів зв'язку додатково загострюється внаслідок безперервного

експоненціального збільшення обсягу переданої інформації. Оскільки збої в шляхах зв'язку неминучі просто через нездатність запобігти значному підмножині викликів, необхідні відповідні модифікації схем маршрутизації, щоб зробити наскрізний зв'язок можливим в умовах виникнення викликів.

1.3 Аспекти стійкості

У літературі запропоновано ряд дисциплін стійкості (див., наприклад, [20, 21] або [22]). Однак найбільш вичерпним є в [23]. Згідно [24, 25], стійкість мережі можна визначити як здатність мережі для забезпечення та підтримки прийнятного рівня обслуговування всупереч різноманітним збоям і проблемам нормальної роботи. Оскільки несправності та проблеми неминучі, стійкість мережі слід розглядати як одну з найважливіших характеристик проектування комунікаційних мереж.

Відповідно до [26], дисципліни стійкості можна класифікувати на дві основні категорії, а саме: толерантність до викликів, зосереджена на підходах до проектування мережі для забезпечення безперервності обслуговування за наявності проблем та достовірності, що описує вимірювані характеристики аналізованих систем зв'язку. Співвідношення між цими двома, яке називається надійністю, є показником продуктивності мережі за збурених умов.

Першу з двох розглянутих дисциплін стійкості можна далі розкласти на: живучість (включаючи відмовостійкість) – стосується інфраструктури комунікаційних мереж, стійкість до збоїв для шляхів зв'язку, стійкість до збоїв і стійкість трафіку до різних проблем, пов'язаних із трафіком (наприклад, додатковий обсяг, який вводиться в мережу).

Живучість зазвичай визначається як здатність системи виконувати свою місію вчасно, за наявності загроз, включаючи атаки або стихійні лиха [27]. Інше визначення з [28] пов'язує живучість зі здатністю мережі відновлювати пошкоджений трафік у середовищі збоїв і безперервно надавати різні послуги. в [29], живучість, у свою чергу, визначається як здатність мережі продовжувати

роботу за наявності збоїв, тоді як у [30] це називається здатністю автоматично реагувати як на фізичні, так і на програмні збої, перенаправляючи трафік із уражених маршрутів на ті, які працюють належним чином.

Таким чином, сфера живучості є ширшою, ніж відмовостійкість, і охоплює проблеми корельованих відмов для необмежених мереж [31], включаючи, наприклад, збої через зловмисну діяльність людини (атаки) [32] або збої великих частин інфраструктури комунікаційної мережі [33]. У порівнянні з відмовостійкістю, окрім резервування, необхідного для забезпечення відновлення служби, живучість додатково вимагає різноманітності [34, 35] запевняючи, що той самий дефект не впливає на кілька елементів системи зв’язку за кількох корельованих відмов.

Кількісна оцінка живучості мережі складніша, ніж відмовостійкість. Одним із можливих способів врахування одночасних відмов є використання багатовимірних ланцюгів Маркова [36], а в [37], функція живучості мережі (тобто функція ймовірності відсотка загального потоку, доставленого після відмови) і атрибути живучості були запропоновані для оцінки живучості будь-якої телекомунікаційної мережі.

Відмовостійкість – це здатність системи зв'язку справлятися з несправностями, що є результатом подій, відмінних від збоїв обслуговування [38]. Він використовує резервування для забезпечення компенсації випадкових і некорельованих відмов компонентів системи. Однак відмовостійкість недостатня для забезпечення відновлення після кількох корельованих відмов, і тому вона розглядається як підмножина живучості.

Толерантність до зриву визначається в [39] як здатність системи терпіти перебої в з’єднанні між її компонентами. Цей зв’язок оцінюється з точки зору характеристик шляхів зв’язку, і на нього можуть впливати проблеми навколишнього середовища, включаючи, наприклад, слабке та епізодичне з’єднання каналів, мобільність вузлів, непередбачувано велику затримку та проблеми з енергією/потужністю [40].

Перебої в наскрізному з’єднанні можуть виникати через:

- динамічна поведінка мережі (як, наприклад, у VANETs [41]),
- великі затримки, які не допускаються традиційними мережевими протоколами (наприклад, у супутниковому зв'язку [42]),
- енергетичні обмеження, що обмежують час роботи мережевих вузлів (наприклад, у бездротових сенсорних мережах – WSN [43]).

Толерантність до рухує останньою фундаментальною дисципліною толерантності до викликів, і, слідуючи [44] відноситься до здатності системи витримувати непередбачуване навантаження трафіку. Трафік можна розглядати як виклик, якщо його обсяг несподівано зростає далеко за межі припущень проектування мережі для нормального робочого стану. Приклади сценаріїв включають законні дії, такі як flash crowd [45] після стихійних лих, таких як землетруси, що передбачає необхідність отримати відповідну інформацію [46] або, наприклад, зловмисних дій, таких як DDoS-атаки [47].

Надійність визначається в термінах вимірних характеристик надання послуг як гарантія того, що система зв'язку працюватиме, як очікується [48]. Він складається з трьох дисциплін, а саме: надійність, безпека та продуктивність.

Надійність дисципліна використовується для кількісного визначення рівня довіри до послуг і в основному складається з надійності та доступності [49].

Надійність є надзвичайно важливою для додатків, орієнтованих на сеанс/з'єднання, які потребують відносно великого значення MTTF. Доступність, у свою чергу, є відповідним заходом для транзакційних служб (наприклад, протоколу передачі гіпертексту – HTTP), які виконують окремі операції за короткий час. Для таких послуг, якщо MTTR є відносно коротким, менш важливо, чи система часто виходить з ладу чи ні. Доступність також зазвичай використовується для оцінки стійкості комунікаційних мереж з практичних причин [50]. Інші характеристики надійності включають:

Ремонтопридатність, тобто схильність системи до оновлень/еволюції.

Безпека– міра надійності системи за катастрофічних збоїв, зокрема стосовно наслідків, а не причини збою, як, наприклад, у контексті кібератак [51]. Будь-яка

система прийнято вважати безпечною, якщо вона нешкідлива для нормального функціонування навколишнього середовища.

Цілісність відсутність неналежних (несанкціонованих) змін системи [52].

Іншим важливим аспектом є безпека, тобто здатність системи захищати себе від різних неавторизованих дій (наприклад, доступу або оновлень на основі відповідних політик безпеки). Безпека має спільні властивості доступності та цілісності з надійністю, а також індивідуальні характеристики, включаючи автентичність, можливість авторизації, можливість аудиту, а також конфіденційність і неспростовність [51].

Працездатністьце дисципліна, яка використовується для вимірювання продуктивності системи порівняно з відповідними вимогами до якості обслуговування, що випливають із специфікацій послуг щодо затримки, тремтіння, пропускної здатності/хорошої пропускної здатності та співвідношення доставки пакетів [52].

З точки зору клієнта, найважливішими характеристиками стійкості є ті, які пов’язані зі сприйманою якістю обслуговування, які називаються характеристиками якості стійкості (QoR), тобто характеристиками QoS, пов’язаними зі стійкістю, яку спостерігають кінцеві користувачі [53].

Навпаки, мережеві оператори в основному зацікавлені в характеристиках, що стосуються операційних аспектів і аспектів впровадження (відомих як функції, пов’язані з експлуатацією), які впливають на вартість рішень. Оскільки цілі цих двох груп явно відрізняються одна від одної, необхідна детальна оцінка, щоб перевірити, чи відповідає пропонована якість вимогам клієнта та чи є вона, водночас, вигідною для оператора мережі.

Варто відзначити значну різницю між характеристиками QoS і QoR щодо часу, необхідного для отримання результатів. На відміну від функцій QoS, які за своєю природою є короткостроковими, більшість заходів стійкості є довгостроковими [54]. Тому стійкість можна оцінити в довгостроковій перспективі лише на основі характеристик наскрізної передачі. Крім того, на відміну від показників QoS, характеристики QoR часто не можуть бути отримані точно,

оскільки в багатьох випадках вони не сприймаються кінцевими користувачами безпосередньо. Наприклад, збільшення затримки передачі/втрати пакетів може бути результатом або перевантаження, або збою елемента мережі.

1.4 Існуючі підходи до забезпечення стійкої маршрутизації

Після виникнення збою процес відновлення ініціюється з виявленням збою. Його можна розпізнати, наприклад, за допомогою механізмів IP-MPLS, таких як MPLS LSP ping або MPLS LSP traceroute [55] (надіслані за маршрутами з комутацією міток – LSP), які, однак,трудомісткий. Іншим варіантом є визначення несправності на основі подій «Втрата світла» або «Втрата годинника».

Виявлення несправності має супроводжуватися локалізацією та ізоляцією несправності (тобто визначенням несправного вузла/зв'язку), що необхідно для припинення подальшої передачі інформації через уражений елемент, який слід відремонтувати [56].

Повідомлення про помилкуповідомлення надсилаються на вузли мережі, відповідальні за подальші дії з відновлення. На цьому етапі зазвичай ініціюються два процеси: процес відновлення та процес відновлення. Перший пов'язаний з ремонтом несправного елемента, тоді як процес відновлення полягає в ідентифікації ураженого трафіку, локалізації збою та визначенні альтернативного шляху, по якому трафік буде перенаправлений далі.

Передбачається, що обидва процеси завершуються нормалізацією, тобто розпізнаванням відремонтованого елемента та поверненням до нормального робочого стану. Що стосується маршрутизації, це, як правило, означатиме повернення до шляхів передачі, які використовувалися до збою (оскільки шляхи відновлення зазвичай є неоптимальними, наприклад, щодо використання ресурсу).

Ідеальний час відновлення (тобто час, необхідний для перемикання трафіку на резервні шляхи) не повинен перевищувати 50 мс, оскільки збій тривалістю до 50 мс розглядається вищими рівнями лише як помилка передачі. Будь-який збій

тривалістю понад 50 мс призводить щонайменше до втрати пакетів або недоступності послуги [57].

Хоча використання шляхів захисту для забезпечення автоматичного перемикання здається досить інтуїтивно зрозумілим, питання про те, як реалізувати ефективні схеми відновлення, будучи не тільки ефективними щодо пропускної спроможності, але також масштабованими та включаючи численні критерії QoS, особливо в середовищах гетерогенної сітчастої мережі, є складним завданням .

Загалом характеристики будь-якого методу відновлення сильно впливають на значення часу відновлення служби [58].

Фундаментальна класифікація механізмів стійкості, заснована на структурі комунікаційних мереж, поділяє існуючі підходи на кільцеві та сітчасті. Перший відноситься до архітектур, запроваджених близько трьох десятиліть тому, включаючи, наприклад, синхронні оптичні мережі/синхронну цифрову ієрархію (SONET/SDH) [59] і ранні архітектури кільцевих мереж DWDM [60]. Залежно від напрямку потоку кільцеві мережі можна класифікувати як односпрямовані або двонаправлені відповідно.

Таким чином, резервні кільця можна розглядати як заздалегідь сплановану схему захисту, що забезпечує дуже короткий час перемикання відновлення. Однак недоліком є високий коефіцієнт резервування мережі (є відношенням захисної здатності до працездатності) рівно 100 % [61].

1.4.1 Еластична маршрутизація в сітчастих мережах

У сучасних мережах часто характеризується сітчастою топологією [62] шляхи передачі є наскрізними, тобто не утворюють кільцевих структур. На відміну від мереж минулого, розроблених для надання лише одного типу послуг (голосу або даних), поточні комунікаційні мережі також повинні надавати різноманітні послуги (наприклад, послуги в режимі реального часу, а також масову передачу даних).) для підтримки широкого діапазону додатків, що мають диференційовані вимоги щодо стійкості, а також якості передачі.

Ця диференціація також може випливати з різного використання однієї програми [63]. Іншими словами, один і той же додаток може мати різні вимоги залежно від того, як користувачі його використовують. Наприклад, навіть у випадку класичної телефонної послуги вимоги до доступності послуги для компанії будуть набагато вищі, ніж ті, які висуває домашній користувач.

Проектування мережі зв'язку, яка завжди відповідає найвищим вимогам до всього спектру послуг (тобто готова надавати найвищий рівень обслуговування), було б надзвичайно дорогим і нерозумним. Таке надмірне забезпечення є особливо дорогим у бездротових мережах і мережах доступу, де пропускна здатність обмежена (порівняно, наприклад, з оптичними мережами дальньої мережі DWDM) [64].

Тому правильна диференціація стійкості в [65] має вирішальне значення у відносинах клієнт-оператор як важливий елемент угод про рівень обслуговування. Оператор, зацікавлений у максимізації прибутку, шукає економічно ефективні механізми стійкості, адаптовані до конкретних вимог QoR. Також диференційована готовність клієнтів платити за послугу. Зокрема, клієнти очікують найнижчу можливу ціну за послугу, здатну підтримувати характеристики додатків, але лише з мінімальним урахуванням мережевих механізмів, які оператор розгорне для підтримки цих додатків. Таким чином, використання кількох механізмів стійкості в мережі може дозволити як клієнтам, так і операторам збільшити свій прибуток.

1.4.2 Схеми резервування ресурсів резервного шляху в мережевих мережах

Розглянемо найважливіші механізми стійкості, запропонованих у літературі для забезпечення відмовостійкої маршрутизації. Диференціація стійкості може бути отримана шляхом поєднання кількох з них в одній мережі.

Що стосується методологій налаштування шляху резервного копіювання, шляхи відновлення можуть бути:

- встановлено заздалегідь запланованим способом (тобто заздалегідь під час пошуку основних шляхів) – часто згадується як заздалегідь запланований

захист у літературі [66],

– визначається динамічно (реактивно) після виникнення збою (відомого як динамічна реставрація).

Перший випадок, історично похідний від автоматичного захисного перемикання (APS) [67], забезпечує швидке відновлення кожного невдалого шляху передачі (оскільки резервні шляхи встановлюються заздалегідь).

Динамічне відновлення, що бере свій початок у мережах IP [68], у свою чергу, є кращим з точки зору ефективності використання мережевих ресурсів (резервні шляхи встановлюються тут лише за необхідності, тобто після збою, і можуть повторно використовувати пропускну здатність зв'язку несправних шляхів передачі). Однак він успадковує всі недоліки, характерні для динамічної IP-маршрутизації, зокрема тривале перемикання відновлення, нестабільність шляху та ризик утворення петель. Це також не гарантує відновлення через непередбачувану кількість резервних ресурсів, доступних після збою.

Загалом, щоб забезпечити 100% відновлюваність для робочих потоків даних, будь-який шлях резервного копіювання повинен не тільки характеризуватися такою ж пропускною здатністю, як і відповідний робочий шлях, але він також повинен бути зв'язаним/вузловим роз'єднаним (тобто не мати спільних зв'язки/транзитні вузли) з робочим шляхом.

Вимога полягає в тому, щоб гарантувати, що будь-який збій посилання/вузла, який впливає на робочий шлях, також не порушить відповідний резервний шлях.

Таким чином, ця роз'єднаність має гарантувати, що два розглянуті шляхи (тобто робочий і резервний шлях) запиту не використовують ресурси мережевих елементів, що належать до однієї групи зв'язків спільного ризику (SRLG), визначеної в [69] як набір мережевих елементів, які є або посиланнями, вузлами, фізичними пристроями, або їх сумішшю, що підпадає під загальний ризик відмови. Згідно [70], будь-який робочий шлях вважається SRLG-роз'єднаним з відповідним резервним шляхом, якщо обидва шляхи не залучені до жодного спільного SRLG.

1.5 Відновлення

Розглядаючи обсяг відновлення, окрім глобального захисту, локальний захист може бути застосований із резервними шляхами, які використовуються для перенаправлення ураженого трафіку через несправний канал/вузол [71]. Проміжне рішення під назвою захист сегмента забезпечує наявність резервних шляхів, кожен з яких захищає даний сегмент робочого шляху, що складається з кількох послідовних елементів мережі).

1.6 Використання ресурсів відновлення

При аналізі схем використання резервних ресурсів слід виділити два рішення, а саме виділений і спільний захист. У виділеній схемі захисту ресурси (ємності зв'язку) будь-якого резервного шляху резервуються для захисту лише одного робочого шляху. Ця техніка є дуже дорогою, але дозволяє швидко відновити пошкоджений трафік. Крім того, якщо застосовано заздалегідь запланований захист, резервні шляхи можуть використовуватися паралельно з робочими шляхами в нормальному робочому стані (тобто схема 1 1 передачі сигналу одночасно по обох шляхах), або активуватися лише на короткі періоди часу, щоб перенаправляти трафік, на який впливає збій (відома як схема захисту 1:1). В останньому випадку резервна ємність може бути використана найкращим трафіком за нормальної роботи [72].

Проблема забезпечення стійкої маршрутизації для набору запитів за допомогою резервних шляхів, які SRLG-не перетинаються з відповідними робочими шляхами в мережах з обмеженою пропускною спроможністю, була показана як NP-повна в [73], що означає необхідність застосування комбінаторних підходів. Наприклад, оптимальне розв'язання задачі прикладу пошуку пар робочого та резервного шляхів для забезпечення захисту від відмови одного вузла для набору вимог, для яких загальна вартість робочого та захисного шляхів, мінімізується, можна визначити, розв'язавши відповідну задачу ILP. Як

представлено в [74] формулювання цієї проблеми має включати обмеження збереження потоку, обмеження на формулу загальної пропускної здатності каналу, обмеження для забезпечення вузлової роз'єднаності для кожної пари робочих і резервних шляхів, а також обмеження на дозволені значення.

Недоліком спеціальної схеми захисту є те, що, навіть якщо вона забезпечує найшвидше відновлення, вона передбачає високі додаткові витрати понад 100 % через коефіцієнт резервування мережі, що перевищує 100 % (оскільки шляхи резервного копіювання зазвичай проходять через більше посилань, ніж відповідні робочі шляхи). Тому, щоб обмежити вартість рішення, була запропонована концепція спільного захисту, у якій пропускна здатність каналу може спільно використовуватися декількома шляхами резервного копіювання. Відповідно до [75], підхід спільного захисту здатний обмежити коефіцієнт резервування до рівня 35–70 %.

Якщо потрібно, щоб потоки були відновлюваними на 100%, спільне використання пропускної здатності з’єднання декількома резервними шляхами можливо, лише якщо відповідні частини робочих шляхів (тобто захищені цими резервними шляхами) є взаємно роз’єднаними, тобто вони не спільно використовують однаковий ризик відмови (тобто, якщо вони не належать до спільного SRLG) [76].

У стійких схемах маршрутизації пропускна здатність будь-якого каналу класифікується на: (1) робочу ємність (тобто використовується існуючими робочими шляхами), (2) резервну ємність (позначає ємність, уже зарезервовану для резервних шляхів) і (3) вільну ємність не використовується жодним шляхом (тобто, яка може бути виділена або для робочих, або для резервних шляхів) [77].

Згідно із спільним використанням резервної ємності, резервна ємність будь-якого зв’язку далі поділяється на два класи: спільні та несумісні. Перший включає резервну ємність, зарезервовану для інших шляхів резервного копіювання, які можуть бути спільними для резервного шляху, який буде встановлено (тобто, коли відповідна частина робочого шляху вхідного запиту SRLG не перетинається з частинами всіх інших робочих шляхів, які захищені шляхом резервного

копіювання з використанням цієї спільної ємності). Останній випадок стосується ємності, яка вже зарезервована для шляхів резервного копіювання, якими не можна поділитися.

1.6.1 Область операцій відновлення

Наскрізну маршрутизацію між віддаленими місцями часто потрібно надавати через кілька мережевих доменів, кожен з яких визначається на основі адміністративного/географічного масштабу або власності постачальника мережі та зазвичай ідентифікується з автономною системою. У контексті наскрізної маршрутизації багатодоменна маршрутизація стикається з проблемами, пов'язаними з доступністю точної інформації про маршрутизацію (тобто, що випливає з топологічних характеристик доменів), яка, через аспекти конфіденційності, зазвичай не передається [78].

Інша проблема стосується відсутності обміну інформацією щодо фізичного розгортання посилань у різних доменах, пов'язаних із роз'єднаністю SRLG. Наприклад, навіть якщо може здатися, що наскрізна маршрутизація за допомогою двох окремих шляхів у кількох доменах відповідає вимогам вузлової роз'єднаності, на практиці канали з різних доменів можуть бути розгорнуті в тому самому каналі, наприклад, фізичномаршрутизовані через один міст, що підвищує ризик одночасного виходу з ладу обох. Таким чином, застосування методів міждоменного відновлення (тобто спільних дій, що здійснюються в кількох доменах для відновлення після збою) часто нереалістично.

1.6.2 Рівень операцій відновлення

Інтернет-трафік IP здебільшого передається через оптичні мережі (наприклад, в магістралі). Це означає, що там застосовано певне розшаровування комунікаційних мереж.

Дійсно, IP-зв’язки часто є віртуальними, тобто вони забезпечуються, наприклад, оптичними маршрутами з кількома стрибками. Таким чином, кінцева віртуальна топологія IP зазвичай формується над основною оптичною транспортною мережею.

Цей простий сценарій згадує лише два рівні: тобто верхній IP-рівень (часто розширений функцією багатопротокольної комутації міток (MPLS) для надання QoS, часто називають IP-MPLS) і нижній мультиплексування з розділенням хвиль (WDM) [79]. У цьому випадку маршрутизатори IP-MPLS підключаються до портів оптичних перехресних з’єднань нижнього рівня (OXC). Самі OXC, у свою чергу, пов’язані між собою у фізичній сітчастій топології за допомогою багатохвильових оптичних каналів.

Загалом цю концепцію можна розширити до випадку мереж, що складаються з більш ніж двох рівнів із взаємозв’язком клієнт-сервер між кожною сусідньою парою рівнів (включаючи, наприклад, SONET/SDH між рівнями IP-MPLS і WDM). Автоматизоване керування багаторівневими мережами було стандартизовано в рамках Generalized Multiprotocol Label Switching (GMPLS), включаючи всі необхідні сутності для використання протоколами маршрутизації та сигналізації, зокрема, інтерфейс користувача-мережі (UNI) та інтерфейс мережа-мережа (NNI).

Розглядаючи питання взаємодії між рівнями, дотримуючись [80] можна виділити три основні схеми, а саме:

- модель накладення припускає, що маршрутизація виконується на кожному рівні окремо (тобто інформація про маршрутізацію не розподіляється між мережевими рівнями),
- однорангову (також звану інтегрованою) модель, що дозволяє обмінюватися інформацією про маршрутізацію між рівнями мережі,
- доповнена (або гібридна) модель є розширенням моделі накладання, що робить інформацію про доступність вузлів доступною в UNI.

У такій багаторівневій схемі відновлювальні дії після збоїв стають ще більш складними. Загалом, завдяки спостережуваному переміщенню низькошвидкісного трафіку з верхніх рівнів на високошвидкісні шляхи нижніх рівнів за допомогою

мультиплексування з тимчасовим поділом (TDM) [81], деталізація перемикання трафіку стає грубішою від вищої до нижчоїшари. Отже, більше дій відновлення необхідно виконувати на вищих рівнях (тобто відновлення багатьох низькошвидкісних потоків), ніж на нижчих рівнях (де відновлення відбувається швидко завдяки виконанню дій відновлення по відношенню до сукупних потоків). Крім того, час відновлення у верхніх шарах може бути додатково збільшено в результаті значної кількості відновлювальних дій, які необхідно виконати.

Що стосується порядку шарів, у яких виконуються дії відновлення, на основі [81] можна виділити такі стратегії ескалації:

- знизу вгору де дії по відновленню ініціюються в самому нижньому шарі і потім поширюються до верхніх шарів. Очевидною перевагою цього методу є виконання дій відновлення з відповідною деталізацією. Зокрема, це означає, що за обробкою найгрубіших дій гранулярності на найнижчому рівні слідують дії відновлення на верхніх рівнях лише щодо потоків, які не вдалося відновити на нижньому рівні (наприклад, збій кінцевого вузла нижнього рівня). - шлях шару),
- з верху до низу, де відновлення починається в самому верхньому шарі. Хоча такий підхід дозволяє краще диференціювати дії по відновленню, що стосуються кількох класів трафіку, вимагає більш складної сигналізації (оскільки нижні рівні не мають прямих засобів виявлення, якщо верхній рівень не вдалося відновити порушений трафік).

Якщо дії відновлення доступні на кількох рівнях, тоді також важливо забезпечити відповідну міжрівневу координацію, включаючи визначення послідовності рівнів, відповідно до яких виконуються дії відновлення.

Така координація між мережевими рівнями необхідна для запобігання багаторазової реакції різних рівнів на один і той же збій. Це можна отримати, наприклад, за допомогою механізму таймера утримання використовується для відкладення дій відновлення на вищому рівні, щоб дати нижчому рівню час для відновлення ураженого трафіку. Після цього дії відновлення запускаються на вищому рівні для всього ураженого трафіку, який не вдалося відновити на нижчому рівні.

Інша пропозиція полягає у використанні маркерів відновлення, які допомагають скоротити час ініціалізації дій відновлення на вищому рівні. У цьому випадку, як тільки нижній рівень завершує процес відновлення, він надсилає сигнал вищому рівню, щоб розпочати там дії з відновлення.

Через взаємовідносини клієнт-сервер несправність вузла вищого рівня (наприклад, маршрутизатора IP-MPLS) не може бути відновлена на нижчому рівні. Однак зворотне, тобто відновлення збою, що стався на нижньому рівні (лінії/вузлі нижнього рівня), можливе на вищому рівні.

Щоб виконати дії з відновлення, кожен рівень повинен оцінити резервну потужність, необхідну для перенаправлення потоків після збоїв. Зокрема, рівень IP-MPLS зазвичай відповідає за обробку збоїв маршрутизатора. Ресурси резервного копіювання можуть спільно використовуватися між мережевими рівнями, утворюючи загальний пул ресурсів таким чином, щоб відповідні шляхи захисту з різних рівнів не мали ризику бути активованими одночасно.

1.7 Висновки та постановка задачі

Таким чином постає завдання забезпечення стійкості комп’ютерних мереж. Для цього необхідним є:

1. дослідити методи забезпечення стійкості корпоративної комп’ютерної мережі;
2. проаналізувати сучасні програмно-технічних засоби забезпечення стійкості корпоративної комп’ютерної мережі;
3. розробити модель забезпечення стійкості корпоративної комп’ютерної мережі;
4. дослідити та описати моделювання комп’ютерних мереж, описати методи моделювання, аналізу мереж в моменти здійснення негативних зовнішніх впливів на мережу, що впливає на її стійкість;
5. розробити метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі;

6. реалізувати метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі.

2 МОДЕЛЮВАННЯ ДИНАМІК ЗБОЇВ ТА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Здійснення моделювання комп'ютерних мереж

Оскільки основна тема дослідження орієнтована на забезпечення стійкості мереж, тому основне питання дослідження: як зробити мережі більш стійкими до поширюваних збоїв. Основною метою дослідження є розробка моделей та інструментів для підвищення стійкості магістральних мереж до збоїв, що поширюються. Розглянемо основні динаміки поширення збоїв: каскади та епідемії. Обидві ці динаміки мають дві спільні характеристики: вони зазвичай виникають у невеликій частині вузлів; вони поширюються мережею і можуть спричинити глобальні перебої в роботі. Однак механізм і наслідки збоїв відрізняються. Причиною каскаду є дефіцит пропускної здатності, а епідемії зумовлені властивістю вірусу поширюватися. Крім того, кожен із збоїв спричинений різним тригером. Каскадний збій викликається виходом з ладу вузлів або зв'язків, які спричинені або випадковим збоєм, або географічно пов'язаними збоями, або навмисною атакою. Хоча цей тип збою пов'язаний з частиною, або розділом графа, він може легко поширитися на всю мережу. Причина такого поширення відома як каскадний ефект. Каскадні збої є результатом збільшення навантаження на канали і вузли після початкового збою. Вузли або лінії зв'язку не можуть витримати надмірне навантаження і тому вони відмовляють в обслуговуванні трафіку, або навіть руйнуються. Після початкового збою в мережах зв'язку середнє навантаження на трафік збільшується. Збільшення інформаційного потоку призводить до ефекту, відомого як переповнення буфера, що викликає затримки і відмову в обслуговуванні.

Епідемія спричинена шкідливою вірусною інфекцією, яка викликана навмисною, детермінованою атакою на ретельно вибрані вузли мережі за допомогою шкідливого програмного забезпечення, яке поширюється на фізично і логічно підключених сусідів. Це також призводить до каскадних збоїв, які відбуваються набагато швидше, ніж каскади збоїв вузлів або каналів зв'язку та

переповнення буферів. Прості збої - не єдиний небезпечний ефект у випадку вірусної атаки.

Функція шкідливого програмного забезпечення може мати й інший шкідливий характер, наприклад, компрометація даних або підслуховування конфіденційного спілкування.

Тому слід вживати адекватних заходів, щоб уповільнити процес зараження і уникнути потенційних негативних наслідків для мережі та послуг, що надаються.

Згідно з [79, 80], можна виділити певні фази щодо порушення роботи системи. Можна виокремити три основні фази, коли йдеться про небажану подію, а саме: підготовка, реагування та фаза відновлення.

Вибір стратегії для підвищення стійкості мережі залежить від того, на якій фазі буде використовуватися дана стратегія. Виходячи з цього, сформульовані деякі підпитання дослідження.

У таблиці 2.1. представлено набір можливих дослідницьких питань і завдань, що стосуються кожної фази і типу збою.

Таким чином розв’язок задачі полягає в розв’язку підзадач:

1. Які вузли або зв'язки слід додатково захистити, щоб зробити мережу більш стійкою до каскадів?
2. Як налаштувати топологію та покращити властивості вузлів, щоб пом'якшити наслідки потенційної відмови?
3. Розробити стратегії активного контролю топології, щоб запобігти подальшому переповненню буферів та локальним перевантаженням.
4. Які вузли слід додатково захистити, щоб зробити мережу більш стійкою до епідемій?
5. Як налаштувати топологію та покращити властивості вузлів, щоб уповільнити поширення потенційної вірусної інфекції?

Таблиці 2.1 - Динаміки поширення збоїв та загроз, що зменшують стійкість мережі

Етап	Каскади	Епідемії
Підготовка	Які вузли або зв'язки слід додатково захистити, щоб зробити мережу більш стійкою до каскадів?	Які вузли слід додатково захистити, щоб зробити мережу більш стійкою до епідемії?
	Як налаштувати топологію та покращити властивості вузлів, щоб пом'якшити наслідки потенційного збою?	Як налаштувати топологію та покращити властивості вузлів, щоб уповільнити поширення потенційної вірусної інфекції?
Реакція	Розробити стратегії активного контролю топології, щоб запобігти подальшому переповненню буферів та локальним заторам.	Як можна змінити топологію мережі після зараження, щоб уповільнити поширення інфекції?
Відновлення	Визначте пріоритетність відновлення вузлів або зв'язків, щоб відновити функціональність мережі.	Визначте пріоритетність відновлення вузлів або зв'язків, щоб відновити функціональність мережі.

2.2 Застосування методів, які використовуються для вирішення поставлених піздазач

Відмова одного набору вузлів може мати більший вплив на мережу, ніж відмова іншого набору. Зазвичай, видалення або вихід з ладу вузлів або ребер внаслідок випадкової поломки або навмисної атаки в напруженій розподіленій системі спричиняє подальший перерозподіл напруги в системі [75]. Мета полягає в тому, щоб визначити найбільш важливі вузли з точки зору впливу таких збоїв на мережу. Показниками, які використовуються для оцінки функціонування мережі, є відносний розмір найбільшого підключеного компонента у випадку моделі Моттера-Лая (ML) та ефективність мережі у випадку моделі Круччітті-Латора-

Марчіорі (CLM). Окрім інших, основною мірою центральності, що використовується в обох моделях, є міжміська центральність. Моделюються збої в мережі, а вплив на мережу вимірюється після і до збоїв. Моделювання збоїв також модифікується в залежності від причини збою, чи це випадковий збій, географічно корельований збій або навмисна атака. Для перевірки деяких результатів у випадку дуже великого простору рішень використовується відповідний генетичний алгоритм. Таким чином, оцінюється стійкість мережі та визначаються найбільш важливі вузли або групи вузлів.

Оцінка стійкості мережі дає нам уявлення про розподіл важливих елементів мережі. Деякі зміни в топології мережі можуть бути зроблені для зменшення критичності певних вузлів і підвищення загальної стійкості мережі. Переміщення або додавання каналів зв'язку не вважається доцільною стратегією в інфраструктурній мережі, такій як магістраль зв'язку. Тому основна увага приділяється покращенню властивостей вузла, зокрема, його пропускної здатності. Чисельне моделювання використовується для оцінки стратегій оптимального збільшення пропускної здатності.

Розробити стратегії активного контролю топології, щоб запобігти подальшому переповненню буферів та локальним перевантаженням.

Стратегії активного контролю топології передбачають модифікацію зв'язків і розташування вузлів у реальному часі, яка ініціюється початковою подією. Метою процесу зміни є пом'якшення наслідків збою, який вже стався. Це має бути зроблено швидко та ефективно. Створення нових зв'язків і вузлів у вже створеній інфраструктурній мережі не є доцільною стратегією через відносно короткий час, необхідний для поширення каскадної відмови. Однак, навмисне видалення вузлів і зв'язків є розумною стратегією для мінімізації каскаду. Чисельне моделювання використовується для визначення вузлів-кандидатів на видалення у випадку критичної відмови.

Вузли, які повинні бути додатково захищені, - це найбільш критичні вузли або ланки мережі, відповідальні за поширення інфекції. Більшість підходів, що

використовуються в літературі, базуються на різних мірах центральності та їх варіаціях. Тут пропонується альтернативний метод оцінки потужності поширення вузла. Міра Node Imposed Response (NiR) використовує концепції з теорії систем LTI.

Більш конкретно, міра NiR базується на значенні відгуку системи на вхідну функцію кроку. Для підтвердження точності NiR проведено широке чисельне моделювання.

Основною характеристикою процесу поширення, яка визначає швидкість зараження, є ймовірність передачі. Це ймовірність того, що сприйнятливий вузол буде інфікований одним інфікованим сусідом за один крок. Зміна ймовірності передачі для певних пар вузлів змінює динаміку епідемії. Однак обмеження у вигляді витрат зазвичай присутні, а найкраще рішення передбачає оптимальний розподіл ресурсів, тому епідемія поводиться так, як очікується. Тут системний підхід LTI використовується для визначення критичних ланок. Результати підтверджуються за допомогою чисельного моделювання.

2.2 Методи дослідження стійкості комп’ютерної мережі

2.2.1 Методи моделювання

Для вирішення поставлених задач було застосовано методи, що використовуються одночасно, чисельний та аналітичний - застосовуються для перехресної перевірки та порівняння результатів, отриманих кожним з них. Вони застосовуються для перехресної перевірки та порівняння результатів, отриманих кожним з них, а також для уточнення моделей відповідно до спостережень і висновків.

Аналітичні методи. Аналітичний підхід допомагає отримати рішення про стан системи, уникаючи симуляцій і не застосовуючи великих обчислювальних потужностей. Для аналізу мереж будуть використані методи теорії систем. Мережі розглядаються як LTI-системи та оцінюються реакції відповідної системи на певні

вхідні впливи. Отримані результати використовуються для оцінки потужності поширення вузлів і, отже, для визначення найбільш критичних елементів.

Чисельні методи. Моделювання широко використовується для спостереження за динамікою всередині мереж. Моделювання мереж є широко розповсюдженим методом дослідження мереж. Моделювання може дати уявлення про динаміку процесу і надати багато інформації, яку неможливо було передбачити заздалегідь. Весь код моделювання був написаний в MATLAB, математичному програмному забезпеченні, яке охоплює багато аспектів математики і може бути використане для мережевого моделювання та обчислень.

2.2.2 Методи аналізу

Основним методом, що використовується для аналізу, є міра кореляції. Міра кореляції використовується для перевірки припущень у випадку оцінки вузлів. Для всіх аналізів використовуємо тау-коефіцієнт рангової кореляції Кендалла. Це непараметрична міра зв'язку між ранжованими даними і потужний інструмент для порівняння результатів, отриманих різними методами моделювання.

Коефіцієнт кореляції τ приймає максимальне значення 1, якщо спостереження мають однакові ранги, і мінімальне значення -1, якщо спостереження мають різні ранги.

Перше спостереження ранжирується за значеннями вектора $\bar{x}$, а друге спостереження - за значеннями вектора $\bar{y}$.

Потім ранги порівнюються за допомогою критерію Кендалла [81] :

$$\tau = \frac{2}{n(n-1)} \sum_{i<j} sgn[(x_i - x_j)(y_i - y_j)],\ sqn(y) = \begin{cases} 1,\ y > 0 \\ -1,\ y < 0 \\ 0,\ y = 0 \end{cases} \qquad (2.1)$$

У випадку впливу, що поширюється, значення x_i розраховується для кожного вузла i.

У випадку моделі SI, x_i - це час, необхідний для інфікування 50% комп'ютерної мережі.

Для моделі SIR x_i - це розмір спалаху. Значення y_i розраховується незалежно для кожної з мір центральності.

В результаті матимемо єдиний (первинний) вектор $\bar{x}$ і шість векторів для порівняння $\overline{y_{nir}}$, $\overline{y_{bet}}$, $\overline{y_{cor}}$, $\overline{y_{deg}}$, $\overline{y_h}$, $\overline{y_{ds}}$ для шести мір центральності: NiR, міжцентровість (betweenness), центральність (centrality), ступінь (degree), h-індекс (h-index) та динамічна чутлива центральність (DS), відповідно.

Потім для кожної з мір центральності обчислюється τ, щоб оцінити її точність в оцінці потужності поширення вузла.

Інший метод аналізу використовує численні міри центральності для визначення найважливіших вузлів.

Крім того, порівняння використовуються для широкомасштабного чисельного аналізу впливу видалення вузлів. Вплив різних стратегій атаки порівнюється між собою.

2.2.3 Застосування метаевристики для моделювання стійкості комп'ютерної мережі

Метаевристики - це загальні алгоритмічні рамки, які зазвичай надихаються процесами в природі. Вони використовуються для вирішення складних оптимізаційних задач [82].

Багато задач в області складних мереж стають все більш складними і динамічними і тому часто вирішуються за допомогою евристик. Окрім евристичного підходу, реалізованого в деяких алгоритмах для мір центральності, таких як міжцентровість, в представленому тут дослідженні інтенсивно використовується генетичний алгоритм.

Генетичний алгоритм (ГА) - це метаевристика, натхненна процесом природного відбору. Генетичні алгоритми зазвичай використовуються для вирішення задач оптимізації та пошуку, покладаючись на операції, натхненні

механізмами еволюції, такими як мутація, кросинговер і відбір. ГА - це метод переходу від однієї популяції "хромосом "1 до нової популяції шляхом використання деяких принципів "природного відбору" разом з операторами, натхненними генетикою. Оператор відбору вибирає хромосоми в популяції, яким буде дозволено розмножуватися, і в середньому більш пристосовані хромосоми дають більше нащадків, ніж менш пристосовані. Кросинговер обмінюється ділянками двох хромосом, приблизно імітуючи біологічну рекомбінацію між двома однохромосомними організмами, а мутація випадковим чином змінює гени деяких ділянок хромосоми [84]. Генетичний алгоритм можна застосовувати для розв'язання різноманітних оптимізаційних задач, включаючи задачі, в яких цільова функція є розривною, недиференційованою, стохастичною або сильно нелінійною. Генетичний алгоритм підходить для швидкого визначення відносно хорошого розв'язку з дуже великого простору розв'язків. Він також може вирішувати задачі змішаного цілочисельного програмування, де деякі компоненти обмежені цілочисельними значеннями. У той час як класичні алгоритми зазвичай генерують розв'язок у вигляді однієї точки на кожній ітерації, GA генерує популяцію точок на кожній ітерації. Найкраща точка в популяції наближається до оптимального розв'язку.

Деякі рішення, представлені в цій роботі, перевіряються генетичним алгоритмом, який реалізовано за допомогою Global Optimization Toolbox в MATLAB [85].

2.2.4 Отримання ациклічних графів при моделювання стійкості комп’ютерних мереж

Всі неорієнтовані мережі складаються з двонаправлених зв'язків, які утворюють цикли між кожною парою вузлів. Щоб отримати ациклічний граф, топологія повинна бути модифікована таким чином, щоб всі цикли були видалені, а кількість вершин залишилася незмінною.

В процесі модифікації топології кількість видалених ребер повинна бути мінімізована, щоб зберегти топологію максимально схожою на вихідну.

У запропонованому алгоритмі використовуються два принципи:

1) зберігається найбільш ймовірний шлях поширення інфекції, наприклад, дерево найкоротшого шляху з вершиною-джерелом в якості батька;

2) пріоритет віддається ребрам, розташованим ближче до вершини-джерела, оскільки важливість топології швидко зменшується з віддаленням від джерела.

Алгоритм отримання ациклічного графа з урахуванням важливості найближчого оточення вершини показано в Алгоритмі 2.1.

Алгоритм 2.1 - Отримання ациклічних графів при моделювання стійкості комп'ютерних мереж

1: Вхідні дані: G(V, E), p, i> i – джерело інфікування
2: отримання найкоротшого дерева G(V, ESPT)
3: отримання множини решти дуг edges I> Erem = E − ESPT
4: створення ієрархічної топології G(V, ESPT)
5: побудувати дуги від вузла-джерела
6: відсортувати дуги, що залишилися, за відстанню від вузла-джерела node I> Ert em
7: поки не усі дуги виконуємо
8: повертаємо виключені дуги Ert em(i)
9: перевіряємо на повтори
10: якщо кількість повтори ≥ 1 тоді
11: видалити повернуту дугу
12: кінець
13: повернути ациклічний граф G(V, Eacyc)

Представлений Алгоритм 2.1 генерації ациклічних графів не гарантує мінімальної кількості видалених зв'язків. Проте, він оптимізує характеристику, що має відношення до явища розповсюдження, а саме локальну топологію навколо вузла-джерела. Вона намагається зберегти якомога більше зв'язків у безпосередній близькості від джерела. Чим далі здійснюється відхід від вузла-джерела, тим більша ймовірність того, що посилання буде видалено. Однак видалення віддалених ребер має дуже обмежений вплив на динаміку поширення.

2.2.5 Методи проєктування стійких комп’ютерних мереж

Після моделювання та аналізу пропонуються синтезу апаратно-програмних засобів для покращення стійкості комп’ютерної мережі. Для того, щоб представити проектне рішення, яке має відповідати декільком критеріям, використовується багатокритеріальний аналіз.

Багатокритеріальний аналіз застосовується для досягнення оптимального рішення в умовах, коли необхідно враховувати багато цілей (багатовимірний простір проектування). Ці цілі зазвичай є конфліктними (рівень обслуговування, стійкість до збоїв, вартість...) і багатоцільове програмування використовується для досягнення межі Парето системи.

2.2.6 Аналітичний підхід у моделюванні складних мереж

Однією з основних цілей цієї дисертації є розробка відповідного аналітичного підходу для моделювання складних мереж. Як правило, розробка точного аналітичного розв'язку системи зі складною динамікою є складним завданням, оскільки воно ґрунтується на розв'язанні результуючої системи диференціальних рівнянь, яка, як правило, є надто великою. Кінцевою метою багатьох вчених є розробка головного рівняння системи. Головне рівняння описує часову еволюцію системи, яка може бути змодельована як така, що перебуває точно в одному зі станів у будь-який момент часу, і де перемикання між станами

трактується ймовірнісно. Рівняння системи зазвичай є набором диференціальних рівнянь, що описують зміну системи в часі. Для деяких систем головне рівняння існує і є простим, в той час як для інших систем головне рівняння може бути отриманий, але є надмірно складним.

Загалом, головне рівняння складних мереж отримують наступним чином [14]: якщо позначити змінну стану як σ_i, де всі можливі стани σ_i = 1, 2, . . . , k для кожного вузла, то конкретну конфігурацію мережі в момент часу t можна позначити як множину σ_t = (σ_1(t), σ_2(t), . . . , σ_N(t)), де i = 1, 2, ... , N, а N - кількість вузлів у мережі.

Динамічна еволюція системи задається динамікою конфігурації σ(t), яка визначається всіма можливими конфігураціями σ. Підхід вивчає ймовірність P (σ, t) того, що система знаходиться в певному стані в момент часу t. Тому рівняння еволюції для P (σ, t) в неперервному часовому наближенні має вигляд:

$$\delta_t P(\sigma, t) = \sum_{\acute{\sigma}} [P(\acute{\sigma}\ , t) W(\acute{\sigma}\ \rightarrow\ \sigma) - P(\sigma, t) W(\sigma\ \rightarrow\ \acute{\sigma})], \qquad (2.2)$$

де сума пробігає по всіх можливих конфігураціях σ, а W ($\acute{\sigma} \rightarrow \sigma$) представляє швидкість переходу від однієї конфігурації до іншої.

За винятком дуже малих систем, розв'язання головного рівняння може бути дуже складним завданням. Для великих систем повністю аналітичний розв'язок стає майже неможливим. Тому для вирішення цієї задачі були використані інші підходи, такі як різні варіації чисельного розв'язання головного рівняння.

Тут коротко представлено два різних аналітичних підходи до аналізу явищ поширення в складних мережах. Перший використовує ланцюг Маркова, вже відомий метод для процесів у дискретному наборі часу, успішно справляючись з випадковими процесами, які зазнають переходів з одного стану в інший у просторі станів.

Можна показати, що підхід з використанням ланцюгів Маркова швидко стає непрактичним з ростом розміру мережі. Інше рішення базується на теорії систем,

використовуючи набір інструментів з теорії LTI систем для подолання явищ розповсюдження в складних мережах.

2.3 Моделювання епідемій у некерованій мережі за допомогою ланцюга Маркова

Як приклад складності аналітичних розв'язків залучимо підхід до імовірнісних задач моделювання епідемій у неорієнтованій мережі за допомогою ланцюга Маркова.

Хоча ця модель є відносно простою і зрозумілою, складність системи робить її рішення обчислювально складним, а для великих систем - практично неможливим.

Природа всіх вірусоподібних динамік полягає в тому, що вони зазвичай передаються в одному напрямку. Якщо один вузол є початково інфікованим, то інфекція поширюватиметься від нього до його сусідів, але не навпаки.

При моделюванні можна знехтувати зворотною передачею шкідливих даних від одного зараженого вузла до іншого, раніше зараженого, оскільки вона не вносить жодних змін у поведінку мережі.

Крім того, можна знехтувати повторним зараженням вже інфікованого вузла в будь-якій точці між останнім інфікованим вузлом і джерелом. Це означає, що всі циклічні шляхи можуть бути видалені.

Тому для моделювання вірусного зараження мережу слід розглядати як спрямовану та ациклічну.

Напрямки ребер у мережі залежать виключно від джерела інфекції. Всі напрямки в мережі формуються в залежності від того, який вузол вважається джерелом. Таким чином, не існує єдиного рішення для зміни топології мережі, оскільки для кожного вузла, обраного в якості джерела, буде застосовуватися різний набір напрямків ребер, і, зрештою, буде стільки типологій, скільки існує можливих вузлів-джерел.

У графі розпізнаються чотири типи зв'язків: Дерево ребер, Заднє ребро, Переднє ребро та Перехресне ребро, як показано на рисунку 2.1.

Для того, щоб зробити граф ациклічним і орієнтованим, ми видаляємо всі задні ребра і залишаємо решту. Оскільки граф спочатку є неорієнтованим, те ж саме можна зробити, вибравши правильний напрямок ребер таким чином, щоб задні ребра були опущені.

Розглянемо два можливих рішення, як зробити граф спрямованим та ациклічним.

Перше рішення базується на алгоритмі пошуку в глибину, детально описаному в [70], який досліджує граф і позначає вершини та зв'язки. Він може бути використаний для виявлення MST графа, а також зворотних зв'язків, які можуть спричинити зациклення.

За винятком зворотних зв'язків, всі інші зв'язки є дозволеними, тому напрямок всіх зв'язків, які не є частиною дерева, слід вибирати наступним чином:

1. Ребра дерева - після того, як визначено мінімальне остовне дерево, ребра слід спрямувати таким чином, щоб обраний вихідний вузол став коренем.
2. Задні краї слід видалити, щоб напрямок вперед залишався активним.
3. Прямі ребра дозволені, але оскільки формується мінімальне остовне дерево, всі прямі ребра стануть частиною дерева.

Другий спосіб базується на деяких алгоритмах пошуку мінімальних остовних дерев. Наприклад, алгоритм Крускала є одним з найпопулярніших [71].

Після того, як мінімальне остовне дерево сформовано і обрано напрямки зв'язків у дереві, порівнюючи вихідний граф з мінімальним остовним деревом, ми можемо визначити інші зв'язки, які можна відновити за алгоритмом 2.1.

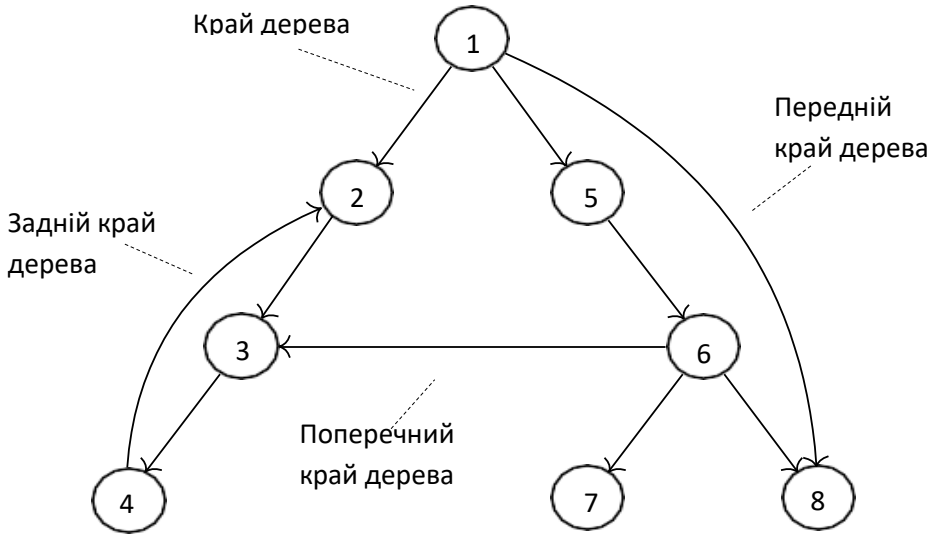


Рисунок 2.1 - Типи ребер у графі. Чотири типи ребер, які є важливими для моделювання розповсюдження: Дерево ребер, Задні ребра, Прямі ребра та Перехресні ребра

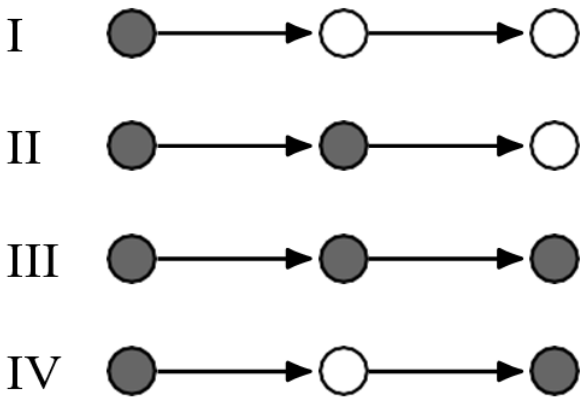


Рисунок 2.2 - Стани системи на лінійному графіку після зараження вірусом. Інфекція починається у вузлі ліворуч і поширюється за моделлю CI. Заражений вузол позначено сірим кольором. Всі можливі стани системи перераховані від I до III (стан IV неможливий).

Для того, щоб зробити граф ациклічним і орієнтованим, ми видаляємо всі задні ребра і залишаємо решту. Оскільки граф спочатку є неорієнтованим, те ж саме можна зробити, вибравши правильний напрямок ребер таким чином, щоб задні ребра були опущені.

Після процедури видалення посилань ми визначаємо всі можливі стани системи. У випадку зараження вірусом кожен вузол мережі може перебувати в одному з двох можливих станів: заражений або здоровий.

Для реалізації аналізу за допомогою ланцюга Маркова визначаються всі можливі стани системи та розраховуються всі ймовірності переходів з одного стану в інший.

У випадку з моделлю епідемії ІС існують певні обмеження щодо кількості можливих станів системи, які значно зменшують кількість станів і, відповідно, спрощують процес аналізу. Ці обмеження пов'язані з напрямком можливого зараження, як показано на рисунку 2.2.

Розглянемо просту мережу, що складається з трьох вузлів у лінійній топології зі спрямованими зв'язками, як показано на рисунку 2.2.

Якщо припустити, що інфекція виникла у вузлі 1, то можливі три стани системи (стан I, II і III). Стан IV неможливий, оскільки відновлення вузлів не розглядається, а інфекція не може обійти вузол одним шляхом. Тому ми можемо використати цю властивість для того, щоб зменшити кількість станів в аналізі.

Приклади трьох простих мереж з відповідними станами системи представлені на рисунку 2.3. Ймовірності передачі вірусу від одного сусіднього вузла до іншого незалежні і всі рівні p. Матриця P_x є матрицею переходів між станами системи для кожної мережі.

Розв'язати задачу з невеликою кількістю вузлів відносно легко, але зі збільшенням кількості вузлів у мережі зростає кількість можливих станів системи.

У випадку відносно великих мереж ідентифікація всіх станів системи стає складною. Тому ми можемо зробити певні кроки, щоб максимально спростити процес ідентифікації.

Одне з можливих рішень - розбити мережу на ряд послідовних сегментів і проаналізувати всі стани системи для кожного сегмента незалежно. Потім всі стани з кожного сегмента можна об'єднати в єдину матрицю переходів.

У моделі, що розглядається, вузол не може одужати від інфекції, і інфекція буде поширюватися в певному напрямку.

Ця властивість епідемії дозволяє розбити мережу на сегменти для аналізу комп’ютерної мережі.

У випадку деревовидної структури мережі без прямих і перехресних ребер, розбиття мережі може бути зроблено багатьма можливими способами.

Оскільки матриця переходів як всієї мережі, так і її частин є верхньотрикутною, можна сформувати єдину глобальну матрицю переходів шляхом розширення початкової матриці.

На рисунку 2.3 показано складність рішення для дуже маленької комп’ютерної системи.

Він може слугувати ілюстрацією складності деяких великих мереж.

Навіть за допомогою методів редукції станів таке рішення для великих систем залишається практично недосяжним.

2.4 Моделювання епідемій в мережах з використанням системного підходу LTI

Короткий вступ до підходу на основі теорії систем для моделювання епідемії в мережі представлено тут.

Мережа розшифровується у вигляді LTI-системи.

Розглянемо мережу, що, спостерігаючи за конкретною реакцією системи, можна сформулювати деякі висновки про потенційну поведінку мережі у випадку зараження вірусом.

Оскільки вузли взаємодіють один з одним, мережу можна розглядати як систему, що складається зі з'єднаних взаємозалежних елементів, де вихід одного елемента є одночасно входом іншого. Тому теорія систем може бути використана для опису поведінки такої системи.

Структура мережі характеризує внутрішні зв'язки. Точніше, вона описує, яким чином стани вузлів впливають один на одного і одночасно впливають на виходи, коли збуджуються входи.

У випадку з інфекцією, інфікований вузол має змінений стан і може впливати на стан сусідніх вузлів.

Оскільки епідемія базується на поширенні через мережу, передача стану вузла його сусіду є фундаментальним будівельним блоком для моделювання епідемії.

Мережа зазвичай представляється у вигляді графа *G(V, E),* з $N = |V|$ вершин або вузлів і $M = |E|$ ребер або зв'язків.

Крім того, топологія мережі зазвичай характеризується матрицею суміжності A_{adj}.

Для графа з N вершинами A_{adj} - це матриця $N \times N$, де $a_{i,j} = 1$, якщо між і-ою та j-ою вершинами є спрямоване ребро, і $a_{i,j} = 0$ в іншому випадку. Адаптована форма матриці суміжності використовується як матриця стану системи в подальшому аналізі.

З метою спрощення та обчислюваності аналізу мережа розглядається як дискретна LTI MIMO (Linear Time-Invariant, Multiple Input- Multiple Output) система з множинними входами та множинними виходами.

Для опису системи використовується формула простору станів:

$$\underline{x}(n+1) = A\underline{x}(n) + B\underline{u}(n) \quad (2.3)$$

$$\underline{y}(n) = C\underline{x}(n) + D\underline{u}(n), \quad (2.4)$$

де $\underline{x}(n) \in R^N$- вектор стану в дискретний момент часу n, $\underline{u}(n) \in R^M$ - вхідний вектор або вектор керування, а $\underline{y}(n) \in R^M$ - вихід.

Матриця $A := (a_{ij})N \times N \in R^{N \times N}$ є матрицею переходів станів, а матриця $B \in R^{N \times M}$ є вхідною матрицею.

Матриця $C \in R^{M \times N}$ є вихідною матрицею, а матриця $D \in R^{M \times M}$ - матрицею прямого зв'язку.

Елементи матриці A позначимо через a_{ij}. Граф вважається неорієнтованим.

Матриця суміжності A_{adj} представляє топологію двонаправленого графа, тому можливі петлі зворотного зв'язку, і стабільність системи буде важко досягти.

Метою побудови моделі простору станів мережі є моделювання епідемії, і тому ми повинні враховувати динаміку епідемічних явищ, що спостерігається в реальних мережах.

Для того, щоб вирішити задачу реалізації простору станів мережі, необхідно визначити внутрішню мережеву структуру системи та закодувати її у вигляді набору матриць простору станів *(A, B, C, D),* які створюють поведінку вхід-вихід.

2.5 Чисельний підхід вирішення задачі моделювання стійкості комп’ютерної мережі

Складна поведінка, що спостерігається у багатьох фізичних системах, робить її дуже складною для аналітичного опису. Складна взаємна динаміка агентів може призводити до практично нерозв'язних рівнянь. У цьому випадку використовуються агент-орієнтовані моделі (АОМ), які іноді називають мікроскопічними комп'ютерними моделями.

Цей підхід використовується, коли відома поведінка одного агента, але невідомий результат взаємодії багатьох агентів. Це один із способів переходу від нижчого (мікро) до вищого (макро) рівня систем.

Зазвичай для кожного агента існує обмежена кількість станів. Кожному агенту дається набір інструкцій, які визначають його поведінку по відношенню до різних змінних, таких як час, правила взаємодії з іншими агентами, зовнішні фактори тощо.

На кожному часовому кроці до кожного агента застосовується специфічна для моделі процедура оновлення. Потім стан кожного агента і системи в цілому оцінюється комп'ютером.

Одним з основних прикладів є агентне моделювання епідемії в мережі. Розглянемо мережу, в якій кожен вузол може перебувати в одному з двох станів A (здоровий) та B (інфікований).

Процес реакції позначимо як $A + B \rightarrow 2B$, що означає, що на кожному часовому кроці вузол зі стану А буде переходити в стан В в контакті з сусіднім вузлом, який вже знаходиться в стані В. Вважатимемо, що на початку всі вузли, крім одного, знаходяться в стані А.

Процедура моделювання однакова для кожного часового кроку і виконується наступним чином: кожен вузол в стані А перевіряє своїх сусідів, і якщо хтось з них знаходиться в стані В, він оновлює свій стан до В.

Таким чином, поведінка складної системи відтворюється в комп'ютері, пропонуючи рішення для певних задач, які можна було б вирішити лише експериментально.

2.6 Висновок

В розділі представлено опис моделювання комп’ютерних мереж, зокрема описано методи моделювання, аналізу мереж в моменти здійснення негативних зовнішніх впливів на мережу, що впливає на її стійкість.

В розділі також подано опис застосування метаевристики для моделювання стійкості комп’ютерної мережі. Описано отримання ациклічних графів при моделювання стійкості комп’ютерних мереж. Розглянуто методи проєктування стійких комп’ютерних мереж, а також подано аналітичний підхід у моделюванні складних мереж, зокрема моделювання епідемій у некерованій мережі за допомогою ланцюга Маркова, моделювання епідемій в мережах з використанням системного підходу LTI, а також чисельний підхід вирішення задачі моделювання стійкості комп’ютерної мережі.

3 МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Теорія лінійних стаціонарних систем та явища розповсюдження в мережах як основа методу синтезу апаратно-програмних засобів забезпечення стійкості

З метою вирішення задачі забезпечення стійкості комп'ютерних мереж необхідним є розроблення методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Одним з можливих шляхів розв'язку задачі є залучення теорії лінійних стаціонарних систем та явища розповсюдження в мережах як основи методу синтезу апаратно-програмних засобів забезпечення стійкості. Різноманітні системи характеризуються складними взаємозалежностями між їхніми елементами. Ці зв'язки зазвичай моделюються у вигляді мереж. З цієї причини мережевий аналіз став важливим інструментом для вивчення деяких типових явищ системної динаміки, таких як поширення інформації або кіберзагроз.

Поширення загроз характеризує численні процеси, що спостерігаються в соціальних і комунікаційних мережах [14], такі як поширення вірусів, новин та ідей серед людей, або трансляція даних і кібератаки на комунікаційні мережі. Задачі вирішуються за допомогою методів теорії лінійних стаціонарних систем (ЛСС). Протягом багатьох років теорія систем ЛСС використовувалася переважно для опису електричних ланцюгів і мереж. ЛСС підходить для опису поведінки системи, що складається з численних взаємопов'язаних компонентів.

3.1 Представлення мереж як лінійної стаціонарної системи

Теорія лінійних стаціонарних систем використовується для опису системи, що складається з багатьох взаємопов'язаних компонентів, які впливають один на одного. Одна з найвідоміших спроб використати ЛСС для опису динаміки в

складній мережі стосується конкретної задачі керованості в динамічних системах [67]. Теорія систем використовується для визначення вузлів мережі, які будуть здатні в основному динамічно впливати на систему. Тому вирішення задачі синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі можна розглядати як задачу керованості для довільних топологій і розмірів мережі, а також для зважених і спрямованих мереж.

Складні комп'ютерні мережі складаються з багатьох взаємопов'язаних компонентів, які взаємодіють один з одним або впливають один на одного, змінюючи стан вузлів, на які вони впливають. Така властивість надихнула ідею перетворення мереж на систему з множинними входами і множинними виходами (MIMO).

Для забезпечення стійкості корпоративної комп'ютерної мережі пропонується застосування теоретичного підходу ЛСС, який уможливлює відображення динаміки поширення епідемії в мережі, що описується моделями "сприйнятливий-інфікований" (CI) та "сприйнятливий-інфікований-вилікуваний".

Розглянемо комп'ютерну мережу, яку представимо у вигляді графа *G(V, E)*, з $N = |V|$ вершин або вузлів і $M = |E|$ ребер або зв'язків.

Топологія комп'ютерної мережі зазвичай характеризується матрицею суміжності A_{adj}. Для мережі з n вузлів A_{adj} - це матриця $n \times n$, де $a_{ij} = 1$, якщо і-й і j-й вузли з'єднані, і $a_{ij} = 0$ в іншому випадку. Таке представлення графа є зручним для системного теоретичного підходу, оскільки воно нагадує матрицю станів A, яка використовується у представленні простору станів фізичної комп'ютерної системи. Альтернативно, топологія комп'ютерної мережі визначимо набором ребер, представленим у вигляді матриці $M \times Z$, де M - кількість ребер, а Z - інформація про ребро. Кількість стовпців зазвичай дорівнює $Z = 3$, де перший, другий і третій стовпці складаються з вузла-джерела, вузла-приймача і ваги ребра відповідно. Передача стану є основною характеристикою моделювання епідемії. Певна небажана інформація (тобто будь-які загрози, що порушити нормальне її функціонування, наприклад віруси) потрапляє в мережу в одній або декількох точках і починає поширюватися. Згодом вона тиражується і передається від одного

вузла до іншого. Місцезнаходження загрози, а отже, і стан комп'ютерної мережі, змінюється з кожною передачею через кілька часових кроків.

Топологія мережі вважається статичною. Ці властивості дозволяють розглядати мережу як дискретну лінійну стаціонарну систему MIMO (Multiple Input - Multiple Output). Представимо простір станів, що описує таку систему як:

$$\underline{x}(n+1) = A\underline{x}(n) + B\underline{u}(n) \quad (3.1)$$

$$\underline{y}(n) = C\underline{x}(n) + D\underline{u}(n), \quad (3.2)$$

де $\underline{x}(n) \in R^N$ - вектор стану в дискретний момент часу n, $\underline{u}(n) \in R^M$ - вхідний вектор або вектор керування, а $\underline{y}(n) \in R^M$ - вихід.

Матриця A := $(a_{ij})N \times N \in R^{N\times N}$ є матрицею переходів станів, а матриця $B \in R^{N\times M}$ є вхідною матрицею. Матриця $C \in R^{M\times N}$є вихідною матрицею, а матриця $D \in R^{M\times M}$- матрицею прямого зв'язку. Для представлення динаміки системи використовується матриця системи A, яка може бути побудована як транспонування матриці суміжності, що описує топологію мережі $A = A_{adj}^T$[31]. Таке представлення передбачає, що певний сигнал збуджує систему, потрапляючи в одну або кілька вхідних точок (вузлів). Потім сигнал передається від одного вузла до іншого. Для ідентифікації вхідних вузлів пропонований метод передбачає використання матриці системи *B*. Це вхідна матриця, і вона визначається структурою системи. Матриця *B* використовується для визначення вхідних точок системи. Входів може бути один або декілька. Матриця *B* має розмірність $1 \times N$, тобто є вектором-стовпчиком з *N* елементів. Припустимо, що вхідний вузол - це *i*, тоді $b_i = 1$, в матриці $B = (b_i)1\times N$.

Під час цього процесу кожен вузол і модулює сигнал, посилюючи його на певний параметр $a_{ij} \leq 1$ перед тим, як передати його сусідньому вузлу *j*. Метод передбачає можливість вибору, які вузли спостерігати, або всі, або лише частину вузлів, і виміряти сигнал у кожному з них у часі. Для визначення спостережуваної множини вузлів використовується матриця *C*. Матриця *C* - це матриця $M \times N$ з

постійними коефіцієнтами c_{ij}, які зважують змінні стану. Зазвичай C має розмір $M \times 1$. Оскільки вузли не можуть бути частково інфіковані, стан кожного вузла в мережі є бінарним (інфікований чи не інфікований). Тому немає необхідності у зважуванні змінних стану, тобто ваги для всіх змінних однакові. Оскільки всі ваги однакові, у вихідній матриці $C := (c_i)$ M всі елементи сі рівні. Отже, в рамках запропонованого методу розумітимемо точки вимірювання як множину давачів, що збирають дані на кожному часовому кроці. Аналізуючи зібрані дані, можна дослідити динаміку в мережі та оцінити можливі наслідки інфікування певної кількості вузлів. Матриці системи генеруються однаково, незалежно від динаміки досліджуваної мережі. Таким чином, для аналізу використовується лише реакція системи на вхідний сигнал.

Матриця D, відома як матриця прямого зв'язку, є матрицею $M \times M$ з постійними коефіцієнтами d_{ij}, які зважують входи системи. Якщо D є нульовою матрицею, то вихідне рівняння зводиться до зваженої комбінації змінних стану, тобто $\underline{y}(n) = C\underline{x}(n)$.

Вхідний вектор $\underline{u}(n)$ є вхідним сигналом. У випадку дискретної системи його називають вхідною послідовністю, оскільки це вектор значень, які послідовно подаються на вхід на кожному часовому кроці. Системи зазвичай збуджуються імпульсною або ступінчастою функцією, що спричиняє відповідно імпульсну та ступінчасту реакцію. Імпульсний сигнал, також відомий як дельта-функція Дірака, позначається через δ і визначається формулою

$$\delta(n) = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases}$$

Інший спосіб, який використовується для аналізу, є одинична крокова функція, відома як функція кроку Хевісайда, що описується як функція дискретної змінної n:

$$1(x) = \begin{cases} 0, & n < 0 \\ 1, & n \geq 0 \end{cases}$$

Виконавши представлення комп'ютерної мережі як лінійну стаціонарну систему, можна використовувати різні інструменти, розроблені для системного аналізу, щоб зібрати та проаналізувати реакцію на сигнал, отриманий від комп'ютерної мережі. З цією метою здійснимо збудження системи в одній або декількох точках, імітуючи таким чином один або декілька початково інфікованих вузлів. Також можна зосередити аналіз на визначеному наборі вузлів і спостерігати за реакцією тільки для них.

Наприклад, комп'ютерна мережа з відповідною матрицею суміжності A_{adj} показана на рисунку 3.1. Представлення простору станів відповідної системи з матрицями *A, B* і *C* показано в (3.3) і (3.4). У цьому прикладі вхідний вектор $\underline{u}(n)$ подано у вигляді одиничної ступінчастої функції Хевісайда.

$$\underline{x}(n+1) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \underline{x}(n) + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \times \mathbb{1}(n)$$

$$\underline{y}(n) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \times \underline{x}(n) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \times \mathbb{1}(n) \qquad \text{(3.4-3.4)}$$

Здійснимо спостереження системи станів усіх вузлів, і тому матриця $C \in R^{M \times N}$ складається з усіх одиниць.

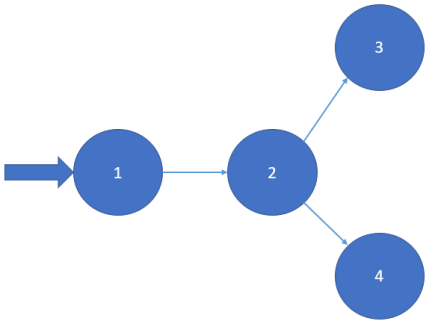


Рисунок 3.1 – Приклад представлення мережі

Для розв'язання рівнянь системи представимо її у вигляді передатної функції *H(s)*, де

$$H(z) = \frac{Y(z)}{X(z)} = C(zI - A)^{-1}B + D. \quad (3.5)$$

Крім того, ступінчасту характеристику системи отримано за формулою

$$y(t) = \mathcal{Z}^{-1}\left(\frac{1}{z}H(z)\right), \quad (3.6)$$

де $\mathcal{Z}^{-1}$ *(F(z))* - обернене $\mathcal{Z}$-перетворення функції *F(z)*.

Однак метод може бути складним для великих графів, оскільки знаходження оберненої матриці для великих матриць вимагає значних обчислювальних витрат. Альтернативним і більш зручним для програмування є рекурсивний підхід [31], який дозволяє уникнути інверсії матриці. З цією метою виконуємо вирішення рівняння простору стану - це набір лінійних різницевих рівнянь першого порядку. Цей спосіб розв'язання є зручним, оскільки його можна легко реалізувати за допомогою будь-якого доступного математичного програмного забезпечення. Ми почнемо з базових рівнянь (3.1) та (3.2). Для початкового моменту часу n0 і для кожного $n > n_0$ маємо:

$$x(n_0 + 1) = Ax(n_0) + Bu(n_0),$$

$x(n_0 + 2) = Ax(n_{0+1}) + Bu(n_0 + 1) = x(n_0 + 1) = A^2x(n_0) + ABu(n_0) + Bu(n_0 + 1)$. (3.6)

Тоді:

$$x(n) = A^{n-n_0}x(n_0) + \sum_{k=n_0}^{n-1} A^{n-1-k}\,Bu(k). \quad (3.7)$$

Виведення результатів системи матиме вигляд:

$$y(n) = CA^{n-n_0}x(n_0) + \sum_{k=n_0}^{n-1} A^{n-1-k}Bu(k) + Du(n). \qquad (3.8)$$

де *y(n)* - система, відповідальна за вхідний сигнал у часовій області.

Тут реакція позначається як *y(n),* а не *y(t),* оскільки системи, які ми спостерігаємо, є дискретними, і реакція фіксується через певні проміжки часу, тобто $n \in N$. Якщо *y(n)* є імпульсною реакцією, то вона визначається як вихідний сигнал, що виникає, коли на вхід системи подається імпульс *δ(n).* е саме стосується і ступінчастої характеристики. У цьому випадку вхідний сигнал має вигляд ступінчастої функції *1(n).* Це дозволяє передбачити, як буде виглядати вихід системи в часовій області. На практиці, у взаємопов'язаних системах вхідний сигнал надходить у мережу в одному або декількох вузлах. Потім сигнал передається від одного вузла до іншого. Він може бути змінений вузлом, через який проходить, або може залишитися незмінним. На виході отримується сума сигналів у вибраних вузлах за певний проміжок часу. Права частина (3.8) має три складові. Перша визначає значення виходу для початкового стану системи, $n = 0$. Друга частина підсумовує сигнал у всіх спостережуваних виходах за бажаний проміжок часу *n*. Третя частина оцінює вплив матриці зворотного зв'язку *D*, яка дозволяє входу системи безпосередньо впливати на вихід системи. Системи, що розглядаються в аналізі в цій дисертації, не мають елемента зворотного зв'язку, і тому матриця *D* є нульовою матрицею.

3.2 Стійкість комп’ютерної мережі в умовах епідемій шляхом застосування віртуального розширення мережі

Для забезпечення стійкості комп’ютерної мережі в умовах епідемій необхідним є дослідження епідемії як процесу, що характеризується параметром p - ймовірністю передачі загрози. Параметр p відображає ймовірність передачі вірусу від одного інфікованого до одного сусіднього сприйнятливого вузла за один крок. Лінійна стаціонарна система описує лише детерміновану поведінку. Тому

необхідно внести певні зміни в мережу, щоб використовувати пропонований підхід. Одним з прикладів є застосування віртуального розширення мережі. Динаміка системи визначається матрицею *A*, побудованою таким чином, що a_{ij} = 1, якщо між вершинами і та j існує зв'язок, за якого вершина j впливає на вершину i. Зв'язок ($j \rightarrow i$) може бути як збуджуючим, так і гальмівним, тобто $sgn(a_{ij})$ = -1 або $sgn(a_{ij})$ = 1 відповідно. У випадку інфікування вірусом у неорієнтованих мережах між кожними двома сполученими вершинами буде два зв'язки. Ваги ребер у таких мережах вважаються рівними одиниці. Зв'язки є спрямованими і збуджуючими, тому матрицю *A* можна отримати як транспоновану матрицю матриці суміжності мережі A_{adj}.

Однак, якщо матриця переходу стану *A* буде побудована просто шляхом транспонування матриці A_{adj} $A = A_{adj}^{T}$, як зазначалося раніше, петлі зворотного зв'язку будуть неминучими, тому стійкість системи за принципом «обмежений-вхід обмежений-вихід» стане серйозною проблемою. Ідея полягає в тому, щоб модифікувати матрицю *A* таким чином, щоб критерій стійкості за принципом «обмежений-вхід обмежений-вихід» виконувався, а динаміка в системі одночасно характеризувала епідемічне явище.

Щоб зробити отриману систему за принципом «обмежений-вхід обмежений-вихід» стійкою у випадку рівномірних значень a_{ij} = 1, $\forall a_{ij} \neq 0$, один з підходів полягає в усуненні всіх можливих петель зворотного зв'язку. Щоб зберегти динаміку епідемії незмінною, необхідно зробити деякі припущення:

1. Один вузол впливає на інший - сигнал в лінійній стаціонарній системі передається від вузла до сусіда без погіршення і з одиничною потужністю на кожному часовому кроці. Це означає, що передача від одного вузла до іншого відбудеться майже напевно, тобто з імовірністю p = 1

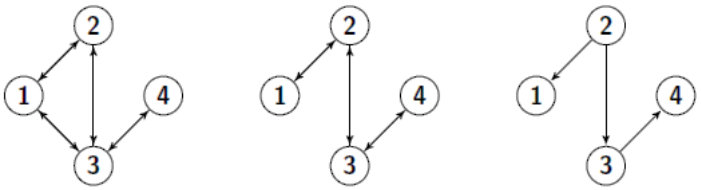
2. Передача інформації не є рекурсивною - один вузол не може бути заражений більше одного разу.

Враховуючи вищезазначені припущення, можна модифікувати топологію таким чином, щоб уникнути зациклення, а модель епідемії залишилася незмінною.

У випадку неминучого інфікування від інфікованого вузла до сусіднього, тобто при швидкості передачі p = 1, інфекція буде розповсюджуватись детерміновано. Вона буде йти найкоротшим шляхом від вузла-джерела до всіх інших досяжних вузлів мережі і час повного інфікування буде мінімальним, що дорівнює мінімальній кількості переходів від джерела до найвіддаленішого вузла. Інфекція поширюватиметься по найкоротшому шляху остового дерева з коренем у початково інфікованому вузлі. Тому побудується мінімальне остове дерево підграфом A_{tree} неорієнтованого графа A_{adj} з E(A_{tree}) ⊆ E(A_{adj}) і V (A_{tree}) = V (A_{adj}).

Наприклад, розглянемо для прикладу невеликий неорієнтований граф *G(V, E)* з M = 4 вершинами і N = 4 ребрами, показаний на рисунку 3.2a. Матрицею суміжності для цієї мережі буде матриця A_{adj}, а одним з можливих мінімальних остових дерев A_{adj} для кореневої вершини 2 буде $A_{tree}{}^{(2)}$ (рисунок 3.2b):

$$A_{adj} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, A_{tree}{}^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$



a) b) c)

Рисунок 3.2 – Приклади графів для мережі

У прикладі можна легко визначити єдине мінімальне остове дерево з коренем у вершині 2. У більших графах, як правило, існує декілька дерев з мінімальним остовим деревом, що походять з однієї вершини. Те ж саме стосується і зважених графів, оскільки сума всіх ваг ребер дерева може бути однаковою для декількох дерев. Однак, не має значення, яке саме мінімальне остове дерево буде

використовуватися у випадку майже впевненої передачі. Довжина шляху від кореня до всіх інших вузлів залишається однаковою, отже, епідемія поширюватиметься з однаковою швидкістю.

Мінімальне остове дерево неорієнтованого графа також є неорієнтованим. Для того, щоб запобігти виникненню петель зворотного зв'язку в отриманому дереві, його необхідно перетворити на спрямоване.

У випадку моделювання епідемії, напрямки, призначені кожному ребру, повинні відображати найбільш ймовірний напрямок розповсюдження епідемії.

Підграф $G_T\,(V, E_T\,)$ графа $G(V, E)$ представляє напрямок потоку інфекції через мережу. Мінімальне остове дерево може бути вирівняне в ієрархічному порядку таким чином, що кореневий вузол розташовується на вершині, перші сусіди на першому рівні, сусіди сусідів на рівні нижче, і так далі. Дотримуючись цієї домовленості, можна призначити напрямок для кожного вузла так, щоб він завжди вів з вищого рівня на нижчий. У прикладі мінімальне остове дерево $A_{tree}{}^{(2)}$ з кореневою вершиною 2 стає $A_{tree}{}^{(2)}$, як показано на рисунку 3.2c:

$$A_{tree}{}^{(2)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Оскільки матриця A є транспонуванням матриці суміжності, то маємо $A = A_{tree}{}^{(2)\mathrm{T}}$. Також, для прикладу на рисунку 3.2, з вхідним вузлом2 B =$[0\ 1\ 0\ 0]'$.

Значення c_i можуть бути визначені без будь-яких обмежень з множини дійсних чисел, але для простоти обрано одиничне значення.

Якщо необхідно спостерігати за всіма вузлами мережі, то $c_i = 1$ для i = 1, 2, 3 ... M . У прикладі на рисунку 3.2, $C = [1\ \ 1\ \ 1\ \ 1]$.

Нарешті, лінійна стаціонарна система, побудована на основі мережі з рис.3.2, складається за допомогою матриць простору станів *A, B і C*.

Після початкового збудження системи функцією Дірака-дельта $\delta(n)$ або Хевісада-кроку 1(n), набору значень було присвоєно вихідний вектор $\underline{y}(n)$. Застосувавши рекурсивний розв'язок з (3.8), отримаємо вихід системи у вигляді імпульсної та ступінчастої характеристики для входів $\delta(n)$ або 1(n) відповідно.

1) імпульсна характеристика системи має вигляд $\underline{y_\delta}(n) = [1\ \ 2\ \ 1\ \ 0]$;
2) ступінчаста реакція системи має вигляд $\underline{y_1}(n) = [1\ \ 3\ \ 4\ \ 4]$.

Змоделюємо поширення епідемії в тій самій мережі з тим самим початковим вузлом (вузлами) та ймовірністю передачі $p = 1$. Модель епідемії, що моделюється тут, є простою моделлю SI. На виході симуляції отримуємо два вектори: $\underline{v}(n)$, де кожне значення представляє кількість інфікованих вузлів на певному часовому кроці, і $\underline{v_u}(n)$, де кожне значення представляє загальну кількість інфікованих вузлів від початку інфікування до певного часового кроку.

1) кількість інфікованих вузлів у кожен момент часу $\underline{v}(n) = [1\ \ 2\ \ 1\ \ 0]$;
2) сума заражених вузлів у кожен момент часу $\underline{v_u}(n), = [1\ \ 3\ \ 4\ \ 4]$.

Видно, що для прикладу ($p = 1$) ступінчастий відгук відповідає загальній кількості інфікованих вузлів, так що $\underline{y_1}(n) = \underline{v_u}(n)$, а імпульсний відгук відповідає кількості інфікованих вузлів на кожному часовому кроці, так що $\underline{y_\delta}(n) = \underline{v}(n)$.

Ще один більш наочний приклад невеликого деревоподібного графа представлений на рисунку А.2 Додатку А. Матриця А є двійковою. Вихід вимірюється у всіх вузлах одночасно, тобто здійснюється спостереження за всіма вузлами як за виходами і обчислюється кінцевий вихід як суму рівнів сигналів у всіх вузлах за кілька часових кроків. На вхід подається один вузол i, розташований в центрі, який є батьківським вузлом дерева, де величина відгуку в часі дорівнює кількості вузлів на відповідних логічних рівнях. Для випадку передачі вірусу в прикладі мережі з джерелом у вузлі i та майже стовідсотковою передачею вірусу від інфікованого до сприйнятливого вузла, імпульсна характеристика показує точну кількість інфікованих вузлів з плином часу. Аналогічно, ступінчаста характеристика показує загальну кількість інфікованих вузлів. Наведений приклад

показує, що підхід може бути використаний для вивчення епідемій в мережах до певної міри. Однак метод аналізу обмежується лише деревовидними графами з майже стовідсотковою передачею інфекції від інфікованого до сприйнятливого вузла. В реальності поширення інфекції характеризується коефіцієнтом передачі нижче 100%, і, як правило, p = 1. Для малоймовірного випадку p = 1, мережа може бути перетворена до дерева найкоротшого шляху з вузлом, оскільки батьківський вузол як шлях інфікування відомий, і непотрібні ребра можуть бути видалені, не впливаючи на динаміку інфікування. З іншого боку, для будь-якого p < 1 не можна нехтувати кількістю декількох вхідних ребер і декількох можливих шляхів. Аналіз стаціонарних систем не враховує стохастичну динаміку взаємної взаємодії між елементами. Крім того, введення ймовірностей в кожну ітерацію рівняння (3.7) призведе до того, що система стане змінною в часі. Тому необхідним є здіснювати трансформування архітектури комп'ютерної мережі в належну лінійну стаціонарну систему з урахуванням ймовірностей передачі. Це може бути використано для прогнозування динаміки інфікування на довільній топології для будь-яких $0 \leq p \leq 1$ (рис.А.2 Додатку А).

3.2.1 Дослідження стійкості комп'ютерної мережі в умовах невизначеної передачі даних та віртуального розширення мережі

Динаміка епідемій в комп'ютерній мережеві майже завжди характеризується ймовірністю передачі *p*. Це ймовірність передачі загрози від інфікованого до сприйнятливого індивіда незалежно один від одного за один часовий крок. Однак для неінфікованого вузла *i* з k_i інфікованими сусідами ймовірність передачі стає $p_i = 1-(1-p)k_i$. Зазвичай, *p* вважається однаковим незалежно від вузла, хоча можна використовувати різні значення p для кожної пари вузлів, тому p є значенням, яке скоріше присвоюється краю, оскільки воно кількісно визначає зв'язок між двома сусідніми вузлами. Його також можна розглядати як вагу конкретного ребра. Сам по собі підхід ЛСС не дає можливості ввести ймовірності. Тому для модифікації вихідної мережі перед перетворенням до форми, придатної для ЛСС, вводиться

альтернативна концепція, яка називається віртуальним розширенням мережі (Virtual Network Expansion).

Розглянемо неорієнтовану мережу $G(V, E)$ з ймовірністю передачі вірусу $0 < p < 1$. Далі припустимо, що існує вторинна мережа $G_E(V_E, E_E)$ з $p = 1$, яка буде демонструвати ті ж властивості, що і вихідна мережа $G(V, E)$ у випадку інфікування вірусом. У запропонованому рішенні сусідню пару вузлів $i \rightarrow j$ з ймовірністю передачі вірусу $0 < p < 1$ можна замінити відповідною кількістю вузлів $i \rightarrow n1 \rightarrow n2 \rightarrow \ldots \rightarrow j$ з ймовірністю передачі вірусу $p = 1$ між кожним з них. Процес вставки проміжних вузлів показано на рисунку 3.4.

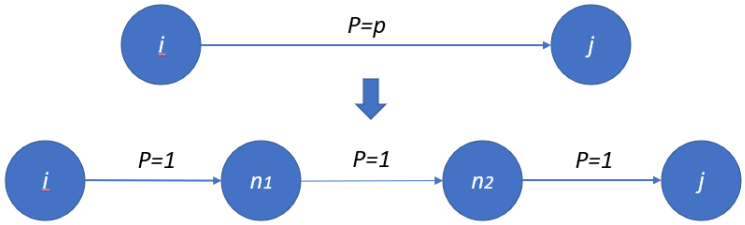


Рисунок 3.4 - Моделювання стійкості комп'ютерної мережі в умовах епідемій шляхом застосування віртуального розширення мережі

Тепер розглянемо випадок, коли вузол і заражений, а його сусід j сприйнятливий до інфікування. На одному часовому кроці вузол j буде заражений з ймовірністю p. Врешті-решт, вузол j буде заражений після певної кількості випробувань. Всі випробування окремо можна представити як додаткові проміжні вузли з ймовірністю передачі $p = 1$ між кожним з них. Тому важливо визначити кількість проміжних вузлів $\bar{k}$. Число $\bar{k}$ можна отримати з дискретного геометричного розподілу ймовірностей, як кількість випробувань до досягнення успіху. Геометричний розподіл, як окремий випадок від'ємного біноміального розподілу, є дискретним розподілом для $k = 0, 1, 2, \ldots$ з функцією щільності ймовірності

$$P(k) = p(1-p)^k, \tag{3.9}$$

де ймовірність успіху позначено через p, де $0 \leq p \leq 1$, а кількість спроб, необхідних для досягнення успіху, позначено через k.

Для процедури розширення мережі для кожного ребра випадковим чином вибирається значення $P(k)$ за рівномірним розподілом з множини дійсних чисел так, що $0 \leq P(k) \leq p$. Потім обчислюється кількість додаткових вузлів k^{-}:

$$k = \frac{\log\left(\frac{P(k)}{p}\right)}{log(1-p)}. \tag{3.10}$$

Значення k, отримане з (3.10), є дійсним числом $k \in R$, а кількість спроб до успіху, тобто кількість додаткових вершин k^{-} є цілим числом $k^{-} \in N$ і визначається як нижня функція від k, оскільки $k^{-} = \lfloor k \rfloor$. Додавши відповідну кількість вузлів між кожною парою вузлів початкової мережі, можна створити розширену мережу $G_E(V_E, E_E)$. Розширена мережа буде складатися з початкової та додаткових вузлів $V \in VE$. Ймовірність передачі вірусу в G_E дорівнює $p = 1$.

Динаміка інфікування у вихідній мережі G відповідає ступінчастому відгуку системи, побудованої з розширеної мережі G_E. при аналізі системи розширеної мережі $G_E(V_E, E_E)$ можна спостерігати тільки вихід у підмножині вузлів V з вихідної мережі $G(V, E)$, тому системна матриця C розширеної мережі має вигляд $C_E = C_E(V)$. Додаткові вузли ігноруються як виходи, і це є основною причиною того, що процес називається розширенням віртуальної мережі.

Для того, щоб порівняти запропонований підхід ЛСС з традиційною динамікою інфікування КМ на основі агентів, було проведено чисельне моделювання. В якості тестового майданчика було використовуємо випадково згенеровані комп'ютерні мережі з хостами мережі $G(V, E)$ з $|V| = 100$ (вузлами) і $|E| \approx 200$ ребрами, згенеровані за допомогою трьох різних мережевих моделей. Результати моделювання усереднено за 100 окремими прогонами. Було перевірено дві гіпотези: чи можна перетворити вихідну мережу з $P = p$ на нову мережу з $P = 1$, яка може мати такі ж властивості поширення, як і вихідна. Перетворення відбувається за допомогою віртуального розширення мережі; та чи можна

змоделювати інфекцію в оригінальній мережі, використовуючи динаміку ЛСС в розширеній мережі.

З цією метою було здійснено перевірку, чи може розширення віртуальної мережі призвести до появи вторинної мережі з ймовірністю передачі вірусу $p = 1$, яка поводитиметься так само, як і початкова мережа у випадку інфікування вірусом. Для моделювання динаміки поширення вірусу в цьому випадку використовуємо модель епідемії "сприйнятливий-інфікований". Тому наступним кроком було здійснено моделювання поширення загрози стійкості КМ на трьох випадкових мережах, згенерованих наступними методами [3-5]. Ймовірність передачі для вихідних графів вибрано рівною $p = 0{,}4$. Потім було розширено вихідні мережі $G(V, E)$ і знову проводимо моделювання з ймовірністю інфікування $p = 1$ на розширених мережах $G_E(V_E, E_E)$. Інфікування загрозою моделюється, починаючи з одного і того ж початкового вузла для вихідної та розширеної мереж. Було здійснено спостереження за кумулятивною кількістю заражених вузлів з плином часу. На рисунку А.1 Додатку А показано майже ідеальний збіг результатів моделювання для вихідної та розширеної мереж, що доводить можливість застосування методу розширення мережі може бути використаний для забезпечення стійкості корпоративної комп'ютерної мережі в умовах епідемій.

Наступним кроком методує є порівняння динаміки інфікування вихідної мережі $G(V, E)$ та реакцію системи, отриманої з розширеної мережі $G_E(V_E, E_E)$.

Подібно до прикладу, показаного на рисунку А.1, спочатку моделюється динаміка поширення за допомогою моделі SI. На кожному часовому кроці t заражений вузол намагається заразити сприйнятливого сусіда. Інфекція передається з ймовірністю $p = 0.4$. Таким чином, сприйнятливий вузол заражається з ймовірністю $P = 1 - (1 - p)k$, де k - кількість інфікованих сусідів. Дані, зібрані за допомогою симуляції, включають кумулятивну кількість інфікованих вузлів $\underline{vu}(n)$ та кількість інфікованих вузлів на кожному часовому кроці $\underline{vu}(n)$, яка є похідною від $\underline{vu}(n)$. Потім система створюється з розширеної мережі $GE(VE, EE)$ з ймовірністю інфікування $p = 0.4$. На рисунку А.2 Додатку А (перший ряд) показано динаміку епідемії як vu(n), змодельовану на вихідній мережі з ймовірністю

інфікування p = 0,4. Значення $\underline{v_U}(n)$ порівнюються зі ступінчастою реакцією $\underline{y_H}(n)$ системи, створеної на основі розширеної вихідної мережі. Результати, отримані в результаті моделювання та реакція системи сильно корелюють. Еволюція епідемії в часі поводиться так, як передбачено запропонованою моделлю ЛСС. Подібні результати показані на рисунку А.2 Додатку А. Результати симуляції SI $\underline{v}(n)$ тепер порівнюються з імпульсним відгуком $\underline{y_\delta}(n)$ відповідної ЛСС-системи. Цього разу кількість заражених вузлів на кожному часовому кроці порівнюється з виходом системи, збудженої імпульсною функцією. Кореляція між результатами є значною.

3.2.2 Оброблення вхідних даних, отриманих зі змодельованої комп'ютерної мережі

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є оброблення вхідних даних, отриманих з комп'ютерної мережі.

Три типи мереж, що використовуються в моделюванні, генеруються випадковим чином за трьома різними мережевими моделями. Як приклад простого випадкового графа було обирано модель, запропоновану в [36]. Мережа будується з набору N вузлів, а потім генеруються ребра. Ймовірність наявності ребра між двома вершинами дорівнює p, а ймовірність відсутності ребра дорівнює 1 - p. Середній ступінь $\langle k \rangle$ обчислюється з кількості ребер $\langle E \rangle$, згенерованих у графі $\langle E \rangle = \frac{1}{2} N (N - 1)p$. Оскільки кожне ребро з'єднує дві вершини, воно бере участь в обчисленні степеня для обох вершин. Отже, маємо $\langle k \rangle \simeq$ Np.

Друга група мереж згенерована з парними властивостями, а саме коефіцієнт кластеризації та середній найкоротший шлях, які є більш схожими на ті, що проявляються в реальних мережах. Мережі малого масштабу є високо кластеризованими і водночас мають короткі довжини шляхів. Мережа генерується за допомогою процедури випадкового перемонтажу для інтерполяції між

звичайною кільцевою решіткою та випадковою мережею, без зміни кількості вершин або ребер у графі.

Третя модель генерує мережу з властивостями, де розподіл ступенів $P(k)$ вузлів мережі з k зв'язками з іншими вузлами підпорядковується степеневій функції $P(k) \sim k^{\gamma}$, де γ - параметр, значення якого зазвичай знаходиться в діапазоні $2 < \gamma < 3$. Мережа формується за принципом преференційної прив'язаності, відомим також як феномен "багатий стає багатшим", принцип Гібрата або кумулятивна перевага [14].

Щоб продемонструвати можливість застосування ЛСС підходу до аналізу динаміки поширення, ми наведемо простий приклад. Візьмемо невелику неорієнтовану мережу $G(V, E)$ з $|V| = 6$ вузлів і $|E| = 5$ ребер (рис. А.3 Додатку А) і застосуємо підхід ЛСС у двох сценаріях.

По-перше, ми покажемо, як зміна ймовірності передачі p впливає на реакцію відповідної системи ЛСС. У прикладі мережі з Рисунку 4.8а топологія залишається незмінною, але ймовірність передачі змінюється з $p1 = 0.6$ до $p2 = 0.2$. Ймовірність передачі однакова для всіх пар сусідніх вузлів, і вважається, що інфекція походить з вузла (1). На основі інформації про топологію $G(V, E)$ ми будуємо дві системи ЛСС: першу з $p_1 = 0.6$ і другу з $p_2 = 0.2$. Потім ми обчислюємо ступінчасті відгуки для отриманих систем і зображаємо їх на рисунку А.3 Додатку А. Було виявлено різницю між нахилами двох отриманих кривих. Крива з більшим нахилом представляє ступінчасту характеристику системи, отриману від мережі з більшою швидкістю передачі. Таким чином, аналізуючи реакцію даної системи, можна оцінити динаміку епідемії у відповідній мережі. Нахил кривої відповідає швидкості поширення епідемії в кожний момент часу.

Для того, щоб оцінити оптимальну стратегію захисту, було побудовано три відповідні системи ЛСС для кожної з можливостей: без модифікації (всі ймовірності переходів залишаються незмінними, $p = 0.6$), ребро $3 \leftrightarrow 4$ модифіковано і ребро $4 \leftrightarrow 6$ модифіковано.

Потім обчислено ступінчасту характеристику всіх систем (рисунок А.4 Додатку А). Нахил кривої ступеневої реакції вказує на швидкість поширення

епідемії, а момент, коли крива досягає максимального значення, вказує на час, необхідний для повного інфікування. Спостерігаючи за кривими на рис. А, було зроблено висновок, що найкращим рішенням є зниження швидкості передачі на межі 3 ↔ 4. Представлена тут мережа є досить простою, а рішення щодо оптимізації - тривіальним. Видно, що підхід ЛСС може бути використаний для аналізу та оптимізації мереж протидії епідеміям та забезпеченння стійкості мережі.

Основною проблемою є необхідність модифікувати мережу, яку необхідно виконати для того, щоб ця модель працювала для забезпечення стійкості комп'ютерної мережі. Це вимагає додаткової модифікації топології шляхом віртуального розширення мережі. Однак результати показують, що стан мережі під час епідемії може бути розрахований на будь-який момент часу, навіть без використання агентного моделювання. Крім того, цей підхід відкриває можливість впровадити набір інструментів з теорії систем у моделювання епідемій.

3.3 Виявлення впливових розповсюджувачів, що порушують стійкість мережі

Наступним кроком запропонваного методу є вирішення проблеми модифікації комп'ютерної мережі. Це вимагає додаткової модифікації топології шляхом віртуального розширення мережі. Однак результати показують, що стан мережі під час епідемії може бути розрахований на будь-який момент часу, навіть без використання агентного моделювання. Крім того, цей підхід відкриває можливість впровадити набір інструментів з теорії систем у моделювання епідемій.

Існує багато методів оцінки важливосчті вузла в мережі. Більшість підходів базуються на різних мірах центральності та їх варіаціях. Такі міри як ступінь (degree), H-індекс (h-index), центральність ядра (coreneess) та динамічна чутлива центральність (DS centrality), намагаються кількісно оцінити, наскільки вузол є центральним у мережі відносно топології [4, 46, 81, 82]. Різні міри центральності призначені для кількісної оцінки важливості вузла для різних процесів поширення, і не всі вони є корисними для всіх типів мереж. Наприклад, для визначення

найвпливовіших розповсюджувачів у соціальних мережах k-shell є більш надійною, ніж ступінь.

Пропонований метод використовує міру Node Imposed Response (NiR), [35], яка фіксує потенціал поширення вузла. Він може точно класифікувати найважливіші вузли на основі їхнього можливого впливу на поширення.

Міра перевершує результати вищевказаних мір. Незважаючи на те, що NiR не залежить від жодних параметрів, його ефективність можна порівняти з такими мірами центральності, як динамічна чутлива центральність (DS) [51], які використовують параметри для кращого пристосування до динаміки розтікання.

Міра NiR використовує концепції теорії систем ЛСС і базується на значенні відгуку системи на вхідну функцію кроку. Таким чином, підхід ЛСС може бути використаний для оцінки потужності поширення вузла.

Крім того, він може бути застосований для визначення різних можливих впливів від одного або декількох джерел на один або декілька кінцевих вузлів. Модифікації вихідного показника можуть бути зроблені простим маніпулюванням відповідними системними матрицями.

NiR - це нормоване максимальне значення крокової характеристики S_i для відповідної ЛСС-системи з вузлом i на вході. Визначимо максимальне значення ступеневої характеристики для вузла i як S_i, тоді

$$S_i = \max y_i(t),\ 1 < t < k. \qquad (3.11)$$

Функція $y_i(t)$, отримана з (3.6), є увігнутою і врешті-решт досягає свого максимального значення при достатньо великих t. Тому S_i завжди буде існувати. Звідси випливає, що

$$NiR(i) = (Si - Smin)/(Smax - Smin), \qquad (3.12)$$

де $S_{max} = max_{j\in\{1,\dots,n\}} S_j$, $S_{min} = min_{j\in\{1,\dots,n\}} S_j$, а n - кількість вузлів у мережі.

Для того, щоб обчислити S_i, необхідно побудувати відповідну систему ЛСС, яка визначається системними матрицями *A, B, C і D*. Перед створенням матриці *A* необхідно виконати деякі модифікації вихідного графа. Для того, щоб зберегти стабільність системи "обмежений вхід - обмежений вихід" (BIBO), топологія повинна бути змінена таким чином, щоб видалити цикли. NiR можна обчислити лише для ациклічних орієнтованих графів. Для процесів поширення, таких як «Сприйнятливі-Інфікований» (SI) та «Сприйнятливі-Інфікований-Відновлений» (SIR), цикли можна вважати несуттєвими, оскільки вершини не можуть бути заражені двічі. Крім того, видалення ребер, які утворюють цикли, не повинно суттєво впливати на динаміку розповсюдження. Алгоритми видалення циклів можуть змінити топологію мережі так, що деякі шляхи стають недоступними, особливо в неорієнтованих мережах, де потрібно вибирати напрямок ребра.

Щоб зберегти найважливіші шляхи з вихідного вузла і мінімізувати кількість видалених ребер, важливо обрати правильний метод видалення циклів. Після маніпуляцій з вихідним графом ми створюємо матрицю системи *A* таким чином, що $A = A_{adj}^{T}$. Всі ненульові елементи замінюються значенням *d*, так що $\forall a_{ij} = 0 : a_{ij} = d$, і $0 < d < 1$. Можна вибрати будь-яке значення *d* між 0 і 1, але краще вибрати $d \ll 1$. Додаткове дослідження показує, що дисперсія між значеннями NiR для всіх вузлів стає вищою при меншому *d*.

У випадку будь-якої відносно великої мережі дисперсія між мірами вузлів стає більш важливою для правильної класифікації вузлів, оскільки існує велика частка не-вузлів, вузлів з дуже схожою і малою потужністю поширення.

У цьому випадку низька дисперсія може призвести до хибної оцінки, особливо враховуючи видалення циклів та деякої інформації про топологію, яка втрачається під час процесу. Тому вибір меншого *d* є важливим для правильної диференціації вузлів. У моделюванні було використано $d = 0.1$.

Матриця $B_{[1\times n]}$ складається з усіх нулів, окрім вхідного вузла і, який оцінюється, у цьому випадку $b_{i=1}$. Матриця $C_{[1\times n]}$ є вектором всіх одиниць, оскільки вихід спостерігається у всіх вузлах і вона не зважена.

Кроковий відгук отриманої системи з часом досягне максимального значення S_{max}. Саме це значення, розраховане для вхідного вузла і нормоване по всіх вузлах в діапазоні [0, 1], і є NiR.

3.4 Знаходження найбільш критичних вузлів в комп'ютерній мережі

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є знаходження найбільш критичних вузлів в комп'ютерній мережі. Для вирішення даної підзадачі було використано модель каскадних відмов [75], яка моделює перевантажені вузли як нефункціональні. Модель дозволяє встановити факт, що атака на один важливий вузол (з високим початковим навантаженням) може викликати каскадний ефект, який може призвести до збою всієї мережі та, як наслідок, серйозного збою служби.

Таким чином, вважатимемо найбільш критичним вузлом той, видалення якого спричинить найбільшу шкоду мережі. Пошкодження визначається як зворотна величина найбільшого підключеного компонента, що залишився після моделювання каскаду. Після видалення вузла і відносний розмір найбільшого з'єднаного компонента, що залишився, дорівнює G_i і так само після видалення j відносний розмір найбільшого з'єднаного компонента дорівнює G_j . Якщо $G_i < G_j$, ми робимо висновок, що вузол і є більш критичним. Процес моделювання представлений у вигляді псевдокоду в Алгоритмі Б.1 Додатку Б.

Після видалення вузла і відносний розмір найбільшого з'єднаного компонента, що залишився, дорівнює G_i і так само після видалення j відносний розмір найбільшого з'єднаного компонента дорівнює G_j . Якщо $G_i < G_j$, ми робимо висновок, що вузол і є більш критичним.

Q(V, E) - це граф, що складається з множини вершин *V* та множини ребер *E*. Навантаження та пропускна здатність вершини позначаються через F_i та M_i відповідно. Розмір найбільшої компоненти, що залишився після каскаду для множини видалених вершин *I*, позначається як G_I . Параметр допуску - α.

Результати моделювання відмов вузлів, що найбільш критичним вузлом є вузол з другим за величиною початковим навантаженням, за яким слідує вузол з сьомим за величиною початковим навантаженням. Припускається, що найбільш критичний вузол (на основі його міри центральності) знаходиться на третьому місці серед найбільш важливих вузлів. Ця міра - відносний розмір найбільшого приєднаного компонента $G = K'/K$. Хоча відносний розмір найбільшого компонента відображає загальний стан мережі, він може іноді вводити в оману, оскільки фокусується виключно на найбільшому компоненті, ігноруючи решту мережі. Може статися так, що КМ буде фрагментована на один великий компонент, оточений багатьма невеликими підмережами. З іншого боку, мережа може бути фрагментована таким чином, що всі маленькі частини з'єднані між собою. Властивості цих двох отриманих мереж можуть бути різними, навіть якщо розміри найбільших компонентів залишаться однаковими.

Крім того, розмір найбільшого підключеного компонента не обов'язково відповідає кількості перевантажених (виведених з ладу) вузлів під час каскаду. Іноді невелика кількість вузлів, що вийшли з ладу, може призвести до значної фрагментації мережі. Вузли з вищою централізацією зв'язку спричиняють відмову інших вузлів, що сильно фрагментує мережу.

Модель каскадних відмов використовує параметр толерантності $\alpha \geq 1$, який кількісно визначає додаткову пропускну здатність вузлів відносно початкового навантаження. Динаміка каскадних відмов значною мірою залежить від обраного значення α. Результати каскадного моделювання з використанням моделі показали, що найбільш критичний вузол залежить від обраного значення α. Для різних α різні вузли виявляються найбільш критичними. У таблиці 3.1 показано вибрані вузли та відповідний вплив на мережу після видалення вузла. Мірою пошкодження є відносний розмір найбільшого підключеного компонента G. Чим менший, тим більший збиток спричинені видаленням вузла. Вплив видалення окремих вузлів, кількісно оцінений за розміром найбільшого приєднаного компонента G після моделювання каскадної відмови за моделлю [83]. Моделювання проведено для

різних значень α. Підкреслено значення підкреслене значення є найнижчим значенням G, а стовпчик у стовпчику вказує на найбільше пошкодження мережі.

Таблиця 3.1 - Вплив видалення окремих вузлів

№ вузла мережі	$G_{\alpha=1.01}$	$G_{\alpha=1.10}$	$G_{\alpha=1.30}$	$G_{\alpha=1.50}$
19	0.311	0.232	0.312	0.411
18	0.299	0.361	0.533	0.544
44	0,443	0.470	0.456	0.378
11	0.456	0.489	0.912	0.912
43	0.542	0.493	0.689	0.697
12	0.572	0.611	0.912	0.941
19	0.598	0.612	0.965	0.9247
46	0.514	0.611	0.632	0.635
45	0.844	0.868	0.899	0.891
47	0.262	0.618	0.626	0.733

У випадку виходу з ладу вузла i, під загрозою опиняється вузол j, оскільки навантаження може перевищити його пропускну спроможність. Нехай визначимо надлишкове навантаження на вузол j як F'_j, а пропускну здатність як M_j. Вузол j залишається працездатним до тих пір, поки $F'_j > M_j$. Всі значення F'_j, які менші або дорівнюють пропускній здатності, не мають значення, оскільки вузол може витримати це навантаження. Для різних параметрів допуску α змінюються потужності всіх вузлів. Надлишкове навантаження, однак, залишається незмінним. Зміна параметра допуску впливає на розподіл потужностей. Тоді надлишкове навантаження має досягти іншого порогу, щоб вузол вийшов з ладу.

Випадкові множинні збої трапляються рідше, ніж поодинокі. Однак, кілька одночасних збоїв можуть бути спричинені зловмисною атакою. Потенційна шкода, спричинена виведенням з ладу двох або більше вузлів, може бути руйнівною. Зловмисник може мати достатньо знань про топологію мережі, а потім виконати

оптимальну атаку. Якщо зловмисник може вибрати *k* вузлів для видалення, то оптимальною атакою буде та, яка завдасть найбільшої шкоди.

3.5 Знаходження множини k найбільш критичних вузлів мережі

Можлива ситуація, коли можуть існувати набори з k вузлів, одночасне видалення яких призведе до однакової або дуже схожої шкоди. Це означає, що для одного значення k існує декілька рішень. Зловмисник може зосередити всі свої ресурси на цьому невеликому наборі вузлів і все одно завдати значної шкоди стійкості мережі. Для вирішення підзадачі знаходження множини k найбільш критичних вузлів мережі було використано генетичний алгоритм. Набір з 100 найбільш критичних вузлів включається в додаткову оцінку. Початковий простір розв'язків різко зменшується, але все ще має значний розмір (F_n=10 = 1,73 × 1013). Генетичний алгоритм уможливлює знайти розв'язок через поступове покращення пристосованості всього покоління. Оптимізація, що проводилася, була цілочисельною задачею, де рішенням є масив з n цілих чисел в діапазоні від 1 до 100, і кожне значення зіставляється з відповідним ідентифікатором вузла. Максимально 100 вузлів можна було об'єднати в групи, що складаються з *k* елементів кожна. Набір з 100 вузлів було визначено за допомогою попереднього аналізу впливу окремих вузлів. Підхід генетичного алгоритму для знаходження критичної групи представлено у вигляді псевдокоду в Алгоритмі 3.1.

Алгоритм 3.1 – Знаходження найбільш критичної групи за допомогою генетичного алгоритму

1: Вхід: G(V, E)

2: Параметри ініціалізації: розмір популяції встановлено на pop = 200 з обмеженням на максимальне Ngen = 1200 поколінь

3: Створення початкової популяції: початкова популяція створюється випадковим чином із рівномірним розподілом

4: поки кількість поколінь досягає максимуму до t> Ngen

5: виконати кросовер

6: тоді як для всіх рішень у популяції

7: видалити вузли t ініціалізувати каскад

8: виконати оцінку t, значенням функції пристосованості, яка є розміром найбільшої компоненти.

9: відсортувати рішення з останнього покоління

10: повернути групу вузлів

Додаткова перевірка за допомогою генетичного алгоритму підтримує рішення зосередити пошук на відносно невеликій кількості критичних вузлів.

3.6 Висновок

У розділі запропоновано метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Для вирішення задачі метод передбачає залучення теорії лінійних стаціонарних систем, та використання метрики NiR, яка може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

Було здійснено апробацію методу шляхом моделювання, результати якого показують високу кореляцію з фактичною динамікою поширення, змодельованою за допомогою процесів SI та SIR.

NiR також показує невелику дисперсію, що означає його надійність для різних топологій комп'ютерних мереж. Парадигма, що лежить в основі підходу ЛСС, допускає численні варіації вихідної метрики.

Наприклад, кількість точок входу та виходу в системі може бути різною. Вибравши декілька вхідних точок, можна оцінити вплив багатьох вузлів мережі, якщо вони будуть збуджені одночасно. Крім того, вибір декількох вихідних точок дасть змогу оцінити вплив цих вузлів у разі поширення процесу.

Більш вразливі вузли з більшою ймовірністю будуть досягнуті з набору обраних вхідних вузлів. Аналіз не обмежується незваженими мережами. Той самий підхід може бути використаний навіть для зважених мереж, просто включивши ваги в матрицю досліджуваної системи.

Також метод передбачає знаходження найбільш критичних вузлів в комп’ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

4 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ МЕТОДУ СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

4.1 Експериментальні дослідження методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

З метою здійснення апробації та перевірки ефективності запропоногого методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі було здійсненого ряд експериментальних досліджень.

На рисунку 4.1 показано приклад невеликої мережі з n = 10 вузлами. Кожен з вузлів має своє значення NiR, вказане вище. Для того, щоб обчислити NiR, топологія повинна бути змінена, щоб зробити мережу ациклічною. Модифікація виконується для кожного вузла незалежно. З цією метою було проведено екперимент з синтезованими довама версіями топологій з двома вузлами-джерелами: вузол з ID1 ліворуч і вузол з ID10 праворуч.

Значення NiR вказує на потужність поширення загрозу, тобто вузол космп'ютерної мережі з вищим NiR швидше заразить всю мережу або більшу її частину.

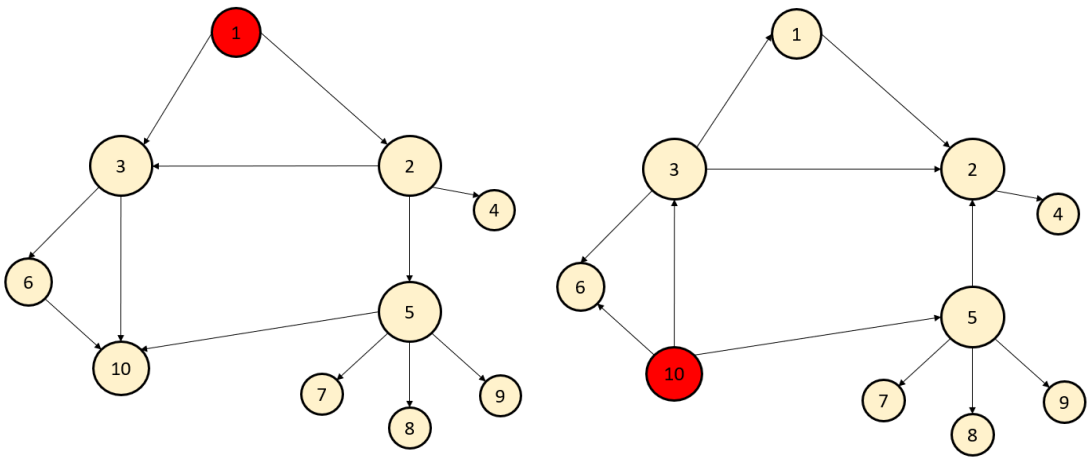


Рисунок 4.1 - Виявлення впливових розповсюджувачів, що порушують стійкість мережі

Твердження підтверджується моделюванням динаміки поширення SI та порівнянням результатів з отриманими значеннями NiR.

Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування.

Якщо час повного інфікування коротший, то вузол має потенціал для швидшого поширення інфекції і вважається більш важливим (тобто більш впливовим).

Для того, щоб порівняти значення NiR та змодельований потенціал розповсюдження, здійснюється мортування вузлів як за значенням NiR, так і за потужністю розповсюдження, отриманою в результаті здійсненого моделювання.

Таким чином, було визначено кілька окремих груп вузлів з різним потенціалом поширення (рисунок 4.2).

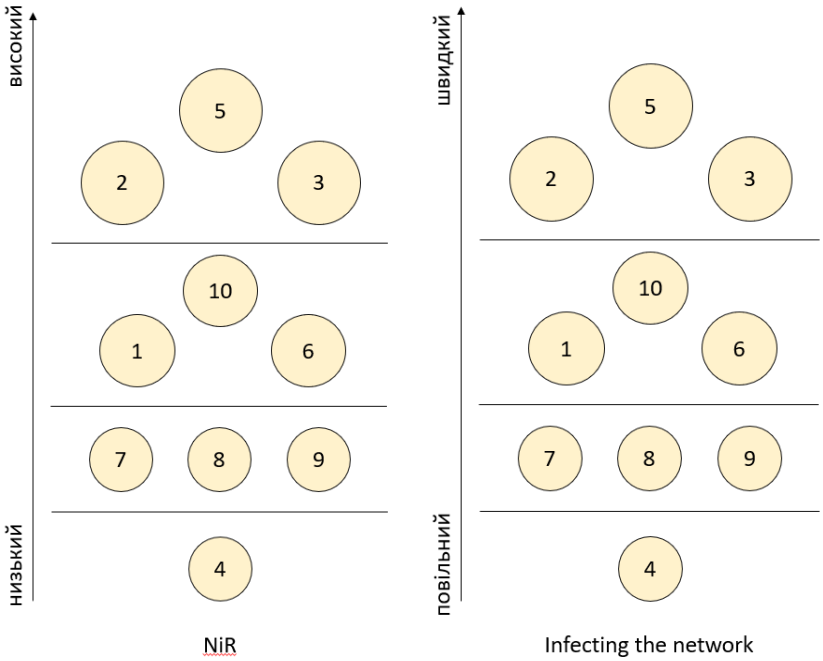


Рисунок 4.2 – Потенціал поширення

У випадку невеликої мережі значення NiR точно відображає потенціал розповсюдження, оскільки групування вузлів збігається з отриманим в результаті

чисельного моделювання. Ймовірно, що для великих мереж, де n>10, буде багато вузлів з дуже схожими значеннями NiR, що відповідає вродженому принципу безмасштабності багатьох мереж, з великою часткою не-вузлів.

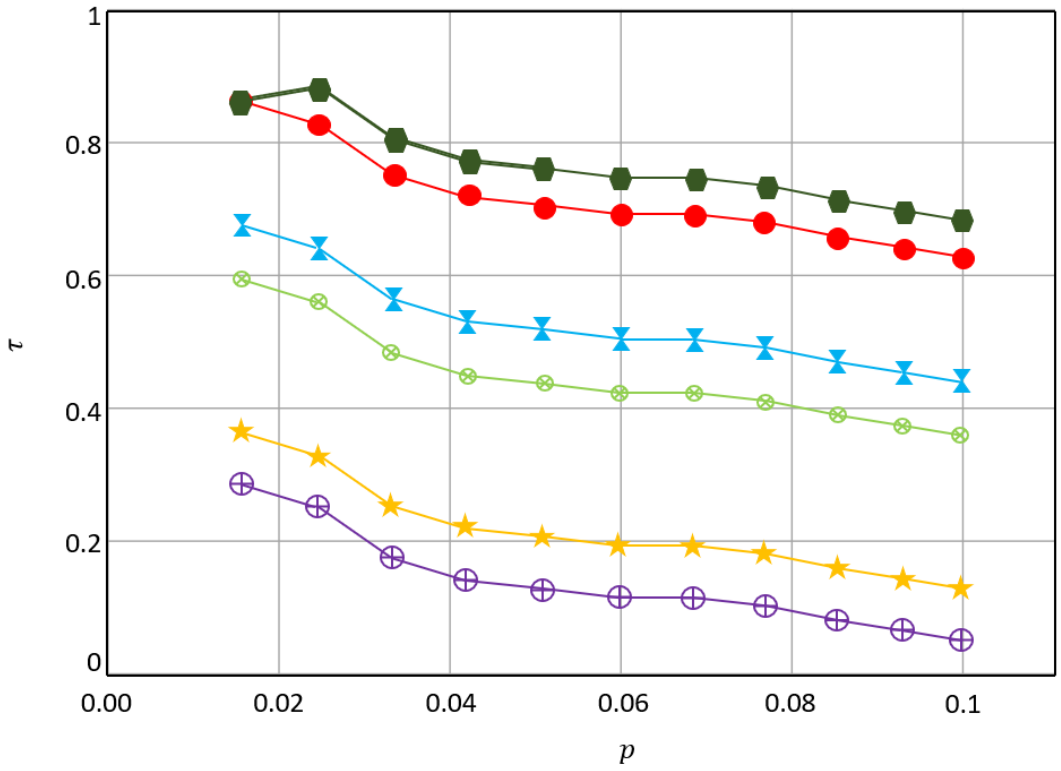
Для того, щоб перевірити кореляцію між NiR та результатами моделювання для всіх сімейств мереж, використаних для аналізу було проведено експерименти.

Моделювання проводилось на декількох мережах з використанням моделей SI та SIR. Базовим значенням для моделі SI є час t, необхідний для часткового (50% або 70% вузлів) інфікування у випадку одного вузла-джерела *i*. Для моделі SIR значенням, яке використовується для порівняння, є розмір спалаху (загальна кількість вузлів, які заразилися) після *t* часових кроків виконання. Результати, отримані за допомогою моделювання для кожного з вузлів, порівнюються з NiR та п'ятьма іншими мірами центральності (міжцентровість, центральність, ступінь, динамічна чутлива центральність (DS) та центральність за H-індексом). Показник NiR демонструє високу кореляцію з результатами моделювання разом з низькою дисперсією, часто перевершуючи всі п'ять показників як у моделях SI, так і SIR. Єдиним показником, який показує однакові результати, є динамічна чутлива центральність DS, параметри якого залежать від динаміки поширення загроз.

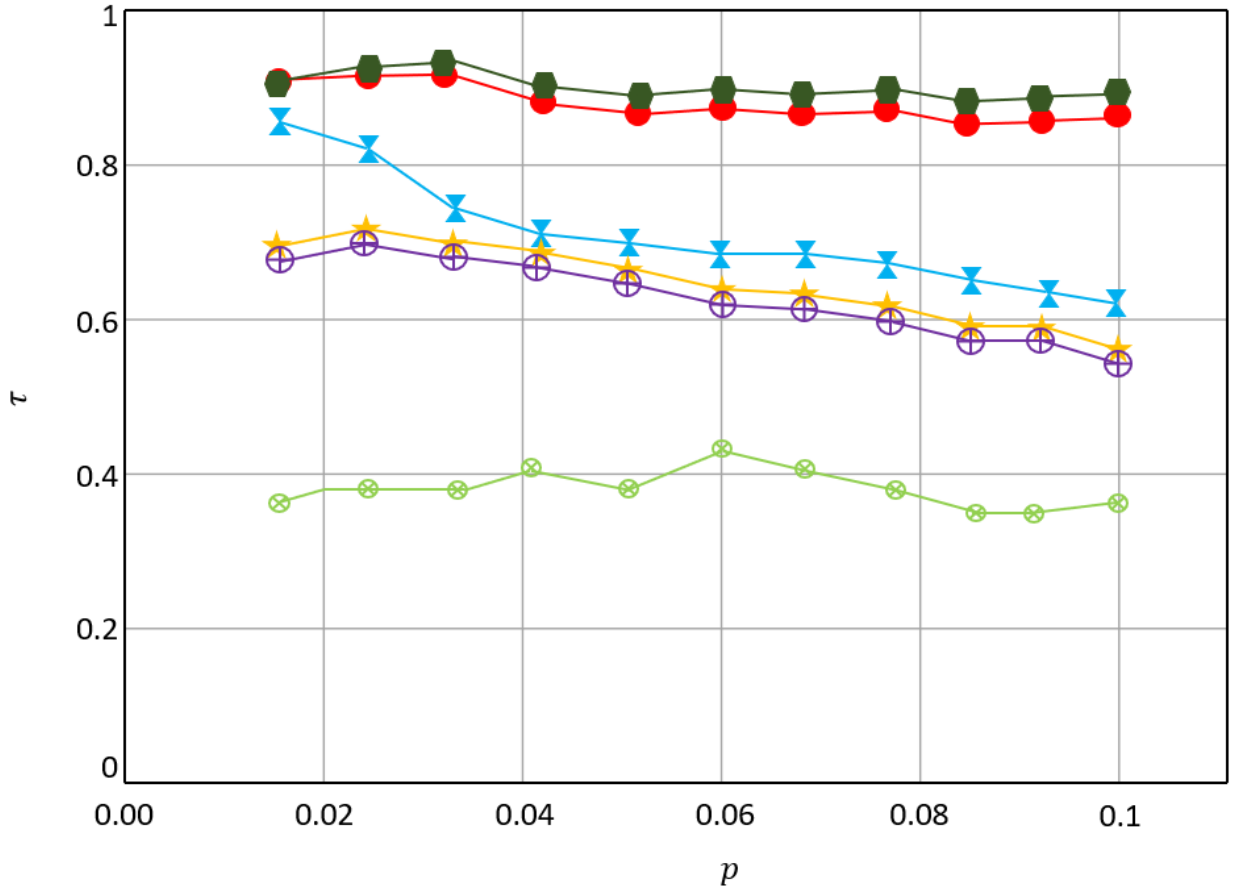
У випадку великих мереж буде велика частка вузлів з дуже схожим потенціалом поширення, тому додаткова різниця в центральності буде незначною.

Тому виправдано взяти репрезентативну вибірку вузлів і використовувати їх для аналізу. Як показано на рисунку 4.3 NiR демонструє гарні результати обох мережах для обох моделей поширення, явно перевершуючи показники ступінь (degree), H-індекс (h-index), центральність ядра (coreneess) та динамічну чутливу центральність (DS centrality).

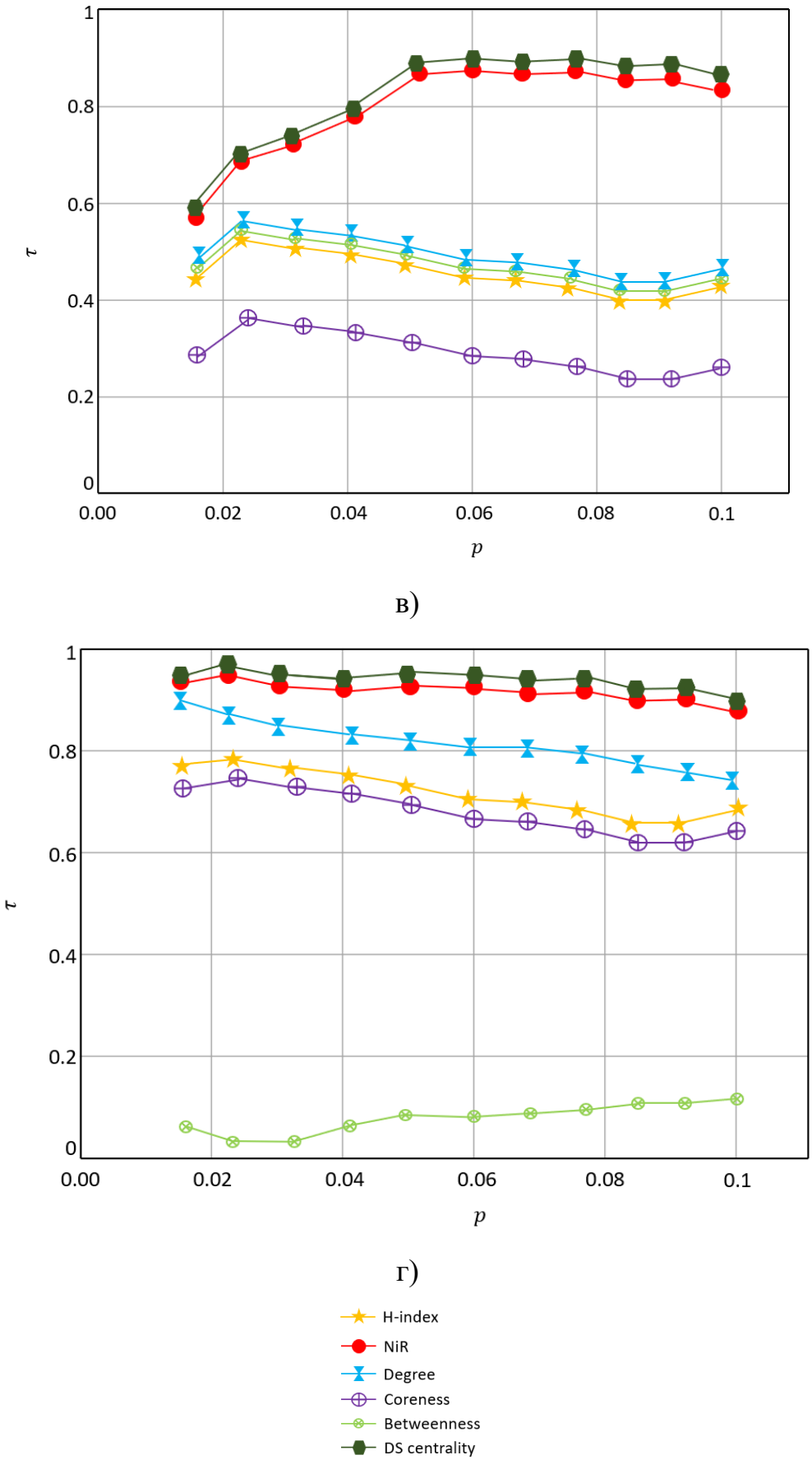
Для моделі SI NiR працює так само добре, як і DS centrality, навіть незважаючи на те, що він не використовує жодних додаткових параметрів з моделі поширення. Очевидно, що кореляція між змодельованою динамікою та показниками centrality падає зі збільшенням p. Це свідчить про те, що оцінка потенціалу поширення вузла для великої ймовірності передачі стає складнішою.


1
0.8
0.6
0.4
0.2
0
τ
0.00
0.02
0.04
0.06
0.08
0.1
p

а)


1
0.8
0.6
0.4
0.2
0
τ
0.00
0.02
0.04
0.06
0.08
0.1
p

б)



в)

г)

Рисунок 4.3 – Кореляція між NiR та результатами моделювання для сімейств мереж

Епідемічна модель SI (Susceptible-Infected). Модель SI розрізняє два можливих стани вузлів: а) сприйнятливі до інфекції та б) вже інфіковані і здатні поширювати інфекцію. У моделі SI можливий перехід від а) до б), але не навпаки. Епідемічний процес починається з частини початково інфікованих вузлів. Всі сусідні вузли вважаються сприйнятливими. На кожному часовому кроці заражений вузол намагається передати інфекцію всім своїм сприйнятливим сусідам незалежно зі значенням швидкості передачі p. Для здорового (неінфікованого) вузла i з k зараженими сусідами ймовірність інфікування на кожному часовому кроці дорівнює $p_i = 1 - (1 - p)^k$. Коли сприйнятливий вузол заражається, він залишається в цьому стані на невизначений час і може поширювати інфекцію далі. Процес інфікування у зв'язному графі врешті-решт вплине на всю мережу до тих пір, поки всі вузли не змінять свій стан з сприйнятливого на інфікований стан. уло змодельовано інфекцію SI, яка походить з одного вузла, що належить до набору вибраних вузлів. Потім було виміряно час t у вигляді кількості кроків, необхідних для інфікування 50% всіх вузлів. Процес розповсюдження повторюється більше 300 разів для кожного з обраних вузлів як джерела.

Середній час t використовується як базовий орієнтир. Потім порівнюються значення NiR для одного і того ж набору вибраних вузлів і вимірюється кореляція. Той самий процес повторюється для 100 різних мереж, отриманих з кожного сімейства мереж.

Модель епідемії SIR (Susceptible-Infected-Recovered - сприйнятливий-інфікований-вилікуваний). У моделі SIR кожен вузол може перебувати в одному з трьох станів: а) сприйнятливий до інфекції, б) вже інфікований і здатний поширювати інфекцію, в) одужав (видалений) і не здатний інфікувати інші вузли. Перехід стану є односпрямованим від а) до б) до в), а не навпаки.

Епідемічний процес починається з частини початково інфікованих вузлів. Всі сусідні вузли вважаються сприйнятливими. На кожному часовому кроці інфікований вузол намагається передати інфекцію всім своїм сприйнятливим сусідам незалежно зі швидкістю передачі p.

Одночасно всі вже інфіковані вузли одужують від інфекції зі швидкістю одужання μ. Для здорового (неінфікованого) вузла i з k інфікованими сусідами ймовірність інфікування на наступному часовому кроці становить $p_i = 1-(1-p)^k$. В той же час, ймовірність одужання залишається однаковою незалежно від оточення вузла. Було змодельовано SIR-інфекцію, яка виникає в одному вузлі, що належить до набору вибраних вузлів.

Швидкість відновлення вважається рівною $\mu = 1$, що передбачає, що всі вузли, інфіковані на часовому кроці t, будуть відновлені через $t + 1$.

Результати проведених досліджень повинні бути дуже схожими для інших значень μ.

Еталонним значенням є розмір спалаху n_{inf} (кількість інфікованих вузлів) після t часових кроків.

4.2 Мережеві дані для дослідження

У експериментальних дослідження було синтезовано два типи комп'ютерних мереж. Чотири мережі було синтезовано для великих та малих мереж відповідно. Вузли стовпця представляють кількість вузлів у вихідній мережі.

Діаметр стовпців, щільність і кластерний коефіцієнт представляють середні значення, розраховані з набору вибіркових мереж. Середній ступінь однаковий як для оригінальної, так і для вибіркової мережі.

Перший тип - це безмасштабні мережі та мережі малого світу, побудовані випадковим чином з використанням різних параметрів.

Безмасштабні мережі було синтезовано на основі моделі [43] з використанням алгоритму, описаного в [84] та реалізованого в MATLAB.

Перша група безмасштабних мереж має мінімальний ступінь вузлів 1, тоді як друга група має мінімальний ступінь вузлів 2. Ці параметри впливають на діаметр і щільність мереж, а отже, на очікувану динаміку процесів розповсюдження загроз в мережі.

Аналогічно, мережі малого світу будуються за допомогою MATLAB з використанням моделі, описаної в [40].

Синтезовано модель базується на двох параметрах, які визначають кількість найближчих сусідів для з'єднання (k) та ймовірність додавання короткого шляху в даному рядку (p_s). Перша група згенерованих малих світових мереж має $k = 1$ і $p_s = 0.5$, тоді як друга група має $k = 2$ і $p_s = 0.5$.

Різноманітність початкових параметрів забезпечує синтез комп'ютерних мереж з різними властивостями, такими як діаметр, щільність або середній ступінь. Отже, випадково синтезовані для здійснення експериментів топології комп'ютерних мереж є зв'язними, неорієнтованими і складаються з 6000 вузлів кожна.

Синтезовані комп'ютерні мережі в другій групі отримані з великих реальних мережевих даних.

Для кожної з реальних мереж було згенеровано 20 вибіркових мереж з 1000 вузлів кожна. Для кожної з випадкових реалізацій топології ми вимірюємо кореляцію динамічних і спостережуваних мір поширення SI і SIR.

Змодельовані мережі генеруються шляхом рівномірної випадкової вибірки 1000 вузлів з оригінальної мережі без повторень.

Потім з вибірки витягується степенева послідовність.

З отриманої послідовності ступенів будуються мережі за допомогою алгоритму Гавела-Хакімі, де моделювання виконувалося для найбільшої зв'язної компоненти в кожній із синтезованих комп'ютерних мереж. Побудова графа з послідовності ступенів зберігає розподіл ступенів вихідної синтезованої комп'ютерної мережі.

Деякі характеристики мережі, такі як спільноти, втрачаються під час цього процесу.

Однак, відносний розмір згенерованих графів у будь-якому випадку перешкоджає відтворенню структур спільнот [85]. Для типу динаміки, що моделюється тут на незважених неорієнтованих мережах, деякі інші

характеристики, такі як витрати, обмеження та напрямок на ребрах, не мають значення і тому ігноруювалися.

Важливість вузла зазвичай характеризується деякими з численних мір центральності. Наступним кроком здійснення екмпериментальних досліджень було здійснено порівняння запропонованого метод, що залучає показник NiR з найпоширенішими показниками центральності: ступінь (degree), H-індекс (h-index), центральність ядра (coreneess) та динамічна чутлива центральність (DS centrality).

Крім того, всі синтезовані комп’ютерні мережі, що використовувалися в експериментах, характеризувалися різними масивами наборів глобальних властивостей.

4.3 Застосування методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі

Для апробації основних положень методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі було проведено дослідження з синтезованими мережами, у яких було здійснено множину дій над топологією мережі для того, щоб пом'якшити вплив відмови частини вузлів.

Ці стратегії є безвитратними, оскільки вони не вимагають значних інвестицій в мережеву інфраструктуру в мережеву інфраструктуру, наприклад, у додаткові лінії зв'язку або збільшення пропускної здатності. Однак, вони вимагають впровадження деяких заходів, які можуть дозволити мережі захистити себе за допомогою активних засобів. Активна зміна топології в даному випадку розглядається навмисне видалення певних вузлів з метою зупинки каскаду або мінімізувати наслідки збою.

В роботі було залучено стратегію навмисного видалення частини вузлів після початкової відмови, незалежно від фактичного положення вузла.

З цією метою було синтезовано мережі з неоднорідним розподілом навантажень, яка потенційно схильна до каскадних збоїв.

Каскад в мережі було поділено на дві основні стадії: (1) початкова атака, коли частина вузлів виходить з ладу, і (2) фаза розповсюдження, коли подальші відмови відбуваються через перевантаження.

Фаза розповсюдження відбувалася в численних часових інтервалах, поки навантаження всіх вузлів мережі, що залишилися, не стане меншим за їхню пропускну спроможність. Розмір каскаду вимірюється як відношення $G = K'/K$, де K і K' — розміри найбільшого підключеного компонента до і після каскаду відповідно. Механізм захисту відбувається після фази (1), але перед фазою (2).

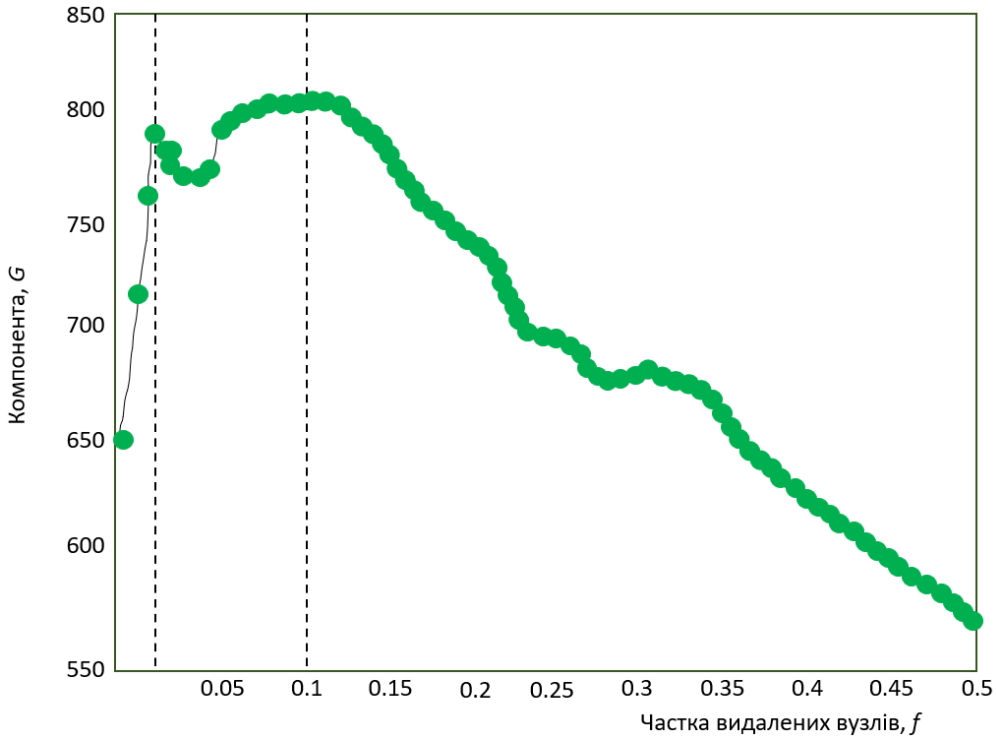
Було зроблено припущення, що єдиною операцією, дозволеною після атаки і перед більшим каскадом, є навмисне видалення вузлів або ребер. Навмисне видалення (НВ) ретельно вибраних вузлів може зменшити каскад. Вузли, обрані для видалення, повинні мати відносно невелике навантаження. Обґрунтуванням цього припущення є те, що вузли в мережі вносять однаковий внесок у навантаження трафіку, але не є однаково перевантаженими.

Таким чином, видалення вузлів з невеликим навантаженням зменшить загальний трафік без необхідності подальшого розподілу навантаження. Навмисне видалення вузлів з малим навантаженням не є простим процесом, оскільки саме видалення негативно впливає на розмір гігантського компонента.

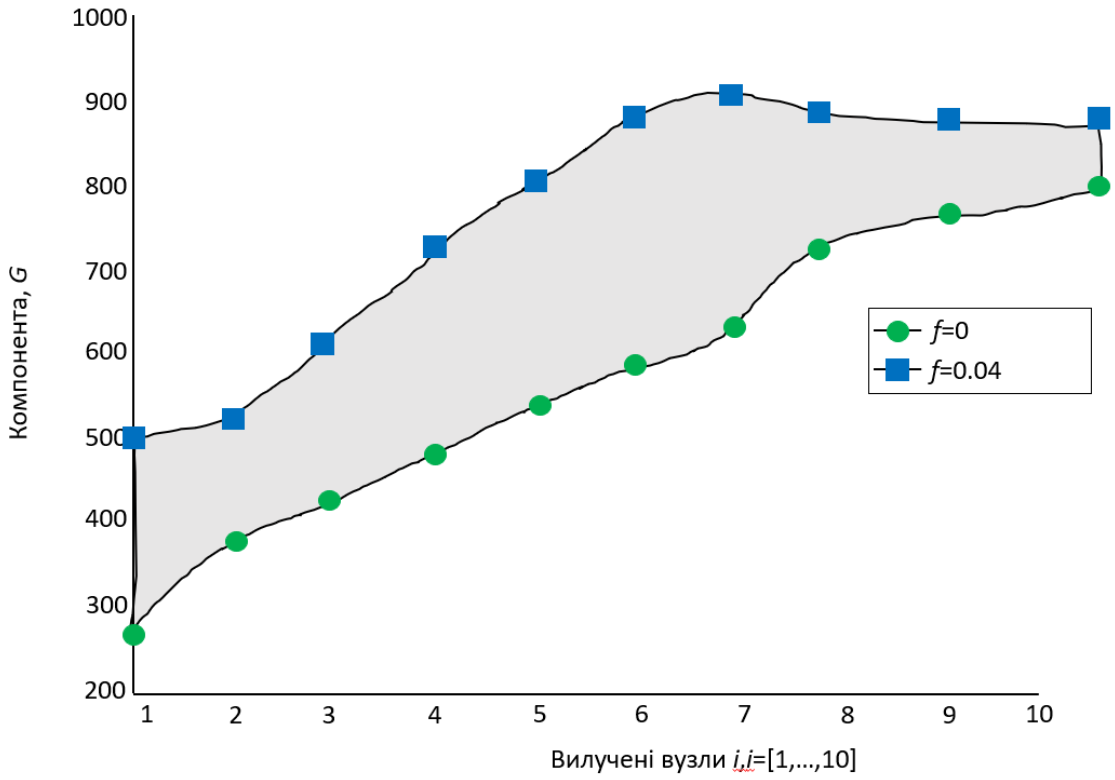
НВ повинен бути ретельно обмежений певною кількістю вузлів, щоб придушити каскад, а гігантський компонент, що залишився, залишався відносно великим. Для випадкової безмасштабної мережі з випадковою атакою на 0,1% вузлів оптимальною часткою НВ-вузлів є $f \approx 0{,}4$ [71]. Однак, для цілеспрямованої атаки на КМ моделювання показує, що частка видалених вузлів може бути набагато меншою, $0{,}02 \leq f \leq 0{,}1$.

На рисунку 4.4 розмір компонента G, що залишився, показано як функцію частки f видалених вузлів з малим навантаженням. Вузли були \видалені після початкової атаки таким чином, що вузли з меншим навантаженням видаляються першими. Після первинної атаки на критичний вузол проводяться захисні заходи. Частка f найменш завантажених вузлів, які видалено, щоб пом'якшити каскадний збій. На рисунку 4.4(а) показано зміну розміру найбільшого компонента зв’язності

G, що залишився після каскаду, як функцію f. Максимальна G досягається для 0:02 f 0:1. Для значень f більше 0,1 вплив навмисного видалення починає негативно впливати на результуючу G. Отриманий графік усереднюється для десяти найбільш критичних вузлів у межах мережі. Рисунок 4.4(б) показує ефект захисних заходів для f = 0.04. Для кожного видаленого критичного вузла і захисний механізм утримує решту G вище. Різниця між двома відповідними точками на двох ділянках є мірою ефективності захисту. Усі очікувані значення G для 0 < f < 0.04, швидше за все, можна знайти в заштрихованій області.



а)



б)

Рисунок 4.4. - Ефект вибіркового видалення фракції найменш навантажених вузлів.

Моделювання проводилося для набору з десяти найбільш критичних вузлів синтезованої комп'ютерної мережі, і було побудовано середнє значення *G*. Видалення лише 2% найменш навантажених вузлів здатне різко зменшити каскад. Від 2% до 10% розмір гігантської складової суттєво не змінюється. Однак, після порогу в 10%, *G* починає лінійно падати. Це означає, що подальше видалення вузлів не додає захисту мережі, але негативно впливає на розмір гігантської складової. Аналіз не проводиться для випадкових відмов і не усереднюється по всіх вузлах мережі. Основна увага приділяється набору критичних вузлів, тобто тих, виведення з ладу яких може спричинити найбільшу шкоду.

У випадку відмови критичного вузла, будь-яка частка між 0,02 до 0,1 найменш навантажених вузлів може бути вилучена, щоб запобігти подальшого каскадування. На рисунку 4.4б показано порівняння розміру компоненти після каскаду з заходами захисту та без них для десяти найбільш критичних вузлів. Частка видалених вузлів після початкової атаки була обрана такою $f = 0.04$. Для

кожного критичного вузла і каскад пом'якшується таким чином, що результуюче значення *G* завжди більше, якщо захисні заходи реалізовано належним чином.

Ідея полягає в тому, щоб визначити набір вузлів, які слід підготувати до вилучення у випадку найнебезпечніших відмов. Відмова одного з десяти найбільш критичних вузлів з Таблиці 4.1 спричинить найбільшу негативний вплив на функціонування КМ. Тому проводиться наступний аналіз: Для кожного з найбільш критичних вузлів моделюється відмова і вибираються найменш навантажені вузли.

Саме ці вузли є кандидатами на навмисне видалення після початкової атаки. Певна кількість вузлів часто з'являється у списку кандидатів на різні відмови і. Це ті вузли, які, швидше за все, матимуть менше навантаження у випадку навмисної атаки. Механізм захисту повинен видалити частку f з усіх вузлів, крім вузлів-кандидатів. В абсолютних числах кількість вершин, які будуть навмисно видалені, становить $23 \leq n_{ir} \leq 115$.

Особа, яка приймає рішення, вільна у виборі вершин, які вона буде видаляти з множини вершин-кандидатів. Не має значення, яку саме вершину буде видалено, доки число n_{ir} не виходить за межі.

Таблиця 4.1 - Вплив видалення вузлів з синтезованої мережі

№ вузла мережі	$G_{\alpha=1.01}$	$G_{\alpha=1.10}$	$G_{\alpha=1.30}$	$G_{\alpha=1.50}$
10	0.312	0.230	0.310	0.409
19	0.289	0.348	0.528	0.542
42	0,439	0.467	0.455	0.387
12	0.458	0.492	0.912	0.915
41	0.532	0.485	0.676	0.687
13	0.562	0.611	0.908	0.932
18	0.598	0.612	0.965	0.9247
44	0.524	0.612	0.641	0.634
43	0.834	0.865	0.898	0.887
46	0.271	0.614	0.626	0.729

4.4 Висновки

З метою здійснення апробації та перевірки ефективності запропонованого методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі було здійсненого ряд експериментальних досліджень.

У експериментальних дослідження було синтезовано два типи комп’ютерних мереж. Чотири мережі було синтезовано для великих та малих мереж відповідно. Вузли стовпця представляють кількість вузлів у вихідній мережі. Для апробації основних положень методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі було проведено дослідження з синтезованими мережами, у яких було здійснено множину дій над топологією мережі для того, щоб пом'якшити вплив відмови частини вузлів.

Результати досліджень показали, що застосування синтезованих апаратно-програмних засобів уможливлюють забезпечення стійкості корпоративної комп’ютерної мережі в умовах здійснення загроз.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено набув подальшого розвитку метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі, який на відміну від відомих враховує усі характеристики стійкості і який забезпечує її підвищення, а також набули подальшого розвитку програмно-технічні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

У першому розділі досліджено методи забезпечення стійкості корпоративної комп'ютерної мережі; а також проаналізовано сучасні програмно-технічних засоби забезпечення стійкості корпоративної комп'ютерної мережі.

У другому розділі представлено опис моделювання комп'ютерних мереж, зокрема описано методи моделювання, аналізу мереж в моменти здійснення загроз. В розділі також подано опис застосування метаевристики для моделювання стійкості комп'ютерної мережі. Описано отримання ациклічних графів при моделювання стійкості комп'ютерних мереж. Розглянуто методи проєктування стійких комп'ютерних мереж, а також подано аналітичний підхід у моделюванні складних мереж, зокрема моделювання епідемій у некерованій мережі за допомогою ланцюга Маркова, моделювання епідемій в мережах з використанням системного підходу LTI, а також чисельний підхід вирішення задачі моделювання стійкості комп'ютерної мережі.

У третьому розділі запропоновано метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Для вирішення задачі метод передбачає залучення теорії лінійних стаціонарних систем, та використання метрики NiR, яка може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі. Було здійснено апробацію методу шляхом моделювання, результати якого показують високу кореляцію з фактичною динамікою поширення, змодельованою за допомогою процесів SI та SIR. NiR також показує невелику дисперсію, що означає його надійність для різних топологій

комп’ютерних мереж. Було виявлено, що вибравши декілька вхідних точок, можна оцінити вплив багатьох вузлів мережі, якщо вони будуть збуджені одночасно. Крім того, вибір декількох вихідних точок дасть змогу оцінити вплив цих вузлів у разі поширення процесу. Більш вразливі вузли з більшою ймовірністю будуть досягнуті з набору обраних вхідних вузлів. Аналіз не обмежується незваженими мережами. Також метод передбачає знаходження найбільш критичних вузлів в комп’ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

У четвертому розділі описано апробацію та перевірку ефективності запропонованого методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі було здійсненого ряд експериментальних досліджень.

У експериментальних дослідження було синтезовано два типи комп’ютерних мереж. Чотири мережі було синтезовано для великих та малих мереж відповідно. Вузли стовпця представляють кількість вузлів у вихідній мережі. Для апробації основних положень методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп’ютерної мережі було проведено дослідження з синтезованими мережами, у яких було здійснено множину дій над топологією мережі для того, щоб пом'якшити вплив відмови частини вузлів.

Результати досліджень показали, що застосування синтезованих апаратно-програмних засобів забезпечили стійкість корпоративної комп’ютерної мережі в умовах здійснення загроз.

За темою кваліфікаційної роботи магістра опублікована одна стаття у фаховому науковому виданні в фаховому журналі «Вісник Хмельницького національного університету» №2 за 2023 рік [1].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Лисенко С.М., Сахнюк В.В., Бондарук О.В. Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. *Вісник Хмельницького національного університету.* 2023.№3.

2. Nicol D.M., Sanders W.H. Trivedi K.S. Model-based evaluation: from dependability to security. *IEEE Trans. Dependable and Secure Comput.* 2017.1.1., 48–65.

3. Neumayer S., Zussman G., Cohen, R., Modiano E. Assessing the vulnerability of the fiber infrastructure to disasters. *IEEE/ACM Trans. Networking*. 2011. 19.6., 1610–1623.

4. Mukherjee B. Optical WDM Networks. Springer, New York. 2016.

5. Mukherjee B., Habib M.F., Dikbiyik, F. Network adaptability from disaster disruptions and cascading failures. *IEEE Commun. Mag.* 2014.52.5., 230–238.

6. Molisz, W., Rak, J.: Region protection/restoration scheme in survivable networks. *Lect. Notes Comput. Sci.* 2009.3685, 442–447.

7. Misseri, X., Gojmerac, I., Rougier, J.-L.: IDRD: enabling inter-domain route diversity. *Proc. IEEE International Conference on Communications .IEEE ICC'13.*, 2013. pp. 3536–3541.

8. Mingsen X., Wen-Zhan S., Deukhyoun H., Jong-Hoon K., Byeong-Sam, K. ECPC: preserve downtime data persistence in disruptive sensor networks. *In: Proc. IEEE Mobile Ad-Hoc and Sensor Systems .MASS'13.,* 2013. pp. 281–289.

9. Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y. General resilience: taxonomy and strategies. *Proc. 2014 International Conference and Utility Exhibition on Green Energ for Sustainable Development .ICUE'14.,* 2014. pp. 1–8.

10. Kompella K., Swallow G.: Detecting Multi-Protocol Label Switched .MPLS. Data Plane Failures, 2016. IETF RFC 4379.

11. Kodian A., Grover W.D. Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection. IEEE/OSA J. *Lightwave Technol.* 2015. 23.10., 3241–3259.

12. Kitamura Y., Lee, Y., Sakiyama, R., Okamura, K.: Experience with restoration of Asia Pacific network failures from Taiwan earthquake. *IEICE Trans. Commun.* E90-B.11., 2017. 3095–3103.

13. Jaumard, B., Rocha, C., Baloukov, D., Grover, W.D. A column generation approach fordesign of networks using path-protecting p-cycles. *Proc. 6th International Workshop on Design of Reliable Communication Networks .DRCN'07.*, 2017. pp. 1–8.

14. Ho, P.-H.: State of the art progress in developing survivable routing schemes in mesh WDM networks. *IEEE Commun. Surv. Tutorials* . 6.4., 2014. 2–16.

15. Ho, P.-H., Tapolcai, J., Mouftah, H. On achieving optimal survivable routing for shared protection in survivable Next-Generation Internet. *IEEE Trans. Reliab.* 2014. 53.2., 216–225.

16. Ho, P.-H., Tapolcai, J., Cinkler, T. Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels. *IEEE/ACM Trans. Networking* 12.6., 2022. 1105–1118.

17. Haider, A., Harris, R. Recovery techniques in Next Generation Networks. *IEEE Commun. Surv. Tutorials.* 2014 9.3., 2–17.

18. H. Aissi and D. Vanderpooten. Robust capacity expansion of a network under demand uncertainty: A bi-objective approach, *Networks.* 68. 2016, 185–199.

19. Grover, W.D. Mesh-based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Prentice Hall PTR, Upper Saddle River .2014. Grover, W.D.: The protected working capacity envelope concept: an alternate paradigm for automated service provisioning. IEEE Commun. Mag. 42.1., 62–69 .2014.

20. Grover, W.D., Shen, G.: Extending the p-cycle concept to path-segment protection. *In: Proc. IEEE International Conference on Communications*, 2, 2013. pp. 1314–1319.

21. Geva, M., Herzberg, A., Gev, Y.: Bandwidth Distributed Denial of Service: attacks and defences. *IEEE Secur. Priv.* 12.1., 54–61 .2014.

22. Fangming, L., Bo, L., Lili, Z., Baochun, L., Hai, J., Xiaofei, L.: Flash crowd in P2P livestreaming systems: fundamental characteristics and design implications. IEEE Trans. Parallel. *Distrib. Syst.* 23.7., 1227–1239 . 2012.

23. Cucurull, J., Asplund, M., Nadjm-Tehrani, S., Santoro, T.: Surviving attacks in challenged networks. IEEE Trans. Dependable and Secure Comput. 2015. 9.6., 917–929.

24. Colle, D., De Maesschalck, S., Develder, C., Van Heuven, P., Groebbens, A., Cheyns, J., Lievens, U., Pickavet, M., Lagasse, P., Demeester, P.: Data-centric optical networks and their survivability. IEEE J. Sel. Areas Commun. 2012. 20.1., 6–20.

25. Cetinkaya, E.K., Sterbenz, J.P.G.: A taxonomy of network challenges. In: Proc. 9th International Conference on Design of Reliable Communication Networks. 2013. pp. 322–330.

26. Caini, C., Cruickshank, H., Farrell, S., Marchese, M.: Delay- and disruption-tolerant networking .DTN.: an alternative solution for future satellite networking applications. *Proc. IEEE* 2021. 99.11.

27. Avizienis, A., Laprie, J.-C., Randell, B.: Dependability and its threats: a taxonomy. *In: Jacquart, R. .ed.. Building the information society,* vol. 156, IFIP International Federation for Information Processing, 2004. pp. 91–120. Springer, New York.

28. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable and Secure Comput.* 2014 . 1.1., 11–33.

29. Asthana, R., Singh, Y.N., Grover, *W.: p-cycles: an overview. IEEE Commun. Surv. Tutorials.* 2013.12.1., 97–111.

30. Agarwal, P.K., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. In: Proc. *30th Annual Joint Conference of the IEEE Computer and Communications Societies .IEEE INFOCOM'11.*, 2013. pp. 1521–1529.

31. D.L. Alderson, G.G. Brown, and W.M. Carlyle, Assessing and improving operational resilience of critical infrastructures and other systems, Tutorials in Operations Research: Bridging Data and Decisions, A. Newman and J. Leung .eds., Institute for Operations Research and Management Science, Hanover, MD, 2014, pp. 180–215.

32. D.L. Alderson, G. Brown, W.M. Carlyle, and R.K. Wood, Assessing and

improving the operational resilience of a large highway infrastructure system to worst-case losses, *Transp. Sci.* 52 .2017., 1012–1034.

33. N. Alguacil, A. Delgadillo, and J.M. Arroyo, A trilevel programming approach for electric grid defense planning, *Comput. Oper. Res.* 41 .2014., 282–290.

34. M.L. Ali, P.-H. Ho, and J. Tapolcai, SRLG failure localization using nested m-trails and their application to adaptive probing, Networks 66 .2015., 347–363.

35. E. Álvarez-Miranda and J. Pereira, Designing and constructing networks under uncertainty in the construction stage: Definition and exact algorithmic approach, *Comput. Oper. Res.* 81 .2017., 178–191.

36. J. Anderies, C. Folke, B. Walker, and E. Ostrom, Aligning key concepts for global change policy: Robustness, resilience, and sustainability, *Ecol. Soc*. 18 .2013., 8.

37. A. Arab, A. Khodaei, Z. Han, and S.K. Khator, Proactive recovery of electric power assets for resiliency enhancement, *IEEE Access*. 3 .2015., 99–109.

38. A. Arab, A. Khodaei, S.K. Khator, and Z. Han, Electric power grid restoration considering disaster economics, I*EEE Access* .4 .2016., 639–649.

39. A. Arulselvan, A. Bley, and I. Ljubi´c, The incremental connected facility location problem, *Comput. Oper. Res. 1*12 .2019., 104763.

40. E. Aslan and M. Çelik, Pre-positioning of relief items under road/facility vulnerability with concurrent restoration and relief transportation, *IISE Trans.* 51 .2019., 847–868.

41. A. Atamturk and A. Bhardwaj, Network design with probabilistic capacities, *Networks* .71 .2018., 16–30.

42. A. Atamturk and M. Zhang, Two-stage robust network flow and design under demand uncertainty, *Oper. Res*. 55 .2007., 662–673.

43. I. Averbakh, Minimizing the makespan in multiserver network restoration problems, *Networks* 70 .2017., 60–68.

44. I. Averbakh and J. Pereira, Network construction problems with due dates, Eur. J. *Oper. Res.* 244 .2015., 715–729.

45. I. Averbakh and J. Pereira, Lateness minimization in pairwise connectivity restoration problems, *INFORMS J. Comput.* 30 .2018., 522–538.

46. A. Balakrishnan, M. Banciu, K. Glowacka, and P. Mirchandani, Hierarchical approach for survivable network design, *Eur. J. Oper. Res.* 225. 2013, 223–235.

47. S. Bao, C. Zhang, M. Ouyang, and L. Miao, An integrated tri-level model for enhancing the resilience of facilities against intentional attacks, *Ann. Oper. Res.* 283 . 2019., 87–117.

48. F. Barbosa, A. de Sousa, and A. Agra, Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes, *Networks* . 75 .2020., 356–373.

49. M. Baxter, T. Elgindy, T.A. Ernst, T. Kalinowski, and M.W.P. Savelsbergh, Incremental network design with shortest paths, *Eur. J. Oper. Res.* 238 .2014., 675–684.

50. N.O. Baycik and T.C. Sharkey, Interdiction-based approaches to identify damage in disrupted critical infrastructures with dependencies, *J. Infrastruct. Syst.* 25 .2019., 04019013.

51. N.O. Baycik and K.M. Sullivan, Robust location of hidden interdictions on a shortest path network, *IISE Trans.* 51 .2019., 1332–1347.

52. N.O. Baycik, T.C. Sharkey, and C. Rainwater, Interdicting layered physical and information flow networks, *IISE Trans.* 50 .2018., 316–331.

53. H. Bayrak and M.D. Bailey, Shortest path network interdiction with asymmetric information, *Networks* . 52 .2008., 133–140.

54. D. Bienstock, Electrical Transmission System Cascades and Vulnerability: An Operations Research Viewpoint, SIAM-MOS, Philadelphia, PA, 2016.

55. J.S. Borrero, O.A. Prokopyev, and D. Saure, Sequential shortest path interdiction with incomplete information, *Decis. Anal.* 13 .2015., 68–98.

56. J.S. Borrero, O.A. Prokopyev, and D. Saure, Sequential interdiction with incomplete information and learning, *Oper. Res.* 67 .2019., 72–89.

57. Q. Botton, B. Fortz, L. Gouveia, and M. Poss, Benders decomposition for the Hop-constrained survivable network design problem, *INFORMS J. Comput.* 25 .2013., 13–26.

58. Q. Botton, B. Fortz, and L. Gouveia, On the Hop-constrained survivable network design problem with reliable edges, *Comput. Oper. Res.* 64. 2015, 159–167.

59. C. Busing, A. Grub, A.M.C.A. Koster, W. Laube, M. Tieves. Robust spectrum allocation in elastic flexgrid optical networks: *Complexity and formulations, Networks* . 70. 2017, 342–359.

60. M. Bynum, A. Staid, B. Arguello, A. Castillo, J.-P. Watson, and C.D. Laird, Proactive operations and investment planning via stochastic optimization to enhance power systems extreme weather resilience, *Optim. Online Repos.* .2018.

61. E. Canale, H. Cancela, F. Robledo, P. Romero, and P. Sartor, Diameter constrained reliability: Complexity, distinguished topologies and asymptotic behavior, Networks 66 .2015., 296–305.

62. E. Canale, P. Romero, and G. Rubino, Factorization and exact evaluation of the source-terminal diameter-constrained reliability, Networks 70 .2017., 283–291.

63. J.M. Carlson and J. Doyle, Highly optimized tolerance: Robustness and design in complex systems, *Phys. Rev. Lett.* 84 .2020., 2529–2532.

64. A. Castillo, T. Nakashima-Paniagua, and J. Doucette, Dual-failure restorability analysis of span-restorable meta-mesh networks, *Networks* . 75 .2020., 405–419.

65. B. Cavdaroglu, E. Hammel, J.E. Mitchell, T.C. Sharkey, and W.A. Wallace, Integrating restoration and scheduling decisions for disrupted interdependent infrastructure systems, *Ann. Oper. Res.* 203 .2013., 279–294.

66. M. Çelik, Network restoration and recovery in humanitarian operations: Framework, literature review, and research directions, *Surv. Oper. Res. Manage. Sci.* 21. 2016., 47–61.

67. M. Çelik, O. Ergun, and P. Keskinocak, The post-disaster debris clearance problem under incomplete information, *Oper. Res*. 63. 2015, 65–85.

68. Y. Cheng, D. Medhi, and J.P.G. Sterbenz, Geodiverse routing with path delay and skew requirement under area-based challenges, *Networks* 66. 2015, 335–346.

69. T.G. Crainic, X. Fu, M. Gendreau, W. Rei, and S.W. Wallace, Progressive hedging-based metaheuristics for stochastic network design, *Networks* 58. 2011, 114–124.

70. C.A. Cullenbine, R.K. Wood, and A.M. Newman, Theoretical and

computational advances for network diversion, *Networks* 62. 2013, 225–242.

71. V. Dakos, S.R. Carpenter, E.H. van Nes, and M. Scheffer, Resilience indicators: Prospects and limitations for early warnings of regime shifts, *Philos. Trans. R. Soc. B: Biol. Sci.* 370. 2015, 20130263.

72. V. Diarrassouba, A.R. Gabrel, L.G. Mahjoub, and P. Pesneau, Integer programming formulations for the k-edge-connected 3-Hop-constrained network design problem, *Networks* 67. 2016, 148–169.

73. T. Ding, C. Li, C. Yan, F. Li, and Z. Bie, A bilevel optimization model for risk assessment and contingency ranking in transmission system reliability evaluation, *IEEE Trans. Power Syst.* 2017. 32, 3803–3813.

74. T. Ding, L. Yao, and F. Li, A multi-uncertainty-set based two-stage robust optimization to defender-attacker-defender model for power system protection, *Reliab. Eng. Syst. Saf.* 2018. 169, 179–186.

75. J.C. Doyle and M. Csete, Rules of engagement, *Nature* 446. 2007, 860.

76. J.C. Doyle and M. Csete, Architecture, constraints, and behavior, Proc. Natl. Acad. Sci. U. S. A. 108 .2011., 15624–15630.

77. D.A. Eisenberg, How to think about resilient infrastructure systems, Ph.D. thesis, Arizona State University, 2018.

78. D.A. Eisenberg, D.L. Alderson, M. Kitsak, A. Ganin, and I. Linkov, Network foundation for command and control .C2. systems: Literature review, *IEEE Access* . 6 .2018., 68782–68794.

79. D.A. Eisenberg, T.P. Seager, and D.L. Alderson, Rethinking resilience analytics, *Risk Anal.* 2019. 39, 1870–1884.

80. K. Engel, T. Kalinowski, and M.W.P. Savelsbergh, Incremental network design with minimum spanning trees, J. *Graph Algorithms Appl.* 21. 2017, 417–432.

81. Lü, Linyuan & Zhou, Tao & Zhang, Qian-Ming & Stanley, H. The H-index of a network node and its relation to degree and coreness. *Nature Communications.* 2016. 7. 10168. 10.1038/ncomms10168.

82. Zhu, X. et al. Roles of degree, H-index and coreness in link prediction of complex networks. *International journal of modern physics. Condensed matter physics,*

statistical physics, applied physics. 2018. 32 (16), 1850197.

83. A. E. Motter. Cascade Control and Defense in Complex Networks. *Physical Review Letters*, 2004. vol. 93, p. 098701.

84. Haibo Wang. Research on the Application of Genetic Algorithm in Physical Education. *Journal of Mathematics*, vol. 2022, Article ID 8477945, 8 pages, 2022. https://doi.org/10.1155/2022/8477945.

85. MATLAB. Global Optimization Toolbox. URL: https://www.mathworks.com/products/global-optimization.html.

ДОДАТОК А
(обов’язковий)

ДОДАТКОВІ ІЛЮСТРАЦІЇ

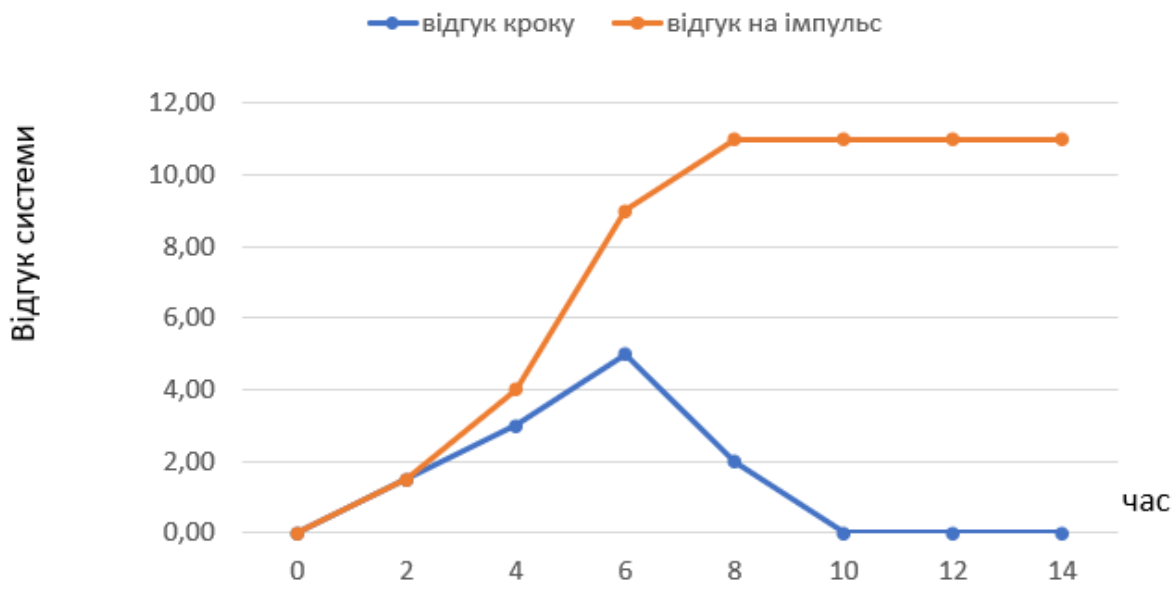
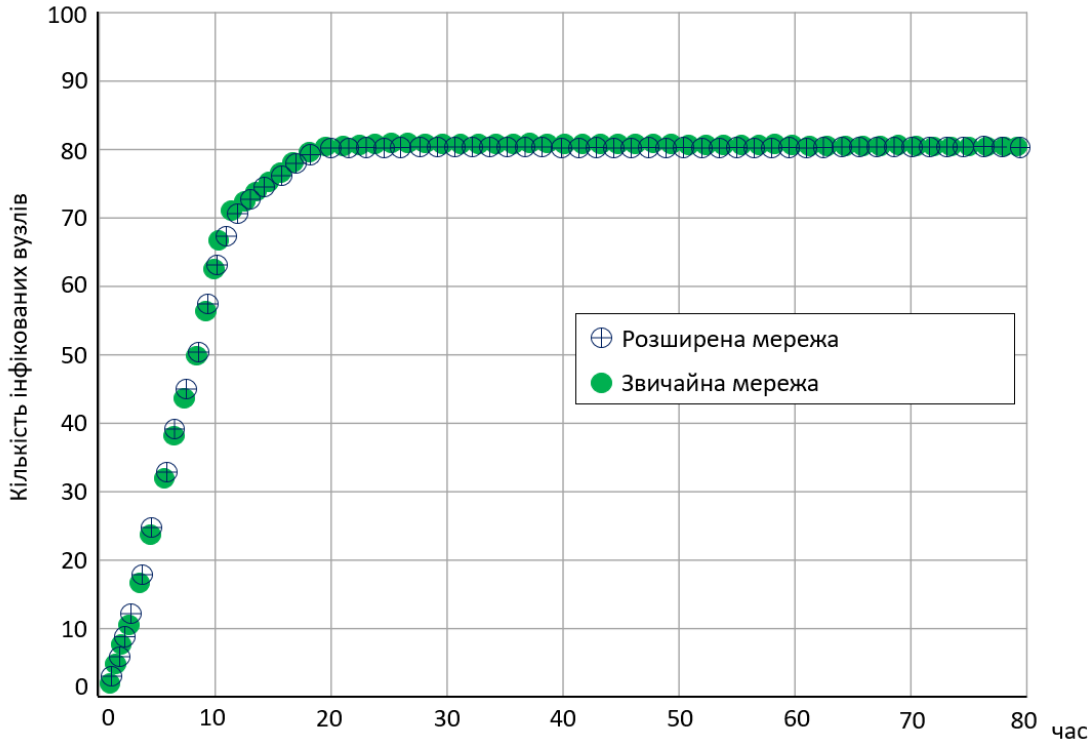
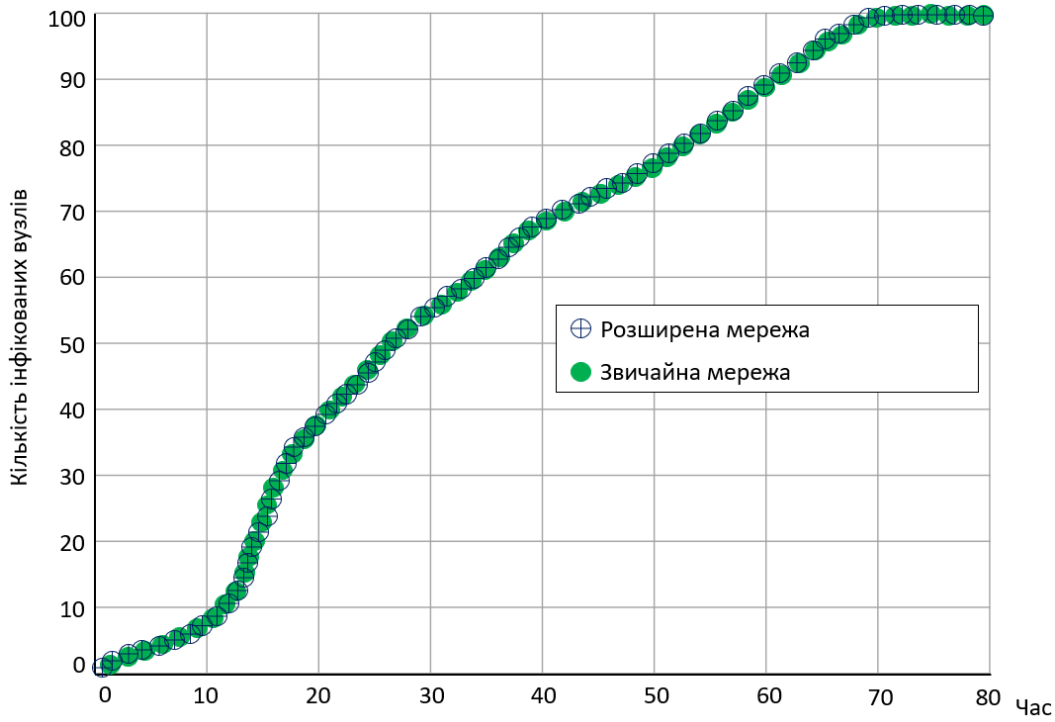


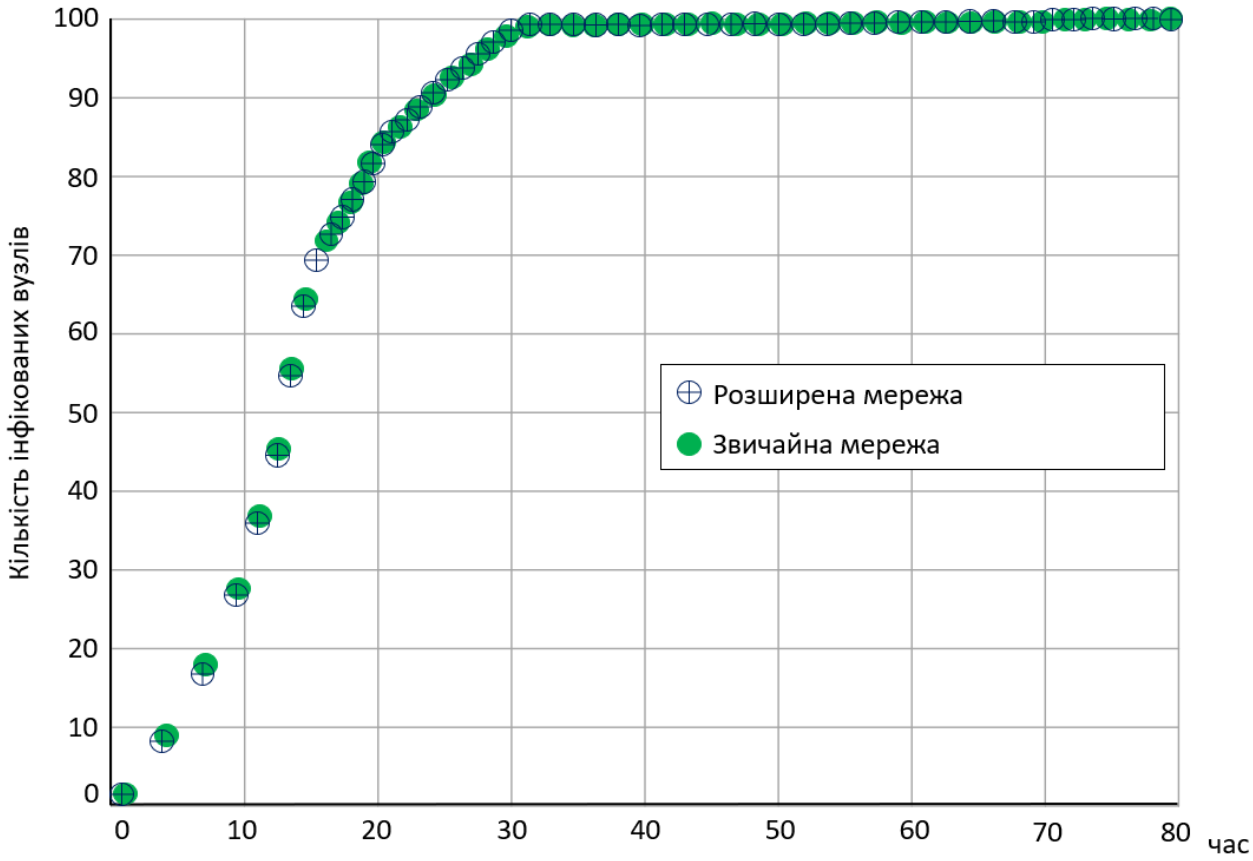
Рисунок А.1 - Лінійна стаціонарна система з розрахунком крокової та імпульсної реакції


Кількість інфікованих вузлів
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
час
Розширена мережа
Звичайна мережа

а)

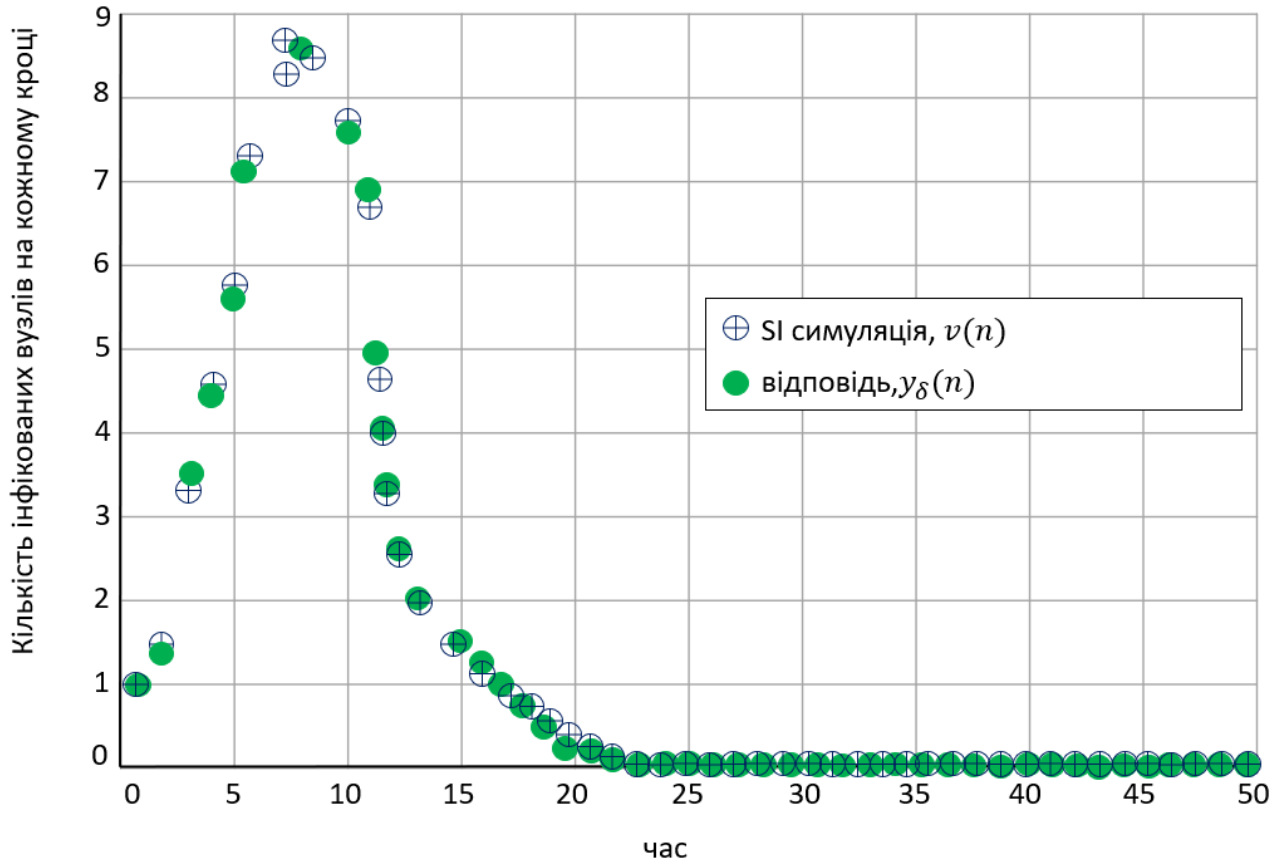

Кількість інфікованих вузлів
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
Час
Розширена мережа
Звичайна мережа

б)

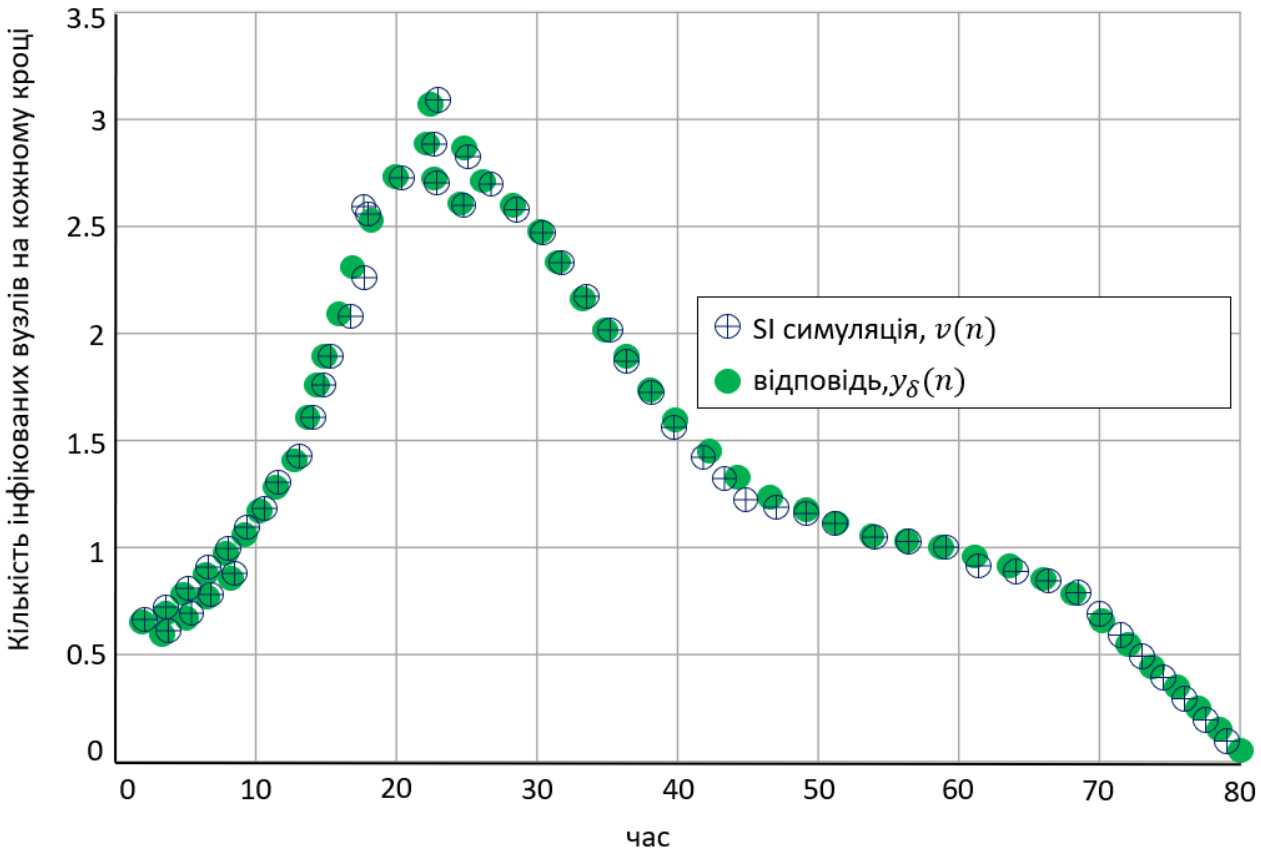


в)

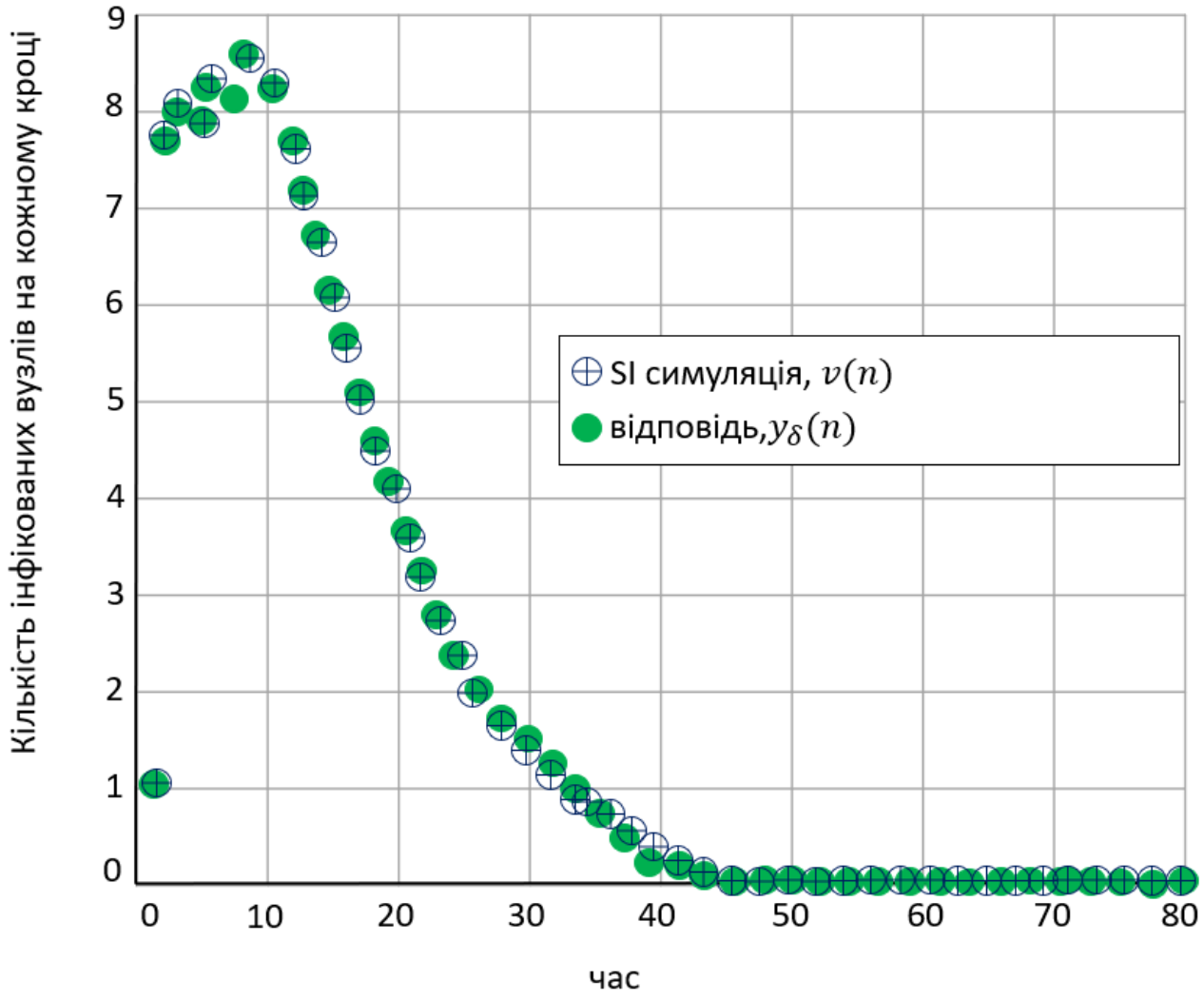
Рисунок А.2 – Динаміка поширення загрози в звичайній мережі та розширеній


Кількість інфікованих вузлів на кожному кроці
9
8
7
6
5
4
3
2
1
0
0
5
10
15
20
25
30
35
40
45
50
час
SI симуляція, $v(n)$
відповідь, $y_\delta(n)$

а)


Кількість інфікованих вузлів на кожному кроці
3.5
3
2.5
2
1.5
1
0.5
0
0
10
20
30
40
50
60
70
80
час
SI симуляція, $\nu(n)$
відповідь, $y_\delta(n)$

б)



в)

Рисунок А.2 – Динаміка поширення загрози в звичайній мережі та розширеній

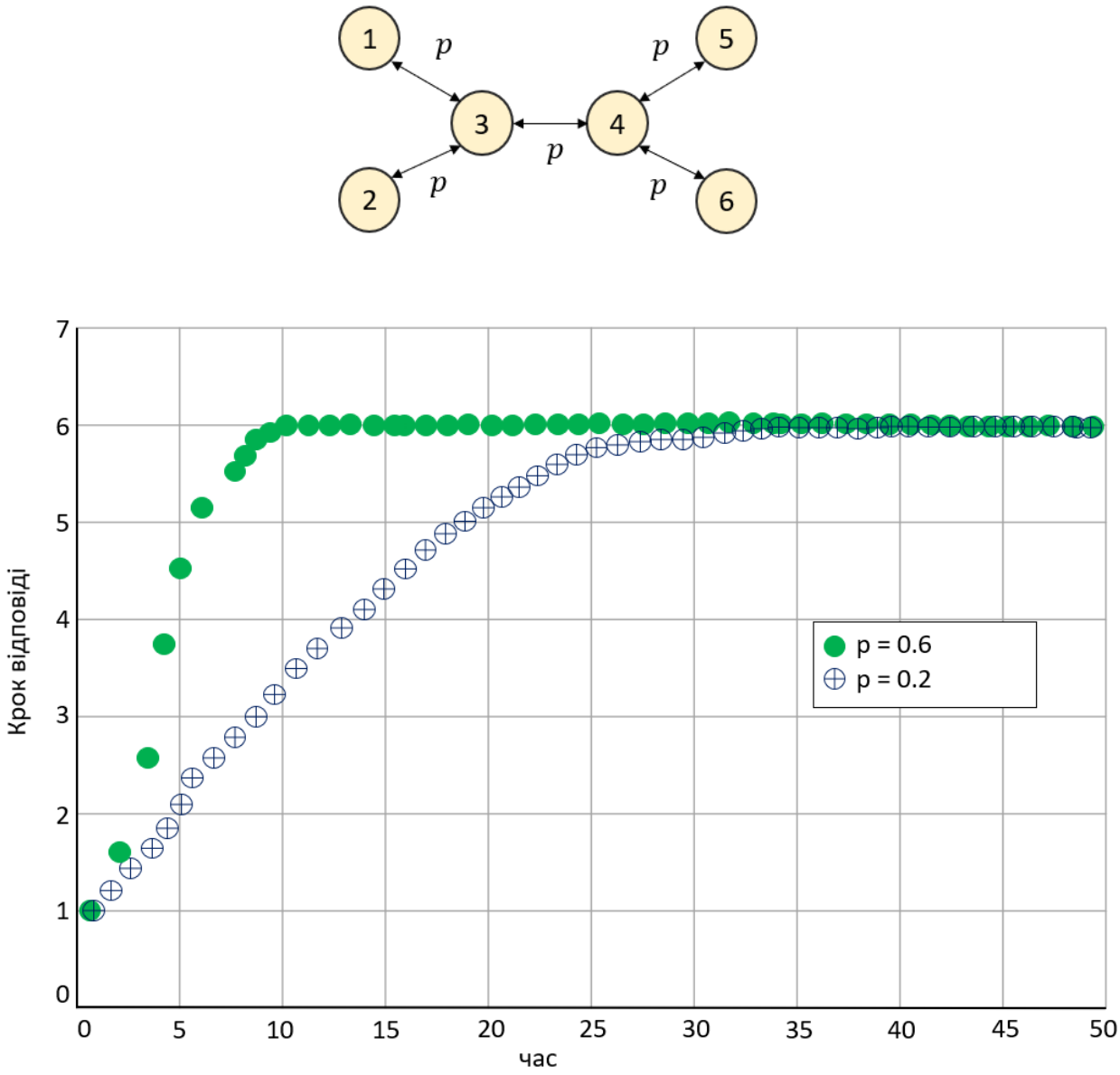
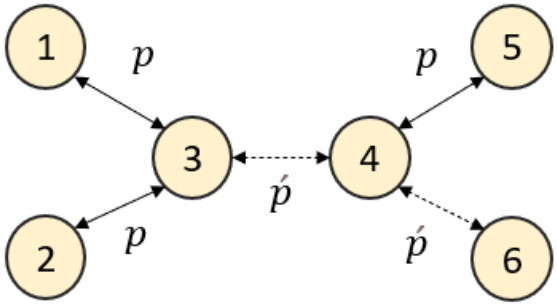


Рисунок А.3 – Проста мережа та відповідні покрокові реакції:

(a) неорієнтована мережа з M = 6 вузлами та N = 5 зв’язками та ймовірністю передачі p;

(b) покрокові реакції системи, отримані з мережі з використанням двох ймовірностей зараження p = 0,6 та p = 0,2



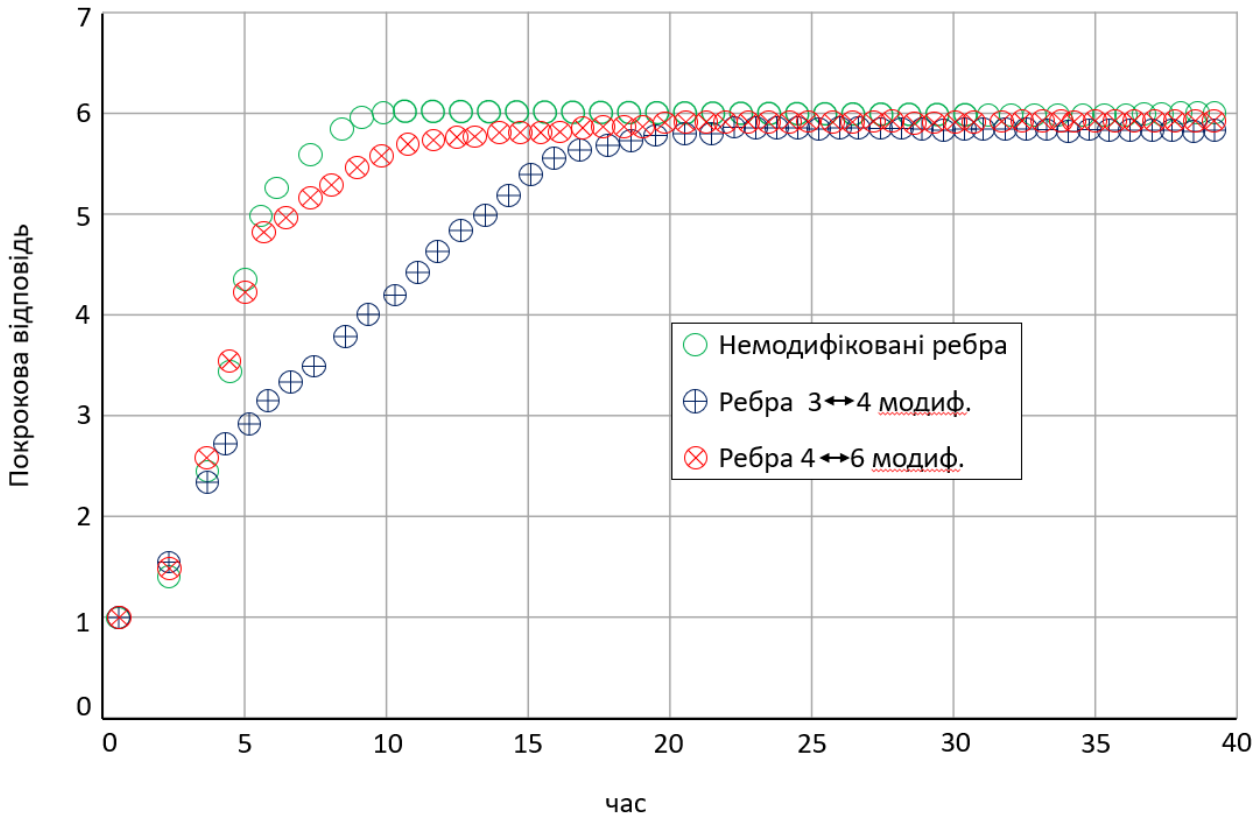


Рисунок А.3 – Приклад захисту мережі:

(a) неорієнтована мережа з M = 6 вузлами, N = 5 посиланнями та двома різними ймовірностями зараження p = 0:6 і p1 = 0:1.

(b) Відповідь на крок систем, отримана від мережі відповідно до вибраного каналу, який повинен бути захищеним

ДОДАТОК Б
(обов'язковий)

АЛГОРИТМ Б.1 ПСЕВДОКОД МОДЕЛІ МОТТЕРА-ЛАЯ

1: **Input:** Q(V, E), α, I . I - the list of removed nodes

2: calculate the size of the largest connected component K

3: calculate the load of each node F_i

4: calculate the capacity of each node M_i

5: remove the node(s) . initialize the cascade

6: **while** G_I (t + 1) = G_I (t) **do** . the new stable efficiency reached

7: calculate loads F_i

8: **if** $F_i > M_i$ **then** . the load exceeds the capacity

9: ai,[1...K] = 0 and a[1...K],i = 0 . the node fails, breaking all

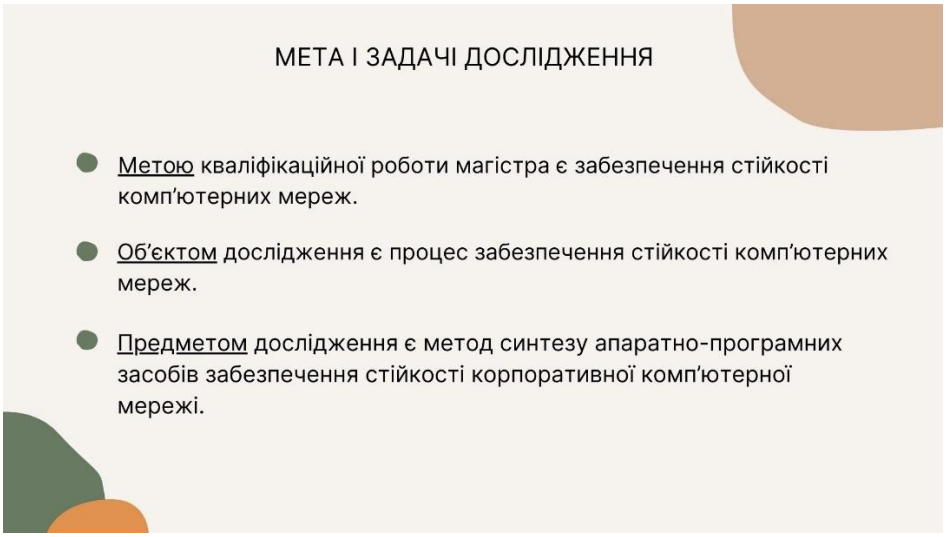
associated edges

10: calculate the size of the giant connected component G_I

11: **return** the relative size of the giant connected component

ДОДАТОК В
(обов'язковий)

ПРЕЗЕНТАЦІЯ



МЕТА І ЗАДАЧІ ДОСЛІДЖЕННЯ

Поставлена мета досягається розв'язанням таких основних задач:

- дослідити методи забезпечення стійкості корпоративної комп'ютерної мережі;
- проаналізувати сучасні програмно-технічних засоби забезпечення стійкості корпоративної комп'ютерної мережі;
- розробити модель забезпечення стійкості корпоративної комп'ютерної мережі;
- розробити метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі;
- реалізувати метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі.

НАУКОВА НОВИЗНА ОТРИМАНИХ РЕЗУЛЬТАТІВ

- Набув подальшого розвитку метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі, який на відміну від відомих для забезпечення стійкості здійснює додаткову модифікації топології комп'ютерної мережі шляхом її віртуального розширення, та який здійснює виявлення впливових розповсюджувачів, а також передбачає знаходження k найбільш критичних вузлів в комп'ютерній мережі, що її порушують стійкість.
- Набули подальшого розвитку програмно-технічні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

ПРАКТИЧНЕ ЗНАЧЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

В результаті виконаного наукового дослідження буде розроблено апаратно-програмні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

Актуальність роботи полягає в розробці удосконаленого методу синтезу апаратно-програмних засобів, який уможливить забезпечення стійкості корпоративної комп'ютерної мережі в умовах здійснення загроз.

АКТУАЛЬНІСТЬ

Актуальність роботи полягає в тому, що комп'ютерні мережі оточують нас всюди і нестабільність корпоративної комп'ютерної мережі може призвести не лише до грошових збитків, але і до людських жертв.

Стійкість комп'ютерної мережі важлива для лікарень, університетів, державних органів тощо.

- Якщо КМ лікарні має несправність у час пік (або відмова одного з вузлів спричиняє перенавантаження інших) - пацієнт може втратити змогу сконтактуватись з лікарнею вчасно, що призведе до людських втрат.
- Відмова кількох вузлів (з подальшим перенавантаженням інших) у банківській системі матиме вплив на прибутки банківської організації.
- Нестабільність серверів у інтернет-провайдера призведе до втрат прибутку (оскільки компанія втрачатиме клієнтів).

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Крок 1. Представлення мережі як лінійної стаціонарної системи (ЛСС)

Для забезпечення стійкості корпоративної комп'ютерної мережі у методі запропоновано застосування теоретичного підходу ЛСС, який дозволить відобразити динаміку поширення епідемії в мережі, що описується моделями "сприйнятливий-інфікований" (СІ) та "сприйнятливий-інфікований-вилікуваний". Виконавши представлення мережі як ЛСС, було здійснено імітацію кількох початково інфікованих вузлів і проведено спостереження за їх реакцією.

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

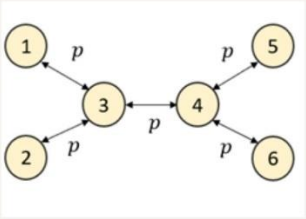
Крок 2. Дослідження стійкості комп'ютерної мережі в умовах інфікування та застосування віртуального розширення мережі

Для забезпечення стійкості комп'ютерної мережі в умовах епідемій необхідним є дослідження епідемії як процесу. Епідемія як процес характеризуєть параметром p, що відображає ймовірність передачі вірусу від одного інфікованого до одного сусіднього сприйнятливого вузла за один крок. Лінійна стаціонарна система описує лише детерміновану поведінку. Сам по собі підхід ЛСС не дає можливості ввести ймовірності. Тому для модифікації вихідної мережі перед перетворенням до форми, придатної для ЛСС, була введена альтернативна концепція, яка називається віртуальним розширенням мережі (Virtual Network Expansion)

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Крок 3. Обробка вхідних даних, отриманих зі змодельованої комп'ютерної мережі

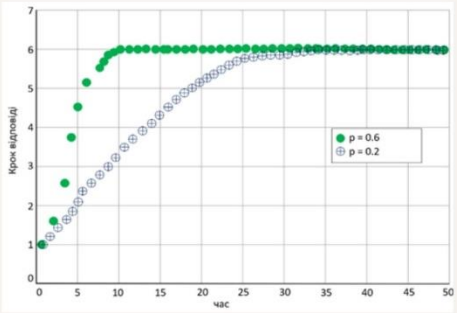
Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є оброблення вхідних даних, отриманих з комп'ютерної мережі.



Щоб продемонструвати можливість застосування ЛСС підходу до аналізу динаміки поширення, ми наведемо простий приклад. Візьмемо невелику неорієнтовану мережу G(V, E) з |V| = 6 вузлів і |E| = 5 ребер і застосуємо підхід ЛСС. Ймовірність передачі однакова для всіх пар сусідніх вузлів, і вважається, що інфекція походить з вузла (1).

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В результаті обчислень ступінчастих відгуків, було виявлено різницю між нахилами двох отриманих кривих. Крива з більшим нахилом представляє ступінчасту характеристику системи, отриману від мережі з більшою швидкістю передачі. Таким чином, аналізуючи реакцію даної системи, можна оцінити динаміку епідемії у відповідній мережі. Нахил кривої відповідає швидкості поширення епідемії в кожний момент часу.



МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Крок 4. Виявлення впливових розповсюджувачів, що порушують стійкість мережі

Існує багато методів оцінки важливості вузла в мережі. Більшість підходів базуються на різних мірах центральності та їх варіаціях. Даний метод використовує міру NIR (Node Imposed Response), яка фіксує потенціал поширення вузла. NIR може точно класифікувати найважливіші вузли на основі їхнього можливого впливу на поширення.

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Крок 5. Знаходження найбільш критичних вузлів в комп'ютерній мережі

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є знаходження найбільш критичних вузлів в комп'ютерній мережі. Для вирішення даної підзадачі було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.
Модель дозволяє встановити факт, що атака на один важливий вузол (з високим початковим навантаженням) може викликати каскадний ефект, який може призвести до збою всієї мережі та, як наслідок, серйозного збою служби.

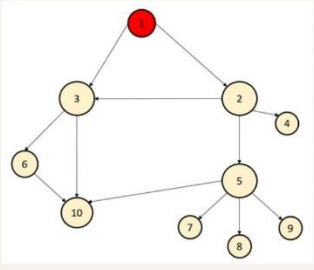
МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

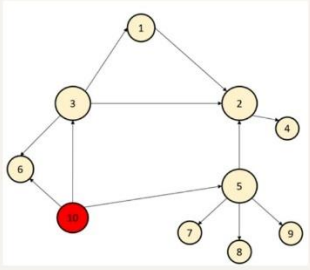
Крок 6. Знаходження множини k найбільш критичних вузлів мережі

Можлива ситуація, коли можуть існувати набори з k вузлів, одночасне видалення яких призведе до однакової або дуже схожої шкоди. Це означає, що для одного значення k існує декілька рішень. Зловмисник може зосередити всі свої ресурси на цьому невеликому наборі вузлів і все одно завдати значної шкоди стійкості мережі. Для вирішення підзадачі знаходження множини k найбільш критичних вузлів мережі було використано генетичний алгоритм.

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

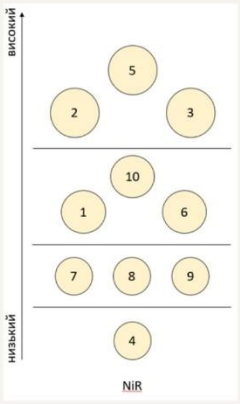
На рис. показано приклад мережію Кожен з вузлів має своє значення NiR. Для того, щоб його обчислити, топологія повинна бути змінена, аби зробити мережу ациклічною. Було проведено екперимент з синтезованими довама версіями топологій з двома вузлами-джерелами: вузол з ID1 ліворуч і вузол з ID10 праворуч.

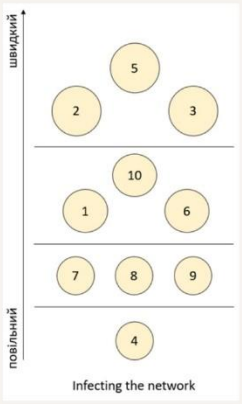




ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

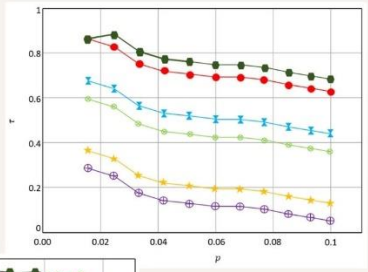
Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування.
Було визначено кілька окремих груп вузлів з різним потенціалом поширення

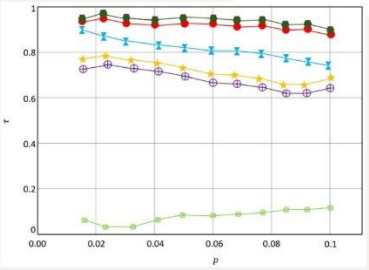


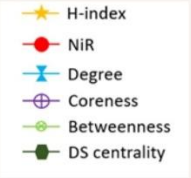


Моделювання проводилось на декількох мережах з використанням моделей SI та SIR. Базовим значенням для моделі SI є час t, необхідний для часткового (50% або 70% вузлів) інфікування у випадку одного вузла-джерела i.
Для моделі SI NiR працює так само добре, як і DS centrality, навіть незважаючи на те, що він не використовує жодних додаткових параметрів з моделі поширення.

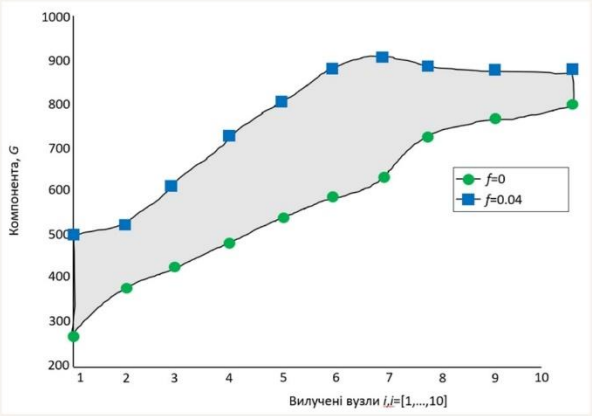
Очевидно, що кореляція між змодельованою динамікою та показниками centrality падає зі збільшенням p. Це свідчить про те, що оцінка потенціалу поширення вузла для великої ймовірності передачі стає складнішою.







ЗАСТОСУВАННЯ МЕТОДУ



На рисунку показано ефект вибіркового видалення фракції найменш навантажених вузлів.

ВИСНОВКИ

У першому розділі досліджено методи забезпечення стійкості корпоративної комп'ютерної мережі; а також проаналізовано сучасні програмно-технічних засоби забезпечення стійкості корпоративної комп'ютерної мережі.

У другому розділі представлено опис моделювання комп'ютерних мереж, зокрема описано методи моделювання, аналізу мереж в моменти здійснення загроз. В розділі також подано опис застосування метаевристики для моделювання стійкості комп'ютерної мережі. Описано отримання ациклічних графів при моделювання стійкості комп'ютерних мереж.

У третьому розділі запропоновано метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Для вирішення задачі метод передбачає залучення теорії лінійних стаціонарних систем, та використання метрики NiR, яка може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

ВИСНОВКИ

Було здійснено апробацію методу шляхом моделювання, результати якого показують високу кореляцію з фактичною динамікою поширення, змодельованою за допомогою процесів SI та SIR. NiR також показує невелику дисперсію, що означає його надійність для різних топологій комп'ютерних мереж.

У експериментальних дослідження було синтезовано два типи комп'ютерних мереж. Чотири мережі було синтезовано для великих та малих мереж відповідно. Вузли стовпця представляють кількість вузлів у вихідній мережі. Для апробації основних положень методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі було проведено дослідження з синтезованими мережами, у яких було здійснено множину дій над топологією мережі для того, щоб пом'якшити вплив відмови частини вузлів. Результати досліджень показали, що застосування синтезованих апаратно- програмних засобів забезпечили стійкість корпоративної комп'ютерної мережі в умовах здійснення загроз.

ПУБЛІКАЦІЇ ЗА МАТЕРІАЛАМИ ДИПЛОМНОЇ РОБОТИ

- Лисенко С.М., Сахнюк В.В., Бондарук О.В. Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Вісник Хмельницького національного університету. 2023.№3.

ДОДАТОК Г
(обов'язковий)

КОПІЯ СТАТТІ

УДК 004.93
DOI:

С.М. ЛИСЕНКО, В.В.САХНЮК, О.В.БОНДАРУК
Хмельницький національний університет

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В роботі представлено метод та програмно-технічний засіб забезпечення стійкості корпоративної комп'ютерної мережі під дією загроз різного виду. У даній статті буде представлено огляд аспектів стійкості та існуючі підходи до забезпечення стійкої маршрутизації. Ця стаття є результатом багатьох досліджень та експериментів, і, оцінюючи кінцевий результат, можна зауважити, що даний метод може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

Ключові слова: комп'ютерна мережа, стійкість корпоративної комп'ютерної мережі ,стійка маршрутизація

S.LYSENKO, B.SAKHNIUK, O.BONDARUK
Khmelnytskyi National University, Khmelnytskyi, Ukraine

A METHOD FOR SYNTHESIZING HARDWARE AND SOFTWARE TOOLS TO ENSURE THE STABILITY OF A CORPORATE COMPUTER NETWORK

The paper represents a method for ensuring the resilience of a corporate computer network under the influence of various types of threats. This article will provide an overview of the aspects of resilience and existing approaches to ensuring resilient routing. This article is the result of many studies and experiments, and evaluating the final result, it can be noted that this method can successfully reflect the possible importance of a node when it comes to epidemic dynamics for various network models to ensure network resilience. A possible way to solve the problem was to use the theory of linear stationary systems and the phenomenon of propagation in networks as the basis of the method. Complex interdependencies between their elements characterize various systems.

The method of synthesizing hardware and software means of ensuring the stability of a corporate computer network consists of such steps as representing networks as a linear stationary system, modelling the stability of a computer network in the context of epidemics by using virtual network expansion, studying the stability of a computer network in the context of uncertain data transmission and virtual network expansion, processing input data received from the modelled computer network, etc.

To solve the problem, the method involves the theory of linear stationary systems and the use of the NiR metric, which can successfully reflect the possible importance of a node when it comes to the dynamics of an epidemic for various network models to ensure network resilience.

The method is tested by simulations, the results of which show a high correlation with the actual propagation dynamics modeled by SI and SIR processes. NiR also shows a small variance, which means it is reliable for different computer

network topologies. The method also involves finding the most critical nodes in a computer network, for which a cascading failure model was used, which models overloaded nodes as non-functional.

Keywords: computer network resilience, computer network, resilient routing

Вступ

Несправності елементів комунікаційної мережі є неуникненним. Причинами цих несправностей можуть бути різні фактори, такі як природні катаклізми, людські помилки або зловмисні атаки, і це лише кілька з них [1]. Незважаючи на різноманітність характеристик цих несправностей, вони мають одну спільну рису: їх неможливо повністю усунути [2]. Наше повсякденне життя все більше стає залежним від комунікаційних мереж, оскільки обмін інформацією росте експоненційно. В результаті, нові збої в мережевих каналах або вузлах призводять до серйозних втрат даних і прибутку [3-6]. Оскільки комунікаційні мережі все більше охоплюють різні сфери нашого суспільства, очікується, що негативні наслідки від несправностей будуть лише зростати [7-9].

Більшість випадків порушень маршрутизації в мережах зв'язку виникає внаслідок випадкових несправностей каналів або комутаційних пристроїв [10-12], таких як відключення кабелю під час робіт на вулицях, пошкодження підводних кабелів рибальськими суднами або відмови в електропостачанні. Згідно з [13], окремі випадки відмов в каналах відіграють важливу роль у глобальних мережах, становлячи більше 70% від усіх випадків збоїв. В мережах дальнього зв'язку на кожні 10 км оптоволоконного зв'язку припадає в середньому одна відмова кабелю за 12 років [14]. Випадки відмов можуть тривати декілька днів або навіть тижнів, призводячи до серйозного зниження продуктивності мережі. У бездротових мережах проблема ще складніша через те, що характеристики зв'язку залежать від різних факторів, включаючи погодні умови. Однак в локальних мережах з проводовими з'єднаннями відмови в вузлах зазвичай більше, оскільки коротші з'єднання можуть бути краще захищені фізично. Локалізація несправностей та подальший ремонт з'єднань або вузлів може займати від годин до декількох днів, що веде до серйозних збоїв в роботі мережевих служб.

Отже, необхідність розробки мережевих механізмів автоматичної реконфігурації, зокрема для відновлення мережевих послуг до моменту фізичного усунення несправностей елементів мережі, має обґрунтовану потребу. Відсутність вбудованого механізму відновлення пошкодженого трафіку може призвести до значних негативних наслідків для клієнтів, які втратять доступ до мережевих послуг. Щоб впоратися з несправностями елементів мережі, необхідно спочатку аналізувати причини, що призводять до їх виникнення. Таким чином, основною метою дослідження є синтез апаратно-програмних засобів, спрямованих на забезпечення стійкості корпоративної комп'ютерної мережі.

Аспекти стійкості та існуючі підходи до забезпечення стійкої маршрутизації

Згідно з джерелами [15-19], поняття стійкості можна розділити на дві основні категорії: толерантність до викликів, що зосереджена на підходах до проектування мережі з метою забезпечення неперервності обслуговування навіть у випадку виникнення проблем, та достовірність, яка відображає вимірювані характеристики аналізованих систем зв'язку. Взаємодія між цими двома категоріями, відома як надійність, вказує на продуктивність мережі в умовах викликів. Виявлення несправностей також повинно включати локалізацію та ізоляцію несправностей, тобто визначення несправного вузла або зв'язку, необхідних для припинення подальшої передачі інформації через пошкоджений елемент, який потребує відновлення, згідно з джерелами [20-26].

В основі поширення збоїв у мережах лежать дві динаміки - каскади та епідемії, які мають спільні характеристики, такі як обмежена кількість вузлів, в яких вони виникають, та здатність поширюватися по мережі, спричиняючи глобальні перебої. Однак механізм та наслідки цих збоїв відрізняються. Каскадні збої виникають через дефіцит пропускної здатності, тоді як епідемії пояснюються властивістю вірусів поширюватися. Кожен збій також має свій власний тригер. Каскадні збої виникають через вийдення з ладу вузлів або зв'язків, що може бути викликане випадковими збоями, географічно пов'язаними збоями або навмисними атаками. Епідемії спричиняються шкідливим вірусним зараженням, яке поширюється на ретельно вибрані вузли мережі за допомогою шкідливого програмного забезпечення, що поширюється на фізично та логічно підключених сусідніх

вузлах. Згідно з [27, 28], можна виділити певні фази порушення роботи системи, такі як підготовка, реагування та фаза відновлення, і вибір стратегії для підвищення стійкості мережі залежить від фази, на якій буде застосована дана стратегія.

Дослідження методів моделювання збоїв корпоративної комп'ютерної мережі

Існують два основних підходи до моделювання - аналітичні та чисельні методи. Аналітичний підхід дозволяє отримати рішення про стан системи без використання симуляцій та великих обчислювальних потужностей. Методи теорії систем застосовуються для аналізу мереж, розглядаючи їх як LTI-системи та оцінюючи реакції системи на вхідні впливи. Отримані результати використовуються для оцінки потужності поширення вузлів та визначення найбільш критичних елементів [29].

Чисельні методи моделювання широко використовуються для спостереження за динамікою всередині мережі. Моделювання мереж є поширеним методом дослідження мереж. Воно дозволяє отримати уявлення про динаміку процесу та надати багато інформації, яку не можна передбачити заздалегідь. Для цього використовується MATLAB - математичне програмне забезпечення, яке охоплює багато аспектів математики та може бути використане для моделювання та обчислень мереж.

Основним підходом до аналізу є використання міри кореляції, зокрема тау-коефіцієнта рангової кореляції Кендалла, який застосовується для перевірки припущень при оцінці вузлів. Ця непараметрична міра зв'язку між ранжованими даними є потужним інструментом для порівняння результатів, отриманих різними методами моделювання [30].

Існує велика кількість методів моделювання збоїв корпоративної комп'ютерної мережі, які далі будуть використані для розробки методу синтезу апаратно-програмних засобів для забезпечення резилієнтності (стійкості) корпоративної комп'ютерної мережі [31].

Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

З метою вирішення задачі забезпечення стійкості комп'ютерних мереж необхідним є розроблення методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Одним з можливих шляхів розв'язку задачі є залучення теорії лінійних стаціонарних систем та явища розповсюдження в мережах як основи методу синтезу апаратно-програмних засобів забезпечення стійкості. Різноманітні системи характеризуються складними взаємозалежностями між їхніми елементами.

Для вирішення задачі метод передбачає залучення теорії лінійних стаціонарних систем, та використання метрики NiR, яка може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

Апробація методу здійснюється шляхом моделювання, результати якого показують високу кореляцію з фактичною динамікою поширення, змодельованою за допомогою процесів SI та SIR.

NiR також показує невелику дисперсію, що означає його надійність для різних топологій комп'ютерних мереж. Також метод передбачає знаходження найбільш критичних вузлів в комп'ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

Одним з найважливіших кроків є дослідження стійкості. Для цього етапу слід врахувати можливі варіант інфікувань. Інфікування загрозою може моделюватись, починаючи з одного і того ж початкового вузла для вихідної та розширеної мереж. В ході роботи було здійснено спостереження за кумулятивною кількістю заражених вузлів з плином часу. На рисунку 1 показано майже ідеальний збіг результатів моделювання для вихідної та розширеної мереж, що доводить можливість застосування методу розширення мережі для забезпечення стійкості корпоративної комп'ютерної мережі в умовах епідемій.

Для дослідження стійкості важливе також порівняння динаміки інфікування вихідної мережі $G(V, E)$ та реакції системи, отриманої з розширеної мережі $G_E(V_E, E_E)$. Подібно до прикладу, показаного на рисунку 1, спочатку моделюється динаміка поширення за допомогою моделі SI. На кожному часовому кроці t заражений вузол намагається заразити сприйнятливого сусіда. Інфекція передається з ймовірністю $p = 0.4$. Таким чином, сприйнятливий вузол заражається з ймовірністю $P = 1 - (1 - p)k$, де k - кількість інфікованих сусідів. Дані, зібрані за допомогою симуляції, включають кумулятивну кількість інфікованих вузлів $\underline{v_U}(n)$ та кількість інфікованих вузлів на

кожному часовому кроці $\underline{vu}(n)$, яка є похідною від $\underline{vu}(n)$. Потім система створюється з розширеної мережі *GE(VE, EE)* з ймовірністю інфікування $p = 0.4$. На рисунку 2 зображено динаміку епідемії як vu(n), змодельовану на вихідній мережі з ймовірністю інфікування $p = 0{,}4$. Значення $\underline{vu}(n)$ порівнюються зі ступінчастою реакцією $\underline{y_H}(n)$ системи, створеної на основі розширеної вихідної мережі. Результати, отримані в результаті моделювання та реакція системи сильно корелюють.

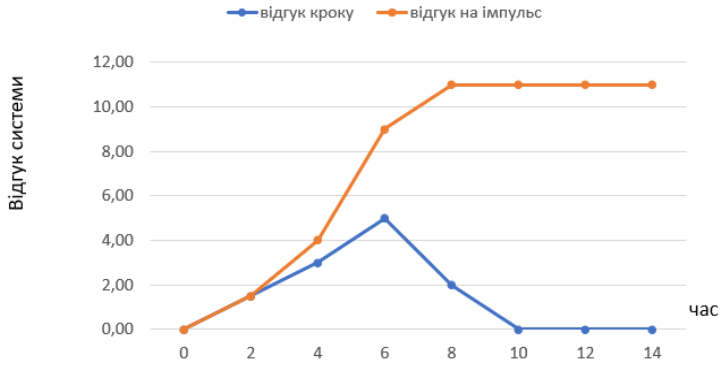


Рисунок 1 - Лінійна стаціонарна система з розрахунком крокової та імпульсної реакції

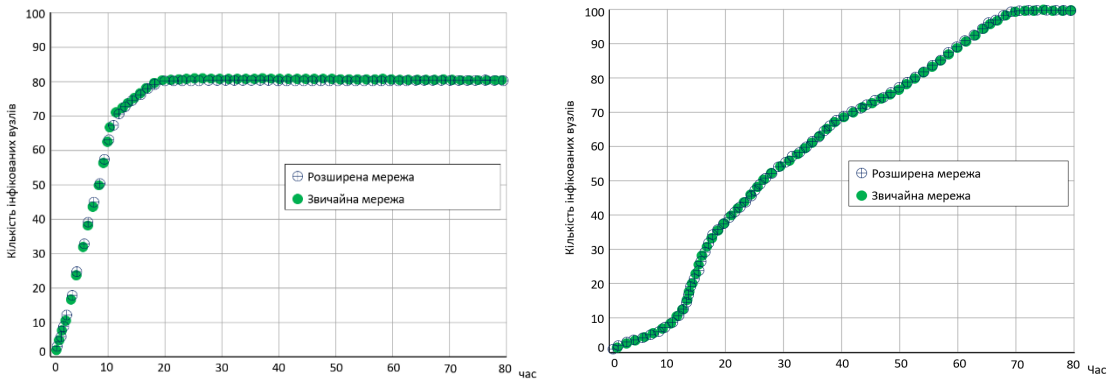


Рисунок 2 – Динаміка поширення загрози в звичайній мережі та розширеній

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є оброблення вхідних даних, отриманих з комп'ютерної мережі. Три типи мереж, що використовуються в моделюванні, генеруються випадковим чином за трьома різними мережевими моделями.

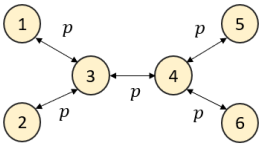


Рисунок 3 - Неорієнтована мережа з M = 6 вузлами та N = 5 зв'язками та ймовірністю передачі p

Щоб продемонструвати можливість застосування ЛСС підходу до аналізу динаміки поширення було взяти неорієнтовану мережу *G(V, E)* з $|V| = 6$ вузлів і $|E| = 5$ ребер (рис. 3) і застосовано підхід ЛСС. Ймовірність передачі змінюється з $p1 = 0.6$ до $p2 = 0.2$. Ймовірність передачі однакова для всіх пар сусідніх вузлів, і вважається, що інфекція походить з вузла. На основі інформації про топологію *G(V, E)* ми будуємо дві системи ЛСС: першу з $p_1 = 0.6$ і другу з $p_2 = 0.2$. Потім було обчислено ступінчасті відгуки для отриманих систем. Було виявлено різницю між нахилами двох отриманих кривих (рис. 4). Крива з більшим нахилом представляє ступінчасту характеристику системи, отриману від мережі з більшою швидкістю передачі. Таким чином, аналізуючи реакцію даної системи,

можна оцінити динаміку епідемії у відповідній мережі. Нахил кривої відповідає швидкості поширення епідемії в кожний момент часу. Ця ж величина відповідає і імпульсному відгуку.

0,6 та p = 0,2

Наступним кроком запропонованого методу є вирішення проблеми модифікації комп'ютерної мережі. Це вимагає додаткової модифікації топології шляхом віртуального розширення мережі. Пропонований метод використовує міру Node Imposed Response (NiR), яка фіксує потенціал поширення вузла. Алгоритми видалення циклів можуть змінити топологію мережі так, що деякі шляхи стають недоступними, особливо в неорієнтованих мережах, де потрібно вибирати напрямок ребра. Щоб зберегти найважливіші шляхи з вихідного вузла і мінімізувати кількість видалених ребер, слід були знайти правильний метод видалення циклів. Після маніпуляцій з вихідним графом ми створюємо матрицю системи A таким чином, що $A = A_{adj}^{T}$. Всі ненульові елементи замінились значенням d, так що $\forall a_{ij} = 0 : a_{ij} = d$, і $0 < d < 1$. Додаткове дослідження показує, що дисперсія між значеннями NiR для всіх вузлів стає вищою при меншому d.

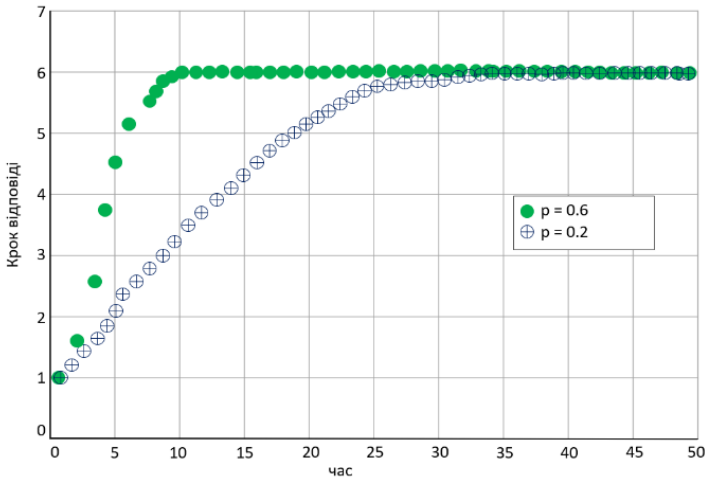


Рисунок 4 - Покрокові реакції системи, отримані з мережі з використанням двох ймовірностей зараження p =

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є знаходження найбільш критичних вузлів в комп'ютерній мережі. Для вирішення даної підзадачі було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні. Модель дозволяє встановити факт, що атака на один важливий вузол (з високим початковим навантаженням) може викликати каскадний ефект, який може призвести до збою всієї мережі та, як наслідок, серйозного збою служби.

Таким чином, вважатимемо найбільш критичним вузлом той, видалення якого спричинить найбільшу шкоду мережі. Пошкодження визначається як зворотна величина найбільшого підключеного компонента, що залишився після моделювання каскаду. Після видалення вузла і відносний розмір найбільшого з'єднаного компонента, що залишився, дорівнює G_i і так само після видалення j відносний розмір найбільшого з'єднаного компонента дорівнює G_j . Якщо $G_i < G_j$, ми робимо висновок, що вузол і є більш критичним.

Для вирішення підзадачі знаходження множини k найбільш критичних вузлів мережі було використано генетичний алгоритм. Набір з 100 найбільш критичних вузлів включається в додаткову оцінку. Початковий простір розв'язків різко зменшується, але все ще має значний розмір (F_n=10 = 1,73 × 1013). Генетичний алгоритм уможливлює знайти розв'язок через поступове покращення пристосованості всього покоління. Оптимізація, що проводилася, була цілочисельною задачею, де рішенням є масив з n цілих чисел в діапазоні від 1 до 100, і кожне значення зіставляється з відповідним ідентифікатором вузла. Максимально 100 вузлів можна було об'єднати в групи, що складаються з k елементів кожна. Набір з 100 вузлів було визначено за допомогою попереднього аналізу впливу окремих вузлів. Підхід генетичного алгоритму для знаходження критичної групи представлено у вигляді псевдокоду нижче.

1: Вхід: G(V, E)

2: Параметри ініціалізації: розмір популяції встановлено на pop = 200 з обмеженням на максимальне Ngen = 1200 поколінь

3: Створення початкової популяції: початкова популяція створюється випадковим чином із рівномірним розподілом

4: поки кількість поколінь досягає максимуму до t> Ngen

5: виконати кросовер

6: тоді як для всіх рішень у популяції

7: видалити вузли t ініціалізувати каскад

8: виконати оцінку t, значенням функції пристосованості, яка є розміром найбільшої компоненти.

9: відсортувати рішення з останнього покоління

10: повернути групу вузлів

Підхід ГА дає однакові або гірші результати для всіх критичних груп. Додаткова перевірка за допомогою генетичного алгоритму підтримує рішення зосередити пошук на відносно невеликій кількості критичних вузлів.

Таким чином, метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі можна умовно розділити на такі кроки:

1) представлення мережі як лінійної стаціонарної системи;
2) моделювання стійкості комп'ютерної мережі в умовах епідемій шляхом застосування віртуального розширення мережі;
3) дослідження стійкості комп'ютерної мережі в умовах невизначеної передачі даних та віртуального розширення мережі;
4) обробка вхідних даних, отриманих зі змодельованої комп'ютерної мережі;
5) виявлення впливових розповсюджувачів, що порушують стійкість мережі;
6) знаходження найбільш критичних вузлів в комп'ютерній мережі;
7) знаходження множини k найбільш критичних вузлів мережі.

Експериментальні дослідження апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

З метою здійснення апробації та перевірки ефективності запропонованого методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі було здійсненого ряд експериментальних досліджень. На рисунку 5 показано приклад невеликої мережі з n = 10 вузлами. Кожен з вузлів має своє значення NiR, вказане вище. Значення NiR вказує на потужність поширення загрозу, тобто вузол космп'ютерної мережі з вищим NiR швидше заразить всю мережу або більшу її частину.

Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування. Твердження підтвердилось моделюванням динаміки поширення SI та порівнянням результатів з отриманими значеннями NiR. Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування. Якщо час повного інфікування коротший, то вузол має потенціал для швидшого поширення інфекції і вважається більш важливим (тобто більш впливовим). Для того, щоб порівняти значення NiR та змодельований потенціал розповсюдження, здійснюється сортування вузлів як за значенням NiR, так і за потужністю розповсюдження, отриманою в результаті здійсненого моделювання.

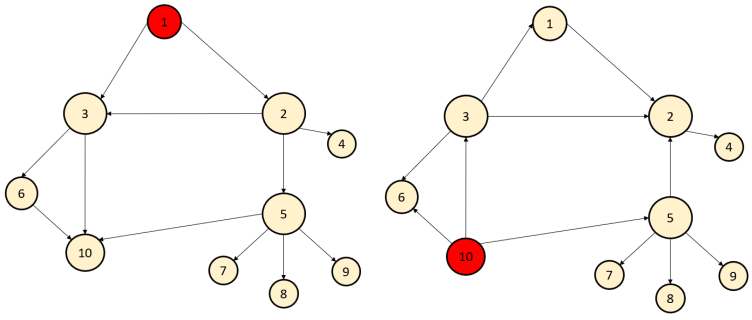


Рисунок 5 - Виявлення впливових розповсюджувачів, що порушують стійкість мережі

Таким чином, було визначено кілька окремих груп вузлів з різним потенціалом поширення (рис. 6).

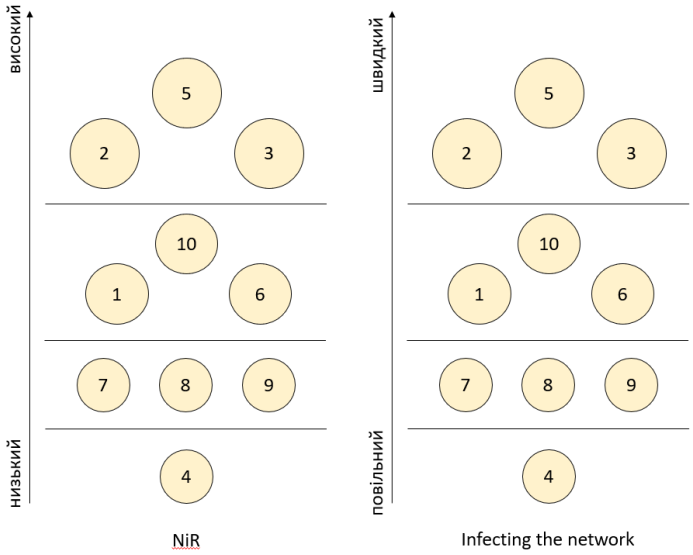


Рисунок 6 – Потенціал поширення

У випадку невеликої мережі значення NiR точно відображає потенціал розповсюдження, оскільки групування вузлів збігається з отриманим в результаті чисельного моделювання. Ймовірно, що для великих мереж, де n>10, буде багато вузлів з дуже схожими значеннями NiR, що відповідає вродженому принципу безмасштабності багатьох мереж, з великою часткою не-вузлів.

Для того, щоб перевірити кореляцію між NiR та результатами моделювання для всіх сімейств мереж, використаних для аналізу було проведено експерименти. Моделювання проводилось на декількох мережах з використанням моделей SI та SIR. Базовим значенням для моделі SI є час t, необхідний для часткового (50% або 70% вузлів) інфікування у випадку одного вузла-джерела i. Для моделі SIR значенням, яке використовується для порівняння, є розмір спалаху (загальна кількість вузлів, які заразилися) після t часових кроків виконання. Результати, отримані за допомогою моделювання для кожного з вузлів, порівнюються з NiR та п'ятьма іншими мірами центральності (міжцентровість, центральність, ступінь, DS та центральність за H-індексом). Показник NiR демонструє високу кореляцію з результатами моделювання разом з низькою дисперсією, часто перевершуючи всі п'ять показників як у моделях SI, так і SIR. Єдиним показником, який показує однакові результати, є центральність DS, параметри якого залежать від динаміки поширення загроз. У випадку відмови критичного вузла, будь-яка частка між 0,02 до 0,1 найменш навантажених вузлів може бути вилучена, щоб запобігти подальшого каскадування. На рисунку 4.4б показано порівняння розміру компоненти після каскаду з заходами захисту та без них для десяти найбільш критичних вузлів.

Частка видалених вузлів після початкової атаки була обрана такою f = 0.04. Для кожного критичного вузла і каскад пом'якшується таким чином, що результуюче значення G завжди більше, якщо захисні заходи реалізовано належним чином. Ідея полягає в тому, щоб визначити набір вузлів, які слід підготувати до вилучення у випадку найнебезпечніших відмов.

Відмова одного з десяти найбільш критичних вузлів з Таблиці 1 спричинить найбільшу шкоду. Тому проводиться наступний аналіз: Для кожного з найбільш критичних вузлів моделюється відмова і вибираються найменш навантажені вузли. Саме ці вузли є кандидатами на навмисне видалення після початкової атаки. Певна кількість вузлів часто з'являється у списку кандидатів на різні відмови i. Це ті вузли, які, швидше за все, матимуть менше навантаження у випадку навмисної атаки. Механізм захисту повинен видалити частку f з усіх вузлів, крім вузлів-кандидатів. В абсолютних числах кількість вершин, які будуть навмисно видалені, становить $23 \leq nir \leq 115$. Не має значення, яку саме вершину буде видалено, доки число nir не виходить за межі.

Таблиця 1 - Вплив видалення вузлів з синтезованої мережі

№ вузла мережі	$G_{\alpha=1.01}$	$G_{\alpha=1.10}$	$G_{\alpha=1.30}$	$G_{\alpha=1.50}$
10	0.312	0.230	0.310	0.409
19	0.289	0.348	0.528	0.542
42	0,439	0.467	0.455	0.387
12	0.458	0.492	0.912	0.915
41	0.532	0.485	0.676	0.687

Висновки

У роботі було досліджено наявні методи забезпечення стійкості корпоративної комп'ютерної мережі, а також розроблено удосконалений метод, який враховує різні загрози у мережах.

Також було запропоновано вдосконалений метод синтезу апаратно-програмних засобів для забезпечення стійкості корпоративної комп'ютерної мережі. Цей метод використовує теорію лінійних стаціонарних систем та метрику NiR, яка дозволяє відображати важливість вузлів в контексті динаміки поширення епідемії для різних мережевих моделей. Метод був протестований шляхом моделювання, результати якого показали високу кореляцію з фактичною динамікою поширення, що була змодельована за допомогою процесів SI та SIR. Метрика NiR також демонструє невелику дисперсію, що свідчить про її надійність для різних топологій комп'ютерних мереж. Парадигма, на якій базується підхід ЛСС, дозволяє використовувати різні варіації вихідної метрики, наприклад, вибір декількох вхідних та вихідних точок, що дозволяє оцінити вплив багатьох вузлів мережі на процес поширення.

Більш вразливі вузли з більшою ймовірністю будуть досягнуті з набору обраних вхідних вузлів. Аналіз не обмежується незваженими мережами. Той самий підхід може бути використаний навіть для зважених мереж, просто включивши ваги в матрицю системи.

Також метод передбачає знаходження найбільш критичних вузлів в комп'ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

Література

1. Agarwal P.K., Efrat A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. *Proc. 30th Annual Joint Conference of the IEEE Computer and Communications Societie*s, 2013. pp. 1521–1529.
2. Asthana R., Singh Y.N., Grover W. p-cycles: an overview. *IEEE Commun. Surv. Tutorials.* 2013. 12(1), 97–111.
3. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable and Secure Comput.* 2014. 1(1), 11–33.
4. Caini C., Cruickshank, H., Farrell, S., Marchese, M.: Delay- and disruption-tolerant networking (DTN): an alternative solution for future satellite networking applications. *Proc. IEEE* 2021. 99(11).
5. Cetinkaya, E.K., Sterbenz, J.P.G.: A taxonomy of network challenges. *Proc. 9th International Conference on Design of Reliable Communication Networks*, 2013. pp. 322–330 ()
6. Chołda P., Jajszczyk A. Recovery and its quality in multilayer networks. IEEE/OSA J. *Lightwave Technol.* 2010. 28(4), 372–389.
7. Chołda, P., Tapolcai, J., Cinkler, T., Wajda, K., Jajszczyk, A.: Quality of Resilience as a network reliability characterization tool. *IEEE Netw.* 2011, 23(2), 11–19.
8. Colle, D., De Maesschalck, S., Develder, C., Van Heuven, P., Groebbens, A., Cheyns, J., Lievens, U., Pickavet, M., Lagasse, P., Demeester, P.: Data-centric optical networks and their survivability. *IEEE J. Sel. Areas Commun.* 2012. 20(1), 6–20.
9. Cucurull, J., Asplund, M., Nadjm-Tehrani, S., Santoro, T.: Surviving attacks in challenged networks. IEEE Trans. Dependable and Secure Comput. 2015. 9(6), 917–929.
10. Fangming L., Bo L., Lili Z., Baochun L., Hai J., Xiaofei L. Flash crowd in P2P livestreaming systems: fundamental characteristics and design implications. *IEEE Trans. Parallel. Distrib. Syst.* 2012. 23(7), 1227–1239.
11. Geva M., Herzberg A., Gev Y. Bandwidth Distributed Denial of Service: attacks and defences. *IEEE Secur. Priv*. 2014. 12(1), 54–61 ()

12. Grover, W.D. Mesh-based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Prentice Hall PTR, Upper Saddle River (2014) Grover, W.D.: The protected working capacity envelope concept: an alternate paradigm for automated service provisioning. *IEEE Commun. Mag.* 2014. 42(1), 62–69 ()

13. Grover, W.D., Shen, G. Extending the p-cycle concept to path-segment protection. In: Proc. IEEE International Conference on Communications (IEEE ICC'03), 2, pp. 1314–1319 (2013)

14. Haddadi H., Rio, M., Iannaccone G., Moore A., Mortier R. Network topologies: inference, modeling, and generation. IEEE Commun. Surv. Tutorials 10(2), 48–69 (2009)

15. Haider, A., Harris, R. Recovery techniques in Next Generation Networks. *IEEE Commun. Surv. Tutorials*, 2014 9(3), 2–17 ()

16. Heegaard, P.E., Trivedi, K.S. Network survivability modeling. *Comput. Netw.* 53(8), 1215–1234 (2011)

17. Ho, P.-H. State of the art progress in developing survivable routing schemes in mesh WDM networks. *IEEE Commun. Surv. Tutorials* 6(4), 2–16 (2014)

18. Ho, P.-H., Tapolcai, J., Cinkler, T. Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels. *IEEE/ACM Trans. Networking* 12(6), 1105–1118 (2022)

19. Ho, P.-H., Tapolcai, J., Mouftah, H.: On achieving optimal survivable routing for shared protection in survivable Next-Generation Internet. *IEEE Trans. Reliab*. 53(2), 216–225 (2014)

20. Jaumard, B., Rocha, C., Baloukov, D., Grover, W.D. A column generation approach fordesign of networks using path-protecting p-cycles. *In: Proc. 6th International Workshop on Design of Reliable Communication Networks (DRCN'07)*, pp. 1–8 (2017)

21. Jung J., Krishnamurthy B., Rabinovich M. Flash crowds and denial of service attacks: characterization and implication for CDNs and web sites. *Proc. 11th International Conference on World Wide Web (WWW'02*), 2012. pp. 293–304.

22. Kappenman, J. A perfect storm of planetary proportions. *IEEE Spect. Mag*. 2012. 49(2), 26–31.

23. Khabbaz, M.J., Assi, C.M., Fawaz, W.F. Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. *IEEE Commun. Surv. Tutorials* 14(2), 2012. 607–640.

24. Kitamura, Y., Lee, Y., Sakiyama, R., Okamura, K. Experience with restoration of Asia Pacific network failures from Taiwan earthquake. *IEICE Trans. Commun*. E90-B(11), 2017. 3095–3103.

25. Kodian, A., Grover, W.D. Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection. *IEEE/OSA J. Lightwave Technol.* 2015. 23(10), 3241–3259.

26. Kompella, K., Swallow, G. Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, IETF RFC 4379. 2016.

27. Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y. General resilience: taxonomy and strategies. *Proc. 2014 International Conference and Utility Exhibition on Green Energ for Sustainable Development (ICUE'14),* 2014. pp. 1–8.

28. Mingsen X., Wen-Zhan S., Deukhyoun H., Jong-Hoon K., Byeong-Sam K. ECPC: preserve downtime data persistence in disruptive sensor networks. *Proc. IEEE Mobile Ad-Hoc and Sensor Systems* (MASS'13), 2013 pp. 281–289.

29. Misseri X., Gojmerac I., Rougier J.-L. IDRD: enabling inter-domain route diversity. *Proc. IEEE International Conference on Communications*, 2013. pp. 3536–3541.

30. Mukherjee, B.: Optical WDM Networks. Springer, New York. 2016.

31. *Nicol D.M., Sanders W.H., Trivedi K.S. Model-based evaluation: from dependability to security. IEEE Trans. Dependable and Secure Comput.* 2017. 1(1), 48–65.

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1014855440

Дата перевірки:
29.04.2023 08:27:14 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
29.04.2023 08:29:18 EEST

ID користувача:
100005591

Назва документа: **Сахнюк_Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративно...**

Кількість сторінок: **99** Кількість слів: **21360** Кількість символів: **164994** Розмір файлу: **990.27 KB** ID файлу: **1014555365**

1.02%
Схожість

Найбільша схожість: **0.64%** з джерелом з Бібліотеки (ID файлу: **1014546614**)

0.48% Джерела з Інтернету	63	Сторінка 101
0.87% Джерела з Бібліотеки	63	Сторінка 101

0% Цитат

Не знайдено жодних цитат

Посилання	1	Сторінка 101

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	12

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 28.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

ID: 112730 Назва: Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі Додано в БД: 2023-04-29 Автора: Сахнюк В. Керівники: Лисенко С.М. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	140997	1099	40231 (29%)	252 (23%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
112082	Назва: ЗВІТ з науково-дослідної практики "Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі" Додано в БД: 2023-03-21 Автора: Сахнюк В.В. Керівники: Нічепорук А.О. Консультанти: Опоненти:	39445 (28.0%)	248 (23.0%)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІНУ РОБОТУ

Здобувач: Сахнюк Віталіна Валентинівна

Тема: Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень - ; кількість сторінок записки 84 .

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено огляд аналіз відомих методів виявлення кібер-загроз в комп'ютерних системах. Досліджено відомі рішення та засоби в цій сфері. У другому розділі запропоновано модель динамік збоїв та забезпечення стійкості корпоративної комп'ютерної мережі. У третьому розділі запропоновано метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. У четвертому розділі проведено реалізацію та дослідження методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

4. Позитивні сторони роботи: Запропонований метод дозволив розробити апаратно-програмні засоби забезпечення стійкості корпоративної комп'ютерної мережі.

5. Негативні сторони роботи: В першому розділі не розглянуті усі аспекти стійкості комп'ютерних мереж.

6. Оцінка графічного оформлення та пояснювальної записки роботи: =

7. Відгук про роботу в цілому: Робота виконана на високому рівні.

8. Інші зауваження: =

9. Оцінка кваліфікаційної роботи:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи вважаю, що робота заслуговує оцінки «відмінно» 4,80 (A)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., професор Мартинюк В.В., завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, Хмельницького національного університету

"28" квітня 2022р.

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Сахнюк Віталіни Валентинівни
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) 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.

03 травня 2023 року

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: «Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі»

Автор: Сахнюк Віталіна Валентивнівна

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Лисенко Сергій Миколайович, д.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. 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 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.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах є збіг зі світом з науково-дослідної практики автора Віталіни Сахнюк «Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі», який було додано в репозитарій ХНУ 21 березня 2023 року;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості Unichek, складає 1.02% і адресується до 63 першоджерела та системою AntiPlagiarism складає 28%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ С. М. Лисенко

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІСч _____ Т. О. Говорущенко