Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки

«Затверджую»
Зав. кафедри теоретичної та
прикладної системотехніки
_____ д.т.н., проф. С. І. Шматков
«___» _____ 2023 р.

Пояснювальна записка

до кваліфікаційної роботи
бакалавра

на тему: «**МОДЕЛЬ ДІАГНОСТИКИ СТАНУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ**»

Захищено на засіданні
Атестаційної комісії № 40
протокол № __ від __.06.2023 р.
Оцінка _____ / _____
Голова Атестаційної комісії
_____ **СКОБ Ю. О.**
(підпис)

Виконав:
студент 4 курсу, групи КІ – 41
Спеціальність: 123 – «Комп'ютерна інженерія»
ПОДПЛЄТНІЙ Євгеній Олександрович _____

Керівник:
к.т.н., доцент кафедри теоретичної та прикладної системотехніки
СТРІЛЕЦЬ Вікторія Євгенівна_____

Рецензент:
к.т.н., доцент, в.о. завідувача кафедри теоретичної та прикладної інформатики
МЕНЯЙЛОВ Євген Сергійович _____

Харків – 2023

АНОТАЦІЯ

Пояснювальна записка до бакалаврської атестаційної роботи складається зі вступу, трьох розділів, висновків, списку використаних джерел і трьох додатків. Загальний обсяг роботи складає 59 сторінки, із яких 43 сторінок основної частини з 4 рисунками, 3 формулами, 10 найменуванням списку використаних джерел та чотирма додатками.

Метою кваліфікаційної роботи є аналіз методів діагностики локальної комп'ютерної мережі та розробка власної локальної комп'ютерної мережі для знаходження способів покращення надійності та якості роботи локальної комп'ютерної мережі

Об'єктом дослідження є локальна комп'ютерна мережа, яка складається з комп'ютерів, серверів, мережевого обладнання (роутери, комутатори тощо), програмного забезпечення та зв'язків між ними.

Предметом дослідження є методи діагностики стану локальної комп'ютерної мережі. Це означає вивчення і розробку різних методів, технік та інструментів, які дозволяють здійснювати моніторинг, аналіз та оцінку роботи мережі, виявляти проблеми, помилки, загрози безпеці та інші аномалії, а також розробляти рекомендації та заходи для вирішення цих проблем.

Завдання дослідження:

1. Виконати огляд підходів, моделей і методів для діагностики стану складних систем.
2. Розглянути поняття та класифікацію складних систем.
3. Виконати аналіз локальних комп'ютерних мереж.
4. Виконати аналіз методів діагностики локальних комп'ютерних мереж.
5. Розробити програмну модель локальної комп'ютерної мережі.

6. Розробити дерево відмов для моделі локальної комп'ютерної мережі.

Методи дослідження: методи аналізу стану локальної комп'ютерної мережі, методи побудови моделей локальних мереж, методи виявлення та аналізу відмов.

Область застосування – використання моделі у цілях виявлення та запобіжним діям відмов. З її допомогою, можна вирахувати вірогідність відмови, і зрозуміти чи мережа працює справно.

Ключові слова: модель, локальна комп'ютерна мережа, стан мережі, діагностика, стан, маршрутизатор, комутатор.

ABSTRACT

The bachelor's thesis consists of an introduction, three chapters, conclusions, a list of references, and three appendices. The total volume of the work is 59 pages, including 43 pages of the main part with 4 figures, 3 formulas, 10 references, and four appendices.

The aim of this qualification work is to analyze methods for diagnosing a local computer network and develop a local computer network to identify ways to improve the reliability and performance quality of the network.

The object of the research is a local computer network consisting of computers, servers, network equipment (routers, switches, etc.), software, and their connections.

The subject of the research is methods for diagnosing the state of a local computer network. This involves studying and developing various methods, techniques, and tools that allow for monitoring, analyzing, and evaluating the network's performance, detecting problems, errors, security threats, and other anomalies, as well as developing recommendations and measures to address these issues.

Application area: the use of the model for the purpose of detecting and preventive actions against failures. With its help, the probability of failure can be calculated, and it can be determined whether the network is functioning properly.

Keywords: model, local computer network, network state, diagnostics, state, router, switch.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Тема дослідження має велику актуальність у сучасному інформаційному суспільстві. З розвитком технологій і залученням комп'ютерних мереж у всі сфери життя, зростає важливість ефективного функціонування та безперебійності мережевих інфраструктур.

Одним із ключових аспектів успішної роботи комп'ютерних мереж є їх стан. Локальні комп'ютерні мережі є важливим елементом для багатьох організацій, незалежно від їх масштабу та галузі діяльності. Втрати продуктивності мережі або її неперервність можуть призвести до серйозних наслідків, таких як втрата даних, зниження ефективності роботи, втрата грошей та навіть потенційні кібератаки.

Тому розробка моделі діагностики стану локальної комп'ютерної мережі є вкрай важливою. Ця модель може допомогти інженерам мережі та адміністраторам мережевого обладнання вчасно виявляти та вирішувати проблеми, які можуть виникати в процесі роботи мережі. Вона забезпечує можливість моніторингу мережі, виявлення несправностей, аналізу трафіку та ідентифікації вразливостей.

Потреба в такій моделі діагностики стану локальної комп'ютерної мережі постійно зростає. З розвитком Інтернету речей, хмарних технологій, мобільних пристроїв та інших інноваційних технологій, обсяги даних, які обробляються в мережах, ростуть експоненційно. Це ставить нові виклики перед фахівцями з мережевої інфраструктури, які повинні забезпечити безперебійну роботу мережі.

Додатково, така модель діагностики може виявити потенційні загрози безпеці мережі. У сучасному цифровому світі кібербезпека є однією з найважливіших проблем. Швидкість та точність виявлення аномалій у

роботі мережі можуть допомогти запобігти кібератакам та зберегти важливі дані від несанкціонованого доступу.

Таким чином, актуальність теми полягає у необхідності забезпечення ефективної та безперебійної роботи мережевої інфраструктури. Розробка такої моделі дозволить вчасно виявляти проблеми та забезпечувати безпеку мережі, що є критичними аспектами у сучасному інформаційному суспільстві.

Мета дослідження полягає в дослідженні та розробці ефективних методів та інструментів для виявлення та аналізу проблем, пов'язаних зі виникненням відмов і дефектів у локальній комп'ютерній мережі.

Об'єктом дослідження є локальна комп'ютерна мережа, яка складається з комп'ютерів, серверів, мережевого обладнання (роутери, комутатори тощо), програмного забезпечення та зв'язків між ними.

Предметом дослідження є методи діагностики стану локальної комп'ютерної мережі. Це означає вивчення і розробку різних методів, технік та інструментів, які дозволяють здійснювати моніторинг, аналіз та оцінку роботи мережі, виявляти проблеми, помилки, загрози безпеці та інші аномалії, а також розробляти рекомендації та заходи для вирішення цих проблем.

РОЗДІЛ 1. ОГЛЯД ПІДХОДІВ, МОДЕЛЕЙ І МЕТОДІВ ДЛЯ ДІАГНОСТИКИ СТАНУ СКЛАДНИХ СИСТЕМ

1.1. Поняття та класифікація складних систем

Складні системи є важливою складовою сучасного світу, включаючи локальні комп'ютерні мережі. Розуміння поняття та класифікації складних систем допомагає нам аналізувати, розробляти та діагностувати такі мережі.

Складна система – це сукупність взаємопов'язаних компонентів, що взаємодіють один з одним з метою виконання певної функції або досягнення певної мети. Вона може бути фізичною, біологічною, соціальною або інформаційною. Складні системи мають такі особливості:

1) *багатоелементність* вказує на те, що складна система складається з великої кількості взаємопов'язаних компонентів, які разом працюють для досягнення спільної мети або виконання певної функції.

Компоненти складної системи можуть бути різних типів, включаючи фізичні об'єкти, процеси, підсистеми, людей, програмне забезпечення, датчики, комунікаційні засоби та багато іншого. Кожен компонент має свої властивості, можливості та роль у системі.

Багатоелементність додає складності до системи, оскільки кожен компонент може мати свої власні характеристики, вимоги та способи роботи. Взаємодія між компонентами може бути складною та нелінійною, оскільки зміна стану одного компонента може мати непропорційний вплив на інші. Врахування всіх компонентів і їх взаємодії вимагає детального аналізу та моделювання системи.

Багатоелементність може мати як позитивні, так і негативні наслідки. З одного боку, різноманітність компонентів може приносити більше можливостей, ефективності та інновацій. З іншого – вона може призводити

до складності управління, виникнення небажаних взаємодій, конфліктів або незбалансованості в системі [1].

Розуміння багатоелементності є важливим при розробці моделей діагностики стану складних систем, оскільки вона впливає на взаємодію компонентів, виявлення несправностей та аналіз системи в цілому. Ефективне управління багатоелементними системами допомагає забезпечити їх стабільну роботу, надійність та досягнення бажаних результатів.

2) *взаємодія* – спосіб, за яким компоненти системи співпрацюють один з одним, обмінюються інформацією, матеріалами, енергією та впливають на результат роботи системи в цілому. Існують різні аспекти взаємодії у складних системах:

а) взаємодія між компонентами: компоненти складної системи взаємодіють між собою, обмінюючи інформацію, сигнали, матеріали та енергію. Ця взаємодія може бути прямою, коли компоненти взаємодіють безпосередньо один з одним, або опосередкованою через спільні ресурси, середовище або систему зв'язків;

б) залежності та взаємозв'язки: у складних системах існує велика кількість залежностей та взаємозв'язків між компонентами. Зміни в одному компоненті можуть мати вплив на інші компоненти або на роботу системи в цілому. Взаємозв'язки можуть бути прямими (наприклад, передача сигналу від одного компонента до іншого) або непрямими (наприклад, зміни в середовищі, що впливають на роботу компонентів);

в) взаємодія з середовищем: складні системи взаємодіють зі своїм фізичним, соціальним або інформаційним середовищем. Взаємодія з середовищем може включати отримання вхідних даних, обмін інформацією, вплив на середовище або відповідь на зміни у середовищі. Взаємодія з середовищем може мати великий вплив на роботу системи і вимагає аналізу та адаптації системи до змін;

г) синергія: взаємодія між компонентами системи може призводити до синергетичного ефекту, коли ціла система виявляє вищі властивості або продуктивність, ніж проста сума внеску окремих компонентів. Синергія може сприяти покращенню ефективності, швидкості, точності або роботи системи в цілому.

Взаємодія у складних системах вимагає розуміння та аналізу взаємодії між компонентами, взаємозв'язків, емерджентності та впливу на середовище. Це допомагає розробити ефективні моделі діагностики стану системи та прийняти відповідні рішення для забезпечення її надійності, ефективності та оптимальної роботи.

Емерджентність – це явище виникнення нових властивостей, структур або функцій на рівні системи, які не можуть бути пояснені або передбачені на основі властивостей її окремих компонентів. Це означає, що коли компоненти системи взаємодіють між собою, вони створюють щось більше, ніж проста сума їх окремих внесків.

Основні аспекти емерджентності:

а) структурна емерджентність: взаємодія між компонентами системи може призводити до формування нових структур на рівні системи, які не існують на рівні окремих компонентів. Наприклад, у природних екосистемах взаємодія між рослинами, тваринами та мікроорганізмами призводить до формування складної структури екосистеми зі своїми взаємозв'язками та взаємозалежностями;

б) функціональна емерджентність: складні системи можуть проявляти нові функції або можливості, які не мають аналогів на рівні окремих компонентів. Наприклад, у соціальних системах взаємодія між індивідами може призводити до виникнення нових соціальних явищ, таких як колективна свідомість, емоційна атмосфера, культурні та соціальні норми.

в) динамічна емерджентність: складні системи можуть мати нелінійну та непередбачувану динаміку, де малий зміщення у взаємодії компонентів

може мати значний вплив на поведінку системи в цілому. Наприклад, у глобальних фінансових системах невеликі зміни в обсязі торгівлі або валютних курсах можуть призвести до неочікуваних резонансних ефектів або коливань на фінансових ринках.

г) контекстуальна емерджентність: емерджентність може залежати від контексту, в якому знаходиться складна система. Одна і та ж система може проявляти різні емерджентні властивості в різних умовах або середовищах. Наприклад, у технологічних системах певні емерджентні властивості можуть проявлятися лише при певних умовах роботи або конфігурації компонентів.

Емерджентність в складних системах показує, що вивчення та розуміння окремих компонентів системи не дозволяє повністю передбачити її поведінку. Для ефективного управління складними системами потрібно враховувати емерджентні властивості, аналізувати їх взаємозв'язки та розробляти моделі, які допомагають передбачити та керувати системою в цілому.

Нелінійність відноситься до взаємодії між компонентами системи, де зміна в одному компоненті може мати непропорційний або нелінійний вплив на інші компоненти. Це означає, що взаємодія між компонентами системи не підкоряється простим арифметичним або пропорційним законам, а може виявляти складні та неочікувані залежності.

Основні аспекти нелінійності:

а) непропорційні залежності: в нелінійних системах зміна в одному компоненті не призводить до пропорційної зміни в інших компонентах. Наприклад, у метеорологічних системах навіть невеликі зміни у вихідних параметрах можуть мати значний вплив на погоду і призводити до непропорційних змін у вітрових швидкостях, температурі або опадах;

б) граничні ефекти: у нелінійних системах можуть спостерігатися граничні ефекти, де невеликі зміни у вхідних параметрах можуть викликати

великі та неочікувані зміни в поведінці системи. Наприклад, у фізичних системах, таких як хаотичні системи або системи з фазовими переходами, навіть дрібні зміни в початкових умовах можуть призводити до повністю різних результатів в подальшому розвитку системи;

в) ваємодія та зворотний зв'язок: нелінійні системи часто виявляють сильний взаємний вплив між компонентами та зворотнім зв'язком, де зміна в одному компоненті викликає зміни в інших компонентах, які впливають назад на перший компонент. Це може призводити до складних циклічних залежностей та взаємозв'язків в системі;

г) нелінійна динаміка: нелінійні системи можуть проявляти складну динаміку, таку як періодичність, хаос або стабільні цикли. Це означає, що зміни в системі можуть мати нелінійні та непередбачувані впливи на подальший розвиток системи [2].

Прості та лінійні методи аналізу не можуть адекватно описати та передбачити поведінку нелінійних систем. Тому для розуміння та управління нелінійними системами використовуються спеціальні математичні моделі та алгоритми, такі як нечітка логіка, нейромережі або генетичні алгоритми, що дозволяють враховувати складність та нелінійність взаємодії компонентів системи.

Складні системи можна класифікувати за різними ознаками. Виділяють загальні категорії *класифікації складних систем*, які застосовуються до локальних комп'ютерних мереж:

а) за природою взаємодії компонентів:

– фізичні складні системи: такі системи включають фізичні об'єкти, які взаємодіють між собою. Наприклад, комп'ютери, маршрутизатори, комутатори та інші пристрої у локальній мережі взаємодіють фізичним способом;

– інформаційні складні системи: такі системи включають обробку і передачу інформації. У локальній комп'ютерній мережі це можуть бути

протоколи передачі даних, програмне забезпечення та механізми передачі інформації.

б) за масштабом:

– мікросистеми: це складні системи, що складаються з невеликої кількості компонентів. Наприклад, локальна комп'ютерна мережа в невеликому офісі або домашня мережа;

– макросистеми: це великі складні системи, що складаються з великої кількості компонентів. Наприклад, велика корпоративна мережа або глобальна комп'ютерна мережа Інтернет.

в) за ступенем самоорганізації:

– статичні складні системи: такі системи мають сталу структуру та поведінку, яка не змінюється з часом. Наприклад, фізична мережа з фіксованою конфігурацією;

– динамічні складні системи: такі системи можуть змінювати свою структуру та поведінку з часом. У локальній мережі це можуть бути автоматичні процеси налаштування, розподілу ресурсів та резервування.

Загальна розуміння поняття та класифікації складних систем є важливим кроком у розробці моделі діагностики стану локальної комп'ютерної мережі. Це допомагає ідентифікувати основні взаємозв'язки та особливості системи, що в свою чергу сприяє розробці ефективних методів діагностики та відновлення роботи мережі при виникненні проблем [1].

1.2. Методи діагностики стану складних систем

Діагностика стану складних систем, таких як локальні комп'ютерні мережі, відіграє важливу роль у забезпеченні надійності, ефективності та безпеки їх функціонування. Діагностика полягає в пошуку, виявленні та аналізі відхилень, проблем або несправностей у системі з метою їх виявлення та виправлення.

Розглянемо методи діагностики стану складних систем.

1. Моніторинг та логування. Цей метод включає постійний контроль за параметрами, подіями та діями в мережі. Мережеві пристрої, такі як маршрутизатори, комутатори та сервери, можуть реєструвати та зберігати дані про роботу системи, такі як пропускна здатність, завантаження, помилки та інші важливі показники. Лог-файли та метрики можуть бути використані для аналізу та виявлення аномалій або проблем.

2. Тестування з використанням спеціального програмного забезпечення. Включає застосування спеціальних програмних засобів для проведення тестів та аналізу різних аспектів мережі. Наприклад, можна використовувати програми для сканування портів, перевірки наявності вразливостей, аналізу пропускної здатності, контролю якості послуг (QoS) тощо. Ці інструменти дозволяють виявляти проблеми та слабкі місця в мережі.

3. Візуальна інспекція та перевірка фізичного з'єднання. Метод містить перевірку фізичного стану мережевих кабелів, роз'ємів, розподільчих панелей та інших компонентів. Перевірка забезпечує виявлення фізичних пошкоджень, неправильного підключення або несправностей, що можуть впливати на працездатність мережі.

4. Аналіз протоколів мережі. Метод включає вивчення протоколів, що використовуються в мережі, та аналіз їх взаємодії. Можна використовувати аналізатори мережі, які дозволяють перехоплювати та аналізувати мережевий трафік для виявлення аномалій, помилок або проблем з протоколами.

5. Моніторинг безпеки мережі. Метод передбачає постійний моніторинг системи на наявність потенційних загроз безпеці. Це може включати виявлення спроб несанкціонованого доступу, атак з використанням зловмисного програмного забезпечення, перехоплення даних та інші види кіберзагроз.

6. Використання сенсорних систем. У деяких випадках можуть бути використані сенсорні системи, що моніторять фізичні параметри, такі як температура, вологість, напруга тощо. Ці дані можуть слугувати індикаторами стану системи та допомагати виявити проблеми або потенційні ризики [3].

Застосування даних методів діагностики допомагає оперативно виявляти, аналізувати та вирішувати проблеми у локальних комп'ютерних мережах. Комбінація різних методів дозволяє забезпечити комплексний підхід до діагностики та підтримки надійності роботи мережі.

1.3. Моделі діагностики стану складних систем

Моделі діагностики стану складних систем використовуються для збору, аналізу та інтерпретації даних, що стосуються роботи системи. Вони допомагають ідентифікувати відхилення в роботі системи, виявляти причини їх виникнення та передбачати можливі наслідки. Ці моделі використовують різноманітні методи, такі як статистичний аналіз, машинне навчання, штучні нейронні мережі та експертні системи, для розуміння поведінки системи і виявлення аномалій. Застосування моделей діагностики стану складних систем, зокрема локальних комп'ютерних мереж, дозволяє оперативно виявляти проблеми, такі як несправність обладнання, витоки даних, мережеві конфлікти тощо. Це дозволяє системним адміністраторам приймати своєчасні заходи для усунення проблем та попередження серйозних відмов системи. Крім того, такі моделі можуть допомагати в плануванні обслуговування, оптимізації ресурсів та підвищенні продуктивності системи шляхом виявлення слабких місць і рекомендацій щодо їх вдосконалення. Нижче наведені моделі діагностики стану складних систем (рис. 1.1).

1. Модель на основі правил ґрунтується на визначенні правил, які вказують на зв'язки між певними ознаками стану системи та можливими

проблемами. Наприклад, можуть бути визначені правила, що описують, які помилки або аномалії вказують на проблеми з мережевими пристроями або протоколами. Ці правила використовуються для виявлення відхилень в реальному часі та прийняття рішень щодо подальших дій.

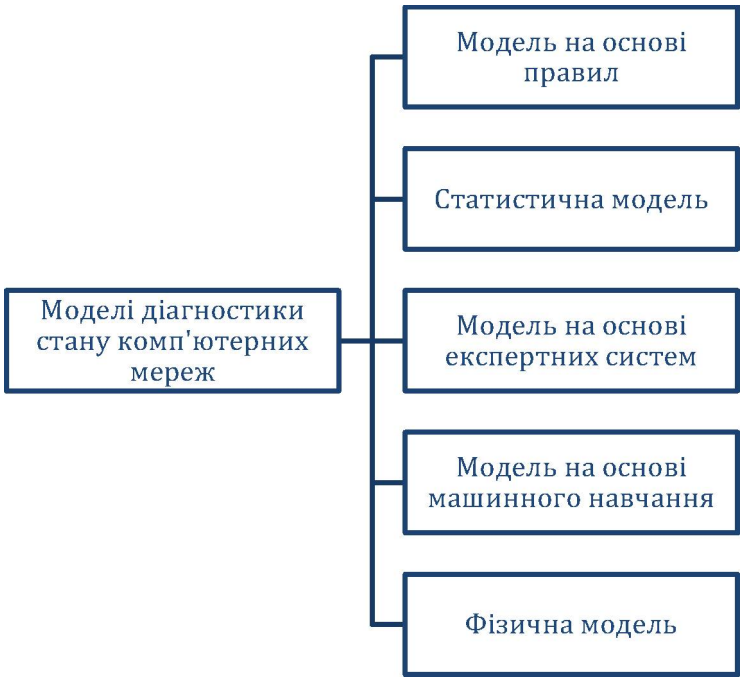

Рисунок 1.1 – Класифікація моделей діагностики стану комп’ютерних мереж

2. Статистична модель базується на статистичному аналізі даних, що відображають стан системи. Вона використовує методи статистики, машинного навчання та аналізу даних для виявлення аномалій або відхилень від норми. Наприклад, модель може навчитися розпізнавати типові патерни роботи мережі та виявляти аномальні зміни, що можуть свідчити про проблеми.

3. Модель на основі експертних систем використовує знання та експертні правила, що розробляються на основі досвіду фахівців у галузі. Експертна система може виявляти проблеми, аналізуючи параметри, використовуючи встановлені правила та здійснюючи порівняння зі

збереженими знаннями. Ця модель може бути особливо корисною в складних системах, де важко визначити формальні правила.

4. Модель на основі машинного навчання використовує алгоритми машинного навчання для аналізу даних та виявлення закономірностей. Вона може навчитися на основі історичних даних про стан системи та розпізнавати патерни або ознаки, що вказують на проблеми. Модель може бути тренована на великій кількості даних для досягнення кращої точності та надійності.

5. Фізична модель базується на фізичних принципах та математичних моделях, що описують поведінку системи. Вона використовує рівняння, формули та моделі, щоб аналізувати та прогнозувати роботу системи. Наприклад, можуть бути створені фізичні моделі передачі даних, розподілу ресурсів або потоку трафіку в мережі для діагностики стану [4].

Усі моделі можуть бути використані окремо або в поєднанні одна з одною для ефективної діагностики стану складних систем. Вибір певної моделі залежить від характеристик системи, наявних даних та конкретних вимог до діагностики.

1.4. Застосування моделей діагностики стану складних систем у різних галузях

Застосування моделей діагностики стану складних систем є широким і розмаїтим у різних галузях. Ці моделі використовуються для аналізу, моніторингу та прогнозування роботи систем з метою виявлення несправностей, оптимізації режимів роботи, підвищення надійності та забезпечення безпеки. Розглянемо деякі приклади застосування моделей діагностики стану складних систем у різних галузях.

1. Телекомунікації. Моделі діагностики в телекомунікаційних системах використовуються для моніторингу та аналізу мережевих інфраструктур. Вони дозволяють виявляти проблеми зі з'єднанням,

перевантаженням мережі, несправностями обладнання, а також виявляти потенційні загрози безпеці та кібератаки. Моделі діагностики стану телекомунікаційних систем допомагають операторам мереж забезпечувати безперебійну роботу та якість обслуговування.

2. Енергетика. У сфері енергетики моделі діагностики стану використовуються для аналізу та моніторингу енергетичних систем, таких як електростанції чи розподільчі мережі. Вони допомагають виявляти несправності, проблеми зі збереженням енергії та оптимізувати режими роботи. Ці моделі також можуть прогнозувати можливі відмови або аварії, що сприяє забезпеченню безпеки та надійності енергетичних систем.

3. Автомобілебудування. Моделі діагностики стану застосовуються в автомобілебудуванні для аналізу роботи автомобільних систем та компонентів. Вони дозволяють виявляти несправності, відступи від нормальних параметрів та допомагають забезпечити надійну роботу транспортних засобів. Застосування моделей діагностики стану допомагає зменшити витрати на обслуговування, виявити потенційні проблеми та забезпечити безпеку пасажирів.

4. Медицина. Моделі діагностики стану складних систем знайшли широке застосування в медицині. Вони використовуються для діагностики хвороб, прогнозування ризиків та моніторингу пацієнтів. Наприклад, моделі діагностики можуть аналізувати медичні дані та симптоми для виявлення хвороб, а також прогнозувати хід хвороби і рекомендувати відповідні лікування.

5. Промисловість. Моделі діагностики стану застосовуються в промисловості для моніторингу та аналізу роботи виробничих систем та обладнання. Вони дозволяють виявляти несправності, відхилення від норми, прогнозувати можливі відмови та оптимізувати процеси виробництва. Застосування моделей діагностики стану допомагає забезпечити ефективну та безпечну роботу промислових систем.

6. Аерокосмічна промисловість. У галузі аерокосмічної промисловості моделі діагностики стану використовуються для аналізу роботи літаків, ракет, супутників та інших аерокосмічних систем. Вони дозволяють виявляти потенційні проблеми з обладнанням, відступи від нормальних параметрів, прогнозувати можливі відмови та забезпечувати безпеку польотів.

7. Інформаційна безпека. Моделі діагностики стану застосовуються в галузі інформаційної безпеки для виявлення загроз, вразливостей та атак на комп'ютерні системи та мережі. Вони допомагають виявити незвичайну активність, вторгнення або шкідливі програми, а також прогнозувати майбутні кіберзагрози.

8. Фінансовий сектор. У фінансовому секторі моделі діагностики стану використовуються для аналізу фінансових систем, ринків та ризиків. Вони допомагають виявляти аномальну поведінку, маніпуляції на фінансових ринках, ризикові ситуації та можливі шахрайства. Моделі діагностики стану також застосовуються для прогнозування руху цін на ринках та розробки стратегій управління ризиками.

9. Машинобудування. У машинобудуванні моделі діагностики стану використовуються для аналізу та моніторингу роботи промислового обладнання, машин та механізмів. Вони дозволяють виявляти несправності, відхилення від норми, прогнозувати можливі поломки та забезпечувати ефективну роботу виробничих процесів.

10. Транспорт. Моделі діагностики стану використовуються в транспортній галузі для аналізу та моніторингу роботи транспортних систем, таких як залізниці, метро, автобусні маршрути та логістичні мережі. Вони допомагають виявляти перебої в роботі, затримки, несправності обладнання, оптимізувати рух транспорту та планування маршрутів.

Ці приклади демонструють широкі можливості застосування моделей діагностики стану складних систем у різних галузях. Вони допомагають

підвищити надійність, безпеку та ефективність роботи систем, зменшити витрати на обслуговування та запобігти можливим проблемам [6].

Застосування моделей діагностики стану складних систем є необхідним у різних галузях. Ці моделі допомагають виявляти несправності, оптимізувати роботу систем, забезпечувати надійність, безпеку та ефективність роботи систем, зменшити витрати на обслуговування та запобігти можливим проблемам. Розуміння застосування моделей діагностики стану у різних галузях сприяє подальшому розвитку технологій та вдосконаленню роботи складних систем.

Висновки до розділу 1

У даному розділі було проведено огляд підходів, моделей і методів для діагностики стану складних систем, зокрема локальних комп'ютерних мереж.

Було розглянуто поняття та класифікацію складних систем. Складні системи характеризуються великою кількістю елементів та взаємодій між ними, що призводить до зростання їх складності та потреби у систематичному аналізі та діагностиці.

Також було висвітлено методи діагностики стану складних систем. Ці методи включають аналіз параметрів системи, виявлення аномалій та відхилень від норми, використання статистичних методів, машинного навчання та інших алгоритмів для виявлення проблемних областей і прогнозування виникнення проблем.

Розглянуті існуючі моделі діагностики стану складних систем. Ці моделі включають математичні, статистичні, IT- та системні підходи, що дозволяють описати структуру та функціонування системи, а також забезпечити її ефективну діагностику.

Було проаналізовано застосування моделей діагностики стану складних систем у різних галузях. Дослідження показали, що такі моделі мають широкий спектр застосування, включаючи інформаційні технології, транспорт, енергетику, медицину та багато інших сфер.

Отже, перший розділ надає загальний огляд підходів, моделей і методів для діагностики стану складних систем з фокусом на локальні комп'ютерні мережі. Це дозволяє визначити основні принципи та інструменти, які можна використовувати для розробки моделі діагностики стану локальної комп'ютерної мережі у подальших розділах дипломної роботи.

РОЗДІЛ 2. РОЗРОБКА ВЛАСНОЇ МОДЕЛІ ДІАГНОСТИКИ СТАНУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1. Аналіз особливостей та проблем локальних комп'ютерних мереж

Локальна комп'ютерна мережа є важливою складовою сучасних організацій та підприємств. Вона дозволяє забезпечити зв'язок між різними комп'ютерами, пристроями та серверами всередині однієї фізичної локалізації. Аналіз особливостей та проблем локальних комп'ютерних мереж є важливим кроком у розробці моделі діагностики стану такої мережі.

1. Фізична інфраструктура включає всі фізичні компоненти, необхідні для побудови локальної комп'ютерної мережі. Це включає в себе кабелі, комутатори (switches), маршрутизатори (routers), концентратори (hubs), роз'єми, панелі підключення, а також активні та пасивні мережеві пристрої.

Проблеми, пов'язані з фізичною інфраструктурою, можуть включати:

1) пошкодження або неправильне підключення кабелів: кабелі можуть бути пошкоджені в результаті фізичних пошкоджень, перетискання або неправильного підключення. Це може призвести до втрати з'єднання або зниження швидкості передачі даних;

2) перенавантаження комутаторів: комутатори можуть стикатися з великою кількістю пакетів даних, що проходять через них, особливо в ситуаціях, коли мережа має велику кількість підключених пристроїв або використовується для інтенсивного передачі даних. Це може призвести до затримок у мережі та погіршення швидкості передачі;

3) недостатня пропускна здатність мережі: якщо мережа не має достатньої пропускної здатності, це може призвести до обмежень у

швидкості передачі даних або недоступності ресурсів для підключених пристроїв;

4) проблеми з електропостачанням: неправильне або нестабільне електропостачання може спричинити відключення мережевих пристроїв або перебої в роботі. Це може вплинути на доступність мережі та її надійність.

Аналіз фізичної інфраструктури допомагає виявити такі проблеми, та за результатами аналізу можуть бути запропоновані відповідні заходи, такі як заміна пошкоджених кабелів, додаткова налаштування комутаторів або підвищення надійності електропостачання [7].

2. Конфігурація та налаштування локальної комп'ютерної мережі грають важливу роль у забезпеченні її ефективної роботи. Неправильна конфігурація та налаштування можуть призвести до проблем зі зв'язком між комп'ютерами, недоступності ресурсів, конфліктів IP-адрес та інших мережевих проблем.

Проблеми, пов'язані з конфігурацією та налаштуванням, можуть включати:

– неправильну IP-адресацію: конфлікти IP-адрес можуть виникати, коли два або більше пристроїв в мережі мають однакову IP-адресу. Це призводить до втрати з'єднання та недоступності мережевих ресурсів;

– несумісність протоколів: різні пристрої в мережі можуть використовувати різні мережеві протоколи. Якщо налаштування протоколів несумісні, це може призвести до проблем зі зв'язком та передачею даних між пристроями;

– недостатній розподіл пропускної здатності: якщо пропускна здатність мережі неправильно розподілена між пристроями, це може призвести до нерівномірного доступу до ресурсів та зниження швидкості передачі даних;

– несправні налаштування безпеки: неправильні налаштування безпеки можуть призвести до вразливості мережі перед зловмисниками, втрати конфіденційної інформації та несанкціонованого доступу до ресурсів.

Аналіз конфігурації та налаштування локальної комп'ютерної мережі включає перевірку правильності налаштувань IP-адрес, мережевих протоколів, розподілу пропускної здатності та налаштувань безпеки. Після аналізу можуть бути запропоновані відповідні коригування налаштувань для забезпечення оптимальної роботи мережі та забезпечення безпеки даних.

3. Безпека мережі. Однією з найважливіших проблем, з якими стикаються локальні комп'ютерні мережі, є забезпечення безпеки. Безпека мережі стає особливо важливою в контексті зростання кількості загроз інформаційній безпеці, таких як несанкціонований доступ, зловживання, віруси та інші шкідливі програми.

Проблеми, пов'язані з безпекою локальної комп'ютерної мережі, можуть включати:

– недостатня аутентифікація та авторизація: слабкі аутентифікаційні методи та недостатні механізми авторизації можуть дозволити несанкціонованим особам отримати доступ до мережі та цінних ресурсів. Це може призвести до втрати конфіденційної інформації та порушення нормативних вимог;

– вразливості мережевих пристроїв: несправність безпеки на мережевих пристроях, таких як маршрутизатори, комутатори, фаєрволи тощо, може стати причиною атак ззовні або внутрішніх загроз, що можуть нанести шкоду мережі та даним;

– несправність мережевих політик: несправність або неправильна конфігурація мережевих політик може призвести до недостатньої

сегментації мережі, недостатньої фільтрації трафіку та інших проблем, що збільшують ризик компрометації мережі;

– віруси та шкідливі програми: Наявність вірусів, шкідливого програмного забезпечення або шпигунського ПЗ може призвести до пошкодження або втрати даних, порушення приватності та сповільнення мережі [2].

Аналіз безпеки мережі допомагає виявити потенційні вразливості та загрози безпеці, перевірити правильність налаштування мережевих пристроїв, аутентифікаційних механізмів та інших безпечних політик. За результатами аналізу можуть бути запропоновані заходи, такі як підвищення рівня аутентифікації та авторизації, встановлення файрволів, шифрування даних, регулярне оновлення програмного забезпечення та навчання персоналу щодо безпеки мережі.

4. Пропускна здатність та навантаження є важливими факторами для ефективної роботи локальної комп'ютерної мережі. Пропускна здатність визначає максимальний обсяг даних, який може бути переданий через мережу за певний проміжок часу, тоді як навантаження вказує на рівень використання цієї пропускної здатності.

Проблеми, пов'язані з пропускною здатністю та навантаженням, можуть включати такі пункти:

– недостатня пропускна здатність: якщо мережа має недостатню пропускну здатність для обсягу даних, що передаються, це може призвести до затримок у передачі, низької швидкості та недостатньої продуктивності мережі;

– навантаження на мережеві пристрої: якщо певні мережеві пристрої, такі як комутатори або маршрутизатори, перевантажені, це може стати причиною збоїв, втрати пакетів даних та зниження швидкості передачі. Такі ситуації можуть виникати, коли кількість підключених пристроїв або обсяг передаваної інформації перевищують можливості мережевих пристроїв;

– нерівномірне навантаження мережі: якщо навантаження мережі не розподілене рівномірно, деякі сегменти або пристрої можуть бути перевантажені, тоді як інші можуть мати низьке використання ресурсів. Це може призвести до недоступності ресурсів та незадовільної продуктивності для деяких користувачів;

– збої в мережевих послугах: надмірне навантаження мережі або проблеми з мережевими пристроями можуть призвести до зниження якості обслуговування, перебоїв у роботі додатків та послуг, недоступності важливих ресурсів.

Аналіз пропускної здатності та навантаження локальної комп'ютерної мережі включає вимірювання швидкості передачі даних, моніторинг завантаження мережевих пристроїв та ідентифікацію можливих точок перевантаження. На основі аналізу можуть бути запропоновані заходи для оптимізації пропускної здатності, такі як налаштування QoS (Quality of Service), розподіл навантаження або підвищення потужності мережевих пристроїв.

5. Моніторинг та діагностика є важливими етапами у виявленні проблем та забезпеченні ефективної роботи локальної комп'ютерної мережі. Ці процеси дозволяють адміністраторам мережі відстежувати стан мережі, виявляти аномалії та проблеми, виконувати аналіз використання ресурсів та приймати вчасні заходи для вирішення проблем.

Проблеми, пов'язані з моніторингом та діагностикою, можуть включати:

– недостатня видимість мережі: відсутність централізованої системи моніторингу та діагностики може ускладнити виявлення проблем та вчасну реакцію на них. Важливо мати доступ до інструментів моніторингу, які забезпечують детальну інформацію про стан мережі, ресурси та використання;

– великий обсяг даних: у великих мережах може виникати проблема з обробкою та аналізом великого обсягу мережевих даних. Це може призвести до втрати важливої інформації або затримок у виявленні проблем;

– неправильна інтерпретація даних: недостатня експертиза адміністраторів мережі у сфері аналізу даних може призвести до неправильної інтерпретації результатів моніторингу та діагностики. Це може вплинути на прийняття неправильних рішень щодо вирішення проблем;

– відсутність автоматизації: ручний моніторинг та діагностика може бути трудомістким та часовомістким процесом. Важливо мати автоматизовані інструменти для збору даних, аналізу та сповіщення про проблеми, що дозволить знизити час реакції на виникнення проблем та прискорити їх вирішення.

Аналіз моніторингу та діагностики локальної комп'ютерної мережі включає встановлення системи моніторингу, налаштування сповіщень та тривіальних правил, аналіз зібраних даних та виявлення аномалій. Інструменти моніторингу можуть включати системи збору журналів подій, мережеві аналізатори, монітори ресурсів та інші програми.

На основі аналізу моніторингу та діагностики можуть бути запропоновані заходи для поліпшення ефективності та надійності мережі. Це можуть бути такі кроки, як оптимізація налаштувань мережевих пристроїв, виявлення і усунення точок перевантаження, встановлення механізмів моніторингу безпеки та автоматичного відновлення мережі [8].

Загалом, моніторинг та діагностика локальної комп'ютерної мережі грають ключову роль у підтримці її безперебійної роботи, виявленні проблем та своєчасному реагуванні на них. Це дозволяє забезпечити надійну та ефективну роботу мережі, зменшити витрати на технічне обслуговування та забезпечити задоволення потреб користувачів.

2.2. Вибір та обґрунтування методу діагностики стану локальної комп'ютерної мережі

Стан локальної комп'ютерної мережі є важливим аспектом її функціонування і ефективності. Якщо проблеми виникають в мережі, це може призвести до перебоїв у роботі системи, зниження швидкості передачі даних та втрати продуктивності. Тому важливо мати ефективні методи діагностики, які дозволять оперативно виявити та вирішити проблеми в мережі.

Перш ніж обрати метод діагностики стану локальної комп'ютерної мережі, слід провести аналіз існуючих методів. Певні методи включають:

1) перевірка доступності вузлів мережі. Полягає у відправленні спеціальних пакетів (ping-запитів) до кожного вузла мережі з метою визначити, чи є вони доступними. Він дозволяє виявити проблеми зі з'єднанням, такі як розриви в кабелі або несправність мережевого пристрою. Однак, цей метод не здатний виявити проблеми, які виникають в мережевому обладнанні, наприклад, збої в комутаторах або маршрутизаторах;

2) моніторинг мережі. Метод моніторингу полягає у використанні спеціального програмного забезпечення, яке постійно контролює стан мережі. Воно збирає дані про роботу мережевих пристроїв, пропускну здатність, використання ресурсів та інші параметри. Цей метод може надати важливу інформацію про загальний стан мережі, але не завжди здатний виявити конкретні проблеми або дати детальну діагностику;

3) аналіз мережевого трафіку. Цей метод включає моніторинг і аналіз мережевого трафіку з метою виявлення аномальних патернів, збоїв у передачі даних, надмірного навантаження мережі та інших проблем. Він може дати детальну інформацію про причини проблем та забезпечити точну

діагностику, але вимагає відповідних знань та спеціалізованого програмного забезпечення.

З урахуванням аналізу існуючих методів, для діагностики стану локальної комп'ютерної мережі в рамках даної дипломної роботи використовувалось поєднання методів моніторингу мережі та аналізу мережевого трафіку.

Моніторинг мережі надасть загальну картину стану мережі, включаючи пропускну здатність, використання ресурсів та статус пристроїв. Це допоможе виявити загальні проблеми та перевантаження мережі.

Аналіз мережевого трафіку дозволить отримати детальну інформацію про саме передачу даних, забезпечить виявлення аномалій та причин проблем. Застосування спеціалізованого програмного забезпечення для аналізу мережевого трафіку дозволить провести глибоку діагностику та ідентифікувати проблемні ділянки мережі [7].

Вибір поєднання методів моніторингу мережі та аналізу мережевого трафіку обґрунтовується їхніми перевагами та синергетичним ефектом. Моніторинг мережі забезпечить загальну оцінку стану мережі та ідентифікацію загальних проблем, тоді як аналіз мережевого трафіку дозволить провести детальну діагностику та виявити конкретні причини проблем.

Крім того, поєднання цих методів забезпечить більш точну та комплексну діагностику, що дозволить ефективно вирішувати проблеми в мережі та підвищувати її продуктивність.

2.3 Побудова математичної моделі діагностики стану локальної комп'ютерної мережі

Для діагностики стану локальної комп'ютерної мережі, що складається з 3 роутерів, з'єднаних між собою, від кожного з яких йде switch, з

підключеними комп’ютерами в кількості від 3 до 5 штук(загальна кількістть яких складає 12).

Визначення змінних:

– R1, R2, R3: стан роутерів 1, 2 та 3 відповідно (1 – працює, 0 – не працює).

– S1, S2, S3: стан комутаторів, які з'єднують роутери 1, 2 та 3 відповідно (1 – працює, 0 – не працює).

– C1, C2, ..., C12: стан комп'ютерів 1, 2, ..., 12 відповідно (1 – працює, 0 – не працює).

Визначення функцій:

– f(R1, R2, R3) = (R1 AND R2 AND R3). Функція f визначає стан локальної мережі залежно від стану роутерів;

– g(S1, S2, S3) = (S1 AND S2 AND S3). Функція g визначає стан локальної мережі залежно від стану комутаторів;

– h(C1, C2, ..., C12) = (C1 AND C2 AND ... AND C12). Функція h визначає стан локальної мережі залежно від стану комп'ютерів.

Визначення функції діагностики:

D(R1, R2, R3, S1, S2, S3, C1, C2, ..., C12) = f(R1, R2, R3) AND g(S1, S2, S3) AND h(C1, C2, ..., C12).

Функція D визначає стан локальної мережі на основі стану роутерів, комутаторів та комп'ютерів. Вона повертає 1, якщо мережа працює належним чином, і 0 в іншому випадку.

Функція f враховує, що мережа може працювати, якщо всі роутери працюють.

Функція g враховує, що мережа працює, якщо всі комутатори працюють.

Функція h враховує, що мережа працює, якщо всі комп'ютери працюють.

Для діагностики стану локальної мережі, потрібно зібрати дані про стан роутерів, комутаторів та комп'ютерів.

На основі зібраних даних можна використовувати функцію D для визначення стану мережі.

Якщо D повертає 1, то мережа працює належним чином, якщо D повертає 0, то мережа має проблеми, і необхідно провести подальшу діагностику для виявлення причин несправностей.

2.4. Реалізація моделі локальної комп'ютерної мережі

Для реалізації моделі локальної комп'ютерної мережі було використано 3 роутери та комутатори. Схема мережі (рис. 2.1) має таку структуру:

- роутер 1 підключений до комутатора 1.
  - комп'ютер 1 підключений до порту 1 на комутаторі 1;
  - комп'ютер 2 підключений до порту 2 на комутаторі 1;
  - комп'ютер 3 підключений до порту 3 на комутаторі 1;
  - комп'ютер 4 підключений до порту 4 на комутаторі 1;
- роутер 2 підключений до комутатора 2.
  - комп'ютер 5 підключений до порту 1 на комутаторі 2;
  - комп'ютер 6 підключений до порту 2 на комутаторі 2;
  - комп'ютер 7 підключений до порту 3 на комутаторі 2;
  - комп'ютер 8 підключений до порту 4 на комутаторі 2;
  - комп'ютер 9 підключений до порту 5 на комутаторі 2;
- роутер 3 підключений до комутатора 3.
  - комп'ютер 10 підключений до порту 1 на комутаторі 3;
  - комп'ютер 11 підключений до порту 2 на комутаторі 3;
  - комп'ютер 12 підключений до порту 3 на комутаторі 3.

Кожен роутер використовується для маршрутизації даних між мережевими підсистемами та забезпечення з'єднання з іншими мережами. Комутатори використовуються для забезпечення з'єднання між комп'ютерами в межах мережі. Кожен комп'ютер має свій унікальний номер IP-адреси та використовується для обміну даними в мережі.

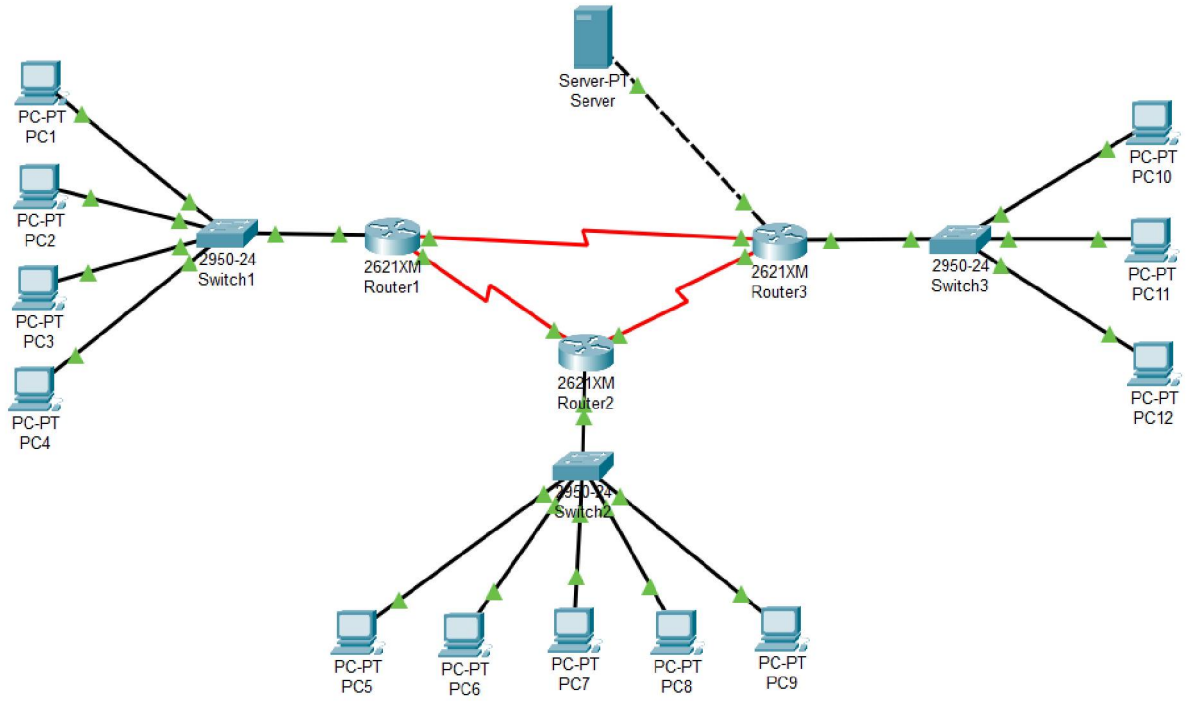

Рисунок 2.1 – Модель локальної комп’ютерної мережі

Ця модель локальної комп'ютерної мережі забезпечує високу швидкість передачі даних та ефективне керування мережевим трафіком. Комп'ютери можуть спілкуватися між собою та отримувати доступ до ресурсів мережі за допомогою цієї мережевої інфраструктури.

Використання такої моделі локальної комп'ютерної мережі дозволяє забезпечити ефективне функціонування мережі та задовольнити потреби користувачів у швидкому та надійному з'єднанні.

Також важно відмітити, що вибір кількості роутерів та комутаторів був здійснений з метою підтримки потреб мережі заздалегідь визначеної кількості комп'ютерів. У даному випадку, перший комутатор підключає 4

комп'ютери, другий – 5, а третій – 3, що загалом складає 12 комп'ютерів у мережі.

Така конфігурація мережі забезпечує можливість встановлення з'єднань між будь-якими комп'ютерами у мережі за допомогою відповідних IP-адрес та мережевих протоколів. Роутери відповідають за маршрутизацію даних між різними мережевими підсистемами, тоді як комутатори забезпечують комутацію даних в межах мережі.

Важливою складовою цієї моделі є вибір IP-адрес для кожного комп'ютера та налагодження правильного налаштування мережевих протоколів, щоб забезпечити правильну роботу всієї мережі.

Ця модель локальної комп'ютерної мережі є надійною та масштабованою, що дозволяє задовольнити потреби користувачів у швидкому обміні даними та ресурсах мережі. Завдяки цій інфраструктурі, користувачі можуть працювати ефективно та спілкуватися один з одним без перешкод.

Висновки до розділу 2

У даному розділі було проведено аналіз особливостей та проблем, що виникають у локальних комп'ютерних мережах. Виявлено такі проблеми, як перевантаження мережі, втрата пакетів даних, проблеми зі з'єднанням та інші, які можуть впливати на продуктивність та стабільність мережі.

Було здійснено вибір та обґрунтування методу діагностики стану локальної комп'ютерної мережі. При виборі методу враховувалися особливості мережі, доступні ресурси та вимоги до точності та ефективності діагностики. Обрано метод, який найкращим чином відповідає потребам і можливостям досліджуваної мережі.

Проведено побудову математичної моделі для діагностики стану локальної комп'ютерної мережі. Математична модель дозволяє описати структуру мережі та виявляти потенційні проблеми в її функціонуванні.

Реалізовано модель локальної комп'ютерної мережі, що базується на розробленій математичній моделі. У процесі реалізації було використано відповідні програмні засоби та технології для створення функціонального прототипу моделі. Реалізація дозволяє проводити експерименти та тестування, щоб перевірити працездатність та ефективність моделі.

Отже, розділ "Розробка власної моделі та діагностика стану локальної комп'ютерної мережі" надає детальний огляд аналізу особливостей та проблем локальних комп'ютерних мереж, обґрунтування вибору методу діагностики, побудову математичної моделі та реалізацію моделі. Цей розділ є основою для подальшого дослідження та вдосконалення діагностики стану локальних комп'ютерних мереж у наступних розділах дипломної роботи.

РОЗДІЛ 3. АНАЛІЗ ВІДМОВ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1. Формулювання задачі виділення відмов локальної комп'ютерної мережі

Дерево відмов (або дерево відмов та відновлення, або Fault Tree Analysis – FTA) – це аналітичний метод, який використовується для моделювання ймовірностей відмов комплексних систем і визначення їх надійності. Дерево відмов дозволяє ідентифікувати потенційні причини відмов, визначити ймовірності відмови системи в цілому та окремих її компонентів, а також оцінити вплив окремих факторів на загальну надійність системи.

Процес розробки дерева відмов включає кілька кроків, які допомагають інженерам систематично аналізувати ймовірність відмов компонентів та системи в цілому. Ось загальна структура процесу розробки дерева відмов:

1. Визначення мети аналізу: перший крок – це визначення мети аналізу дерева відмов. Це може включати в себе виявлення ключових ризиків, ідентифікацію критичних компонентів, оцінку надійності системи або розробку стратегій поліпшення надійності. Визначення мети допоможе зорієнтуватися під час розробки дерева відмов.

2. Вибір системи та компонентів: другий крок – це вибір системи, яку необхідно проаналізувати, та ідентифікація компонентів, які складають цю систему. Це може включати аналіз існуючої системи або проектування нової системи. Важливо точно визначити компоненти, щоб побудувати дерево відмов на основі їх взаємозв'язків та впливу на надійність системи.

3. Декомпозиція системи: третій крок – це декомпозиція системи на більш прості компоненти або функціональні блоки. Це включає ідентифікацію подій або станів, які можуть спричинити відмову системи.

Компоненти та їх зв'язки можуть бути представлені у вигляді вузлів та гілок дерева відмов.

4. Визначення ймовірностей відмов: четвертий крок – це оцінювання ймовірностей відмов для кожного компонента або події у дереві відмов. Це може включати використання статистичних даних про відмови компонентів, експертні оцінки або моделювання системи. Метою цього кроку є отримання об'єктивних оцінок ймовірностей відмов для подальшого аналізу.

5. Аналіз дерева відмов: п'ятий крок – це аналіз дерева відмов для виявлення критичних шляхів, ключових компонентів та оцінки загальної надійності системи. Це включає ідентифікацію критичних шляхів, дослідження впливу окремих компонентів на загальну надійність та оцінку надійності системи за допомогою аналітичних методів або симуляцій.

6. Розробка стратегій поліпшення: останній крок – це розробка стратегій поліпшення надійності системи на основі результатів аналізу дерева відмов. Це може включати рекомендації щодо додаткового тестування, змін в конструкції або використання резервування компонентів. Метою цього кроку є прийняття рішень, які допоможуть забезпечити оптимальну надійність та безпеку системи.

Дерево відмов складається з кореня, вузлів і листків. Корінь представляє собою систему, а вузли відображають події або стани, які можуть спричинити відмову системи. Листки відповідають кінцевим станам системи, які вважаються відмовою. На рис. 3.1 дерево відмов для локальної мережі, що згадувалась вище у роботі.

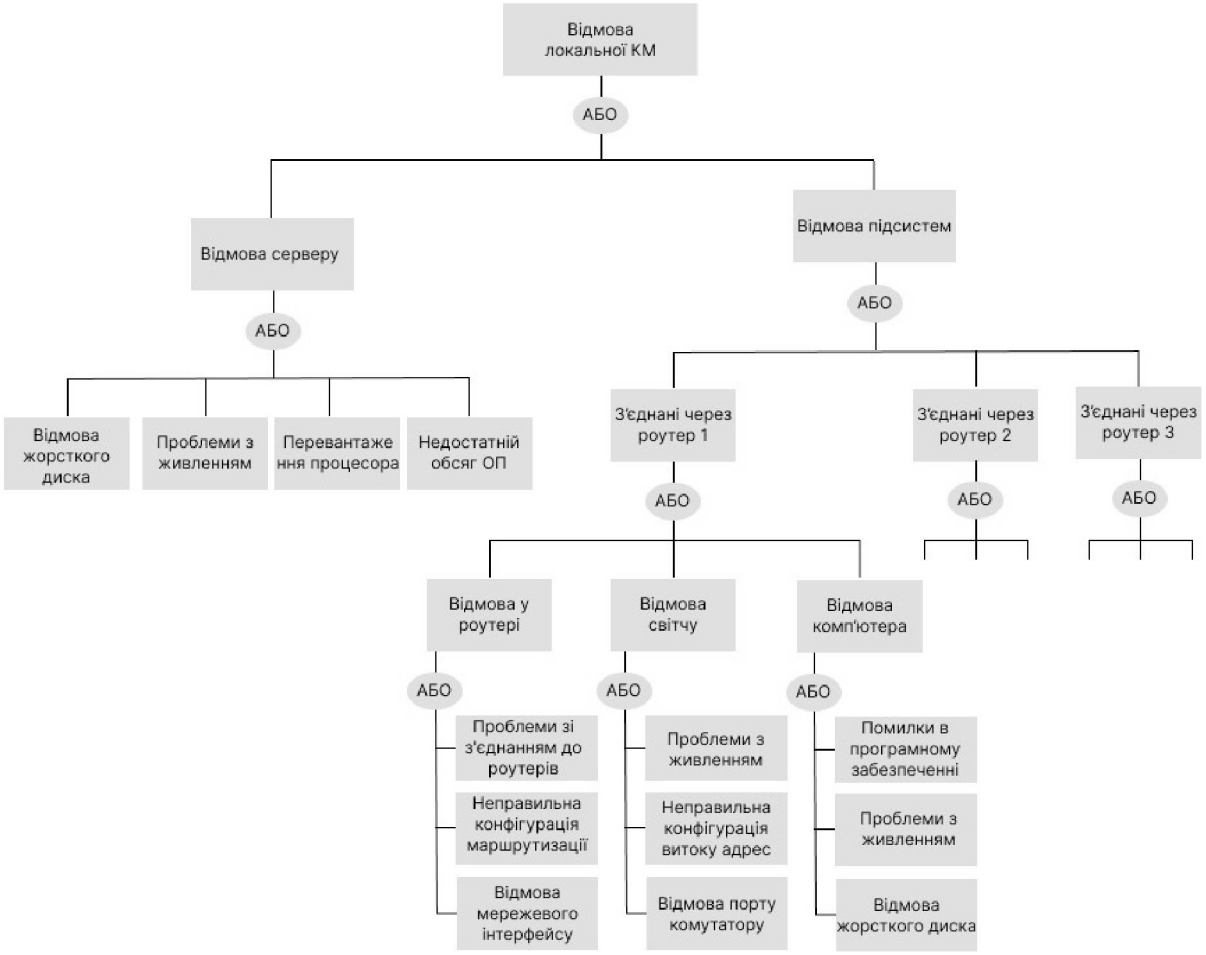

Рисунок 3.1 – Дерево відмов для локальної комп’ютерної мережі

Побудова дерева відмов є важливим інструментом для аналізу та управління ризиками в складних системах. Цей процес дозволяє ідентифікувати потенційні вразливості, причини відмов та їх можливі наслідки. Використання дерева відмов допомагає визначити критичні шляхи та події, які можуть призвести до небажаних результатів, що дає можливість розробити стратегії запобігання та управління ризиками. Цей аналітичний підхід є корисним як для планування передбачуваних ризиків, так і для виявлення потенційних проблем, що допомагає покращити надійність та ефективність системи. Побудова дерева відмов також сприяє ідентифікації критичних компонентів системи, які можуть бути причиною відмов. Це дозволяє зосередитись на цих компонентах для забезпечення високої надійності та підвищення рівня безпеки системи в цілому. Крім

того, дерево відмов може бути використане для оцінки впливу різних заходів запобігання та відновлення на загальний стан системи, допомагаючи вибрати оптимальні стратегії для зниження ризику та мінімізації втрат у разі виникнення відмов [9]. Умовна схема побудови дерева відмов та приклад дерева відмов зображені на рис. 3.2 – 3.3.

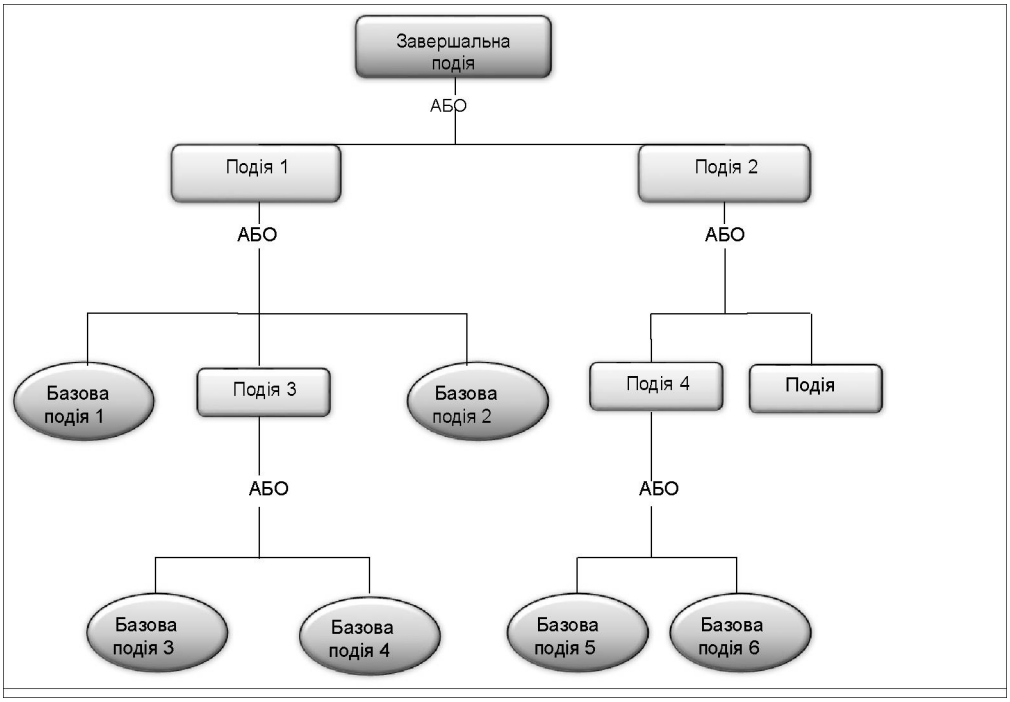

Рисунок 3.2. – Приклад діаграми дерева відмов

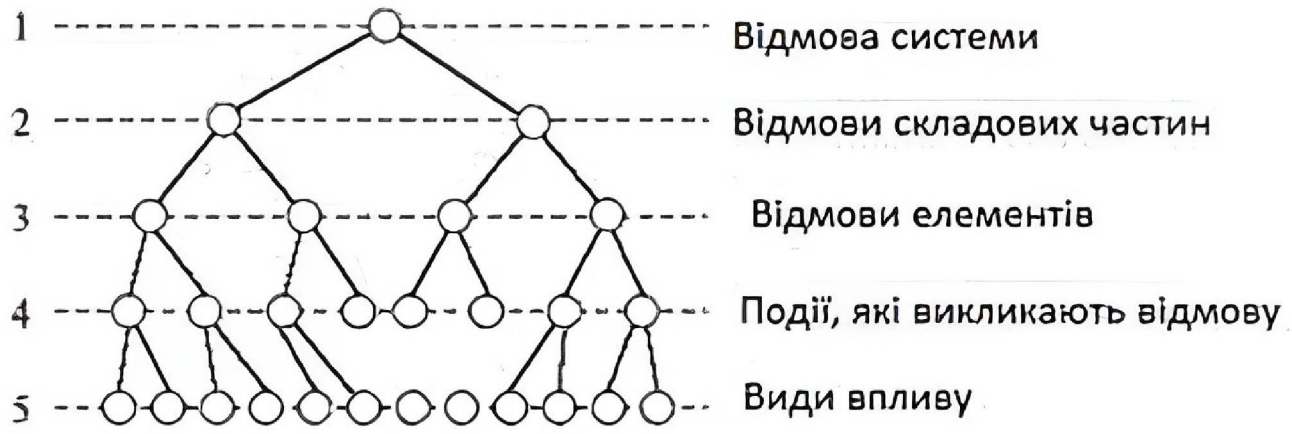

Рисунок 3.3 – Умовна схема побудови дерева відмов

При створенні дерева відмов проводиться декомпозиція системи на компоненти, а потім аналізується вплив кожного компонента на надійність системи в цілому. Для цього використовуються різні логічні оператори, такі як І (AND), АБО (OR) та НЕ (NOT).

Логічний оператор І (AND) використовується, коли відмова системи залежить від одночасної відмови всіх підкомпонентів. Наприклад, якщо система складається з трьох компонентів, і всі три повинні працювати належним чином, щоб система функціонувала, то логічний оператор І (AND) використовується для з'єднання цих компонентів.

Логічний оператор АБО (OR) використовується, коли відмова системи може статися за умови відмови хоча б одного з підкомпонентів. Наприклад, якщо система має дублюючі компоненти, і достатньо, щоб працював хоча б один з них, щоб система продовжувала працювати, то логічний оператор АБО (OR) використовується.

Логічний оператор НЕ (NOT) використовується для вираження надійності компонентів, які працюють в протилежному напрямку. Наприклад, якщо відмова системи залежить від того, щоб два компоненти не працювали одночасно, то логічний оператор НЕ (NOT) використовується для з'єднання цих компонентів [9].

Інформація про надійність компонентів системи (ймовірності відмови) може бути отримана з різних джерел, таких як статистика відмов, експертні оцінки, результати тестування тощо. Ці дані використовуються для побудови ймовірнісних моделей дерева відмов.

3.2 Оцінка дерева відмов

Під час оцінки дерева відмов визначають обставини, за яких може статись кожна з наступних подій. На основі розроблення цих визначень також оцінюється відносна можливість чи ймовірність появи цих незалежних чи можливих подій. Ймовірність знаходять з результатів

випробувань, досвіду, опублікованих даних, записів відмов, поломок чи експертною оцінкою. Ця можливість вихідних подій безпосередньо над наступною (нижньою) подією потім визначається з ймовірності відмови.

У нашому випадку визначимо для компонентів значення ймовірності відмови компонентів. Задаємо такі значення:

P1: Відмова Router 1 [0.05];

P2: Відмова Switch 1 [0.1];

P3: Відмова PC 1 [0.08];

P4: Відмова Switch 2 [0.15];

P5: Відмова PC 6 [0.07];

P6: Відмова Switch 3 [0.12];

P7: Відмова PC 11 [0.09].

Для розрахунку загальної ймовірності відмови системи можна використовувати формулу множення ймовірностей для незалежних подій.

Ймовірність відмови системи можна розрахувати таким чином:

P(відмова системи) = 1 - P(жодної відмови),

P(жодної відмови) = (1 - P1) * (1 - P2) * (1 - P3) * (1 - P4) * (1 - P5) * (1 - P6) * (1 - P7).

Заміняючи значення ймовірностей, отримуємо:

P(жодної відмови) = (1 - 0.05) * (1 - 0.1) * (1 - 0.08) * (1 - 0.15) * (1 - 0.07) * (1 - 0.12) * (1 - 0.09).

Підраховуючи значення, отримуємо:

P(жодної відмови) ≈ 0.38417.

Тепер можна розрахувати загальну ймовірність відмови системи:

P(відмова системи) ≈ 1 - 0.38417 ≈ 0.61583.

Отже, загальна ймовірність відмови системи локальної комп'ютерної мережі складає приблизно 0.61583 або 61.583%.

Процес (оцінка) продовжується вверх по дереву до тих пір, поки не буде визначено можливість небажаної події, яка показана на вершині

дерева. При побудові і спрощенні ймовірностей дерева відмов можуть бути використані математичні методи, які дають змогу виконати їх кількісну оцінку [10]. Необхідно визначити багато чинників: загальну ймовірність небажаної події; комбінацію подій, які найбільш ймовірно призведуть до небажаної події; події, що найбільше сприяють цій комбінації, а також найбільш ймовірні наслідки події чи шляхи до вершини дерева відмов. Ймовірність відмови на будь-якому рівні P(t) може бути розраховано за допомогою наступних рівнянь:

– для входів АБО дерева відмов:

$$P(t) = \sum_{i=1}^{n} P_i(t) = \sum_{i=1}^{n} 1 - R_i(t), \qquad (3.1)$$

– для входів І дерева відмов:

$$P(t) = \prod_{i=1}^{n} P(t) = \prod_{i=1}^{n} 1 - R_i(t), \qquad (3.2)$$

$$R_i(t) = e^{-\lambda_i t},$$

де $P_i(t)$ – ймовірність відмови і-го компонента на наступному нижньому рівні;

$R_i(t)$ – ймовірність безвідмовної роботи і-го компонента;

t – час роботи компонента;

λ_i – інтенсивність відмов і-го компонента (константа оцінки, отримана на основі досвіду експлуатації об’єкта);

n – кількість компонентів на наступному нижньому рівні.

Ймовірність безвідмовної відмови системи $R_c(t)$ визначається використанням ймовірності відмови системи $P_c(t)$:

$$R_c(t) = 1 - P_c(t). \qquad (3.3)$$

Використовуючи таку методику оцінки, надійність будь-якої системи може бути оцінена у ймовірнісному аспекті, і це може бути використано для керування операціями і прийняттям рішення. На основі оцінки дерева відмов можна визначити появу події, яка може призвести до небажаного порушення роботи. Таким чином відносно просто ідентифікувати події, які треба уникнути і робити вплив, щоб зменшити небажану подію.

Одним з ключових аспектів дерев відмов є оцінювання ймовірностей відмов компонентів та системи в цілому. Він допомагає інженерам та дослідникам виявляти критичні компоненти, які можуть призвести до відмови всієї системи, і розробляти стратегії для підвищення надійності системи, такі як дублювання компонентів або запасні шляхи. Для цього можуть використовуватися різні підходи:

– статистичні дані. Використання статистичних даних про відмови компонентів або подібних систем може надати підставу для оцінювання ймовірностей відмов;

– експертні оцінки. Експерти з домену можуть надавати оцінки ймовірностей відмов на основі своїх знань та досвіду;

– моделювання системи. Використання математичних моделей для моделювання системи та розрахунку ймовірностей відмов.

У деревах відмов важливим поняттям є критичні шляхи. Критичний шлях – це послідовність подій або станів, які ведуть до відмови системи. Це шлях, на якому відмова може виникнути з найвищою ймовірністю. Ідентифікація та аналіз критичних шляхів допомагає зосередитись на найважливіших аспектах системи для поліпшення її надійності.

Для побудови дерев відмов і оцінювання ймовірностей відмов часто використовується статистика відмов компонентів або подібних систем [10]. Ця статистика може включати дані про час роботи до відмови (MTTF – Mean Time To Failure) та час відновлення після відмови (MTTR – Mean Time

To Repair). Використання такої статистики дозволяє зробити більш об'єктивні оцінки ймовірностей відмов.

У деревах відмов можна приділити особливу увагу компонентам, які мають велике значення для надійності системи. Ці компоненти, відмова яких може мати найбільший вплив на загальну надійність системи, називаються ключовими компонентами або вузлами. Ідентифікація та підвищення надійності цих ключових компонентів може бути пріоритетним завданням для поліпшення системи в цілому.

Дерева відмов дозволяють проводити аналіз чутливості, що означає визначення впливу окремих компонентів або факторів на загальну надійність системи. Це допомагає інженерам виявити найбільш вразливі або критичні компоненти та визначити, які зміни або покращення можуть мати найбільший вплив на надійність системи.

Також вони можуть мати різний рівень деталізації, від загального огляду системи до докладного аналізу окремих компонентів. Вибір рівня деталізації залежить від мети аналізу, наявної інформації та обсягу ресурсів, доступних для проведення аналізу.

Дерева відмов можуть бути інтегровані з іншими методами аналізу надійності, такими як аналіз ризиків, аналіз впливу та іншими. Це дозволяє отримати більш повне уявлення про надійність та безпеку системи та приймати більш обґрунтовані рішення.

Узагальнюючи, дерево відмов є потужним інструментом для аналізу надійності та безпеки комплексних систем. Воно дозволяє виявляти потенційні вразливості, прогнозувати ймовірності відмови та розробляти стратегії для поліпшення надійності та безпеки систем.

3.3 Рекомендації щодо покращення надійності та якості роботи локальної комп'ютерної мережі

Зважаючи на аналіз структури локальної комп'ютерної мережі, якій було надано детальний опис раніше, були розроблені рекомендації щодо покращення надійності та якості роботи мережі.

Під час вивчення системи було виявлено кілька потенційних проблем, які можуть призвести до відмов компонентів мережі. З метою забезпечення найвищого рівня надійності та оптимальної продуктивності мережі, наведені нижче рекомендації варто розглянути та впровадити:

– дублювання роутерів. Рекомендується розглянути можливість використання дублюючих роутерів для кожної підмережі. Це забезпечить резервний роутер, який автоматично візьме на себе функцію маршрутизації у випадку відмови основного роутера;

– застосування стабільного програмного забезпечення. Рекомендується переконатися, що використовуване програмне забезпечення для роутерів і свічів є стабільним і має останні оновлення. Регулярне оновлення програмного забезпечення допоможе уникнути відомих помилок та забезпечить оптимальну функціональність;

– забезпечення надійного живлення. Рекомендується використовувати безперебійні джерела живлення (UPS) для всіх компонентів мережі. Це допоможе уникнути відмов через непередбачені переривання живлення та забезпечить безперебійну роботу;

– регулярне резервне копіювання конфігурації. Рекомендується регулярно створювати резервні копії конфігурацій роутерів і свічів. Це дозволить відновити налаштування в разі відмови або неправильних змін у конфігурації;

– моніторинг та керування. Рекомендується використовувати систему моніторингу мережі для постійного відстеження стану компонентів, навантаження мережі та виявлення проблем з ранньою попереджувальною системою. Використовуйте системи керування

мережею для централізованого керування та налаштування компонентів мережі;

– захист від кібератак. Рекомендується встановити міжмережеві брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення для забезпечення захисту мережі від кібератак [11];

– регулярне обслуговування. Рекомендується регулярно проводити обслуговування компонентів мережі, включаючи перевірку стану кабелів, чистку пристроїв, перевірку роботи вентиляторів і систем охолодження. Це допоможе уникнути відмов через фізичні пошкодження або перегрів компонентів;

– навчання користувачів. Рекомендується проводити навчання користувачів з питань правильного використання мережі, безпеки та вирішення простих проблем. Це сприятиме зменшенню ризику помилок та покращенню продуктивності мережі.

Впровадження цих рекомендацій сприятиме покращенню надійності та якості роботи локальної комп'ютерної мережі. Застосування цих заходів буде сприяти забезпеченню безперебійної роботи мережі, зниженню ризику відмов та забезпеченню задоволення користувачів.

Висновки до розділу 3

У даному розділі була сформульована задача виділення відмов локальної комп'ютерної мережі. Задача полягає в оцінці ймовірності виникнення відмов та їх наслідків у мережі, що дозволяє виявляти потенційні проблеми та приймати заходи для запобігання або мінімізації їх впливу.

Була проведена оцінка дерева відмов, що допомагає визначити ймовірність виникнення відмов в окремих компонентах мережі та їх

взаємозв'язок. Це дозволяє ідентифікувати критичні елементи мережі, які можуть спричинити серйозні проблеми при виникненні відмов.

Також були надані рекомендації щодо покращення надійності та якості роботи локальної комп'ютерної мережі на основі отриманих результатів. Ці рекомендації можуть включати в себе зміни у конфігурації мережі, підвищення надійності окремих компонентів, резервування ресурсів та інші заходи, спрямовані на забезпечення більш стабільної та ефективної роботи мережі.

Отже, розділ надає практичні висновки та рекомендації щодо виявлення та управління відмовами в мережі. Результати дослідження можуть бути використані для покращення надійності та якості роботи локальних комп'ютерних мереж у різних сферах застосування.

ВИСНОВКИ

У кваліфікаційній роботі було розроблено модель діагностики стану локальної комп'ютерної мережі, що дозволяє виявляти потенційні проблеми, аналізувати їх вплив та рекомендувати заходи для покращення надійності та якості роботи мережі. Робота складалася з трьох основних розділів, кожен з яких пропонує важливі висновки та рекомендації.

У першому розділі був проведений огляд підходів, моделей і методів для діагностики стану складних систем. Було розглянуто поняття та класифікація складних систем, методи діагностики та моделі, а також їх застосування у різних галузях. Цей огляд дав загальне розуміння діагностики стану складних систем і визначив основні підходи, які можна використовувати у розробці моделі для діагностики локальної комп'ютерної мережі.

У другому розділі була проведена розробка власної моделі та діагностика стану локальної комп'ютерної мережі. Були проаналізовані особливості та проблеми локальних комп'ютерних мереж, вибрано та обґрунтовано метод діагностики, побудована математична модель та реалізовано прототип моделі. Цей розділ надав детальну інформацію щодо структури та функціонування локальних комп'ютерних мереж, а також методів та засобів для їх діагностики.

У третьому розділі були розглянуті ймовірності виділення відмов локальної комп'ютерної мережі за допомогою розробленої моделі. Була сформульована задача виділення відмов, оцінено дерево відмов та надані рекомендації щодо покращення надійності та якості роботи мережі. Цей розділ спрямований на виявлення та управління відмовами у локальних комп'ютерних мережах для забезпечення їх безперебійної та ефективної роботи.

Загальний висновок з кваліфікаційної роботи вказує на успішну розробку моделі діагностики стану локальної комп'ютерної мережі. Результати дослідження виявляють значимість та перспективи подальшого розвитку діагностики стану локальних комп'ютерних мереж з використанням моделей та методів, що були розглянуті в роботі. Дана робота може бути використана як основа для подальших досліджень у сфері діагностики комп'ютерних мереж та сприяти вдосконаленню їх функціонування у різних галузях застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tanenbaum, A. S., Wetherall, D. J. (2011). Computer Networks. Pearson Education.
2. local area network (LAN). URL:https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN. Дата звертання: 12.05.2023
3. Kurose, J. F., Ross, K. W. (2017). Computer Networking: A Top-Down Approach. Pearson Education.
4. Comer, D. E. (2014). Computer Networks and Internets. Pearson Education.
5. Forouzan, B. A., Fegan, S. C. (2012). Data Communications and Networking. McGraw-Hill Education.
6. Stallings, W. (2013). Data and Computer Communications. Pearson Education.
7. Peterson, L. L., Davie, B. S. (2011). Computer Networks: A Systems Approach. Morgan Kaufmann.
8. Cisco Networking Academy. (2019). CCNA Routing and Switching: Introduction to Networks Companion Guide.
9. Alapati, S. (2017). Modern Linux Administration: How to Become a Cutting-Edge Linux Administrator. Packt Publishing.
10. Beale, P., Turner, R. (2013). Ethernet: The Definitive Guide. O'Reilly Media.
11. Mitchell, B. (2012). TCP/IP Sockets in C: Practical Guide for Programmers. Morgan Kaufmann.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки
Рівень вищої освіти (освітньо-кваліфікаційний рівень) бакалавр
Галузь знань: 12 – Інформаційні технології.
Спеціальність 123 – Комп'ютерна інженерія.

ЗАТВЕРДЖУЮ
Завідувач кафедри теоретичної
та прикладної системотехніки
_____д.т.н., проф. Шматков С. І.

«17»листопада 2022 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Подплєтнього Євгенія Олександровича

1. Тема роботи **«Метод афінних перетворень в комп'ютерних системах обробки графічної інформації»**
керівник роботи Стрілець Вікторія Євгенівна, канд. техн.наук, доц., доцент кафедри теоретичної та прикладної системотехніки.
затверджені наказом по університету від «23» травня 2023 року № 4101-5/895

2. Строк подання студентом роботи 26 травня 2023

3. Перелік питань, які потрібно розробити
1. Аналіз сучасних засобів і методів моніторингу стану та діагностики комп'ютерних мереж.

2. Розробка моделі діагностики стану локальної комп'ютерної мережі заданої топології.

3. Реалізація та тестування моделі діагностики стану локальної комп'ютерної мережі.

4. План роботи

№ з/п	Назви етапів роботи	Термін виконання етапів роботи
1	Аналіз літератури та сучасних засобів, підходів і методів моніторингу стану та діагностики комп'ютерних мереж	Листопад – грудень 2022
2	Вибір топології локальної комп'ютерної мережі для аналізу	Січень 2022
3	Створення моделі діагностики стану локальної комп'ютерної мережі заданої топології	Лютий 2022
4	Реалізація моделі діагностики стану локальної комп'ютерної мережі	Березень 2023
5	Тестування моделі діагностики стану локальної комп'ютерної мережі	Квітень 2023
6	Оформлення пояснювальної записки	Травень 2023
7	Представлення кваліфікаційної роботи керівнику та рецензенту	Травень 2023

5. Дата видачі завдання 25 листопада 2022 р.

Студент Подплєтній Є. О.
(підпис, прізвище) (підпис)

Керівник роботи Стрілець В. Є.
(підпис, прізвище) (підпис)

Додаток Б

Затверджую

_____

«23» травня 2023 р.

Технічне завдання
на розробку програмного виробу «Модель діагностики стану локальної комп'ютерної мережі»

1.	Введення	1.1. Назва: Модель діагностики стану локальної комп'ютерної мережі 1.2. Галузь застосування: Інформаційні технології
2.	Підстава для розробки	2.1. Навчальний план за спеціальністю 123 – Комп'ютерна інженерія 2.2. Завдання на кваліфікаційну роботу бакалавра № __4101-5/895__ від «_23_» ____05_____2023 (представити як Додаток А до пояснювальної записки до кваліфікаційної роботи).
3.	Призначення розробки	3.1. Мета розробки: розробка комп'ютерної мережі для кафедри чи лабораторії, що розподілена на деякі стани. 3.2. Призначення розробки надає можливість визначити стану роботи мережі, наявність неполадок та помилок та присутніх несправностей. 3.3. Вихідні дані розробки: локальна комп'ютерна мережа для кафедри чи лабораторії; вхідні дані: несправна мережа.
4.	Технічні вимоги до програмного виробу	4.1. Вимоги до функціональних характеристик: автоматичне виявлення помилок, розпізнавання видів проблеми, відстеження стану мережі та простота використання. 4.2. Вимоги до надійності: забезпечення безперебійної роботи програмного виробу при будь-яких вимогах користувача в рамках призначення виробу . 4.3 Вимоги до умов експлуатації: немає 4.4. Вимоги до складу і параметрів технічних засобів: для виконання програми повинен підходити ПК із будь-якою операційною системою сімейства Windows, Linux/Unix, Mac OS X, OS/2. Крім того, для роботи потрібний інтерпретатор мови програмування. 4.5. Вимоги до інформаційної та програмної

<table>
<tr><td></td><td></td><td colspan="2">сумісності: підтримка ОС Linux або Windows 10, підтримка мови програмування, підтримка різних платформ.
4.6. Вимоги до маркування та упаковки: вимоги до маркування та упакування не представляються.
4.7. Вимоги до транспортування і зберігання: вимоги до транспортування та зберігання не представляються.
4.8. Спеціальні вимоги: спеціальні вимоги до програмного виробу не пред'являються.</td></tr>
<tr><td>5.</td><td>Вимоги до програмної документації</td><td colspan="2">Програмною документацією до виробу «Метод аналізу інформативності змінних стану при діагностиці систем з використанням інформаційних критеріїв» вважати:
1) Справжнє Технічне завдання на розробку виробу (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи).
2) Методику розрахунку інформативності змінних стану (у вигляді глав 3.2 та 3.3 пояснювальної записки до кваліфікаційної роботи).
3) Опис виробу (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи)</td></tr>
<tr><td>6.</td><td>Вимоги до техніко-економічних показників</td><td colspan="2">Програмною документацією до виробу «Модель діагностики стану локальної комп'ютерної мережі» вважати:
1) Справжнє Технічне завдання на розробку виробу (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи).
2) Опис програмного виробу (представити в Розділі 3 пояснювальної записки до кваліфікаційної роботи).
3) Джерела базової інформації.</td></tr>
<tr><td>7.</td><td>Стадії і етапи розробки</td><td>Дата</td><td>Назва етапу</td></tr>
<tr><td></td><td></td><td>Листопад – грудень 2022

Січень 2023

Лютий 2023</td><td>Аналіз літератури та сучасних засобів, підходів і методів моніторингу стану та діагностики комп'ютерних мереж

Вибір топології локальної комп'ютерної мережі для аналізу

Створення моделі</td></tr>
</table>

			діагностики стану локальної комп'ютерної мережі заданої топології
		Березень 2023	Реалізація моделі діагностики стану локальної комп'ютерної мережі
		Квітень 2023	Тестування моделі діагностики стану локальної комп'ютерної мережі
		Травень 2023	Оформлення пояснювальної записки
		Травень 2023	Представлення кваліфікаційної роботи керівнику та рецензенту
8.	Порядок контролю і приймання програмного продукту (моделі)	1. Перевірку ходу розробки програми виконувати раз в 3 тижні. 2. Захист розробленої моделі провести на засіданні Атестаційної комісії. 3. Пояснювальну записку подати на паперових носіях в 1 примірнику і в електронному вигляді в 1 примірнику на CD-R компакт-диску.	

Виконавець
студент групи КІ- 41
Подплетній Є. О.
_____

Замовник
канд. техн. наук
Стрілець В. Є.
_____

Додаток В

Програма і методика випробувань програмного виробу

«Модель діагностики стану локальної комп'ютерної мережі»

1 **Об'єкт випробувань**

2 Назва програмного виробу : «Модель діагностики стану локальної комп'ютерної мережі»

3 Галузь застосування : Інформаційні технології

4 Перераховані відомості запозичуються з відповідних розділів Технічного завдання.

2. Мета випробувань

Перевірка відповідності функціональності програмної реалізації системи заявленим функціональним можливостям в технічному завданні (Додаток Б до пояснювальної записки до кваліфікаційної роботи).

3. Загальні положення

1. Підстави для проведення випробувань

Підставою для проведення випробувань є наказ про призначення атестаційної комісії.

2. Місце і тривалість випробувань

Приймальні (приймально-здавальні) випробування проводяться на базі комп'ютерного класу кафедри в період роботи атестаційної комісії.

3. Обсяг випробувань

Приймальні випробування програмного виробн проводяться в обсязі відповідному цієї програми і методики випробувань.

4. Організації, які беруть участь у випробуваннях

Приймальні випробування проводяться атестаційною комісією напередодні засідання (або в процесі засідання) за участю Замовника, Виконавця та інших осіб, присутніх на засіданні.

4. Вимоги до програми або програмного виробу

Модель повинна задовольняти наступним вимогам:

4.1. Вимоги до функціональних характеристик: автоматичне виявлення помилок, розпізнавання видів проблеми, відстеження стану мережі та простота використання.

4.2. Вимоги до надійності: забезпечення безперебійної роботи програмного виробу при будь-яких вимогах користувача в рамках призначення виробу .
4.3 Вимоги до умов експлуатації: немає
4.4. Вимоги до складу і параметрів технічних засобів: для виконання програми повинен підходити ПК із будь-якою операційною системою сімейства Windows, Linux/Unix, Mac OS X, OS/2. Крім того, для роботи потрібний інтерпретатор мови програмування.
4.5. Вимоги до інформаційної та програмної сумісності: підтримка ОС Linux або Windows 10, підтримка мови програмування, підтримка різних платформ.
4.6. Вимоги до маркування та упаковки: вимоги до маркування та упакування не представляються.
4.7. Вимоги до транспортування і зберігання: вимоги до транспортування та зберігання не представляються.
4.8. Спеціальні вимоги: спеціальні вимоги до програмного виробу не пред'являються.

5. Вимоги до програмної документації

Документацією до виробу «Комп'ютерна система планування IT-проєктів» вважати:

1) Документація по мові програмування та додаткові мануали.

2) Програму і методику випробувань розробленої програми (представити як Додаток В до пояснювальної записки до кваліфікаційної роботи).

3) Опис програмного виробу (представити в Розділі 3 пояснювальної записки до кваліфікаційної роботи).

4) Джерела базової інформації.

6. Засоби і порядок випробувань

6.1 Засоби випробувань

Засоби випробувань представлено на ПК на яких встановлено наступні програмні засоби: інтерпретатор мови програмування.

6.2 Порядок проведення випробувань

Як правило, випробування проводяться в два етапи:

- ознайомчий (1-й етап);
- власне випробування програмного виробу (2-й етап).

Перелік перевірок, що проводяться на 1 етапі випробувань, включає в себе:

1) Перевірку комплектності складу програмної документації здійснюється за критерієм наявності зазначеної в ТЗ документації.

2) Перевірку якості програмної документації. Перевірку здійснювати за критерієм відповідності вимогам ГОСТ 19.301-79 ЕСПД. «Програма і методика випробувань».

Перелік перевірок, що проводяться на 2 етапі випробувань, включає в себе:

1) Перевірку відповідності технічних характеристик програми вимогам технічного завдання.

2) Перевірку ступеня виконання функціональних вимог до програми.

3) Методику проведення перевірок

a) Запустити програмне забезпечення.

b) Порядок проведення випробувань:

- Зробити налаштування.
- Перевірити чи працює програма.
- Перевірити чи формується звіт.

4) Якщо перевірки на першому та другому етапах виконано успішно, то виріб вважається таким, що пройшов випробування.

Для проведення випробувань пропонується тест 1, тест 2 та тест 3.

Тест 1

1. Перевірка виконання програми;
2. Індикація з'єднань;
3. Отримання відповіді серверу про успішне створення об'єкту.

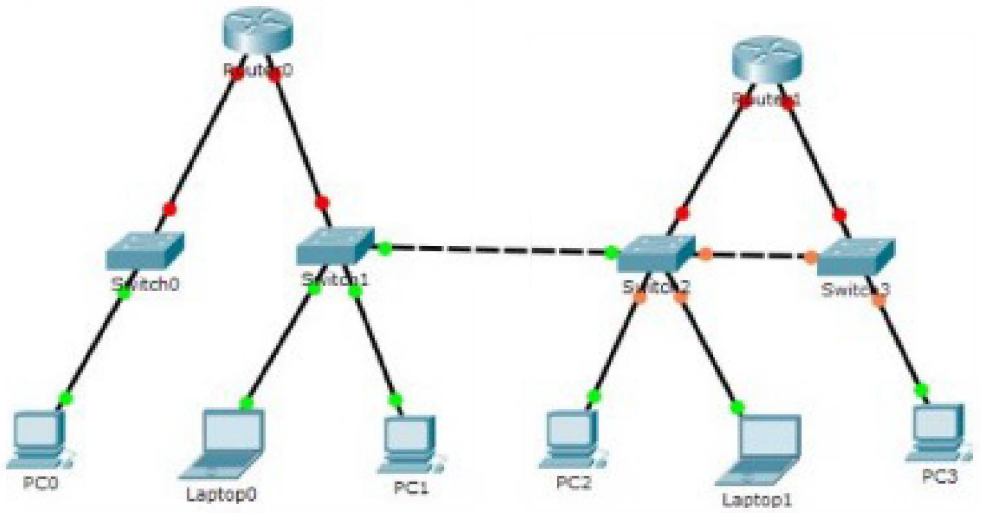

Рис. В.1 Тест 1

Тест 2

1. Перевірка виконання програми
2. Режим симуляції;
3. Отримання результатів.

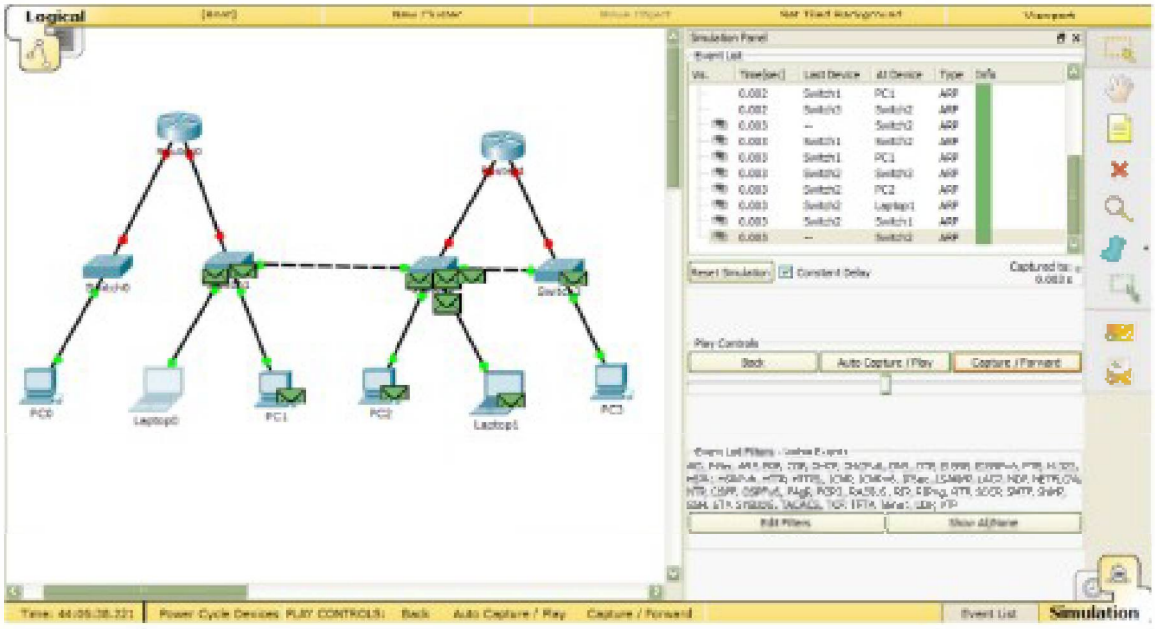

Рис. В.2 Тест 2

Тест 3

4. Перевірка виконання програми
5. Вікно PDU Information;

6. Отримання результату.

Рис. В.3 Тест 3

Тест вважається пройденим, якщо відбуваються вказані операції і їх відображення у програмному продукті.

Висновки: тест 1 успішно пройшов випробування, тест 2 успішно пройшов випробування і тест 3 успішно пройшов випробування. Випробування пройшло успішно.

Виконавець: студент групи КІ-41, Подплетній Є. О.