МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерних наук

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему АНАЛІЗ НАДІЙНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Виконав: студент 2 курсу, групи ІКК 2.1
спеціальності
122 Комп'ютерні науки

Гайса Олексій Михайлович

Керівник Розенвассер Д.М.

Рецензент Григор'єва Т.І.

Одеса – 2023

Д О В І Д К А

кафедри КН про виконану магістерську роботу

студента 2 курсу ФКПІ та КН групи ІКК 2.1

Гайси Олексія Михайловича

на тему Аналіз надійності комп'ютерної мережі

Висновок нормоконтролера кваліфікаційна записка до кваліфікаційної роботи викон. з дотрим. вимог ДСТУ. Оформлено згідно внутрішнього положення КПІ

Нормоконтролер викл. каф. ТПІ 15.11.2023 Кліщенко ІВ

(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Висновок відповідального за наявність плагіату згідно з сертифікатом ID унікальність роботи підтверджено

Відповідальна особа викл. каф. ТПІ 15.12.2023 Кліщенко ІВ

(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Попередня експертиза (захист) магістерської роботи

(бакалаврської роботи чи магістерської роботи)

студ. Гайси О.М. проведена "15" 12 2023р.

(прізвище і.б.)

Висновки Кваліфікаційна робота виконана у повному обсязі. В роботі проведено аналіз надійності комп'ютерної мережі. Кваліфікаційна робота відповідає вимогам до випускних кваліфікаційних робіт зі спеціальності 122 Комп'ютерні науки та рекомендована до захисту.

Члени комісії ____ к.т.н., доц. Соловська І.М.

(підпис) (науковий ступінь, вчене звання,посада, прізвище і.б.)

____ к.т.н., доц. Русу О.П.

(підпис) (науковий ступінь, вчене звання, посада, прізвище і.б.)

____ к.т.н., доц. Розенвассер Д.М.

(підпис) (науковий ступінь, вчене звання, посада, прізвище і.б.)

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерних наук
Освітній ступінь магістр
Галузь знань 12 Інформаційні технології
Спеціальність 122 Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедри КН
к.т.н., доц.
_____ І.М.Соловська
"25" 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ

Гайсі Олексію Михайловичу

1. Тема роботи: Аналіз надійності комп'ютерної мережі

керівник роботи Розенвассер Денис Михайлович
затверджені наказом закладу вищої освіти від 25.09.2023 р. № 1959

2. Строк подання студентом роботи 11.12.2023

3. Вихідні дані до роботи: Виконати аналіз надійності комп'ютерної мережі, її компонентів, програмного забезпечення за допомогою різних методів, таких як аналіз ймовірності, аналіз відмов та інших, зробити рекомендації щодо підвищення надійності комп'ютерних мереж.

4. Зміст розрахунково-пояснювальної записки
Розділ 1: Надійність як комплексна властивість об'єкта
Розділ 2: Надійність комп'ютерної мережі
Розділ 3: Моделі надійності комп'ютерної мережі
Розділ 4: Аналіз надійності комп'ютерної мережі

5. Перелік графічного матеріалу (з зазначенням обов'язкових креслень)
Слайд 1 – Постановка задачі

Слайд 2 – Відмови та безвідмовність

Слайд 3 – Фактори надійності

Слайд 4 – Надійність комп'ютерної мережі за структурно-логічним аналізом

Слайд 5 – Висновки та рекомендації

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав	Завдання прийняв

7. Дата видачі завдання 25.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Вступ	25.09.2023-5.10.2023	вик
2	Надійність як комплексна властивість об'єкта	6.10.2023-19.10.2023	вик
3	Надійність комп'ютерної мережі	20.10.2023-31.10.2023	вик
4	Моделі надійності комп'ютерної мережі	1.11.2023-9.11.2023	вик
5	Аналіз надійності комп'ютерної мережі	10.11.2023-20.11.2023	вик
6	Висновки та рекомендації	21.11.2023-28.11.2023	вик
7	Перелік посилань	29.11.2023-5.12.2023	вик
8	Оформлення презентації	6.12.2023-11.12.2023	вик

Студент _____ О.М. Гайса
(підпис)

Керівник роботи _____ Д.М. Розенвассер
(підпис)

ВІДГУК КЕРІВНИКА

магістерської роботи студента Гайси О.М.
на тему: «Аналіз надійності комп'ютерної мережі»

Завдання надійності комп'ютерної мережі, її компонентів, а також програмного забезпечення завжди є актуальною темою.

У роботі описано аналіз надійності комп'ютерної мережі різними методами, такими як аналіз за структурно-логічною схемою, аналіз дерева відмов, аналіз кореневої причини, аналіз марківських ланцюгів та інші. Визначено їх переваги та недоліки.

Студент Гайса О.М. добре розібрався з проблемами даної тематики, приділив увагу докладному аналізу методів підвищення надійності комп'ютерних мереж.

Робота проводилася значною мірою самостійно. Графік консультацій не порушувався.

Завдання на ВКР виконано. При оформленні пояснювальної записки та демонстраційних слайдів використовувались комп'ютерні технології.

Під час виконання магістерської роботи студент Гайса О.М. вивчив класифікацію станів роботи, факторів надійності, моделей надійності комп'ютерних мереж та програмного забезпечення, показав уміння користуватись навчальною та технічною літературою, ставити та розв'язувати інженерні задачі.

Магістерська робота відповідає вимогам до випускних робіт та заслуговує оцінки «задовільно».

Студент Гайса О.М. заслуговує присвоєння кваліфікації магістр з комп'ютерних наук за спеціальністю 122 Комп'ютерні науки.

Керівник
к.т.н., доцент кафедри КН Д.М. Розенвассер

РЕЦЕНЗІЯ

магістерської роботи студента Гайси О.М.
на тему: «Аналіз надійності комп'ютерної мережі»

Магістерська робота містить 4 розділи текстової частини, демонстраційні слайди, виконана згідно з завданням на магістерську роботу.

У роботі розглядаються методи аналізу надійності комп'ютерних мереж.

Актуальність теми полягає в тому, що на сьогоднішній день спостерігається зростання складності комп'ютерних мереж, збільшення залежності бізнесу від комп'ютерних мереж, поширення кіберзагроз. За таких умов важливим завданням є підвищення надійності комп'ютерних мереж, їхніх компонент та програмного забезпечення.

Магістерська робота виконана відповідно до завдання. Демонстраційні матеріали й пояснювальна записка виконані охайно й відповідно до вимог ЄСКД. Прийняті рішення обґрунтовано.

Автором показана достатня теоретична підготовка. Робота виконана грамотно, текст її послідовний та зрозумілий, оформлення роботи та демонстраційних слайдів якісне.

До недоліків роботи варто віднести те, що у роботі:

- не розглянуто приклад аналізу надійності для конкретної комп'ютерної мережі;
- немає чисельної оцінки надійності мережі.

Зазначені недоліки суттєво не знижують якості виконаної роботи.

Магістерська робота відповідає вимогам до випускних робіт та заслуговує оцінки «задовільно».

Студент Гайса О.М. заслуговує присвоєння кваліфікації магістр з комп'ютерних наук за спеціальністю 122 Комп'ютерні науки.

Рецензент
к.т.н., доцент, заф. кафедри ІТ  Григорєва Т.І.

UNICHECK
by Turnitin

Ім'я користувача:
Анна Серединко

Дата перевірки:
19.12.2023 12:18:32 EET

Дата звіту:
20.12.2023 12:27:39 EET

ID перевірки:
1016021228

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100001433

Назва документа: Вступ диплом Гайса

Кількість сторінок: 33 Кількість слів: 5652 Кількість символів: 45183 Розмір файлу: 217.45 KB ID файлу: 1015709273

11.5%
Схожість

Найбільша схожість: 4.97% з Інтернет-джерелом (http://elartu.tntu.edu.ua/bitstream/lib/21073/1/%D0%9D%D0%B0%D0..

11.3% Джерела з Інтернету | 50 ..... Сторінка 35

0.16% Джерела з Бібліотеки | 1 ..... Сторінка 35

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

РЕФЕРАТ

Текстова частина магістерської роботи: 45 с., 4 рисунки, 1 таблиця, одаток, 12 джерел.

НАДІЙНІСТЬ, КОМП'ЮТЕРНІ МЕРЕЖІ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ДМОВИ, ОБЛАДНАННЯ, ГРАФ, ЙМОВІРНІСТЬ, СТРУКТУРНО-ЛОГІЧНИЙ НАЛІЗ, МОДЕЛЬ

Об'єкт дослідження – комп'ютерні мережі та їхні компоненти.

Мета роботи – виконати аналіз надійності комп'ютерної мережі, її омпонентів, програмного забезпечення за допомогою різних методів, таких як наліз ймовірності, аналіз відмов та інших, зробити рекомендації щодо ідвищення надійності комп'ютерних мереж.

Метод дослідження – аналітичний з використання комп'ютерних технологій.

У магістерській роботі описано аналіз надійності комп'ютерної мережі різними методами, такими як аналіз за структурно-логічною схемою, аналіз дерева відмов, аналіз кореневої причини, аналіз марківських ланцюгів та інші. Визначено їх переваги та недоліки. Результати аналізу надійності мережі можуть використовуватися для прийняття рішень про те, як поліпшити надійність мережі.

ABSTRACT

The text part of the master paper: 45 pp., 4 figures, 1 table, 1 appendix, 12 references.

RELIABILITY, COMPUTER NETWORKS, SOFTWARE, FAILURES, HARDWARE, GRAPH, PROBABILITY, STRUCTURAL LOGICAL ANALYSIS, MODEL

Object of research are computer networks and their components.

The purpose of the work is to perform an analysis of the reliability of a computer network, its components, and software using various methods, such as probability analysis, failure analysis, and others, make recommendations for improving the reliability of computer networks.

The research method is analytical with the use of computer technologies.

In the master's paper, the analysis of the reliability of the computer network by various methods is described, such as the analysis according to the structural and logical scheme, the analysis of the failure tree, the analysis of the root cause, the analysis of Markov chains and others. Their advantages and disadvantages are determined. The results of network reliability analysis can be used to make decisions about how to improve network reliability.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

АДВ – аналіз дерева відмов

АМЛ – аналіз марківських ланцюгів

АМК – аналіз Монте-Карло

АПНЗ – аналіз причинно-наслідкового зв'язку

АКП – аналіз кореневої причини

АМДВ – аналіз модифікованого дерева відмов

КМ – комп'ютерна мережа

СЛА – структурно-логічний аналіз

ПЗ – програмне забезпечення

MTBF – mean time between failures – середній час безвідмовної роботи

ВСТУП

Надійність комп'ютерної мережі є важливим фактором, який слід враховувати при проектуванні, експлуатації та адмініструванні мережі.

Надійність системи є складною характеристикою, яка залежить від багатьох факторів.

Задача аналізу надійності комп'ютерної мережі є актуальною з декількох причин:

- збільшення залежності бізнесу від комп'ютерних мереж. У сучасному світі комп'ютерні мережі є основою для багатьох бізнес-процесів. Збої в роботі мережі можуть призвести до значних фінансових втрат, а також до порушення роботи бізнесу.
- поширення кіберзагроз. Кіберзагрози, такі як атаки зловмисників, можуть призвести до збоїв у роботі комп'ютерних мереж.
- зростання складності комп'ютерних мереж. Сучасні комп'ютерні мережі є складними системами, які складаються з багатьох компонентів. Це підвищує ймовірність збоїв у роботі мережі.

Задача забезпечення надійності комп'ютерної мережі полягає в тому, щоб забезпечити безперебійну роботу мережі протягом заданого періоду часу. Для вирішення цієї задачі необхідно вжити заходів щодо підвищення надійності мережі.

Аналіз надійності комп'ютерної мережі - це процес оцінки ймовірності того, що мережа буде працювати без збоїв протягом заданого періоду часу.

Аналіз надійності мережі може проводитися за допомогою різних методів, таких як:

- аналіз ймовірності. Цей метод використовується для оцінки ймовірності того, що окремий компонент мережі вийде з ладу.
- аналіз відмов. Цей метод використовується для оцінки ймовірності того, що мережа не буде працювати без збоїв протягом заданого періоду часу.

- аналіз чутливості. Цей метод використовується для оцінки того, як зміна надійності одного компонента мережі впливає на надійність всієї мережі.

Для підвищення надійності системи необхідно вжити заходів для покращення складових, які на неї впливають.

Результати аналізу надійності мережі можуть використовуватися для прийняття рішень про те, як поліпшити надійність мережі. Наприклад, якщо аналіз надійності показує, що обладнання мережі є основною проблемою, то можна прийняти рішення про заміну обладнання на більш надійне.

1 НАДІЙНІСТЬ ЯК КОМПЛЕКСНА ВЛАСТИВІСТЬ ОБ’ЄКТА

1.1 Відмови та безвідмовність

Надійність комп'ютерної мережі є важливим фактором, який слід враховувати при проектуванні, експлуатації та адмініструванні мережі.

Надійність системи є складною характеристикою, яка залежить від багатьох факторів.

Відмова - це подія, яка полягає в втраті об'єктом здатності виконувати потрібні функції. Відмови в комп'ютерних мережах можуть бути викликані різними факторами, такими як:

- фізичні пошкодження обладнання мережі, наприклад, через пожежу, повінь або землетрус.
- експлуатаційні помилки, наприклад, неправильне налаштування обладнання або програмного забезпечення.
- програмні помилки в програмному забезпеченні мережі.
- кіберзагрози, такі як атаки зловмисників.

Фізичні пошкодження обладнання мережі є одним з найпоширеніших факторів, що призводять до відмов у мережах. Фізичні пошкодження можуть бути викликані різними причинами, такими як:

- природні катаклізми, такі як пожежі, повені та землетруси.
- несприятливі умови навколишнього середовища, такі як підвищена вологість, температура або пил.
- механічні пошкодження, наприклад, удари, падіння або дії людини.
- електричні перевантаження.

Фізичні пошкодження обладнання мережі можуть призвести до різних проблем, таких як:

- вихід з ладу обладнання.
- зниження продуктивності обладнання.

- пошкодження даних.

Для захисту обладнання мережі від фізичних пошкоджень можна використовувати такі заходи:

- розміщення обладнання в безпечному місці. Обладнання мережі слід встановлювати в місці, де воно буде захищене від природних катаклізмів і несприятливих умов навколишнього середовища.
- застосування засобів захисту обладнання. Обладнання мережі можна захистити від механічних пошкоджень, використовуючи спеціальні корпуси або кожухи. Для захисту обладнання від електричних перешкод можна використовувати стабілізатори напруги або джерела безперебійного живлення.
- виконання регулярного технічного обслуговування обладнання. Регулярне технічне обслуговування обладнання дозволяє виявити і усунути потенційні проблеми до того, як вони призведуть до фізичних пошкоджень.

Приклади того, як можна захистити обладнання мережі від фізичних пошкоджень:

- встановлювати обладнання в спеціальних серверних кімнатах, які захищені від пожеж, повеней та інших природних катаклізмів.
- використовувати броньовані корпуси для обладнання, яке може бути пошкоджено в результаті ударів або падінь.
- забезпечити захист обладнання від перепадів напруги, використовуючи стабілізатори напруги або джерела безперебійного живлення.
- регулярно перевіряти обладнання на наявність пошкоджень.

Заходи щодо захисту обладнання мережі від фізичних пошкоджень є важливим елементом забезпечення безвідмовності мережі.

Експлуатаційні помилки можуть бути викликані різними причинами, такими як:

- неправильне налаштування обладнання або програмного забезпечення.
- неправильні дії користувачів.

- використання обладнання або програмного забезпечення не за призначенням.

Для запобігання експлуатаційним помилкам можна використовувати такі заходи:

- надання користувачам чітких інструкцій по експлуатації обладнання та програмного забезпечення.
- проведення навчання користувачів.
- впровадження систем управління та моніторингу.

Для запобігання експлуатаційним помилкам можна:

- створювати чіткі інструкції по експлуатації обладнання та програмного забезпечення. Інструкція повинна містити інформацію про призначення обладнання або програмного забезпечення, правила його використання та технічні характеристики.
- проводити навчання користувачів. Навчання користувачів дозволяє їм ознайомитися з інструкціями по експлуатації та правильно використовувати обладнання або програмне забезпечення.
- впроваджувати системи управління та моніторингу. Системи управління та моніторингу дозволяють виявляти потенційні проблеми на ранній стадії, що може допомогти запобігти експлуатаційним помилкам.

Програмні помилки в програмному забезпеченні мережі - це одна з найсерйозніших проблем, які можуть призвести до відмов у мережах. Програмні помилки можуть бути викликані різними причинами, такими як:

- недостатній контроль якості під час розробки програмного забезпечення. Це може бути пов'язано з недостатньою кваліфікацією або досвідом розробників, недостатнім фінансуванням або часом, виділеним на розробку, або відсутністю належних процесів контролю якості.
- неправильна архітектура програмного забезпечення. Це може бути пов'язано з помилками в проектуванні програмного забезпечення, такими як використання неправильних алгоритмів або структур даних.
- недостатнє тестування програмного забезпечення. Це може бути

пов'язано з недостатньою кількістю тестів, проведених на програмному забезпеченні, або з використанням неправильних методів тестування.

Для запобігання програмним помилкам в програмному забезпеченні мережі можна використовувати такі заходи:

- впровадження процесів контролю якості під час розробки програмного забезпечення. Це включає в себе рецензування коду, автоматизоване тестування та тестування на основі поведінки.
- використання сучасних методів розробки програмного забезпечення, таких як ітераційна розробка та тестування на основі поведінки. Ці методи дозволяють виявити і виправити помилки на ранніх етапах розробки.
- впровадження системи управління змінами, яка дозволяє контролювати всі зміни в програмному забезпеченні. Це допомагає уникнути помилок, пов'язаних із внесенням змін до програмного забезпечення.

Кіберзагроза - це будь-яка діяльність, яка може призвести до несанкціонованого доступу, використання, розкриття, модифікації або знищення даних або систем. Кіберзагрози можуть бути викликані різними факторами, такими як:

- кіберзлочинці - це особи або групи, які використовують кібертехнології для незаконної або шкідливої діяльності. Кіберзлочинці можуть використовувати кіберзагрози для крадіжки даних, вимагання, розповсюдження шкідливого програмного забезпечення або інших незаконних дій.
- вороги держави - це країни, які використовують кібертехнології для шпигунства, саботажу або інших ворожих дій. Вороги держави можуть використовувати кіберзагрози для отримання доступу до секретної інформації, порушення роботи критичної інфраструктури або інших ворожих дій.
- неусвідомлені користувачі - це особи, які випадково або через незнання завдають шкоди комп'ютерним системам. Неусвідомлені користувачі

можуть використовувати кіберзагрози, поширюючи шкідливе програмне забезпечення або відвідуючи підроблені веб-сайти.

Кіберзагрози можуть мати серйозні наслідки для організацій і окремих осіб. До наслідків кіберзагроз можна віднести:

- втрата даних - це найпоширеніша кіберзагроза. Втрата даних може призвести до фінансових втрат, порушення конфіденційності та інших проблем.
- розкрадання даних - це кіберзагроза, при якій злочинці отримують несанкціонований доступ до даних. Розкрадання даних може призвести до фінансових втрат, порушення конфіденційності та інших проблем.
- саботаж - це кіберзагроза, при якій злочинці намагаються пошкодити або знищити комп'ютерні системи. Саботаж може призвести до фінансових втрат, порушення роботи критичної інфраструктури та інших проблем.
- шпигунство - це кіберзагроза, при якій злочинці намагаються отримати доступ до секретної інформації. Шпигунство може призвести до фінансових втрат, порушення безпеки та інших проблем.

Для захисту від кіберзагроз організації та окремі особи можуть використовувати різні заходи, такі як:

- впровадження кібербезпеки - це комплекс заходів, спрямованих на захист від кіберзагроз. До заходів кібербезпеки можна віднести використання антивірусного програмного забезпечення, брандмауера, фільтрів спаму та інших засобів.
- освіта користувачів - це важливий захід, який допомагає користувачам розуміти кіберзагрози та вживати заходів для захисту себе та своїх систем.
- вчасне оновлення програмного забезпечення - це важливий захід, який допомагає захистити від кіберзагроз, оскільки виробники програмного забезпечення часто випускають оновлення, які усувають вразливості.

Кіберзагрози є серйозною проблемою, яка може мати серйозні наслідки для організацій і окремих осіб. Для захисту від кіберзагроз важливо впроваджувати

заходи кібербезпеки, навчати користувачів та своєчасно оновлювати програмне забезпечення.

Безвідмовність - це характеристика надійності, яка визначає ймовірність того, що система буде працювати без збоїв протягом заданого періоду часу. Безвідмовність часто вимірюється коефіцієнтом безвідмовності, який є відношенням часу без відмов до загального часу роботи системи.

1.2 Стани роботи

Стан роботи мережі - це характеристика мережі, яка визначає її здатність виконувати свої функції.

Стан роботи мережі може бути описаний такими параметрами, як:

- доступність - здатність мережі надавати доступ до ресурсів.
- якість обслуговування - здатність мережі забезпечувати певний рівень продуктивності та надійності.
- безпека - здатність мережі захищати свої ресурси від несанкціонованого доступу.

Залежно від цих параметрів стан роботи мережі може бути класифікований наступним чином:

- нормальний стан - мережа працює в штатному режимі і забезпечує доступ до ресурсів на заданому рівні якості обслуговування і безпеки.
- порушення (граничний стан) - мережа не може надавати доступ до ресурсів або надає його на нижчому рівні якості обслуговування або безпеки.
- аварія (відмова) - мережа повністю непрацездатна.

Нормальний стан роботи мережі є бажаним станом, який забезпечує безперебійну роботу мережі та доступ до її ресурсів.

Доступність мережі в нормальному стані означає, що всі компоненти мережі працюють і можуть надавати доступ до ресурсів.

Якість обслуговування мережі в нормальному стані означає, що мережа забезпечує певний рівень продуктивності та надійності. Це означає, що користувачі можуть отримувати доступ до ресурсів мережі в потрібний час і в потрібній кількості.

Безпека мережі в нормальному стані означає, що мережа захищена від несанкціонованого доступу. Це означає, що тільки уповноважені користувачі можуть отримувати доступ до ресурсів мережі.

Граничний стан роботи комп'ютерної мережі виникає внаслідок фізичного зносу компонентів мережі або неправильної експлуатації. Цей стан може бути викликаний такими факторами, як:

- фізичні пошкодження мережі, наприклад, в результаті аварії або дії природних факторів.
- експлуатаційні навантаження, які перевищують допустимі значення.
- хімічні процеси, які призводять до корозії або інших форм руйнування.

Прикладом граничного стану роботи комп'ютерної мережі є підвищення навантаження на мережу, наприклад, в результаті зростання кількості користувачів або використання ресурсів мережі. У цьому випадку мережа може не зможе забезпечити заданих вимог до якості обслуговування, наприклад, може спостерігатися зниження продуктивності або зростання затримок.

1.3 Довговічність та збереженість

Довговічність і збереженість - це два взаємопов'язаних поняття, які характеризують здатність об'єкта зберігати свої властивості протягом певного часу.

Довговічність - це характеристика надійності, яка визначає час, протягом якого система може виконувати свої функції до настання граничного стану. Граничним станом може бути фізичний знос, моральний знос або граничний стан, встановлений експлуатаційними нормами.

Збереженість - це характеристика надійності, яка визначає ймовірність того, що система буде зберігати свої характеристики протягом заданого періоду часу. Збереженість часто вимірюється коефіцієнтом збереженості, який є відношенням часу збереженості до загального часу роботи системи.

Довговічність та збереженість мережі визначається такими факторами, як:

- конструкція мережі. Надійні конструкції, які забезпечують рівномірний розподіл навантажень, менш схильні до зносу і руйнування.
- матеріали, з яких виготовлені компоненти мережі. Деякі матеріали, наприклад, метали, більш довговічні, ніж інші, наприклад, пластик.
- умови експлуатації мережі. Мережі, які експлуатуються в агресивних середовищах, швидше зношуються або руйнуються.

Для забезпечення довговічності та збереженості мережі необхідно проводити такі заходи:

- вибір надійних матеріалів і конструкцій. При проектуванні і виготовленні мережі слід враховувати фактори, які впливають на її довговічність та збереженість.
- застосування заходів захисту від агресивних середовищ. Мережі, які експлуатуються в агресивних середовищах, слід захищати від їх впливу.
- регулярне технічне обслуговування. Регулярне технічне обслуговування дозволяє виявити і усунути потенційні проблеми з мережею до того, як вони призведуть до її зносу або руйнування.

1.4 Ремонтопридатність та відновлення

Ремонтопридатність - це характеристика надійності, яка визначає ймовірність того, що система може бути відновлена до робочого стану після відмови. Ремонтопридатність часто вимірюється коефіцієнтом

ремонтопридатності, який є відношенням часу ремонтопридатності до загального часу роботи системи.

Надійні мережі, які легко ремонтуються, можуть забезпечити безперебійну роботу і мінімізувати фінансові збитки в разі відмови або пошкодження.

Для підвищення ремонтопридатності мережі зазвичай впроваджують:

- використання модульної архітектури. Модульна архітектура дозволяє легко замінити пошкоджені компоненти мережі.
- використання стандартизованих компонентів. Стандартизовані компоненти більш доступні і легше замінюються.
- впровадження системи моніторингу. Система моніторингу дозволяє виявити проблеми з мережею на ранній стадії, що може допомогти запобігти їх поширенню.

Відновлення роботи мережі - це процес, який дозволяє відновити роботу мережі після відмови або пошкодження. Відновлення роботи мережі може бути складним і тривалим процесом, залежно від характеру відмови або пошкодження.

Основні етапи відновлення роботи мережі:

1. ідентифікація проблеми. На цьому етапі необхідно визначити причину відмови або пошкодження мережі. Це може бути зроблено за допомогою аналізу даних з системи моніторингу мережі, а також за допомогою опитування користувачів мережі.
2. усунення проблеми. На цьому етапі необхідно усунути причину відмови або пошкодження мережі. Це може бути зроблено шляхом заміни пошкоджених компонентів, налаштування параметрів мережі або інших заходів.
3. відновлення працездатності мережі. На цьому етапі необхідно відновити працездатність мережі. Це може бути зроблено шляхом запуску мережевих служб, відновлення даних і інших заходів.

Для успішного відновлення роботи мережі необхідно:

- мати план відновлення. План відновлення повинен включати в себе процедури для ідентифікації проблеми, усунення проблеми та відновлення працездатності мережі.

- мати доступ до необхідних ресурсів. Для відновлення роботи мережі можуть знадобитися запасні частини, обладнання та персонал.
- мати кваліфікований персонал. Персонал, який відповідає за відновлення роботи мережі, повинен бути кваліфікований для виконання цих робіт.

2 НАДІЙНІСТЬ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Надійність обладнання

Фактори, які впливають на надійність можна класифікувати як показано на рисунку 2.1:

Рисунок 2.1 – Класифікація факторів надійності

Технічні фактори є найбільш важливими факторами, що впливають на надійність системи. Надійність обладнання та програмного забезпечення є основними факторами, які визначають надійність системи в цілому. Надійність структури системи також відіграє важливу роль, оскільки вона може впливати на ймовірність виникнення збоїв.

Експлуатаційні фактори також можуть мати значний вплив на надійність системи. Кваліфікований персонал, який проводить технічне обслуговування системи, може підвищити її надійність. Правильна організація експлуатації системи також може допомогти запобігти збоїв.

Зовнішні фактори зазвичай неможливо контролювати, але їх вплив можна знизити за допомогою відповідних заходів. Наприклад, обладнання можна розміщувати в безпечних місцях, щоб захистити його від природних катаклізмів.

Надійність обладнання мережі - це ймовірність того, що обладнання буде працювати безперебійно протягом заданого інтервалу часу. Надійність обладнання мережі залежить від багатьох факторів.

Конструкція обладнання. Чим краще продумана конструкція обладнання, тим менше ймовірність його відмови.

Якість матеріалів. Чим якісніші матеріали, з яких виготовлено обладнання, тим менше ймовірність його відмови.

Технологія виготовлення. Чим більш досконала технологія виготовлення обладнання, тим менше ймовірність його відмови.

Умови експлуатації. Чим жорсткіші умови експлуатації обладнання, тим вища ймовірність його відмови.

Заходи щодо підвищення надійності обладнання мережі:

- вибір обладнання від надійних виробників - це один з найважливіших заходів щодо підвищення надійності обладнання мережі. Надійні виробники використовують якісні матеріали і технології виготовлення, а також проводять ретельну перевірку обладнання перед випуском.
- проведення своєчасного обслуговування і ремонту обладнання також є важливим заходом щодо підвищення надійності обладнання мережі. Під час обслуговування і ремонту обладнання усуваються виявлені дефекти, що може запобігти відмовам обладнання в майбутньому.
- застосування резервування обладнання - це ще один ефективний захід щодо підвищення надійності обладнання мережі. Резервування дозволяє

забезпечити безперебійну роботу мережі у разі відмови одного з компонентів.

На кожному етапі життєвого циклу комп'ютерних систем та мереж існують свої методи забезпечення надійності.

На етапі складання технічного завдання збирають всі дані, які є, про аналогічні та близькі системи, дані про умови застосування комп’ютерних систем і вимоги, що висуваються до функцій, які виконуються розглянутою системою. За сукупністю цих даних і вимог розробляються основні вимоги до надійності нової системи.

На етапі ескізного проектування обирається елементна база і визначаються особливості структури, архітектури та організації системи, яка розробляється. За цими даними проводиться попередній розрахунок надійності, виявляються найменш надійні підсистеми, і на цій основі приймається рішення про резервування системи, а також рішення про засоби та організацію технічного обслуговування, тобто профілактичні та ремонтні роботи. Досліджується питання про доцільність резервування і методи автоматичного відновлення та підвищення відмовостійкості системи.

Під час виконання технічного і робочого проектування перевіряються та уточнюються раніше прийняті рішення. Для цього використовують уточнені дані про надійність, отримані на основі розрахунків, зважаючи на режими роботи і точну номенклатуру елементів системи, а також результати експериментів над моделями, макетами, дослідними та промисловими зразками. Розробляється програмне забезпечення системи, проводиться його перевірка та діагностування за тестами і шляхом імітаційного моделювання на моделі системи, яка проектується. З метою забезпечення надійності здійснюють виявлення та виправлення всіх помилок в документації, яка розробляється.

На етапі виробництва основним є технічний контроль, який охоплює всі стадії виробничого процесу, починаючи від вхідного контролю якості матеріалів, які надходять, і комплектуючих виробів, включаючи контроль якості та відповідність технічній документації виготовлених друкованих плат, блоків,

пристроїв, схемних з’єднань, конструкції, і закінчуючи випробуваннями готової продукції. Виявляються недоліки в розробці, які впливають на надійність системи, та приймаються заходи з метою їх усунення.

На етапі експлуатації здійснюється контроль та забезпечення умов навколишнього середовища, які передбачаються проектом, забезпечення достатньої кваліфікації та необхідного складу обслуговуючого персоналу, організація та проведення техобслуговування і ремонтів. Продовжується збирання інформації про відмови апаратури і програмного забезпечення, які передаються розробникам з метою усунення причин відмов.

2.2 Надійність програмного забезпечення

Надійність програмного забезпечення - це ймовірність того, що програмне забезпечення буде працювати безперебійно протягом заданого інтервалу часу. Надійність програмного забезпечення залежить від якості коду, процедури розробки та умов експлуатації.

Заходи щодо підвищення надійності програмного забезпечення:

- вибір надійних інструментів розробки - це один з найважливіших заходів щодо підвищення надійності програмного забезпечення. Надійні інструменти розробки дозволяють створювати якісний код з меншою кількістю помилок.
- проведення ретельного тестування програмного забезпечення також є важливим заходом щодо підвищення надійності програмного забезпечення. Під час тестування програмного забезпечення виявляються і усуваються виявлені помилки, що може запобігти відмовам програмного забезпечення в майбутньому.
- застосування резервування програмного забезпечення - це ще один ефективний захід щодо підвищення надійності програмного забезпечення.

Підвищити надійність програмного забезпечення можливо наступними методами:

- використовувати статичний аналіз коду. Статичний аналіз коду дозволяє виявити помилки в коді до того, як він буде запущений.
- використовувати динамічний аналіз коду. Динамічний аналіз коду дозволяє виявити помилки в коді під час його виконання.
- впроваджувати рефакторинг коду. Рефакторинг коду дозволяє покращити якість коду і зробити його більш надійним.
- проводити тестування програмного забезпечення на різних платформах. Тестування програмного забезпечення на різних платформах дозволяє виявити помилки, які можуть виникнути на певних платформах.
- впроваджувати систему моніторингу програмного забезпечення. Система моніторингу програмного забезпечення дозволяє виявляти проблеми з програмним забезпеченням на ранній стадії.

2.3 Зовнішні фактори

Зовнішні фактори можуть призвести до збоїв у роботі комп’ютерних мереж. До зовнішніх факторів відносяться:

- природні катаклізми, такі як землетруси, урагани, повені та інші, можуть пошкодити обладнання мережі, що призведе до її відмови. Наприклад, землетрус може пошкодити кабелі, що зв'язують різні компоненти мережі, ураган може пошкодити будівлі, в яких розташовані компоненти мережі, а повінь може залити обладнання мережі.
- атаки зловмисників, такі як DDoS-атаки, атаки на програмне забезпечення або атаки на обладнання, також можуть призвести до збоїв у роботі мережі. DDoS-атака - це атака, яка спрямована на перевантаження мережі запитами, що може призвести до її відмови. Атака на програмне забезпечення може призвести до порушення роботи програмного забезпечення, що може привести до відмови мережі. Атака

на обладнання може призвести до пошкодження обладнання, що може призвести до відмови мережі.

- фактори навколишнього середовища, такі як перепади напруги, перебої з електропостачанням або пожежі, також можуть призвести до збоїв у роботі мережі.

Повністю захистити мережу від зовнішніх факторів неможливо. Однак, впроваджуючи відповідні заходи, можна істотно знизити ризик збоїв у роботі мережі. Важливо розуміти, що зовнішні фактори можуть призвести до збоїв у роботі мережі в будь-який час. Тому важливо розробити план управління надійністю мережі, який враховує потенційний вплив зовнішніх факторів і впроваджує відповідні заходи для його зниження.

Серед способів підвищення надійності комп'ютерної мережі можна виділити наступні:

- використання надійного обладнання. Обладнання мережі, яке має високу надійність, менш схильне до збоїв;
- використання надійного програмного забезпечення. Програмне забезпечення мережі, яке має високу якість, менш схильне до помилок;
- використання резервування. Резервування дозволяє відновити роботу мережі у разі виходу з ладу одного з компонентів;
- використання моніторингу. Моніторинг дозволяє виявити проблеми з мережею на ранній стадії, що може допомогти запобігти збоїв.

3 МОДЕЛІ НАДІЙНОСТІ КОМП’ЮТЕРНОЇ МЕРЕЖІ

3.1 Надійність комп’ютерної мережі за топологією

Топологія комп'ютерної мережі - це схема, яка визначає спосіб підключення компонентів мережі один до одного. Топологія мережі може впливати на її надійність, оскільки вона визначає, як відмова одного з компонентів може вплинути на роботу інших компонентів.

Надійність комп'ютерної мережі за топологією можна оцінити за допомогою таких факторів:

- кількість точок відмови. Точкою відмови називається компонент мережі, відмова якого може призвести до відмови всієї мережі. Чим менше точок відмови в мережі, тим вона надійніша.
- взаємозв'язок між компонентами. Чим більшою є взаємозв'язок між компонентами мережі, тим більша ймовірність того, що відмова одного компонента призведе до відмови інших компонентів.
- резервування. Резервування дозволяє забезпечити безперебійну роботу мережі у разі відмови одного з її компонентів.

Основні типи топологій комп'ютерних мереж:

- шина. У шинній топології всі компоненти мережі підключені до одного кабелю. Це найпростіша топологія, але вона має низьку надійність, оскільки відмова одного з компонентів може призвести до відмови всієї мережі.
- зірка. У зірковій топології всі компоненти мережі підключені до центрального комутатора. Це більш надійна топологія, ніж шинна, оскільки відмова одного з компонентів не призведе до відмови всієї мережі.
- кільце. У кільцевій топології всі компоненти мережі підключені один до одного в кільце. Це більш надійна топологія, ніж шинна, оскільки

відмова одного з компонентів не призведе до відмови всієї мережі.

- гібридна. Гібридна топологія - це комбінація двох або більше основних топологій.

Надійність комп'ютерної мережі за топологією може бути покращена за допомогою таких заходів:

- використання топології з меншою кількістю точок відмови, наприклад, зірки або кільця.
- використання резервування для критичних компонентів мережі.
- використання балансування навантаження для рівномірного розподілу навантаження на компоненти мережі.

Застосування цих заходів може допомогти підвищити надійність комп'ютерної мережі і мінімізувати ризик її відмови.

Наведемо приклади того, як топологія мережі може впливати на її надійність:

- у шинній топології відмова одного з компонентів може призвести до відмови всієї мережі, оскільки всі компоненти мережі підключені до одного кабелю.
- у зірковій топології відмова одного з компонентів, крім центрального комутатора, не призведе до відмови всієї мережі, оскільки інші компоненти мережі підключені до центрального комутатора.
- у кільцевій топології відмова одного з компонентів може призвести до відмови всієї мережі, оскільки всі компоненти мережі підключені один до одного в кільце.

При виборі топології комп'ютерної мережі необхідно враховувати всі ці фактори, щоб забезпечити оптимальну комбінацію надійності, вартості та інших характеристик мережі.

3.2 Надійність комп’ютерної мережі за структурно-логічним аналізом

Надійність комп'ютерної мережі за структурно-логічним аналізом - це оцінка ймовірності того, що мережа буде працювати безперебійно, враховуючи її структуру і логіку роботи.

Структурно-логічний аналіз (СЛА) - це метод, який дозволяє оцінити надійність системи, розглядаючи її як сукупність взаємодіючих компонентів. При структурно-логічному аналізі мережі враховуються такі фактори, як:

- структура мережі. Які компоненти мережі є, як вони підключені один до одного, і які функції вони виконують.
- логіка роботи мережі. Які процеси і потоки даних існують у мережі.
- надійність компонентів мережі. Яка ймовірність відмови кожного з компонентів мережі.

Для оцінки надійності комп'ютерної мережі за структурно-логічним аналізом можна використовувати такі методи:

- математичний аналіз. Цей метод передбачає використання математичних моделей для розрахунку надійності мережі.
- симуляція. Цей метод передбачає використання комп'ютерної симуляції для моделювання поведінки мережі і оцінки її надійності.
- аналіз відмов. Цей метод передбачає аналіз історичних даних про відмови мережі для оцінки її надійності.

Математична модель надійної комп'ютерної мережі - це модель, яка дозволяє оцінити надійність мережі за допомогою математичних розрахунків.

Наведемо підходи до побудови математичної моделі надійної комп'ютерної мережі:

1) модель графу. Мережа може бути представлена як граф, де вершини представляють компоненти мережі, а ребра представляють зв'язки між компонентами. Надійність мережі може бути оцінена на основі надійності компонентів мережі і характеристик зв'язків між ними.

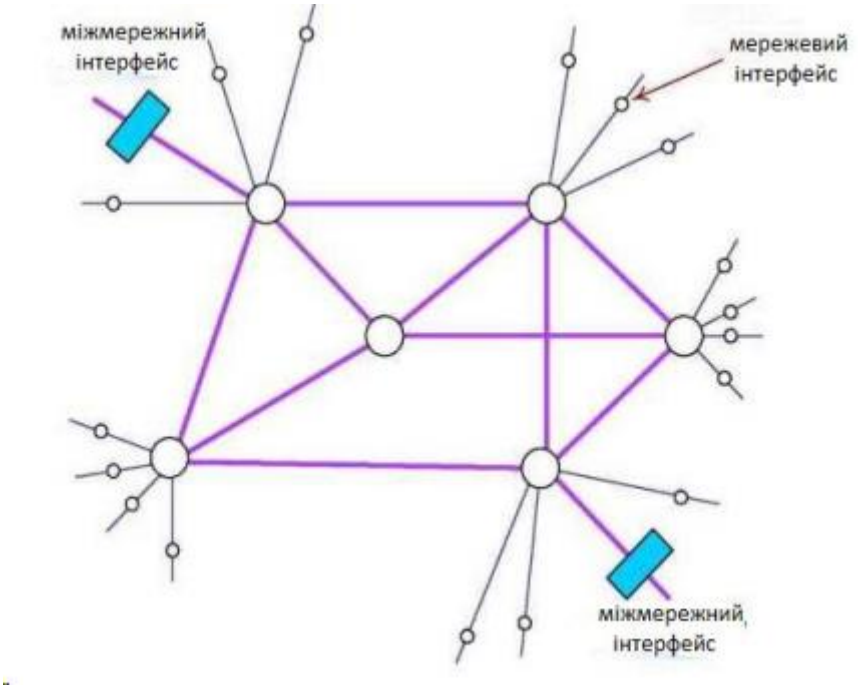

Рисунок 3.1 – Приклад представлення комп’ютерної мережі у вигляді графа

2) модель марковських процесів. Марковський процес - це процес, в якому майбутній стан системи залежить лише від її стану в поточний момент часу. Мережа може бути представлена як марковський процес, де стани системи представляють різні конфігурації мережі. Надійність мережі може бути оцінена на основі матриці переходів марковського процесу.

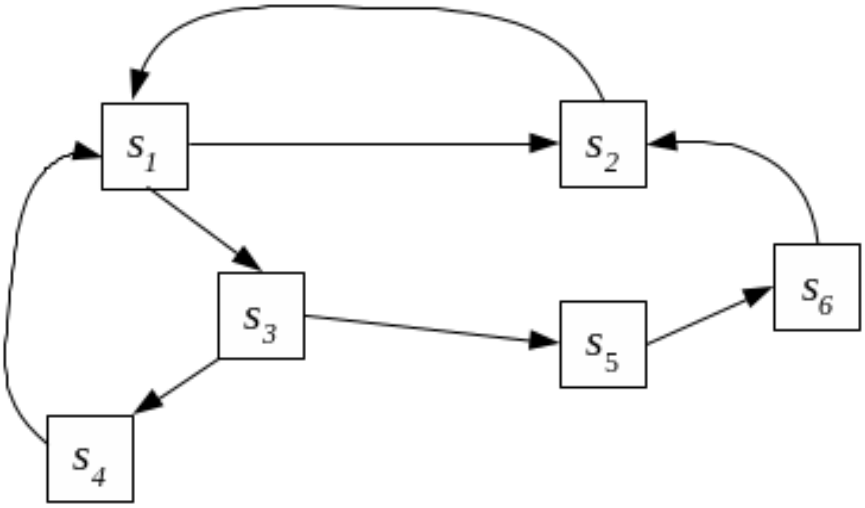

Рисунок 3.2 – Приклад представлення комп’ютерної мережі у вигляді марковського ланцюга

3) модель Монте-Карло. Метод Монте-Карло - це метод, який дозволяє оцінити ймовірність події шляхом проведення великої кількості випадкових експериментів. Мережа може бути представлена як модель Монте-Карло, де випадкові експерименти моделюють відмову компонентів мережі. Надійність мережі може бути оцінена на основі даних, отриманих в результаті випадкових експериментів.

Симуляція надійної комп'ютерної мережі є потужним інструментом для оцінки надійності мережі. При правильному використанні вона може допомогти організації розробити ефективні заходи для підвищення надійності мережі.

До переваг симуляції надійної комп'ютерної мережі належать:

1) симуляція дозволяє оцінити надійність мережі в реальних умовах експлуатації.

2) симуляція дозволяє швидко і легко проводити експерименти з різними конфігураціями мережі.

3) симуляція дозволяє оцінити вплив різних факторів на надійність мережі.

Серед недоліків симуляції надійної комп'ютерної мережі можна виділити:

1) симуляція може бути складною і трудомісткою.

2) симуляція може бути неточною, якщо модель мережі не відображає реальні умови експлуатації.

Загалом, симуляція є ефективним методом оцінки надійності комп'ютерної мережі. Однак, при використанні симуляції необхідно враховувати її переваги і недоліки.

3.3 Моделі надійності програмного забезпечення

Математичні моделі дозволяють оцінювати характеристики помилок в програмах та прогнозувати їх надійність при проектуванні та експлуатації. Моделі мають ймовірнісний характер, та достовірність прогнозів залежить від

точності початкових даних й глибини прогнозування за часом. Ці математичні моделі призначені для оцінки:

– показників надійності програмного забезпечення в процесі відлагодження;

– кількості помилок, що залишилися невиявленими;

– часу, необхідного для виявлення наступної помилки в функціонуючій програмі;

– часу, необхідного для виявлення всіх помилок із заданою ймовірністю.

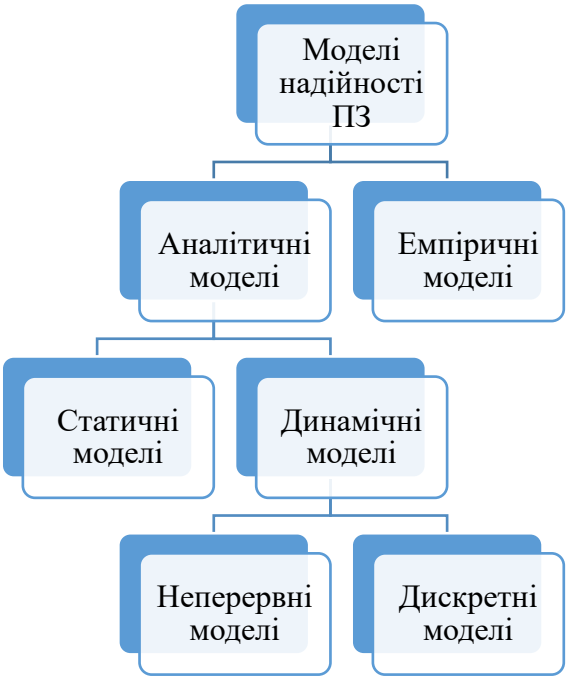

Рисунок 3.3 - Класифікація моделей надійності ПЗ [6]

Аналітичні моделі дають можливість розраховувати кількісні показники надійності, ґрунтуючись на даних про поведінку програми в процесі тестування (моделі вимірювання та оцінювання).

Емпіричні моделі базуються на аналізі структурних особливостей програм. Вони розглядають залежність показників надійності від числа міжмодульних зв'язків, кількості циклів в модулях, тощо. Часто емпіричні моделі не дають кінцевих результатів показників надійності, проте вони включені в класифікаційну схему, оскільки розвиток цих моделей дозволяє виявляти взаємозв'язок між складністю ПЗ та його надійністю. Ці моделі можна

використовувати на етапі проектування ПЗ, коли здійснюється розбивка на модулі та відома його структура.

Аналітичні моделі представлені двома групами: динамічні моделі та статичні. У динамічних поведінку ПЗ (поява відмов) розглядається в часі. У статичних моделях появу відмов не пов'язують з часом, а враховують тільки залежність кількості помилок від числа тестових прогонів (по області помилок) або залежність кількості помилок від характеристики вхідних даних (по області даних).

Для використання динамічних моделей необхідно мати дані про появу відмов у часі. Якщо фіксуються інтервали кожного відмови, то виходить неперервна картина появи відмов у часі (група динамічних моделей з неперервним часом). З іншого боку, може фіксуватися тільки число відмов за довільний інтервал часу (дискретні моделі).

3.4 Кількісні характеристики надійності

Кількісні характеристики надійності - це ймовірнісні характеристики, які використовуються для оцінки надійності системи.

Основні кількісні характеристики надійності:

- ймовірність безвідмовної роботи $P(T)$ - це ймовірність того, що система буде працювати безперебійно протягом заданого інтервалу часу T;
- ймовірність відмови $Q(T)$

$$Q(T) = 1 - P(T) \tag{3.1}$$

- середній час безвідмовної роботи (MTBF) - це середній час, протягом якого система працює безперебійно до першої відмови;
- середнє напрацювання на відмову T_i – математичне сподівання часу роботи до чергової відмови

$$T_i = \int_0^t t \cdot f(t)dt \tag{3.2}$$

- інтенсивність відмов $\lambda(t)$ - це ймовірність того, що система відмовить в

одиницю часу

$$\lambda(t) = f(t)/P(T) \tag{3.3}$$

де $f(t)$ – щільність імовірності відмови в момент часу t;

- коефіцієнт надійності $R(t)$ - це ймовірність того, що система буде працювати безперебійно до часу t;
- коефіцієнт готовності $G(t)$ - це ймовірність того, що система буде готова до роботи в момент часу t.

Ймовірнісні характеристики надійних комп'ютерних мереж можуть бути визначені для випадку статистично незалежних вузлів. Будь-яка двополюсна мережа з m вузлів буде зв'язаною з ймовірністю $g(p)$ та замкнута з ймовірністю $h(p)$:

$$g(p) = \sum_{k=0}^{m} B_i p^i (1-p)^{m-i} \tag{3.4}$$

$$h(p) = \sum_{k=0}^{m} A_i p^i (1-p)^{m-i} \tag{3.5}$$

де p – ймовірність того, що вузол розімкнено;

B_i (аналогічно A_i) – кількість комбінацій з i вузлів, таких, що мережа розмикається (замикається), якщо ці i вузлів розмикаються (замикаються), а інші m-i вузлів замикаються (розмикаються).

4 АНАЛІЗ НАДІЙНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

4.1 Аналіз ймовірності

Аналіз надійності мережі - це процес оцінки ймовірності відмови мережі або її компонентів. Аналіз надійності може бути важливим для таких цілей, як:

- проектування мережі. Аналіз надійності може використовуватися для визначення того, чи буде мережа достатньо надійною для задоволення встановлених вимог.
- оцінка надійності мережі. Аналіз надійності може використовуватися для оцінки того, чи відповідає надійність мережі встановленим вимогам.
- планування технічного обслуговування. Аналіз надійності може використовуватися для визначення того, які компоненти мережі потребують технічного обслуговування в першу чергу.

Існує багато різних методів аналізу надійності мережі. Вибір методу залежить від конкретних умов і вимог.

Однією з найпоширеніших методик аналізу надійності мережі є аналіз ймовірності. Аналіз ймовірності заснований на припущенні, що відмова кожного компонента мережі є випадковою подією. Імовірність відмови компонента можна оцінити на основі статистичних даних про відмову компонентів того ж типу.

Аналіз ймовірності можна використовувати для оцінки надійності мережі в цілому, а також надійності окремих компонентів мережі. Аналіз ймовірності може бути використаний для визначення того, чи відповідає надійність мережі встановленим вимогам.

До методів аналізу ймовірності, які використовуються для аналізу надійності мережі можна віднести:

- аналіз дерева відмов (АДВ) - це метод, який використовується для побудови дерева, що представляє всі можливі шляхи відмови мережі. Імовірність відмови мережі може бути оцінена на основі ймовірностей

відмови окремих компонентів мережі. Аналіз дерева відмов є ефективним для оцінки надійності мережі з невеликою кількістю компонентів.

- аналіз марківських ланцюгів (АМЛ) - це метод, який використовується для моделювання поведінки мережі в часі. Імовірність відмови мережі може бути оцінена на основі ймовірностей переходу мережі з одного стану в інший. Аналіз марківських ланцюгів є ефективним для оцінки надійності мережі з великою кількістю компонентів.
- аналіз Монте-Карло (АМК) - це метод, який використовується для оцінки ймовірності випадкової події шляхом проведення великої кількості випадкових експериментів. Імовірність відмови мережі може бути оцінена шляхом проведення великої кількості експериментів, в яких моделюється відмова мережі. Аналіз Монте-Карло є ефективним для оцінки надійності мережі з складною поведінкою.

4.2 Аналіз відмов

Аналіз відмов - це метод аналізу надійності мережі, який використовується для виявлення та аналізу причин відмов мережі. Аналіз відмов є важливим інструментом для підвищення надійності мережі, оскільки він дозволяє виявити і усунути потенційні джерела відмов.

Аналіз відмов може проводитися за допомогою різних методів.

Аналіз причинно-наслідкового зв'язку (АПНЗ) - це метод, який використовується для встановлення причинно-наслідкового зв'язку між відмовою мережі та її компонентами. Аналіз причинно-наслідкового зв'язку дозволяє визначити, який компонент мережі був причиною відмови, і які фактори призвели до відмови цього компонента.

Аналіз кореневої причини (АКП) - це метод, який використовується для виявлення кореневої причини відмови мережі. Аналіз кореневої причини і

дозволяє визначити основну причину відмови, яка може бути не очевидна на перший погляд.

Ці два методи складаються з практично однакових етапів.

1. Збір даних. На цьому етапі збираються дані про відмову мережі. До даних можуть входити:
    - опис відмови
    - час і місце відмови
    - компоненти мережі, які були залучені в відмову
    - дані про роботу мережі перед відмовою
2. Ідентифікація можливих причин. На цьому етапі ідентифікуються можливі причини відмови. Можливі причини можуть бути:
    - технічні проблеми з компонентами мережі
    - неправильне використання мережі
    - природні катаклізми
    - атаки зловмисників
3. Формування гіпотез. На цьому етапі формуються гіпотези про те, яка причина була основною причиною відмови.
4. Перевірка гіпотез. На цьому етапі перевіряються гіпотези. Це може бути зроблено шляхом проведення експериментів, аналізу даних або опитування експертів.
5. Визначення основних причин. На цьому етапі визначаються основні причини відмови. Основні причини - це причини, які призвели до відмови безпосередньо.
6. Рекомендації щодо усунення причин. На цьому етапі розробляються рекомендації щодо усунення причин відмови.

Аналіз модифікованого дерева відмов (АМДВ) - це метод, який використовується для виявлення потенційних джерел відмов мережі. Аналіз модифікованого дерева відмов створює дерево, яке представляє всі можливі

шляхи відмови мережі. Потім аналізуються кожна гілка дерева, щоб визначити потенційні джерела відмов.

АМДВ складається з наступних етапів.

1. Опис мережі. На цьому етапі описується мережа, яка аналізується. Опис повинен бути якомога більш детальним, щоб можна було зрозуміти, як мережа працює.
2. Ідентифікація компонентів мережі. На цьому етапі ідентифікуються компоненти мережі, які можуть відмовити.
3. Побудова дерева відмов. На цьому етапі будується дерево, яке представляє всі можливі шляхи відмови мережі.
4. Аналіз дерева відмов. На цьому етапі аналізуються кожна гілка дерева, щоб визначити потенційні джерела відмов.
5. Рекомендації щодо усунення причин. На цьому етапі розробляються рекомендації щодо усунення потенційних джерел відмов.

4.3 Аналіз чутливості

Аналіз чутливості - це метод аналізу надійності мережі, який використовується для оцінки впливу зміни ймовірності відмови одного або декількох компонентів мережі на ймовірність відмови мережі в цілому.

Аналіз чутливості є важливим інструментом для підвищення надійності мережі. Він дозволяє оцінити вплив зміни ймовірності відмови одного або декількох компонентів мережі на ймовірність відмови мережі в цілому, що може призвести до розробки більш ефективних заходів щодо підвищення надійності мережі.

Таблиця 4.1 – Порівняння методів аналізу надійності комп’ютерних мереж

Метод	Переваги	Недоліки
Аналіз ймовірності	Точний метод оцінки ймовірності відмови мережі	Може бути трудомістким методом, особливо якщо мережа є складною
	Дозволяє розробити ефективні заходи щодо підвищення надійності мережі	Може бути складним методом, особливо якщо мережа є складною
Аналіз причинно-наслідкового зв'язку та Аналіз кореневої причини	Дозволяє встановити основні причини відмови, які можуть бути не очевидними на перший погляд	Може бути трудомістким методом, особливо якщо необхідно зібрати багато даних
	Дозволяє розробити ефективні заходи щодо усунення причин відмови	Може бути суб'єктивним методом, оскільки він залежить від досвіду і знань експертів, які проводять аналіз
Аналіз дерева відмов	Дозволяє швидко і ефективно виявити потенційні джерела відмов	Може бути не точним методом, оскільки він не враховує всі можливі причини відмов
	Є відносно простим у застосуванні методом	Може бути суб'єктивним методом, оскільки він залежить від досвіду і знань експертів, які проводять аналіз
Аналіз модифікованого дерева відмов	Дозволяє отримати більш точну оцінку ймовірності відмови мережі	Може бути більш трудомістким методом, ніж стандартний метод
	Дозволяє розробити більш ефективні заходи щодо підвищення надійності мережі	Може бути більш складним методом, ніж стандартний метод
Аналіз відмов	Швидкий і ефективний метод виявлення потенційних джерел відмов мережі	Може бути не точним методом, оскільки не враховує всі можливі причини відмов
	Дозволяє розробити ефективні заходи щодо усунення потенційних джерел відмов	Може бути суб'єктивним методом, оскільки залежить від досвіду і знань експертів, які проводять аналіз
Аналіз чутливості	Дозволяє оцінити вплив зміни ймовірності відмови одного або декількох компонентів мережі на ймовірність відмови мережі в цілому	Може бути трудомістким методом, особливо якщо необхідно оцінити вплив зміни ймовірності відмови багатьох компонентів мережі
	Дозволяє розробити більш ефективні заходи щодо підвищення надійності мережі	Може бути складним методом, особливо якщо мережа є складною

ВИСНОВОК ТА РЕКОМЕНДАЦІЇ

У роботі описано аналіз надійності комп'ютерної мережі різними методами, такими як аналіз за структурно-логічною схемою, аналіз дерева відмов, аналіз кореневої причини, аналіз марківських ланцюгів та інші. Визначено їх переваги та недоліки.

Для підвищення надійності комп'ютерної мережі рекомендовано:

- вибір надійного обладнання. При виборі обладнання мережі слід враховувати такі фактори, як надійність, продуктивність та вартість.
- використання надійного програмного забезпечення. При виборі програмного забезпечення мережі слід враховувати такі фактори, як надійність, сумісність та підтримка.
- використання резервування. Резервування дозволяє відновити роботу мережі у разі виходу з ладу одного з компонентів.
- використання моніторингу. Моніторинг дозволяє виявити проблеми з мережею на ранній стадії, що може допомогти запобігти збоїв.

Заходи щодо підвищення надійності комп'ютерної мережі слід вжити на всіх етапах її життєвого циклу, починаючи з проектування і закінчуючи експлуатацією.