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

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Система оцінювання надійності багаторівневої архітектури IoT-мереж»

КвРКІП. 013042.18.16.02 ПЗ

Виконав: студент 2 курсу, група КІ2м-23-2 _____ Владислав ПАСІЧНИК
Підпис Ім'я, прізвище

Керівник канд. техн. наук, доцент _____ Олексій ІВАНОВ
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, докто філософії, доцент
Ольга ПАВЛОВА
25 04 2025 р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

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

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

"1" 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Владиславу ПАСІЧНИКУ
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система оцінювання надійності багаторівневої архітектури IoT-мереж

Керівник проекту (роботи) Олексій ІВАНОВ, к.т.н., доцент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 08.01.2025 №8

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2025 р.

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

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

Аналіз відомих рішень та методів оцінювання надійності мереж IoT; постановка задачі

Багаторівнева архітектура IoT мережі та оцінка надійності

Моделі представлення функцій надійності рівнів для багаторівневої архітектури IoT мережі

Система оцінювання надійності багаторівневої архітектури IoT-мереж

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

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Сергій ЛИСЕНКО, професор кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «1» 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2024	виконано
3	Робота над розділом 1 – аналіз відомих рішень та методів оцінювання надійності мереж IoT; постановка задачі	01.11.2024	виконано
4	Робота над розділом 2 – розробка багаторівневої архітектури IoT мережі та оцінка надійності	01.12.2024	виконано
5	Робота над науковою публікацією	01.02.2025	виконано
6	Робота над розділом 3 – розробка моделей представлення функцій надійності рівнів для багаторівневої архітектури іот мережі	15.02.2025	виконано
7	Робота над розділом 4 – проектування системи оцінювання надійності IoT мережі	01.04.2025	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2025	виконано
9	Попередній захист ДРМ	29.04.2025	виконано
10	Захист ДРМ на засіданні ЕК	До 15.05.2025	

Студент _____ Владислав ПАСІЧНИК
Підпис Ім'я, прізвище

Керівник роботи _____ Олексій ІВАНОВ
Підпис Ім'я, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Система оцінювання надійності багаторівневої архітектури IoT-мереж

Автор роботи: Пасічник В.О.

Керівник роботи: Іванов О.В.

Пояснювальна записка: 71 с., 16 рис., 3 табл., 2 дод., 76 джерел.

ОЦІНЮВАННЯ НАДІЙНОСТІ, ІНТЕРНЕТ РЕЧЕЙ, БАГАТОРІВНЕВА АРХІТЕКТУРА

Об’єктом дослідження є процеси оцінювання надійності багаторівневої IoT-архітектури на основі методу RBD.

Предметом дослідження є система оцінювання надійності багаторівневої архітектури IoT-мереж.

Метою кваліфікаційної роботи магістра є визначення поточного стану надійності IoT мережі, періодів її стабільного функціонування, перехідних станів та критичних зон деградації шляхом залучення системи оцінювання надійності багаторівневої архітектури IoT-мереж.

Для розв’язання поставлених задач використовувалися методи моделювання надійності, статистичної оцінки, комп’ютерного моделювання.

Наукова новизна отриманих результатів:

− набула подальшого розвитку система оцінювання надійності багаторівневої архітектури IoT-мереж, яка дозволяє визначити поточний стан надійності багаторівневої IoT-мережі, виявити періоди її стабільного функціонування, перехідні стани та критичні зони деградації, і яка відрізняється від відомих залученням системного підходу до моделювання кожного рівня системи IoT через діаграми надійності (RBD), що дозволило враховувати особливості кожного рівня, аналізувати вплив окремих компонентів на загальну надійність системи;

− удосконалено прогнозно-аналітичний метод оцінювання надійності системи, який дозволяє визначати точки перегину функції надійності та

прогнозувати майбутні відмови, який відрізняється від відомих виявленням перехідних станів системи та зон критичного зниження надійності.

Практична значимість отриманих результатів полягає у можливості оцінювання надійності багаторівневих IoT-архітектур, що дозволяє виявляти вузькі місця в структурі системи, прогнозувати відмови та оптимізувати розподіл ресурсів.

У першому розділі здійснено аналіз існуючих рішень щодо підвищення надійності систем Інтернету речей та методів оцінювання надійності складних систем, що дозволило визначити їх сильні та слабкі сторони та сформулювати основну проблему дослідження.

На основі проведеного аналізу в другому розділі була запропонована п’ятирівнева архітектура IoT-мережі, яка включає рівні сприйняття, мережевого доступу, ядра мережі, проміжного програмного забезпечення та застосунків. Запропонована архітектура забезпечує ефективну інтеграцію різних IoT-пристроїв і технологій, модульність та гнучкість системи. Головним акцентом стала її адаптація для застосування методу RBD з метою оцінювання надійності, що дозволило чітко визначити критичні вузли системи та підвищити її загальну відмовостійкість.

У третьому розділі було запропоновано модель представлення функцій надійності для кожного рівня багаторівневої архітектури IoT-мережі. Використання методу діаграм надійності дозволило детально моделювати структурні особливості системи, аналізувати можливі сценарії відмов та визначати ключові компоненти, які впливають на загальну надійність мережі.

У четвертому розділі представлено систему оцінювання надійності IoT-мереж, що включає дві підсистеми: підсистему визначення функції надійності та підсистему прогнозно-аналітичного оцінювання надійності. Перша підсистема базується на методі RBD та дозволяє здійснювати системний аналіз архітектури IoT-мережі, тоді як друга підсистема використовує прогнозно-аналітичний підхід для визначення поточного стану мережі та передбачення майбутніх відмов.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АС – Автономна система

МТ – Мережева технологія

ОС – Операційна система

КЗМ – Канал зв’язку маршрутизації

СОН – Система оцінювання надійності

СРС – Сутність рівня сприйняття

BD – Big data

IoT – Internet of Things

RBD – Reliability Block Diagram

ВСТУП

Стрімкий розвиток Інтернету речей сприяє впровадженню складних багаторівневих систем, які забезпечують автоматизацію, моніторинг і управління у сферах промисловості, транспорту, енергетики та розумних міст. В основі таких систем лежать взаємопов’язані пристрої, датчики, комунікаційні модулі та серверна інфраструктура, що функціонують як єдина мережа для збору, обробки та передачі даних.

Оскільки надійність таких систем безпосередньо впливає на їхню ефективність та безперебійність роботи, постає питання розробки підходів до її оцінювання.

У контексті даного дослідження під IoT-мережами розуміється саме комплексна система, що складається з взаємопов’язаних пристроїв, датчиків, комунікаційних модулів та серверної інфраструктури, які працюють у єдиній архітектурі для збору, обробки та передачі даних.

З огляду на багаторівневий характер таких систем, питання їхньої надійності набуває критичного значення, адже відмова окремих компонентів може спричинити збої в роботі всієї мережі.

Для оцінювання та підвищення надійності систем Інтернету речей доцільно використовувати метод Reliability Block Diagram (RBD), що дозволяє аналізувати вплив відмов різних елементів, прогнозувати рівень надійності та розробляти стратегії підвищення стійкості до відмов. Враховуючи різноманітність IoT-архітектур, необхідно розробити підхід, який дозволить оцінювати надійність мережі, адаптуючись до її структурних особливостей та умов експлуатації.

Метою кваліфікаційної роботи магістра є визначення поточного стану надійності IoT мережі, періодів її стабільного функціонування, перехідних станів та критичних зон деградації шляхом залучення системи оцінювання надійності багаторівневої архітектури IoT-мереж.

Поставлена мета досягається розв’язанням таких основних завдань:

− проаналізувати відомі методи оцінювання надійності складних систем;

− дослідити багаторівневу архітектуру IoT мережі;

− розробити моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі;

− розробити систему оцінювання надійності багаторівневої архітектури IoT-мереж;

− розробити прогнозно-аналітичний метод оцінювання надійності системи та провести оцінку надійності системи Інтернету речей із різними підсистемами.

− провести дослідження оцінки надійності системи Інтернету речей, що складається із різних підсистем.

Об’єктом дослідження є процеси оцінювання надійності багаторівневої IoT-архітектури на основі методу RBD.

Предметом дослідження є система оцінювання надійності багаторівневої архітектури IoT-мереж.

Наукова новизна отриманих результатів:

− набула подальшого розвитку система оцінювання надійності багаторівневої архітектури IoT-мереж, яка дозволяє визначити поточний стан надійності багаторівневої IoT-мережі, виявити періоди її стабільного функціонування, перехідні стани та критичні зони деградації, і яка відрізняється від відомих залученням системного підходу до моделювання кожного рівня системи IoT через діаграми надійності (RBD), що дозволило враховувати особливості кожного рівня, аналізувати вплив окремих компонентів на загальну надійність системи;

− удосконалено прогнозно-аналітичний метод оцінювання надійності системи, який дозволяє визначати точки перегину функції надійності та прогнозувати майбутні відмови, який відрізняється від відомих виявленням перехідних станів системи та зон критичного зниження надійності.

На основі проведених досліджень розроблено систему оцінювання надійності багаторівневої архітектури IoT мереж.

Практична значимість отриманих результатів полягає у можливості оцінювання надійності багаторівневих IoT-архітектур, що дозволяє виявляти вузькі

місця в структурі системи, прогнозувати відмови та оптимізувати розподіл ресурсів.

Для розв’язання поставлених задач використовувалися методи моделювання надійності, статистичної оцінки, комп’ютерного моделювання.

За темою кваліфікаційної роботи опубліковано одну публікацію [76] у Збірнику наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2024». (Хмельницький – 2024. – С. 421-424).

1 АНАЛІЗ ВІДОМИХ РІШЕНЬ ОЦІНЮВАННЯ НАДІЙНОСТІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Аналіз методів оцінювання надійності складних систем

Методи оцінювання надійності складних технічних систем базуються на різних підходах, які дозволяють аналізувати ймовірність відмов, прогнозувати роботу системи та визначати її слабкі місця.

Один із найпоширеніших методів – діаграма надійності системи (Reliability Block Diagram, RBD). Він полягає в представленні системи у вигляді блокової структури, де кожен компонент має власну ймовірність безвідмовної роботи. Основними параметрами оцінювання в цьому методі є ймовірність відмови та середній час безвідмовної роботи (MTTF). Основною перевагою такого підходу є його візуальна зрозумілість та простота аналізу. Проте значним обмеженням є те, що він не враховує часову змінність параметрів, тобто зміни ймовірності відмов у процесі експлуатації системи.

Іншим підходом є марковські моделі, які застосовуються для аналізу надійності на основі ймовірнісного переходу між різними станами системи. У таких моделях система розглядається як сукупність можливих станів (наприклад, робочий стан, часткове пошкодження, повна відмова), між якими вона переходить відповідно до певних імовірностей. Основними параметрами оцінювання тут є ймовірність знаходження в тому чи іншому стані та інтенсивність відмов. Марковські моделі дозволяють більш точно оцінювати змінні стани системи та їх вплив на загальну надійність, однак їхній головний недолік – складність розрахунків, особливо для великих і складних систем.

Ще одним рішенням є метод Монте-Карло, який базується на проведенні численних імітаційних експериментів для оцінки ймовірнісних характеристик відмов та часу до відмови системи. Завдяки цьому підходу можна враховувати випадкові фактори та моделювати поведінку складних систем з великою кількістю взаємопов’язаних компонентів. Графічне подання оцінки надійності системи за допомогою методу Монте-Карло зображено на рис. 1.1

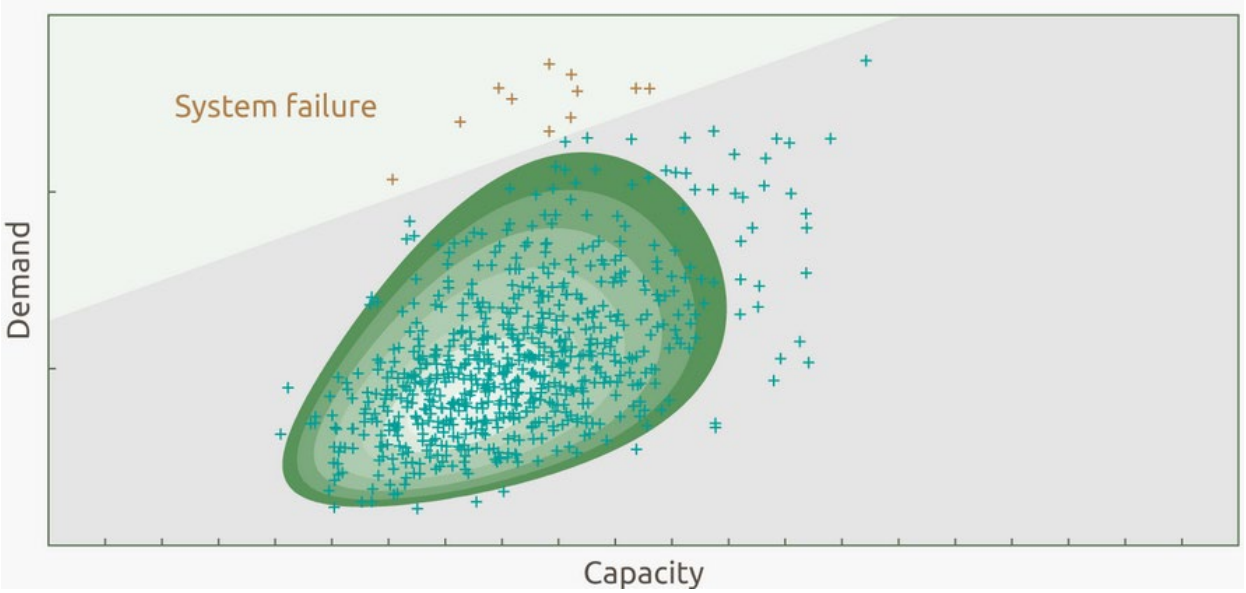


Рисунок 1.1 – Оцінка надійності за допомогою методу Монте-Карло [11]

Зображення ілюструє оцінку надійності системи за допомогою методу Монте-Карло. На графіку відображено співвідношення між попитом і пропускною здатністю системи. По горизонтальній осі показана пропускна здатність, яка визначає максимальне можливе навантаження, що може витримати система. По вертикальній осі відображається попит, тобто рівень навантаження, що пред'являється до системи в певний момент часу.

Зелена область із найбільшою щільністю точок показує імовірні сценарії, за яких система функціонує нормально, тобто попит не перевищує доступні ресурси. Однак у верхній частині графіка є зона, позначена як System failure, яка вказує на ситуації, коли попит перевищує пропускну здатність, що призводить до відмови системи. Окремі точки за межами основної хмари свідчать про рідкісні, але можливі випадки, коли система не справляється з навантаженням. Метод Монте-Карло тут використовується для статистичного моделювання, де багаторазово генеруються випадкові сценарії попиту та пропускної здатності. Для кожного з них визначається, чи зможе система працювати в нормальному режимі, чи вийде з ладу. Аналізуючи отримані результати, можна оцінити ймовірність відмови та зробити висновки щодо рівня надійності системи. Якщо більшість точок зосереджені в зеленій області, система є стабільною та здатною витримувати навантаження.

Якщо ж значна частина точок потрапляє в зону відмови, це свідчить про високий ризик збоїв і необхідність покращення ресурсів або оптимізації навантаження. Головною перевагою цього методу є його гнучкість та можливість врахування складних взаємозв'язків між компонентами. Проте значним обмеженням є високі обчислювальні витрати, що можуть робити його менш придатним для реального часу або аналізу надвеликих систем.

В умовах невизначеності або браку точних статистичних даних ефективним методом є застосування нечіткої логіки (Fuzzy Logic). Вона дозволяє оцінювати рівень надійності системи та ризик відмови на основі нечітких правил та експертних оцінок. Такий підхід особливо корисний у ситуаціях, коли класичні методи, що потребують точних числових даних, не можуть бути застосовані. Основною перевагою нечіткої логіки є можливість працювати в умовах невизначеності, проте значним недоліком є необхідність експертного налаштування правил і параметрів системи.

Ще одним структурним підходом до аналізу надійності є аналіз дерева відмов (Fault Tree Analysis, FTA). Ця методика дозволяє визначити основні причини відмов, оцінити їхню ймовірність та знайти критичні вузли системи, які потребують особливої уваги. Методика заснована на побудові ієрархічного дерева, де вершини відображають можливі несправності, а зв'язки між ними – їхні взаємозалежності. Це дозволяє виявляти найбільш вразливі місця системи та розробляти заходи щодо їх усунення. Проте основним недоліком цього підходу є складність побудови для великих систем із багатьма взаємозалежними компонентами.

Останнім часом все більшої популярності набирають методи, засновані на машинному навчанні, які дозволяють прогнозувати відмови на основі аналізу даних сенсорів та історичних записів про роботу системи. Такі методи можуть включати нейронні мережі, рішення на основі кластеризації або інші алгоритми штучного інтелекту. Вони дають змогу виявляти приховані закономірності та прогнозувати відмови з високою точністю, що дозволяє здійснювати превентивне технічне обслуговування. Основною перевагою такого підходу є його здатність до

самооптимізації та покращення прогнозів у процесі накопичення нових даних. Проте ключовим викликом є необхідність великих обсягів навчальних даних, без яких точність прогнозів може бути недостатньою.

Таблиця 1.1 – Аналіз методів оцінювання надійності складних систем

№	Метод оцінювання надійності	Параметри оцінювання	Переваги	Недоілки
1	Reliability Block Diagram (RBD)	Вірогідність відмови, середній час безвідмовної роботи (MTTF)	Візуалізація, простота аналізу	Не враховує часову змінність параметрів
2	Марковські моделі	Ймовірність станів, інтенсивність відмов	Врахування змінних станів системи	Складність розрахунків для великих систем
3	Монте-Карло моделювання	Імовірнісні характеристики відмов, час до відмови	Гнучкість, можливість моделювання складних систем	Високі обчислювальні витрати
4	Fuzzy Logic (нечітка логіка)	Рівень надійності, ризик відмов	Підходить для невизначених умов	Потребує експертного налаштування
5	Аналіз дерева відмов (FTA)	Основні причини відмов, ймовірність відмови	Виявлення критичних точок	Складність побудови для великих систем
6	Моделі на основі машинного навчання	Прогнозування відмов, аналіз даних сенсорів	Висока точність прогнозів	Необхідність великих обсягів навчальних даних

Отже, кожен із методів оцінювання надійності має свої особливості, які визначають його придатність до різних типів систем та умов їх експлуатації. RBD забезпечує простоту аналізу, марковські моделі дозволяють враховувати змінні стани, Монте-Карло підходить для моделювання складних випадкових процесів, нечітка логіка корисна в умовах невизначеності, FTA дозволяє знаходити критичні точки, а машинне навчання дає можливість прогнозувати відмови на основі великих даних.

1.2 Огляд відомих рішень визначення та оцінювання надійності систем Інтернету речей

У роботі [1] запропоновано механізм забезпечення відмовостійкості для програмно визначеного Інтернету речей (Software Defined IoT), який забезпечує безперервність роботи системи у разі збоїв у мережі, відмови пристроїв або перевантаження трафіку. Представлений механізм використовує штучний інтелект для виявлення та обробки відмов, що дозволяє підтримувати функціональність без необхідності змінювати апаратну або програмну інфраструктуру. Основні етапи реалізації FTM включають: 1) виявлення сервісів – використання гетерогенних обчислювальних пристроїв для моніторингу середовища та інтеграції віртуальних сервісів, що можуть замінити фізичні сервіси у разі відмови. Для цього застосовується регресійний аналіз, який визначає кореляцію між сенсорами та створює резервні сервіси без фізичного дублювання пристроїв; 2) відображення сервісів – попереднє та динамічне (під час виконання) відображення сервісів і функцій додатків. На основі зібраних даних оновлюються віртуальні сервіси, що дозволяє адаптивно змінювати мережеві параметри відповідно до поточних умов; 3) виконання сервісів – ієрархічний моніторинг стану сервісів та їх працездатності під час кластеризації у Software Defined-IoT. Використання ефективних механізмів моніторингу зменшує комунікаційні витрати та забезпечує швидке реагування на збої. Запропонована техніка дозволяє розробникам тестувати додатки на стійкість до відмов, оцінювати їхню надійність у реальному часі та усувати помилки ще до

розгортання у хмарному середовищі. Крім того, механізм підтримує два режими роботи: для адміністраторів віртуальних машин (VM admin) та адміністраторів хмарних середовищ (Cloud admin), що забезпечує гнучкість конфігурації та обробки різних типів збоїв.

У роботі [2] запропоновано агентно-орієнтовану, надійну та відмовостійку ієрархічну IoT-хмарну архітектуру, здатну витримувати збої серверів. Пропонована авторами архітектура має чотири рівні (хмара–туман–мла–роса), що забезпечує відмовостійкість через реплікацію даних на периферії мережі. У разі збою серверів додатки перенаправляються на альтернативні сервери відповідного рівня залежно від їхньої чутливості до затримок. Для забезпечення надійності дані реплікуються на всіх рівнях архітектури. У хмарних середовищах використовується механізм Availability Zone (AZ) для резервування, а на рівнях туману та мли – резервні сервери. Це гарантує збереження роботи IoT-додатків навіть у разі відмови серверів. Мобільні агенти (MA) відіграють ключову роль у керуванні збоями та моніторингу ресурсів. Вони збирають інформацію про стан системи та передають її іншим агентам у ієрархії. У разі збою агент визначає пріоритети IoT-додатків, шукає альтернативні сервери та виконує перенесення додатків і перенаправлення підключень. Якщо потужності рівня недостатньо, навантаження передається вище в ієрархії. Для підтвердження ефективності запропонованого рішення, авторами була проведена симуляція у середовищі Matlab.

Автори роботи [3] досліджують стратегії розміщення механізмів відмовостійкості в IoT-системах. Автори аналізують виклики, пов’язані з високою динамічністю, розподіленістю та обмеженими ресурсами IoT-пристроїв, що ускладнює реалізацію традиційних методів забезпечення надійності. Основна увага приділяється оптимальному розташуванню механізмів відмовостійкості в архітектурі IoT, включаючи хмарні, периферійні (edge) та гібридні середовища. Автори розглядають компроміс між продуктивністю, затримками та витратами ресурсів у різних сценаріях, оцінюючи ефективність методів реплікації, контрольних точок (checkpointing) і активного резервування (active replication). У дослідженні запропоновано модель розподілу механізмів відмовостійкості на

основі аналізу характеристик трафіку та обчислювальних можливостей вузлів IoT-мережі. Автори використовують емпіричне моделювання для оцінки продуктивності різних підходів. Результати дослідження демонструють, що комбіноване використання edge та cloud-рішень дозволяє покращити надійність IoT-систем при зниженні витрат на обчислення та передачу даних. Отримані висновки можуть бути корисними для розробників IoT-архітектур, що потребують балансування між відмовостійкістю та ефективним використанням ресурсів.

У роботі [4] досліджується надійність систем Sensor-Cloud Systems (SCS), які поєднують сенсорні мережі та хмарні обчислення для збору та обробки даних. Автори реалізували експериментальну систему для інтелектуальних продуктів і проаналізували способи підвищення її надійності в п’яти ключових напрямках: продуктивність мережевого зв’язку, автоматичне відновлення, локальне резервне копіювання, автоматизоване тестування програмного забезпечення та безпека системи. У статті запропоновано нову формулу для оцінювання надійності SCS на основі метрик із зазначених напрямків. Проведено порівняльний аналіз функціонування системи з і без впроваджених покращень, що показало значне підвищення її надійності завдяки впровадженню п’ятирівневої методики забезпечення відмовостійкості.

У роботі [5] досліджується інтеграція Інтернету речей (IoT) та сервіс-орієнтованих обчислень (SOC), зокрема питання надійності надання послуг і обмеженості ресурсів. Запропоновано ймовірнісний підхід для формального опису та аналізу надійності й вартості композиції сервісів у IoT. Спочатку модель композиції сервісів будується у вигляді скінченного автомата (FSM) для опису функціональних аспектів. Потім ця модель розширюється до марковського процесу прийняття рішень (MDP), що дозволяє оцінювати надійність операцій сервісів. Додатково MDP розширюється структурою витрат, яка враховує параметри якості сервісу, такі як енергоспоживання та вартість зв’язку. Для перевірки та аналізу цих властивостей використовується ймовірнісний розширений темпоральний логічний аналіз (PCTL) за допомогою інструменту PRISM.

У роботі [6] запропоновано підхід, заснований на сервісно-орієнтованій архітектурі (SOA), яка забезпечує IoT рівнем абстракції для інтеграції та управління сервісами. Авторами було розроблено проміжне програмне забезпечення (middleware), яке дозволяє пристроям взаємодіяти між собою для реалізації міжмодальної відмовостійкості. Якщо якийсь пристрій виходить з ладу, пропонована система може автоматично переналаштуватися, використовуючи інші пристрої для компенсації несправностей. Вирішення цієї проблеми розглядається на трьох рівнях управління сервісами: виявлення сервісів, їх зіставлення та виконання. На етапі виявлення сервісів було запропоновано метод адаптації сенсорів, який дозволяє створювати віртуальні сервіси. Це дає змогу компенсувати вихід з ладу реального пристрою, використовуючи дані з інших сенсорів. Для цього використовується регресійний аналіз, що дозволяє визначати та генерувати такі віртуальні сервіси, використовуючи методи рекурсивних найменших квадратів (RLS) або адаптивних мультиваріативних сплайнів (MARS), залежно від типу кореляції сенсорів. Це рішення допомагає значно збільшити кількість резервних сервісів без потреби в додатковому обладнанні. На етапі зіставлення сервісів цей процес розділено на два етапи. Перший передбачає попереднє картографування сервісів перед їх запуском, що формулюється як задача цілочисельного квадратичного програмування. В цьому процесі враховуються правила розміщення, які дозволяють користувачам визначати свої переваги та оптимізувати рішення. Другий етап відбувається в реальному часі, коли сервісна система використовує вже створені віртуальні сервіси для забезпечення відмовостійкості. Ця задача формулюється як багатоцільова оптимізаційна проблема, яка вирішується за допомогою генетичного алгоритму NSGA-II. Оновлення сенсорних даних дозволяє системі періодично виконувати повторне зіставлення сервісів, адаптуючись до змін у середовищі. На етапі виконання сервісів було розроблено ієрархічний механізм моніторингу, який дозволяє відстежувати стан пристроїв та оперативно виявляти несправності. Для цього було запропоновано метод кластеризації пристроїв з метою ефективного моніторингу. Завдання було змодельовано як варіацію проблеми багатьох комівояжерів (mTSP) без фіксованого

депо, де необхідно мінімізувати комунікаційні витрати на перевірку працездатності пристроїв. Для його вирішення запропоновано евристичні алгоритми, які дозволяють формувати оптимальні кластери та маршрути моніторингу. Симуляційні результати показали, що ці алгоритми дозволяють значно скоротити витрати на моніторинг, зберігаючи при цьому високу ефективність.

У роботі [7] запропоновано підхід до підвищення відмовостійкості багатошарової IoT-мережі шляхом впровадження прямокутної та інтерстиціальної сітчастої топології в шлюзовому рівні. Це рішення дозволяє зменшити ризик відмови мережі за рахунок усунення вузьких місць, характерних для традиційних методів з єдиним або обмеженою кількістю шлюзів. Авторами зозроблено ймовірнісну модель для оцінки рівня відмовостійкості запропонованої топології, а також два алгоритми: перший дозволяє будувати дерево відмов мережі (Fault Tree Analysis – FTA), другий – генерувати таблицю розрахунку коефіцієнта відмов на основі цього дерева. Методика оцінки відмовостійкості IoT-мережі базується на розрахунку показників надійності для різних рівнів мережі з використанням моделей ймовірнісного аналізу. Запропонований підхід був протестований за допомогою моделювання та експериментального аналізу. Виконано порівняльне дослідження з іншими методами підвищення відмовостійкості в шлюзовому рівні IoT-мереж, що показало переваги запропонованої топології.

У роботі [8] досліджується проблема забезпечення відмовостійкості в багаторівневих IoT-системах, враховуючи їхню складність, динамічність та гетерогенність. Автори пропонують підхід, що передбачає співпрацю між рівнями системи для запобігання поширенню помилок та підвищення надійності. Розроблено подієво-орієнтовану архітектуру FaTEMa, яка створює спеціальний канал зв’язку для поширення інформації про помилки між рівнями. Це дозволяє швидко виявляти збої та забезпечувати безперервність обслуговування. FaTEMa підтримує розширюваність для роботи з різними комунікаційними протоколами, що дозволяє адаптувати систему до нових технологій без значного ускладнення її структури. Запропонована архітектура включає: міжрівневий канал зв’язку, що дозволяє рівням обмінюватися даними про збої та адаптувати механізми

відмовостійкості; стандартизовану комунікацію, яка забезпечує сумісність між різнорідними пристроями та протоколами IoT; подієво-орієнтований підхід, що сприяє швидкій адаптації системи до змін у середовищі; колаборативне виявлення та усунення помилок, що дозволяє кожному рівню приймати рішення на основі локальної та отриманої інформації. Експериментальні результати показали, що використання FaTEMa покращує процес виявлення та усунення помилок, зменшує кількість відмов у системі та підвищує її доступність.

У роботі [9] запропоновано модель для аналізу доступності (availability) систем Інтернету речей (IoT), які використовують механізми візантійської відмовостійкості (Byzantine Fault Tolerance, BFT). Візантійська відмовостійкість є критично важливою для забезпечення безпеки, надійності та децентралізації в IoT-системах, особливо у контексті блокчейн-механізмів, які забезпечують взаємодію та транзакції між пристроями. Модель, розроблена в дослідженні, базується на використанні ланцюгів Маркова в неперервному часі (continuous-time Markov chains), що дозволяє аналізувати поведінку системи в умовах відмов та відновлення її компонентів. Основна увага в роботі приділена дослідженню залежності доступності системи від кількості вузлів (серверів) у мережі та співвідношення між чесними та візантійськими (нечесними або вузлами, що відмовили) вузлами. Модель враховує, що час між відмовами та час відновлення вузлів підпорядковуються експоненційним розподілам, а кількість візантійських вузлів може варіюватися за різними розподілами. Це дозволяє більш точно оцінити вплив різних параметрів на загальну доступність системи. Числові результати, отримані в ході дослідження, демонструють нелінійну залежність між кількістю вузлів у системі та її доступністю. Зокрема, показано, що доступність системи зменшується зі збільшенням кількості вузлів, і ця залежність стає більш вираженою при збільшенні співвідношення між частотою відмов та частотою відновлення. Це свідчить про те, що збільшення кількості серверів у мережі не завжди призводить до підвищення надійності, особливо в умовах високої ймовірності відмов.

У роботі [10] запропоновано механізм відмовостійкості, який спрямований на вирішення проблем, що виникають у Fog-IoT мережах, зокрема забезпечення

надійної та безпомилкової передачі даних. Fog Computing (FC) є перспективною парадигмою обчислень, яка дозволяє виконувати офлоадинг (offloading) завдань на пристрої туманних мереж, забезпечуючи більшу обчислювальну потужність, нижчі витрати, підвищену доступність та гнучкість. Однак зростання кількості завдань та їх складність створюють виклики для ефективного офлоадингу, що потребує розробки спеціалізованих механізмів для мінімізації відмов та оптимізації витрат. Основною метою дослідження є запропонувати та впровадити новий підхід до забезпечення відмовостійкості в Fog-IoT мережах. Для цього автори розробили два ключові механізми: Priority-based Task Offloading with Fault Tolerance (PToFT) – схему, яка дозволяє ідентифікувати несправні вузли туманної мережі (Fog Nodes, FNs) на основі залишкової енергії вузлів. Це дозволяє своєчасно виявляти та ізолювати несправні вузли, що забезпечує стабільну роботу системи; Min-cost Neighbour Candidate Node Discovery based on replication and forwarding (MNCND-RaF) – техніку, яка використовується для пошуку найбільш підходящих сусідніх вузлів для заміни несправних. Цей механізм забезпечує ефективну обробку завдань шляхом реплікації та перенаправлення інформації до нових вузлів, що дозволяє уникнути втрати даних та зниження продуктивності. Для оцінки ефективності запропонованих методів було проведено моделювання та порівняння з існуючими підходами до забезпечення відмовостійкості, такими як Without FT, NFT-WOA та DFTLA. Результати експериментів показали, що запропоновані методи перевершують існуючі підходи за показниками ефективності. Зокрема, PToFT та MNCND-RaF демонструють покращення продуктивності на 42,3 %, 36,2 % та 27,7 % порівняно з Without FT, NFT-WOA та DFTLA відповідно.

Результуючий порівняльний аналіз досліджених методів забезпечення відмовостійкості та їх методів оцінки надійності наведено у таблиці 1.1. Таким чином проведений огляд відомих рішень показав, що більшість робіт пропонують спеціалізовані механізми для підвищення надійності IoT-систем, такі як реплікація даних, використання агентів, віртуальних сервісів та ймовірнісних моделей. Проте головні недоліки пов’язані зі складністю реалізації, обмеженнями ресурсів та залежністю від точності моделювання.

Таблиця 1.2 – Порівняльний аналіз відомих методів забезпечення відмовостійкості та їх методів оцінки надійності

Робота	Метод оцінки надійності	Рівень/Архітектура	Основні механізми	Інструменти/Методології	Додаткові переваги
[1]	Регресійний аналіз для виявлення сервісів, моніторинг, AI для обробки відмов	Software Defined IoT	Виявлення, відображення, виконання сервісів	Немає конкретних інструментів, але використовується AI	Адаптивність, не потребує змін інфраструктури
[2]	Реплікація даних, ієрархічна архітектура	Хмара-Туман-Мла-Роса	Реплікація даних, мобільні агенти для керування збоями	Matlab для симуляції	Гнучкість при перенаправленні завдань
[3]	Аналіз компромісів між продуктивністю, затримками та ресурсами	Хмара, Edge, Гібрид	Реплікація, контрольні точки, активне резервування	Емпіричне моделювання	Оптимізація розміщення відмовостійкості
[4]	Формула для оцінювання надійності на основі	Sensor-Cloud Systems	Автоматичне відновлення, локальне	Експериментальна система для	Покращення надійності за кількома напрямками

	метрик продуктивності, відновлення, резервного копіювання, тестування та безпеки		резервне копіювання	інтелектуальних продуктів	
[5]	Ймовірнісний підхід, моделі FSM та MDP	Інтеграція IoT з SOC	Аналіз надійності через марковські процеси, оцінка вартості	PRISM для аналізу PCTL	Оцінка якості сервісу, включаючи енергоспоживання
[6]	Адаптація сенсорів, регресійний аналіз, кластеризація	SOA з middleware	Виявлення, зіставлення та виконання сервісів	Генетичні алгоритми (NSGA-II), метод багатьох комівояжерів	Висока відмовостійкість без додаткового обладнання
[7]	Ймовірнісна модель для оцінки відмовостійкості	Рівень шлюзів IoT	Прямокутна та інтерстиціальна сітчаста топологія	Моделювання, FTA, таблиця розрахунку коефіцієнта відмов	Зменшення вузьких місць у мережі

[8]	Подієво-орієнтована архітектура для співпраці між рівнями	Мультирівнева IoT система	Канал зв'язку для обміну інформацією про збої	FaTEMa для виявлення та усунення помилок	Підвищена доступність та швидкість реакції на збої
[9]	Аналіз доступності за допомогою ланцюгів Маркова в неперервному часі	Візантійська відмовостійкість для IoT	Врахування часу між відмовами та відновленням	Математичні моделі на основі ланцюгів Маркова	Дослідження нелінійних залежностей доступності
[10]	Пріоритетне оффлоадінг завдань, пошук найкращих альтернативних вузлів	Fog-IoT	PToFT, MNCND-RaF	Моделювання для порівняння ефективності	Значне покращення продуктивності та надійності

1.3 Постановка задачі

Таким чином поставлена мета дослідження досягається розв’язанням таких основних завдань:

- проаналізувати відомі методи оцінювання надійності складних систем;
- дослідити багаторівневу архітектуру IoT мережі;
- розробити моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі;
- розробити систему оцінювання надійності багаторівневої архітектури IoT-мереж;
- розробити прогнозно-аналітичний метод оцінювання надійності системи та провести оцінку надійності системи Інтернету речей із різними підсистемами.

1.4 Висновки до першого розділу

В результаті проведеного дослідження проведено огляд відомих рішень для підвищення надійності систем Інтернету речей, а також методів оцінювання надійності складних систем. Виокремлено їх сильні та слабкі сторони. Виконано постановку задачі дослідження.

2 БАГАТОРІВНЕВА АРХІТЕКТУРА ІОТ-МЕРЕЖІ ТА ОЦІНКА НАДІЙНОСТІ

2.1 Багаторівнева архітектура IoT-мережі

Класичні IoT-архітектури зазвичай поділяються на трирівневу модель (Perception-Network-Application) та п’ятирівневу модель (Perception-Transport-Processing-Application-Business). Трирівнева архітектура є найпростішою та включає рівень сприйняття (пристрої та сенсори), мережевий рівень (передача даних) і рівень застосування (аналіз та використання даних) [23-31]. Вона є основою багатьох IoT-рішень, проте має обмеження щодо масштабованості та безпеки. П’ятирівнева архітектура розширює цей підхід, додаючи рівні транспортування (передача міжмережевих даних) та обробки (хмарні чи периферійні обчислення), що забезпечує кращу гнучкість та можливості інтеграції.

Окрім класичних моделей, у літературі запропоновано численні архітектурні рішення, багато з яких розробляються під егідою консорціумів і форумів, таких як IoT World Forum (IoTWF), де провідні компанії активно беруть участь у формуванні майбутнього IoT-інфраструктур. Інші підходи з’являються в результаті роботи органів стандартизації, таких як ETSI та ITU, які визначають ключові технічні аспекти забезпечення сумісності та надійності IoT-систем.

У межах цього дослідження розгляд архітектури не обмежуватиметься лише однією архітектурною моделлю, а натомість реалізуємо переваги різних підходів відповідно до їхньої значущості для оцінювання надійності IoT-систем. Такий підхід дозволяє інтегрувати найкращі практики з різних архітектур, забезпечуючи баланс між продуктивністю, безпекою та відмовостійкістю в умовах реального використання.

Запропонована архітектура складається з п’яти взаємопов’язаних рівнів, кожен з яких виконує унікальні функції (рис. 2.1):

1. Рівень сприйняття (Perception Layer) – це основа IoT-системи, що включає сенсори, виконавчі механізми та інші пристрої (так звані "речі" або Things). Окремо ці пристрої не можуть виконувати складні завдання, тому їх об’єднують у сенсорні

мережі (SNs). Використання бездротових сенсорних мереж (WSN) забезпечує зручність розгортання, економію енергії та широкий спектр застосувань.

2. Рівень мережевого доступу (Access Network Layer) – відіграє ключову роль у забезпеченні зв’язку між пристроями рівня сприйняття та центральними вузлами обробки даних. Цей рівень об’єднує сенсорні мережі у більші системи та забезпечує їхній вихід в Інтернет. У межах цього рівня використовуються різні протоколи зв’язку, такі як Wi-Fi, LoRaWAN, Zigbee, Bluetooth, 4G/5G та інші. Основна задача рівня – забезпечити ефективний обмін даними між пристроями у межах локальних чи регіональних мереж, а також гарантувати стабільний зв’язок із віддаленими обчислювальними ресурсами.

3. Рівень ядра мережі (Core Network Layer) – відповідає за передачу даних на глобальному рівні. Його основне завдання полягає у створенні ефективної інфраструктури для транспортування інформації від сенсорних вузлів та локальних мереж до потужних обчислювальних ресурсів, таких як хмарні платформи, дата-центри та сервери, що обробляють великі обсяги даних у реальному часі. Це рівень, який пов'язує локальні сегменти IoT-системи з більш широкими цифровими екосистемами, забезпечуючи масштабованість, безпеку та оптимізацію пропускної здатності. Окрім звичайної передачі даних, рівень ядра мережі також виконує роль інтелектуального маршрутизатора, що оптимізує потоки інформації залежно від їхньої пріоритетності. Наприклад, критично важливі повідомлення від систем безпеки чи медичних пристроїв мають бути передані з мінімальною затримкою, тоді як менш термінові дані, такі як звіти про споживання енергії або погодні умови, можуть оброблятися з використанням механізмів буферизації та пакетної передачі. Це дозволяє значно підвищити ефективність використання ресурсів і мінімізувати затримки у функціонуванні IoT-додатків.

4. Рівень проміжного програмного забезпечення (Middleware Layer) – служить для управління різними типами пристроїв та даних.Однією з головних проблем у сучасних IoT-екосистемах є велика різноманітність пристроїв, стандартів і протоколів зв’язку. Кожен виробник може використовувати власні технологічні рішення, що ускладнює інтеграцію IoT-систем у єдину мережу.

Middleware слугує своєрідним «перекладачем» між різними пристроями та платформами, дозволяючи їм працювати разом незалежно від технічних відмінностей. На цьому рівні реалізуються такі ключові функції, як агрегація даних, обробка потокової інформації, управління доступом до пристроїв, забезпечення безпеки та оптимізація використання ресурсів. Рівень проміжного програмного забезпечення дозволяє здійснювати попередню фільтрацію та обробку даних ще до їхньої передачі у хмарні або локальні сервери, що значно зменшує навантаження на мережу і покращує продуктивність системи. Наприклад, якщо сенсори реєструють зміну температури, яка не виходить за встановлені межі, middleware може відфільтрувати ці дані, щоб не перевантажувати канал зв'язку непотрібною інформацією. Водночас, якщо виявлено критичні зміни параметрів, повідомлення може бути передано негайно з найвищим пріоритетом. Іншим важливим аспектом роботи проміжного програмного забезпечення є управління безпекою. Враховуючи величезну кількість IoT-пристроїв, що підключаються до глобальної мережі, питання кібербезпеки стають особливо актуальними. Middleware-рішення можуть реалізовувати механізми автентифікації та авторизації пристроїв, шифрування переданих даних, виявлення аномальної поведінки в мережі та автоматичне блокування підозрілих з'єднань. Це особливо важливо для промислових IoT-систем, де кіберзагрози можуть призводити до значних економічних втрат або навіть фізичної небезпеки.

Окрім того, рівень проміжного програмного забезпечення відіграє важливу роль у створенні механізмів самовідновлення та автоматичного управління конфігурацією IoT-системи. Якщо якийсь вузол мережі виходить з ладу або виникає збій у зв'язку, рівень проміжного програмного забезпечення може переналаштувати маршрути передачі даних або активувати резервні канали. Це дозволяє підвищити загальну надійність IoT-інфраструктури та зменшити ризики відмов. Ще одним важливим напрямом розвитку middleware-рішень є підтримка моделей обчислень на основі туману (fog computing) та периферійних обчислень (edge computing). Традиційно IoT-системи значною мірою покладалися на хмарні обчислення, але передача великих обсягів даних до віддалених серверів може

спричиняти затримки та підвищувати навантаження на мережу. Використання edge та fog computing дозволяє виконувати обробку даних безпосередньо на пристроях або локальних вузлах мережі, що прискорює реакцію системи та зменшує залежність від централізованих серверів.

5. Рівень застосунків (Application Layer) – є верхнім рівнем IoT-архітектури, на якому реалізуються сервіси та інтерфейси для кінцевих користувачів. Саме тут відбувається створення програмних рішень, які використовують можливості IoT для автоматизації процесів, моніторингу та керування. До основних сфер застосування IoT-рішень належать розумні будинки, інтелектуальні транспортні системи, промислова автоматизація, екологічний моніторинг, охорона здоров'я, агропромисловий сектор та багато інших галузей. Гнучкість цього рівня дозволяє адаптувати IoT-системи до різних потреб, забезпечуючи зручність у використанні та ефективність у виконанні завдань.

Такий підхід до архітектури дозволяє не лише ефективно інтегрувати IoT-пристрої, а й підвищити надійність системи загалом.

Варто відзначити, що у даній кваліфікаційній роботі задача оцінки надійності буде обмежена першими чотирма рівнями, оскільки ключові фактори надійності зосереджені на рівнях мережі, обробки та зберігання даних. Саме ці рівні визначають безперервність роботи системи, тоді як прикладний рівень здебільшого впливає на користувацький досвід і має можливість адаптації без критичних збоїв. Тобто якщо інші рівні працюють стабільно, то програми можуть перезапускатися чи адаптуватися без втрати функціональності всієї системи.

Крім того, у різних IoT-системах прикладний рівень може бути реалізований по-різному (веб-інтерфейси, мобільні додатки, API тощо), що ускладнює уніфіковану оцінку надійності. Тому з цих причин було зосереджено увагу на аналізі надійності нижчих рівнів, які забезпечують стабільність функціонування IoT-інфраструктури.

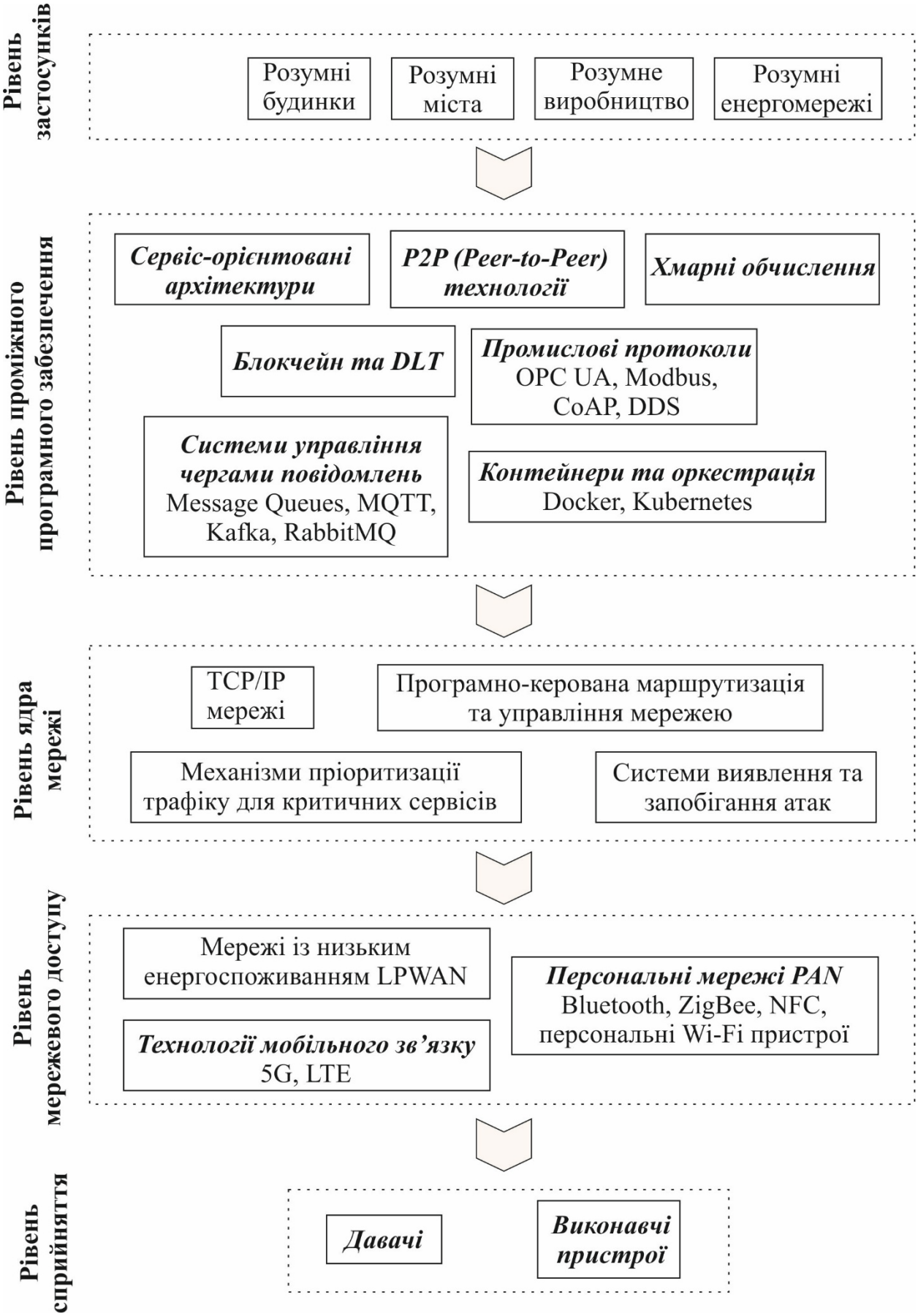


Рисунок 2.1 – Пропонована багаторівнева архітектура системи Інтернету речей

2.2 Метод блок-схем надійності

Метод блок-схем надійності (Reliability Block Diagram, RBD) – це один із найпоширеніших методів аналізу надійності систем. Він дозволяє графічно представити систему у вигляді взаємопов’язаних блоків, де кожен блок відповідає окремому компоненту або підсистемі. Метод RBD використовується для розрахунку ймовірності безвідмовної роботи системи на основі надійності її окремих складових [26-28].

Метод базується на тому, що будь-яку технічну систему можна представити у вигляді схеми з’єднаних елементів. Залежно від їхнього взаємозв’язку, система може мати послідовну, паралельну або комбіновану структуру. Основна ідея полягає в тому, що надійність усієї системи залежить від надійності кожного окремого блоку і того, як ці блоки взаємодіють між собою.

Метод блок-схем надійності дозволяє оцінити функціональність системи на основі ймовірності її працездатності. У разі виходу з ладу окремих елементів метод дає змогу визначити, чи зможе система продовжувати виконувати свої функції.

Можна виділити наступні перевари використання методу блок-схем надійності:

– гнучкість – метод дозволяє моделювати будь-які конфігурації системи, включаючи складні багаторівневі структури.

– візуалізація – графічне представлення дає змогу інженерам і аналітикам краще розуміти структуру та слабкі місця системи.

– можливість використання в автоматизованих розрахунках – сучасні програми, такі як MATLAB, ReliaSoft BlockSim або IBM SPSS, дозволяють автоматично будувати RBD і виконувати розрахунки надійності.

– легкість інтеграції з іншими методами – RBD можна поєднувати з методами Марковських ланцюгів, дерев відмов (fault-tolerance analyze) та статистичним моделюванням.

Розглянемо процес визначення надійності системи відповідно до методу блок-схем надійності.

Нехай задано систему C, що складається із n компонентів позначених як i, де $i \in \{1,2,3,..,n\}$. Тоді змінна стану для компоненту i можна записати у наступному вигляді:

$$Y_i(t) = \begin{cases} 1, \text{якщо компонент } i \text{ у справному стані в момент часу } t \\ 0, \text{якщо компонент } i \text{ відмовив в момент часу } t \end{cases} \quad (2.1)$$

де $Y_i(t)$ – випадкова змінна, що асоційована із компонентом i.

Тоді вектор стану $Y(t)$ у момент часу t складається із n оновлень змінної стану:

$$Y(t) = \langle Y_1(t), Y_2(t), \dots, Y_n(t) \rangle \quad (2.2)$$

Схожим чином, стан всіє системи може бути поданий через бінарну функцію μ, яку називають структурною функцією:

$$\mu(Y(t)) = \mu(Y_1(t), Y_2(t), \dots, Y_n(t)) \quad (2.3)$$

де

$$\mu(Y(t)) = \begin{cases} 1, \text{якщо компонент } i \text{ у справному стані в момент часу } t \\ 0, \text{якщо компонент } i \text{ відмовив в момент часу } t \end{cases} \quad (2.4)$$

Можна відзначити наступні корисні ймовірності, які інтерпретуються відповідно як надійність компонента i та надійність системи в заданий момент часу t:

$$P(Y_i(t) = 1) = p_i(t), i = \overline{1,n} \quad (2.5)$$

$$P(\mu(Y(t)) = 1) = p_C(t) \quad (2.6)$$

З метою спрощення аналізу, припустимо, що відмови розглядаються як незалежні події. Отже, змінні стану в момент часу t $Y_i(t)$, є стохастично незалежними.

Також введемо ще одне припущення, яке полягає у тому, що компонент i вважається неремонтованим. Неремонтовані компоненти це компоненти, для яких проводиться заміна одразу після першої відмови. Таким чином у даному дослідженні розглядаються лише перші виникнення відмови. У такому контексті функції надійності та виживання є однаковими та мають наступні форми:

$$p_i(t) = R_i(t), \qquad i = \overline{1,n} \tag{2.7}$$

Тоді для всієї системи C можна визначити:

$$p_C(t) = R_C(t) \tag{2.8}$$

З точки зору схем з'єднання у методі блок-схем надійності виділяють три типи з'єднань: послідовне, паралельне та змішане.

Послідовне з'єднання – це такий тип структури, де всі компоненти підключені один за одним, і робота всієї системи залежить від роботи кожного з них. Якщо хоча б один компонент виходить з ладу, вся система перестає працювати. Такий тип з'єднання часто зустрічається в простих електричних колах або в системах, де всі елементи виконують критично важливі функції. Його основний недолік – низька надійність, оскільки вихід з ладу навіть одного елемента веде до повної відмови.

Паралельне з'єднання дозволяє підключати компоненти так, що система продовжує працювати, навіть якщо один або кілька з них виходять з ладу. Надійність такого з'єднання значно вища, оскільки є резервні шляхи для роботи системи. Паралельне з'єднання часто використовується в критичних системах, де потрібна безперервна робота, наприклад у серверних кластерах або резервних джерелах живлення.

Змішане з’єднання поєднує в собі елементи як послідовного, так і паралельного підключення. Воно забезпечує баланс між надійністю та ефективністю, дозволяючи певним частинам системи мати резервні компоненти, а іншим працювати в строго визначеній послідовності. Такі структури часто використовуються в складних інженерних системах, де важливо зберігати надійність, але при цьому уникати зайвих витрат на повне резервування.

Розглянемо детальніше методику визначення функції надійності для кожного виду з’єднань.

Послідовне з’єднання визначається структурою, яка подана на рис. 2.2.

Рисунок 2.2 – Послідовне з’єднання компонентів

Відповідна структурна функція, що описує послідовне з’єднання компонентів можна записати як:

$$\mu\big(Y(t)\big) = \prod_{i=1}^{n} Y_i(t) \tag{2.9}$$

де i компонент модельованої функції, $Y(t)$ – вектор стану.

Тоді через наступний вираз можна описати функцію надійності:

$$R_C(t)^{\text{пос}} = E\left(\mu\big(Y(t)\big)\right) = E\left(\prod_{i=1}^{n} Y_i(t)\right) = \prod_{i=1}^{n} E\big(Y_i(t)\big) = \prod_{i=1}^{n} R_i(t) \tag{2.10}$$

Паралельна структура організовує компоненти таким чином, що загальний збій системи відбувається лише тоді, коли виходять з ладу всі компоненти. Така структура представлена на рис. 2.3.

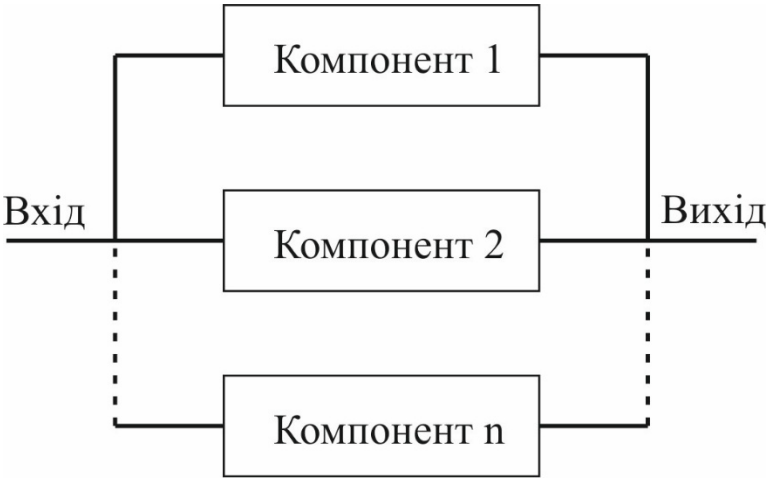


Рисунок 2.3 – Паралельне з’єднання компонентів

Структурна функція паралельного з’єднання компонентів буде визначатись відповідно до наступного виразу:

$$\mu\big(Y(t)\big) = 1 - \prod_{i=1}^{n}(1 - Y_i(t)) \tag{2.11}$$

Тоді функція надійності для функції надійності паралельного з’єднання визначатиметься як:

$$\begin{aligned} R_C(t)^{\text{пар}} &= E\left(\mu\big(Y(t)\big)\right) = E\left(1 - \prod_{i=1}^{n}(1 - Y_i(t))\right) \\ &= 1 - \prod_{i=1}^{n} E((1 - Y_i(t))) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) \end{aligned} \tag{2.12}$$

Структура системи k-з-n означає, що вона працює тоді і тільки тоді, коли принаймні k з n компонентів, що її утворюють, працюють. На рис. 2.2 наведено таку структуру.

Відповідна структурна функція системи k-з-n може бути записана як:

$$\mu\big(Y(t)\big) = \begin{cases} 1, \text{якщо } \sum_{i=1}^{n} Y_i(t) \geq k \\ 0, \text{якщо } \sum_{i=1}^{n} Y_i(t) < k \end{cases}, \tag{2.13}$$

де i компонент системи, $Y(t)$ – вектор станів системи.

Тоді функція надійності для даного з'єднання компонентів можна подати через наступний вираз:

$$R_C(t)^{k-з-n} = \sum_{y=k}^{n} \binom{n}{k} R(t)^y \times (1 - R(t))^{n-y} \tag{2.14}$$

Дана формула буде справедлива, при умові, що надійність всіх компонентів є однаковою. З'єднання k-з-n компонентів представлено на рис. 2.4.

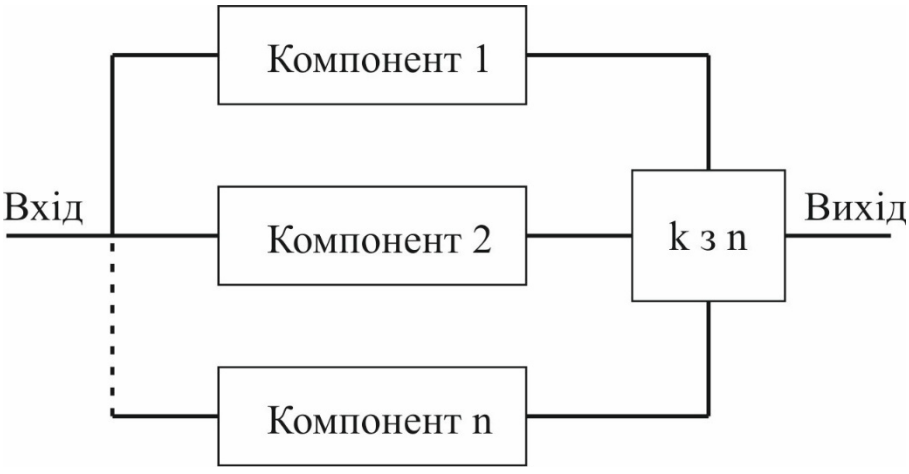


Рисунок 2.4 – З'єднання k-з-n компонентів

Метод блок-схем надійності був обраний для системи оцінювання надійності багаторівневої архітектури IoT-мереж через його здатність наочно і ефективно моделювати структуру системи, оцінюючи її загальну працездатність на основі взаємозв'язку компонентів. У складних IoT-мережах, що містять численні пристрої, датчики, шлюзи та сервери, важливо не лише визначити ймовірність відмови окремих елементів, а й оцінити, як ці відмови впливають на функціональність всієї системи.

Завдяки методу блок-схем надійності можна враховувати різні топології мереж Інтернету речей, включаючи послідовні, паралельні та змішані конфігурації підключення пристроїв. Це особливо корисно при оцінюванні критично важливих IoT-систем, де певні компоненти можуть мати резервні копії або дублюючі механізми. Використання цього методу дозволяє ідентифікувати "вузькі місця" системи, визначити слабкі ланки та розробити стратегії підвищення її надійності, наприклад, через впровадження резервування або зміну архітектури.

Крім того, метод блок-схем може досить легко інтегрується з іншими методами аналізу, такими як дерева відмов або марковські моделі, що дозволяє отримати ще точнішу оцінку надійності IoT-мереж. У поєднанні з програмними інструментами цей підхід дає змогу ефективно проводити моделювання та прогнозування роботи системи при різних сценаріях експлуатації.

Отже, вибір методу блок-схем надійності для оцінювання мереж IoT зумовлений його наочністю, гнучкістю та здатністю точно оцінювати надійність розподілених систем, що є критично важливим для забезпечення безперервної роботи IoT-інфраструктури.

2.3 Оцінка впливу параметрів IoT-мережі на її надійність

Оцінка впливу параметрів IoT-мережі на її надійність є важливим аспектом при проектуванні та експлуатації таких систем. IoT-мережі, або інтернет речей, складаються з великої кількості пристроїв, які взаємодіють між собою через мережу, збирають дані та передають їх для подальшої обробки. Надійність таких

мереж визначається їх здатністю стабільно виконувати свої функції навіть у разі виникнення збоїв або несприятливих умов.

Одним із ключових параметрів є топологія мережі або з'єднання елементів. Наприклад, у зірковій топології вихід з ладу центрального вузла призводить до відмови всієї мережі, що можна формалізувати як ймовірність відмови системи:

$$R_{star} = R_{hub} \prod_{i=1}^{n} R_i \tag{2.15}$$

де R_{hub} – надійність центрального вузла, а R_i – надійність окремих пристроїв. У випадку mesh-топології мережа може зберігати працездатність навіть при виході з ладу кількох вузлів, що підвищує її надійність.

Протоколи зв'язку також впливають на надійність IoT-мережі. Для LPWAN-технологій, таких як LoRa або NB-IoT, характерна висока дальність передачі даних, але низька пропускна здатність. Це створює ризики втрати даних у випадку перевантаження каналу. Надійність зв'язку можна оцінити через коефіцієнт помилок у передачі (BER):

$$R_{link} = e^{-\lambda T} \tag{2.16}$$

де λ – середня інтенсивність помилок, а T – час передачі пакета.

Ще одним важливим фактором є енергоспоживання вузлів, оскільки багато пристроїв працюють від батарей. Надійність вузла залежить від ємності батареї C, споживаної потужності P та середнього часу передачі даних T, що можна описати рівнянням:

$$L_{battery} = \frac{C}{P \cdot T} \tag{2.17}$$

де $L_{battery}$ – час автономної роботи.

Менший рівень споживання енергії дозволяє продовжити термін служби вузлів і підвищити загальну надійність мережі.

У даній роботі оцінювання надійності системи буде виконуватися на основі з’єднання елементів IoT-мережі. Саме спосіб з’єднання визначає, наскільки система здатна зберігати працездатність за різних умов експлуатації. Вибір цього підходу обґрунтований тим, що в багаторівневих архітектурах IoT-мереж ключову роль у загальній надійності відіграють особливості взаємодії між окремими вузлами. Кожен елемент мережі має певну ймовірність відмови, а спосіб їхнього з'єднання визначає, як ці відмови поширюються по системі та впливають на загальну працездатність.

Аналізуючи надійність через з’єднання елементів, можна визначити, які структурні особливості IoT-мережі є критичними для її стабільності. Наприклад, у централізованих топологіях вихід з ладу центрального вузла може спричинити зупинку всієї системи, тоді як у децентралізованих архітектурах відмова окремого елемента не впливає на функціональність інших компонентів. Вибір методів з’єднання визначає рівень відмовостійкості та можливість відновлення після збоїв. Оцінка таких структурних параметрів дозволяє передбачити, як система буде поводитися в реальних умовах експлуатації та наскільки вона здатна працювати у довготривалій перспективі без значних перебоїв.

Методологія оцінки, яка пропонується у даній роботі, передбачає побудову математичної моделі, що описує ймовірність безвідмовної роботи мережі залежно від параметрів її з’єднань. Використовуючи ймовірнісні підходи, можна визначити функцію надійності системи, що дозволяє аналізувати її поведінку у часі. Це дає можливість побудувати криву надійності, яка показує зміну ймовірності працездатності мережі на різних часових інтервалах. Точки на цій кривій вказуватимуть на моменти, коли надійність суттєво змінюється, наприклад, при накопиченні відмов або при перевищенні порогового значення збоїв у ключових елементах.

На основі отриманих даних можна визначити періоди надійності всієї системи, тобто часові проміжки, протягом яких IoT-мережа залишається працездатною із заданою ймовірністю. Це дозволяє прогнозувати необхідність обслуговування, оптимізувати роботу системи та розробляти механізми підвищення її стійкості. Виявлення критичних точок на кривій надійності також дає змогу встановити моменти, коли потрібно вживати заходів для забезпечення безперервної роботи IoT-мережі, наприклад, шляхом дублювання вузлів або змін у топології з'єднань.

Таким чином, оцінка надійності IoT-мережі через її з’єднання дозволяє отримати комплексну картину впливу архітектурних рішень на загальну працездатність системи. Це дає можливість як теоретично прогнозувати рівень надійності, так і практично застосовувати результати для оптимізації розгортання IoT-інфраструктури та її подальшої експлуатації.

2.4 Висновки

Класичні IoT-архітектури, такі як трирівнева (Perception-Network-Application) та п’ятирівнева (Perception-Transport-Processing-Application-Business), забезпечують базову структуру для побудови IoT-систем. Трирівнева модель є простою та зрозумілою, але має обмеження щодо масштабованості та безпеки. П’ятирівнева модель, розширюючи цей підхід, додає рівні транспортування та обробки, що робить її більш гнучкою та придатною для складних IoT-рішень. Однак для оцінки надійності таких систем необхідно враховувати не лише структуру архітектури, а й взаємодію між її компонентами.

Запропонована п’ятирівнева архітектура, яка включає рівні сприйняття, мережевого доступу, ядра мережі, проміжного програмного забезпечення та застосунків, дозволяє ефективно інтегрувати різні IoT-пристрої та технології. Кожен рівень виконує унікальні функції, що забезпечує модульність та гнучкість системи. Наприклад, рівень сприйняття відповідає за збір даних, рівень мережевого доступу забезпечує зв’язок між пристроями, а рівень проміжного програмного

забезпечення абстрагує складність інфраструктури, що дозволяє легко інтегрувати різні технології.

Використання методу діаграм надійності для оцінки надійності такої архітектури є ефективним підходом. RBD дозволяє моделювати взаємозв'язки між компонентами кожного рівня, визначати критичні точки та оцінювати вплив відмов окремих елементів на загальну працездатність системи. Наприклад, на рівні сприйняття відмова одного сенсора може призвести до втрати даних, але завдяки RBD можна визначити, чи це вплине на всю систему чи лише на локальну ділянку. Аналогічно, на рівні ядра мережі RBD дозволяє оцінити, як відмова одного маршрутизатора чи каналу зв'язку вплине на передачу даних між вузлами.

Таким чином, запропонована архітектура разом із методом RBD забезпечує комплексний підхід до оцінки надійності IoT-мереж. Це дозволяє не лише виявляти слабкі місця в системі, а й розробляти стратегії їхнього усунення, що є критично важливим для забезпечення стабільної роботи IoT-систем у реальних умовах. Використання RBD дозволяє враховувати як локальні, так і глобальні аспекти надійності, що робить цей метод незамінним інструментом для аналізу та оптимізації IoT-архітектур.

3 МОДЕЛІ ПРЕДСТАВЛЕННЯ ФУНКЦІЙ НАДІЙНОСТІ РІВНІВ ДЛЯ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ ІОТ МЕРЕЖІ

3.1 Загальний підхід до представлення функцій надійності рівнів для багаторівневої архітектури IoT мережі

Оцінка надійності багаторівневої IoT-архітектури є критично важливим завданням для забезпечення безперебійної роботи систем, що включають велику кількість гетерогенних пристроїв, комунікаційних каналів та обчислювальних платформ. У нашому підході кожен рівень архітектури представлений як окрема підсистема, що моделюється за допомогою методів аналізу надійності, зокрема за допомогою методу діаграм надійності (Reliability Block Diagram, RBD).

Методологія представлення функцій надійності передбачає розгляд кожного рівня з позиції його ролі в загальній системі, оцінку потенційних точок відмови та розробку відповідних структурних моделей для визначення параметрів надійності. RBD-моделі дозволяють описати зв’язки між елементами на кожному рівні, визначити конфігурацію резервування та оцінити вплив відмов окремих компонентів на загальну працездатність IoT-мережі.

Розглянута у попередньому розділі п’ятирівнева архітектура дозволяє сформувати детальну та комплексну модель надійності, у якій кожен рівень має власну функцію надійності. Ця функція визначається особливостями внутрішньої структури рівня, а також способом взаємодії його компонентів як між собою, так і з іншими рівнями системи. Аналіз надійності проводиться не лише на рівні окремих пристроїв та підсистем, а й на рівні всієї екосистеми IoT-мережі загалом. Такий підхід дозволяє враховувати вплив можливих відмов окремих елементів на функціонування всієї системи, що дає змогу розробляти стратегії підвищення її стійкості та ефективності.

Застосування методу діаграм надійності на кожному рівні допомагає оцінити критичні вузли системи, оптимізувати розподіл ресурсів і покращити загальну відмовостійкість інфраструктури Інтернету речей. Надалі кожен рівень

буде розглянутий детальніше із відповідною схемою представлення функції надійності.

3.2 Модель рівня сприйняття

Рівень сприйняття (Perception Layer) складається з речей (things), які взаємодіють для виконання визначеної місії. До його складу можуть входити апаратні компоненти, операційні системи, комунікаційні модулі, а також модулі живлення.

Згідно з теорією систем, кожна підсистема є самостійною системою, яка, своєю чергою, може містити інші підсистеми. Наприклад, апаратна підсистема складається з центрального процесора, пам’яті та модулів введення-виведення (I/O). Важливу роль також відіграє модуль комунікації, який забезпечує передачу даних між вузлами всієї системи Інтернету речей, дозволяючи речам взаємодіяти як усередині рівня сприйняття, так і з вищими рівнями у багаторівневій архітектурі.

Цей процес може повторюватися, доки не буде досягнутий рівень абстракції, достатній для ефективного вирішення проблеми. Обраний рівень деталізації залежить від контексту та складності проблеми. Загалом, сутність рівня сприйняття можна змоделювати, як показано на рис. 3.1.

У випадках, коли внутрішня структура елементів рівня сприйняття не є предметом дослідження, цей рівень можна розглядати як атомарну систему. Якщо одна з його складових виходить з ладу, це може спричинити відмову всього рівня. Наприклад, несправність апаратного шару може призвести до повного збою системи. В інших сценаріях причинами відмови можуть бути різке зниження рівня живлення, переповнення пам’яті або несприятливі умови навколишнього середовища. Подібний ефект спостерігається у випадку несправності програмних компонентів.

Дана кваліфікаційна робота зосереджене на аналізі відмов на високому рівні архітектури, що дозволяє створити діаграму надійності, яку представлено на рис. 3.1.

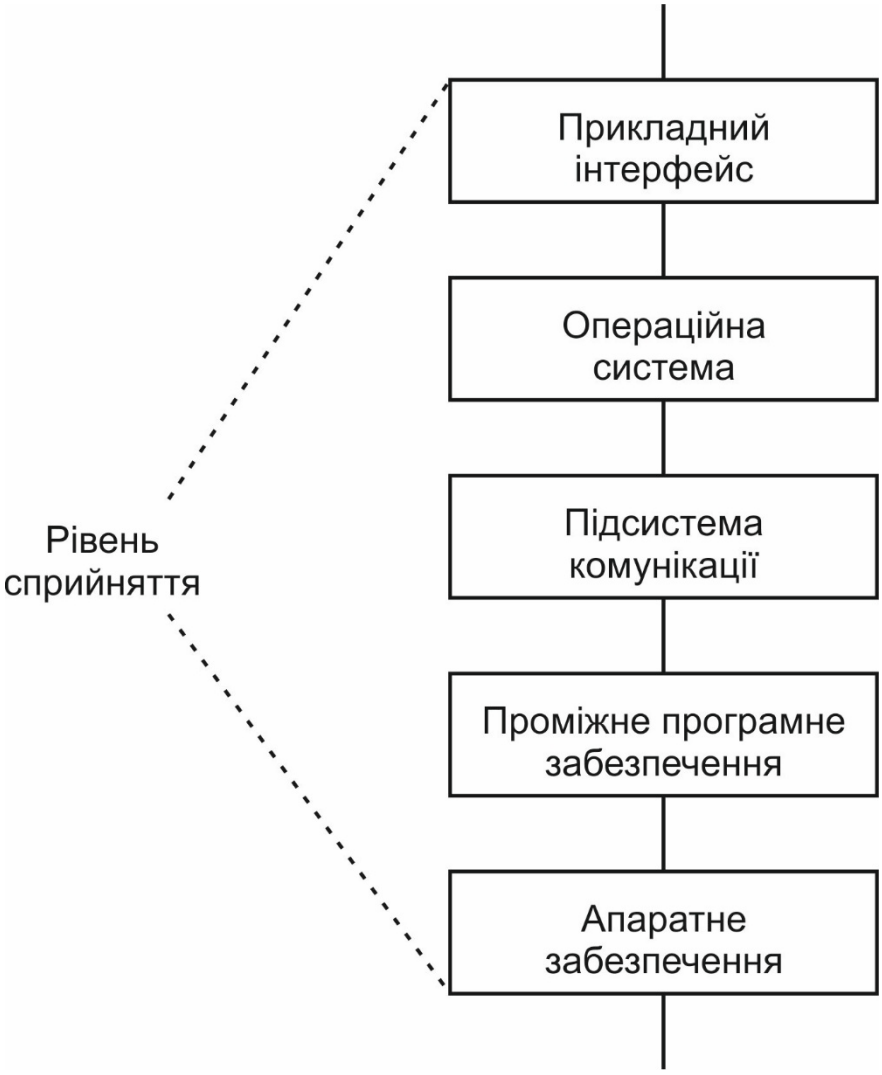


Рисунок 3.1 – Модель RBD сутності рівня сприйняття

Згідно з запропонованою діаграмою надійності на рис. 3.1, сутність рівня сприйняття (СРС) еквівалентна п’ятьом підсистемам, які з'єднані в послідовній схемі. Це означає, що в пропонованій моделі вихід з ладу хоча б однієї з підсистем призведе до відмови всієї СРС.

Виходячи з цього припущення, у даній роботі не будуть враховуватись конкретні причини відмов. Натомість пропонується моделювати їх за допомогою

випадкової змінної $y_j(t)$, яка позначає стан підсистеми j. Тоді функціональна структура, пов'язана з СРС , $\mu_{\text{CPC}}(y(t))$ може бути записана у вигляді:

$$\mu_{\text{CPC}}(y(t)) = \prod_{j=1}^{k} y_j(t), \tag{3.1}$$

де k – кількість підсистем у сутності рівня сприйняття (СРС), а $y_j(t)$ – випадкові величини, що описують стан підсистем апаратного забезпечення (Hardware), проміжного програмного забезпечення (Middleware), операційної системи (OS), модуля взаємодії (Communication) та прикладного рівня (Application) відповідно. Функція надійності, пов'язана з сутністю рівня сприйняття (СРС), визначається наступним чином:

$$R_{\text{CPC}}(t) = \prod_{j=1}^{k} R_j(t), \tag{3.2}$$

де $R_j(t)$, $j = \overline{1,5}$ є відповідно функціями надійності, пов'язаними із апаратним забезпеченням (Hardware), проміжним програмним забезпеченням (Middleware), операційною системою (OS), модулем комунікації (Communication) та підсистемами застосунків (Application).

Функція $R_j(t)$, відображає ймовірність безвідмовної роботи підсистеми j протягом часу t. Оскільки надійність підсистеми може залежати від різних випадкових факторів, її можна моделювати за допомогою випадкової змінної $y_j(t)$, яка описує її стан у певний момент часу.

Математичне сподівання $y_j(t)$, яке позначене як $E[y_j(t)]$, дає середнє значення стану підсистеми за всіма можливими реалізаціями випадкового процесу. Це дозволяє оцінити середню надійність підсистеми на основі її поведінки в часі. Таким чином, функція надійності $R_j(t)$ може бути визначена як:

$$R_j(t) = E[y_j(t)], \quad (3.3)$$

де $E[y_j(t)]$ обчислюється інтегруванням функції щільності ймовірності відповідної випадкової змінної:

Крім того, якщо доступні статистичні дані або характеристики інтенсивності відмов, $R_j(t)$ можна визначити аналітично, використовуючи параметри експоненційного або більш складного розподілу надійності для конкретного типу підсистеми.

3.3 Модель рівня сенсорних мереж/рівня доступу

Цей рівень забезпечує можливість для сутностей рівня сприйняття (СРС) об'єднуватися у кластери та встановлювати зв’язки між собою на невеликих відстанях. Це здійснюється відповідно до топологій, які підтримують базові мережеві технології, такі як Bluetooth, Zigbee, Z-Wave, Wi-Fi або LoRa. Завдяки цьому забезпечується ефективний обмін інформацією між пристроями, що входять до складу IoT-системи, а також можливість їхньої колективної роботи над спільними завданнями.

Проте у більшості сценаріїв використання виключно короткодіапазонних технологій зв’язку є недостатнім. Основна причина цього полягає у технічних обмеженнях самих пристроїв рівня сприйняття. Багато з них мають малий об’єм пам’яті, обмежену обчислювальну потужність та незначний рівень енергоспоживання. Через це вони не можуть самостійно виконувати повноцінну обробку зібраних даних або забезпечувати їхню довготривалу передачу без підтримки інших рівнів IoT-архітектури.

З огляду на ці фактори, сутності рівня сприйняття змушені виходити за межі локальних сенсорних мереж і передавати дані на вищі рівні. Це дозволяє розширити можливості їхньої взаємодії та забезпечити якісне виконання основних функціональних завдань, таких як аналіз інформації, її обробка та подальше

збереження у централізованих системах, зокрема у хмарних сервісах або на віддалених серверах.

На цьому рівні поєднуються дві основні групи технологій:

1. Технології, що відповідають за створення короткодіапазонної сенсорної мережі, яка об’єднує розумні об’єкти.

2. Технології, що не є специфічними для сенсорних мереж, але забезпечують передачу даних між розумними об'єктами та іншими типами даних.

Розглянемо спочатку клас сенсорних мереж. Припустимо, що кожна підсистема рівня сприйняття СРС_j є атомарною системою, тобто складається з єдиного компонента. Для обміну даними між собою об’єкти СРС_j повинні встановлювати зв’язки в межах певної області. Кількість таких зв’язків залежить від контексту, базових технологій і прийнятої топології мережі. У нашому випадку виконаємо припущення, що компонент системи, позначений як МД_j (мережевого доступу), представляє всі можливі зв’язки, які може використовувати певна сутність. Підсистема МД_j може бути детально проаналізована, наприклад, шляхом обчислення її структурної функції відповідно до заданих параметрів сценарію (наприклад, стратегій маршрутизації).

Крім того, відмова окремого СРС_j, як правило, не призводить до відмови всієї мережі. Для того щоб мережа вийшла з ладу, має бути досягнуто певний поріг кількості відмов. Тому із цією метою пропонується наступна діаграма надійності, що відповідає цим класам сенсорних мереж.

На рис. 3.2 представлено структурну модель класів сенсорних мереж, де підсистема сенсорної мережі СМ вважається несправною лише в тому випадку, якщо вийшли з ладу *k+1* пар підсистем ($\text{СРС}_j, \text{МД}_j$). Кожна пара ($\text{СРС}_j, \text{МД}_j$) утворює послідовну підсистему. Для спрощення припустимо:

$$\begin{cases} R_{\text{СРС}_j}(t) = R_{\text{СРС}}(t) \\ R_{\text{МД}_j}(t) = R_{\text{МД}}(t) \end{cases} \tag{3.4}$$

Тоді відповідну функцію надійності такої системи можна подати як:

$$R_{\text{СМ}}(t) = \sum_{x=k}^{m} \binom{m}{x} R(t)^x \times (1 - R(t))^{m-x} \quad (3.5)$$

де

$$R(t) = R_{\text{СРС}}(t) \times R_{\text{МД}}(t) \quad (3.6)$$

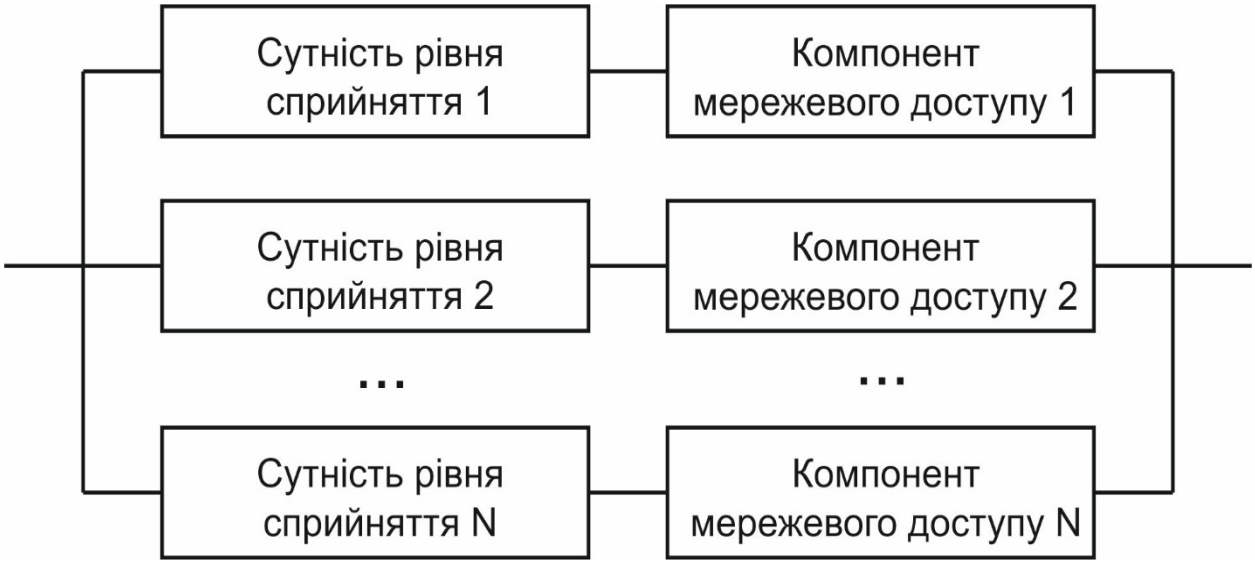


Рисунок 3.2 – Модель RBD (діаграма надійності) сутностей рівня сенсорних мереж

Друга частина цього рівня включає мережеві технології, які використовуються для доступу до локальних вузлів обробки даних або для виходу в Інтернет. Їх детальний аналіз виходить за рамки цієї роботи з двох причин. По-перше, контекст даного дослідження не передбачає такого рівня деталізації. По-друге, вже існують дослідження, присвячені оцінці надійності таких мережевих технологій. У нашому випадку загального високорівневого представлення про ці системи достатньо для побудови відповідних моделей надійності.

На цьому рівні можна спостерігати, що мережева технологія МТ_j може використовуватися окремо для передачі даних у вузли обробки або разом з іншою

$МТ_i$ (причому i ≠ j). Таким чином, процес передачі даних може здійснюватися через шлюзи, розташовані на межах вузла $МТ_j$. У контексті діаграми надійності (RBD) взаємодії в межах рівня доступу можуть бути представлені двома основними компонентами:

1. Компонент $МТ_j$ – позначає мережеву технологію *j*, де *j* – це індекс, що відповідає певній технології доступу.

2. Компонент шлюзу (Gateway) – може розглядатися як окремий фізичний пристрій або як підсистема, що потребує визначення структури та функцій, якщо складається з декількох шлюзів. У цьому дослідженні програмні компоненти, що вбудовані у шлюзи, не враховуються.

Модель на рис. 3.3 ілюструє механізми відмов, які можуть виникнути на рівні доступу. Високорівнева модель передбачає, що підсистема, яка складається з *n* мережевих технологій $МТ_j$ працює в паралельній конфігурації, а шлюзові компоненти підключені послідовно. Таким чином це означає, що вся система перестає функціонувати у двох випадках:

1. Якщо всі впроваджені мережеві технології $МТ_j$ виходять з ладу.

2. Якщо виходить з ладу хоча б один із компонентів шлюзу.

Формули для функціональної структури, пов'язаної із МД можна представити наступним чином:

$$\mu_{МД}(Y_{МД}(t)) = Y_{Шлюзу}(t) \times (1 - \prod_{j=1}^{k}(1 - Y_{МТ_j}(t))) \times Y_{Шлюзу}(t) \qquad (3.7)$$

де $\mu_{МД}$ – функціональна структура для мережі доступу (МД);

$Y_{МД}(t)$ – вектор стану мереж доступу;

$Y_{Шлюзу}(t)$ – вектор стану підсистеми шлюзів;

$Y_{МТ_j}(t)$ – множина застосованих мережевих технологій $МТ_j$.

Функція надійності, пов’язана з сутністю рівня мережевого доступу (МД), визначається наступним чином:

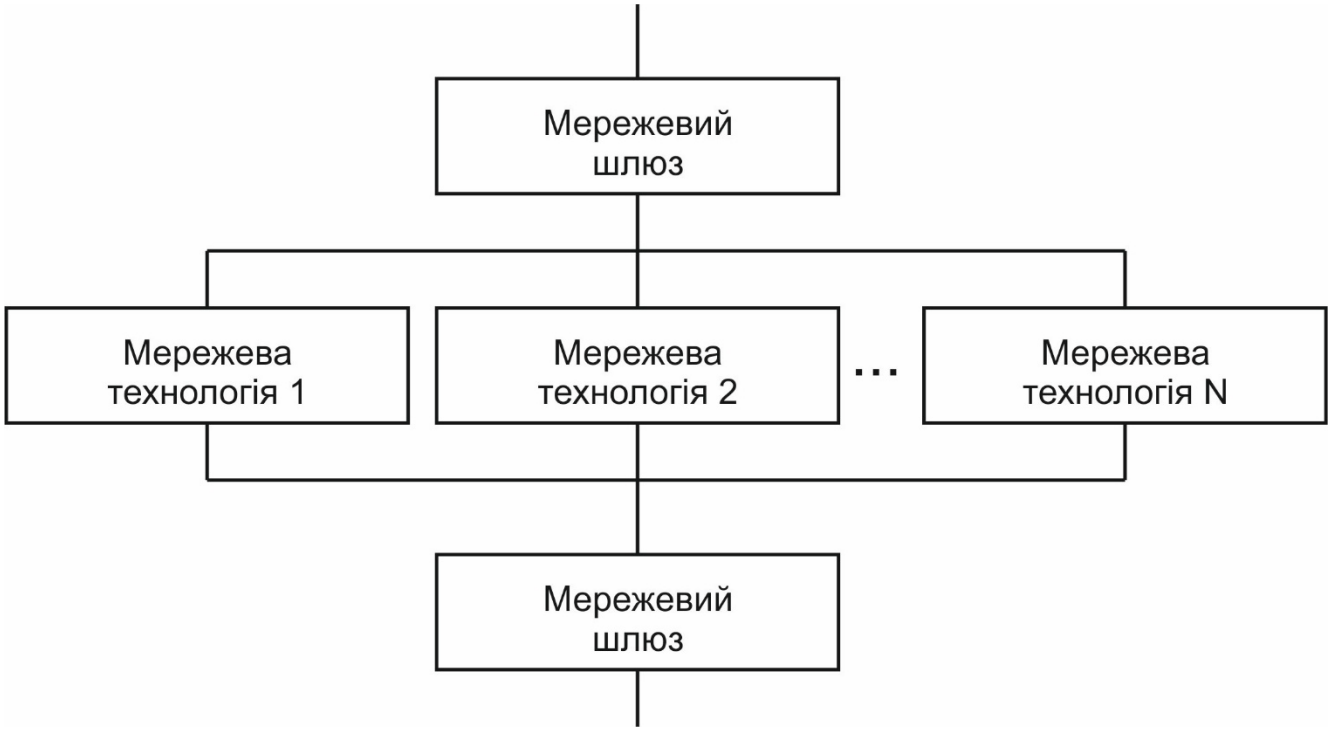


Рисунок 3.3 – Модель RBD мережі доступу

$$R_{\text{МД}}(t) = R_{\text{Шлюзу}}(t) \times (1 - \prod_{j=1}^{k}(1 - R_{\text{МТ}_j}(t))) \times Y_{\text{Шлюзу}}(t) \quad (3.8)$$

де $R_{\text{МД}}(t)$ – функція надійності для системи мережевого доступу;

$R_{\text{МТ}_j}(t)$– функція надійності застосованої мережевої технології МТ_j.

$R_{\text{Шлюзу}}(t)$ – функція надійності підсистеми шлюзу.

Якщо виразити:

$$R_{\text{МТ}}(t) = (1 - \prod_{j=1}^{k}(1 - R_{\text{МТ}_j}(t))) \quad (3.9)$$

Тоді функцію надійності, пов’язану із сутністю рівня мережевого доступу (МД) можна подати:

$$R_{\text{МД}}(t) = R_{\text{Шлюзу}}(t) \times R_{\text{МТ}}(t) \times Y_{\text{Шлюзу}}(t) \quad (3.10)$$

де $R_{\text{МТ}}(t)$ – це функція надійності реалізованої підсистеми мережевої технології в змодельованій мережі доступу.

3.4 Модель рівня ядра мережі

Маршрутизація та ідентифікація розумних об'єктів у мережі є основними завданнями рівня ядра мережі. На цьому рівні дані можуть досягати одного й того самого пункту призначення різними шляхами. Вибір найкращого маршруту ґрунтується на розподілених алгоритмах, що виконуються на розосереджених вузлах, а саме маршрутизаторах. Парадигми, такі як стан з'єднання (link state) або вектор відстані (vector-distance), є основою для роботи маршрутних алгоритмів та створення таблиць маршрутизації.

Крім того, цей рівень також відповідає за маршрутизацію в сенсорних мережах. Вузли піддаються апаратним і програмним збоями, а канали зв’язку можуть виходити з ладу через перешкоди, шум або несприятливі умови навколишнього середовища. Зокрема, велика мережа маршрутизаторів, як-от Інтернет, може бути розділена на кілька автономних систем (АС), кожна з яких контролюється певною організацією та використовує внутрішній шлюзовий протокол (ВШП). Дві або більше автономних систем можуть бути з'єднані між собою за допомогою зовнішнього шлюзового протоколу (ЗШП).

Кожна автономна система (АС) складається із зон (O_i), які можуть забезпечувати кілька маршрутів до одного й того самого вузла призначення. Ці маршрути є комбінацією вузлів та каналів зв’язку, організованих у послідовну структуру. Таким чином, використання діаграм надійності (RBD) для моделювання

маршрутів є ключовим підходом, що дозволяє побудувати загальну модель системи, дотримуючись принципу "знизу-вгору".

Усе це призводить до моделі, представленої на рис. 3.4. Можливий шлях між вихідним вузлом (ВВ) і вузлом призначення (ВП) моделюється як система, що складається з компонентів у послідовній конфігурації. Цими компонентами є вузли маршрутизації ($ВМ_j$) та канали зв'язку маршрутизації ($КЗМ_j$). Альтернативні маршрути між тими самими вихідним та кінцевим вузлом представлені за допомогою паралельної структури. Маршрути можуть бути згруповані в зони (O_i), які також слідують тій самій логіці, що й на рівні маршрутів. Для вищого рівня абстракції маршрути можна розглядати як компоненти, що формують систему зони. Ще один рівень абстракції можна досягти, якщо розглядати автономні системи (АС) як окремі компоненти, а всю міжмережеву систему як єдине ціле. Подамо рівняння надійності лише для першого випадку, на основі якого можна вивести рівняння для інших рівнів абстракції.

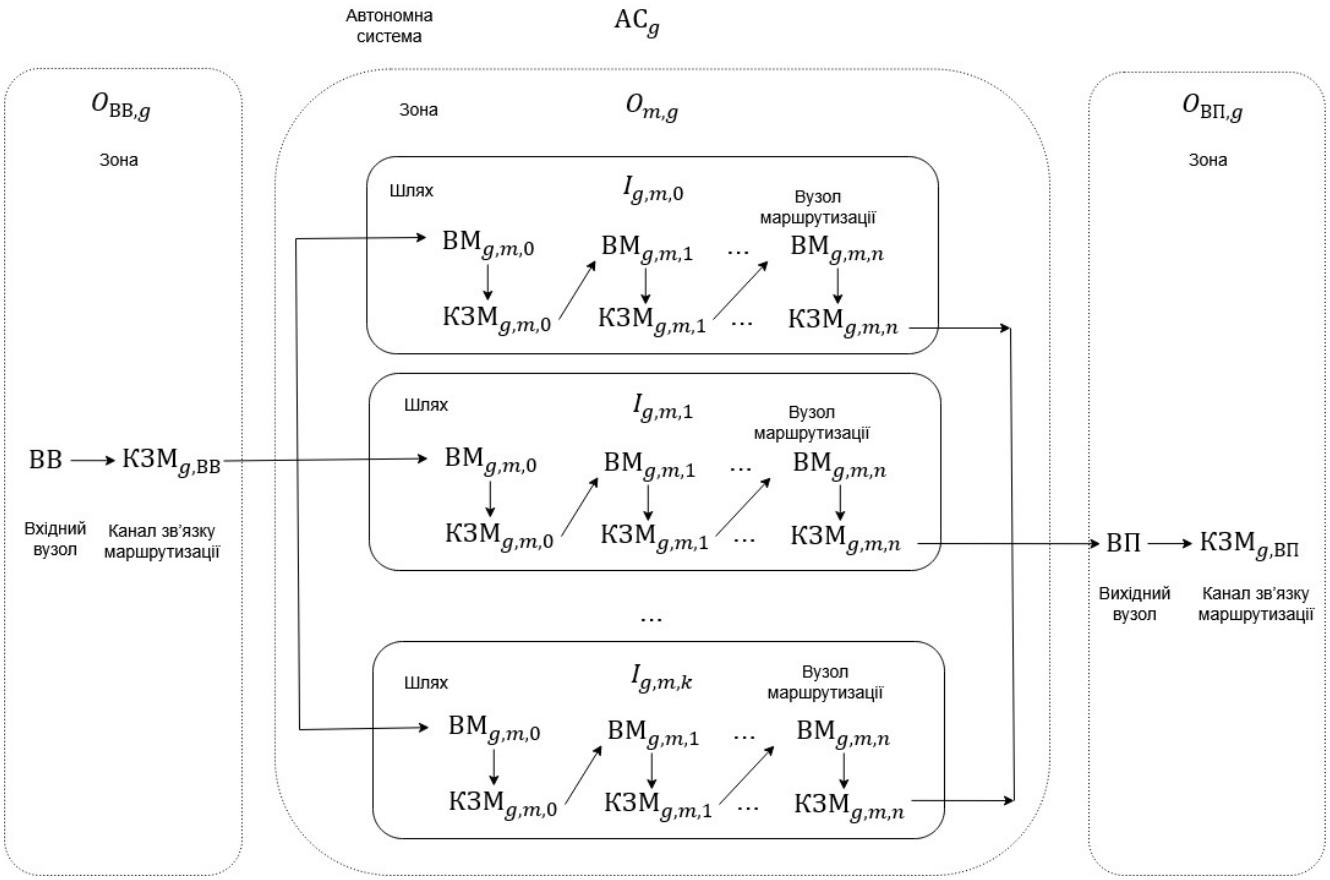


Рисунок 3.4 - RBD модель рівня ядра мережі

Представимо функціональну структуру шляху I_j наступним чином:

$$\mu I_{g,m,i}\left(Y_{I_{l,m,i}}(t)\right) = \prod_{j=1}^{n}\prod_{l=1}^{n-1} X_{\text{ВМ}_{g,m,i,j}}(t) \times X_{\text{КЗМ}_{g,m,i,l}}(t) \qquad (3.11)$$

де $\mu I_{g,m,i}$ – функціональна структура шляху i для зони m, що належить $AC\ g$;

$Y_{I_{g,m,i}}(t)$ – вектор стану шляху i у зоні m, яка належить $AC\ g$;

$X_{\text{ВМ}_{g,m,i,j}}(t)$ – вектор стану вузла маршрутизації j шляху i у зоні m, яка належить $AC\ g$;

$X_{\text{КЗМ}_{g,m,i,l}}(t)$ – вектор стану каналу зв'язку маршрутизації l шляху i у зоні m, яка належить $AC\ g$.

Функція надійності, пов'язана з сутністю рівня мережевого доступу (МД), визначається наступним чином:

Тоді функцію надійності шляху i у зоні m, яка належить $AC\ g$ подамо наступним чином:

$$RI_{g,m,i}(t) = \prod_{j=1}^{n}\prod_{l=1}^{n-1} R_{\text{ВМ}_{g,m,i,j}}(t) \times R_{\text{КЗМ}_{g,m,i,l}}(t) \qquad (3.12)$$

$RI_{g,m,i}(t)$ – функція надійності шляху i в зоні m, яка належить $AS\ g$;

$R_{\text{ВМ}_{g,m,i,j}}(t)$ – функція надійності вузла маршрутизації j шляху i у зоні m, яка належить $AC\ g$;

$R_{\text{КЗМ}_{g,m,i,l}}(t)$ – функція надійності каналу зв'язку маршрутизації l шляху i в зоні m, яка належить $AC\ g$.

Для непересічних шляхів у мережі можна записати рівняння відносно $O_{m,g}$:

$$R_{O_{m,g}}(t) = (1 - \prod_{i=1}^{n}(1 - RI_{g,m,i}(t))) \quad (3.13)$$

де $R_{O_{m,g}}(t)$ – функція надійності для зони *m,* що належить до *AC g.*

Тоді загальну модель рівня ядра мережі можна записати у наступному вигляді:

$$R_{\mathrm{AC}_g}(t) = R_{\mathrm{ВВ},g}(t) \times R_{\mathrm{КЗМ}_{\mathrm{ВВ},g}}(t) \times R_{O_{m,g}}(t) \times R_{\mathrm{КЗМ}_{\mathrm{ВП},g}}(t) \times R_{\mathrm{ВП},g}(t) \quad (3.14)$$

де $R_{\mathrm{ВВ},g}(t)$ – функція надійності вихідного вузла, що належить до *AC g*;

$R_{\mathrm{КЗМ}_{\mathrm{ВВ},g}}(t)$ – функція надійності прямого з'єднання до вихідного вузла, що належить до *AC g*;

$R_{\mathrm{КЗМ}_{\mathrm{ВП},g}}(t)$– функція надійності прямого з'єднання до вузла призначення, що належить до *AC g*;

$R_{\mathrm{ВП},g}(t)$ – функція надійності вузла призначення, що належить до *AC g*;

3.5 Модель рівня проміжного програмного забезпечення

Цей шар забезпечує взаємодію різних розумних об'єктів, виготовлених різними виробниками, що використовують різні формати даних та обмінюються інформацією за допомогою несумісних протоколів, так, ніби вони є однаковими сутностями. Цю здатність називають забезпеченням інтероперабельності розумних об'єктів.

Ще однією ключовою функцією цього шару є надання наступному шару, а саме прикладному, абстракції щодо гетерогенності нижчих рівнів. Завдяки цьому розробники IoT-застосунків можуть зосередитися більше на бізнес-логіці, а не на управлінні відмінностями між технологіями. Варто зазначити, що у даній роботі розглядаються лише ті технології проміжного програмного забезпечення, які належать до розподілених систем. Тому використання хмарних обчислень для

розміщення цього програмного забезпечення та керування значними обсягами створюваних даних є бажаним.

Таким чином, пропонована діаграма надійності для шару проміжного програмного забезпечення виглядає так, як показано на рис. 3.5.

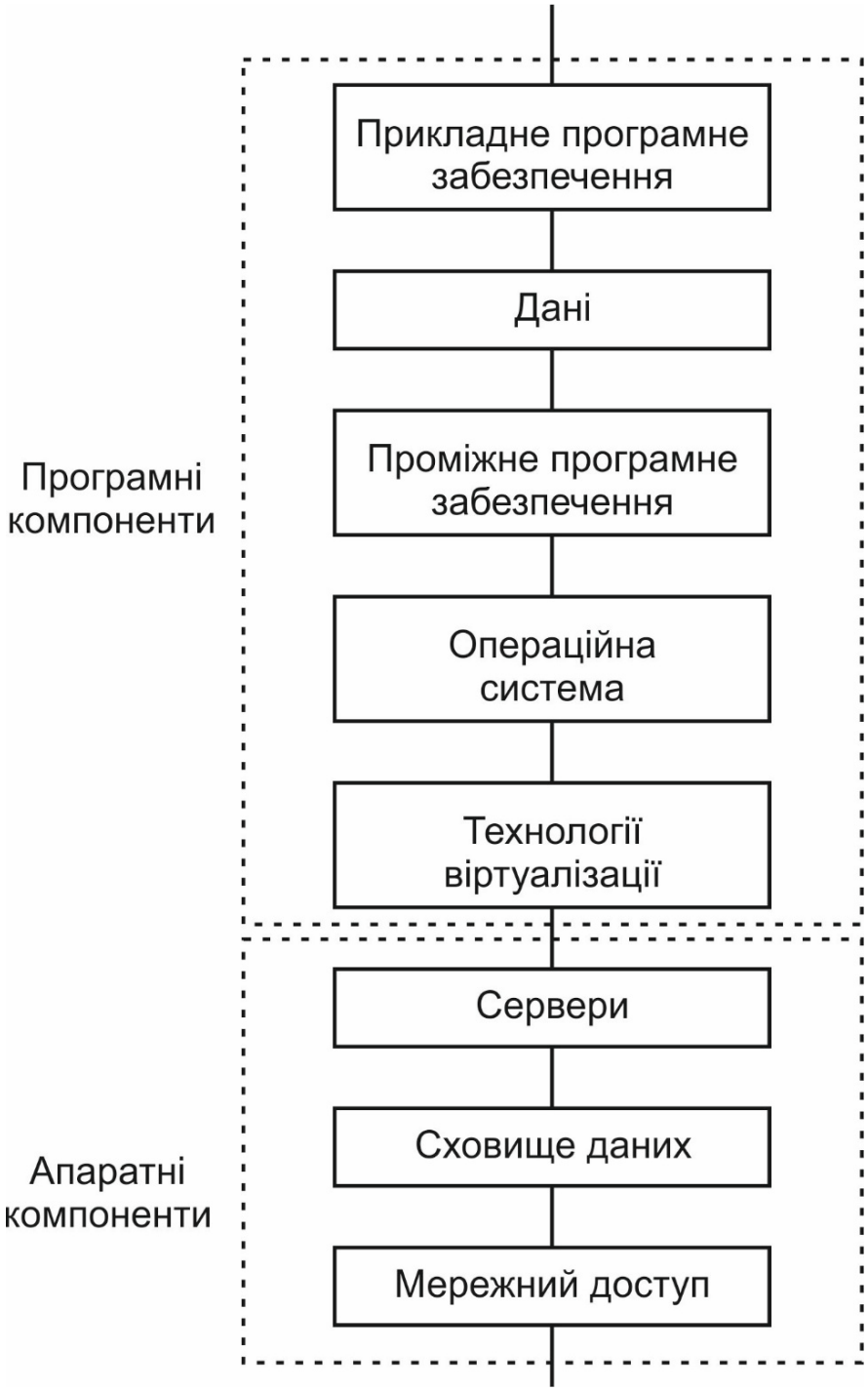


Рисунок 3.5 – RBD модель рівня проміжного програмного забезпечення

Для спрощення процесу опису моделі знехтуємо зайвими деталями, що розрізняють моделі сервісів між собою, і візьмемо до уваги спільні характеристики усіх моделей. Виходячи з цього припущення, виконаємо об'єднаємо всі вищезазначені моделі в єдину систему, яка складається з дев'яти рівнів, спільних для кожної із них. Це більш ніж достатньо з точки зору нашого системного підходу.

Апаратна частина прийнятої моделі може бути представлена у вигляді графа, у якому вузли є або Обчислювальними Вузлами ОВ, вузлами зберігання даних ВЗД, вузлами маршрутизації ВМ, комутаційними вузлами КВ або вузлами забезпечення безпеки ВЗБ. Ребра цього графа – це з'єднання між вузлами, які можуть бути різного типу, наприклад, оптоволоконні або мідні кабелі тощо.

Ці характеристики повертають нас до ситуації, подібної до моделі ядра мережі, що розглядалась раніше. Єдина відмінність – це типи вузлів. Таким чином, для моделювання цієї частини системи можна припустити модель на основі шляхів, у якій усі критично важливі вузли розташовані послідовно.

Альтернативні шляхи можуть бути організовані у паралельну схему на першому етапі наближення. Хоча апаратна частина відіграє ключову роль у забезпеченні надійних сервісів, програмна частина має не менше значення, а в деяких випадках навіть більше.

Крім того, певні властивості програмного забезпечення роблять його унікальним. Зокрема, більшість, якщо не всі, програмні компоненти, що використовуються у шарі Middleware, побудовані на основі архітектур Big Data через великий обсяг, різноманітність та швидкість генерованих IoT-пристроями даних. Водночас ці архітектурні стилі постійно змінюються, щоб максимально відповідати вимогам до якості. Це робить архітектурні рішення програмного забезпечення динамічними та еволюційними.

Найпоширенішою архітектурою у хмарних IoT-платформах є так звана Lambda-архітектура, що реалізує стиль взаємодії публікація/підписка (publish/subscribe).

Програмний шар, зображений на рис. 3.5, складається з рівнів віртуалізації, операційної системи (OS), проміжного програмного забезпечення (Middleware),

даних (Data) та прикладного рівня (Application). Вихід з ладу будь-якого з цих рівнів призводить до відмови всього програмного підсистеми.

Подальший аналіз цих підсистем можна здійснити, враховуючи архітектурні стилі, на яких вони побудовані. У цьому контексті доцільно розглянути підхід, що використовує діаграми надійності (RBD) для оцінки впливу архітектурного рівня програмного забезпечення на загальну надійність системи.

У даній роботі використаємо найбільш широко використовувану архітектуру, як зазначено вище, яка базується на Lambda-стилі. Топологічний вигляд Lambda-архітектури представлений на рис. 3.6.

З точки зору оцінки надійності, Lambda-архітектура має наступні особливості:

− відмовостійкість через дублювання обчислень. Дані одночасно обробляються у двох потоках (пакетному та потоковому рівнях), що дозволяє компенсувати можливі збої у швидкому рівні за рахунок історичних даних у пакетному рівні;

− резервування даних. Підсистема пакетної обробки зазвичай використовує надійні розподілені файлові системи (наприклад, HDFS), що дозволяє зменшити ризики втрати даних.

− точність проти доступності. Підсистема потокової обробки жертвує точністю заради мінімізації затримок, але у разі відмови він може отримувати коригування з підсистеми пакетної обробки, що підвищує загальну стійкість системи;

− залежність від базової інфраструктури. Надійність архітектури напряму залежить від таких факторів, як відмовостійкість розподілених обчислювальних платформ (Spark, Kafka, Flink), методів балансування навантаження та механізмів автоматичного масштабування.

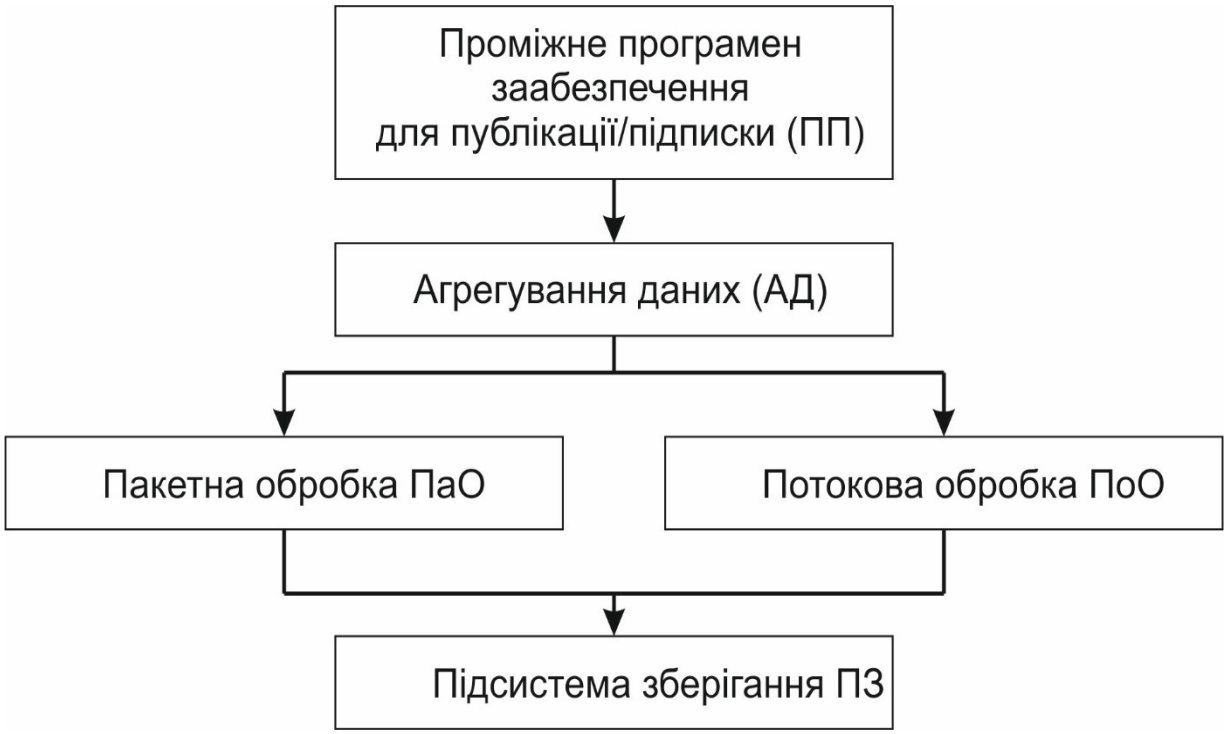


Рисунок 3.6 – Структура Lambda-архітектури

Компоненти першої підсистеми, що відповідає першому шляху, включають публікацію/підписку ПП, агрегування даних АД, пакетну обробку ПаО і підсистему зберігання ПЗ, які організовані в послідовну схему.

Друга підсистема аналогічна першій, за винятком того, що підсистема пакетної обробки ПаО (ВР) замінена підсистемою потокової обробки ПоО.

Слід зазначити, що всі блоки можуть бути репліковані для досягнення масштабованості, що призводить до створення паралельних підсистем (дочірніх), аналогічних тій, яку потрібно масштабувати (батьківській).

З метою спрощення запропонованої моделі, сформуємо припущення, з якого слідує, що всі підсистеми є достатньо потужними для обробки великих обсягів потоків даних в мережі Інтернету речей без додавання будь-яких паралельних компонентів.

$$R_{\text{ППЗ}}(t) = R_{\text{ПП}}(t) \times R_{\text{АД}}(t) \times (1 - (1 - R_{\text{ПаО}})) \times (1 - R_{\text{ПоО}}(t)) \times R_{\text{ПЗ}}(t) \quad (3.15)$$

де $R_{\text{ППЗ}}(t)$ – модель шару проміжного програмного забезпечення, що заснована на лямбда архітектурі; $R_{\text{ПП}}$ – функція надійності підсистеми публікації/підписки; $R_{\text{АД}}$ – функція надійності підсистеми агрегування даних; $R_{\text{ПоО}}$ – функція надійності підсистеми потокової обробки; $R_{\text{ПаО}}$ – функція надійності підсистеми пакетної обробки; $R_{\text{ПЗ}}$ – функція надійності підсистеми зберігання.

3.6 Висновки

Запропонована модель представлення функцій надійності рівнів для багаторівневої архітектури IoT-мережі базується на детальному аналізі кожного рівня системи як окремої підсистеми, що підлягає дослідженню за допомогою методів оцінки надійності. Зокрема, використання методу діаграм надійності дозволяє більш точно моделювати структурні особливості кожного рівня та враховувати всі можливі сценарії відмов. Основна ідея такого підходу полягає у визначенні внутрішньої структури кожного рівня, виявленні його ключових компонентів та дослідженні їхньої взаємодії як між собою, так і з іншими рівнями багаторівневої IoT-архітектури.

Кожен рівень має свою власну функцію надійності, яка визначає ймовірність його безвідмовної роботи протягом заданого часу. Враховуючи, що IoT-системи є складними розподіленими мережами, надійність кожного рівня відіграє критично важливу роль у забезпеченні загальної працездатності. Саме тому у запропонованій методології основна увага приділяється оцінці потенційних точок відмов, моделюванню їхнього впливу на загальну систему та розробці механізмів підвищення стійкості архітектури. Застосування RBD-моделей у цьому контексті дозволяє створити формалізоване представлення зв’язків між елементами кожного рівня, визначити логічну конфігурацію резервування, а також оцінити можливі наслідки виходу з ладу окремих компонентів.

Оскільки IoT-мережі складаються з великої кількості різнорідних пристроїв, кожен з яких може мати власні технічні характеристики та рівень відмовостійкості, важливою частиною аналізу є визначення способів забезпечення стійкості системи

навіть у разі часткової втрати її елементів. Це передбачає розробку моделей, що враховують як апаратні, так і програмні рівні архітектури. Для апаратного рівня особливе значення має наявність резервування критично важливих компонентів, що дозволяє мінімізувати ризик втрати працездатності всієї мережі. З іншого боку, програмний рівень потребує механізмів відновлення після відмов, а також алгоритмів, які забезпечують безперервність обробки та передачі даних навіть у разі порушення роботи окремих підсистем.

Таким чином, методологія представлення функцій надійності багаторівневої IoT-архітектури дозволяє систематично підходити до оцінки ризиків, пов’язаних із відмовами на кожному рівні, а також визначати ефективні способи підвищення загальної стійкості мережі. Враховуючи стрімкий розвиток технологій та постійне ускладнення IoT-інфраструктур, такі підходи є необхідними для забезпечення стабільної роботи сучасних розподілених систем та їхньої адаптації до можливих несправностей.

4 СИСТЕМА ОЦІНЮВАННЯ НАДІЙНОСТІ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ ІОТ-МЕРЕЖ

4.1 Узагальнена структура системи оцінювання надійності багаторівневої архітектури IoT-мереж

З метою визначення поточного стану надійності системи Інтернету речей, періодів її стабільного функціонування, перехідних станів та критичних зон деградації запропоновано систему оцінювання надійності багаторівневої архітектури IoT-мереж.

Об’єктом аналізу пропонованої системи оцінювання надійності багаторівневої архітектури IoT-мереж є система Інтернету речей, яка розглядається через призму запропонованої багаторівневої архітектури, що запропонована у попередніх розділах. Такий підхід дозволяє комплексно оцінювати її надійність, враховуючи особливості взаємодії між різними рівнями мережі. Структура запропонованої системи оцінювання надійності багаторівневої архітектури IoT-мереж подано на рис. 4.1.

Запропонована система оцінювання надійності складається із двох підсистем. Першою підсистемою є підсистема визначення функції надійності для багаторівневої архітектури IoT-мереж. Дана підсистема відповідає за визначення функції надійності архітектури Інтернету речей, що передбачає системний аналіз усіх рівнів мережі та використання моделі діаграм надійності RBD. Це дозволяє не лише візуалізувати структуру системи, а й оцінити вплив окремих компонентів на загальну надійність.

Друга підсистема зосереджена на безпосередньому оцінюванні надійності, використовуючи прогнозно-аналітичний метод. Вона аналізує поточний стан мережі, дозволяючи передбачати можливі відмови чи зниження ефективності роботи. У результаті оцінювання визначаються три основні періоди:

– стабільного функціонування, коли система працює без критичних збоїв;

– перехідного стану, під час якого відбувається часткове погіршення показників і може знадобитися втручання;

– критичної зони деградації, де система перебуває на межі відмови або вже не виконує свої функції належним чином.

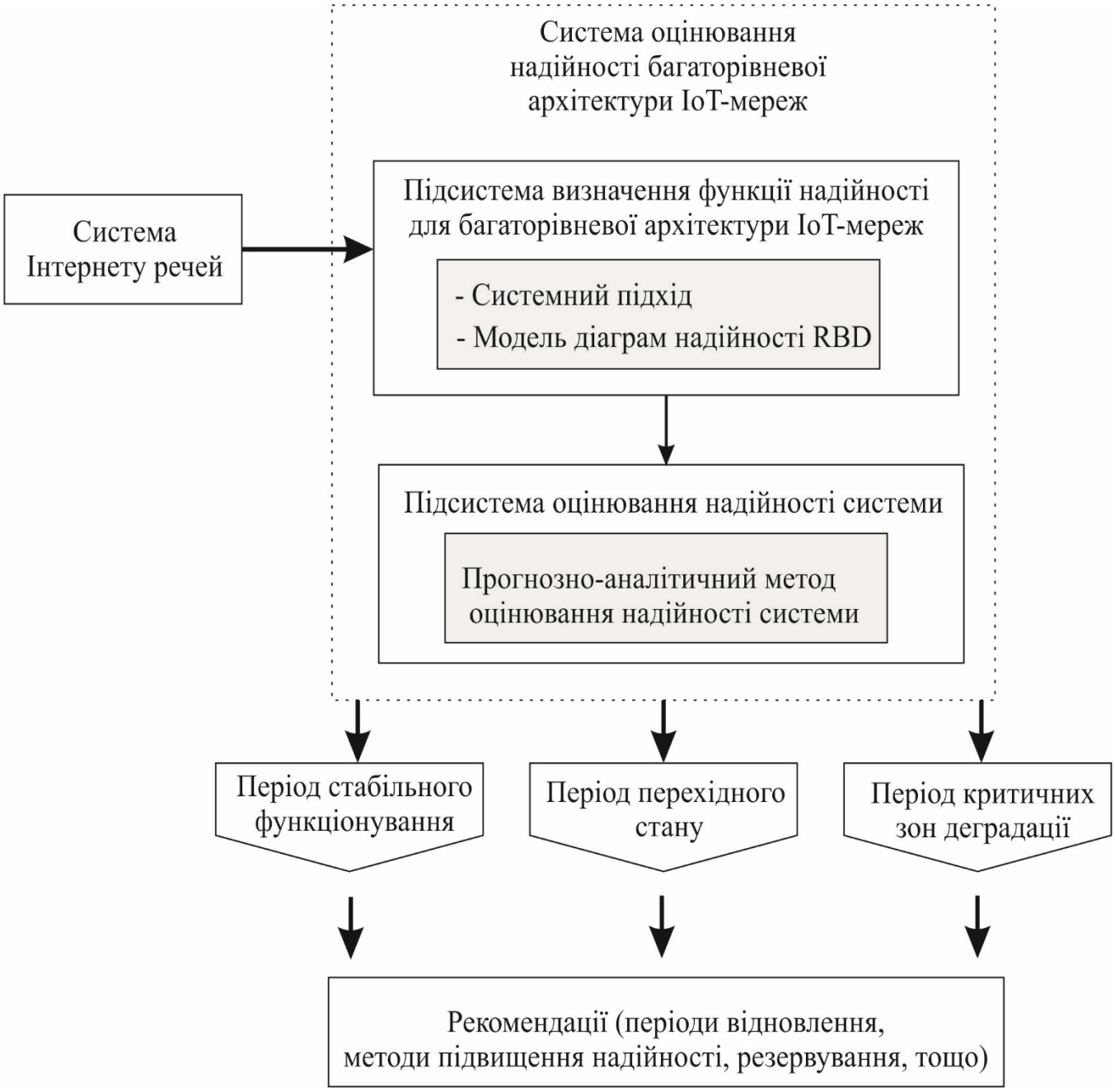


Рисунок 4.1 – Узагальнена структура системи оцінювання надійності багаторівневої архітектури IoT-мереж

На основі проведеного аналізу надійності багаторівневої архітектури IoT-мереж формується набір рекомендацій, які допомагають забезпечити стабільне

функціонування системи, запобігати відмовам та оперативно реагувати на можливі збої.

Одним із ключових підходів є визначення періодів відновлення, що передбачає планування часу, необхідного для ремонту або заміни несправних компонентів. Це може включати як короткострокові заходи (наприклад, перезапуск вузлів, виправлення програмних помилок), так і довгострокові стратегії модернізації обладнання.

Застосування методів підвищення надійності є ще одним важливим аспектом. Це може включати апаратне резервування (наприклад, дублювання критично важливих датчиків, вузлів обробки даних або комунікаційних каналів) та програмні механізми (алгоритми самовідновлення, адаптивне управління навантаженням, автоматичне переключення на альтернативні маршрути передачі даних).

Резервування критичних компонентів допомагає зменшити ризик повного виходу з ладу системи. Наприклад, використання дубльованих серверів у хмарній архітектурі або аварійного живлення для безперервної роботи пристроїв під час відключення електроенергії. У випадку сенсорних IoT-мереж резервування може передбачати встановлення додаткових датчиків у ключових точках для запобігання втраті даних.

Окрім резервування, важливим методом є розподіл навантаження між різними рівнями архітектури. Це дозволяє зменшити перевантаження окремих вузлів та запобігти їх виходу з ладу. Використання балансувальників навантаження, алгоритмів динамічного перерозподілу ресурсів та інтелектуальних механізмів управління трафіком дозволяє зберігати продуктивність системи навіть при зростанні кількості підключених пристроїв.

Також значну роль відіграють алгоритми самодіагностики та прогнозного технічного обслуговування. Використання машинного навчання та аналітики даних дозволяє виявляти приховані аномалії в роботі системи та передбачати потенційні відмови ще до їх виникнення. Це дає можливість проводити профілактичне обслуговування, зменшуючи час простою та витрати на аварійний ремонт.

Таким чином, результатом роботи пропонованої системи оцінювання надійності систем Інтернету речей є можливість прогнозування стану мережі та визначення критичних моментів її функціонування. На основі отриманих даних формується набір рекомендацій, які можуть включати встановлення періодів відновлення, застосування методів резервування критичних компонентів, оптимізацію розподілу навантаження, впровадження адаптивних механізмів управління трафіком, а також використання самовідновлюваних алгоритмів для мінімізації ризиків відмов.

Структурно підсистема визначення функції надійності для багаторівневої архітектури IoT-мереж складається із чотирьох підсистем (рис. 4.2).

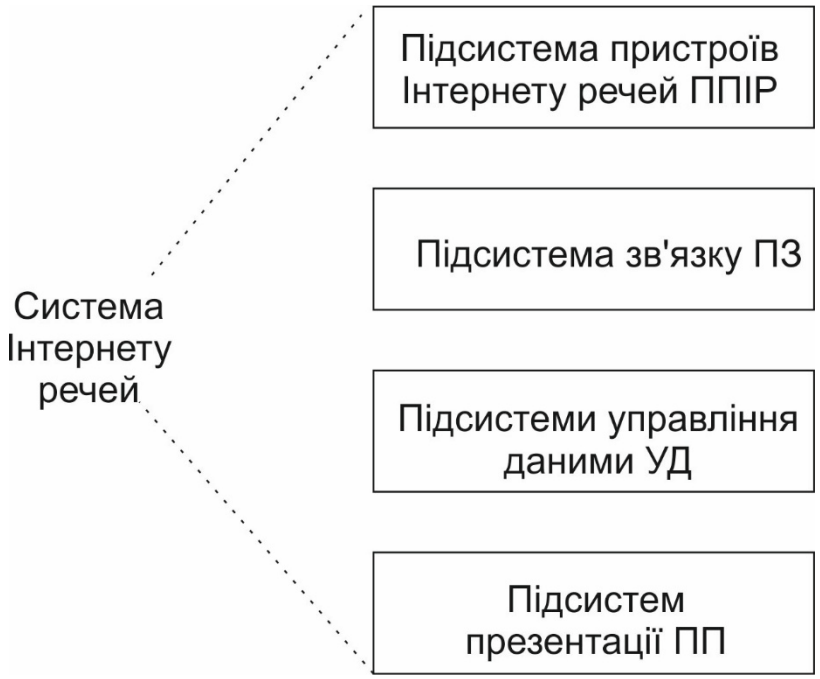


Рисунок 4.2 – Узагальнена структура схема підсистеми визначення функції надійності для багаторівневої архітектури IoT-мереж

Перша підсистема – підсистема пристроїв Інтернету речей ППІР, яка відповідає рівням сприйняття та мережевого доступу.

Інша підсистема – підсистема зв’язку ПЗ, що узагальнює послідовне з’єднання підсистем доступу до мережі і ядра мережі.

Підсистеми управління даними УД відповідає рівню проміжного програмного забезпечення, а підсистем презентації ПП відповідає рівню застосунків.

Відповідно до Рисунка 14, ці підсистеми утворюють послідовну структуру. Тоді загальне рівняння надійності може бути виражене як:

$$R_{\text{Системи}}(t) = R_{\text{ППІР}}(t) \times R_{\text{ПЗ}}(t) \times R_{\text{УД}}(t) \times R_{\text{ПЗ}}(t) \quad (4.1)$$

4.2 Процес функціонування підсистеми визначення функції надійності для багаторівневої архітектури IoT-мереж

На рис. 4.3 наведено схему процесу функціонування системи оцінювання надійності багаторівневої архітектури IoT-мереж. Дана схема представляє покроковий підхід до оцінки надійності IoT-системи, ґрунтуючись на ієрархічному розбитті архітектури на рівні та поступовому їхньому аналізі.

Весь процес розпочинається з введення системи Інтернету речей як об’єкта дослідження, після чого відбувається її розділення на окремі рівні. Кожен рівень позначається як l_i, де i – це порядковий номер рівня в архітектурі. До таких рівнів зазвичай відносяться рівень сприйняття, рівень мережевого доступу, ядро мережі, проміжний рівень програмного забезпечення та рівень застосунків.

На першому етапі аналізу система перевіряється на наявність цих рівнів. Якщо певний рівень входить до структури IoT-системи, він формується як окремий блок у схемі RBD (Reliability Block Diagram) – методі, який використовується для графічного представлення залежності між компонентами системи в контексті її надійності. Далі проводиться перевірка, чи є цей рівень останнім у системі. Якщо так, процес переходить до наступного етапу, який включає оцінку функції надійності для всієї системи. Якщо ж рівень не є останнім, алгоритм продовжує роботу, аналізуючи наступний рівень.

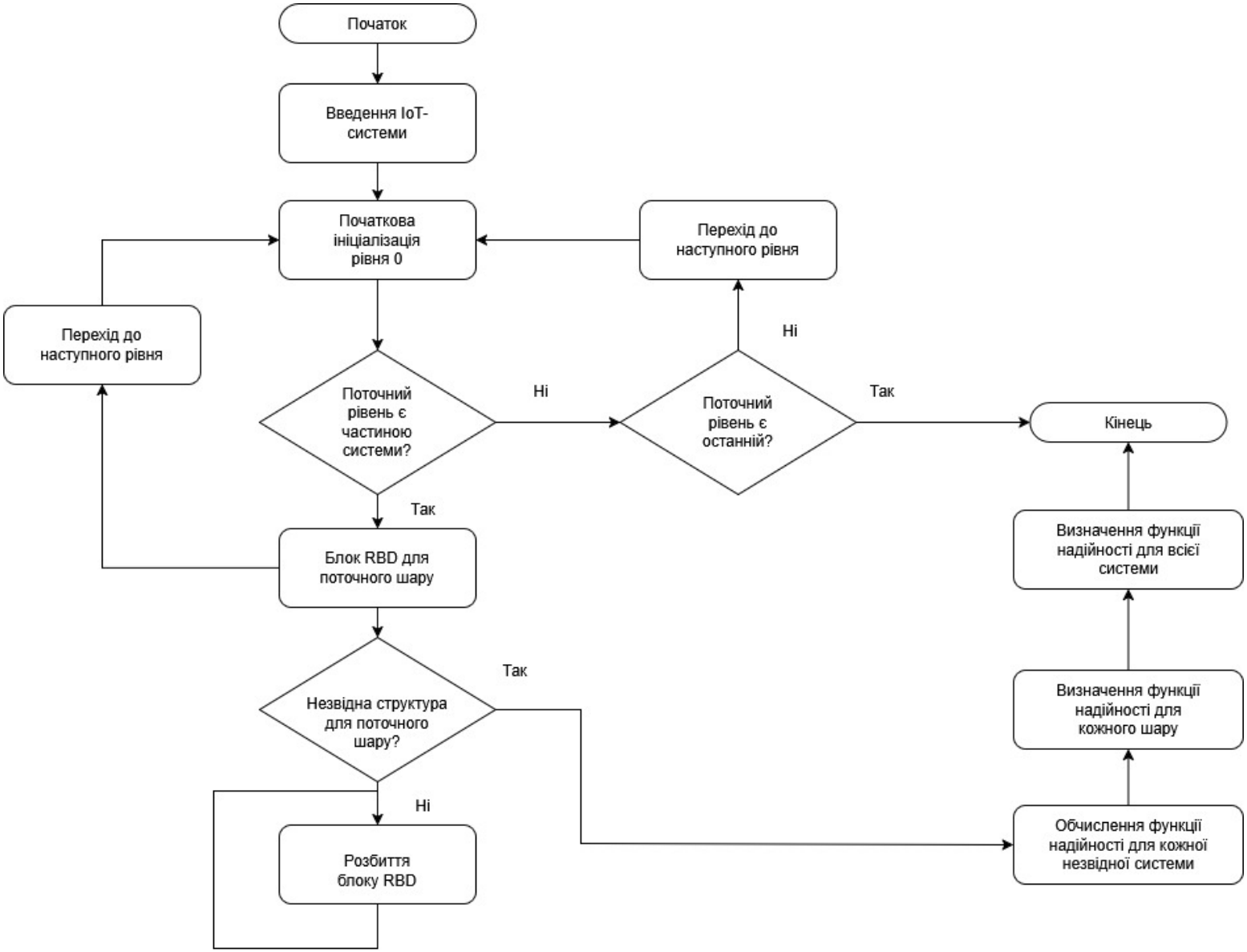


Рисунок 4.3 – Схема процесу функціонування системи оцінювання надійності багаторівневої архітектури IoT-мереж

Для рівнів, що не є кінцевими, здійснюється подальший розподіл. Кожен рівень перевіряється на наявність нерозкладної структури. Якщо структура рівня є нерозкладною, її аналізують як єдиний елемент, оцінюючи функцію надійності без додаткового розбиття. Якщо ж рівень складається з багатьох підкомпонентів, він підлягає подальшій декомпозиції, розбиваючись на менші складові частини. Цей підхід дозволяє зменшити складність аналізу, працюючи на більш дрібних рівнях, що робить обчислення точнішими.

На останньому рівні оцінки виконується аналіз залежності між компонентами та їхньої динамічної поведінки. Якщо компоненти мають взаємозв’язки або їхня поведінка змінюється у часі, тоді використовується моделювання на основі станів, наприклад, метод Марковських ланцюгів. Якщо ж залежностей немає, кожен компонент розглядається незалежно, і для нього визначається окрема функція надійності.

Після того як всі рівні та їхні компоненти було оцінено, відбувається зворотній процес – агрегування результатів. Спочатку обчислюється функція надійності для всіх нерозкладних структур, потім – для кожного рівня окремо, і, нарешті, проводиться загальний розрахунок функції надійності для всієї IoT-системи. Цей процес реалізується за підходом "знизу вгору", що дозволяє крок за кроком отримати повну оцінку надійності системи.

Такий метод аналізу має кілька ключових переваг. По-перше, він забезпечує масштабованість, оскільки працює з ієрархічною структурою, що дозволяє ефективно оцінювати як малі, так і великі IoT-системи. По-друге, він зменшує обчислювальну складність, адже внутрішні ітерації обмежуються окремими рівнями, що дозволяє локалізувати аналіз та уникати зайвих повторних обчислень. По-третє, підхід є досить гнучким, оскільки дозволяє використовувати різні методи оцінки надійності, такі як RBD або Марковські моделі, що дозволяє адаптувати його під різні випадки застосування.

Загалом, представлена схема дозволяє проводити структурований аналіз надійності складних багаторівневих IoT-систем. Вона може застосовуватися в розробці як простих рішень, так і великих інфраструктурних проектів, що

використовують IoT-технології. Завдяки чітко визначеній послідовності дій та ефективній ієрархічній організації, ця методика дозволяє отримати точну та достовірну оцінку надійності IoT-системи, що є критично важливим для її безперебійної роботи.

4.3 Прогнозно-аналітичний метод оцінювання надійності системи

Ще однією підсистемою у запропонованій системі оцінювання надійності є безпосередньо підсистема оцінювання надійності, процес функціонування якої, реалізується через прогнозно-аналітичний метод оцінювання надійності.

Прогнозне оцінювання надійності є важливим етапом аналізу експлуатаційних характеристик складних технічних систем, особливо тих, що працюють у критично важливих умовах, таких як IoT-архітектури. Пропонований прогнозно-аналітичний метод оцінювання надійності системи дозволяє не тільки оцінити поточний стан системи, але й спрогнозувати майбутні відмови та виробити стратегії підвищення надійності.

Метод прогнозного оцінювання надійності системи подамо у вигляді наступних етапів:

1. Формування функції надійності системи для багаторівневої архітектури IoT-мереж (реалізується підсистемою визначення функції надійності для багаторівневої архітектури IoT-мереж).

2. Аналіз динаміки змін надійності у часі. Після визначення функції надійності здійснюється обчислення значення $R(t)$ для різних моментів часу. Це дозволяє побудувати графік надійності. На цьому етапі важливо звернути увагу на швидкість зниження надійності. У перший період роботи система зазвичай працює стабільно, потім починається процес деградації, а пізніше – різке зниження надійності.

3. Визначення зон. Щоб зрозуміти, коли потрібно вживати заходів для підвищення надійності, пропонується розбити часовий інтервал на три основні

зони: початкова фаза експлуатації, перехідна фаза або зона деградації та фаза критичного зниження надійності. Визначення даних зон дозволяють:

– визначення «безпечного» періоду експлуатації. Якщо відомо межі першої та другої зони, можна оцінити, наскільки довго система може працювати без значного ризику відмов.

– прогнозування часу для технічного обслуговування. Якщо відомо точку, де відбувається різке зниження надійності (перехід із другої у третю зону), можна встановити оптимальний час для технічного обслуговування.

– можливість адаптації резервування. Якщо система входить у третю зону, варто передбачити механізми відмовостійкості (гарячий резерв, модульна заміна тощо).

Перша зона визначається як область, де надійність всієї системи залишається на високому рівні ((t) >0.9). Це відповідає початковому періоду роботи, коли система ще не зазнає масових відмов. Умовний критерій для даної зони $t \leq t_1, R(t_1)$ =0.9

Друга зона визначається як область, де відмови починають проявлятися значніше, тобто функція надійності має найбільший нахил. Це можна знайти через точку перегину кривої $R(t)$, тобто:

$$\frac{d^2R(t)}{dt^2} = 0 \qquad (4.2)$$

У загальному випадку необхідно вирішити рівняння:

$$R''(t) = 0 \qquad (4.3)$$

Якщо $R(t)$ задано у вигляді дискретного ряду значень, то друга похідна може бути апроксимована через кінцеві різниці:

$$R''(t_i) \approx \frac{R(t_{i+1}) - 2R(t_i) + R(t_{i-1})}{\Delta t^2} \quad (4.4)$$

де Δt – крок дискретизації.

Тоді для визначення точки перегину для деякого t_i слід перевірити умови (друга умова визначає зміну знаку):

$$\begin{cases} R''(t_i) \approx 0 \\ R''(t_{i-1}) \cdot R''(t_i) < 0 \end{cases} \quad (4.5)$$

Третя зона це область, де надійність падає нижче за 0.5, і система досягає критичного рівня. Умовний критерій для даної зони визначається як $R(t)$ <0.5.

Таким чином пропонований прогнозно-аналітичний метод оцінювання надійності IoT-систем дозволяє не лише визначити її поточний стан, а й спрогнозувати динаміку змін у часі. Основна ідея методу полягає у визначенні функції надійності системи та подальшому аналізі її поведінки, що дає змогу ідентифікувати періоди стабільної роботи, деградації та критичного зниження надійності.

На основі обчислення значень функції надійності для різних моментів часу будується графік, за яким можна виявити ключові точки, такі як момент початку помітного зниження надійності та точку перегину, що відображає перехід від стабільного функціонування до зони підвищеного ризику. Розбиття всього періоду експлуатації на три зони – початкову фазу, період деградації та фазу критичного зниження – дозволяє визначити, коли необхідне технічне обслуговування або резервування компонентів.

Такий підхід забезпечує можливість своєчасного реагування на потенційні відмови, дозволяє розробити стратегії резервування та оптимізувати процес технічного обслуговування системи, що в кінцевому підсумку підвищує її загальну стійкість і продовжує термін експлуатації.

4.4 Експериментальні дослідження системи оцінювання надійності багаторівневої архітектури IoT-мереж

Метою проведення експериментів було визначення поточного стану надійності системи Інтернету речей, а також періодів її стабільного функціонування, перехідного стану та критичної зони деградації шляхом моделювання роботи системи оцінювання надійності багаторівневої архітектури мереж Інтернету речей.

В якості вхідних параметрів, що були задіяні для проведення оцінки надійності, було визначено параметр інтенсивності відмов λ, закон розподілу та час проведення моделювання.

Параметр інтенсивності відмов λ склав $1{,}174 \cdot 10^{-5}$, що відповідає стандартним промисловим характеристикам сенсорних пристроїв. Даний показник був однаковим для всіх пристроїв, що брали участь у процесі симуляції.

Тривалість симуляції склала 4380 годин, що відповідає періоду половині року.

Рівняння, яке потрібно враховувати в симуляційній частині цієї роботи, є спрощеною формою того, що описує модель, запропонована у попередньому розділі (4.1). Для проведення експериментальних досліджень модель IoT представлялась як система, що складається з чотирьох основних підсистем (рис. 4.2). Кожна з цих підсистем має аналітичну модель:

Для підсистема пристроїв Інтернету речей ППІР задіяно модель k-з-n.

Для решти підсистем використані паралельні та послідовні структури, як було розглянуто в попередніх розділах.

Для проведення експериментальних досліджень введемо деякі спрощення попередніх рівнянь, виходячи із таких припущень:

– підсистема доступу до мережі та ядро мережі розглядаються як одна підсистема з точки зору діаграми надійності. Причина цього полягає в тому, що шлях передавання даних може проходити через одну з двох паралельних структур,

що складаються з вузлів мережевих технологій та вузлів ядра мережі, які знаходяться в послідовному з'єднанні;

– було зафіксовано функцію надійності на рівні одиниці для підсистем управління даними УД та презентації ПП. Мотивація цього припущення полягає в тому, що дослідження цих підсистем не входить у межі даної кваліфікаційної роботи через їхню високу складність та специфіку.

Враховуючи наведені припущення, відповідно до виразу (4.1) розглядаємо таке рівняння:

$$R_{\text{Системи}}(t) = R_{\text{ППІР}}(t) \times R_{\text{ПЗ}}(t) \tag{4.6}$$

Враховуючи експоненційний закон розподілу, обрахунок функції надійності здійснювався за наступною формулою:

$$R(t_i) = e^{-\lambda t} \tag{4.7}$$

Таким чином всі параметри, що були використані для експерименту наведені у таблиці 4.1.

Таблиця 4.1 – Параметри, що використанні для проведення експерименту

Параметр	Опис
Інтенсивність відмов (λ)	$1{,}174 \cdot 10^{-5}$
Закон розподілу	Експоненціальний
Тривалість симуляції склала	4380 год
Кількість елементів у послідовному з'єднанні	3
Кількість елементів у паралельнму з'єднанні	2
Імовірність працездатності системи у з'єднанні n-по-k	85% та 90%

Спочатку експеримент проводився для системи n-по-k при 85%. Криві, даного експерименту подані на рис. 4.4.

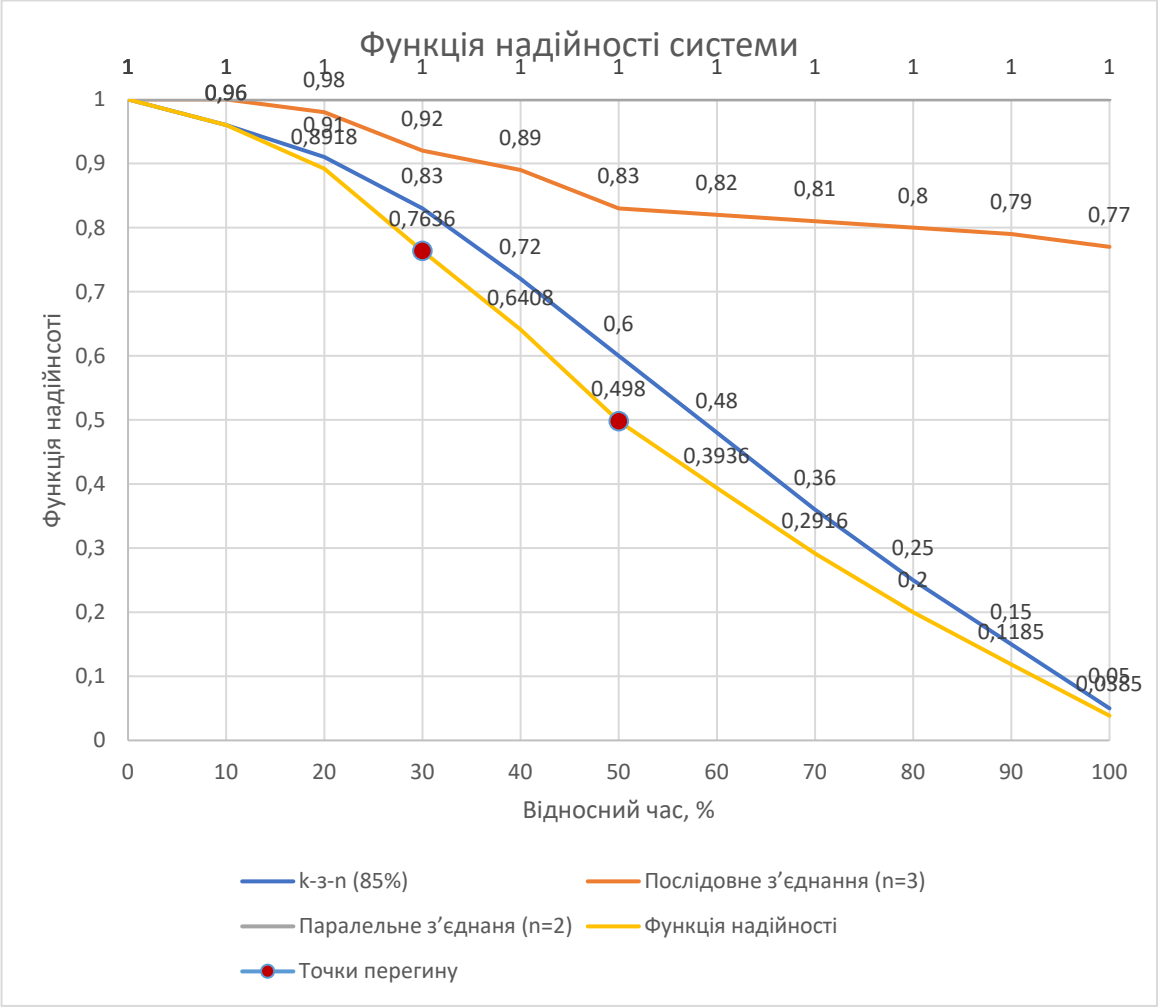


Рисунок 4.4 – Оцінка надійності системи Інтернету речей із підсистемою n-по-k (85%)

Наведені графіки показують, як змінюється функція надійності різних конфігурацій системи Інтернету речей у часі. Сформовано чотири основні криві, кожна з яких відповідає певному способу побудови системи.

Синя крива представляє систему k-out-of-n (85%), де система працює, якщо щонайменше 85% компонентів залишаються справними. Ця крива спочатку знижується повільно, але з часом її нахил стає більш різким, що свідчить про поступове зростання ймовірності відмови системи.

Помаранчева крива відповідає послідовному з’єднанню з трьома компонентами. У такій конфігурації надійність спадає найшвидше, оскільки вихід з ладу будь-якого з компонентів спричиняє відмову всієї системи Інтернету речей. Це добре видно на графіку: хоча на початку функція надійності залишається близькою до одиниці, вона швидко зменшується, досягаючи 0,77 до кінця експерименту.

Сіра крива відображає паралельне з’єднання (n=2), де система працює, поки хоча б один із двох компонентів залишається справним.

Остання, жовта крива показує загальну функцію надійності всієї системи. Вона поєднує ефекти різних підсистем і демонструє загальний тренд у зміні надійності всієї IoT-архітектури. Видно, що її поведінка найбільше нагадує k-з-n систему, оскільки саме цей підхід має ключовий вплив на загальну стійкість системи.

Також за допомогою прогнозно-аналітичного методу оцінювання надійності IoT системи, було визначено дві точки перегину на рівні 0,76 та 0,498, що дозволяє виділити три зони відповідно до прогнозно-аналітичного методу. У першій зоні, де значення надійності перевищує 0,76, система знаходиться у стабільному стані, забезпечуючи високий рівень надійності. Друга зона, між 0,76 та 0,498, характеризується поступовим зниженням надійності, що вказує на можливі ризики та необхідність моніторингу або коригуючих дій. Третя зона, де надійність падає нижче 0,498, є критичною, оскільки система досягає межі деградації, що може призвести до втрати працездатності без відповідних заходів.

Також було проведено моделювання роботи системи оцінки надійності системи Інтернету речей, у складі якої k-з-n склала 90% (оцінку надійності системи Інтернету речей із підсистемою n-по-k, що встановлена на рівні 90% наведено на рис. 4.5). Можна відмітити, що загальна крива надійності спадає повільніше. Крім того, на другому графіку точки перегину, які визначають зони стабільного функціонування, перехідних станів та критичних зон, зміщені в порівнянні з першим графіком. Це вказує на те, що система зберігає стабільність протягом більшого періоду часу, перш ніж починає деградувати.

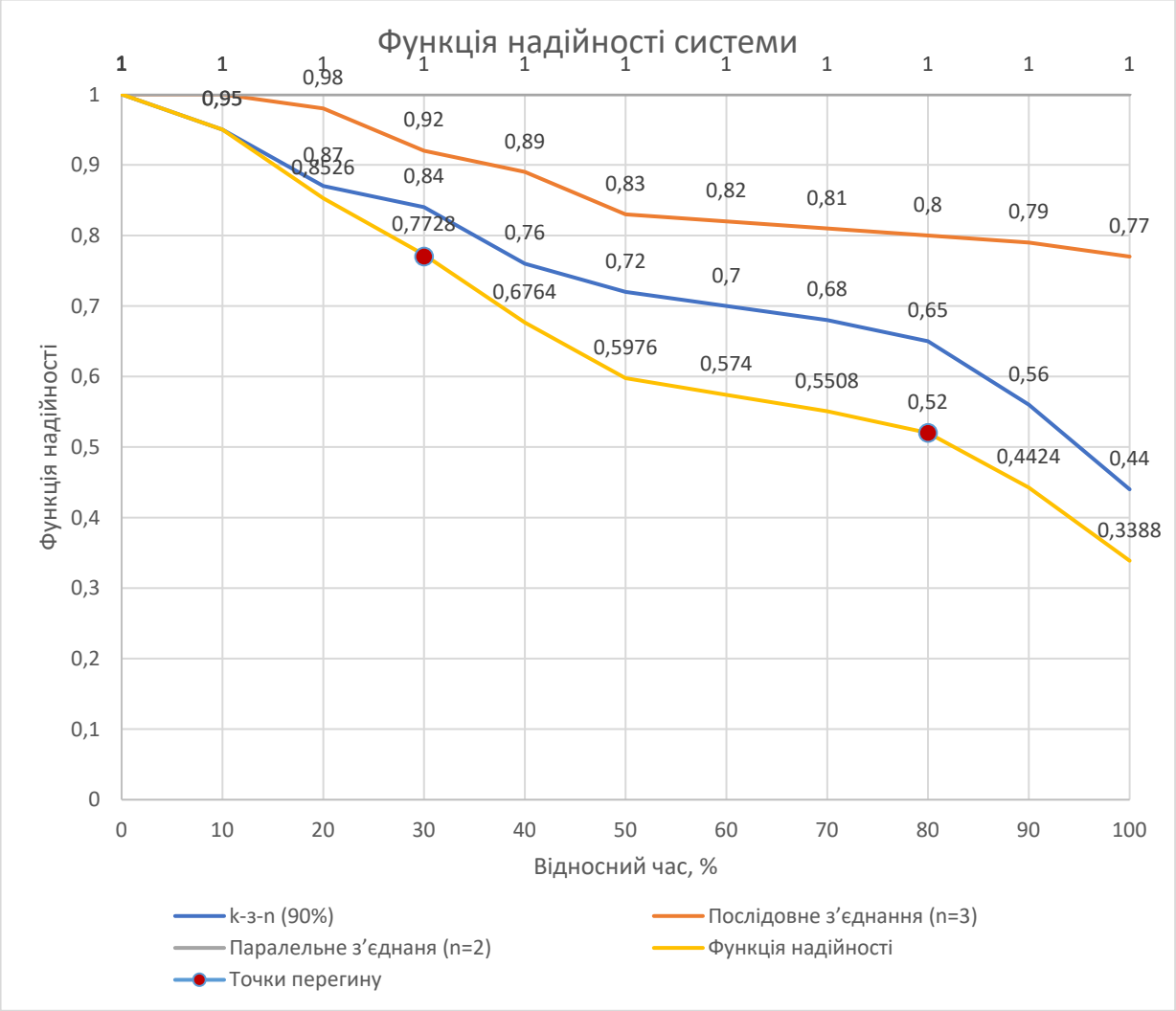


Рисунок 4.5 – Оцінка надійності системи Інтернету речей із підсистемою n-по-k (90%)

4.5 Висновки

Таким чином запропонована систему оцінювання надійності IoT мереж, що складається із двох підсистем. Першою підсистемою є підсистема визначення функції надійності для багаторівневої архітектури IoT-мереж. Дана підсистема відповідає за визначення функції надійності архітектури Інтернету речей, що передбачає системний аналіз усіх рівнів мережі та використання моделі діаграм надійності RBD. Це дозволяє не лише візуалізувати структуру системи, а й оцінити вплив окремих компонентів на загальну надійність. Друга підсистема зосереджена

на безпосередньому оцінюванні надійності, використовуючи прогнозно-аналітичний метод. Вона аналізує поточний стан мережі, дозволяючи передбачати можливі відмови чи зниження ефективності роботи.

Запропонований прогнозно-аналітичний метод оцінювання надійності IoT-мереж дозволяє визначити поточний стан системи та спрогнозувати майбутні відмови. Метод базується на аналізі функції надійності у часі та поділі експлуатаційного періоду на три зони: стабільної роботи, деградації (перехідна зона, визначається через точку перегину), та критичного зниження ($R(t) < 0.5$). Це дає змогу оцінити безпечний період роботи, визначити оптимальний час для технічного обслуговування та передбачити необхідність резервування для підвищення надійності системи.

Проведено експериментальне дослідження оцінки надійності системи Інтернету речей із різними конфігураціями. Зокрема, порівнювались системи, у яких підсистеми сенсорних мереж мали різну ймовірність безвідмовної роботи. Основна відмінність між ними полягала у використанні різних конфігурацій k-з-n: у першому випадку система функціонувала за умови справності 85% компонентів, тоді як у другому – за умови збереження 90% працездатних елементів.

ВИСНОВКИ

Запропоновано систему оцінювання надійності багаторівневої архітектури IoT-мереж, яка дозволяє визначати поточний стан надійності мережі, періоди її стабільного функціонування, перехідні стани та критичні зони деградації. Досягнення цієї мети стало можливим завдяки розробці методики аналізу надійності IoT-мереж із використанням методу RBD (Reliability Block Diagram) та прогнозно-аналітичного підходу до оцінювання ймовірності відмов компонентів системи.

У першому розділі проведено огляд відомих рішень для підвищення надійності систем Інтернету речей, а також методів оцінювання надійності складних систем. Виокремлено їх сильні та слабкі сторони. Виконано постановку задачі дослідження.

У другому розділі запропонована п’ятирівнева архітектура, яка включає рівні сприйняття, мережевого доступу, ядра мережі, проміжного програмного забезпечення та застосунків. Така структура дозволяє ефективно інтегрувати різні IoT-пристрої та технології, забезпечуючи модульність і гнучкість системи. Запропонована архітектура розроблена з урахуванням можливості застосування методу RBD для оцінки надійності системи. Чітке розмежування рівнів сприяє точному моделюванню відмовостійкості кожного компонента, що дозволяє визначити критичні вузли та оптимізувати систему з погляду забезпечення її безперервного функціонування.

У третьому розділі запропонована модель представлення функцій надійності рівнів для багаторівневої архітектури IoT-мережі базується на детальному аналізі кожного рівня системи як окремої підсистеми, що підлягає дослідженню за допомогою методів оцінки надійності. Зокрема, використання методу діаграм надійності дозволяє більш точно моделювати структурні особливості кожного рівня та враховувати всі можливі сценарії відмов. Основна ідея такого підходу полягає у визначенні внутрішньої структури кожного рівня, виявленні його

ключових компонентів та дослідженні їхньої взаємодії як між собою, так і з іншими рівнями багаторівневої IoT-архітектури.

У четвертому розділі представлено систему оцінювання надійності мереж Інтернету речей. Пропонована система складається із двох підсистем. Першою підсистемою є підсистема визначення функції надійності для багаторівневої архітектури IoT-мереж. Ця підсистема відповідає за визначення функції надійності архітектури Інтернету речей, що передбачає системний аналіз усіх рівнів мережі та використання моделі діаграм надійності RBD. Це дозволяє не лише візуалізувати структуру системи, а й оцінити вплив окремих компонентів на загальну надійність. Друга підсистема зосереджена на безпосередньому оцінюванні надійності, використовуючи прогнозно-аналітичний метод. Вона аналізує поточний стан мережі, дозволяючи передбачати можливі відмови чи зниження ефективності роботи.

Також запропонований прогнозно-аналітичний метод оцінювання надійності IoT-мереж дозволяє визначити поточний стан системи та спрогнозувати майбутні відмови. Метод базується на аналізі функції надійності у часі та поділі експлуатаційного періоду на три зони: стабільної роботи, деградації (перехідна зона, визначається через точку перегину), та критичного зниження ($R(t) < 0.5$). Це дає змогу оцінити безпечний період роботи, визначити оптимальний час для технічного обслуговування та передбачити необхідність резервування для підвищення надійності системи.

За темою кваліфікаційної роботи опубліковано одну публікацію у Збірнику наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2024». (Хмельницький – 2024. – С. 421-424).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Kumar S., Ranjan P., Singh P., Tripathy M. R. Design and Implementation of Fault Tolerance Technique for Internet of Things (IoT). *Proceedings of the 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*. Bhimtal, India, 2020. P. 154–159. DOI: 10.1109/CICN49253.2020.9242553.

2. Grover J., Garimella R. M. Reliable and Fault-Tolerant IoT-Edge Architecture. *Proceedings of the 2018 IEEE SENSORS*. New Delhi, India, 2018. P. 1–4. DOI: 10.1109/ICSENS.2018.8589624.

3. Kozar A., Del Monte B., Zeuch S., Markl V. Fault Tolerance Placement in the Internet of Things. *Proceedings of the ACM on Management of Data*. 2023. 2(3), 138. P. 1–29. DOI: 10.1145/3654941.

4. Coman C., D'Amico G., Coman A., Florescu A. Techniques to Improve Reliability in an IoT Architecture Framework for Intelligent Products. *IEEE Access*. 2021. P. 1–1. DOI: 10.1109/ACCESS.2021.3072168.

5. Li L., Jin Z., Li G., Zheng L., Wei Q. Modeling and Analyzing the Reliability and Cost of Service Composition in the IoT: A Probabilistic Approach. *Proceedings of the 2012 IEEE 19th International Conference on Web Services (ICWS)*. Honolulu, HI, USA, 2012. P. 584–591. DOI: 10.1109/ICWS.2012.25.

6. Zhou S. Supporting Fault Tolerance in the Internet of Things. Ph.D. dissertation. Dept. Elect. Eng. Comput. Sci., Univ. of California, Irvine, CA, USA, 2015.

7. Jammalamadaka S., Chokara B., Jammalamadaka S. B., Duvvuri D. B. K. K. Enhancing the Fault Tolerance of a Multi-Layered IoT Network through Rectangular and Interstitial Mesh in the Gateway Layer. *Journal of Sensor and Actuator Networks*. 2023. 12(5), 76. DOI: 10.3390/jsan12050076.

8. Melo M., Aquino G. FaTEMa: A Framework for Multi-Layer Fault Tolerance in IoT Systems. *Sensors*. 2021. 21(21), 7181. DOI: 10.3390/s21217181.

9. Marcozzi M., Gemikonakli O., Gemikonakli E., Ever E., Mostarda L. Availability Evaluation of IoT Systems with Byzantine Fault-Tolerance for Mission-critical Applications. *arXiv:2305.09262*. 2023. DOI: 10.1016/j.iot.2023.100889.

10. Premalatha P. B., Prakasam P. Priority-Based Fault Tolerance Mechanism with Neighbour Candidate Node Discovery Algorithm and Task Processing by Replication and Forwarding Technique under Fog-IoT Wireless Computing Environments. *Simulation Modelling Practice and Theory*. 2024. 135, 102980. DOI: 10.1016/j.simpat.2024.102980.

11. Monte Carlo Simulation. Доступно онлайн: https://eracons.com/resources/monte-carlo-simulation (дата звернення 19.03.2025).

12. Satyanarayanan M., Bahl P., Cáceres R., Davies N. Edge Analytics in the Internet of Things. *IEEE Pervasive Computing*. 2015. Vol. 14, No. 2. P. 24–31. DOI: 10.1109/MPRV.2015.32.

13. Satyanarayanan M. The Emergence of Edge Computing. *Computer*. 2017. Vol. 50, No. 1. P. 30–39. DOI: 10.1109/MC.2017.9.

14. Datta S.K., Bonnet C., Haerri J. Fog Computing Architecture to Enable Consumer-Centric Internet of Things Services. *Proceedings of the 2015 IEEE International Symposium on Consumer Electronics (ISCE)*. Madrid, Spain, 2015. P. 1–2. DOI: 10.1109/ISCE.2015.7177808.

15. What Is Fault Tolerance? Definition, benefits, components of, and considerations for fault tolerant systems. URL: https://www.fortinet.com/resources/cyberglossary/fault-tolerance (дата звернення 19.03.2025).

16. Fault-tolerance Techniques in Computer System, URL: https://www.geeksforgeeks.org/fault-tolerance-techniques-in-computer-system/ (дата звернення 19.03.2025).

17. Salvador R., Otero A., Mora J., de la Torre E., Sekanina L., Riesgo T. Fault Tolerance Analysis and Self-Healing Strategy of Autonomous, Evolvable Hardware Systems. *Proceedings of the 2011 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*. Cancun, Mexico, 2011. P. 164–169. DOI: 10.1109/ReConFig.2011.37.

18. What is fault tolerance, and how to build fault-tolerant systems, URL: https://www.cockroachlabs.com/blog/what-is-fault-tolerance/ (дата звернення 19.03.2025).

19. Caseiro L., Mendes A. Fault Analysis and Non-Redundant Fault Tolerance in 3-Level Double Conversion UPS Systems Using Finite-Control-Set Model Predictive Control. *Energies*. 2021. 14, 2210. DOI: 10.3390/en14082210.

20. Zhang W., Xu D., Enjeti P., Li H., Hawke J., Krishnamoorthy H. Survey on Fault-Tolerant Techniques for Power Electronic Converters. *IEEE Trans. Power Electron*. 2014. 29, 6319–6331.

21. Lezana P., Pou J., Meynard T., Rodriguez J., Ceballos S., Richardeau F. Survey on Fault Operation on Multilevel Inverters. *IEEE Trans. Ind. Electron*. 2010. 57, 2207–2218.

22. Hu K., Liu Z., Yang Y., Iannuzzo F., Blaabjerg F. Ensuring a Reliable Operation of Two-Level IGBT-Based Power Converters: A Review of Monitoring and Fault-Tolerant Approaches. *IEEE Access*. 2020. 8, 89988–90022.

23. Zhang Y., Zhu Q., Tan X., Zhang T., Wang M. Fault-Tolerant Control for Neutral-Point-Clamped Converter Based on a Fourth Asymmetric Leg. *Proceedings of the 2016 IEEE 8th International Power Electronics and Motion Control Conference (IPEMC-ECCE Asia)*, Hefei, China, 22–26 May 2016, 1065–1071.

24. Болдуєв М., Болдуєва О., Лищенко О. Сучасні підходи до забезпечення надійності та безпеки інформації в корпоративних телекомунікаційних системах. *Агросвіт*. 2024. № 13, с. 40. DOI: 10.32702/2306-6792.2024.13.40.

25. Ku H.K., Im W.S., Kim J.M., Suh Y.S. Fault Detection and Tolerant Control of 3-Phase NPC Active Rectifier. *Proceedings of the 2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, Raleigh, NC, USA, 15–20 September 2012, 4519–4524.

26. Ku H.K., Kim J.M. Multiple Open-Switch Faults Detection and Faults Tolerant Method of Three-Level Three-Phase NPC Active Rectifier. *Proceedings of the IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*, Vienna, Austria, 10–13 November 2013, 1062–1067.

27. Choi U., Lee J., Blaabjerg F., Lee K. Open-Circuit Fault Diagnosis and Fault-Tolerant Control for a Grid-Connected NPC Inverter. *IEEE Transactions on Power Electronics*. 2016. 31. 7234–7247.

28. Why do you need a Reliability Block Diagram? URL: https://www.armsreliability.com/page/resources/blog/why-do-you-need-a-reliability-block-diagram (дата звернення 19.03.2025).

29. Reliability Block Diagram, URL: https://www.jmp.com/support/help/en/18.1/index.shtml#page/jmp/reliability-block-diagram.shtml (дата звернення 19.03.2025).

30. Reliability Block Diagram Fundamentals, URL: https://accendoreliability.com/reliability-block-diagram-fundamentals/ (дата звернення 19.03.2025).

31. Reliability in Maintenance Series: Understanding Reliability Block Diagrams (RBD), URL: https://www.trmnet.com/2022/01/reliability-in-maintenance-series-understanding-reliability-block-diagrams-rbd/ (дата звернення 19.03.2025).

32. Довженко Н., Іваніченко Є., Складанний П., Аушева Н. Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 1, № 25, с. 390–400. DOI: 10.28925/2663-4023.2024.25.390400.

33. Liu J., Chen M., Wang L. A new model of industrial internet of things with security mechanism – An application in complex workshop of diesel engine. *Proceedings of the Institution of Mechanical Engineers*, Part C. 2019. 234. 2, 564–574. DOI: 10.1177/0954406219884970.

34. Lu Y., Xu L. D. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal*. 2019. 6. 2. 2103–2115. DOI: 10.1109/JIOT.2018.2869847.

35. Czeczot G., Rojek I., Mikołajewski D. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors // Electronics. 2023. 12. 2503. DOI: 10.3390/electronics12112503.

36. Katebi R., He J., Bobeck T.A., Khan W.A., Weise N. High-Efficiency Fault-Tolerant Three-Level SiC Active NPC Converter for Safety-Critical Renewable Energy Applications. *Proceedings of the 2019 IEEE 10th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Xi'an, China, 3–6 June 2019, 665–669.

37. Abdelghani A.B.B., Abdelghani H.B., Richardeau F., Blaquière J., Mosser F., Slama-Belkhodja I. Versatile Three-Level FC-NPC Converter With High Fault-Tolerance Capabilities: Switch Fault Detection and Isolation and Safe Postfault Operation. *IEEE Transactions on Industrial Electronics*. 2017. 64. 6453–6464.

38. Lee J.S., Lee K.B. Open-Circuit Fault-Tolerant Control for Outer Switches of Three-Level Rectifiers in Wind Turbine Systems. *IEEE Transactions on Power Electronics*. 2016. 31. 3806–3815.

39. Yu Y., Li X., Wei L. Fault Tolerant Control of Five-Level Inverter Based on Redundancy Space Vector Optimization and Topology Reconfiguration. *IEEE Access*. 2020. 8. 194342–194350.

40. Zhang Z., Liu X., Cai K., Gao F., Kennel R. Fault Tolerant Predictive Control of Three-Level Neutral-Point-Clamped Back-to-Back Power Converters. *Proceedings of the 2018 International Power Electronics Conference (IPEC-Niigata 2018 -ECCE Asia)*, Niigata, Japan, 20–24 May 2018. 3965–3970.

41. Halabi L.M., Alsofyani I.M., Lee K.B. Multiple-Fault-Tolerant Strategy for Three-Phase Hybrid Active Neutral Point Clamped Converters Using Enhanced Space Vector Modulation Technique. *IEEE Access*. 2020. 8. 180113–180123.

42. Halabi L.M., Mohd Alsofyani I., Lee K.B. Open-Circuit Fault Tolerance Method for Three-Level Hybrid Active Neutral Point Clamped Converters. *Electronics*. 2020. 9. 1535.

43. Mohamed A., Wang F., Butun I., Qadir J., Lagerström R., Gastaldo P., Caviglia D.D. Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks. *Sensors*. 2022. 22. 3498.

44. Pospisil O., Fujdiak R., Mikhaylov K., Ruotsalainen H., Misurec J. Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study. *Applied Sciences*. 2021. 11. 7642.

45. Sabovic A., Delgado C., Subotic D., Jooris B., De Poorter E., Famaey J. Energy-Aware Sensing on Battery-Less LoRaWAN Devices with Energy Harvesting. *Electronics*. 2020. 9. 904.

46. Carnevali L., Ciani L., Fantechi A., Gori G., Papini M. An Efficient Library for Reliability Block Diagram Evaluation. *Applied Sciences*. 2021. 11. 4026. https://doi.org/10.3390/app11094026

47. Alfawaz O., Khedr A.M., Alwasel B., Osamy W. Reliability Evaluation for Chain Routing Protocols in Wireless Sensor Networks Using Reliability Block Diagram. *Journal of Sensor and Actuator Networks*. 2023. 12. 34. https://doi.org/10.3390/jsan12020034

48. Wategaonkar D.N., Deshpande V.S. Characterization of reliability in WSN. *Proceedings of the 2012 World Congress on Information and Communication Technologies*, Trivandrum, India, 30 October–2 November 2012. 970–975

49. Chowdhury C., Aslam N., Ahmed G., Chattapadhyay S., Neogy S., Zhang L. Novel algorithms for reliability evaluation of remotely deployed wireless sensor networks. *Wireless Personal Communications*. 2018. 98. 1331–1360.

50. Kabashkin I., Kundler J. Reliability of sensor nodes in wireless sensor networks of cyber physical systems. *Procedia Computer Science*. 2017. 104. 380–384.

51. Papini M. Reliability Evaluation of an Industrial System Through Predictive Diagnostics: Ph.D. Thesis. Universitá degli Studi di Firenze, Florence, Italy, 2021.

52. Kumar V., Patel R.B., Singh M., Vaid R. Reliability analysis in wireless sensor networks. *International Journal of Engineering and Technology*. 2011. 3. 74–79.

53. Chakraborty S., Goyal N.K., Mahapatra S., Soh S. Minimal path-based reliability model for wireless sensor networks with multistate nodes. *IEEE Transactions on Reliability*. 2019. 69. 382–400.

54. Tan J., Liu W., Wang T., Xiong N.N., Song H., Liu A., Zeng Z. An adaptive collection scheme-based matrix completion for data gathering in energy-harvesting wireless sensor networks. *IEEE Access*. 2019. 7. 6703–6723.

55. Mzyk R., Paszkiel S. Influence of Program Architecture on Software Quality Attributes. *In: Control, Computer Engineering and Neuroscience Ed. Paszkiel S. Springer International Publishing*, Cham, Switzerland, 2021. 322–329.

56. Catelani M., Ciani L., Bartolini A., Del Rio C., Guidi G., Patrizi G. Reliability Analysis of Wireless Sensor Network for Smart Farming Applications. *Sensors*. 2021. 21. 7683.

57. Liu F. Majority Decision Aggregation with Binarized Data in Wireless Sensor Networks. *Symmetry*. 2021. 13. 1671.

58. Aziz A., Osamy W., Khedr A.M., El-Sawy A.A., Singh K. Grey Wolf based compressive sensing scheme for data gathering in IoT based heterogeneous WSNs. *Wireless Networks*. 2020. V. 26. 3395–3418.

59. Pantazis N.A., Nikolidakis S.A., Vergados D.D. Energy-efficient routing protocols in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*. 2012. T. 15, c. 551–591.

60. Nidhya M., Chinnaiyan R. Reliability Evaluation of Wireless Sensor Networks Using EERN Algorithm. *Proceedings of the International Conference on Computer Networks and Communication Technologies*, Coimbatore, India, 23–24 May 2019. Springer: Singapore, 2019. 849–856.

61. Xiao Y., Li X., Li Y., Chen S. Evaluate reliability of wireless sensor networks with OBDD. *Proceedings of the 2009 IEEE International Conference on Communications*, Dresden, Germany, 14–18 June 2009. 1–5.

62. Lu Y., Dong Y.W., Wei X.M., Xiao M.R. A Hybrid Method of Redundancy System Reliability Analysis Based on AADL Models. *Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon, Portugal, 16–20 July 2018.

63. Mian Z.B., Bottaci L., Papadopoulos Y., Mahmud N. Model transformation for analyzing dependability of AADL model by using HiP-HOPS. *Journal of Systems and Software*, 2019, 151, 258–282.

64. Zhang Q., Wang S., Liu B. Approach for integrated modular avionics reconfiguration modelling and reliability analysis based on AADL. *IET Software*, 2016, 10, 18–25.

65. Wu D.H., Wei Z. Formal model-based quantitative reliability analysis using timed Coloured Petri Nets. *Reliability Engineering & System Reliability*, 2018, 176, 62–79.

66. Lu Z., Zhang Z.W., Zhuang L., Zhou J. Reliability Model of the Fly-By-Wire System Based on Stochastic Petri Net. *International Journal of Aerospace Engineering*, 2019, 2019, 2124836.

67. Mehdi I., Boudi E.M. Qualitative Functional and Dysfunctional Analysis and Physical Modeling of an Eco-Designed Mechatronics System Using Coloured Petri-nets: Application on a Regenerative Braking System. *Proceedings of the International Conference on Advanced Technologies for Humanity*, Rabat, Morocco, 26–27 November 2021.

68. Osamy W., Khedr A.M., Salim A., AlAli A.I., El-Sawy A.A. Recent studies utilizing artificial intelligence techniques for solving data collection, aggregation and dissemination challenges in wireless sensor networks: A review. *Electronics*, 2022, 11, 313.

69. Mehdi I., Boudi E.M. Towards a sustainable conceptual design of mechatronic systems application to a regenerative braking system. *Proceedings of the Materials Today: Proceedings*, Virtual, 20–22 May 2021.

70. Liu L. Verification of the SIP transaction using coloured Petri nets. *Proceedings of the Thirty-Second Australasian Conference on Computer Science*, Wellington, New Zealand, 1 January 2009.

71. Westergaard M., Verbeek H.M.W. Efficient implementation of prioritized transitions for high-level Petri nets. *Proceedings of the International Workshop on Petri Nets and Software Engineering, Newcastle upon Tyne*, UK, 20–21 June 2011.

72. Ding L., Wang H., Kang K., Wang K. A novel method for SIL verification based on system degradation using reliability block diagram. *Reliability Engineering & System Safety*, 2014, 132, 36–45.

73. Coen A., Gutiérrez L., Mena R.H. Modelling failures times with dependent renewal type models via exchangeability. *Statistics*, 2019, 53, 1112–1130.

74. Mehdi I., Boudi E.M., Mehdi M.A. Reliability, Availability, and Maintainability Assessment of a Mechatronic System Based on Timed Colored Petri Nets. *Applied Sciences*, 2024, 14, 4852.

75. Reliability Block Diagram (RBD) – System Reliability Analysis URL: https://prostask.com/2024/01/06/reliability-block-diagram-rbd/ (дата звернення 19.03.2025).

76. Пасічник В.О., Іванов О.В., Нічепорук А.О. Система оцінювання надійності багаторівневої архітектури IoT-мереж. *Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024»*. 2024. С. 421–424.

ДОДАТОК А

(обов’язковий)

КОПІЯ НАУКОВОЇ ПУБЛІКАЦІЇ

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп’ютерних наук АПКН-2024»

15-16 листопада 2024

Хмельницький 2024

УДК 004.052.3

Пасічник В.О., Іванов О.В., Нічепорук А.О.

Хмельницький національний університет

СИСТЕМА ОЦІНЮВАННЯ НАДІЙНОСТІ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ IOT-МЕРЕЖ

У даній роботі розглядається важливість надійності в системах Інтернету речей (IoT) та застосування методу діаграм надійності блоків (RBD) для їх аналізу. Досліджено чотири рівні IoT-архітектури: рівень IoT-пристроїв, рівень комунікацій, рівень управління даними та рівень відображення.

This paper examines the importance of reliability in Internet of Things (IoT) systems and the application of the Reliability Block Diagram (RBD) method for their analysis. Four levels of IoT architecture are explored: the IoT Devices Level, the Communication Level, the Data Management Level, and the Presentation Level.

Результати досліджень в області Інтернету речей (IoT) привертають значну увагу наукового співтовариства. Часто Інтернету речей розглядається як поступове розширення існуючого Інтернету, а не як щось революційне. Інший підхід бачить Інтернет речей як поєднання кількох окремих підсистем, які вже існують як самостійні технології. Однак цей підхід ігнорує важливий принцип синергії, за яким система як єдине ціле є ефективнішою, ніж просто сума її частин. Коли IoT сприймається як єдиний комплекс, стають помітними нові класи проблем, які не видно, якщо розглядати її як набір окремих елементів.

IoT підтримує роботу багатьох галузей, і для стабільності таких систем важливо забезпечити безпеку, щоб уникнути непередбачуваних збоїв. Це є ключовим фактором для досягнення надійності, яка визначає успіх будь-якої системи. Особливо важливою надійність є для наскрізних IoT-систем через їхню різнорідність. Щоб забезпечити сумісність, необхідно стандартизувати та правильно інтегрувати інтерфейси комунікаційних підсистем. Фізичні компоненти є основною частиною IoT, і саме вони часто можуть призводити до непередбачуваних збоїв у всій системі. Надійність апаратних елементів досліджується вже давно, щоб знизити ризики аварій і зберегти безпеку для користувачів.

На сьогоднішній день у науковій спільності використовуються різні моделі та підходи для аналізу надійності систем. Серед них можна виділити такі якісні методи, як аналіз режимів, наслідків і критичності відмов (FMECA), аналіз дерева

відмов (FTA), діаграми причин і наслідків (CED), а також діаграми надійності блоків (RBD) [1-3].

У даній пропонується підхід на основі RBD, що зумовлено в першу чергу складністю досліджуваної системи. Метод діаграм надійності блоків – це підхід, який застосовується для аналізу надійності складних систем. В основі цього методу лежить представлення системи у вигляді блоків, де кожен блок відповідає певному елементу або підсистемі. Діаграма зображає, як різні елементи пов'язані між собою з точки зору надійності, що допомагає виявити потенційні "слабкі місця" і оцінити вплив окремих елементів на загальну надійність системи.

Основні етапи використання методу RBD:

1. побудова блок-схеми системи: Спочатку систему розбивають на складові частини, кожна з яких представляє певну функціональну одиницю (наприклад, датчики, модулі обробки, мережеві компоненти).

2. визначення зв'язків між блоками: блоки можна з'єднати послідовно, паралельно або комбіновано. Послідовне з'єднання означає, що вся система перестане працювати, якщо хоча б один блок відмовить. Це підходить для елементів, які мають критичне значення для безперебійної роботи. Паралельне з'єднання дозволяє системі продовжувати функціонувати, навіть якщо один із блоків відмовив. Це забезпечує додаткову надійність за рахунок дублювання.

3. обчислення загальної надійності системи: після того як схема побудована, використовуються ймовірності надійності для кожного окремого блоку. Залежно від конфігурації з'єднання (послідовне, паралельне) на основі цих ймовірностей обчислюється загальна надійність системи. Для послідовного з'єднання надійність системи дорівнює добутку надійностей всіх блоків, оскільки відмова будь-якого блоку веде до відмови всієї системи. Для паралельного з'єднання надійність обчислюється за формулою, яка враховує ймовірності того, що хоча б один блок працює.

4. аналіз і оптимізація: RBD дозволяє побачити, які елементи є критичними для роботи системи та як можна підвищити її надійність. Наприклад, можна вирішити дублювати найбільш вразливі блоки або покращити параметри надійності певних елементів, що значно впливають на стабільність системи.

Для застосування методу RBD до багаторівневої архітектури IoT-мережі, першим кроком стає моделювання кожного рівня IoT як окремого блоку в схемі [1]. Наприклад, фізичний рівень може включати датчики та актуатори, які виконують ключові функції збору даних та управління. На цьому рівні важливо врахувати, що відмова одного критичного датчика може зупинити всю систему, тому для підвищення надійності можна розглянути дублювання датчиків або додати резервні пристрої.

На мережевому рівні метод RBD допомагає оцінити, наскільки стійкими є маршрутизатори, передавачі та шлюзи, адже від них залежить якісне передавання даних між датчиками та серверами обробки. Тут можливо паралельне з'єднання деяких компонентів, щоб уникнути збоїв у разі виходу з ладу окремих модулів.

Рівень обробки даних, що зазвичай включає сервери або хмарні платформи, може бути представлений як комбінація послідовних і паралельних блоків. RBD дозволяє врахувати ризики відмови як локальних, так і хмарних обчислень, особливо якщо обробка даних виконується безпосередньо в хмарі та передбачає високу пропускну здатність для стабільного функціонування. Тут RBD може підказати, чи є сенс додати дубльовані сервери або підтримувати альтернативні центри обробки даних для забезпечення безперервної роботи.

Таким чином, застосування методу RBD до IoT-мережі дозволяє виявити слабкі місця в архітектурі, визначити найбільш критичні елементи, і на основі цього оцінити, де доцільно додати резервування або підвищити надійність певних компонентів, щоб забезпечити стабільну роботу всієї системи.

У даній роботі IoT-система розглядається як структура, що складається з чотирьох рівнів (рисунок 1):

– рівень IoT-пристроїв – включає всі датчики та актуатори, які взаємодіють із фізичним середовищем та збирають необхідні дані.

– рівень комунікацій – забезпечує передачу даних від пристроїв до вищих рівнів через мережу, включаючи локальні та глобальні мережі.

– рівень управління даними – обробляє та зберігає отримані дані, виконує їх фільтрацію, аналіз та збереження для подальшого використання.

– рівень відображення – забезпечує інтерфейс для користувача або додатків, де результати аналізу стають доступними для візуалізації або дій.

Рисунок 1 – Досліджувані рівні Інтернету речей в контексті оцінювання надійності

Тоді загальний вираз для оцінки надійності буде визначатись:

$$P = P_{пп} \times P_{пк} \times P_{пуд} \times P_{пв} \quad (1)$$

Таким чином у даній науковій роботі акцентується увага на важливості надійності в системах Інтернету речей і використанні методу діаграм надійності блоків для їх аналізу. Розглянуто чотири рівні IoT-архітектури: рівень IoT-пристроїв, рівень комунікацій, рівень управління даними та рівень відображення. Метод RBD дозволяє виявити критичні компоненти та запропонувати рішення для підвищення стабільності системи через резервування та оптимізацію. Таким чином, підхід до аналізу надійності IoT-систем забезпечує основи для покращення їх функціонування та інтеграції в різні сфери.

Перелік посилань

1. Deif D., Gadallah Y. A comprehensive wireless sensor network reliability metric for critical Internet of Things applications. EURASIP J. Wirel. Commun. Netw. 2017.
2. Dâmaso A., Rosa N., Maciel P. Reliability of wireless sensor networks. Sensors 2014, 14, 15760-15785.
3. L. Xing Reliability and Resilience in the Internet of Things (Advances in Reliability Science), Elsevier; 1st edition, 2024, 374 P.

ДОДАТОК Б

(обов'язковий)

КОПІЯ ПРЕЗЕНТАЦІЇ ДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Система оцінювання надійності багаторівневої архітектури IoT-мереж

Студент групи КІ2м-23-2, **Владислав ПАСІЧНИК**

Керівник: к.т.н.,доцент**Олексій Іванов**

Хмельницький
2025

1

Об'єкт, предмет, мета дослідження

- **Об'єктом** дослідження є процеси оцінювання надійності багаторівневої IoT-архітектури на основі методу RBD.
- **Предметом** дослідження є система оцінювання надійності багаторівневої архітектури IoT-мереж.
- **Метою кваліфікаційної роботи магістра** є визначення поточного стану надійності IoT мережі, періодів її стабільного функціонування, перехідних станів та критичних зон деградації шляхом залучення системи оцінювання надійності багаторівневої архітектури IoT-мереж.

2

Наукова новизна

- набула подальшого розвитку система оцінювання надійності багаторівневої архітектури IoT-мереж, яка дозволяє визначити поточний стан надійності багаторівневої IoT-мережі, виявити періоди її стабільного функціонування, перехідні стани та критичні зони деградації, і яка відрізняється від відомих залученням системного підходу до моделювання кожного рівня системи IoT через діаграми надійності (RBD), що дозволило враховувати особливості кожного рівня, аналізувати вплив окремих компонентів на загальну надійність системи;
- удосконалено прогнозно -аналітичний метод оцінювання надійності системи, який дозволяє визначати точки перегину функції надійності та прогнозувати майбутні відмови, який відрізняється від відомих виявленням перехідних станів системи та зон критичного зниження надійності .

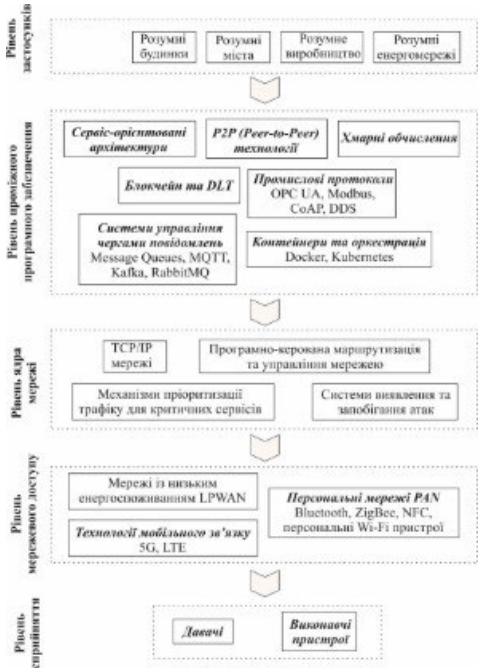
3

Актуальність дослідження. Постановка задачі

Проблеми та актуальність дослідження надійностIoT-мереж

- Зростання використання IoT → збільшення залежності від надійності мереж.
- Критичні сфери застосування → відмова систем може призвести до серйозних наслідків (аварії, збитки, загроза безпеці).
- Надійність впливає на ефективність та безперебійну роботу систем.
- Потрібні методи оцінювання для підвищення стійкості архітектури.

4



Пропонована багаторівнева архітектура IoT-мережі

5

Моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі

Модель рівня сприйняття

Рівень сприйняття складається з речей, які взаємодіють для виконання визначеної місії. До його складу можуть входити апаратні компоненти, операційні системи, комунікаційні модулі, а також модулі живлення.

Функцію надійності даного рівня визначено як

$$R_{\text{СРС}}(t) = \prod_{j=1}^{k} R_j(t),$$

де $R_j(t)$, $j = \overline{1,5}$ є відповідно функціями надійності, пов'язаними із апаратним забезпеченням, проміжним програмним забезпеченням, операційною системою (OS), модулем комунікації та підсистемами застосунків

6

Моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі

Модель рівня сенсорних мереж/рівня доступу

Функцію надійності даного рівня визначено як

$$R_{\text{СМ}}(t) = \sum_{x=k}^{m} \binom{m}{x} R(t)^x \times (1 - R(t))^{m-x}$$

де

$$R(t) = R_{\text{СРС}}(t) \times R_{\text{МД}}(t)$$

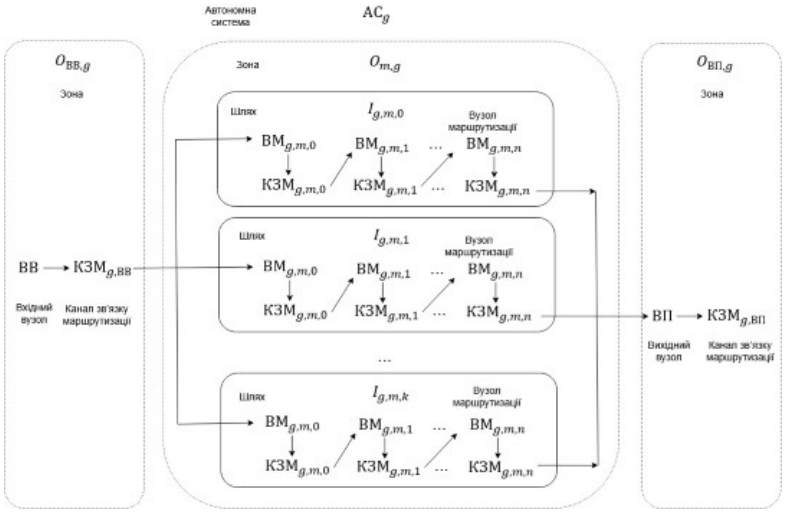
де $R_{\text{СРС}}$ – сутність рівня сприйняття,

$R_{\text{МД}}$ – компонент мережевого доступу

7

Моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі

Модель рівня ядра мережі



8

Моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі

Модель рівня ядра мережі

Загальна модель рівня ядра мережі

$$R_{\text{AC}_g}(t) = R_{\text{ВВ},g}(t) \times R_{\text{КЗМ}_{\text{ВВ},g}}(t) \times R_{O_{m,g}}(t) \times R_{\text{КЗМ}_{\text{ВП},g}}(t) \times R_{\text{ВП},g}(t)$$

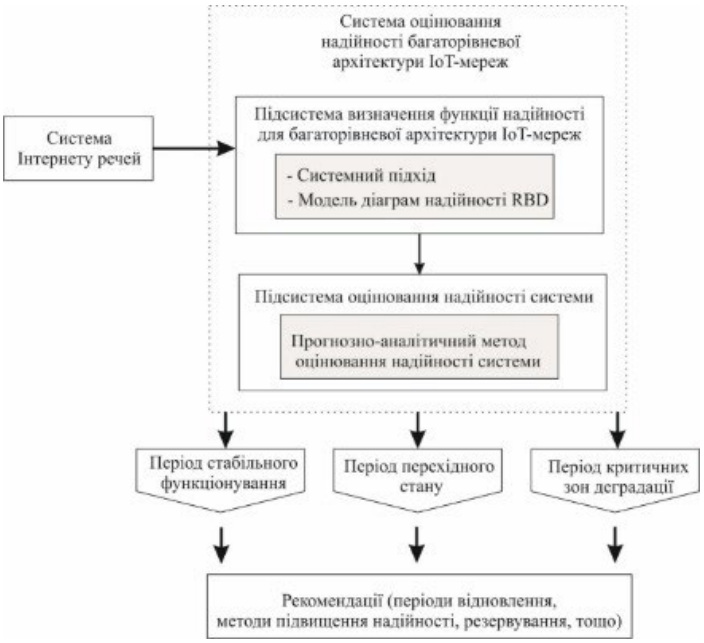
де $R_{\text{ВВ},g}(t)$ – функція надійності вихідного вузла, що належить до $AC\ g$;

$R_{\text{КЗМ}_{\text{ВВ},g}}(t)$ – функція надійності прямого з'єднання до вихідного вузла, що належить до $AC\ g$;

$R_{\text{КЗМ}_{\text{ВП},g}}(t)$– функція надійності прямого з'єднання до вузла призначення, що належить до $AC\ g$;

$R_{\text{ВП},g}(t)$ – функція надійності вузла призначення, що належить до $AC\ g$;

9



Узагальнена структура системи оцінювання надійності багаторівневої архітектури IoT-мереж

10

Прогнозно-аналітичний метод оцінювання надійності системи

Методпрогнозногооцінювання надійності системи подамо у вигляді наступних етапів:

1. Формування функції надійності системи для багаторівневої архітектури IoT-мереж (реалізується підсистемою визначення функції надійності для багаторівневоїархітектуриIoT-мереж).

2. Аналіз динаміки змін надійності у часі. Після визначення функції надійності здійснюється обчислення значення $R(t)$ для різних моментів часу. Це дозволяєпобудуватиграфік надійності. На цьому етапі важливо звернути увагу на швидкість зниження надійності. У перший період роботи система зазвичай працює стабільно, потім починається процес деградації, а пізніше – різкезниження надійності.

3. Визначення зон. Щоб зрозуміти, коли потрібно вживати заходів для підвищення надійності, пропонуєтьсярозбити часовий інтервал на три основні зони: початкова фаза експлуатації, перехідна фаза або зона деградації та фаза критичногозниження надійності.

Якщо $R(t)$ задано у вигляді дискретного ряду значень, то друга похідна може бути апроксимована через кінцеві різниці:

$$R''(t_i) \approx \frac{R(t_{i+1}) - 2R(t_i) + R(t_{i-1})}{\Delta t^2}$$

11

Експериментальні дослідження системи оцінювання надійності багаторівневої архітектури IoT-мереж

Для проведення експериментальних досліджень введено деякі спрощення попередніх рівнянь, виходячи із таких припущень:

- підсистема доступу до мережі та ядро мережі розглядаються як одна підсистема з точки зору діаграми надійності. Причина цього полягає в тому, що шлях передавання даних може проходити через одну з двох паралельних структур, що складаються з вузлів мережевих технологій та вузлів ядра мережі, які знаходяться в послідовному з'єднанні
- було зафіксовано функцію надійності на рівні одиниці для підсистем управління даними УД та презентації ПП. Мотивація цього припущення полягає в тому, що дослідження цих підсистем не входить у межі даної кваліфікаційної роботи через їхню високу складність та специфіку.

Враховуючинаведені припущення розглядалосьтаке рівняння:

$$R_{\text{Системи}}(t) = R_{\text{ППІР}}(t) \times R_{\text{ПЗ}}(t)$$

12

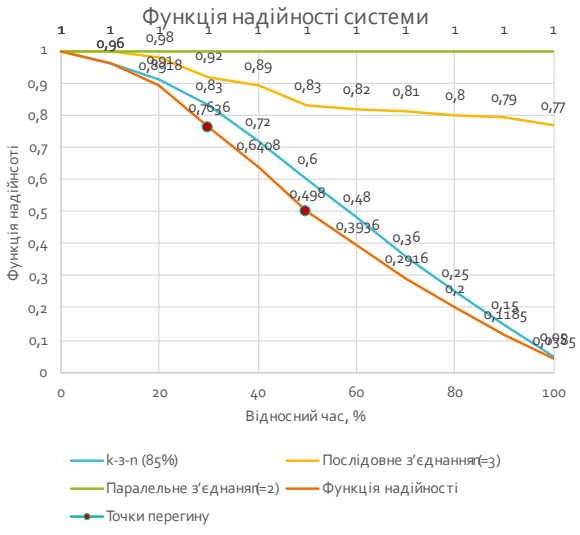
Експериментальні дослідження системи оцінювання надійності багаторівневої архітектури IoT-мереж

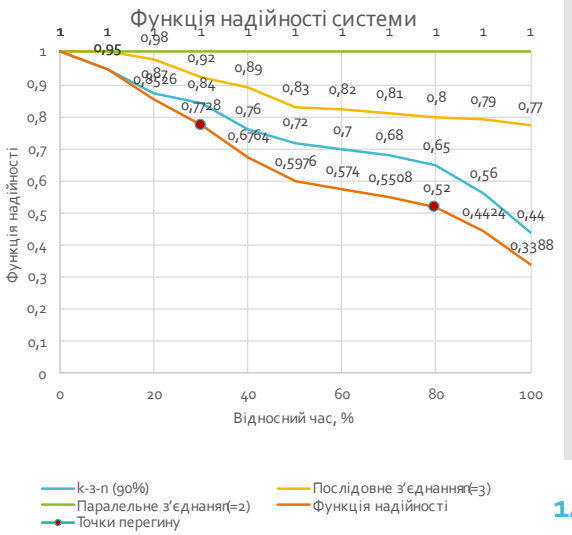
Параметри, що використанні для проведення експерименту

Параметр	Опис
Інтенсивність відмов (λ)	$1{,}174 \cdot 10^{-5}$
Закон розподілу	Експоненціальний
Тривалість симуляції склала	4380 год
Кількість елементів у послідовному з'єднанні	3
Кількість елементів у паралельнму з'єднанні	2
Імовірність працездатності системи у з'єднанні n-по-k	85% та 90%

13

Експериментальні дослідження системи оцінювання надійності багаторівневої архітектури IoT-мереж





14

Завідувачу кафедри КІІС
доктору філософії, доценту
Ользі ПАВЛОВІЙ

Пасічник Владислав Олегович
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-23-2

ЗАЯВА

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

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

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

14 квітня 2025 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Владислав ПАСІЧНИК

Тема: Система оцінювання надійності багаторівневої архітектури IoT-мереж

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 75

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано систему систему оцінювання надійності багаторівневої архітектури IoT-мереж

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

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз відомих рішень та методів оцінювання надійності мереж IoT; постановка задачі. У другому розділі розроблено багаторівневу архітектуру IoT мережі та оцінку надійності. У третьому розділі розроблено моделі представлення функцій надійності рівнів для багаторівневої архітектури іот мережі. У четвертому розділі проведено проектування системи оцінювання надійності IoT мережі

4. Позитивні сторони роботи: Запропонований прогнозно-аналітичний метод оцінювання надійності IoT-мереж дозволяє визначити поточний стан системи та спрогнозувати майбутні відмови.

5. Негативні сторони роботи: З роботи не зрозуміло чому саме у прогнозно-аналітичному методі здійснювався аналіз трьох зон на для функції надійності.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «добре» 4.25 (В)

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

"1 травня" 2025р.

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Система оцінювання надійності багаторівневої архітектури IoT-мереж

Автор: Пасічник Владислав Олегович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Іванов О.В., к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.
4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 4% і адресується до 30 першоджерела; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Олексій ІВАНОВ

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав ПАСІЧНИК

Співавтор:

Назва: ПАСІЧНИК_Система оцінювання надійності багаторівневої архітектури IoT-мереж

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:4%

Коефіцієнт подібності 2:1.3%

Мікропробіли: 7

Заміна букв: 2

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2025-04-15 12:53:44.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-04-15 Доцент Андрій Нічепорук

Дата експерт

Tue Apr 15 14:02:32 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.260 Educational

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

	Документ		Сумарний збіг по Базі Даних	
ID: 229450 Назва: МКР Система оцінювання надійності багаторівневої архітектури IoT-мереж Додано в БД: 2025-04-15 Автора: Владислав ПАСІЧНИК Керівники: Олексій ІВАНОВ Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	107995	801	1207 (1%)	16 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми