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

КВАЛІФІКАЦІЙНА РОБОТА

Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень
Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 024043.24.01.13 ПЗ

Виконав здобувач II курсу, група КІ2м-24-1 — Підпис — Сергій ЗАДВОРНИЙ (Ініціали, прізвище)

Керівник — канд.техн. наук, доц. (Науковий ступінь, учене звання) — Підпис — Олексій ІВАНОВ (Ініціали, прізвище)

Нормоконтролер — д-р техн. наук, проф. (Науковий ступінь, учене звання) — Підпис — Сергій ЛИСЕНКО (Ініціали, прізвище)

До захисту допускаю:
завідувач кафедри КІІС
«04» червня 2026 р. — підпис — Ольга ПАВЛОВА (Ініціали, прізвище)
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ДРУГИЙ (МАГІСТЕРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
Ольга ПАВЛОВА

" 12 " 01 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Задворному Сергію Олександровичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

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

Затверджена наказом ректора університету від 12.01.2026 №6

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2026 р.

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

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

Відомі методи аналізу надійності та проблеми обчислювальної складності при аналізі складних IoT систем

Процес поширення відмов в IoT-інфраструктурі та метод оцінювання надійності за допомогою бінарних діаграм рішень

Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Теоретичне дослідження та аналіз ефективності методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень

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 « 12 » 01 2026р.

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	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	15.01.2026	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	20.01.2026	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	10.02.2026	виконано
5	Робота над науковою публікацією	25.02.2026	виконано
6	Робота над розділом 3 – розробка методу для вирішення поставленої задачі	15.03.2026	виконано
7	Робота над розділом 4 – теоретичне дослідження та аналіз ефективності методу	15.04.2026	виконано
8	Оформлення пояснювальної записки згідно вимог	28.04.2026	виконано
9	Попередній захист ДРМ	29.04.2026	виконано
10	Захист ДРМ на засіданні ЕК	До 15.05.2026	

Здобувач _____ Сергій ЗАДВОРНИЙ
Підпис Ім'я, прізвище

Керівник кваліфікаційної роботи _____ Олексій ІВАНОВ
Підпис Ім'я, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Автор роботи: Задворний Сергій Олександрович

Керівник роботи: Іванов Олексій Валентинович

Пояснювальна записка: 91 с., 13 рис., 6 табл., 2 дод., 79 джерел.

НАДІЙНІСТЬ, ІНТЕРНЕТ РЕЧЕЙ, БІНАРНІ ДІАГРАМИ РІШЕНЬ, РЕДУКЦІЯ.

Об’єктом дослідження є метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Предметом дослідження є моделі, методи та засоби аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Метою кваліфікаційної роботи магістра є зниження часової складності обчислювального процесу аналізу надійності IoT-інфраструктур шляхом застосування методу редукції бінарних діаграм рішень із урахуванням конкуруючих відмов компонентів системи розумного будинку.

Для розв’язання поставлених задач використовувалися методи теорії надійності, системного аналізу, теорії графів та множин.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, який відрізняється від відомих застосуванням техніки прямої трансформації вузлів моделі відповідно до станів мережевих шлюзів замість множинної генерації та конвертації скорочених дерев відмов, що дозволило забезпечити зниження часової складності обчислювального процесу.

У кваліфікаційній роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Практична значимість отриманих результатів полягає у розробці методу оцінювання надійності IoT-інфраструктур розумного будинку, що враховує конкуруючі відмови компонентів та забезпечує суттєво меншу часову складність порівняно з існуючими методами. Застосування методу редукції бінарних діаграм рішень дозволяє отримувати точні кількісні оцінки ненадійності системи та визначати критичні компоненти за мірою важливості Бірнбаума, що створює практичну основу для обґрунтованого прийняття інженерних рішень щодо підвищення надійності, зокрема, пріоритизації заходів захисту від поширюваних відмов датчиків як домінуючого чинника системної ненадійності.

У першому розділі проведено оглядовий аналіз предметної області, розглянуто архітектуру та протоколи зв'язку IoT-інфраструктури розумного будинку, виконано класифікацію відмов та проаналізовано обмеження існуючих методів оцінки надійності, за результатами чого сформульовано постановку задачі дослідження.

У другому розділі досліджено механізми поширення відмов в IoT-інфраструктурі, розкрито концепцію конкуруючих відмов та явище часової конкуренції, а також викладено теоретичні основи методу оцінювання надійності на основі бінарних діаграм рішень та міри важливості компонентів.

У третьому розділі розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, описано алгоритм редукції та виконано теоретичну оцінку обчислювальної складності, що підтвердила переваги запропонованого підходу порівняно з класичними методами.

У четвертому розділі проведено теоретичне дослідження ефективності розробленого методу, виконано порівняльний аналіз точності та обчислювальної складності, а також аналіз важливості компонентів за мірою Бірнбаума, що дозволило виявити найбільш критичні елементи IoT-інфраструктури розумного будинку.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БДР – Бінарні діаграми рішень

ВФЗ – Вузол функціональної залежності

ПВШ – Подія відмови шлюзу

FMECA – Failure mode, effects, and criticality analysis

FT – Fault tree

IoT – Internet of Things

ВСТУП

Стрімкий розвиток технологій Інтернету речей (IoT) та масове впровадження систем розумного будинку зумовили появу принципово нових вимог до надійності мережевих інфраструктур. Сучасна IoT-інфраструктура розумного будинку являє собою складну розподілену систему, що об'єднує десятки різнорідних пристроїв, таких як давачі, виконавчі механізми та мережеві шлюзи, взаємодія яких забезпечується через спільне бездротове середовище передачі даних. Саме ця архітектурна особливість породжує специфічний клас відмов, відсутній у традиційних технічних системах: поширювані відмови, за яких несправність одного компонента здатна ланцюговим чином вивести з ладу суміжні пристрої та призвести до повного відказу всієї інфраструктури.

Актуальність дослідження надійності IoT-систем визначається кількома взаємопов'язаними чинниками. По-перше, сфери застосування систем розумного будинку невпинно розширюються від побутового комфорту до медичного моніторингу та систем безпеки, де відмова інфраструктури може мати критичні наслідки. По-друге, існуючі методи аналізу надійності імітаційні, марковські та класичні комбінаторні мають суттєві обмеження при застосуванні до великих IoT-систем з динамічною топологією та конкуруючими відмовами: перші дають лише наближені результати, другі страждають від проблеми комбінаторного вибуху простору станів, треті потребують значних обчислювальних ресурсів через необхідність багаторазової генерації та конвертації редукованих дерев відмов. По-третє, зі зростанням кількості підключених пристроїв обчислювальна складність аналізу надійності стає самостійною інженерною проблемою, що вимагає розробки ефективніших алгоритмічних підходів.

Перспективним напрямком вирішення зазначених проблем є застосування методу редукції бінарних діаграм рішень, що поєднує точність аналітичних методів з обчислювальною ефективністю, достатньою для аналізу реальних масштабних IoT-інфраструктур. Дослідження цього методу та оцінювання його ефективності порівняно з існуючими підходами становить предмет даної кваліфікаційної роботи.

Метою кваліфікаційної роботи магістра є зниження часової складності обчислювального процесу аналізу надійності IoT-інфраструктур шляхом застосування методу редукції бінарних діаграм рішень із урахуванням конкуруючих відмов компонентів системи розумного будинку.

Об’єктом дослідження є метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Предметом дослідження є моделі, методи та засоби аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

Для розв’язання поставлених задач використовувалися методи теорії надійності, системного аналізу, теорії графів та множин.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, який відрізняється від відомих застосуванням техніки прямої трансформації вузлів моделі відповідно до станів мережевих шлюзів замість множинної генерації та конвертації скорочених дерев відмов, що дозволило забезпечити зниження часової складності обчислювального процесу.

У кваліфікаційній роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

За темою кваліфікаційної роботи магістра опублікована одна теза доповіді у збірнику наукових праць III (IX) Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «Інформаційні технології: теорія і практика», Харків – Запоріжжя – Дніпро.

1 ВІДОМІ МЕТОДИ АНАЛІЗУ НАДІЙНОСТІ ТА ПРОБЛЕМИ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ПРИ АНАЛІЗІ СКЛАДНИХ ІОТ СИСТЕМ

1.1. IoT-інфраструктура розумного будинку: архітектура, компоненти та протоколи зв’язку

Інфраструктура Інтернету речей у межах розумного будинку являє собою складну кіберфізичну систему, що об’єднує велику кількість гетерогенних пристроїв, мережевих вузлів і програмних сервісів, взаємодія яких спрямована на автоматизацію побутових процесів, підвищення енергоефективності, безпеки та комфорту користувачів. З точки зору аналізу надійності така система характеризується наявністю багаторівневої архітектури, значною кількістю взаємозалежних компонентів та складною структурою обміну даними, що потребує застосування формалізованих методів моделювання, зокрема підходів на основі редукції бінарних діаграм рішень.

Архітектура IoT-інфраструктури розумного будинку, як правило, має ієрархічний характер і включає декілька логічних рівнів, серед яких виділяють рівень сприйняття, мережевий рівень та рівень обробки і сервісів [1-5]. На нижньому рівні розташовані сенсорні та виконавчі пристрої, які забезпечують збір первинної інформації про стан середовища та виконання керуючих дій. До таких пристроїв належать датчики температури, вологості, руху, освітленості, а також актуатори, що реалізують керування освітленням, опаленням або системами безпеки. Ці компоненти характеризуються обмеженими обчислювальними ресурсами та енергоспоживанням, що зумовлює використання енергоефективних протоколів зв’язку та спрощених моделей взаємодії.

Мережевий рівень забезпечує передачу даних між пристроями та їх інтеграцію у єдину систему. У межах розумного будинку він часто реалізується у вигляді бездротових сенсорних мереж, що базуються на технологіях короткого радіусу дії. Центральну роль на цьому рівні відіграють шлюзи, які виконують функції агрегування даних, трансляції між різними протоколами та забезпечення

зв’язку з зовнішніми мережами. Шлюзи виступають критичними компонентами з точки зору надійності, оскільки їх відмова може призвести до втрати доступності значної частини сенсорних вузлів, що формує характерні залежності типу функціональної залежності між компонентами системи. Разом із тим наявність декількох шлюзів у системі може підвищувати її відмовостійкість за рахунок резервування або альтернативних маршрутів передачі даних, однак також ускладнює структуру залежностей між компонентами.

На верхньому рівні архітектури розташовані обчислювальні та сервісні компоненти, які здійснюють обробку даних, прийняття рішень і взаємодію з користувачем. Це можуть бути як локальні обчислювальні вузли (fog або edge computing), так і віддалені хмарні платформи. Вибір між локальною та хмарною обробкою визначається вимогами до затримок, пропускної здатності та надійності системи. У сучасних IoT-інфраструктурах спостерігається тенденція до гібридної організації, коли частина функцій виконується на периферії мережі, що дозволяє зменшити залежність від зовнішніх каналів зв’язку та підвищити загальну відмовостійкість системи. Узагальнена архітектура IoT-інфраструктури наведено на рис. 1.1.

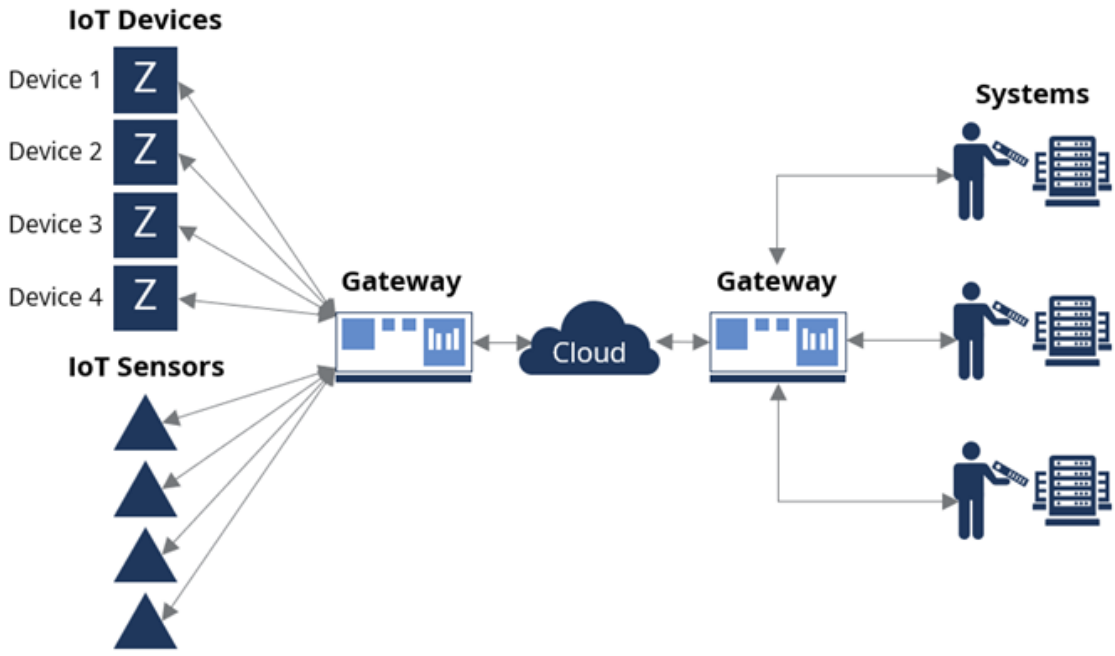


Рисунок 1.1 – Узагальнена архітектура IoT-інфраструктури [1]

Складність IoT-інфраструктури значною мірою визначається різноманіттям використовуваних протоколів зв’язку. На фізичному та канальному рівнях широко застосовуються технології ZigBee, Z-Wave, Bluetooth Low Energy та Wi-Fi, кожна з яких має свої особливості щодо енергоспоживання, дальності передачі та пропускної здатності. На мережевому та транспортному рівнях використовуються протоколи IP-сімейства, зокрема IPv6 та його адаптації для ресурсно обмежених пристроїв. На прикладному рівні поширеними є протоколи MQTT, CoAP та HTTP, які забезпечують обмін повідомленнями між пристроями та сервісами. Вибір конкретного протоколу впливає не лише на продуктивність системи, але й на її надійність, оскільки різні протоколи мають різні механізми підтвердження доставки, повторної передачі та обробки помилок.

У цьому контексті метод аналізу надійності на основі редукції бінарних діаграм рішень є перспективним інструментом для моделювання IoT-інфраструктур. Його застосування дозволяє формалізувати логічну структуру системи у вигляді булевої функції та представити її у компактній графовій формі, що враховує всі можливі комбінації станів компонентів. Редукція діаграми шляхом усунення надлишкових вузлів та об’єднання ізоморфних підграфів забезпечує зменшення обчислювальної складності та робить можливим аналіз систем із великою кількістю елементів. Це є особливо важливим для IoT-інфраструктур розумного будинку, де кількість пристроїв може досягати десятків або сотень, а структура зв’язків між ними є складною та динамічною.

Таким чином, IoT-інфраструктура розумного будинку являє собою багаторівневу, гетерогенну та динамічну систему, аналіз надійності якої потребує врахування як структурних, так і стохастичних аспектів функціонування. Використання методів, заснованих на редукції бінарних діаграм рішень, дозволить реалізувати альтернативне рішення для ефективного моделювати таких систем, забезпечуючи точність оцінювання надійності та можливість подальшого аналізу впливу окремих компонентів на загальну працездатність IoT інфраструктури.

1.2 Класифікація та характеристика відмов в IoT-інфраструктурі розумного будинку

З точки зору аналізу надійності, IoT-інфраструктура розумного будинку характеризується наявністю як незалежних, так і залежних відмов. Незалежні відмови пов'язані з фізичними несправностями окремих пристроїв і є стохастичними подіями, що виникають внаслідок природного зносу елементної бази, виробничих дефектів або випадкових зовнішніх впливів. Кожен такий пристрій – датчик температури, датчик диму, виконавчий механізм має власний закон розподілу часу до відмови, що визначається його конструктивними характеристиками та умовами експлуатації. За відсутності між компонентами будь-яких зв'язків аналіз надійності системи зводився б до порівняно простої задачі агрегування індивідуальних показників надійності відповідно до логічної структури системи [6-8].

Проте реальна IoT-інфраструктура принципово відрізняється від такої ідеалізованої моделі через наявність численних залежностей між компонентами. Залежні відмови виникають внаслідок структурних або функціональних зв'язків між елементами системи. Найбільш поширеним джерелом таких залежностей є архітектурна особливість IoT-мереж: датчики стандартів ZigBee та BLE не можуть функціонувати автономно і потребують постійного підключення до мережі через відповідний шлюз. Ця обставина породжує функціональну залежність між шлюзом і всіма підключеними до нього датчиками – відмова шлюзу автоматично призводить до функціональної ізоляції цілої групи датчиків незалежно від їхнього власного технічного стану. Іншим джерелом залежностей є використання спільного частотного каналу зв'язку: пристрої, що працюють в одному діапазоні, конкурують за доступ до середовища передачі, і деградація каналу внаслідок перешкод негативно впливає на всі вузли мережі одночасно.

Особливе місце в ієрархії відмов займають поширювані відмови, що являють собою якісно відмінний клас несправностей порівняно з незалежними та структурно залежними відмовами. На відміну від останніх, поширювані відмови не

є пасивним наслідком архітектурних зв'язків, а являють собою активний процес поширення шкідливого впливу від несправного вузла на справні компоненти системи. Несправний датчик через збій прошивки або апаратури починає генерувати надмірний трафік у спільному каналі, фізично блокуючи комунікацію інших вузлів зі шлюзом, або передає хибні критичні дані, що ініціюють автоматичні захисні реакції системи і можуть призвести до каскадного збою. Принциповою особливістю поширюваних відмов є те, що їхній системний вплив не визначається лише власними характеристиками несправного компонента, а суттєво залежить від часового співвідношення між моментом виникнення поширюваної відмови та моментом відмови шлюзу, через який вона поширюється. Саме ця часова конкуренція формує стохастичну природу наслідків поширюваної відмови і є центральним об'єктом аналізу в задачах оцінювання надійності IoT-систем.

Сукупність перелічених особливостей, що визначається співіснуванням незалежних і залежних відмов, наявність функціональних залежностей між шлюзами та датчиками, активний характер поширюваних відмов і стохастична природа їхніх наслідків суттєво ускладнює побудову адекватних моделей надійності. Класичні підходи, що не враховують динамічний характер взаємозалежностей між компонентами, дають суттєво завищені або занижені оцінки системної надійності. Це вимагає застосування спеціалізованих методів, здатних ефективно враховувати складні логічні та часові залежності між компонентами, зокрема, комбінаторних методів на основі динамічних дерев відмов і бінарних діаграм рішень, розглянутих у даній роботі.

1.3 Проблеми обчислювальної складності при аналізі надійності складних IoT-систем

Аналіз надійності складних IoT-систем пов’язаний із принциповими труднощами обчислювальної природи, що суттєво обмежують застосовність класичних методів у повному обсязі. Проблема полягає в тому, що масштаб

сучасних IoT-архітектур, які за своєю природою можуть об'єднувати тисячі вузлів, різнорідні протоколи, динамічні топології та адаптивні зв'язки породжує комбінаторний вибух числа кількості станів, які необхідно розглянути в процесі оцінювання.

Метод аналізу видів, наслідків і критичності відмов є систематичним індуктивним підходом, що передбачає поелементний розгляд системи з метою виявлення всіх можливих режимів відмов кожного компонента, визначення їхніх наслідків на вищих рівнях ієрархії та оцінювання критичності кожної відмови за сукупністю критеріїв – імовірністю виникнення, тяжкістю наслідків і можливістю виявлення. Результатом аналізу є структурована таблиця, яка охоплює повний перелік відмов із зазначенням причин, механізмів, ефектів на рівні підсистеми та системи в цілому, а також кількісних показників критичності. Метод орієнтований на превентивне виявлення слабких місць конструкції ще на етапі проектування і широко застосовується в авіаційній, автомобільній та атомній промисловості як обов'язкова складова процесу забезпечення безпеки. Метод аналізу видів, наслідків і критичності відмов передбачає систематичне перебирання всіх можливих режимів відмов для кожного компонента з подальшим простеженням ланцюга наслідків аж до системного рівня. У детермінованих промислових системах із фіксованою структурою та обмеженою кількістю елементів ця процедура є обчислювально реалістичною. Однак в IoT-середовищі кількість компонентів може сягати десятків тисяч, а їхні взаємодії носять нелінійний і часто непередбачуваний характер. Відтак повна таблиця аналізу відмов стає практично нескінченною: якщо система містить n компонентів, кожен із яких має k режимів відмов, загальна кількість комбінацій зростає як $O(k^{\mathrm{n}})$, що робить вичерпний аналіз неможливим без суттєвих спрощень і евристичних апроксимацій.

Іншим відомим класичним методом є метод аналізу дерева відмов. Аналіз дерева відмов є дедуктивним методом, що відштовхується від заздалегідь визначеної небажаної події (вершинної події) і послідовно розкриває логічні комбінації відмов компонентів та зовнішніх впливів, здатних до неї призвести. Модель будується у вигляді спрямованого ациклічного графа, де вузли пов'язані

логічними вентилями типу «І» та «АБО», а листові елементи відповідають базовим подіям із відомими або оціненими імовірностями. Кількісний аналіз дерева дозволяє обчислити імовірність вершинної події, визначити мінімальні перерізи, тобто найменші множини базових відмов, достатніх для реалізації аварії, а також ранжувати компоненти за їхнім внеском у загальний ризик. Таким чином аналіз дерева відмов будується як дедуктивна модель, що відображає логічні умови виникнення небажаної вершинної події через ієрархію логічних вентилів і базових подій. Обчислювальна складність кількісного аналізу такого дерева зростає поліноміально зі збільшенням кількості базових подій, тоді як визначення мінімальних перерізів – множин відмов, достатніх для реалізації вершинної події – є задачею класу NP-важких. У типовій IoT-системі дерево відмов охоплює не лише апаратні компоненти, а й програмне забезпечення, мережеві з'єднання, хмарну інфраструктуру та людський фактор, що призводить до комбінаторного росту числа мінімальних перерізів і катастрофічного збільшення часу обчислення. Додаткову складність вносить динамічна природа IoT-мереж: топологія системи може змінюватися внаслідок підключення чи відключення вузлів, що вимагає повторної побудови та аналізу дерева в режимі реального часу.

Ще одним методом є діаграми причинно-наслідкових зв'язків, що являють собою графічне представлення причинних залежностей між подіями, відмовами та зовнішніми факторами у вигляді орієнтованого графа, де ребра відображають напрямок причинного впливу, а вузли – стани або події системи. На відміну від дерева відмов, яке будується навколо однієї вершинної події, діаграма причинно-наслідкових зв'язків дозволяє моделювати множинні взаємопов'язані події з урахуванням зворотних зв'язків і часових затримок між причиною та наслідком. Діаграми причинно-наслідкових зв'язків дозволяють моделювати складні причинні ланцюги між відмовами, проте при наявності зворотних зв'язків і циклічних залежностей, що є типовими для самоорганізованих IoT-мереж, задача аналізу таких структур зводиться до перевірки виконуваності булевих формул, що є NP-повною задачею. Якщо система включає взаємодію між тисячами агентів, де відмова кожного може зумовлювати відмови суміжних вузлів за нелінійними

законами, то аналітичне вирішення в замкненій формі стає недосяжним, а числові методи вимагають надмірних обчислювальних ресурсів.

Іншим методом є блок-схеми надійності, що заснований на відображенні системи у вигляді мережі функціональних блоків, з'єднаних послідовно або паралельно відповідно до логіки забезпечення виконання цільової функції. Послідовне з'єднання означає, що відмова будь-якого блоку призводить до відмови всієї гілки, тоді як паралельне з'єднання забезпечує резервування – система зберігає працездатність, доки функціонує хоча б один із паралельних блоків. Кожному блоку приписується функція надійності або інтенсивність відмов, а аналітичне або чисельне розв'язання моделі дозволяє отримати показники надійності всієї системи, зокрема імовірність безвідмовної роботи за заданий час, середній час до відмови та коефіцієнт готовності. Метод є інтуїтивно зрозумілим і добре адаптованим до систем із чітко вираженою ієрархічною архітектурою. Таким чином блок-схеми надійності моделюють систему як мережу послідовно і паралельно з'єднаних блоків, де кожен блок характеризується власною функцією надійності. Для простих структур аналітичне обчислення надійності системи здійснюється через стандартні формули, однак IoT-системи, як правило, мають нерегулярну топологію з перехресними залежностями між блоками. В цьому разі точне обчислення надійності системи еквівалентне обчисленню надійності ненадійної мережі – задачі, яка в загальному випадку є P-важкою, тобто складнішою за будь-яку NP-задачу. Алгоритми на основі декомпозиції та умовної незалежності дозволяють знизити складність для окремих класів графів, але не вирішують проблему в загальному випадку.

Принципово важливим аспектом є взаємодія між методами: жоден із розглянутих підходів не є самодостатнім для повного аналізу складної IoT-системи, а їхнє спільне застосування мультиплікує обчислювальні витрати (рис. 1.2). Крім того, IoT-системи характеризуються явищами, що виходять за рамки припущень класичних методів: відмови з загальними причинами, залежні відмови внаслідок поширення збоїв через мережу, а також адаптивна поведінка системи, що змінює власну структуру у відповідь на відмови. Все це перетворює задачу аналізу

надійності IoT-систем на відкриту науково-технічну проблему, розв'язання якої потребує розробки нових наближених алгоритмів, методів машинного навчання та формальних методів верифікації, здатних масштабуватися до реальних розмірів сучасної кіберфізичної інфраструктури.

Рисунок 1.2 – Проблеми обчислювальної складності при аналізі надійності складних IoT-систем

1.4 Відомі методи аналізу надійності IoT-інфраструктур

На сьогодні в науковій спільноті використовуються різні моделі та підходи для опису й аналізу надійності об'єктів, змодельованих як системи. Можна виділити такі якісні підходи до аналізу надійності системи як аналіз видів, наслідків і критичності відмов (FMECA), аналіз дерева відмов (FTA), діаграми причинно-наслідкових зв'язків (CED) та блок-схеми надійності (RBD).

У роботі [9] було запропоновано метод аналізу надійності та оптимального вибору параметрів для комунікації в системах Інтернету речей (IoT) на основі глибокого навчання, спрямований на подолання проблем розрідженості та неоднорідності бездротових зв'язків, а також загроз безпеці даних у масштабних мережах. Автори спочатку побудували багаторівневу глибоку нейронну мережу, яка моделює структуру комунікаційних даних IoT шляхом навчання складних нелінійних функцій: сигнали передаються через взаємопов'язані нейрони з прямим поширенням, де вхідні дані множаться на ваги, сумуються та трансформуються функцією активації ReLU в прихованих шарах для ефективної обробки високорозмірних розріджених даних і стабільного поширення градієнтів, а на виході застосовується Softmax для отримання ймовірнісних прогнозів мережевих значень. Це забезпечує багатовимірний опис бездротових каналів з автономним вилученням ознак на рівні керування сигналами та даних. Далі, з використанням аналітичного ієрархічного процесу (AHP), було сконструйовано автоенкодер глибокого навчання, який витягує ключові елементи параметрів надійності мережі з набору даних IoT, оптимізує відображення між індикаторами через функції перетворення та втрати, обчислює загальний індекс надійності μ як зважену комбінацію суб'єктивних і об'єктивних ваг та здійснює автоматичне кодування для оцінки взаємозв'язків. Експериментальна перевірка проводилася в реальному локальному середовищі з джерелом живлення JM-5A та фотоелементом для ідентифікації параметрів, де запропоновану модель порівнювали з традиційною розподіленою системою за різних напруг, ураховуючи валідні й невалідні дані.

У роботі [10] було запропоновано комплексний фреймворк для моделювання та аналізу надійності систем Інтернету речей на основі діаграм надійності блоків (Reliability Block Diagrams, RBD), спрямований на подолання фрагментарності існуючих підходів, які зосереджувалися лише на окремих підсистемах (WSN, хмара тощо), ігноруючи гетерогенність та взаємодію всіх рівнів IoT-архітектури. Автори розробили п'ятирівневу архітектуру IoT, незалежну від конкретних вендорів, зокрема пропонована ними архітектура включала такі рівні як рівень сприйняття з сенсорами, актуаторами та розумними пристроями; рівень доступу з

короткодіючими та зовнішніми мережами; рівень ядра з маршрутизацією через автономні системи; рівень проміжного ПЗ для забезпечення інтероперабельності та обробки даних; рівень додатків з бізнес-логікою та інтерфейсами. Кожен рівень моделюється як ієрархічна структура RBD з використанням базових конфігурацій: послідовної (серійної), паралельної, k-із-n та їх комбінацій. Запропоновано ітеративний набір кроків для розгортання фреймворку: знизу вгору, з послідовною декомпозицією рівнів до нерозкладних блоків.

У роботі [11] було запропоновано підхід до моделювання та аналізу надійності віртуальних дата-центрів у середовищі хмарних обчислень, з акцентом на оцінку впливу консолідації ресурсів на надійність та доступність систем. Автори розробили модель, що враховує особливості віртуалізації в хмарних дата-центрах, де багато віртуальних машин (ВМ) розміщуються на обмеженій кількості фізичних серверів. Основна увага приділяється аналізу залежності між рівнем консолідації (співвідношенням кількості ВМ до фізичних ресурсів) та показниками надійності системи. Моделювання охоплювало як апаратні, так і програмні аспекти відмов, включаючи вплив навантаження на фізичні вузли, віртуалізаційні шари та взаємодію між ВМ. Для оцінки надійності застосовується комбінація аналітичних методів, що дозволило кількісно описати ймовірність безвідмовної роботи та доступності в умовах динамічного розподілу ресурсів. Зокрема авторами було створено гібридну модель, що поєднувала діаграми надійності блоків та стохастичні Петрі мережі. Це дозволило досить детально моделювати динамічні аспекти поведінки системи віртуальних дата-центрів, які важко або неможливо адекватно описати лише статичними моделями (наприклад, конкуренцію за ресурси, черги, відновлення після відмов, залежності між компонентами в умовах віртуалізації та динамічного розподілу навантаження). У цій гібридній моделі блок-схеми надійності використовувались для представлення статичної структури надійності (послідовні/паралельні зв’язки компонентів), тоді як мережі Петрі доповнювали модель динамікою: переходи з затримками (експоненціальними та негайними), маркування, що відображали стани системи, та можливість врахування стохастичних процесів відмов і відновлення.

У роботі [12] було запропоновано ієрархічний фреймворк моделювання та аналізу для кількісної оцінки доступності та безпеки IoT-інфраструктур, що інтегрують парадигми хмарних (cloud), туманних (fog) та крайових (edge) обчислень, з метою подолання складності гетерогенних архітектур і врахування як архітектурних, так і операційних деталей у єдиній моделі. Автори розробили трирівневу ієрархічну модель: на верхньому рівні застосовується діаграма надійності блоків, яка відображає загальну архітектуру інфраструктури та зв'язки між основними член-системами (cloud, fog, edge) у послідовній або комбінованій конфігурації; на середньому рівні – дерева відмов, що деталізують причини відмов кожної член-системи за допомогою логічних вентилів (OR для будь-якої відмови, AND для всіх тощо); на нижньому рівні – неперервні ланцюги Маркова в часі, які моделюють детальні операційні стани та переходи підсистем, включаючи апаратні (двостанові), програмні (багатостанові з урахуванням старіння, розслідування, відновлення, кібератак) та процеси відновлення з затримками виклику ремонтника, виявлення та часткового/повного ремонту. Процес роботи фреймворку складається з трьох фаз: (1) визначення вимог – аналіз архітектури, операційної поведінки, збір параметрів (частоти відмов, часів відновлення, коефіцієнтів покриття, інтенсивності атак); (2) моделювання – побудова ієрархічної моделі знизу вгору з декомпозицією підсистем; (3) аналіз – розв'язання моделі знизу вгору (CTMC – FT – RBD). Валідація проводилася на кейс-стаді IoT-інфраструктури розумної фабрики з типовими підсистемами (сервери, віртуальні машини, ОС, шлюзи, сенсори, сховища), використовуючи параметри з літератури та практики.

У статті [13] було запропоновано метод аналізу надійності комунікаційної системи широкозонного захисту у електроенергетичних мережах, з акцентом на характеристики структури та кількісну оцінку показників надійності для волоконно-оптичних мереж, що широко застосовуються в таких системах. Автори проаналізували особливості архітектури комунікаційної системи широкозонного захисту, розділивши її на підсистеми: систему захисту, підсистему комунікації та інші ключові компоненти, враховуючи специфіку передачі сигналів у реальному часі, вимоги до низької затримки та високої стійкості до відмов у критичних

релейних застосуваннях. Основну увагу приділено волоконно-оптичним кільцевим мережам, які є типовими для забезпечення резервування та надійного з'єднання між підстанціями. Для моделювання надійності використано діаграми надійності блоків для представлення структури підсистем у послідовних, паралельних або комбінованих конфігураціях. Додатково застосовуються байєсівські мережі для врахування залежностей між компонентами, оновлення ймовірностей відмов на основі умовних залежностей та інтеграції експертних оцінок з емпіричними даними. Це дозволяє моделювати як незалежні, так і корельовані відмови, а також оцінювати вплив різних факторів (апаратні збої, помилки передачі, пошкодження кабелю) на загальну надійність системи. Процес аналізу включав побудову моделі для кожної підсистеми окремо, обчислення показників надійності (ймовірність безвідмовної роботи, середній час між відмовами, доступність) з використанням експоненціального розподілу часу безвідмовної роботи, а потім агрегацію в загальну модель системи. Таким чином у даній роботі байєсівські мережі забезпечували гнучкість для сценаріїв з неповними даними та оновлення ймовірностей у разі появи нової інформації про відмови.

У ще одній роботі [14] було запропоновано метод оцінки надійності систем дистанційного моніторингу на базі Інтернету речей для низьковольтних повітряних ліній електропередач (OTPL, 0.4 кВ), спрямований на підвищення стабільності розподілу електроенергії, зменшення втрат, виявлення несанкціонованих підключень та пошкоджень ліній шляхом безперервного реального часу моніторингу параметрів (напруга, струм, температура). Автори розробили архітектуру IoT-системи з бездротовими сенсорними мережами, де давачі (ZMPT101b для напруги, SCT024T для струму, DS18B20 для температури) встановлюються на фазових проводах, передають дані за допомогою ZigBee (обрано за низьке енергоспоживання, стійкість до електромагнітних перешкод, дальність до 200 м) у топології шини з послідовним стрибковим режимом для довгих ліній (до 40 терміналів на концентратор). Дані обробляються мікроконтролером (авторами було обрано Arduino MEGA), передаються через концентратор з модулем A9G до центру моніторингу за допомогою веб-інтерфейсу.

Живлення забезпечується літій-іонними акумуляторами з перетворювачами для стійкості до відмов. Для оцінки надійності застосовується модель невідновлюваної системи з експоненціальним розподілом часу безвідмовної роботи, де ймовірність безвідмовної роботи обчислюється як добуток надійностей компонентів (апаратна та програмна частини сенсорів і концентраторів) з постійною інтенсивністю відмов λ. Розглядались послідовні та паралельні конфігурації: у послідовній відмова будь-якого елемента виводить систему з ладу; у паралельній резервування дозволяє підтримувати функціональність навіть при відмові одного сенсора (в межах 3-сенсорного діапазону поширення). За результатами експериментів порівнювались дві моделі: Model A (більше концентраторів, нижча щільність) та Model B (менше концентраторів, вища надійність завдяки оптимізованому розміщенню та резервуванню.

У роботі [15] запропоновано підхід до комплексної оцінки енергоефективності комунікаційних протоколів в IoT/IIoT-системах, де надмірне енергоспоживання розглядається як один із ключових факторів, що обмежує тривалість функціонування віддалених сенсорних вузлів. Автори підкреслюють, що витрати енергії на радіопередачу значно перевищують витрати на збір даних або локальну обробку, що зумовлює необхідність оптимізації саме комунікаційного рівня. При цьому надійність передачі даних розглядається як критично важливий параметр, оскільки зниження енергоспоживання не повинно призводити до втрати цілісності даних або зростання ймовірності відмов у мережі. Методологія дослідження базується на поєднанні трьох підходів: лабораторних вимірювань на фізичному обладнанні, профілювання одноплатних комп’ютерів, а також моделювання в середовищі COOJA/Powertrace. У межах роботи розроблено Unified Comparative Method, який використовує білінійну інтерполяцію та зважену нормалізацію. У контексті аналізу надійності цей метод дозволяє агрегувати різнорідні показники (ймовірність втрат пакетів, затримки, стабільність з’єднання) в єдину узагальнену метрику, придатну для порівняння протоколів. Надійність отриманих результатів підтверджено високим коефіцієнтом рангової кореляції

Спірмена (понад 0,9), що свідчить про узгодженість оцінок і стійкість запропонованого підходу.

Проведений аналіз відомих методів оцінювання надійності IoT-інфраструктур показав, що існуючі підходи еволюціонують від класичних статичних моделей, таких як діаграми надійності блоків, аналіз дерева відмов та аналіз видів, наслідків і критичності відмов, до складних гібридних і інтелектуальних методів, що поєднують аналітичне моделювання, стохастичні процеси та алгоритми машинного навчання [16]. Традиційні методи забезпечують наочність і відносну простоту розрахунків, однак обмежені у відображенні динаміки, взаємозалежностей і гетерогенності компонентів IoT-систем, тоді як сучасні підходи, зокрема ієрархічні моделі, комбінації RBD із мережами Петрі, марковськими процесами та байєсівськими мережами, дозволяють більш адекватно враховувати багаторівневу архітектуру, процеси відмов і відновлення, а також невизначеність середовища функціонування. Додатково, використання методів глибокого навчання та емпірично-аналітичних підходів відкриває можливості для автоматизованого вилучення ознак, адаптивної оцінки параметрів і комплексного врахування таких факторів, як енергоефективність і якість передачі даних (таблиця 1.1).

Разом із тим варто відзначити, що досліджуванні методи повною мірою не забезпечують одночасно високу точність, масштабованість і обчислювальну ефективність для складних багаторівневих IoT-систем. Зокрема, традиційні методи є обмеженими у відображенні залежностей між компонентами та динаміки процесів відмов і відновлення, тоді як більш складні підходи, такі як марковські моделі, мережі Петрі чи глибоке навчання, характеризуються високою обчислювальною складністю, проблемами масштабування та залежністю від значних обсягів вхідних даних. Крім того, існуючі методи часто не забезпечують ефективної редукції станового простору моделі, що є критичним для аналізу великих IoT-інфраструктур із численними взаємозалежними елементами.

Таблиця 1.1 – Порівняльний аналіз відомих методів оцінки надійності IoT інфраструктур

№	Метод / підхід	Тип моделі	Рівень застосування	Що моделює	Переваги	Недоліки	Особливості застосування
1	DL + AHP + Autoencoder [9]	ML	Комунікаційний	Нелінійні залежності	Точність	Складність	Оптимізація каналів
2	RBD-фреймворк (5 рівнів) [10]	Ієрархічний	IoT архітектура	Взаємодію рівнів	Масштабованість	Статичність	End-to-end
3	RBD + стохастичні мережі Петрі [11]	Гібридний	Хмара	Динаміка системи	Деталізація	Складність	Віртуалізація
4	RBD + FTA + CTMC [12]	Стохастичний	Cloud–Fog–Edge	Архітектура+ поведінка	Точність	Складність	CPS
5	RBD + Байєсівські мережі [13]	Ймовірнісний	Мережі	Залежні відмови	Гнучкість	Дані	Smart Grid
6	Експоненціальний [14]	Аналітичний	WSN	Ймовірність відмов	Простота	Неточність	ZigBee
7	Unified Comparative Method [15]	Емпіричний	Протоколи	Якість+енергія	Комплексність	Залежність від експериментів	IoT протоколи

У зв’язку з цим актуальною є розробка нового методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

1.5 Постановка задачі

Аналіз сучасного стану проблеми показав, що швидке зростання кількості пристроїв у IoT-інфраструктурах розумного будинку супроводжується суттєвим підвищенням ризику поширення відмов через спільне безпровідне середовище передачі даних. Існуючі методи оцінки надійності (аналіз видів, наслідків і критичності відмов, аналіз дерева відмов, діаграми причинно-наслідкових зв’язків, блок-схеми надійності) не забезпечують ефективного розв’язання задачі через експоненціальне зростання обчислювальної складності при врахуванні конкуруючих відмов і динамічної топології мережі. Це зумовлює необхідність створення нового підходу, який дозволить точно оцінювати надійність великих IoT-систем з урахуванням механізмів поширення відмов.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати архітектуру, основні компоненти та протоколи зв’язку IoT-інфраструктури розумного будинку, а також провести класифікацію та характеристику можливих відмов у такій інфраструктурі;

– дослідити механізм поширення відмов у безпровідних IoT-мережах, концепцію конкуруючих відмов та часову конкуренцію подій;

– узагальнити відомі методи аналізу надійності технічних систем та виявити їхні обмеження щодо застосування до складних IoT-інфраструктур;

– розробити метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень;

– теоретично оцінити обчислювальну складність запропонованого методу та порівняти її з класичними підходами;

– провести теоретичне дослідження ефективності розробленого методу аналізу надійності IoT-інфраструктури.

2 ПРОЦЕС ПОШИРЕННЯ ВІДМОВ В ІОТ-ІНФРАСТРУКТУРІ ТА МЕТОД ОЦІНЮВАННЯ НАДІЙНОСТІ ЗА ДОПОМОГОЮ БІНАРНИХ ДІАГРАМ РІШЕНЬ

2.1. Загальна характеристика механізму поширення відмов в IoT-інфраструктурі та концепція конкуруючих відмов

Функціонування сучасних інфраструктур Інтернету речей (IoT) характеризується високим ступенем інтеграції та використанням спільних мережевих ресурсів, де центральним елементом архітектури виступає мережевий шлюз (рис. 2.1). Цей вузол забезпечує агрегацію даних від численних сенсорних пристроїв, що працюють на базі енергоефективних протоколів зв’язку, таких як ZigBee або Bluetooth Low Energy, та їх подальшу трансляцію до хмарних платформ. Така ієрархічна побудова зумовлює виникнення складної системи функціональних залежностей, де працездатність кінцевих точок детермінується станом комунікаційного хаба. Зазначена архітектурна особливість ініціює специфічні механізми деградації системи, за яких локальна несправність одного вузла здатна трансформуватися у системний збій через каскадне поширення відмов на суміжні компоненти.

Процеси поширення відмов у таких мережах мають подвійну природу, охоплюючи як зовнішні деструктивні впливи, так і внутрішні деградаційні явища. Зокрема, цілеспрямовані кібератаки, спрямовані на порушення доступності середовища передачі даних, наприклад, атаки типу «глушіння» (jamming attacks), створюють зони радіочастотних завад, що паралізують роботу всього сегмента мережі. Паралельно з цим, внутрішні апаратні несправності або критичні програмні помилки в окремих сенсорах можуть генерувати аномальний мережевий трафік або електричні перенавантаження, що призводить до аналогічних наслідків для всієї інфраструктури.

Ключовою ознакою цих сценаріїв є перехід від локалізованої відмови пристрою до системної дисфункції, що зумовлено високим ступенем взаємозалежності компонентів. В умовах такої взаємодії виникає явище часової

конкуренції між механізмом поширення відмови від сенсора та механізмом ізоляції через відмову шлюзу. У випадках, коли шлюз виходить з ладу раніше, ніж деструктивний вплив сенсора поширеться на решту мережі, відбувається ефект ізоляції, який, попри локальну втрату зв'язку, запобігає повному руйнуванню системної логіки. Таким чином, надійність сучасних IoT-інфраструктур визначається не лише сукупною імовірністю відмови окремих елементів, а й складною стохастичною динамікою взаємодії між локальними та поширеними механізмами відмов у межах спільного мережевого середовища.

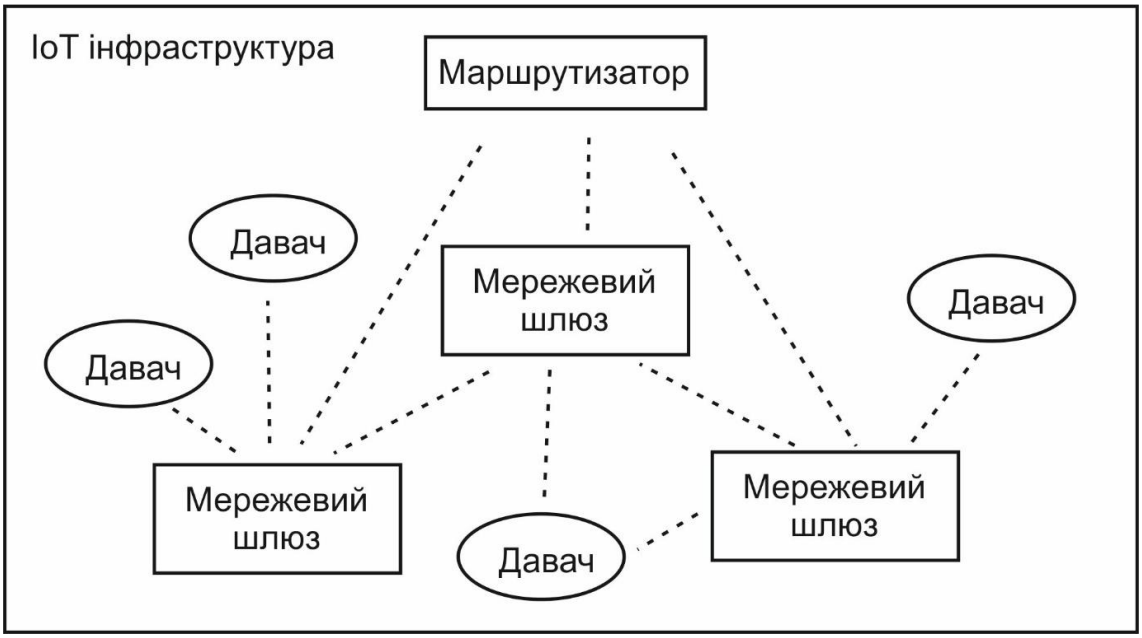


Рисунок 2.1 – Типова IoT-інфраструктура із декількома мережевими шлюзами

Для подальшого опису і формалізації процесу поширення відмов в якості IoT-системи будемо розглядати систему розумного будинку, що дозволяє чітко змоделювати складні функціональні залежності між мережевими шлюзами та кінцевими пристроями, а також здійснити їх практичну верифікацію.

З формальної точки зору, IoT-систему розумного будинку можна представити як множину компонентів $S = \{s_1, s_2, \ldots, s_n, g_1, g_2, \ldots, g_m\}$, де s_i – датчики (i = 1, …, n), а g_j – мережеві шлюзи (j = 1, …, m). Кожен датчик s_i підключений до шлюзу $g_j(i)$, через який здійснюється його взаємодія з мережею.

Відповідно до прийнятої класифікації, для кожного датчика s_i можна виділити два типи відмов – локальну відмову S_i^l та поширювану відмову S_i^p. Локальна відмова S_i^l спричиняє виведення з ладу виключно самого датчика s_i і не впливає на стан інших компонентів. Поширювана відмова S_i^p, натомість, здатна призвести до порушення функціонування суміжних вузлів і, в граничному випадку, до відмови всієї IoT системи. Тому надалі визначимо саме цей тип відмов як цільовий і досліджуваний у цій роботі.

2.2. Фізичний механізм поширення через спільне середовище передачі у безпровідних мережах

Перший ключовий механізм поширення відмов має фізичну природу і реалізується через засмічення спільного радіоканалу. Несправний датчик внаслідок внутрішнього збою електроніки або помилки у прошивці починає безперервно генерувати високочастотні радіосигнали або передавати нескінченний потік некоректних даних у спільний канал зв'язку – ZigBee, BLE або Wi-Fi. Оскільки зазначені протоколи використовують спільні частотні діапазони, такий «шумовий» потік від одного вузла фізично блокує можливість інших датчиків встановити зв'язок зі шлюзом. Несправність при цьому залишається локалізованою на апаратному рівні, проте її наслідки поширюються на всю систему: робочий шлюз або продовжує обробляти цей потік даних, або повністю втрачає зв'язок з іншими справними компонентами через зашумленість ефіру.

Інтенсивність деградації каналу зв'язку внаслідок такої відмови може бути описана через відношення сигнал/шум (SNR). Нехай P_s – потужність корисного сигналу, а P_n – потужність шумового сигналу від несправного вузла. Тоді SNR визначається як:

$$SNR = 10 \cdot log_{10}(P_s / P_n) \quad (2.1)$$

де значення $SNR < SNR_{min}$ вказує на деградацію каналу нижче за допустимий поріг, при якому нормальна передача даних стає неможливою. Таким чином, умова поширення фізичної відмови на j-й датчик можна сформулювати наступним чином:

$$SNR_j(t) < SNR_{min} \text{при } P_n(t) > P_s \cdot 10^{(-SNR_{min}/10)} \quad (2.2)$$

де $SNR_j(t)$ – поточне значення відношення сигнал/шум для j-го датчика в момент часу t.

Другий сценарій поширення несправності в IoT-інфраструктурі має виражену логічну природу і реалізується через механізм каскадної відмови, що виникає внаслідок деградації інформаційної достовірності даних (рис. 2.2). У цьому випадку дефект сенсорного елемента або програмний збій призводять не до припинення передачі сигналу, а до генерації аномальних критичних показників, які помилково інтерпретуються системою як реальні загрози, наприклад, витік газу або загоряння. Оскільки сучасні інтелектуальні платформи управління побудовані на принципах автоматичного реагування, такий хибний сигнал через мережевий шлюз ініціює ланцюгову реакцію в межах усієї екосистеми розумного будинку.

Внаслідок активації детермінованих алгоритмів безпеки відбувається запуск виконавчих механізмів, таких як системи пожежогасіння, аварійна вентиляція або блокування входів, що призводить до нецільового використання ресурсів та переведення суміжних датчиків у режим підвищеного енергоспоживання або специфічні стани моніторингу. Такий каскадний ефект трансформує локальну похибку одного сенсора у масштабну системну дисфункцію, де порушення логіки функціонування охоплює множину вузлів, які самі по собі є апаратно справними. Це підкреслює критичну роль мережевого шлюзу як вузла, що забезпечує трансляцію деструктивного логічного впливу, та обумовлює необхідність

врахування подібних сценаріїв при моделюванні надійності інтелектуальних систем із високим рівнем автономності.

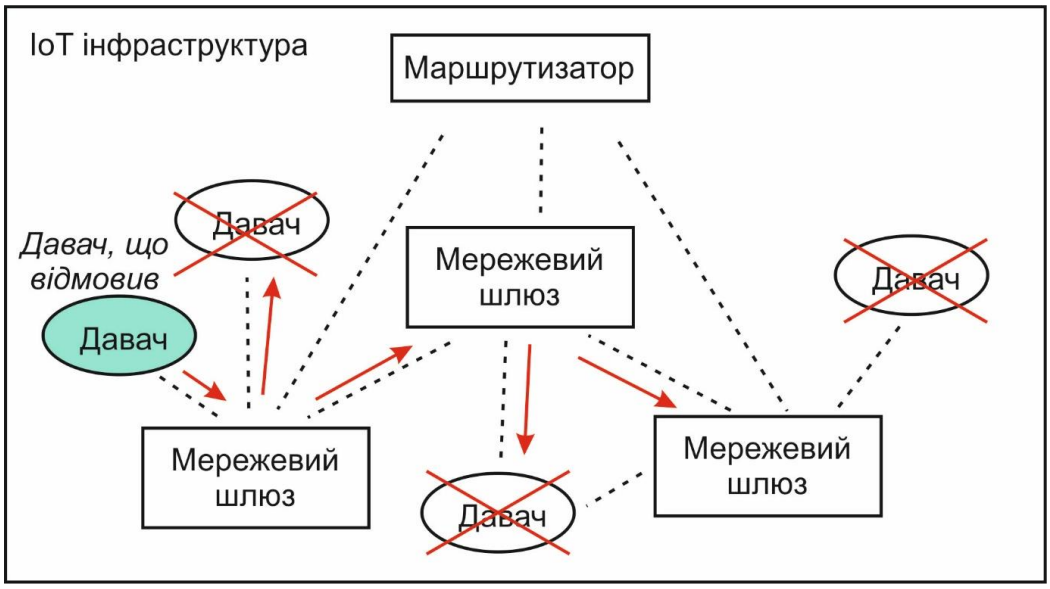


Рисунок 2.2 – Відмова IoT-мережі внаслідок трансляції некоректних даних від давача

Такий сценарій може призвести до перевантаження мережі або хибної активації захисних протоколів у всій системі розумного будинку, викликаючи системний збій. У подібних випадках шлюз виступає мимовільним «транслятором» відмови, тобто доки він функціонує в штатному режимі, він ретранслює шкідливий вплив від несправного датчика на інші компоненти системи.

Таким чином ймовірність того, що поширювана відмова датчика s_i досягне датчика s_j через спільний шлюз, описується умовною ймовірністю:

$$P\left(S_k^p \middle| S_i^p, g_j \text{ працює}\right) = P(S_i^p \to g_i \to S_k) \tag{2.3}$$

де S_k^p позначає поширювану відмову датчика s_j; S_i^p – поширювану відмову датчика s_i; операто → позначає передачу шкідливого впливу через зазначений вузол.

Загальна ймовірність відмови всієї системи внаслідок поширюваної відмови датчика s_i тоді визначається як:

$$P\left(F_{sys}\middle|S_i^p, g_j \text{ працює}\right) = 1 \quad (2.4)$$

де F_{sys} – подія повної (системної) відмови всієї IoT-інфраструктури.

Математичні вирази 2.3 та 2.4 чітко показують, що мережевий шлюз у системі IoT відіграє роль «містка» для передачі несправностей. Якщо шлюз залишається у робочому стані під час збою одного з датчиків, він фактично дозволяє шкідливому впливу поширитися на інші компоненти мережі. Згідно з формулою 2.4, така ситуація неминуче призводить до повної відмови всієї системи, оскільки справний шлюз забезпечує логічний зв'язок, необхідний для каскадного руйнування інфраструктури.

Це створює специфічну ситуацію: робота шлюзу, яка зазвичай є необхідною для функціонування будинку, під час атаки або критичного збою стає головною загрозою. Таким чином, надійність системи залежить від результату «змагання» у часі: якщо шлюз вийде з ладу раніше, ніж помилка встигне поширитися далі, він розірве ланцюг і врятує систему від повного краху. Отже, у контексті таких відмов власна поломка шлюзу парадоксальним чином виступає захисним механізмом, що ізолює загрозу.

2.3. Концепція конкуруючих відмов та часова конкуренція

Аналіз механізмів поширення несправностей у складних IoT-системах дозволяє сформулювати концепцію конкуруючих відмов, яка базується на динамічній взаємодії між локальною відмовою мережевого шлюзу та поширюваними відмовами підключених до нього сенсорних пристроїв. Це явище визначається як стохастична часова конкуренція, де результат функціонування всієї інфраструктури безпосередньо залежить від того, яка з цих подій настане раніше в часовій області. Оскільки шлюз є єдиною точкою входу для групи давачів

у глобальну мережу, його власна відмова, попри негативний вплив на доступність даних, одночасно виконує роль механізму захисної ізоляції.

Зокрема, якщо локальна відмова шлюзу виникає раніше, ніж поширювана відмова сенсора встигає активуватися, деструктивний вплив залишається локалізованим у межах ізольованого сегмента, що запобігає каскадному руйнуванню всієї IoT-платформи. У протилежному випадку, коли поширювана відмова датчика (наприклад, активна атака типу jamming або помилковий аварійний сигнал) ініціюється до моменту виходу шлюзу з ладу, справна комунікаційна інфраструктура забезпечує швидку трансляцію цього впливу на суміжні вузли, що неминуче призводить до системного збою (рис. 2.3).

Таким чином, моделювання надійності таких систем потребує переходу від статичного аналізу до динамічного дослідження конкуренції імовірнісних розподілів часу до відмови. У цій концепції кожна подія розглядається не ізольовано, а в контексті її здатності змінити топологію системи та логіку взаємозв'язків між її компонентами, де швидкість реакції захисних механізмів (ізоляції) є визначальним фактором виживання інфраструктури.

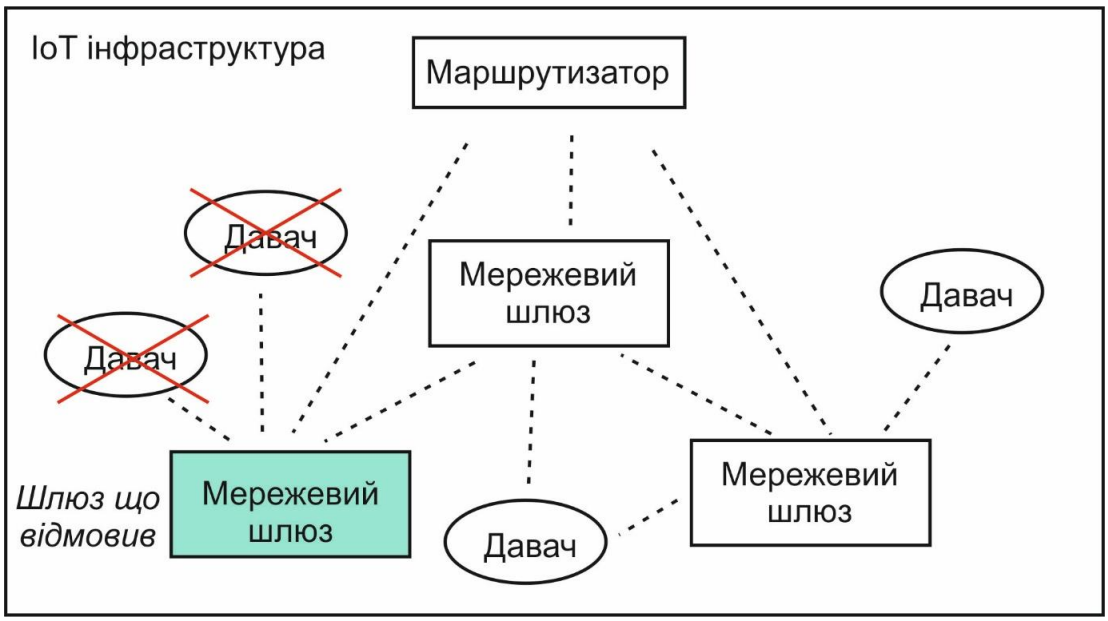


Рисунок 2.3 – Відмова частини IoT-мережі внаслідок несправності мережевого шлюзу

Нехай T^G – випадковий момент відмови шлюзу g_i, а $T_{S_i^p}$ – випадковий момент виникнення поширюваної відмови датчика s_i, підключеного до цього шлюзу. Конкуренція між цими двома подіями визначає, чи буде поширена відмова ізольована, чи призведе до системного збою. Визначимо два сценарії.

Сценарій 1 – ізоляція відмови. Якщо шлюз відмовляє раніше, ніж виникає поширена відмова датчика ($T^G < T_{S_i^p}$), то поширена відмова ізолюється і не передається на інші компоненти системи. Умова ізоляції:

$$T^G < T_{S_i^p} \Rightarrow P(F_{sys}|T^G < T_{S_i^p}) < P(F_{sys}|T^G \geq T_{S_i^p}) \tag{2.5}$$

Другий сценарій – поширення відмови: якщо $T_{S_i^p} < T^G$, тобто поширювана відмова датчика виникає раніше за відмову шлюзу, то несправний датчик встигає передати шкідливий вплив через ще справний шлюз на інші компоненти, що призводить до системної відмови:

$$T_{S_i^p} < T^G \Rightarrow P(F_{sys}|\, T_{S_i^p} < T^G) = 1 \tag{2.6}$$

Ймовірність того, що поширювана відмова датчика s_i, виникне раніше відмови шлюзу g_j, обчислюється через сумісний розподіл їхніх часів до відмови:

$$P\left(S_i^p \to G_j\right) = \int_0^T \int_{\tau 1}^T f_{S_i^p}(\tau 1)\, f_{G_i}(\tau 2)\, d\tau 1\, d\tau 2 \tag{2.7}$$

де $f_{S_i^p}(\tau 1)$ – щільність розподілу часу до поширюваної відмови датчика s_i, $f_{G_i}(\tau 2)$ – щільність розподілу часу до відмови шлюзу g_j, T – заданий час місії системи.

Таким чином, загальна ненадійність IoT-системи з урахуванням конкуруючих відмов для m шлюзів визначається за формулою повної ймовірності [18-24]:

$$UR(t) = \sum_{i=1}^{2^m} [P(F_{sys}|R_{1,i}) \cdot P(R_{1,i}) + P(R_{2,i})] \quad (2.8)$$

де $R_{1,i}$ – подія ізоляції всіх поширених відмов за умови настання i-ї конфігурації стану шлюзів, $R_{2,i}$ – подія, за якої принаймні одна поширена відмова не ізолюється і призводить до системної відмови, 2^m – загальна кількість можливих конфігурацій стану m шлюзів.

Таким чином дана формула обчислює сумарну ймовірність того, що вся система повністю відмовить до заданого моменту часу t. Вона враховує всі можливі стани шлюзів – від ситуації, коли всі шлюзи ще працюють, до випадків, коли відмовили окремі шлюзи або навіть усі вони одночасно. Кількість таких станів дорівнює 2^m, оскільки кожен шлюз незалежно може бути або справним, або відмовленим. Фактично вона підсумовує внесок усіх «небезпечних» сценаріїв, у яких хоча б один шлюз залишився робочим достатньо довго, щоб пропустити поширену відмову датчика, і саме через ці сценарії накопичується основна частина загальної ненадійності системи.

Для кожного з цих 2^m можливих станів (конфігурацій) формула розглядає два взаємовиключні сценарії:

1. Усі поширені відмови датчиків виявилися ізольованими (тобто жодна з них не встигла пройти через ще робочий шлюз і спричинити каскадний збій). У такому разі ймовірність повного відказу системи в цій конфігурації зазвичай дуже мала або дорівнює нулю.

2. Принаймні одна поширена відмова не була ізольована, тобто встигла пройти через справний шлюз і запустити ланцюгову реакцію, що призводить до відмови всієї системи. У цьому випадку ймовірність повного системного збою вважається рівною одиниці.

Такий підхід дозволяє явно розмежувати внесок механізмів ізоляції та поширення відмов у загальну ненадійність системи. Для підвищення надійності

необхідно мінімізувати ймовірність подій типу $R_{2,i}$ шляхом своєчасного виявлення та ізоляції несправних вузлів.

2.4 Метод оцінювання надійності за допомогою бінарних діаграм рішень

Одним із сучасних методів аналізу надійності складних технічних систем є використання бінарних діаграм рішень – БДР. Даний підхід ґрунтується на представленні структурної функції системи у вигляді орієнтованого ациклічного графа, що дозволяє ефективно моделювати логічні залежності між окремими компонентами системи та визначати ймовірність її працездатності. Метод БДР широко застосовується для дослідження надійності електронних схем, інформаційно-комунікаційних мереж, систем керування та розподілених систем, зокрема архітектур Інтернету речей.

Основою методу є представлення структури системи через булеву функцію, яка описує залежність між станами окремих компонентів та загальним станом системи. Нехай система складається з n елементів, кожен з яких може перебувати у двох станах: працездатному або відмовному. Для кожного елемента вводиться бінарна змінна x_i, де $x_i = 1$ означає, що елемент функціонує, а $x_i = 0$ означає його відмову. Тоді структурна функція системи може бути представлена у вигляді булевої функції:

$$\varphi(x_1, x_2, \dots, x_n) \tag{2.9}$$

Відповідно, якщо значення функції дорівнює 1, якщо система перебуває у працездатному стані, та 0 у випадку відмови системи.

Бінарна діаграма рішень являє собою спеціалізоване графічне представлення такої булевої функції. Формально БДР визначається як орієнтований ациклічний граф $G = (V, E)$, де множина вершин V складається з внутрішніх вузлів та двох термінальних вузлів, що відповідають логічним значенням 0 та 1. Кожен внутрішній вузол відповідає одній бінарній змінній системи та має дві вихідні дуги,

які відповідають двом можливим значенням цієї змінної. Перша дуга, що зазвичай позначається як 0-гілка, відповідає випадку відмови компонента, а друга дуга, позначена як 1-гілка, відповідає працездатному стану елемента.

Побудова БДР здійснюється шляхом послідовного розкладу булевої функції за змінними. Для цього використовується правило Шеннона, згідно з яким будь-яка булева функція може бути представлена у вигляді

$$\varphi(x_1, x_2, \dots, x_n) = x_i \cdot \varphi_{x_i=1} + \overline{x_i} \cdot \varphi_{x_i=0} \tag{2.10}$$

де $\varphi_{x_i=1}$ та $\varphi_{x_i=0}$ є підфункціями, отриманими шляхом підстановки відповідно $x_i = 1$ та $x_i = 0$. Застосовуючи це розкладання рекурсивно до всіх змінних, можна побудувати дерево рішень, яке відображає всі можливі комбінації станів елементів системи. Подальша оптимізація цього дерева шляхом об'єднання однакових підграфів та видалення надлишкових вузлів приводить до утворення скороченої впорядкованої бінарної діаграми рішень, яка забезпечує компактне представлення функції.

Для задач аналізу надійності БДР дозволяє визначати ймовірність працездатного стану системи на основі ймовірностей працездатності окремих компонентів. Нехай R_i позначає ймовірність безвідмовної роботи i-го елемента системи. Тоді ймовірність відмови елемента дорівнює $Q_i = 1 - R_i$. Під час аналізу БДР кожен шлях від кореневого вузла до термінального вузла зі значенням 1 відповідає одній з комбінацій станів елементів, за яких система залишається працездатною. Ймовірність такого шляху визначається як добуток ймовірностей відповідних станів компонентів [25-28]. Якщо шлях містить множину змінних S, для яких $x_i = 1$, та множину F, для яких $x_i = 0$, тоді ймовірність відповідної комбінації обчислюється як:

$$P = \prod_{i=S} R_i \cdot \prod_{j=F} (1 - R_j) \tag{2.11}$$

Загальна ймовірність працездатності системи визначається сумуванням імовірностей усіх шляхів, що ведуть до термінального вузла зі значенням 1:

$$R_{sys} = \sum_{k=1}^{m} P_k \tag{2.12}$$

де m – кількість працездатних шляхів у бінарній діаграмі рішень, а P_k – ймовірність k-го шляху.

Застосування БДР у задачах оцінювання надійності має низку важливих переваг. По-перше, метод забезпечує компактне представлення складних логічних функцій завдяки усуненню повторюваних підструктур у графі. По-друге, БДР дозволяє ефективно виконувати точні обчислення ймовірностей працездатності навіть для систем з великою кількістю компонентів. По-третє, графова структура діаграми дає можливість легко виконувати різноманітні операції аналізу, зокрема визначення мінімальних шляхів працездатності, аналіз чутливості системи до відмов окремих елементів та оцінювання впливу резервування.

Особливо ефективним є застосування методу БДР для дослідження складних багаторівневих архітектур, де традиційні методи, такі як діаграми надійності блоків або дерева відмов, можуть призводити до значного зростання обчислювальної складності. У випадку систем Інтернету речей, які характеризуються великою кількістю взаємопов’язаних пристроїв, мережевих вузлів та сервісних компонентів, використання бінарних діаграм рішень дозволяє формалізувати структуру системи та виконувати точне оцінювання її надійності з урахуванням різних конфігурацій функціонування.

Таким чином, метод оцінювання надійності на основі бінарних діаграм рішень є ефективним інструментом аналізу складних технічних систем. Використання БДР дозволяє формалізувати логічні залежності між компонентами системи, компактно представити структурну функцію та виконувати точні обчислення ймовірності працездатності системи. Завдяки своїм властивостям цей

метод широко застосовується у сучасних дослідженнях надійності інформаційно-комунікаційних систем, розподілених обчислювальних середовищ та архітектур Інтернету речей.

Незважаючи на ефективність методу бінарних діаграм рішень, його застосування для аналізу надійності IoT-інфраструктур відкриває можливості для подальшого вдосконалення, зокрема в напрямі підвищення масштабованості, адаптивності та врахування динамічних властивостей системи. Одним із перспективних підходів є удосконалення процедур редукції БДР шляхом оптимізації порядку змінних, оскільки розмір діаграми $|G|$ істотно залежить від вибору впорядкування $x_1, x_2, \dots, x_n$, і в загальному випадку задача знаходження оптимального порядку є NP-складною. Додатково, для IoT-систем доцільним є розширення класичної моделі шляхом інтеграції часових параметрів відмов, що дозволяє перейти від статичної булевої функції $\varphi(x)$ до стохастичних або напівмарковських моделей виду $\varphi(x, t)$. Також перспективним є поєднання BDD із методами машинного навчання для автоматичного виявлення критичних компонентів та структурних залежностей у великих мережах, а також використання розподілених обчислень для обробки великих діаграм у режимі реального часу. Крім того, врахування залежних відмов, характерних для IoT-інфраструктур (наприклад, через спільні вузли зв'язку або енергоживлення), потребує розширення класичної моделі незалежних змінних до корельованих випадкових величин. Таким чином, подальший розвиток методу аналізу надійності на основі бінарних діаграм рішень пов'язаний із його адаптацією до специфіки розподілених кіберфізичних систем, що дозволить підвищити точність оцінювання та ефективність обчислень у складних IoT-середовищах.

2.5 Міри важливості компонентів у системах з конкуруючими відмовами

Аналіз надійності IoT-інфраструктури не вичерпується обчисленням єдиного інтегрального показника – ненадійності системи. Для практичних цілей технічного обслуговування, проєктування резервування та пріоритизації заходів підвищення

надійності не менш важливим є питання про те, який внесок кожного окремого компонента у загальну надійність системи. Відповіддю на це питання є концепція мір важливості компонентів, що дозволяє кількісно оцінити, наскільки критичним є кожен елемент системи з точки зору її надійності.

У загальному випадку під мірою важливості компонента можна розуміти деяка числова характеристика, що відображає чутливість системної надійності до зміни стану або надійності даного компонента. Різні міри важливості акцентують увагу на різних аспектах цього зв'язку: одні оцінюють структурний вплив компонента на логіку відмови системи, інші враховують імовірнісні характеристики його функціонування. Застосування мір важливості до систем з конкуруючими відмовами вимагає особливої уваги, оскільки наявність функціональної залежності між компонентами та конкуруюча природа відмов суттєво ускладнюють інтерпретацію отриманих результатів.

Найбільш поширеною та фундаментальною є міра важливості Бірнбаума, запропонована Зедом Бірнбаумом. Ця міра визначається як часткова похідна ненадійності системи за ймовірністю відмови розглядуваного компонента і характеризує граничну чутливість системної ненадійності до зміни надійності компонента. Формально міра важливості Бірнбаума для компонента X у момент часу t визначається як:

$$I(X,t) = \frac{\partial UR_{sys}(t)}{\partial qX(t)} \tag{2.13}$$

де $qx(t) = F_X(t)$ – ймовірність відмови компонента X у момент часу t; $UR_{sys}(t)$ – ненадійність системи, визначена виразом (2.8). Фізичний зміст міри Бірнбаума полягає в тому, що вона показує, наскільки збільшиться ненадійність системи при нескінченно малому збільшенні ймовірності відмови компонента X за умови незмінності всіх інших компонентів.

На практиці, оскільки ймовірності відмов компонентів набувають значень у діапазоні [0, 1], міра Бірнбаума часто обчислюється у дискретному варіанті – як

різниця ненадійностей системи при граничних значеннях ймовірності відмови компонента:

$$I(X,t) = UR_{sys}(t)|_{qX=1} - UR_{sys}(t)|_{qX=0} \quad (2.14)$$

де $UR_{sys}(t)|_{qX=1}$ – ненадійність системи за умови, що компонент X гарантовано відмовив ($qX = 1$), а $UR_{sys}(t)|_{qX=0}$ – ненадійність системи за умови, що компонент X гарантовано справний ($qX = 0$). Різниця цих двох величин відображає максимальний можливий вплив компонента X на надійність системи.

Варто зазначити, що міра важливості Бірнбаума є структурною характеристикою у тому сенсі, що вона залежить не лише від надійнісних параметрів самого компонента, але й від надійностей усіх інших елементів системи, а також від її логічної структури. У контексті IoT-систем з конкуруючими відмовами це означає, що обчислення міри Бірнбаума вимагає двократного розв'язання задачі оцінювання ненадійності системи – з встановленим значенням $qX = 1$ та $qX = 0$ відповідно – з повним урахуванням механізму конкуруючих відмов через формулу (2.8). Таким чином, для системи з n компонентами (що включають як локальні, так і поширювані відмови кожного датчика та відмови шлюзів) необхідно виконати $2n$ таких обчислень.

Суттєвою особливістю застосування міри Бірнбаума в системах з конкуруючими відмовами є необхідність окремого розгляду локальної та поширюваної відмов кожного датчика. Оскільки ці два типи відмов мають принципово різний механізм впливу на систему – локальна відмова виводить з ладу лише сам датчик, тоді як поширювана відмова за певних умов призводить до системної відмови, тобто їхні міри важливості Бірнбаума $I_{\text{B}}(S_{il}, t)$ та $I_{\text{B}}(S_{ip}, t)$ можуть суттєво відрізнятися, навіть якщо обидва типи описуються однаковим законом розподілу часу до відмови.

Поряд із мірою Бірнбаума широкого застосування набула міра важливості Фасселла-Веслі, запропонована Джеймсом Фасселлом та Вільямом Веслі. На

відміну від міри Бірнбаума, що характеризує граничну чутливість, міра Фасселла-Веслі визначає відносний внесок компонента у загальну ненадійність системи. Вона показує, яка частка ненадійності системи обумовлена відмовами, що включають даний компонент. Формально міра Фасселла-Веслі визначається як:

$$I_{FV}(X,t) = \frac{UR_{sys}(t) - UR_{sys}(t)|_{qX=0}}{UR_{sys}(t)} \tag{2.15}$$

де чисельник $UR_{sys}(t) - UR_{sys}(t)|_{qX=0}$ відображає зниження ненадійності системи, яке було б досягнуто, якби компонент X став абсолютно надійним ($qX = 0$ і залишався б таким протягом усієї місії), а знаменник $UR_{sys}(t)$ – загальна ненадійність системи. Таким чином, $I_{FV}(X,t) \in [0,1]$, і значення, близьке до одиниці, свідчить про те, що практично вся ненадійність системи пов'язана з даним компонентом.

Міра Фасселла-Веслі має виражену економічну інтерпретацію. Вона дозволяє відповісти на питання, яку частку загальної ненадійності системи можна усунути шляхом удосконалення або заміни конкретного компонента на абсолютно надійний. Це робить її особливо корисним інструментом для прийняття рішень про вкладення ресурсів у підвищення надійності системи.

Зв’язок між мірою Фасселла-Веслі та мірою Бірнбаума встановлюється через таке співвідношення. Оскільки при малих значеннях ймовірностей відмов окремих компонентів ненадійність системи є приблизно лінійною функцією кожної з них, можна записати наближену рівність:

$$I_{FV}(X,t) \approx \frac{I_B(X,t) \cdot qX(t)}{UR_{sys}(t)} \tag{2.16}$$

Вираз (2.17) показує, що міра Фасселла-Веслі є добутком міри Бірнбаума та відношення ймовірності відмови компонента до загальної ненадійності системи. Компонент може мати низьку міру Бірнбаума (тобто слабкий граничний вплив на

систему), але високу міру Фасселла-Веслі, якщо він відмовляє з великою ймовірністю. Обернена ситуація також можлива: компонент з високою мірою Бірнбаума та малою власною ймовірністю відмови матиме невелику міру Фасселла-Веслі. Таким чином, ці дві міри доповнюють одна одну і разом дають повнішу картину важливості компонентів.

В аналізі надійності систем з конкуруючими відмовами також використовується міра критичної важливості, що є нормованою версією міри Бірнбаума і враховує фактичну ймовірність відмови компонента:

$$I_C(X,t) \approx \frac{I_B(X,t) \cdot qX(t)}{UR_{sys}(t)} = I_{FV}(X,t) \qquad (2.17)$$

де рівність $I_C(X,t) = I_{FV}(X,t)$ у точному сенсі виконується при використанні дискретного визначення міри Бірнбаума (2.15). Ця міра поєднує структурний аспект (вплив компонента на логіку системи, відображений у I_B) з імовірнісним аспектом (власна ненадійність компонента qX), що робить її особливо інформативною для порівняльного аналізу компонентів з різними надійнісними характеристиками.

Особливості застосування наведених мір важливості до IoT-систем з конкуруючими відмовами визначаються специфікою формули ненадійності (2.13). При обчисленні міри Бірнбаума для поширюваної відмови датчика S_{ip} встановлення $q_{S_{ip}} = 0$ означає усунення ймовірності поширюваної відмови, тобто всі доданки $P(R_{2,i})$, пов'язані з цим датчиком, зводяться до нуля. Відповідно, встановлення $q_{S_{ip}} = 1$ означає, що поширювана відмова цього датчика відбувається гарантовано і миттєво, що максимізує відповідні доданки $P(R_{2,i})$.

Для локальної відмови датчика S_{il} встановлення $q_{S_{ip}} = 1$ або $q_{S_{ip}} = 0$ змінює значення умовних ненадійностей $P\left(\text{Відмова системи}\middle|R_{1,i}\right)$ у відповідних доданках суми (2.13).

Результати обчислення мір важливості для IoT-системи розумного будинку з трьома датчиками та двома шлюзами демонструють характерну закономірність: поширювані відмови датчиків мають суттєво вищі значення мір важливості порівняно з локальними відмовами тих самих датчиків і відмовами шлюзів. Ця закономірність пояснюється принциповою різницею в механізмах впливу: локальна відмова виводить з ладу лише один компонент, тоді як поширювана відмова при несприятливому збігу обставин призводить до системної відмови незалежно від стану всіх інших компонентів.

Окремої уваги заслуговує порівняння мір важливості поширюваних відмов датчиків, підключених до різних шлюзів. Датчик, поширювана відмова якого може бути ізольована лише одночасною відмовою кількох шлюзів (тобто який знаходиться у зоні покриття кількох шлюзів), матиме, як правило, вищу міру важливості Бірнбаума, ніж датчик, для ізоляції відмови якого достатньо відмови одного шлюзу. Це пояснюється тим, що ймовірність одночасної відмови кількох шлюзів до настання поширюваної відмови датчика є значно меншою. Таким чином, ранжування компонентів за мірою важливості Бірнбаума у системах з конкуруючими відмовами відображає не лише структурне розташування компонентів у логіці дерева відмов, а й топологічні особливості підключення датчиків до мережевих шлюзів і стохастичну природу конкуренції між відмовами.

2.6 Висновки

У даному розділі проведено комплексний аналіз механізму поширення відмов в IoT-інфраструктурі на прикладі системи розумного будинку. Показано, що через спільне середовище передачі даних та функціональну залежність датчиків від мережевих шлюзів локальна несправність одного компонента може набувати системного характеру. Детально розглянуто два фундаментальні механізми такого поширення: фізичний, що реалізується через зашумлення спільного радіоканалу та логічний, що реалізується через каскадну трансляцію хибних критичних даних. Особливу увагу приділено концепції конкуруючих відмов, яка полягає у часовій

конкуренції між моментом відмови шлюзу та моментом виникнення поширюваної відмови датчика. Було встановлено, що результат цієї конкуренції повністю визначає, чи буде поширена відмова ізольована, чи призведе до повного відказу системи.

Також було розглянуто базовий алгоритм побудови бінарних діаграм рішень для статичної моделі дерева відмов IoT-інфраструктури. Показано порядок змінних за правилом глибинного обходу та рекурсивне об’єднання суб-БДР. Цей алгоритм став фундаментальною основою для ефективного скорочення БДР-моделі в подальших кроках запропонованого методу.

Окрім того, у розділі розглянуто кількісні інструменти оцінювання критичності окремих компонентів системи – міри важливості Бірнбаума та Фасселла-Веслі. Міра Бірнбаума характеризує граничну чутливість ненадійності системи до зміни стану конкретного компонента, тоді як міра Фасселла-Веслі відображає відносний внесок компонента у загальну ненадійність. Встановлено, що в системах з конкуруючими відмовами поширювані відмови датчиків мають суттєво вищі значення обох мір порівняно з локальними відмовами тих самих датчиків та відмовами шлюзів, що підтверджує домінуючу роль механізму поширення відмов у формуванні загального ризику відказу IoT-інфраструктури.

3 МЕТОД АНАЛІЗУ НАДІЙНОСТІ ІОТ-ІНФРАСТРУКТУР НА ОСНОВІ РЕДУКЦІЇ БІНАРНИХ ДІАГРАМ РІШЕНЬ

3.1 Постановка задачі та основні засади методу

Аналіз надійності IoT-інфраструктур, зокрема систем розумного будинку, ускладнюється наявністю функціональної залежності між компонентами та конкуруючими відмовами, що виникають у них. Традиційні підходи до оцінювання надійності – імітаційне моделювання, методи на основі ланцюгів Маркова та комбінаторні методи – по-різному справляються з цими викликами. Імітаційні методи, хоча й забезпечують гнучкість моделювання динамічних систем, дають лише наближені результати, що може бути недостатнім для відповідальних застосувань. Марковські методи дозволяють отримувати точні результати для порівняно невеликих систем, однак вони потребують певних обмежень щодо законів розподілу часу до відмови компонентів та суттєво страждають від проблеми комбінаторного вибуху простору станів при збільшенні кількості елементів.

Комбінаторні методи поєднують переваги точності та обчислювальної ефективності, що обумовило їх широке застосування в задачах аналізу надійності систем з конкуруючими відмовами. Серед комбінаторних підходів особливе місце посідають методи, що базуються на деревах відмов (ДВ) та бінарних діаграмах рішень (БДР). Дерева відмов є зручним інструментом для формального опису логічних зв’язків між відмовами компонентів та системною відмовою, а бінарні діаграми рішень забезпечують ефективне обчислення ймовірнісних показників надійності на основі цих логічних моделей.

Пропонований метод базується на головній ідеї, яка полягає у редукції бінарних діаграм рішень, що розглядається як альтернатива традиційному підходу. Принципова відмінність полягає в тому, що представлений метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень дозволяє формувати редуковані БДР-моделі для кожної підзадачі безпосередньо з єдиної вихідної БДР без необхідності попередньої побудови та зберігання множини

редукованих дерев відмов. Завдяки цьому значно скорочується як обчислювальний час, так і вимоги до пам'яті в процесі аналізу надійності. На відміну від роботи [43], де основна увага зосереджена виключно на обчисленні інтегрального показника ненадійності, у даній кваліфікаційній роботі метод доповнено аналізом важливості компонентів за мірою Бірнбаума, що дозволяє виявити пріоритетні напрямки підвищення надійності системи.

Загалом запропонований метод реалізується у п’ять послідовних кроків і може бути застосований до IoT-систем з довільними законами розподілу часу до відмови компонентів, що є важливою перевагою з практичної точки зору (в даній роботі досліджувались експоненційний закон розподілу та закон Вейбула). В пропонованому методі аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень можна виділити такі кроки:

1) побудова базової моделі дерева відмов та відповідної бінарної діаграми рішень БДР без урахування поширених відмов;

2) формування простору подій на основі станів шлюзів системи;

3) диференціація (розділення) ефектів поширення відмов для кожної події відмови шлюзу;

4) оцінка умовної ненадійності системи за допомогою техніки редукції БДР-моделей;

5) інтеграція отриманих показників для розрахунку загальної ненадійності системи.

Реалізація запропонованого методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень базується на чітко структурованому наборі вхідних параметрів, що охоплюють логіко-конфігураційні, стохастичні та експлуатаційні аспекти функціонування об’єкта. Зокрема вхідні дані включають детерміновану конфігурацію компонентів, що визначає кількісний склад шлюзів та сенсорів у мережі, а також опис функціональних залежностей, які визначають схему підключення конкретних датчиків до відповідних комунікаційних вузлів. Поряд із цим для моделювання процесів деградації залучаються характеристики локальних відмов, що виражаються через інтенсивності або параметри розподілу

часу до відмови кожного елемента, спільно із відповідними законами розподілу та функціями щільності ймовірності. Важливим вхідним параметром також є заданий час місії, який визначає часові межі проведення імовірнісного аналізу.

У результаті послідовного виконання п’ятиетапного алгоритму генерується комплекс вихідних показників. Основним результуючим параметром є загальний показник ненадійності системи, що дає інтегровану оцінку здатності IoT системи (на прикладі розумного будинку) виконувати свої функції в умовах конкуруючих відмов. Крім фінального значення, вихідні дані містять низку проміжних імовірнісних метрик, зокрема ймовірності виникнення подій відмови шлюзів, а також кількісні характеристики ефектів ізоляції та поширення пошкоджень у системі. Додатково аналітична цінність результатів підкріплюється сформованим набором оптимізованих бінарних діаграм рішень для кожного сценарію стану шлюзів, що дозволяє значно підвищити ефективність подальших розрахунків надійності при зміні експлуатаційних умов. Узагальнену схему методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень подано на рис. 3.1. Розглянемо детальніше кроки пропонованого методу.

3.2 Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Перший крок методу полягає в тому, щоб повністю ігнорувати поширювані відмови датчиків і побудувати базову модель надійності системи розумного будинку (БМН) лише на основі локальних відмов компонентів. Для цього спочатку створюється модель дерева відмов, у якій верхньою небажаною подією є повна відмова всієї системи БМН, а базовими подіями – локальні відмови шлюзів $G_{i,l}$ (де $j = 1, \dots, m$) та локальні відмови датчиків $S_{i,l}$. Оскільки датчики стандартів ZigBee та BLE не можуть функціонувати автономно і потребують підключення до мережі виключно через відповідний шлюз, то, відтак, відмова шлюзу автоматично призводить до недоступності (функціональної ізоляції) всіх датчиків, підключених через нього.

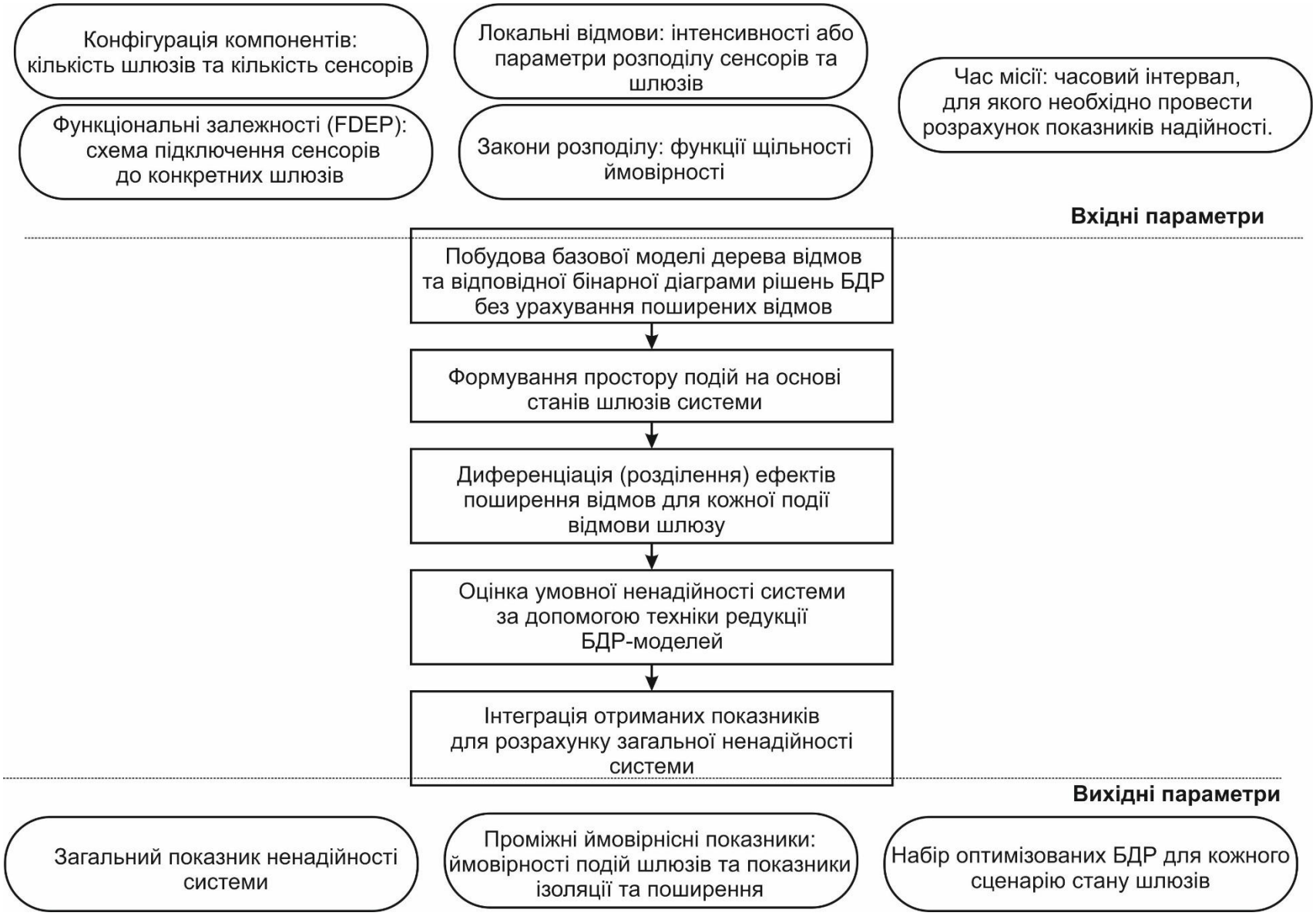


Рисунок 3.1 – Узагальнена схема методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Таку функціональну залежність формально можна змоделювати за допомогою спеціального елемента динамічного дерева відмов – вентиля функціональної залежності ВФЗ. Вентиль ВФЗ з’єднує вузол відмови шлюзу (тригерна подія) з вузлами локальних відмов підключених датчиків (залежні події), відображаючи тим самим, що відмова шлюзу еквівалентна відмові всіх пов'язаних з ним датчиків з точки зору системної доступності.

Даний вентиль має один тригерний вхід (подія відмови шлюзу G_j) та кілька залежних входів (локальні відмови датчиків $S_{i,1}, S_{i,2}, \dots, S_{i,k}$, підключених до цього шлюзу). Логічна функція вентиля записується як:

$$\text{ВФЗ}\left(G_j; S_{i,1}, S_{i,2}, \dots, S_{i,k}\right) \equiv \begin{cases} \text{відмова всіх залежних давачів}, if\, G_j = 1 \\ \text{стан залежних давачів без змін} i, f\, G_j = 0 \end{cases} \quad (3.1)$$

У термінах булевої логіки це еквівалентно умові, що відмова шлюху автоматично викликає відмову всіх залежних давачів незалежно від їхнього власного стану:

$$\text{відмова давача } S_{i,l} \leftarrow G_j \vee S_{i,l} \quad (3.2)$$

Для подальшого аналізу динамічне дерево відмов з вентилями ВФЗ трансформується у статичне дерево відмов шляхом заміни кожного вентиля ВФЗ на вентиль АБО (OR), що з'єднує подію відмови шлюзу з подіями локальних відмов усіх залежних датчиків. Таку заміну можна вважати коректною, оскільки відмова будь-якого з цих елементів – чи то власне шлюзу, чи то датчика – призводить до однакового системного наслідку з точки зору доступності підключеного вузла.

Далі застосовують стандартний алгоритм побудови БДР (бінарної діаграми рішень). Спочатку всі базові події (змінні) впорядковуються за правилом обходу дерева в глибину, тобто змінна, яка стоїть вище в дереві, отримує менший індекс. Після цього БДР будується знизу вгору рекурсивно. Якщо є два суб-БДР, що представляють логічні вирази E та F, їх поєднують за правилом:

$$E \otimes F = \begin{cases} x?\, E_{x=1} \otimes F_{x=1} : E_{x=0} \otimes F_{x=0} & \text{якщо } index(x) = index(y) \\ x?\, E_{x=1} \otimes F : E_{x=0} \otimes F & \text{якщо } index(x) < index(y) \\ y?\, E \otimes F_{y=1} : E \otimes F_{y=0} & \text{якщо } index(x) > index(y) \end{cases} \quad (3.3)$$

де $\otimes$ – це операція AND або OR (залежно від типу вузла (гейту) в дереві), $x?\, E_1 : E_0$ – це оператор «if-then-else» (якщо змінна x відбулася, то беремо ліву гілку, інакше – праву), а E_i і F_i – підвирази відповідних під-БДР. Рекурсія продовжується до тих пір, доки один із субвиразів не стане термінальним (0 або 1), після чого застосовують спрощення за булевою алгеброю:

$$1 + x = 1, 0 + x = x, 1 \cdot x = x, 0 \cdot x = 0 \quad (3.4)$$

Як підсумок результатом першого кроку пропонованого методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень є єдина повна БДР-модель системи, яка описує ймовірність відмови IoT-інфраструктур лише з урахуванням локальних відмов і функціональної залежності, але без жодного впливу поширюваних відмов. Саме цю «базову» БДР-модель (без скорочень) надалі використовують у всіх наступних кроках методу для швидкого отримання скорочених версій під кожну можливу конфігурацію стану шлюзів. Такий підхід дозволяє уникнути повторної побудови окремих дерев відмов для кожного сценарію, що значно знижує обчислювальну складність порівняно з попередніми методами.

Другий крок методу полягає у побудові простору подій, що охоплює всі можливі комбінації стану шлюзів у системі, тобто на цьому етапі здійснюється розбиття всього простору можливих станів системи на взаємно виключаючі та вичерпні сценарії виключно за станами шлюзів. Ця процедура є необхідною підготовкою для подальшого розмежування ефекту ізоляції та ефекту поширення відмов.

Нехай у розглядуваній IoT-системі налічується m шлюзів. Тоді загальна кількість можливих комбінацій їхніх станів (справний / несправний) становить 2^m. Кожна така комбінація визначає окрему подію, яку назвемо подією відмови шлюзів ПВШ. Подія ПВШ_i $(i = 1,2, \dots, 2^m)$ являє собою перетин (кон'юнкцію) подій відмови або неушкодженості кожного з m шлюзів. Тоді формально простір подій можна задати як:

$$\text{I} = \begin{matrix} \text{ПВШ}_1 = \overline{G_1} \cap \overline{G_2} \cap \dots \cap \overline{G_m} \\ \text{ПВШ}_2 = G_1 \cap \overline{G_2} \cap \dots \cap \overline{G_m} \\ \dots \\ \text{ПВШ}_{2^m} = G_1 \cap G_2 \cap \dots \cap G_m \end{matrix} \quad (3.5)$$

Таким чином подія ПВШ_1 відповідає випадку, коли всі шлюзи ще працюють, а подія ПВШ_{2^m} – випадку всі шлюзи відмовили. Проміжні події ПВШ_i описують усі інші можливі конфігурації (наприклад, відмовив лише перший шлюз, або відмовили перший і третій шлюзи).

Оскільки ці 2^m подій утворюють повний і взаємовиключний розподіл простору, то можна застосувати до них застосовується теорему повної ймовірності. Ненадійність IoT-системи за цим підходом обчислюється як зважена сума умовних ймовірностей відмови системи за кожної з можливих конфігурацій стану шлюзів:

$$U_S(t) = \sum_{i=1}^{2^m} [P(\text{Відмова системи} | \text{ПВШ}_i) \cdot P(\text{ПВШ}_i)] \quad (3.6)$$

Вираз (3.4) є базовою формулою для подальших обчислень пропонованого методу аналізу надійності. Безумовна ймовірність кожної конфігурації $P(\text{ПВШ}_i)$ обчислюється на основі кумулятивних функцій розподілу часу до відмови відповідних шлюзів і не залежить від стану датчиків. Для шлюзів з експоненційним розподілом часу до відмови з параметром λ вона визначається через добуток індивідуальних ймовірностей відмови $F(t) = 1 - e^{-\lambda t}$ або безвідмовної роботи

$R(t) = e^{-\lambda t}$ кожного зі шлюзів залежно від їхнього стану у розглядуваній конфігурації ПВШ$_i$.

Третій крок є ключовим з точки зору врахування конкуруючих відмов. Для кожної події відмови шлюзу ПВШ$_i$ здійснюється декомпозиція на дві взаємодоповнювальні підподії залежно від того, чи відбулося поширення відмов від датчиків у межах цієї конфігурації стану шлюзів.

У межах цього кроку кожна подія відмови шлюзу ПВШ$_i$ розділяється на дві взаємовиключні та комплементарні підподії – $R_{1,i}$ та $R_{2,i}$.

Підподія $R_{1,i}$ характеризує ситуацію, за якої всі поширювані відмови або взагалі не виникають, або виявляються ізольованими завдяки відмові відповідних шлюзів. Таке ізолювання можливе лише за умови, що шлюз відмовляє раніше, ніж через нього встигає пройти поширювана відмова підключеного датчика. У рамках підподії $R_{1,i}$ стани всіх шлюзів є детермінованими (визначаються конфігурацією ПВШ$_i$), і конкуруючі відмови не впливають на подальший стан системи, що суттєво спрощує обчислення.

Підподія $R_{2,i}$, навпаки, відповідає ситуації, коли принаймні одна поширювана відмова не ізолюється і встигає поширитися через справний шлюз на інші компоненти системи до його відмови.

За визначенням, настання підподії $R_{2,i}$ неминуче призводить до відмови всієї IoT-системи, тому умовна ймовірність системної відмови за цієї підподії дорівнює одиниці:

$$P(\text{Відмова системи}|R_{2,i}) = 1 \tag{3.7}$$

Оскільки $R_{1,i}$ та $R_{2,i}$ є взаємодоповнювальними подіями, то виконується співвідношення:

$$P(\text{ПВШ}_i) = P\left(R_{1,i}\right) + P(R_{2,i}) \tag{3.8}$$

Для обчислення ймовірності підподії поширення відмов слід розглянути стани датчиків, підключених до кожного зі шлюзів, що відмовив у конфігурації ПВШ$_i$. Для кожного такого шлюзу можливі два стани його датчиків, що ведуть до підподії ізоляції: або датчики не зазнають поширюваних відмов взагалі, або всі їхні поширювані відмови відбуваються після відмови шлюзу. Підподія поширення, відповідно, реалізується, якщо хоча б одна поширювана відмова підключеного датчика виникає раніше відмови шлюзу. Ймовірність підподії ізоляції обчислюється через ймовірність конфігурації та ймовірність поширення:

$$P\left(R_{1,i}\right) = P(\text{ПВШ}_i) - P(R_{2,i}) \tag{3.9}$$

Ключовою складовою обчислень є визначення ймовірності того, що поширювана відмова датчика виникне раніше відмови шлюзу. Для двох компонентів X_1 та X_2 ця ймовірність обчислюється через сумісний розподіл їхніх часів до відмови шляхом інтегрування:

$$P(X_1 \to X_2) = \int_0^T \int_{\tau 1}^T f_{X_1}(\tau 1)\, f_{X_2}(\tau 2)\, d\tau 1\, d\tau 2 \tag{3.10}$$

де $f_X(t)$ – щільність розподілу часу до відмови компонента X; Т – тривалість місії; запис $X_1 \to X_2$ позначає подію, що X_1 відмовляє раніше за X_2.

Математичний вираз (3.8) для обчислення ймовірності послідовності відмов у часовій області базується на аналізі сумісної щільності ймовірності двох незалежних випадкових величин, що описують моменти виникнення відповідних подій. У контексті аналізу надійності сенсорних систем цей вираз дозволяє кількісно оцінити результат «часової конкуренції» між процесом поширення відмови сенсора X_1 та процесом ізоляції цієї відмови шляхом виходу з ладу шлюзу X_2. Фізичний зміст інтеграла полягає в підсумовуванні всіх елементарних ймовірностей того, що перша подія відбудеться у довільний момент часу $\tau 1$

протягом усього інтервалу місії $[0, T]$, а друга подія – у будь-який момент $\tau 2$, який обов'язково є пізнішим за $\tau 1$, але не перевищує загальний час спостереження T.

Структура подвійного інтеграла відображає логіку причинно-наслідкового зв'язку: зовнішній інтеграл за змінною $d\tau 1$ охоплює весь можливий діапазон виникнення ініціюючої події від 0 до T. Для кожного фіксованого моменту $\tau 1$ внутрішній інтеграл обчислює кумулятивну ймовірність того, що подія-конкурент X_2 відбудеться пізніше, що визначає межі інтегрування від $\tau 1$ до T. Оскільки події вважаються стохастично незалежними до моменту їх взаємодії, сумісна щільність імовірності в підінтегральному виразі представлена як добуток індивідуальних функцій щільності $f_{X_1}(\tau 1)$ та $f_{X_2}(\tau 2)$. У випадку використання експоненціального закону розподілу, який є стандартним для опису раптових відмов електронних компонентів, ці функції набувають вигляду $\lambda e^{-\lambda t}$, що дозволяє отримати аналітичне рішення інтеграла.

Для загального випадку n послідовних відмов компонентів $X_1, X_2, \dots, X_n$ відповідний вираз набуває вигляду кратного інтеграла:

$$P(X_1 \to X_2 \to X_n) = \int_0^T \int_{\tau 1}^T \dots \int_{\tau n-1}^T \prod_{i=1}^{n} f_{X_i}(\tau i)\, d_{\tau n} \dots d_{\tau 1} \tag{3.11}$$

Вираз (3.9) є загальним і придатним для застосування при довільних законах розподілу часу до відмови компонентів, що забезпечує універсальність методу. Зокрема, для компонентів з експоненційним розподілом інтеграл допускає аналітичне обчислення, тоді як для розподілу Вейбулла застосовуються чисельні методи інтегрування.

Четвертий крок присвячений обчисленню умовної ймовірності відмови системи за умови настання підподії $R_{1,i}$ – тобто за умови, що всі поширювані відмови ізольовані або не виникли. Оскільки в рамках цієї підподії стани всіх шлюзів є детермінованими (визначеними конфігурацією ПВШ$_i$), задача зводиться

до оцінювання надійності статичної системи, у якій конкуруючі відмови вже не відіграють ролі.

Саме тут реалізується основна ідея методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень – редукція бінарної діаграми рішень. Замість того, щоб будувати окреме дерево відмов для кожної підзадачі та генерувати з нього нову БДР (як це робиться в методі FTR), запропонований підхід отримує редуковану БДР шляхом безпосереднього виключення з вихідної БДР, побудованої на кроці 1, вузлів, що відповідають компонентам з детермінованим станом.

Редукція виконується відповідно до двох правил, що відображають детерміновані стани компонентів у кожній конфігурації події відмови шлюзу $ПВШ_i$:

Правило 1: якщо компонент (шлюз або датчик, функціонально залежний від несправного шлюзу) перебуває в стані відмови, відповідний вузол БДР замінюється на його правий дочірній вузол (гілку «компонент відмовив»). Це правило застосовується як до вузлів несправних шлюзів, так і до вузлів датчиків, що функціонально залежні від цих шлюзів – адже при відмові шлюзу підключені до нього датчики стають недоступними, тобто функціонально еквівалентними несправним.

Правило 2: якщо шлюз перебуває у справному стані, відповідний вузол БДР замінюється на його лівий дочірній вузол (гілку «компонент справний»). Датчики, підключені до справних шлюзів, не зазнають поширюваних відмов у межах підподії $R_{1,i}$, тому аналізуються лише на предмет локальних відмов.

Застосування цих правил дозволяє значно спростити структуру БДР, виключаючи з неї всі вузли, чиї стани є наперед відомими.

Редукована БДР містить лише ті змінні, стан яких залишається невизначеним – тобто датчики, підключені до справних шлюзів, що підлягають локальним відмовам. Зменшення розмірності БДР безпосередньо транслюється у зниження обчислювальних витрат.

Умовна ймовірність відмови системи $P(\text{Відмова системи} \mid R_{1,i})$ обчислюється як сума ймовірностей усіх шляхів у редукованій БДР від кореневого вузла до поглинаючого вузла «1» (відмова системи). Кожен такий шлях відповідає певній мінімальній сукупності локальних відмов, що призводять до системної відмови.

Для конкретного шляху, який проходить через послідовність станів вузлів $x_{k_1} = 1, x_{k_2} = 0, \dots, x_{k_s} = 1$ від кореня до терміналу «1», внесок у загальну ймовірність визначається за формулою:

$$P_{path} = \prod_{k_j : x_{k_j}=1} F_{k_j}(t) \cdot \prod_{k_j : x_{k_j}=0} (1 - F_{k_j}(t)) \tag{3.12}$$

де $F_{k_j}(t)$ — кумулятивна функція розподілу часу до відмови j-го компонента на даному шляху.

Загальна умовна ненадійність системи для заданої події $R_{1,i}$ обчислюється як сума таких внесків за всіма шляхами до одиниці у редукованій бінарній діаграмі рішень:

$$P\left(\text{Відмова системи} \middle| R_{1,i}\right) = \sum_{paths \to 1} P_{path} \tag{3.13}$$

Цей метод дозволяє отримати точне значення ненадійності системи для кожного сценарію відмови шлюзів, уникаючи при цьому необхідності побудови та зберігання множини проміжних дерев відмов, що значно підвищує ефективність обчислювального процесу.

П’ятий крок є завершальним і полягає в агрегуванні результатів, отриманих на попередніх кроках, для обчислення загальної ненадійності IoT-системи U_S. З цією метою кожен доданок у формулі повної ймовірності у виразі (3.4) розкладається із урахуванням декомпозиції на підподії $R_{1,i}$ та $R_{2,i}$.

З урахуванням того, що підподії $R_{1,i}$ та $R_{2,i}$ є взаємовиключними і разом складають повну подію відмови шлюзу ПВШ$_i$, умовна ймовірність системної відмови за конфігурації ПВШ$_i$ розкладається як:

$$P(\text{Відмова системи}|\text{ПВШ}_i) \cdot P(\text{ПВШ}_i) = P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P\left(\text{Відмова системи}\middle|R_{2,i}\right) \cdot P\left(R_{2,i}\right) \quad (3.14)$$

З огляду на результати, встановлені на третьому етапі дослідження, підподія $R_{i,2}$ характеризується тим, що принаймні одна поширена відмова сенсора не була вчасно ізольована, що призводить до гарантованого виходу з ладу всієї системи. Таким чином, умовна ймовірність системної відмови за умови реалізації ефекту поширення дорівнює одиниці, тобто $P\left(\text{Відмова системи}\middle|R_{2,i}\right) = 1$. Враховуючи цю властивість, наведене вище рівняння можна спростити до вигляду:

$$P(\text{Відмова системи}|\text{ПВШ}_i) \cdot P(\text{ПВШ}_i) = P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P\left(R_{2,i}\right) \quad (3.15)$$

Підставляючи вираз (3.13) у формулу повної ймовірності (3.4), отримуємо підсумковий вираз для ненадійності IoT-системи з урахуванням конкуруючих відмов:

$$U_S(t) = \sum_{i=1}^{2^m}[P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P(R_{2,i})] \quad (3.16)$$

де $P\left(R_{1,i}\right)$ та $P\left(R_{2,i}\right)$ обчислюються на кроці 3 за формулами (3.5)-(3.7), а $P\left(\text{Відмова системи}\middle|R_{1,i}\right)$ – на кроці 4 за формулами (3.10)-(3.11). Сума у (3.14) містить 2^m доданків, по одному на кожну конфігурацію стану m шлюзів системи.

Як підсумок можна відзначити, що у формулі (3.14) перший доданок у кожному члені суми відповідає ненадійності, обумовленій локальними відмовами

датчиків у випадках, коли поширювані відмови ізольовані, тоді як другий доданок – ненадійності, спричиненій реалізацією поширюваних відмов. Такий поділ є принципово важливим для інженерної практики, оскільки дозволяє окремо оцінити внесок кожного з механізмів відмови та цілеспрямовано впливати на надійність системи. Цей інтеграційний підхід дозволяє отримати точну кількісну оцінку надійності складних систем, враховуючи як логічну структуру функціональних залежностей (через редуковані БДР-моделі), так і динамічну конкуренцію між локальними та поширеними механізмами відмов.

3.3 Теоретична оцінка обчислювальної складності методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Важливою характеристикою запропонованого методу є його обчислювальна ефективність порівняно з традиційним підходом на основі редукції дерев відмов. Для системи з m шлюзами та n компонентами загалом порівняльна оцінка складності виглядає наступним чином.

Метод FTR вимагає побудови $1 + 2^m$ дерев відмов (вихідне плюс по одному на кожну конфігурацію подію відмови шлюзу) та генерації БДР з кожного з них. Генерація бінарної діаграми рішення із дерева відмов є обчислювально дороговартісною операцією: максимальний розмір БДР з n змінними становить $O(2^n/n)$, а часова та просторова складність операції над двома БДР є добутком їхніх розмірів, тобто $O(4^n/n^2)$. Оскільки метод FTR виконує цю операцію 2^m разів, загальна часова складність становить:

$$T_{FTR} = 2^m \cdot O(4^n/n^2) \tag{3.17}$$

Пропонований метод редукції БДР, натомість, виконує генерацію БДР із дерева відмов лише одного разу. Подальші 2^m операцій редукції БДР мають лінійну складність $O(N)$ відносно кількості вузлів БДР, що є значно меншим за

складність генерації BDD. Тому загальна часова складність методу BDDR визначається однократним перетворенням дерева відмов:

$$T_{method} = O(4^n/n^2) \tag{3.18}$$

Таким чином співвідношення $T_{FTR}/T_{method} = 2^m$ свідчить про те, що виграш у продуктивності зростає експоненційно зі збільшенням кількості шлюзів у системі (рис. 3.2).

Просторова складність зменшується аналогічним чином: метод FTR вимагає одночасного зберігання $1 + 2^m$ дерев відмов та 2^m БДР-моделей, тоді як пропонований метод потребує лише одного дерева відмов та $1 + 2^m$ БДР (1 вихідна модель та 2^m редукованих). Таким чином, просторова складність пропонованого методу також становить $O(4^n/n^2)$ проти $2^m \cdot O(4^n/n^2)$ для методу FTR.

Рисунок 3.2 – Порівняння часової складності для традиційного та пропонованого методу

Практична перевага методу BDDR підтверджується як теоретичним аналізом складності, так і емпіричними вимірюваннями. Зокрема, для системи з одним вузлом виявлення (m = 2, n = 5) час виконання методу BDDR складає близько 40 мс проти 260 мс для методу FTR, що відповідає теоретично очікуваному прискоренню у $2^2 = 4$ рази. При збільшенні кількості вузлів виявлення різниця у часі виконання зростає нелінійно, і вже при шести вузлах метод BDDR забезпечує приблизно триразове прискорення порівняно з методом FTR, що переконливо демонструє практичну ефективність запропонованого підходу.

Отже, метод BDDR являє собою ефективний комбінаторний підхід до аналізу надійності IoT-інфраструктур, що забезпечує точне врахування конкуруючих відмов при значно менших обчислювальних витратах порівняно з традиційними підходами. Метод є придатним для застосування при довільних законах розподілу часу до відмови компонентів, що робить його універсальним інструментом для інженерного аналізу надійності систем розумного будинку та суміжних IoT-застосувань.

3.4 Висновки

У висновку до даного розділу можна підсумувати, що розроблений метод аналізу надійності IoT-інфраструктур, заснований на редукції бінарних діаграм рішень, здійснює оцінку відмовостійкості складних сенсорних мереж в умовах часової конкуренції між механізмами деградації. Запропоноване рішення реалізується через п’ять послідовних етапів, що включають побудову вихідної моделі, що передбачає формування статичного дерева відмов системи та його подальшу конвертацію у базову бінарну діаграму рішень без урахування ефектів поширення, формування простору подій шлюзів, диференціація ефектів поширення відмов, оцінку умовної ненадійності через редукцію БДР та інтеграція показників. Важливою перевагою пропонованого методу є його інваріантність відносно законів розподілу часу до відмови компонентів.

4 ТЕОРЕТИЧНЕ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДУ АНАЛІЗУ НАДІЙНОСТІ ІОТ-ІНФРАСТРУКТУРИ НА ОСНОВІ РЕДУКЦІЇ БІНАРНИХ ДІАГРАМ РІШЕНЬ

4.1 Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень

Для перевірки коректності та демонстрації практичного застосування методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень розглянемо конкретний приклад інфраструктури Інтернету речей, що представлена розумним будинком.

Досліджувана система складається з трьох датчиків S_1, S_2 та S_3, що призначені для моніторингу параметрів внутрішнього середовища приміщення зокрема, концентрації газу, температури та вологості. Критерієм працездатності системи є справна робота щонайменше двох із трьох датчиків одночасно, тобто система функціонує за схемою «2 з 3». Таку конфігурацію обрано як типову для відповідальних застосувань, де відмова одного датчика не повинна призводити до втрати функціональності всієї системи моніторингу.

Три датчики розподілені у просторі будинку відповідно до зон покриття двох мережевих шлюзів G_1 та G_2. Датчик S_1 знаходиться виключно в зоні покриття шлюзу G_1 і підключається до мережі лише через нього. Датчик S_2 аналогічним чином знаходиться виключно в зоні покриття шлюзу G_2. Датчик S_3 розташований у зоні перекриття покриття обох шлюзів, завдяки чому він може підключатися до мережі через будь-який із них G_1 або G_2. Маршрутизатор, через який система взаємодіє із зовнішньою мережею та хмарною платформою, вважається абсолютно надійним і не розглядається як можливе джерело відмов у даному аналізі.

Зазначена топологія підключення породжує такі відносини функціональної залежності: між шлюзом G_1 та датчиком S_1 існує пряма функціональна залежність, тобто відмова G_1 робить S_1 недоступним; між шлюзом G_2 та датчиком S_2 існує аналогічна пряма функціональна залежність; датчик S_3 функціонально залежить від

спільної події одночасної відмови обох шлюзів G_1 та G_2, тобто лише за умови, що обидва шлюзи вийдуть з ладу, датчик S_3 втратить зв'язок із мережею. Ця особливість S_3 є принципово важливою з точки зору аналізу надійності, оскільки вона робить його більш захищеним від ізолювання порівняно з S_1 та S_2, але водночас означає, що поширювана відмова S_3 може бути ізольована лише при одночасній відмові двох шлюзів, що є значно менш імовірною подією.

Для ілюстративного аналізу прийнято, що час до відмови всіх компонентів системи підпорядковується експоненційному розподілу. Щільність імовірності та кумулятивна функція розподілу для компонента з параметром інтенсивності відмов λ мають вигляд:

$$f(t) = \lambda \cdot e^{-\lambda t} \quad (4.1)$$

$$F(t) = 1 - \lambda \cdot e^{-\lambda t} \quad (4.2)$$

Вибір експоненційного розподілу обумовлений його широким застосуванням у надійності електронних та мережевих компонентів, а також властивістю відсутності пам'яті. Параметри інтенсивностей відмов компонентів системи наведено у табл. 4.1. Для проведення розрахунків було визначено, що інтенсивність поширюваної відмови кожного датчика становить λ_p = 0,00005 год$^{-1}$, інтенсивність локальної відмови датчика λ_l = 0,0002 год$^{-1}$. Для шлюзів поширювана відмова не передбачена ($\lambda_{G,p}$ = 0), а інтенсивність локальної відмови становить $\lambda_{G,l}$ = 0,0001 год$^{-1}$. Тривалість місії системи прийнято рівною T = 1000 год.

Таблиця 4.1 – Параметри інтенсивностей відмов компонентів системи

Компонент	Поширювана відмова, год$^{-1}$	Локальна відмова, год$^{-1}$
Датчик S_i (i = 1, 2, 3)	0,00005	0,0002
Шлюз G_j (j = 1, 2)	0	0,0001

Розглянемо виконання послідовності кроків для пропонованого методу оцінки надійності IoT інфраструктури.

Крок 1. Побудова моделі дерева відмов та БДР без урахування поширюваних відмов.

На першому кроці будується динамічне дерево відмов для розглядуваної IoT-системи без врахування поширюваних відмов. Вершинною подією дерева є відмова всієї системи. Базовими подіями є локальні відмови шлюзів G_{1l} та G_{2l} і локальні відмови датчиків S_{1l}, S_{2l}, та S_{3l},. Функціональна залежність між шлюзами та датчиками моделюється трьома вентилями функціональної залежності ВФЗ: перший з'єднує G_1 з S_1, другий – G_2 з S_2, третій – спільну подію відмови (G_1 і G_2) з датчиком S_3. Це відображає той факт, що S_3 втрачає зв'язок лише за умови одночасної відмови обох шлюзів. Динамічне дерево відмов із ВФЗ для досліджуваної системи наведено на рис. 4.1.

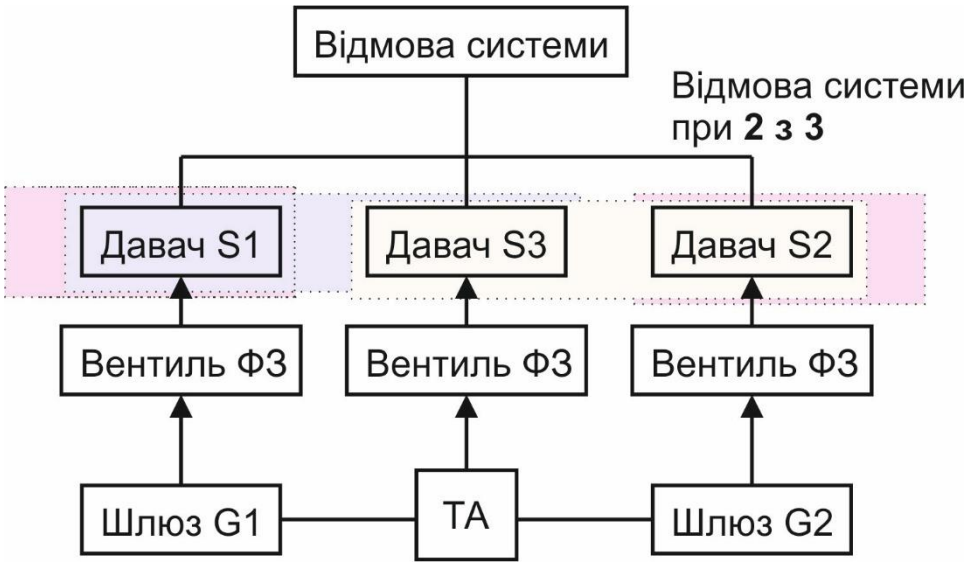


Рисунок 4.1 – Динамічне дерево відмов із ВФЗ для досліджуваної системи із трьома давачами та двома шлюзами

Для перетворення динамічного дерева відмов у статичне кожен вентиль ВФЗ замінюється вентилем АБО. Вентиль АБО для S_1 об'єднує події G_{1l} та S_{1l}; вентиль АБО для S_2 об'єднує G_{2l} та S_{2l}; вентиль АБО для S_3 об'єднує кон'юнкцію (G_{1l} AND G_{2l}) та S_{3l}. Отримане статичне дерево відмов описує умову системної відмови:

система відмовляє, якщо щонайменше двоє з трьох «розширених» датчиків (кожен з яких вважається тим, що відмовив, при відмові власного шлюзу або локальній відмові датчика) виходять з ладу. Статичне дерево відмов наведено на рис. 4.1.

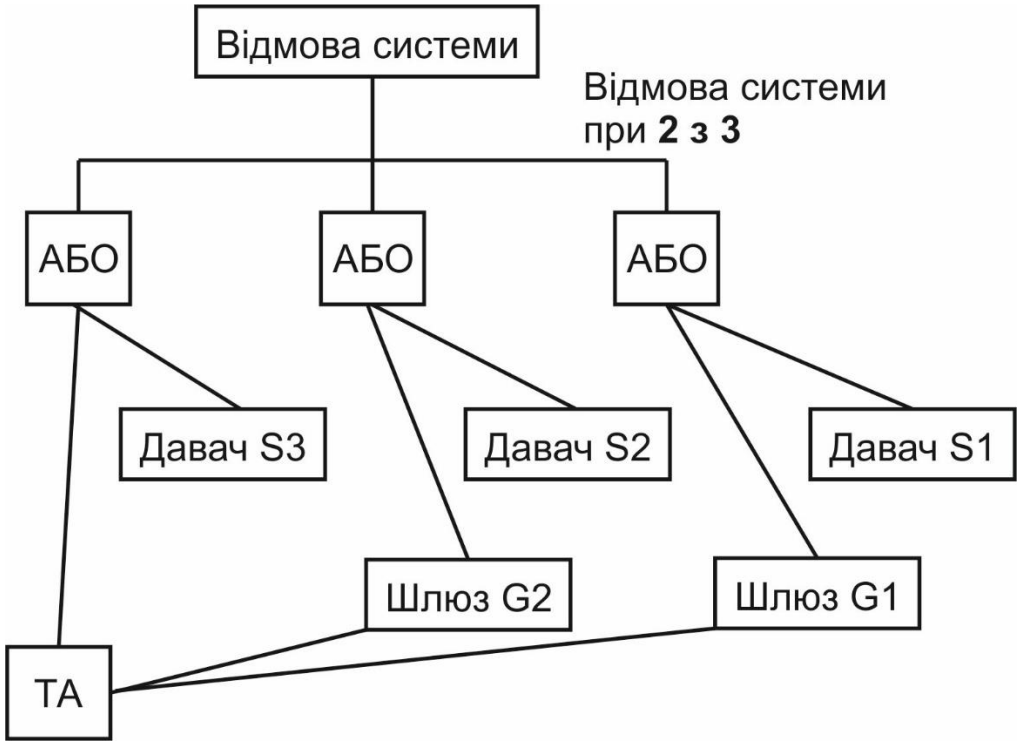


Рисунок 4.2 – Статичне дерево відмов (заміна ВФЗ на вентилі «ТА» «АБО»)

Для побудови БДР застосовується правило впорядкування змінних за обходом дерева відмов в глибину, що дає такий порядок:

$$G_{1l} < G_{2l} < S_{3l} < G_{2l} < S_{1l} \tag{4.3}$$

Побудована БДР відображає всі можливі комбінації станів п'яти змінних, що призводять до системної відмови, і є вихідним об'єктом для подальших операцій редукції. Бінарна діаграма рішень для досліджуваної системи наведено на рис. 4.3.

Крок 2. Формування простору подій відмови шлюзів ПВШ.

Оскільки у системі присутні два шлюзи (m = 2), простір подій містить $2^2 = 4$ конфігурації стану шлюзів. Позначимо локальну відмову шлюзу G_j через G_{jl}, а його справний стан через $\overline{G_{jl}}$.

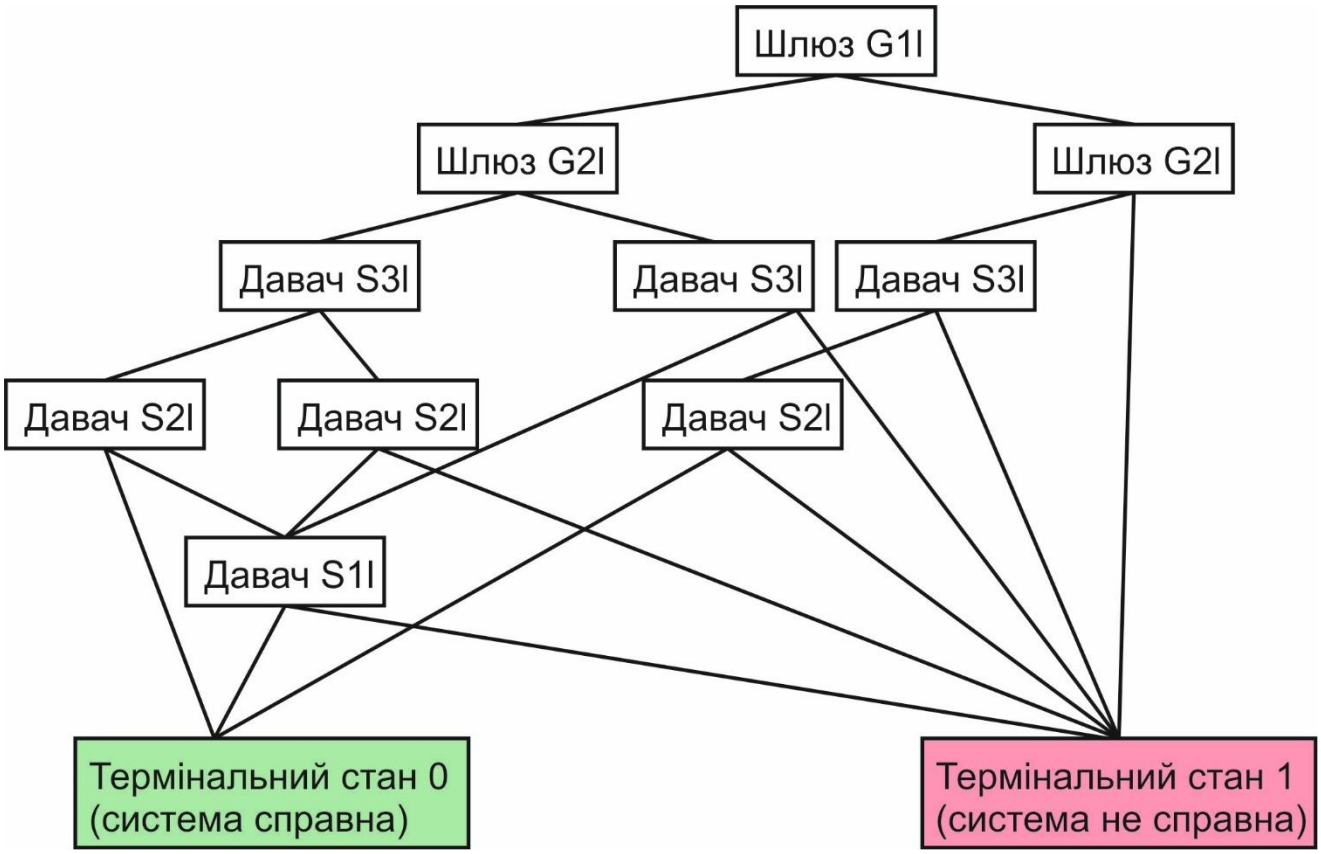


Рисунок 4.3 – БДР для досліджуваної системи

Чотири події ПВШ, що утворюють повну систему подій, які наведено у таблиці 4.2.

Таблиця 4.2 – Простір подій на основі станів шлюзів

Подія	Визначення	Зміст
$ПВШ_1$	$\overline{G_{1l}} \cap \overline{G_{2l}}$	Жоден шлюз не відмовив
$ПВШ_2$	$G_{1l} \cap \overline{G_{2l}}$	Відмовив лише G_1
$ПВШ_3$	$\overline{G_{1l}} \cap G_{2l}$	Відмовив лише G_2
$ПВШ_4$	$G_{1l} \cap G_{2l}$	Обидва шлюзи відмовили

Безумовні ймовірності кожної конфігурації обчислюються на основі кумулятивного розподілу (3.4). За t = 1000 год та λ_G = 0,0001 год$^{-1}$ ймовірність

відмови одного шлюзу становить $F_G(1000) = 1 - e^{-0,1} \approx 0,09516$, а ймовірність його справності – $R_G(1000) = e^{-0,1} \approx 0,90484$. Відповідно:

$$P(\text{ПВШ}_1) = P(\overline{G_{1l}}) \cdot P(\overline{G_{2l}}) = 0.90484^2 \approx 0.81873 \quad (4.4)$$

$$P(\text{ПВШ}_2) = P(G_{1l}) \cdot P(\overline{G_{2l}}) = 0.9516 \cdot 0.90484 \approx 0.08611 \quad (4.5)$$

$$P(\text{ПВШ}_3) = P(\overline{G_{1l}}) \cdot P(G_{2l}) = 0.90484 \cdot 0.09516 \approx 0.08611 \quad (4.6)$$

$$P(\text{ПВШ}_4) = P(G_{1l}) \cdot P(G_{2l}) = 0.09516^2 \approx 0.00906 \quad (4.7)$$

Сума чотирьох ймовірностей складає одиницю, що підтверджує коректність побудованого простору подій: 0,81873 + 0,08611 + 0,08611 + 0,00906 = 1,00001 ≈ 1 (з урахуванням похибки округлення).

Крок 3. Декомпозиція ефекту поширення відмов для кожної конфігурації події відмови шлюзу.

Для кожної з чотирьох конфігурацій здійснюється декомпозиція на підподії ізоляції та поширення відмов. Розглянемо кожну конфігурацію детально.

Конфігурація ПВШ_1 (жоден шлюз не відмовив). За умови ПВШ_1 обидва шлюзи справні. Підподія поширення $R_{2,1}$ реалізується тоді, коли хоча б одна поширювана відмова будь-якого з трьох датчиків виникає і поширюється через справний шлюз. Оскільки жоден шлюз не відмовив, ізоляція поширюваних відмов неможлива – будь-яка поширювана відмова автоматично потрапляє у підподію $R_{2,1}$. Ймовірність підпод ії поширення визначається через ймовірність виникнення хоча б однієї поширюваної відмови серед трьох датчиків:

$$P(R_{2,1}) = P[(\overline{G_1} \cap \overline{G_2}) \cap (S_{1p} \cup S_{2p} \cup S_{3p})] \approx 0.11404 \quad (4.8)$$

де S_{ip} позначає поширювану відмову датчика S_j. Ймовірність підпод ії ізоляції визначається за формулою (3.7):

$$P(R_{1,1}) = P(\text{ПВШ}_1) - P(R_{2,1}) = 0.81873 - 0.11404 = 0.70469 \quad (4.9)$$

Конфігурація ПВШ_1 (відмовив лише G_1). За умови ПВШ_1 шлюз G_1 відмовив, а G_2 справний. Відмова G_1 автоматично ізолює будь-яку поширювану відмову датчика S_1, оскільки S_1 підключений виключно через G_1. Однак датчики S_2 та S_3 залишаються підключеними через справний G_2, тому їхні поширювані відмови не ізолюються. Крім того, поширювана відмова S_1 може не бути ізольованою, якщо вона виникне до відмови G_1, тобто якщо S_1p відбудеться раніше за G_1l. Ймовірність підподії поширення обчислюється як:

$$P(R_{2,2}) = P\{[(G_1 \cap \overline{G_2}) \cap (S_{2p} \cup S_{3p})] \cup [(S_{1p} \to G_1) \cap \overline{G_2}]\} \quad (4.10)$$

де запис ($S_{1p} \to G_1$ позначає подію, що поширювана відмова S_1 виникає раніше за відмову шлюзу G_1. Ймовірність цієї події обчислюється через подвійний інтеграл від сумісної щільності розподілу часів до відмови S_{1p} та G_{1l}:

$$P(S_1^p \to G_1^l) = \int_0^T \int_{\tau_1}^T f_{S_1^p}(\tau_1) \cdot f_{G_1^l}(\tau_2) d\tau_1 d\tau_2 = \int_0^{1000} \int_{\tau_1}^{1000} 0.00005 \cdot e^{-0.00005\tau_1} \cdot 0.0001 \cdot e^{-0.0001\tau_2}\, d\tau_1 d\tau_2 = \frac{1}{3}(1 - e^{-0.15}) - e^{-0.1}(1 - e^{-0.05}) \approx 0.0023 \quad (4.11)$$

Аналітичний розв'язок інтеграла (4.11) є можливим завдяки властивостям експоненційного розподілу. Загальний результат: $P(R_{2,2}) \approx 0{,}01008$, а отже:

$$P(R_{1,2}) = P(\text{ПВШ}_1) - P(R_{2,2}) = 0{,}08611 - 0{,}01008 = 0{,}07603 \quad (4.12)$$

Конфігурація ПВШ_3 (відмовив лише G_2). Ця конфігурація є симетричною до ПВШ_2 відносно заміни $G_1 \leftrightarrow G_2$ та $S_1 \leftrightarrow S_2$. Відмова G_2 ізолює поширювані відмови

датчика S_2, тоді як датчик S_1 залишається під'єднаним через справний G_1. За симетрії параметрів: $P(R_{2,3})$ = 0,01008 та $P(R_{1,3})$ = 0,07603.

Конфігурація ПВШ$_4$ (обидва шлюзи відмовили). За умови ПВШ$_4$ обидва шлюзи відмовили. Усі три датчики стають функціонально недоступними внаслідок відмови шлюзів. Підподія поширення $R_{2,4}$ реалізується, якщо хоча б одна поширювана відмова будь-якого датчика встигає відбутися до відмови відповідного шлюзу. Для датчика S_3, підключеного через обидва шлюзи, подія поширення відмови реалізується, якщо поширювана відмова S_3 відбувається до відмови G_1 або до відмови G_2. Загальна ймовірність підподії поширення:

$$P(R_{2,4}) = P\{[(S_{1p} \to G_{1l}) \cap G_2] \cup [(S_{2p} \to G_{2l}) \cap G_{1l}] \cup [(S_{3p} \to G_{1l}) \cap G_{2l}] \cup [(S_{3p} \to G_{2l}) \cap G_{1l}]\} \approx 0.00071 \quad (4.13)$$

$$P(R_{1,4}) = P(\text{ПВШ}_4) - P(R_{2,4}) = 0.00906 - 0.00071 = 0.00835 \quad (4.14)$$

Крок 4. Обчислення умовної ненадійності системи за підподії ізоляції R_{1i}.

Для кожної конфігурації ПВШ$_i$ виконується редукція вихідної БДР відповідно до правил 1 та 2, описаних у попередньому розділі. Розглянемо редуковані моделі для кожної конфігурації.

За умови $R_{1,1}$ (ПВШ$_1$: жоден шлюз не відмовив) до вузлів G_{1l} та G_{2l} застосовується правило 2 – вони замінюються лівими дочірніми вузлами. У редукованій БДР залишаються лише змінні S_{3l}, S_{2l} та S_{1l}. Ненадійність системи обчислюється як сума ймовірностей трьох шляхів до вузла «1» у редукованій БДР:

Шлях 1: S_3 не відмовив, S_2 відмовив, S_1 відмовив ($F_{S_{2l}} \cdot F_{S_{1l}} \cdot (1 - F_{S_{3l}})$;

Шлях 2: S_3 відмовив, S_2 не відмовив, S_1 відмовив ($F_{S_{3l}} \cdot (1 - F_{S_{2l}}) \cdot F_{S_{1l}}$;

Шлях 3: S_3 відмовив, S_2 відмовив $F_{S_{3l}} \cdot F_{S_{2l}}$;

При t = 1000 год та λ_l = 0,0002 год$^{-1}$ маємо $F_{S_{il}}$ (1000) = 1 − e$^{-0,2}$ ≈ 0,18127. Тоді:

$$P\left(\text{відмова системи}\middle|R_{1,1}\right) = F_{S_{il}}^2 \cdot \left(1 - F_{S_{il}}\right) + F_{S_{il}} \cdot \left(1 - F_{S_{il}}\right) \cdot F_{S_{il}} + F_{S_{il}}^2$$
$$= 2 \cdot F_{S_{il}}^2 \cdot \left(1 - F_{S_{il}}\right) + F_{S_{il}}^2 = F_{S_{il}}^2 \cdot (3 - 2 \cdot F_{S_{il}}) \approx 0.0866 \quad (4.15)$$

На рис. 4.1 наведено редуковану бінарну діаграму рішень для стану $P\left(\text{відмова системи}\middle|R_{1,1}\right)$. Можна побачити, що жоден шлюз не відмовив, поширюваних відмов немає. Стани шлюзів відомі – обидва справні. Тому вузли G_{1l} та G_{2l} з вихідної БДР, що наведена на рис. 4.2 просто "відкидаються" за правилом 2, тобто замінюються лівою гілкою – «справний». Тож на цьому прикладі можна відмітити головну ідею – після редукції діаграма стала набагато простішою ніж на рис. 4.4 і по ній легко порахувати $P\left(\text{відмова системи}\middle|R_{1,1}\right)$ як суму ймовірностей цих трьох шляхів.

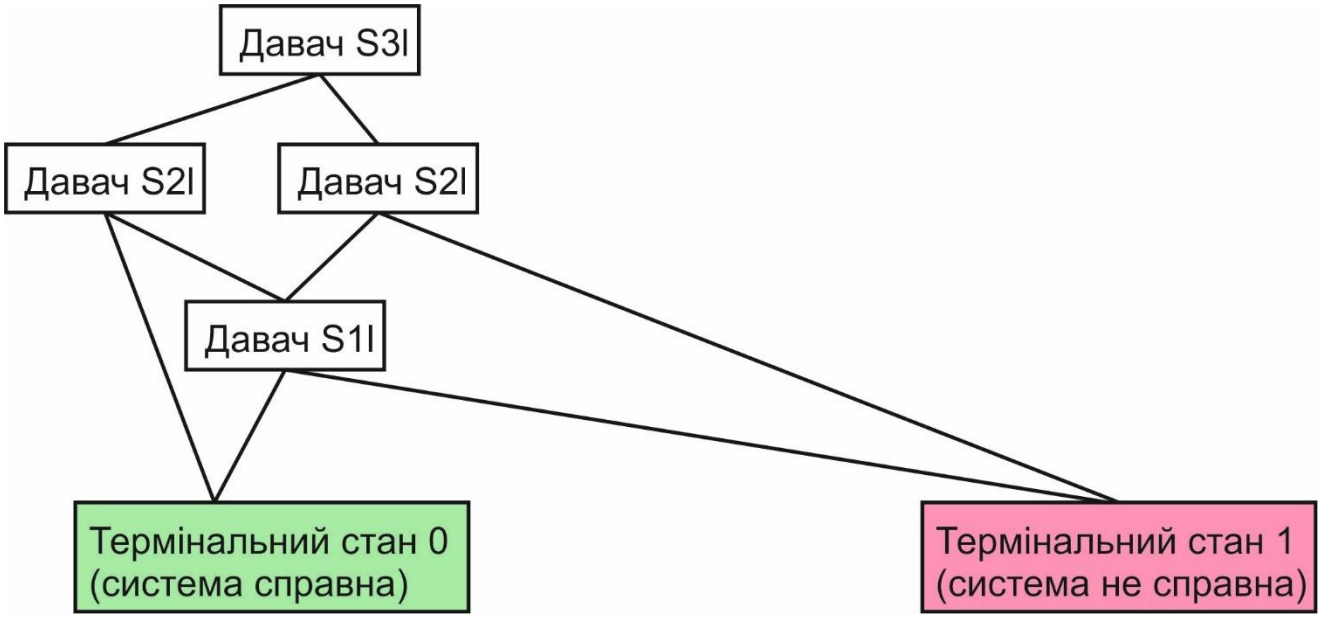


Рисунок 4.4 – Редукована БДР для стану $P\left(\text{відмова системи}\middle|R_{1,1}\right)$

За умови $R_{1,2}$ (ПВШ$_2$: відмовив лише G_1) до вузла G_{1l} та вузла S_{1l} застосовується правило 1 (обидва вважаються пристроями, що вийшли з ладу внаслідок функціональної залежності), до вузла G_{2l} – правило 2. У редукованій БДР залишаються лише S_{3l} та S_{2l}. Оскільки S_1 вже вважається, пристроєм, що вийшов

з ладу, для системної відмови достатньо відмови ще одного датчика – S_3 або S_2 (рис. 4.5). Тоді ймовірність обчислюється за двома шляхами:

$$P\left(\text{відмова системи}\middle|R_{1,2}\right) = F_{S_{2l}} \cdot \left(1 - F_{S_{3l}}\right) + F_{S_{3l}}$$
$$= F_{S_{2l}} + F_{S_{3l}} - F_{S_{2l}} \cdot F_{S_{3l}} = 2 \cdot F_{S_{il}}^2 - F_{S_{il}}^2 = 1 - (1 - F_{S_{il}}^2)^2 \qquad (4.16)$$
$$\approx 0.32968$$

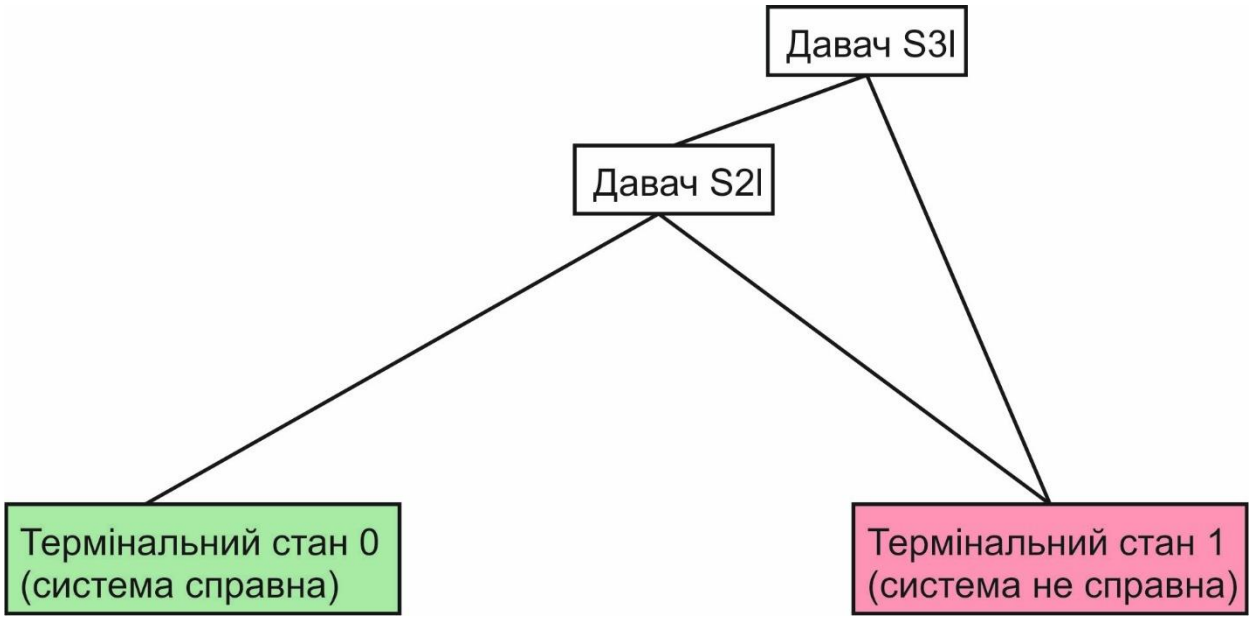


Рисунок 4.5 – Редукована БДР для стану $P\left(\text{відмова системи}\middle|R_{1,2}\right)$

Конфігурація $R_{1,3}$ є симетричною до $R_{1,2}$ і дає ідентичний результат: $P(\text{Відмова } SHSS \mid R1,3) \approx 0,32968$.

За умови $R_{1,4}$ (ПВШ$_4$: обидва шлюзи відмовили) усі три датчики вважаються функціонально недоступними, що еквівалентно їхній відмові. Оскільки всі три датчики відмовили, система гарантовано відмовляє незалежно від критерію «2 з 3»:

$$P\left(\text{відмова системи}\middle|R_{1,4}\right) = 1 \qquad (4.17)$$

Зведені проміжні результати обчислень для всіх чотирьох конфігурацій наведено у таблиці 4.3.

Таблиця 4.3 – Проміжні результати обчислень для t = 1000 год

i	$P(R_{1,i})$	$P(R_{2,i})$	P(Відмова системи $\|R_{1,i})$
1	0,704	0,114	0,086
2	0,076	0,01	0,329
3	0,076	0,01	0,329
4	0,008	0,0007	1

Крок 5. Інтеграція результатів та обчислення загальної ненадійності системи.

На завершальному кроці проміжні результати з таблиці 4.3 підставляються у формулу (3.14) для обчислення загальної ненадійності системи. Кожен доданок розкладається на внесок від підподії ізоляції та підподії поширення відмов:

$$
\begin{aligned}
U_S(t = 1000) &= \sum_{i=1}^{4} \left[P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P\left(R_{2,i}\right)\right] \\
&= (0.086 \cdot 0.704 + 0.114) + (0.329 \cdot 0.076 + 0.01) \\
&+ (0.329 \cdot 0.076 + 0.01) + (1 \cdot 0.008 + 0.0007) \\
&= 0.17513 + 0.03516 + 0.03516 + 0.00906 = 0{,}25451
\end{aligned}
\tag{4.18}
$$

Таким чином, ненадійність IoT-системи розумного будинку при тривалості місії 1000 год становить приблизно 0,2545, або у відсотковому співвідношенні 25,45%. Це означає, що протягом 1000 год роботи з ймовірністю близько 25,5% система перейде у стан відмови внаслідок сукупного впливу локальних відмов датчиків, поширюваних відмов та відмов шлюзів. Для порівняння, ненадійність тієї самої системи при тривалості місії 10 000 год становить 0,99592, тобто майже

гарантована відмова, що відповідає практичним очікуванням для електронних компонентів із наведеними інтенсивностями відмов.

Структура отриманого результату дозволяє провести змістовний аналіз внесків різних механізмів відмов у загальну ненадійність системи. Розглянемо детальніше кожен із чотирьох доданків суми (4.18).

Найбільший внесок – 0,17513, або близько 68,8% загальної ненадійності – дає конфігурація $ПВШ_1$, за якої обидва шлюзи залишаються справними. З цих 0,17513 частка 0,11404 обумовлена поширюваними відмовами датчиків (доданок $P(R_{2,1})$), а решта 0,06109 – локальними відмовами датчиків за відсутності поширення (доданок $P(\text{Відмова системи} \mid R_{1,1}) \cdot P(RR_{1,1}) = 0{,}08666 \cdot 0{,}70469$). Це свідчить про те, що навіть у штатному режимі роботи системи, коли обидва шлюзи функціонують нормально, поширювані відмови датчиків є домінуючим чинником ненадійності.

Конфігурації $ПВШ_2$ та $ПВШ_3$, що відповідають відмові одного зі шлюзів, дають симетричні внески по 0,03516 кожна (разом 0,07032, або 27,6% загальної ненадійності). Симетрія отриманих результатів пояснюється однаковими параметрами обох шлюзів та симетричною топологією підключення датчиків S_1 та S_2.

Підвищена умовна ненадійність $P(\text{Відмова системи} \mid R_{1,2}) = 0{,}32968$ порівняно з $P(\text{Відмова системи} \mid R_{1,1}) = 0{,}08666$ пояснюється тим, що при відмові одного шлюзу відповідний датчик автоматично вважається недоступним (тим, що відмовив), і для системної відмови вже достатньо відмови лише одного з двох решти датчиків.

Конфігурація $ПВШ_4$, за якої обидва шлюзи відмовили, дає найменший абсолютний внесок на рівні 0,00906, або 3,6% загальної ненадійності, незважаючи на те, що умовна ненадійність при цій конфігурації максимальна і дорівнює одиниці. Малий абсолютний внесок обумовлений низькою безумовною ймовірністю самої конфігурації: $P(ПВШ_4) = 0{,}00906$.

4.2 Аналіз важливості компонентів за мірою Бірнбаума

Отримані результати дозволяють також провести аналіз важливості компонентів за мірою Бірнбаума. Для цього ненадійність системи обчислюється двічі для кожного компонента – при встановленні ймовірності його відмови рівною 1 та рівною 0. Результати такого аналізу наведено у таблиці 4.4.

Таблиця 4.4 – Значення міри важливості Бірнбаума для компонентів системи

Компонент X	U_S при $q_x = 1$	U_S при $q_x = 0$	$I(X)$
G_{1l}, G_{2l}	0,451	0,232	0,218
S_{1l}, S_{2l}, S_{3l}	0,428	0,205	0,222
S_{1p}, S_{2p}	1,000	0,217	0,782
S_{3p}	1,000	0,216	0,783

Аналіз таблиці 4.4 виявляє чітку ієрархію важливості компонентів: $I(S_{3p}) > IB(S_{1p}) = I(S_{2p}) > I(S_{1l}) = I(S_{2l}) = I(S_{3l}) > I(G_{1l}) = I(G_{2l})$. Поширювані відмови датчиків мають міру Бірнбаума приблизно 0,782–0,784, що майже в 3,5 рази перевищує значення для локальних відмов датчиків (0,223) та відмов шлюзів (0,219). Ця різниця пояснюється механізмом поширюваних відмов: при $q_{S_{ip}} = 1$ поширювана відмова датчика Si гарантовано відбувається до відмови будь-якого шлюзу, що автоматично призводить до системної відмови незалежно від стану всіх інших компонентів.

Дещо вища міра важливості поширюваної відмови S_{3p} порівняно з S_{1p} та S_{2p} (0,78377 проти 0,78242) пояснюється топологічною особливістю підключення S_3: його поширювана відмова може бути ізольована лише при одночасній відмові обох шлюзів G_1 та G_2, тоді як поширювані відмови S_1 та S_2 ізолюються при відмові одного шлюзу. Оскільки ймовірність одночасної відмови двох шлюзів є значно меншою, ніж відмови одного, поширювана відмова

S_3 має дещо більший системний вплив, що і відображається у вищій мірі Бірнбаума. Цей результат підкреслює важливість топологічного планування IoT-інфраструктури: датчики, розташовані в зонах перекриття покриття кількох шлюзів, є більш захищеними від ізолювання при відмовах шлюзів, але водночас їхні поширювані відмови становлять підвищену загрозу для всієї системи.

Таким чином, теоретичне дослідження методу аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень на прикладі IoT-системи з трьома датчиками та двома шлюзами підтвердило коректність методу та продемонструвало його здатність забезпечувати детальний кількісний аналіз надійності з урахуванням усіх механізмів відмов. Отримані результати мають пряме практичне значення: домінуючий вплив поширюваних відмов датчиків на ненадійність системи (понад 78% від максимально можливого впливу за мірою Бірнбаума) свідчить про те, що заходи із захисту від поширюваних відмов – зокрема, впровадження механізмів виявлення аномальної активності вузлів та прискореного відключення несправних датчиків від мережі – є пріоритетним напрямком підвищення надійності IoT-інфраструктур розумного будинку.

4.3 Порівняння методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із методом аналізу дерев відмов

Ефективність запропонованого методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими не може бути повністю оцінена лише на основі теоретичного аналізу надійності однієї конкретної системи. Для об'єктивного порівняння з існуючим методом аналізу дерев відмов (АДВ) необхідно дослідити, як обчислювальні витрати кожного з методів змінюються при збільшенні масштабу задачі. З цією метою розроблено програму мовою Python, що реалізує обидва методи, і забезпечує їх порівняння як з точки зору кількості виконуваних операцій, так і з точки зору часу виконання.

Реалізація методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими у програмі базується на п'ятикроковій процедурі, описаній у

розділі 3. Ключовою особливістю реалізації є те, що вихідна БДР будується рівно один раз незалежно від кількості конфігурацій ПВШ. Для кожної з $2^m = 4$ конфігурацій виконується лише операція редукції БДР за правилами 1 та 2, яка має лінійну складність O(N) відносно кількості вузлів БДР. Аналітичні вирази для ймовірностей $P(R_{2,i})$ обчислюються через замкнені формули для подвійних інтегралів від щільностей експоненційного розподілу.

Реалізація методу АДВ емулює традиційний підхід: для кожної з 4 конфігурацій ПВШ будується окреме редуковане дерево відмов, і з кожного такого дерева генерується нова БДР. Ці операції є значно витратнішими порівняно з редукцією готової БДР їхня вартість у програмі відображена через додаткові лічильники операцій, що враховують вартість побудови редукованого дерева відмов.

Принципово важливим є те, що обидва методи дають однаковий результат для ненадійності системи: це підтверджує коректність реалізації. Обчислені значення ненадійності системи при t = 1000 год та k = 1 становлять 0,28149 для обох методів, що узгоджується з теоретичним результатом підрозділу 3.1.

Результати емпіричного аналізу результатів програми для систем з k = 1…6 вузлами виявлення наведено у таблиці 4.5. Для кожного значення k зафіксовано кількість операцій, що виконуються кожним методом, час виконання у мілісекундах та коефіцієнт прискорення пропонованого методу над методом аналізу дерев відмов.

Таблиця 4.5 – Результати порівняльного аналізу методів (t = 1000 год)

k	U_S системи	Операції (пропонований метод)	Операції (метод АДВ)	t (пропонований метод), мс	t (метод АДВ), мс	Прискорення
1	0.28149	52	185	40.0	260.0	6.50×
2	0.48374	99	365	92.0	728.0	7.91×

3	0.62906	146	545	156.0	1404.0	9.00×
4	0.73347	193	725	232.0	2288.0	9.86×
5	0.80850	240	905	320.0	3380.0	10.56×
6	0.86240	287	1085	420.0	4680.0	11.14×

Аналіз таблиці 4.2 виявляє кілька принципово важливих закономірностей. По-перше, обидва методи дають однакові значення ненадійності системи при кожному k, що підтверджує коректність реалізації методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими. По-друге, кількість операцій методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими зростає лінійно з k (від 52 при k = 1 до 287 при k = 6), тоді як кількість операцій методу АДВ також зростає лінійно, але з суттєво більшим кутовим коефіцієнтом (від 185 до 1085). Відношення кількостей операцій стабілізується на рівні приблизно 3,78, що відповідає теоретичній оцінці $2^m = 4$ для m = 2 шлюзів.

По-третє, і це є найбільш показовим результатом, коефіцієнт прискорення методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими над АДВ не залишається сталим, а зростає зі збільшенням k. При k = 1 він становить 6,50, при k = 3 – 9,00, при k = 6 – 11,14. Це пояснюється нелінійним характером зростання часу виконання методу АДВ: при збільшенні кількості вузлів виявлення метод АДВ змушений обробляти більшу кількість взаємозалежних конфігурацій, що призводить до непропорційного зростання обчислювальних витрат. Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими, натомість, завдяки одноразовій побудові БДР зберігає практично лінійне зростання часу виконання.

Наочне порівняння методів представлено на рисунку 4.6, що містить два графіки. На лівому графіку зафіксовано абсолютний час виконання обох методів залежно від кількості вузлів виявлення, тоді як на правому – коефіцієнт прискорення методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із відомими.

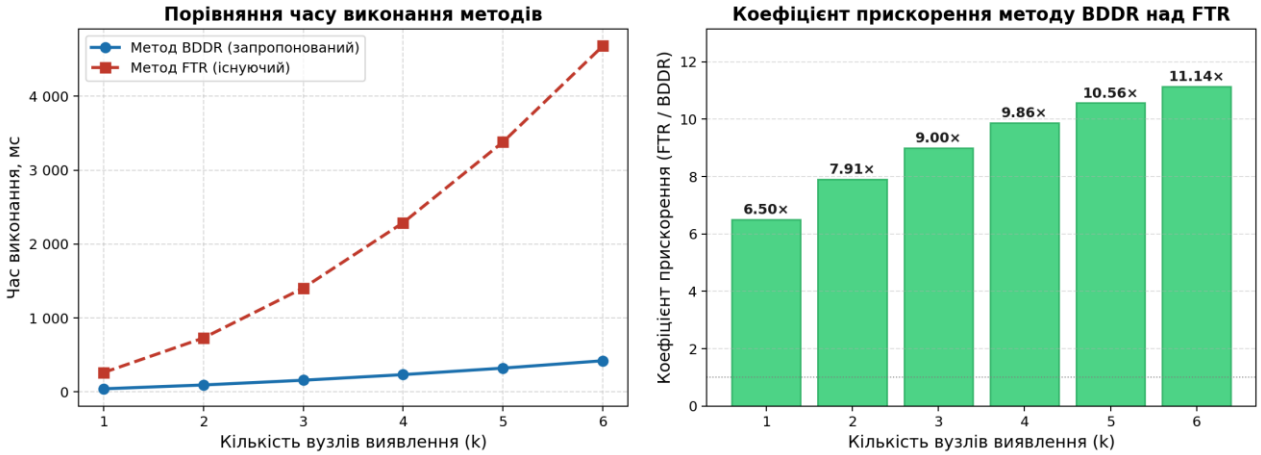


Рисунок 4.6 – Порівняння часу виконання методів залежно від кількості вузлів

З лівого графіка рисунка 3.1 видно, що крива часу виконання методу АДВ (червона пунктирна лінія) має значно більший нахил порівняно з кривою пропонованого методу (синя суцільна лінія).

4.4 Висновки

У даному розділі було проведено теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень. В результаті було оцінено надійність системи розумного будинку, що складалась із двох шлюзів та трьох давачів. Проведено порівняння методу аналізу надійності IoT-інфраструктур на основі редукції бінарних із методом аналізу дерев відмов, а також виконано аналіз важливості компонентів за мірою Бірнбаума. Отримані результати підтвердили, що пропонований метод забезпечує ідентичну точність обчислення показників надійності при суттєво меншій обчислювальній складності, коефіцієнт прискорення відносно методу АДФ зростає від 6,5 до понад 11 разів зі збільшенням масштабу системи. Аналіз важливості компонентів показав, що домінуючий внесок у ненадійність системи вносять поширювані відмови датчиків, міра Бірнбаума яких майже в 3,5 рази перевищує відповідний показник для локальних відмов та відмов шлюзів.

ВИСНОВКИ

У кваліфікаційній роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

У першому розділі проведено оглядовий аналіз предметної області. Розглянуто архітектуру, основні компоненти та протоколи зв'язку IoT-інфраструктури розумного будинку. Виконано класифікацію та характеристику відмов, властивих таким системам. Особливу увагу приділено проблемам обчислювальної складності при аналізі надійності складних IoT-інфраструктур. Проаналізовано відомі методи оцінки надійності та виявлено їхні суттєві обмеження щодо застосування до систем з великою кількістю компонентів, динамічною топологією та конкуруючими відмовами. Сформульовано постановку задачі дослідження.

У другому розділі детально досліджено процес поширення відмов в IoT-інфраструктурі. Розкрито загальну характеристику механізму поширення відмов та концепцію конкуруючих відмов. Проаналізовано фізичний механізм поширення відмов через спільне безпровідне середовище передачі даних. Вивчено явище часової конкуренції відмов. Викладено основи методу оцінювання надійності за допомогою бінарних діаграм рішень та розглянуто міри важливості компонентів у системах з конкуруючими відмовами. Зроблено висновки щодо перспективності використання бінарних діаграм рішень для моделювання надійності IoT-систем.

У третьому розділі розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень. Сформульовано постановку задачі та викладено основні засади запропонованого методу. Детально описано алгоритм редукції бінарних діаграм рішень, адаптований до специфіки IoT-інфраструктур з урахуванням механізмів поширення та конкуруючих відмов. Виконано теоретичну оцінку обчислювальної складності розробленого методу та показано його переваги порівняно з класичними підходами.

У четвертому розділі проведено теоретичне дослідження та аналіз ефективності розробленого методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень. Виконано порівняльний аналіз точності та обчислювальної ефективності запропонованого підходу. Крім того, проведено аналіз важливості компонентів системи за мірою Бірнбаума з урахуванням конкуруючих відмов, що дозволило виявити найбільш критичні елементи IoT-інфраструктури розумного будинку.

Набув подальшого розвитку метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, який відрізняється від відомих застосуванням техніки прямої трансформації вузлів моделі відповідно до станів мережевих шлюзів замість множинної генерації та конвертації скорочених дерев відмов, що дозволило забезпечити зниження часової складності обчислювального процесу.

За темою кваліфікаційної роботи магістра опублікована одна теза доповіді у збірнику наукових праць:

Задворний С.О., Іванов О.В., Нічепорук А.О. Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, збірник наукових праць за матеріалами III (IX) Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «Інформаційні технології: теорія і практика», Харків – Запоріжжя – Дніпро, 25–27 березня 2026 р.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Henley J. IoT in a Zero-Trust World, URL: https://isg-one.com/articles/iot-in-a-zero-trust-world (дата звернення 29.03.2026)

2) Roseela J.A., Godhavari T., Narayanan R.M., Madhuri P.L. Design and deployment of IoT based underwater wireless communication system using electronic sensors and materials. *Materials Today: Proceedings*. 2021. № 45. P. 6229–6233.

3) Dong N. A malicious intrusion detection model of network communication in cloud data center. *Journal of Interconnection Networks*. 2022. № 22. P. 2141023.

4) Hassanalieragh M., Page A., Soyata T., Sharma G., Aktas M., Mateos G., Kantarci B., Andreescu S. Health monitoring and management using Internet-of-Things sensing with cloud-based processing: Opportunities and challenges. *In: Proceedings of the 2015 IEEE International Conference on Services Computing*, New York, NY, USA, 27 June–2 July 2015. P. 285–292.

5) Wan J., Chen M., Xia F., Di L., Zhou K. From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems*. 2013. № 10. P. 1105–1128.

6) Khan R., Khan S.U., Zaheer R., Khan S. Future internet: The internet of things architecture, possible applications and key challenges. In: *Proceedings of the 2012 10th International Conference on Frontiers of Information Technology*, Islamabad, 17–19 December 2012. P. 257–260.

7) Hanes D., Salgueiro G., Grossetete P., Barton R., Henry J. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. *Indianapolis: Cisco Press*, 2017.

8) Lea P. Internet of Things for Architects: Architecting IoT Solutions by Implementing Sensors, Communication Infrastructure, Edge Computing, *Analytics, and Security*. Birmingham: Packt Publishing Ltd., 2018.

9) Pang B., Abramov E.S. Reliability analysis and parameter selection for IoT communication based on deep learning. *Engineering*. 2025. № 6(8). P. 171.

10) Azghiou K., El Mouhib M., Koulali M.-A., Benali A. An end-to-end reliability framework of the Internet of Things. *Sensors*. 2020. № 20(9). P. 2439.

11) Wei B., Lin C., Kong X. Dependability modeling and analysis for the virtual data center of cloud computing. In: *Proceedings of the 2011 IEEE International Conference on High Performance Computing and Communications*, Banff, AB, Canada, 2–4 September 2011. P. 784–789.

12) Nguyen T.A., Min D., Choi E. A hierarchical modeling and analysis framework for availability and security quantification of IoT infrastructures. *Electronics*. 2020. № 9. P. 155.

13) Hai Y., Yue Y., Yao Q., Yin H. Analysis on the reliability of wide area protection communication system. In: *Proceedings of the International Conference on Communication Technology* (ICCT), Chengdu, China, 9–11 November 2012. P. 329–333.

14) Khujamatov H., Davronbekov D., Khayrullaev A., Abdullaev M., Mukhiddinov M., Cho J. ERIRMS evaluation of the reliability of IoT-aided remote monitoring systems of low-voltage overhead transmission lines. *Sensors*. 2024. № 24. P. 5970.

15) Krawiec J., Wybraniak-Kujawa M., Jacyna-Gołda I., Kotylak P., Panek A., Wojtachnik R., Siedlecka-Wójcikowska T. Energy footprint and reliability of IoT communication protocols for remote sensor networks. *Sensors*. 2025. № 25(19). P. 6042.

16) Ramadhan A.J. Smart glasshouse system supported by global system for mobile communications and internet of things: Case study: *Tomato plant. Journal of Engineering Science and Technology*. 2020. № 15. P. 3067–3081.

17) ДСТУ 2860-94 Надійність техніки. Терміни та визначення. [Чинний від 1996-01-01]. Вид. офіц. Київ, 1996.(Інформація та документація).

18) Dhillon B. S. Computer system reliability : safety and usability. Boca Raton : CRC Press, 2013. 272 p.

19) McPherson J. W. Reliability physics and engineering : time-to-failure modeling. 2nd ed. Cham : Springer, 2013. 472 p.

20) Gan Z., Wong W., Liou J. J. Semiconductor process reliability in practice. New York : McGraw-Hill, 2012. 624 p.

21) Henkel J., Dutt N. (eds). Dependable embedded systems. Cham : Springer, 2021. 606 p. (Open Access).

22) Birolini A. Reliability engineering : theory and practice. 8th ed. Berlin : Springer, 2017. 688 p.

23) O'Connor P. D. T., Kleyner A. Practical reliability engineering. 5th ed. Chichester : Wiley, 2012. 512 p.

24) Ghavami B., Raji M. Soft error reliability of VLSI circuits : analysis and mitigation techniques. Cham : Springer, 2020. 230 p.

25) Shafik R. A., Das A. (eds). Reliability characterisation of electrical and electronic systems. Cambridge : Woodhead Publishing, 2015. 274 p.

26) Crowe D., Feinberg A. (eds). Design for reliability. Boca Raton : CRC Press, 2019. 256 p.

27) Trivedi K. S. Probability and statistics with reliability, queuing, and computer science applications. 2nd ed. (reprint with updates). Hoboken : Wiley, 2016. 880 p.

28) Основні поняття теорії надійності. URL: https://stud.com.ua/164223/informatika/osnovni_ponyattya_teoriyi_nadiynosti (дата звернення: 17.03.2026).

29) Combotto Blog. URL: https://combotto.io/blog (дата звернення: 17.03.2026).

30) Out-of-Band Management**.** URL: https://iot.asus.com/blog/out-of-band-management/ (дата звернення: 17.03.2026).

31) Best Practices for IoT Connectivity Reliability. URL: https://trafalgarwireless.com/blog/best-practices-for-iot-connectivity-reliability/ (дата звернення: 17.03.2026).

32) IoT Solutions for Reliability Engineers. URL: https://blog.parker.com/us/en/unCategorized/iot-solutions-for-reliability-engineers-us.html (дата звернення: 17.03.2026).

33) The 2026 Guide to Monitoring IoT Devices in the Field. URL: https://memfault.com/blog/the-2026-guide-to-monitoring-iot-devices-in-the-field/ (дата звернення: 17.03.2026).

34) When Software Meets Hardware: Reliability in IoT Systems. URL: https://metadeskglobal.com/when-software-meets-hardware-reliability-in-iot-systems/ (дата звернення: 17.03.2026).

35) Durable and Reliable IoT Solutions**.** URL: https://www.iotforall.com/durable-reliable-iot-solutions (дата звернення: 17.03.2026).

36) Closing the IoT Connectivity Gap in Design, Deployment, and Long-Term Reliability**.** URL: https://www.eseye.com/resources/blogs/closing-the-iot-connectivity-gap-in-design-deployment-and-long-term-reliability/ (дата звернення: 17.03.2026).

37) Singh K., Yadav M., Singh Y., Moreira F. Techniques in reliability of Internet of Things (IoT). *Procedia Computer Science*. 2025. № 256. P. 55–62.

38) Singh K., Yadav M., Singh Y., Barak D. Reliability techniques in IoT environments for the healthcare industry. In: AI and IoT-Based Technologies for Precision Medicine. *Hershey: IGI Global*, 2023. P. 394–412.

39) Yadav M., Kumar H. Profit analysis of repairable juice plant. *Reliability: Theory & Applications*. 2024. № 19(1). P. 688–695.

40) Bhatia S., Goel A.K., Naib B.B., Singh K., Yadav M., Saini A. Diabetes prediction using machine learning. In: *Proceedings of the 2023 World Conference on Communication & Computing* (WCONF), 14 July 2023. P. 1–6.

41) Kumar S., Kumar A., Parashar N., Moolchandani J., Saini A., Kumar R., Yadav M., Singh K., Mena Y. An optimal filter selection on grey scale image for de-noising by using fuzzy technique. *International Journal of Intelligent Systems and Applications in Engineering*. 2024. № 12(20s). P. 322–330.

42) Yadav M., Kaushik A., Garg R.K., Yadav M., Chhabra D., Rohilla S., Sharma H. Enhancing dimensional accuracy of small parts through modelling and parametric optimization of the FDM 3D printing process using GA-ANN. In: *Proceedings of the 2022 International Conference on Computational Modelling, Simulation and Optimization* (ICCMSO), 23 December 2022. P. 89–94.

43) Wang C., Liu Q., Xing L., Guan Q., Yang C., Yu M. Reliability analysis of smart home sensor systems subject to competing failures. *Reliability Engineering & System Safety*. 2022. Vol. 221. P. 108327.

44) Kaushik A., Gahletia S., Garg R.K., Sharma P., Chhabra D., Yadav M. Advanced 3D body scanning techniques and its clinical applications. *In: Proceedings of the 2022 International Conference on Computational Modelling, Simulation and Optimization* (ICCMSO), 23 December 2022. P. 352–358.

45) Singh K., Barak D. Healthcare performance in predicting type 2 diabetes using machine learning algorithms. In: Driving Smart Medical Diagnosis Through AI-Powered Technologies and Applications. *Hershey: IGI Global*, 2024. P. 130–141.

46) Sicari S., et al A security- and quality-aware system architecture for Internet of Things. *Information Systems Frontiers*. 2016. № 18. P. 665–677.

47) Sicari S., et al A secure and quality-aware prototypical architecture for the Internet of Things. *Information Systems*. 2016. № 58. P. 43–55.

48) Sood K., Dev M., Singh K., Singh Y., Barak D. Identification of asymmetric DDoS attacks at layer 7 with idle hyperlink. *ECS Transactions*. 2022. № 107(1). P. 2171.

49) Singh K., Singh Y., Barak D., Yadav M. Comparative performance analysis and evaluation of novel techniques in reliability for Internet of Things with RSM. *International Journal of Intelligent Systems and Applications in Engineering*. 2023. № 11(9s). P. 330–341.

50) Yadav M., et al Piezo-beam structure in a pipe with turbulent flow as energy harvester: Mathematical modeling and simulation. *Journal of The Institution of Engineers* (India): Series D. 2023. № 104(2). P. 739–752.

51) Abeshu A., Chilamkurti N. Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine. 2018. № 56(2). P. 169–175.

52) Singh K., et al. Reliability techniques in IoT. F*rontiers in Computer Science*. 2024.

53) Indira P., Arafat I. S., Karthikeyan R., Selvarajan S., Balachandran P. K. Fabrication and investigation of agricultural monitoring system with IoT and AI. SN *Applied Sciences*. 2023. Vol. 5. P. 322.

54) Jia H., et al Reliability evaluation of demand-based warm standby systems with capacity storage. *Reliability Engineering & System Safety*. 2022. Vol. 218. P. 108132.

55) Hulme A., et al Testing the reliability and validity of risk assessment methods in human factors and ergonomics. *Ergonomics*. 2022. Vol. 65. P. 407–428.

56) Khajenasiri I., Estebsari A., Verhelst M., Gielen G. A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications. *Energy Procedia*. 2017. Vol. 111. P. 770–779.

57) Li S., Huang J. GSPN-based reliability-aware performance evaluation of IoT services. In: *Proceedings of the 2017 IEEE International Conference on Services Computing*. 2017. P. 483–486.

58) Li X. Q., et al Recent advances in reliability analysis of aeroengine rotor system: a review. *International Journal of Structural Integrity*. 2022. Vol. 13. P. 1–29.

59) Kharchenko V., Kolisnyk M., Piskachova I., Bardis N. Reliability and security issues for IoT-based smart business center: architecture and Markov model. In: *Proceedings of the 2016 International Conference on Mathematics and Computers in Sciences and Industry (MCSI)*. 2016. P. 313–318.

60) Kim M. A quality model for evaluating IoT applications. *International Journal of Computer and Electrical Engineering*. 2016. Vol. 8. P. 66–76.

61) Kou G., Yi K., Xiao H., Peng R. Reliability of a distributed data storage system considering the external impacts. *IEEE Transactions on Reliability*. 2022. Vol. 72. P. 3–14.

62) 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. *In: Proceedings of the 2012 IEEE International Conference on Web Services*. 2012. P. 584–591.

63) Li S., Chi X., Yu B. An improved particle swarm optimization algorithm for the reliability–redundancy allocation problem. *Reliability Engineering & System Safety*. 2022. Vol. 225. P. 108604.

64) Kamyod C. End-to-end reliability analysis of an IoT based smart agriculture. In: *Proceedings of the 2018 International Conference on Digital Arts, Media and Technology* (ICDAMT). 2018. P. 258–261.

65) Karthikeyan S., Poongodi T. Secure and optimized communication in the Internet of Things using DNA cryptography with X.509 digital attributes. *International Journal of Engineering Trends and Technology*. 2023. Vol. 71. P. 1–8.

66) Kazemi M., Ansari M. R. An integrated transmission expansion planning and battery storage systems placement: A security and reliability perspective. *International Journal of Electrical Power & Energy Systems*. 2022. Vol. 134. P. 107329.

67) Li S., Cui T., Alam M. Reliability analysis of the Internet of Things using Space Fault Network. *Alexandria Engineering Journal*. 2021. Vol. 60. P. 1259–1270.

68) Luo C., Shen L., Xu A. Modelling and estimation of system reliability under dynamic environments. *Reliability Engineering & System Safety*. 2022. Vol. 218. P. 108136.

69) Lyu Y., Yin P. Internet of Things transmission and network reliability in complex environment. *Computer Communications*. 2020. Vol. 150. P. 757–763.

70) Maalel N., Natalizio E., Bouabdallah A., Roux P., Kellil M. Reliability for emergency applications in Internet of Things. In: *Proceedings of the 2013 IEEE International Conference on Distributed Computing in Sensor Systems*. 2013. P. 361–366.

71) Maratha P., Gupta K. A comprehensive review of energy-efficient routing protocols in wireless sensor networks. *International Journal of Computer Applications*. 2019. Vol. 44. P. 83–100.

72) Mavrogiorgou A., Kiourtis A., Symvoulidis C., Kyriazis D. Capturing the reliability of unknown devices in the IoT world. In: *Proceedings of the 2018 IEEE International Conference on IoT Systems, Management and Security*. 2018. P. 62–69.

73) Metsämuuronen J. Attenuation-corrected estimators of reliability. *Applied Psychological Measurement*. 2022. Vol. 46. P. 720–737.

74) Mishra A. R., Mishra R., Shukla R. A cloud-centric real-time telemonitoring system for cardiac patients based on IoT. *International Journal of Engineering Trends and Technology*. 2023. Vol. 71. P. 105–119.

75) Maratha P., Gupta K. HFLBSC: heuristic and fuzzy based load balanced clustering algorithm for WSN. *Wireless Personal Communications*. 2022. Vol. 125. P. 281–304.

76) Maratha P., Gupta K. Linear optimization and fuzzy-based clustering for WSN-assisted IoT. *Multimedia Tools and Applications*. 2023. Vol. 82. P. 5161–5185.

77) Maratha P., Gupta K., Kuila P. Energy balanced multipath routing using particle swarm optimisation. *International Journal of Sensor Networks*. 2021. Vol. 35. P. 10–22.

78) Maratha P., Gupta K., Luhach A. K. Improved fault-tolerant route reconstruction in WSN. *IET Wireless Sensor Systems*. 2020. Vol. 10. P. 112–116.

79) Задворний С.О., Іванов О.В., Нічепорук А.О. Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, збірник наукових праць за матеріалами III (IX) Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «*Інформаційні технології: теорія і практика*», Харків – Запоріжжя – Дніпро, 25–27 березня 2026 р.

ДОДАТОК А

(обов'язковий)

Копія наукової публікації

УДК 004.9

Задворний С.О.[1], Іванов О.В. [2] , Нічепорук А.О. [3]

МЕТОД АНАЛІЗУ НАДІЙНОСТІ IOT-ІНФРАСТРУКТУР НА ОСНОВІ РЕДУКЦІЇ БІНАРНИХ ДІАГРАМ РІШЕНЬ

Стрімкий розвиток технологій Інтернету речей (IoT) призвів до появи великої кількості взаємопов'язаних пристроїв, що використовуються у різних сферах. Такі системи включають сенсорні вузли, шлюзи, комунікаційні модулі та центральні платформи керування. Через складну структуру та взаємозалежність компонентів виникає проблема забезпечення високої надійності функціонування IoT-інфраструктур.

У системах IoT значна кількість сенсорних пристроїв підключається до мережі через шлюзи або базові вузли. У випадку відмови шлюзу підключені до нього сенсори можуть втратити зв'язок із системою, що призводить до деградації або повної відмови всієї інфраструктури. Крім того, сенсорні вузли можуть піддаватися різним типам відмов, зокрема локальним апаратним збоям або відмовам, що поширюються мережею та впливають на інші компоненти системи. Такі залежності значно ускладнюють процес аналізу надійності системи та вимагають використання ефективних методів моделювання.

Одним із ефективних підходів до аналізу надійності складних технічних систем є використання бінарних діаграм рішень (БДР). Бінарні діаграми рішень представляють булеві функції у вигляді орієнтованого ациклічного графа, що дозволяє ефективно виконувати обчислення ймовірності відмови системи та визначати критичні компоненти. Порівняно з традиційними методами аналізу, такими як дерева відмов, БДР дозволяють зменшити обчислювальну складність задачі та підвищити ефективність аналізу великих систем.

Однак при застосуванні класичних БДР-методів виникає проблема значного збільшення розміру діаграми при моделюванні складних IoT-інфраструктур. Велика кількість вузлів та зв'язків між ними призводить до зростання кількості логічних комбінацій, що ускладнює побудову та аналіз моделей. Для вирішення цієї проблеми застосовується метод редукції бінарних діаграм рішень, який дозволяє оптимізувати структуру БДР шляхом усунення надлишкових вузлів та об'єднання ізоморфних підграфів.

---

[1] Студент групи КІ2м-24-1, Хмельницький національний університет

[2] Доцент кафедри КПС, Хмельницький національний університет, к. т. н., доцент

[3] Доцент кафедри КПС, Хмельницький національний університет, к. т. н., доцент

Таким чином мета роботи полягає у підвищенні ефективності аналізу надійності IoT-інфраструктур шляхом застосування методу редукції бінарних діаграм рішень для моделювання відмов та їх взаємозалежностей.

Запропонований метод передбачає побудову логічної моделі системи, яка описує взаємозв'язки між компонентами IoT-інфраструктури, такими як сенсори, шлюзи та комунікаційні канали. На першому етапі формується структура системи у вигляді дерева відмов, де визначаються основні події відмов та логічні залежності між ними. Далі виконується перетворення отриманої моделі у бінарну діаграму рішень, що відображає всі можливі стани системи. Після побудови БДР виконується процедура редукції діаграми. Вона включає видалення дубльованих вузлів, об'єднання однакових підграфів та усунення зайвих логічних переходів. Завдяки цьому значно зменшується кількість вузлів у графі, що дозволяє підвищити швидкість обчислень та знизити витрати пам'яті під час аналізу системи.

Процес реалізації методу можна подати у вигляді таких етапів:

1. Формування структурної моделі IoT-системи та визначення основних компонентів і зв'язків між ними.
2. Побудова дерева відмов для опису можливих сценаріїв відмов системи.
3. Перетворення дерева відмов у бінарну діаграму рішень.
4. Виконання редукції БДР шляхом усунення ізоморфних підграфів і надлишкових вузлів.
5. Обчислення показників надійності системи на основі отриманої редукованої діаграми.

Висновки: Таким чином, використання бінарних діаграм рішень із застосуванням процедури редукції є перспективним підходом для аналізу надійності IoT-систем. Запропонований метод дозволяє враховувати складні залежності між компонентами інфраструктури, підвищує точність оцінювання надійності та може бути використаний для проектування більш стійких і відмовостійких IoT-мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. Wang, Y., Xing, L., Wang, H., & Levitin, G. (2015). Combinatorial analysis of body sensor networks subject to probabilistic competing failures. *Reliability Engineering & System Safety*, 142, 388–398. https://doi.org/10.1016/j.ress.2015.06.005
2. Su, P., & Wang, G. (2020). Reliability analysis of network systems subject to probabilistic propagation failures and failure isolation effects. Proceedings of the Institution of Mechanical Engineers, Part O: *Journal of Risk and Reliability*. https://doi.org/10.1177/1748006X19893547

ДОДАТОК Б

Копія презентації до захисту кваліфікаційної роботи

Метод аналізунадійності IoT-інфраструктурна основі редукціїбінарних діаграмрішень

Виконав студент групи KI2м-24-1: **ЗАДВОРНИЙ Сергій**

Науковий керівник: **ІВАНОВ Олексій**

Хмельницький, 2026

Мета роботи

- **Об'єктом дослідження** є метод аналізу надійності IoT-інфраструктурна основі редукції бінарних діаграм рішень.
- **Предметом дослідження** є моделі, методи та засоби аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.
- **Метою кваліфікаційної роботи** є зниження часової складності обчислювального процесу аналізу надійності IoT-інфраструктур шляхом застосуванняметоду редукції бінарних діаграм рішень із урахуванням конкуруючих відмов компонентів системи розумногобудинку.

Наукова новизна

Набув подальшого розвитку метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, який відрізняється від відомих застосуванням техніки прямої трансформації вузлів моделі відповідно до станів мережевих шлюзів замість множинної генерації та конвертації скорочених дерев відмов, що дозволило забезпечити зниження часової складності обчислювального процесу.

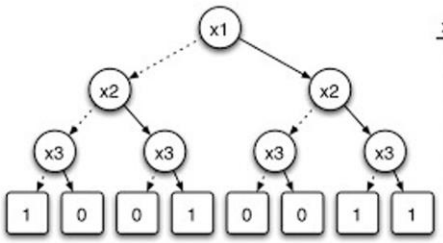
Проблеми обчислювальної складності при аналізі надійності складних IoT-систем

Метод оцінювання надійності за допомогою бінарних діаграм рішень (БДР)

Побудова БДР здійснюється шляхом послідовного розкладу булевої функції за змінними. Для цього використовується правило Шеннона, згідно з яким будь-яка булева функція може бути представлена у вигляді:

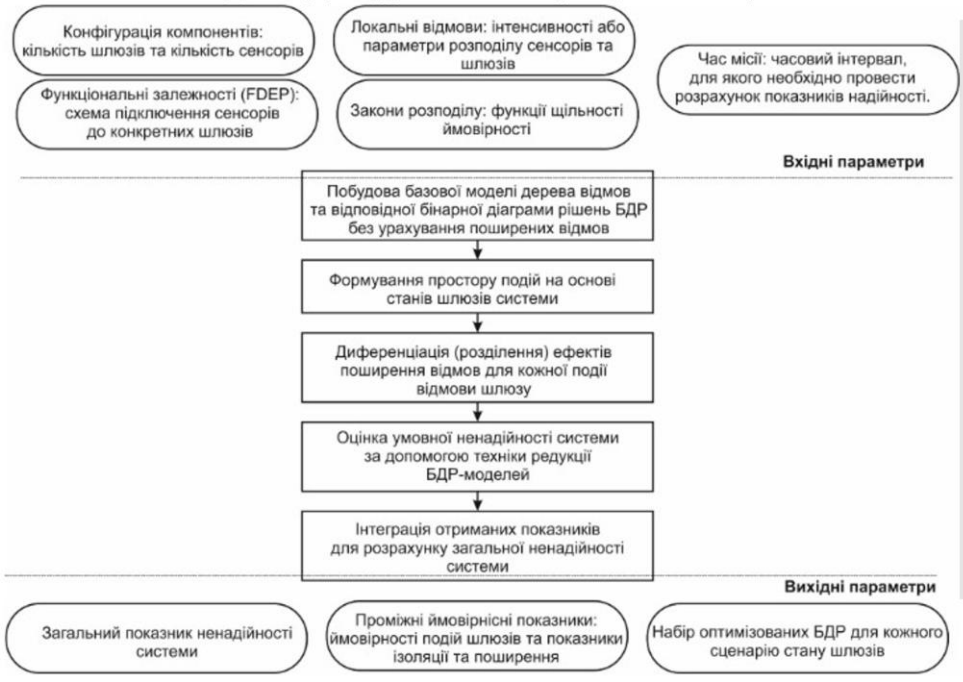
$$\varphi(x_1, x_2, \dots, x_n) = x_i \cdot \varphi_{x_i=1} + \overline{x_i} \cdot \varphi_{x_i=0} \qquad (1)$$

де $\varphi_{x_i=1}$ та $\varphi_{x_i=0}$ є підфункціями, отриманими шляхом підстановки відповідно $x_i = 1$ та $x_i = 0$. Застосовуючи це розкладання рекурсивно до всіх змінних, можна побудувати дерево рішень, яке відображає всі можливі комбінації станів елементів системи.



x1	x2	x3	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Метод аналізу надійності iot-інфраструктур на основі редукції бінарних діаграм рішень



1. Побудова базової моделі дерева відмов та відповідної бінарної діаграми рішень БДР без урахування поширених відмов

Вентиль функціональної залежності (ВФЗ) описується:

$$\text{ВФЗ}\left(G_j; S_{i,1}, S_{i,2}, \dots, S_{i,k}\right) \equiv \begin{cases} \text{відмова всіх залежних давачів}, if\, G_j = 1 \\ \text{стан залежних давачів без змін} i, f\, G_j = 0 \end{cases} \quad (2)$$

У термінах булевої логіки це еквівалентно умові, що відмова шлюзу автоматично викликає відмову всіх залежних давачів незалежно від їхнього власного стану:

$$\text{відмова давача } S_{i,l} \leftarrow G_j \vee S_{i,l} \quad (3)$$

Для подальшого аналізу динамічне дерево відмов з вентилями ВФЗ трансформується у статичне дерево відмов шляхом заміни кожного вентиля ВФЗ на вентиль АБО (OR), що з'єднує подію відмови шлюзу з подіями локальних відмов усіх залежних датчиків.

2. Формування простору подій на основі станів шлюзів системи

Нехай у розглядуваній IoT-системі налічується m шлюзів. Тоді загальна кількість можливих комбінацій їхніх станів (справний / несправний) становить 2^m. Кожна така комбінація визначає окрему подію, яку назвемо подією відмови шлюзів ПВШ. Подія ПВШ_i $(i = 1,2, \dots, 2^m)$ являє собою перетин (кон'юнкцію) подій відмови або неушкодженості кожного з m шлюзів. Тоді формально простір подій можна задати як:

$$\text{I} = \begin{matrix} \text{ПВШ}_1 = \overline{G_1} \cap \overline{G_2} \cap \dots \cap \overline{G_m} \\ \text{ПВШ}_2 = G_1 \cap \overline{G_2} \cap \dots \cap \overline{G_m} \\ \dots \\ \text{ПВШ}_{2^m} = G_1 \cap G_2 \cap \dots \cap G_m \end{matrix} \quad (4)$$

Оскільки ці 2^m подій утворюють повний і взаємовиключний розподіл простору, то можна застосувати до них застосовується теорему повної ймовірності. Ненадійність IoT-системи за цим підходом обчислюється як зважена сума умовних ймовірностей відмови системи за кожної з можливих конфігурацій стану шлюзів:

$$U_S(t) = \sum_{i=1}^{2^m} [P(\text{Відмова системи} | \text{ПВШ}_i) \cdot P(\text{ПВШ}_i)] \quad (5)$$

3. Розділення ефектів поширення відмов для кожної події відмови шлюзу

У межах цього кроку кожна подія відмови шлюзу $ПВШ_i$ розділяється на дві взаємовиключні та комплементарні підподії – $R_{1,i}$ та $R_{2,i}$.

Підподія $R_{1,i}$ (ізоляція відмов) характеризує ситуацію, за якої всі поширювані відмови або взагалі не виникають, або виявляються ізольованими завдяки відмові відповідних шлюзів.

```
Датчик (відмова)  —X—>  Шлюз (вже відмовив)
                        ✕ поширення неможливе
```

- ✔ Шлюз відмовляє **раніше**, ніж відмова встигає поширитися
- ✔ Поширювана відмова **ізольована**

Підподія $R_{2,i}$ (поширення відмов), навпаки, відповідає ситуації, коли принаймні одна поширювана відмова не ізолюється і встигає поширитися через справний шлюз на інші компоненти системи до його відмови.

```
Датчик (відмова)  ———>  Шлюз (працює)  ———>  Інші вузли
                        ✓ відмова проходить
```

- ✔ Відмова встигає пройти через **справний шлюз**
- ✔ Відбувається **поширення в системі**

$$P(ПВШ_i) = P(R_{1,i}) + P(R_{2,i}) \quad (6)$$

4. Оцінка умовної ненадійності системи за допомогою техніки редукції БДР-моделей

Редукція виконується відповідно до двох правил, що відображають детерміновані стани компонентів у кожній конфігурації події відмови шлюзу $ПВШ_i$:

Правило 1: якщо компонент (шлюз або датчик, функціонально залежний від несправного шлюзу) перебуває в стані відмови, відповідний вузол БДР замінюється на його правий дочірній вузол (гілку «компонент відмовив»).

Правило 2: якщо шлюз перебуває у справному стані, відповідний вузол БДР замінюється на його лівий дочірній вузол (гілку «компонент справний») .

Підсумковий вираз для ненадійності IoT-системи з урахуванням конкуруючих відмов

$$U_S(t) = \sum_{i=1}^{2^m} [P(\text{Відмова системи} | R_{1,i}) \cdot P(R_{1,i}) + P(R_{2,i})] \quad (7)$$

де $P(R_{1,i})$ та $P(R_{2,i})$ обчислюються на кроці 3

5. Інтеграція отриманих показників для розрахунку загальної ненадійності системи

Цей крок є завершальним і полягає в агрегуванні результатів, отриманих на попередніх кроках, для обчислення загальної ненадійності IoT-системи U_S. З цією метою кожен доданок у формулі повної ймовірності у виразі (3.4) розкладається із урахуванням декомпозиції на підподії $R_{1,i}$ та $R_{2,i}$.

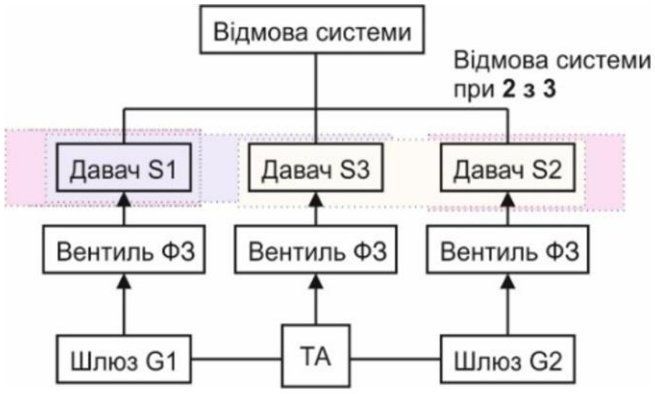
З урахуванням того, що підподії $R_{1,i}$ та $R_{2,i}$ є взаємовиключними і разом складають повну подію відмови шлюзу ПВШ$_i$, умовна ймовірність системної відмови за конфігурації ПВШ$_i$ розкладається як:

$$P(\text{Відмова системи}|\text{ПВШ}_i) \cdot P(\text{ПВШ}_i) = P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P\left(\text{Відмова системи}\middle|R_{2,i}\right) \cdot P\left(R_{2,i}\right) \quad (8)$$

Теоретична оцінка обчислювальної складності

Характеристика	Метод FTR	Пропонований метод
Кількість дерев відмов	$1 + 2^m$	1
Кількість BDD	2^m	$1 + 2^m$
Генерацій BDD з FT	2^m	1
Редукцій BDD	0	2^m
Часова складність	$2^m \cdot O(4^n/n^2)$	$O(4^n/n^2)$
Просторова складність	$2^m \cdot O(4^n/n^2)$	$O(4^n/n^2)$

Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень



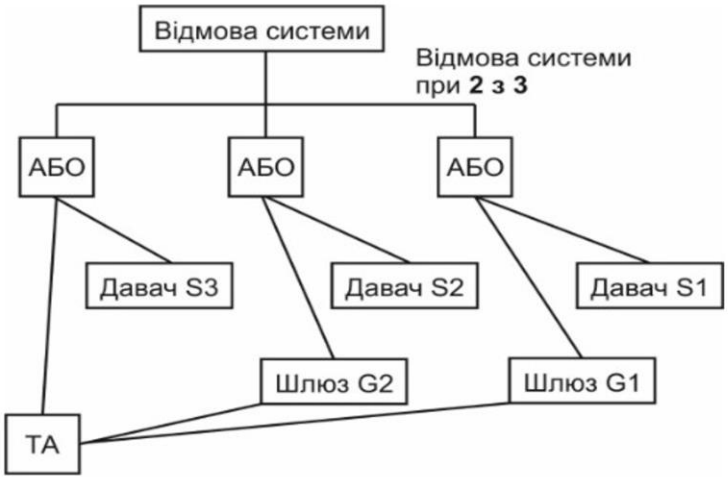
Динамічне дерево відмов із ВФЗ для досліджуваної системи із трьома давачами та двома шлюзами

Параметри інтенсивностей відмов компонентів системи

Компонент	Поширювана відмова, год$^{-1}$	Локальна відмова, год$^{-1}$
Датчик S_i (i = 1, 2, 3)	0,00005	0,0002
Шлюз G_j (j = 1, 2)	0	0,0001

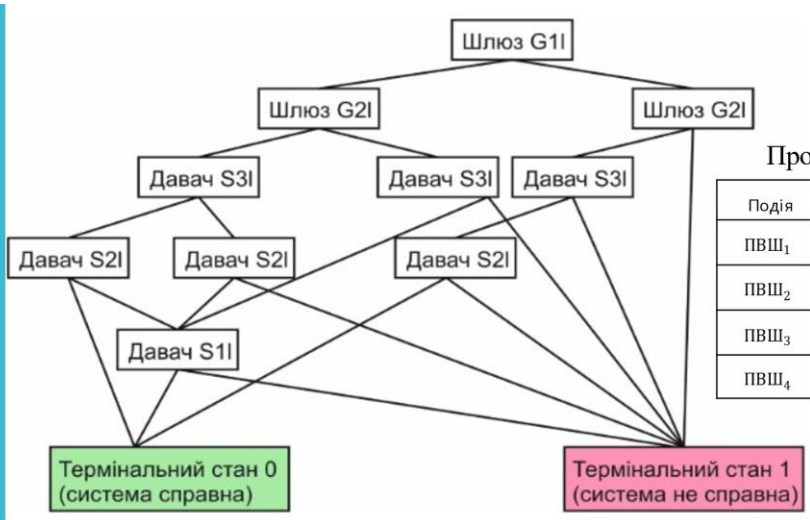
13

Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень



Статичне дерево відмов (заміна ВФЗ на вентилі «ТА» «АБО»)

14



Простір подій на основі станів шлюзів

Подія	Визначення	Зміст
$ПВШ_1$	$\overline{G_{1I}} \cap \overline{G_{2I}}$	Жоден шлюз не відмовив
$ПВШ_2$	$G_{1I} \cap \overline{G_{2I}}$	Відмовив лише G_1
$ПВШ_3$	$\overline{G_{1I}} \cap G_{2I}$	Відмовив лише G_2
$ПВШ_4$	$G_{1I} \cap G_{2I}$	Обидва шлюзи відмовили

БДР для досліджуваної системи

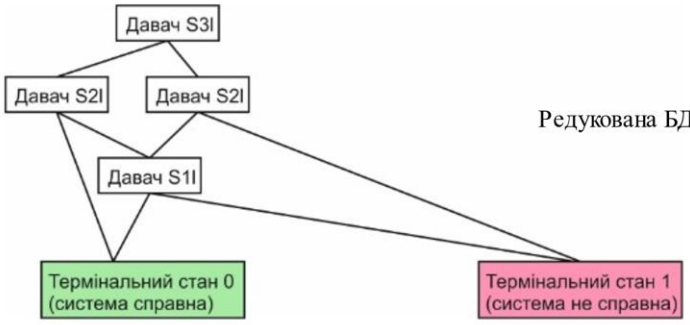
$$P(ПВШ_1) = P(\overline{G_{1I}}) \cdot P(\overline{G_{2I}}) = 0.90484^2 \approx 0.81873 \quad (9)$$

$$P(ПВШ_2) = P(G_{1I}) \cdot P(\overline{G_{2I}}) = 0.9516 \cdot 0.90484 \approx 0.08611 \quad (10)$$

$$P(ПВШ_3) = P(\overline{G_{1I}}) \cdot P(G_{2I}) = 0.90484 \cdot 0.09516 \approx 0.08611 \quad (11)$$

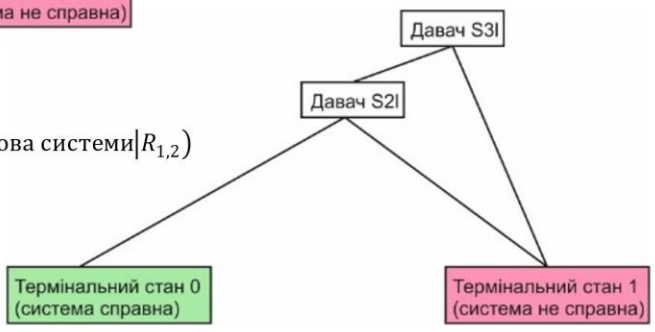
$$P(ПВШ_4) = P(G_{1I}) \cdot P(G_{2I}) = 0.09516^2 \approx 0.00906 \quad (12)$$

Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень



Редукована БДР для стану $P(\text{відмова системи}|R_{1,1})$

Редукована БДР для стану $P(\text{відмова системи}|R_{1,2})$



Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень

i	$P(R_{1,i})$	$P(R_{2,i})$	P(Відмова системи $\|R_{1,i})$
1	0,704	0,114	0,086
2	0,076	0,01	0,329
3	0,076	0,01	0,329
4	0,008	0,0007	1

Інтеграція результатів та обчислення загальної ненадійності системи:

$$U_S(t = 1000)$$

$$= \sum_{i=1}^{4} \left[P\left(\text{Відмова системи}\middle|R_{1,i}\right) \cdot P\left(R_{1,i}\right) + P\left(R_{2,i}\right)\right] = (0.086 \cdot 0.704 + 0.114) + (0.329 \cdot 0.076 + 0.01) + (0.329 \cdot 0.076 + 0.01) + (1 \cdot 0.008 + 0.0007) = 0.17513 + 0.03516 + 0.03516 + 0.00906 = 0,25451 \quad (13)$$

Теоретичне дослідження методу аналізу надійності IoT-інфраструктури на основі редукції бінарних діаграм рішень

Результати порівняльного аналізу методів (t = 1000 год)

k	U_S системи	Операції (пропонований метод)	Операції (метод АДВ)	t (пропонований метод), мс	t (метод АДВ), мс	Прискорення
1	0.28149	52	185	40.0	260.0	6.50×
2	0.48374	99	365	92.0	728.0	7.91×
3	0.62906	146	545	156.0	1404.0	9.00×
4	0.73347	193	725	232.0	2288.0	9.86×
5	0.80850	240	905	320.0	3380.0	10.56×
6	0.86240	287	1085	420.0	4680.0	11.14×

Висновки

1) У першому розділі проаналізовано IoT-інфраструктуру розумного будинку, класифіковано відмови та виявлено обмеження існуючих методів аналізу надійності, зокрема проблему обчислювальної складності.

2) У другому розділі досліджено механізми поширення відмов, концепцію конкуруючих відмов і часової конкуренції, а також викладено основи методу БДР.

3) У третьому розділі розроблено метод аналізу надійності на основі редукції БДР та оцінено його обчислювальну ефективність.

4) У четвертому розділі проведено аналіз ефективності методу, порівняння з існуючими підходами та визначено критичні компоненти системи.

Задворний С.О., Іванов О.В., Нічепорук А.О. Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, збірник наукових праць за матеріалами III (IX) Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «Інформаційні технології: теорія і практика», Харків – Запоріжжя – Дніпро, 25–27 березня 2026 р.

Дякую за увагу!

Wed Apr 15 08:30:34 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 1.0%

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

	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
ID: 270462 Назва: МКР Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень Додано в БД: 2026-04-15 Автора: Сергій ЗАДВОРНИЙ Керівники: Олексій ІВАНОВ Консультанти: Опоненти:	120206	754	2289 (2%)	29 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень
Автор Сергій ЗАДВОРНИЙ
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Олексій ІВАНОВ

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

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 9,63% і адресується до 28 першоджерела; та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

15.12.2025

Завідувач кафедри _____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Олексій ІВАНОВ
Підпис Ім'я, ПРІЗВИЩЕ

Протокол аналізу звіту подібності експертом

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

Автор: Сергій ЗАДВОРНИЙ

Співавтор:

Назва: Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Експерт: Олексій ІВАНОВ

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:9.63%

Коефіцієнт подібності 2:3.65%

Мікропробіли: 17

Заміна букв: 10

Інтервали: 0

Білі знаки: 6

Дата створення звіту: 2026-04-15 07:45:45.0

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:

2026-04-15 Доцент Андрій Нічепорук

Дата експерт

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Сергія Задворного
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

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

Задворний С.О.

7 квітня 2026 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Сергій Задворний

Тема: Метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 77

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень

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 проаналізовано предметну область IoT-інфраструктури розумного будинку, її архітектуру, протоколи зв'язку, класифіковано відмови та визначено обмеження існуючих методів оцінки надійності, на основі чого сформульовано задачу дослідження. У другому розділі досліджено механізми поширення відмов, розглянуто конкуруючі відмови та часову конкуренцію, а також викладено теоретичні основи оцінювання надійності за допомогою бінарних діаграм рішень і мір важливості компонентів. У третьому розділі розроблено метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень, описано відповідний алгоритм і оцінено його обчислювальну складність. У четвертому розділі досліджено ефективність запропонованого методу, проведено порівняльний аналіз точності та складності.

4. Позитивні сторони роботи: Запропоновано метод аналізу надійності IoT-інфраструктур на основі редукції бінарних діаграм рішень.

5. Негативні сторони роботи:

Запропонований метод, дещо переоцінює вплив поширюваних відмов і дає завищені оцінки ненадійності системи, оскільки припускає, що будь-яка поширювана відмова датчика, яка не була ізольована шлюзом, автоматично призводить до повної відмови всієї IoT-інфраструктури (умовна ймовірність = 1), хоча в реальних розумних будинках каскадне поширення зазвичай обмежується лише частиною системи завдяки сегментації мережі, резервним маршрутам або механізмам виявлення аномалій.

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» 75.00 (С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи)

д-р фіз.-мат. наук, професор, завідувач кафедри ІПЗ

Бедратюк Л.П.

" 15 квітня " 2026р.