НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна
наукова праця
на правах рукопису

Скоробогатько Станіслав Віталійович

УДК 004.052:519.248:504.064.3(043)

ДИСЕРТАЦІЯ
МОДЕЛІ ТА ПРОГРАМНІ ЗАСОБИ ОЦІНЮВАННЯ НАДІЙНОСТІ ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ

Спеціальність 123 Комп’ютерна інженерія
Галузь знань 12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ С. В. Скоробогатько
(підпис)

Науковий керівник Фесенко Герман Вікторович, д.т.н., професор

Харків – 2026

АНОТАЦІЯ

Скоробогатько Станіслав Віталійович. Моделі та програмні засоби оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія. – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертаційна робота присвячена розробленню моделей і програмних засобів для оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

Об'єктом дослідження є сенсорні мережі систем моніторингу потенційно небезпечних територій.

Вперше запропоновано структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень, які, на відміну від відомих, ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, що дозволяє планувати розподіл ресурсів і забезпечити надійне функціонування системи в умовах деградації мережі.

Удосконалено аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території, їхні показники безвідмовності та фатальні комбінації множинних відмов сенсорів за різними критеріями, що дозволяє розраховувати та прогнозувати показники надійності мереж.

Отримали подальшого розвитку марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання,

що дозволяє розраховувати функції готовності мереж для різних стратегій їх технічного обслуговування.

Ключові слова: безпілотний літальний апарат, моніторинг, надійність, математична модель, марковські ланцюги, бездротова сенсорна мережа, Інтернет речей, хмарні обчислення, граничні обчислення, туманні обчислення, моделі надійності, імітаційне моделювання, машинне навчання, штучний інтелект, дистанційне зондування.

Список публікацій здобувача:

1. Скоробогатько С. В., Фесенко Г. В. Перспективи використання літаючих хмарних, граничних та туманних обчислень компонентами системи моніторингу потенційно небезпечних об’єктів. *Системи управління, навігації та зв’язку*. 2022. Вип. 4 (70). С. 145–152. DOI: 10.26906/SUNZ.2022.4 (наукове фахове видання категорії Б).

2. Fesenko H., Illiashenko O., Kharchenko V., Kliushnikov I., Morozova O., Sachenko A., Skorobohatko S. Flying Sensor and Edge Network-Based Advanced Air Mobility Systems: Reliability Analysis and Applications for Urban Monitoring. *Drones*. 2023. Vol. 7, no. 7, article no. 409. P. 1–27. DOI: 10.3390/drones7070409 (закордонне періодичне наукове видання, Scopus, Q1). URL: https://www.mdpi.com/2504-446X/7/7/409.

3. Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Edge-based Sensors Network for Critical Object Monitoring: Reliability Models Considering the Location of Failed Sensors. *Dependable Systems, Services and Technologies (DESSERT’2023)* : Proc. 13th IEEE Int. Conf., Athens, Greece, Oct. 13–15, 2023. P. 1–7. DOI: 10.1109/DESSERT61349.2023.10416471 (стаття у працях конференції, Scopus).

4. Leichenko K., Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Reliability of Sensor Network-Based Systems for Arbitrary Shape Plot Monitoring Considering Multiple Failures. *Dependable Systems, Services and Technologies (DESSERT’2024)* : Proc. 14th IEEE Int. Conf., Athens, Greece, Oct. 11–13, 2024. DOI: 10.1109/DESSERT65323.2024.11122204 (стаття у працях конференції, Scopus).

5. Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Architecture and Reliability Models of Hybrid Sensor Networks for Environmental and Emergency Monitoring Systems. *Cybernetics and Systems Analysis*. 2024. Vol. 60, no. 2. P. 293–304. DOI: 10.1007/s10559-024-00670-x (наукове фахове видання категорії А, Scopus, Q3).

6. Skorobohatko S., Fesenko H., Kharchenko V., Volochiy B. Availability Models of a Recoverable Wireless Sensor Network for Forest Fire Monitoring System. *Reliability Engineering and Computational Intelligence (RECI'2024)* : Proc. 3rd Int. Workshop, Žilina, Slovakia, Nov. 6–8, 2024. P. 13. URL: https://reci.fri.uniza.sk/wp-content/uploads/2024/11/Abstracts-of-RECI-2024-v.5.pdf (стаття у працях конференції).

7. Leichenko K., Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Assessment of the Reliability of Wireless Sensor Networks for Forest Fire Monitoring Systems Considering Fatal Combinations of Multiple Sensor Failures. *Cybernetics and Systems Analysis*. 2025. Vol. 61, no. 1. P. 137–147. DOI: 10.1007/s10559-025-00753-3 (наукове фахове видання категорії А, Scopus, Q3).

8. Скоробогатько С., Фесенко Г., Харченко В. Послідовність і програмний засіб для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. Вип. 4 (84). С 68–80 DOI: 10.31891/2219-9365-2025-84-8 (наукове фахове видання категорії Б).

ANNOTATION

Skorobohatko Stanislav Models and software tools for assessing the reliability of hybrid sensor networks in monitoring systems for potentially dangerous areas. The thesis for a degree of Doctor of Philosophy (PhD) in specialty 123 Computer Engineering. – National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.

The dissertation is devoted to the development of models and software tools for assessing the reliability of hybrid sensor networks of monitoring systems for potentially dangerous areas.

The object of the research is the sensor networks of monitoring systems for potentially dangerous areas.

For the first time, structural and reliability models of hybrid sensor networks of monitoring systems for potentially hazardous areas have been proposed. These models are based on ground and flying components of cloud, edge, and fog computing. Unlike existing ones, they take into account various options for the placement and interaction of intelligent computing resources, as well as the operability levels of components depending on the completeness of monitoring functions execution. This allows for planning resource allocation and ensuring reliable system operation under conditions of network degradation.

Analytical and simulation models for assessing the failure-free operation of sensor networks of monitoring systems for potentially dangerous areas have been improved. These models consider the specific features of sensor coverage of the monitored area, their reliability indicators, and fatal combinations of multiple sensor failures according to various criteria, which allows calculating and predicting network reliability indicators.

Markov models for evaluating the availability of sensor networks of monitoring systems for potentially dangerous areas have been further developed. They take into account failures and recovery options for sensors and network equipment, which allows calculating network availability functions for various maintenance strategies.

Keywords: unmanned aerial vehicle, monitoring, reliability, mathematical model, Markov chains, wireless sensor network, Internet of Things, cloud computing, edge computing, fog computing, reliability models, simulation modeling, machine learning, artificial intelligence, remote sensing.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БПЛА – безпілотний літальний апарат
БСМ – бездротова сенсорна мережа
ГЗЕ – група зовнішніх експертів
ГСМ – гібридна сенсорна мережа
ДІ – довірчий інтервал
ЙБР – ймовірність безвідмовної роботи
КЦ – кризовий центр
ЛГО – літаючі граничні обчислення
ЛТО – літаючі туманні обчислення
ЛХО – літаючі хмарні обчислення
НГО – наземні граничні обчислення
НТО – наземні туманні обчислення
НХО – наземні хмарні обчислення
ПДП – пункт дистанційного пілотування
ПЗ – програмний засіб
ПНО – потенційно небезпечний об’єкт
ПНТ – потенційно небезпечна територія
СМ – система моніторингу
ССН – структурна схема надійності
ФКНС – фатальна комбінація непрацездатних сенсорів
ШІ – штучний інтелект
BFS – Breadth-First Search
DL – Deep Learning
DRL – Deep Reinforcement Learning
FANET – Flying Ad hoc Networks
FEN – Flying Edge Node
FL – Federated Learning
FoFEN – Fleet of Flying Edge Nodes

FoFSen – Fleet of Flying Sensors

FSen – Flying Sensor

FI – Fuzzy Inference

GCS – Ground Control Station

GUI – Graphical User Interface

IoFT – Internet of Flying Things

IoT – Internet of Things

MCC – Main Crisis Centre

RL – Reinforcement Learning

RL−ACO – Reinforcement Learning based on Ant-Colony Optimization

VCC – Virtual Crisis Centre

WSN – Wireless Sensor Networks

ВСТУП

Сучасні системи екологічного та аварійного моніторингу відіграють важливу роль у своєчасному виявленні загроз, запобіганні катастрофам та мінімізації їхніх наслідків на потенційно небезпечних територіях. Функціонування таких систем відбувається у суворих умовах навколишнього середовища (екстремальні температури, задимленість, фізичне зношення компонентів), що неминуче призводить до деградації мережі та вимагає функціонування в умовах жорсткої обмеженості ресурсів.

Еволюція технологій моніторингу обумовила перехід від традиційних сенсорних мереж до гібридних сенсорних мереж (ГСМ). Такі мережі є перспективною основою сучасних систем моніторингу, оскільки вони ефективно поєднують стаціонарні наземні сенсори та мобільні літаючі компоненти (флоти БПЛА) з широким використанням технологій хмарних, граничних і туманних обчислень. Застосування цих обчислювальних технологій дозволяє наблизити обробку даних безпосередньо до об’єктів моніторингу, що суттєво зменшує затримки передачі даних та підвищує загальну автономність мережі.

Неоднорідність компонентів гібридних сенсорних мереж істотно ускладнює задачі забезпечення та достовірного оцінювання їх безвідмовності. Проведений аналіз існуючих наукових робіт показав, що сучасні підходи до моделювання безвідмовності та готовності сенсорних мереж не повною мірою враховують специфічні особливості гібридних систем. Зокрема, існуючі моделі недостатньо враховують особливості довільного покриття контрольованої території сенсорами, а також вплив утворення просторових непрацездатних кластерів сенсорів, поява яких призводить до виникнення зони, не покритою сенсорною мережею, що унеможливлює виконання завдання моніторингу на визначеному потенційно небезпечно об’єкті.

Крім того, існуючі методи недостатньо адаптовані для аналізу систем із багаторівневою працездатністю. В реальних умовах ГСМ здатна до багаторівневої працездатності шляхом перерозподілу завдань між наявними обчислювальними

ресурсами. Також потребують подальшого розвитку підходи до оцінювання надійності з урахуванням процесів відмов та варіантів відновлення мережевого обладнання за різних стратегій технічного обслуговування. Відсутність спеціалізованих програмних інструментів не дозволяє системно аналізувати перелічені фактори та ускладнює проєктування надійнісних архітектур ГСМ.

У зв'язку з цим виникає об'єктивна необхідність у розробленні комплексу нових структурних, аналітичних, імітаційних та марковських моделей оцінювання надійності й готовності гібридних сенсорних мереж. Впровадження таких моделей та відповідних спеціалізованих програмних засобів дозволить враховувати особливості їх функціонування, прогнозувати показники надійності та обґрунтовувати рішення щодо раціонального розподілу ресурсів для забезпечення безперервності процесу моніторингу потенційно небезпечних територій.

Об'єкт дослідження – сенсорні мережі систем моніторингу потенційно небезпечних територій.

Предмет дослідження – моделі та програмні засоби оцінювання надійності сенсорних мереж систем моніторингу потенційно небезпечних територій.

Мета і завдання дослідження – метою дослідження є підвищення повноти множини рішень та точності оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

Для досягнення мети дослідження необхідно вирішити наступні завдання:

– провести аналіз існуючих моделей та засобів оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, обґрунтувати мету та завдання досліджень;

– розробити структури та аналітичні моделі надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій;

– розробити марковські моделі оцінювання готовності наземних сенсорних мереж систем моніторингу потенційно небезпечних територій;

– розробити імітаційні моделі оцінювання надійності наземних сенсорних мереж систем моніторингу потенційно небезпечних територій;

– розробити програмні засоби для оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій;

– впровадити розроблені методи та засоби в навчальному процесі, наукових проєктах та індустрії.

Методи дослідження. У дисертаційній роботі використовувались методи системного аналізу, оптимізації, математичного моделювання, теорії надійності, теорії графів.

Наукова новизна отриманих результатів:

– **вперше запропоновано** структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень, які, на відміну від відомих, ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, що дозволяє планувати розподіл ресурсів і забезпечити надійне функціонування системи в умовах деградації мережі;

– **удосконалено** аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території, їхні показники безвідмовності та фатальні комбінації множинних відмов сенсорів за різними критеріями, що дозволяє розраховувати та прогнозувати показники надійності мереж;

– **отримали подальшого розвитку** марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання, що дозволяє розраховувати функції готовності мереж для різних стратегій їх технічного обслуговування.

Особистий внесок здобувача полягає у розроблені методів і програмних засобів, які забезпечують вирішення поставлених задач, описаних вище. Всі основні результати, отримані автором особисто, опубліковані у роботах [1]–[8]. У

працях, які опубліковані у співавторстві, автору належать: структурні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень [1]; надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень та ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, а також програмний засіб для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі [2]; програмний засіб, моделі та методи надійності з урахуванням розташування несправних сенсорів [3]; методи оцінювання надійності бездротових сенсорних мереж систем моніторингу з урахуванням фатальних комбінацій множинних відмов сенсорів [4]; аналітичні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території та їхні показники безвідмовності [5]; марковські моделі готовності відновлюваної бездротової сенсорної мережі для системи моніторингу лісових пожеж [6]; імітаційну модель оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, яка враховує особливості покриття сенсорами контрольованої території та фатальні комбінації множинних відмов сенсорів за різними критеріями [7]; програмний засіб для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж для різних сценаріїв відмов з використанням візуалізації розташування сенсорів та ділянок покриття мережі [8].

Апробація матеріалів дисертації. Основні положення та ідеї дисертаційної роботи доповідалися та обговорювалися на:

– науково-технічному семінарі «Гарантоздатні Інформаційні Технології» (ГІТ) кафедри комп’ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ» (Харків, 04 жовтня 2023 р.);

– 13-ій Міжнародній науково-технічній конференції “Dependable Systems, Services and Technologies (DESSERT’23)” (Афіни, Греція, 2023);

– 14-ій Міжнародній науково-технічній конференції “Dependable Systems, Services and Technologies (DESSERT’24)” (Афіни, Греція, 2024);

– 3-му Міжнародному воркшопі “Reliability Engineering and Computational Intelligence (RECI’2024)” (Жиліна, Словаччина, 2024).

Зв’язок з науковими програмами, темами. Дисертаційна робота виконана у Національному аерокосмічному університеті «Харківський авіаційний інститут» відповідно з державними програмами та планами НДР:

– НДР «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об’єктів» (№ Д/Р 0121U112172, 2021-2023);

– НДР «Методологія та інформаційні технології оцінювання та забезпечення безпеки цифрової інфраструктури малих модульних реакторів» (№ Д/Р 0122U000977, 2022-2024);

– НДР «Методи та засоби виявлення вибухонебезпечних предметів з використанням багатофункційних інтелектуальних систем БПЛА» (№ Д/Р 0123U101992, 2023-2024);

– НДР «Методи, моделі та інформаційні технології підвищення надійності та безпечності складних ІТ-систем на етапах розроблення та впровадження» (№ Д/Р 0121U113842, 2021-2023);

– НДР «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об’єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час).

Роль автора у зазначених НДР, в яких автор був безпосереднім виконавцем, полягає у розробці методів та засобів підвищення повноти множини рішень та точності оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

Практичне значення отриманих результатів. Практичні результати полягають у доведенні теоретичних положень дисертаційної роботи до конкретних алгоритмів та програмних засобів для планування та здійснення заходів для підвищення надійності сенсорних мереж. Результати дисертаційної роботи впроваджено:

– у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій ХАІ у вигляді лекційного матеріалу і практичних занять з використання моделей та засобів оцінювання та забезпечення надійності, зокрема, моделей гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій у навчальній дисципліні «Надійність та відмовостійкість комп'ютерних систем» (4 години);

– при виконанні науково-дослідних робіт, перелік яких надано вище;

– в Українському ордена «Знак пошани» науково-дослідному інституті лісового господарства та агролісомеліорації ім. Г. М. Висоцького Державного агентства лісових ресурсів України та Національної академії наук України.

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновку, списку використаних джерел і додатків. Загальний обсяг дисертації складає 177 сторінок, з яких анотація двома мовами на 4 сторінках, зміст на 3 сторінках, перелік умовних скорочень на 2 сторінках, основний текст на 118 сторінках, список використаних джерел із 78 найменувань на 9 сторінках, додатки на 37 сторінках. Робота містить 22 таблиці та 56 рисунків.

Публікації. За темою дисертаційної роботи було опубліковано 8 наукових праць, серед яких: 2 статті у наукових фахових виданнях України категорії Б; 2 статті у англомовному науковому фаховому виданні України категорії А, проіндексованому у базі даних Scopus (квартиль Q3); 1 стаття у закордонному періодичному науковому виданні, проіндексованому у базі даних Scopus (квартиль Q1); 3 апробаційних публікації в працях міжнародних конференцій, 2 з яких проіндексовано у базі даних Scopus.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ТА ЗАСОБІВ ОЦІНЮВАННЯ НАДІЙНОСТІ ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ. ОБҐРУНТУВАННЯ МЕТИ ТА ЗАВДАНЬ ДОСЛІДЖЕНЬ

1.1 Аналіз принципів і технологій побудови наземних та літаючих сенсорних мереж систем моніторингу

У сучасних умовах бездротові сенсорні мережі (БСМ) є ключовою ланкою у проєктуванні та розгортанні систем моніторингу потенційно небезпечних територій (ПНТ). Характерною рисою сучасних систем контролю ПНТ є інтеграція безпілотних літальних апаратів (БПЛА), які забезпечують доступ до важкодоступних ділянок та оперативний збір даних.

Для обґрунтування доцільності впровадження БПЛА необхідно проаналізувати обмеження стаціонарних БСМ. У роботі [9] досліджено надійність сенсорних мереж в умовах лісових пожеж, враховуючи фактори енергоефективності, технічні специфікації вузлів та протоколи передачі даних. Дослідження [10] присвячене створенню систем інтелектуального моніторингу на основі класичних БСМ та концепції Інтернету речей (Internet of Things, IoT). У статті [11] підкреслюється, що навіть за умови оптимізації маршрутів передачі даних, наземні системи залишаються вразливими до деструктивних зовнішніх факторів, зокрема механічних пошкоджень інфраструктури.

Комплексний огляд технологій побудови літаючих сенсорних мереж на базі БПЛА представлено у роботі [12]. Автори систематизують принципи проєктування на апаратному, програмному та комунікаційному рівнях, охоплюючи стратегії планування маршрутів та алгоритми калібрування вимірювань. Порівняння архітектур стаціонарних станцій із мобільними повітряними платформами дозволяє визначити оптимальні сценарії їхнього комбінованого застосування.

Прикладом практичної реалізації є використання БПЛА з вертикальним зльотом і посадкою (Vertical Take-off and Landing, VTOL) для гамма-спектрометричного картографування [13]. Результати польових випробувань підтверджують ефективність гібридних систем, що поєднують мобільні літаючі детектори із наземними станціями обробки даних.

У дослідженні [14] обґрунтовано переваги дистанційного зондування (remote sensing) з повітря, зокрема: відсутність наземних перешкод, збільшений радіус дії та висока швидкість розгортання. Це критично важливо для обстеження радіаційних аномалій на територіях, де розгортання наземних датчиків є технічно неможливим або небезпечним для персоналу.

Автори роботи [15] запроваджують концепцію «літаючого Інтернету речей» (Internet of Flying Things, IoFT), яка розширює можливості класичного IoT. У межах IoFT розглядаються такі архітектурні парадигми:

- літаючі хмарні обчислення (ЛХО);
- літаючі туманні обчислення (ЛТО);
- літаючі граничні обчислення (ЛГО).

Особливості моніторингу в замкнутих просторах та алгоритми обходу перешкод розглядаються у працях [16] та [17]. Стаття [18] містить огляд архітектур, де БПЛА виступають як мобільні периферійні вузли, що забезпечують зв’язок між наземними пристроями та хмарною інфраструктурою. Автори систематизують типи взаємодії у трирівневій структурі ЛГО, приділяючи увагу обчислювальному розвантаженню (offloading) та енергоспоживанню. Питання автоматизації керування такими апаратами висвітлено у дослідженні [19].

Для підвищення ефективності моніторингу лісових масивів автори [20] пропонують використання туманних обчислень для прискорення передачі даних. У роботі [21] аналізуються літаючі спеціалізовані мережі (Flying Ad hoc Networks, FANET), які функціонують без залучення наземних базових станцій, що дозволяє суттєво зменшити затримки. Концепція ЛГО також успішно адаптується для потреб сільського господарства [22], де БПЛА виконують попередню фільтрацію

великих масивів даних перед їх відправленням у «хмару». Сучасним трендом є обробка даних безпосередньо на борту БПЛА за допомогою алгоритмів машинного та глибокого навчання [23].

Синергія наземних та повітряних компонентів є необхідним кроком для підвищення якості моніторингу складних об’єктів. На прикладі контролю витоків газу в роботі [24] продемонстровано переваги поєднання стаціонарних сенсорів із високоточними лазерними детекторами на борту БПЛА. Такий підхід дозволяє оперативно виявляти аномалії наземними засобами та здійснювати їх точну локалізацію методами дистанційного зондування.

Результати аналізу розглянутих джерел дозволяють зробити такі висновки:

– інтеграція БПЛА у наземні сенсорні мережі дозволяє подолати обмеження стаціонарних систем щодо стійкості до руйнувань та забезпечити оперативне дистанційне зондування у важкодоступних і небезпечних зонах;

– впровадження концепції «літаючого Інтернету речей» (IoFT) та ЛХО (ЛТО, ЛГО) мінімізує затримки в передачі даних завдяки інтелектуальній обробці інформації безпосередньо на борту повітряних платформ;

– використання алгоритмів машинного навчання та автоматизованого керування в літаючих мережах (FANET) гарантує високу точність моніторингу та стабільність зв’язку в умовах обмежених енергетичних і мережевих ресурсів;

– формування сучасних гібридних мереж потребує системного поєднання апаратного, програмного та комунікаційного рівнів проєктування для забезпечення цілісності інформаційного поля та безперервного дистанційного контролю стану ПНТ.

1.2 Аналіз вимог до надійності сенсорних мереж систем моніторингу

Технології, розглянуті у попередньому підрозділі, висувають підвищені вимоги до надійності систем моніторингу. Ускладнення архітектури шляхом інтеграції нових компонентів безпосередньо корелює зі зростанням ймовірності

відмови всієї системи, що зумовлює необхідність ґрунтовного аналізу показників надійності бездротових сенсорних мереж (БСМ).

У роботі [25] представлено метод аналізу надійності зв’язності та покриття для лінійних БСМ, призначених для моніторингу протяжних об’єктів. Автор формулює вимоги до надійності через імовірнісні моделі зв’язності вузлів, враховуючи випадкові відмови та обмеження радіусу дії радіоканалу. Запропонований підхід дозволяє кількісно визначити мінімальну щільність розміщення сенсорів для досягнення заданого рівня безвідмовності.

Питання експлуатаційної надійності БСМ у специфічних умовах (наприклад, моніторинг температури у транспортних контейнерах) розглянуто у дослідженні [26]. Автори доводять, що використання методів машинного навчання для апроксимації даних від несправних вузлів дозволяє компенсувати апаратну ненадійність сенсорів. Загальні стратегії підвищення надійності, що базуються на оптимізації топології та архітектури комунікацій, висвітлено у працях [27] та [28].

У дослідженні [29] окремий сенсорний вузол розглядається як багатокомпонентна система, схильна до відмов окремих модулів: сенсора, трансивера, процесора та джерела живлення. Питання готовності критичних систем досліджується у роботі [30], де акцент зроблено на автоматизованій генерації дерев відмов для мережевого обладнання. Щільність розміщення сенсорів як критичний фактор надійності екологічного моніторингу визначено у праці [31]. Для систем візуального моніторингу цей показник є ключовим, оскільки відмова будь-якого вузла призводить до появи неконтрольованих ділянок.

Автори роботи [32] пропонують трирівневу структуру забезпечення відмовостійкості: виявлення, діагностика та відновлення. Системи класифікуються за рівнем продуктивності алгоритмів ідентифікації помилок. У праці [33] представлено модифікований підхід на основі суми непересічних добутків (Sum of Disjoint Products) для оцінювання надійності БСМ у динамічних станах. Метод передбачає перерахування найкоротших шляхів доставки даних до центрального вузла.

Особливості надійності кластерних архітектур розглянуто у роботі [34]. Встановлено, що відмова периферійного агрегуючого вузла (cluster head) еквівалентна відмові всього кластера. Важливим фактором також є обмеженість енергоресурсів. Для систем, що підлягають обслуговуванню, у дослідженні [35] критичним показником визначено час до виявлення відмови та заміни сенсора, що безпосередньо впливає на коефіцієнт готовності.

Додавання мобільних вузлів до статичних мереж аналізується у роботі [36]. Порівняльний аналіз затримки передачі, масштабованості та енергоефективності демонструє переваги гібридного підходу для розширення зони покриття. Проте надійність таких систем критично залежить від стабільності з'єднання мобільних агентів. Підвищення безвідмовності за рахунок вузлів із модулями енергозбору (energy harvesting) та інтелектуальної маршрутизації розглянуто у працях [37], [43].

Проблема ідентифікації причин збоїв у системах із «маскованими» даними вирішується у роботі [38] за допомогою алгоритму максимізації очікувань (EM-algorithm). У контексті лінійних мереж автори [39] підкреслюють небезпеку послідовних відмов, що призводять до розриву інформаційного ланцюга, та пропонують компромісні рішення між структурною надмірністю та надійністю доставки пакетів. Сучасні моделі надійності передачі даних, представлені у роботах [40] та [41] враховують випадкові флуктуації пропускної здатності каналів та стабільність електроживлення.

За результатами аналізу розглянутих у цьому підрозділі джерел можна зробити такі висновки:

– Більшість джерел ([25], [34], [39]) фокусуються на вузькоспеціалізованих топологіях: суто лінійних або кластерних структурах. У контексті гібридних мереж (де наземні вузли взаємодіють із мобільними БПЛА) ці моделі не забезпечують повноти множини рішень, оскільки не враховують динамічну зміну топології. Робота [36] лише побіжно порівнює затримки, але не дає цілісної математичної моделі надійності, яка б об'єднувала статичні та мобільні компоненти в єдину аналітичну систему.

– Для моніторингу ПНТ критично важливою є не просто «зв’язність» (на якій акцентують увагу джерела [25] та [40]), а безперервність покриття. Джерела [30] та [33] пропонують класичні методи (дерева відмов, сума непересічних добутків), які добре оцінюють імовірність доставки пакета, але абсолютно не враховують виникнення локальних зон «інформаційної сліпоти». Це суттєво знижує точність оцінювання, оскільки система може вважатися «працездатною» з точки зору мережі, але бути «відмовою» з точки зору виявлення небезпеки на конкретній ділянці.

– Хоча робота [29] деталізує вузол як багатокомпонентну систему, вона, як і більшість інших праць, розглядає відмови як незалежні події. У реальних умовах ПНТ (пожежі, викиди, радіація) відмови мають каскадний або корельований характер. Відсутність у джерелах моделей кластерних відмов не дозволяє досягти високої точності в екстремальних сценаріях, що є критичним недоліком для систем моніторингу.

Джерела [37] та [42] зосереджені на збиранні енергії (energy harvesting) та оптимізації живлення. Однак у них надійність розглядається як похідна від наявності енергії, а не як функційна готовність до виконання місії. Для підвищення повноти рішень необхідно інтегрувати показники «часу життя» вузла з імовірністю виконання цільового завдання моніторингу, чого в наведених джерелах не зроблено в достатній мірі.

1.3 Аналіз моделей та методів оцінювання надійності сенсорних мереж систем моніторингу

У роботі [44] для оцінювання надійності БСМ застосовано два підходи: алгоритм на основі впорядкованих діаграм бінарних рішень (Binary Decision Diagrams) та імітаційне моделювання методом Монте-Карло. Дослідження враховує як одиничні відмови сенсорів, так і збої загальносистемних компонентів, проте питання кластерних відмов залишається поза увагою. Автори праці [45] здійснюють порівняльний аналіз структурних схем надійності (ССН), їхніх

гібридних форм та дерев відмов. Встановлено, що використання дерев відмов є ефективним для систем із незначною кількістю вузлів, проте при масштабуванні мережі до тисячі одиниць обчислювальна складність методу стає критичною.

У дослідженні [46] для опису надійності БСМ використано апарат марковських ланцюгів за припущення послідовного з'єднання компонентів, де модель відмов апроксимується розподілом Вейбулла. Розвиваючи тему стохастичного моделювання, автори роботи [47] застосовують марковські ланцюги з безперервним часом для формалізації переходів системи між працездатними та аварійними станами. Праця [48] присвячена аналізу моделі готовності БСМ шляхом розв'язання систем диференціальних рівнянь, що дозволяє враховувати інтенсивність відмов та відновлення елементів. Використання прихованих марковських моделей та методу копули для ідентифікації латентних дефектів та аномальних станів описано у роботі [49], де математичні результати підтверджені емпіричними даними.

Питання геометричного покриття та його впливу на надійність розглянуто у працях [50] та [51]. Автори формалізують моделі максимального покриття заданої території, використовуючи методи обчислювальної геометрії та нелінійної оптимізації. Практичне застосування цих методів для моніторингу лісових пожеж описано у дослідженні [52], де топологія мережі детермінована рельєфом місцевості. Оптимізація розміщення вузлів у таких умовах підвищує надійність системи без надлишкового дублювання компонентів.

Для оптимізації площі покриття автори роботи [53] застосовують алгоритм «пошуку зозулі» (Cuckoo Search) на засадах ройового інтелекту (Swarm Intelligence). Попри те, що дослідження не фокусується безпосередньо на теорії надійності, оптимізація розміщення вузлів прямо впливає на кількісні показники за рахунок забезпечення зв'язності та стабільної передачі даних.

У роботі [54] досліджується надійність з'єднань при різних топологіях кластеризації із застосуванням нейро-нечіткої моделі оптимізації (Reliable Neuro-Fuzzy Optimization Model, RNFOM), що покращує ідентифікацію відмов. Питання відновлення зв'язності висвітлено у праці [55], де запропоновано алгоритм вузла

збору некритичного вантажу (Pickup Non-Critical Node, PINC) для переміщення працездатних некритичних вузлів на позиції критичних елементів, що вийшли з ладу.

Окремий напрям досліджень присвячений мобільним компонентам БСМ. У роботі [56] запропоновано метод аналізу доступності для систем типу «k-out-of-n», що дозволяє визначити критичні компоненти рою БПЛА. Стаття [57] описує моделі надійності для флотів БПЛА з різними типами керування (централізоване та децентралізоване) на основі бінарних станів. У праці [58] розроблено марковську модель для оцінювання ймовірності виживання флотів БПЛА в умовах виконання бойових завдань.

Комплексну методологію побудови промислових систем моніторингу на основі БПЛА, IoT та цифрових двійників (Digital Twins) представлено у роботі [59]. Автори доводять, що інтеграція цих технологій забезпечує вищу загальну надійність порівняно з існуючими рішеннями.

За результатами аналізу розглянутих у цьому підрозділі джерел можна зробити такі висновки:

Виявлено, що традиційний математичний апарат, зокрема дерева відмов [45], діаграми бінарних рішень [44] та марковські ланцюги у джерелах [46] та [47], демонструє високу точність лише для локальних сегментів мережі. При масштабуванні системи моніторингу ПНТ до рівня гібридної інфраструктури (понад 1000 вузлів) обчислювальна складність цих методів зростає експоненціально, що обмежує повноту множини рішень та вимагає впровадження комбінованих підходів на основі імітаційного моделювання та статистичної верифікації.

Більшість існуючих моделей, представлених у джерелах [44], [46], [48] та [49], базується на припущенні про незалежність відмов окремих сенсорів, що суттєво знижує точність оцінювання надійності в реальних умовах ПНТ. Оскільки зовнішні загрози (наприклад, лісові пожежі [52]) зазвичай викликають групові збої, виникає потреба у формалізації «кластерних відмов» як фатальних комбінацій, що призводять до появи неконтрольованих зон при збереженні загальної мережевої зв’язності (джерела [54] та [55]).

Аналіз показав, що надійність наземних БСМ та мобільних флотів БПЛА (джерела [56], [57] та [58]) переважно досліджується ізольовано. Для підвищення достовірності результатів необхідно розробити цілісну методологію, яка б об’єднувала показники мережевої надійності та геометричного покриття території (джерела [50], [51] та [53]) у межах єдиного розрахункового циклу для стаціонарних та мобільних компонентів системи моніторингу [59].

1.4 Аналіз існуючих засобів оцінювання надійності сенсорних мереж систем моніторингу

У даному підрозділі проаналізовано сучасні джерела, що висвітлюють програмний інструментарій для оцінювання надійності та готовності сенсорних, гібридних мереж, а також їхніх окремих компонентів.

Протягом тривалого часу для дискретно-подійного моделювання комп’ютерних мереж використовувався інструмент OMNeT++ [60], що володіє графічним інтерфейсом та можливостями моделювання радіоканалів. Засоби NS-2 та NS-3 [61] також переважно орієнтовані на симуляцію комп’ютерних мереж; їх застосовують для оцінювання стійкості протоколів маршрутизації в умовах відмов окремих вузлів.

Для дослідження БСМ автори роботи [62] пропонують використовувати симулятор COOJA. Проте його функціональні можливості обмежені аналізом відмов мікроконтролерів, що не дозволяє здійснювати комплексну оцінку надійності мереж, які складаються з тисяч сенсорних вузлів. Для порівняльного аналізу ефективності засобів симуляції БСМ автори у праці [63] пропонують власну методологію оцінювання їхніх технічних характеристик.

У статті [64] представлено систематичний огляд сучасних симуляторів IoT-мереж, зокрема RelIoT, iFogSim, CupCarbon та FogNetSim++, з акцентом на моделюванні надійності, енергоспоживання та продуктивності. Автори порівнюють функціональні параметри цих засобів та аналізують їхню здатність

прогнозувати безвідмовність сенсорів. Особливу увагу приділено фреймворку RelIoT, який інтегрує модулі розрахунку потужності, температурних режимів та надійності в середовище мережевого симулятора NS-3.

Для кількісного оцінювання надійності систем різного ступеня складності застосовуються спеціалізовані програмні продукти:

– ASNA [65] − потужний інструментарій для обчислення надійності систем на основі теорії стохастичного моделювання експлуатаційної надійності інформаційних систем. Засіб дозволяє розраховувати показники надійності з використанням векторів станів та структурно-автоматних моделей (САМ), що забезпечує моделювання систем із надлишковою кількістю станів.

– ReliaSoft BlockSim [66] − програмне забезпечення, що є галузевим стандартом для розрахунку надійності за допомогою методу структурних схем надійності (ССН).

– Reliability Workbench [67] − комплексне рішення, що підтримує розрахунки методами ССН, марковських моделей, дерев відмов тощо.

Слід зауважити, що попри високу точність, зазначені комерційні інструменти переважно орієнтовані на оцінювання надійності окремих компонентів або ієрархічних систем і не пристосовані для специфічного аналізу сенсорних мереж великої розмірності (тисячі вузлів).

Робота [68] аналізує сучасні засоби для симуляції систем з флотами БПЛА, констатуючи, що більшість засобів приділяють увагу не оцінюванню надійності, а методам обходу перешкод, уникненню зіткнень та аеродинаміці. Засіб імітаційного моделювання, запропонований авторами у роботі [69], дозволяє аналізувати функціонування окремих БПЛА, проте він не передбачає можливості виконання обчислень на борту та роботи пристрою як сенсорного вузла. У дослідженні [70] представлено фреймворк на базі мови Java, призначений для фізичної симуляції роїв БПЛА. Попри інноваційність, цей інструмент не дозволяє моделювати відмови та розраховувати кількісні показники надійності. Аналіз наявного спеціалізованого ПЗ для мобільних систем свідчить, що більшість рішень орієнтована на відтворення

процесів функціонування, а не на оцінювання надійності окремих вузлів чи системи загалом.

Робота [71] присвячена програмному підходу до аналізу поведінки сенсорів в IoT-системах із застосуванням статистичної верифікації моделей. Автори використовують інструментарій UPPAAL SMC для побудови стохастичних моделей сенсорних вузлів та автоматичного виявлення аномалій. Запропонований метод поєднує машинне навчання з формальною верифікацією, що забезпечує оцінку надійності сенсорної мережі на ранніх стадіях проєктування без залучення фізичної інфраструктури.

У статті [72] наведено систематичний огляд програмних фреймворків для аналізу безпеки та надійності IoT, зокрема на основі дерев відмов, мереж Байєса та модельно-орієнтованих підходів. Автори класифікують інструменти за типами аналізу (статичний, динамічний, гібридний) та оцінюють їхню придатність для різних архітектур. Дослідження окреслює прогалини в існуючому інструментарії та визначає перспективні напрямки розвитку засобів оцінювання надійності.

Питання надійності IoT-систем у сільському господарстві розглянуто у праці [73], де оцінюється територія покриття та доступність вузлів. Попри врахування значної кількості параметрів, у роботі не досліджується можливість виникнення кластерних відмов компонентів. Автори дослідження [74] пропонують засіб RelIoT, здатний моделювати деградацію компонентів та оцінювати надійність систем за таких умов, проте завдання ідентифікації кластерних відмов також залишається поза увагою.

У статті [75] за допомогою інструментів на базі мови Python проведено оцінку надійності сенсорних мереж для авіабудування. Для верифікації моделі автори застосовують методологію RGA4FEM (Region Growing Algorithm for Finite Element Method). У роботі [76] запропоновано модель для оцінювання надійності сенсорів та виконавчих пристроїв IoT на основі аналізу даних із використанням методів нечіткої логіки та багатокритеріального прийняття рішень. Такий підхід дозволяє виявляти вразливі елементи та оптимізувати вибір пристроїв ще на етапі проєктування.

Питання дослідження програмно-конфігурованих бездротових мереж (Software-Defined Networking, SDN) та загальна еволюція засобів моделювання БСМ детально висвітлені у роботах [77] та [78]. Результати комплексного огляду свідчать, що більшість симуляторів фокусуються на аналізі протоколів зв'язку та енергоефективності. Проте питання комплексного моделювання структурної надійності та впливу просторових відмов на безвідмовність мережі залишаються недостатньо вивченими.

За результатами аналізу розглянутих у цьому підрозділі джерел можна зробити такі висновки:

– Більшість сучасних програмних засобів (OMNeT++, NS-3, COOJA) орієнтована переважно на моделювання мережевих протоколів, аеродинамічних параметрів та енергоспоживання, залишаючи поза увагою комплексне оцінювання структурної надійності систем. Спеціалізовані комерційні продукти (ReliaSoft, Reliability Workbench) зосереджені на аналізі окремих компонентів або статичних ієрархічних структур, що не дозволяє адекватно відтворювати динаміку функціонування гібридних мереж.

– Існуючий інструментарій моделювання флотів БПЛА та IoT-інфраструктур часто не має засобів для розрахунку кількісних показників надійності у великих масштабах (понад 1000 вузлів). Зокрема, розроблені фреймворки зазвичай не розглядають БПЛА як активні обчислювальні сенсорні вузли, що обмежує можливість оцінювання надійності систем моніторингу ПНТ, де мобільні елементи відіграють ключову роль у підтримці зв'язності та покриття. Критичним недоліком проаналізованих засобів (включаючи RelIoT, iFogSim та UPPAAL SMC) є відсутність можливостей для ідентифікації та моделювання просторових (кластерних) відмов. Це обґрунтовує доцільність розроблення нових програмних рішень, здатних симулювати мережі довільної топології та великої розмірності з можливістю визначення фатальних комбінацій відмов, що безпосередньо впливають на надійність систем моніторингу ПНТ.

1.5 Постановка задачі та обґрунтування методики досліджень

1.5.1 Задачі досліджень та обґрунтування математичного апарату

Загальне завдання: розроблення моделей та програмних засобів оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

Часткові завдання:

1. Провести аналіз та обґрунтування підходів до оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

2. Розробити структурні та надійнісні моделі гібридних сенсорних мереж системи моніторингу потенційно небезпечної території.

3. Розробити аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж.

4. Розробити марковські моделі оцінювання готовності сенсорних мереж системи моніторингу потенційно небезпечної території.

5. Розробити програмні засоби для реалізації запропонованих моделей та методів оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій.

6. Впровадити розроблені методи та засоби в навчальному процесі, наукових проєктах та індустрії.

Для розв’язання поставлених задач у дисертаційній роботі використовуються методи системного аналізу, оптимізації, математичного моделювання, теорії надійності. Вибір конкретного математичного апарату обґрунтовується наступними потребами:

1. Для побудови аналітичних моделей надійності використовується апарат системного аналізу, математичного моделювання, та комбінаторики. Це необхідно для формалізації функції недопустимих комбінацій, яка визначає загальну кількість просторових станів мережі, за яких утворюються критичні відмови на територіях регулярної форми. Крім того, математичний опис трирівневої архітектури вимагає

апарату теорії надійності для систем з багаторівневою працездатністю, щоб розрахувати ймовірності перебування системи у частково працездатних станах.

2. Для розроблення моделей готовності відновлюваних мереж обрано апарат марковських ланцюгів неперервного часу та структурно-автоматний підхід. Він дозволяє скласти системи диференціальних рівнянь Колмогорова-Чепмена для врахування інтенсивностей відмов сенсорів, відмов периферійного обладнання, а також інтенсивностей процедур відновлення компонентів.

3. Для побудови імітаційних моделей надійності територій довільної форми застосовується метод імітаційного моделювання (метод Монте-Карло). Оскільки аналітичне оцінювання просторових відмов для ділянок довільної форми є занадто складним, метод Монте-Карло дає змогу генерувати стохастичні відмови сенсорів за експоненціальним законом розподілу. Для автоматичної ідентифікації кластерних відмов обґрунтовано використання алгоритму обходу графа в ширину, який дозволяє знаходити суміжні непрацездатні сенсори та перевіряти їх на відповідність критеріям відмови.

1.5.2 Етапи та взаємозв’язок задач і результатів досліджень

Вирішення сформульованих наукових задач здійснюється у чотири логічно взаємопов’язані етапи, результати яких послідовно розкриваються у відповідних розділах дисертації.

Етап 1. Аналітичний етап. Спрямований на вирішення задачі 1. Здійснюється системний аналіз принципів побудови гібридних сенсорних мереж, що поєднують наземні сенсори, літаючі БПЛА та технології ЛГО, ЛХО та ЛТО. Досліджуються вимоги до надійності та виявляються обмеження існуючих математичних моделей і програмних симуляторів щодо здатності враховувати враховувати багаторівневу працездатність та просторові відмови. Результатом етапу є постановка задачі дослідження.

Етап 2. Етап структурного та аналітичного моделювання. Спрямований на вирішення Задачі 2 та частково Задачі 3. На основі висновків першого етапу розробляється трирівнева архітектура ГСМ з інтеграцією граничних обчислень. Формується класифікація моделей надійності, що відрізняє нерезервовані та

резервовані системи, системи з відновленням та без нього. Вперше пропонуються аналітичні моделі ГСМ як системи з багаторівневою працездатністю та розробляються математичні залежності для оцінювання надійності сенсорних мереж з урахуванням прямокутних просторових кластерів відмов. Отримані аналітичні результати є основою для побудови наступних, більш складних моделей.

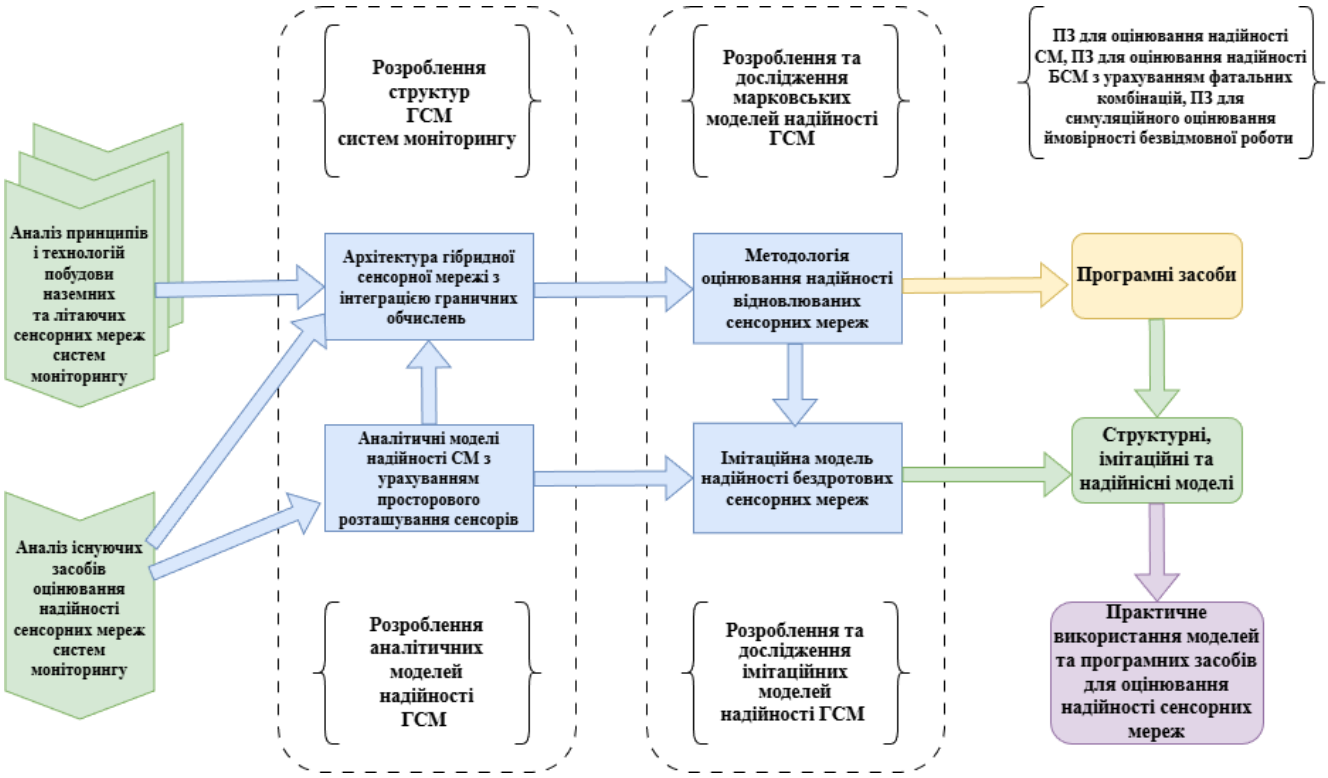

Рисунок 1.1 – Діаграма залежності сформульованих наукових задач

Етап 3. Етап марковського та імітаційного моделювання. Спрямований на вирішення Задач 3 та 4. Оскільки аналітичні моделі мають обмеження щодо форми території, розробляються імітаційні моделі надійності, що базуються на методі Монте-Карло та алгоритмі пошуку у ширину (Breadth-First Search, BFS) для виявлення кластерних відмов на ділянках довільної форми. Розробляється марковська модель готовності сенсорної мережі з відновленням, яка, враховує інтенсивності відмов сенсорів та периферійного обладнання, середній час відновлення та час очікування ремонту. Запропоновані моделі формують вимоги до алгоритмів майбутнього програмного комплексу.

Етап 4. Програмна реалізація та впровадження. Спрямований на вирішення Задач 5 та 6. Імітаційні та аналітичні моделі, розроблені на Етапах 2 та 3, реалізується у вигляді комплексу програмних засобів. Створюються інструменти для автоматизації аналітичних обчислень систем з багаторівневою працездатністю. Створюється засіб для симуляції відмов сенсорної мережі в залежності від кількості та розмірності фатальних комбінацій непрацездатних сенсорів. На основі засобу для виявлення фатальних комбінацій непрацездатних сенсорів (ФКНС) створюється засіб імітаційного моделювання з використання методу Монте-Карло для генерації випадкових відмов сенсорної мережі на основі експоненційного розподілу для імітаційного оцінювання ймовірності безвідмовної роботи мережі за стохастичних сценаріїв відмов з візуалізацією розміщення сенсорної мережі на мапі та просторових кластерних відмов. Здійснюється валідація отриманих результатів та впровадження розроблених методів і засобів у навчальний процес і науково-дослідні роботи.

Таким чином, результати кожного попереднього етапу є вхідними даними для наступного, формуючи цілісну методологію дослідження: від теоретичного аналізу та структурних моделей до створення імітаційних моделей та їх програмної реалізації.

1.6 Висновки до першого розділу

Традиційні наземні БСМ мають обмежену стійкість до деструктивних зовнішніх чинників та механічних пошкоджень інфраструктури. Інтеграція БПЛА та впровадження концепцій «літаючого Інтернету речей» (IoFT) і ЛГО є критично необхідними для подолання цих обмежень, забезпечуючи оперативне зондування важкодоступних ділянок та мінімізацію затримок у передачі даних.

Традиційний математичний апарат, зокрема дерева відмов, діаграми бінарних рішень та марковські ланцюги, демонструє високу точність лише для систем малої розмірності. При масштабуванні мережі до рівня гібридної системи моніторингу ПНТ (понад 1000 вузлів) обчислювальна складність цих методів зростає експоненціально, що потребує впровадження комбінованих підходів на основі імітаційного моделювання та статистичної верифікації.

Більшість існуючих моделей базується на припущенні про незалежність відмов окремих сенсорів. Проте в умовах моніторингу ПНТ загрози (пожежі, викиди) викликають корельовані (групові) збої. Відсутність у джерелах формалізації «кластерних відмов» як фатальних комбінацій несправних вузлів суттєво знижує точність оцінювання надійності, оскільки система може зберігати зв’язність, але втрачати здатність до моніторингу конкретних ділянок.

Сучасні дослідження переважно аналізують надійність наземних БСМ та мобільних флотів БПЛА відокремлено. Для підвищення достовірності результатів необхідно розробити цілісну методологію, яка об’єднає показники мережевої надійності та геометричного покриття території у межах єдиного розрахункового циклу для стаціонарних і мобільних компонентів.

Існує певний дефіцит спеціалізованого програмного інструментарію. Наявні симулятори (OMNeT++, NS-3, COOJA) фокусуються на мережевих протоколах та енергоефективності, а комерційні продукти (ReliaSoft) − на статичних структурах. Відсутні також програмні засоби, здатні моделювати динаміку гібридних мереж великої розмірності з можливістю автоматичної ідентифікації просторових кластерних відмов.

Визначено цілісну стратегію розв’язання наукової задачі, яка базується на поєднанні апарату системного аналізу, теорії надійності та імітаційного моделювання для підвищення точності оцінювання гібридних сенсорних мереж.

Науково обґрунтовано використання марковських ланцюгів неперервного часу для аналізу готовності відновлюваних компонентів, методу Монте-Карло для стохастичного моделювання відмов на територіях довільної форми та алгоритму обходу графа в ширину (BFS) для автоматичної ідентифікації кластерних відмов.

Запропоновано чотириетапну структуру дослідження, яка забезпечує логічний перехід від формалізації аналітичних залежностей і структурних моделей ГСМ до створення спеціалізованого програмного комплексу, здатного візуалізувати та кількісно оцінювати надійність систем моніторингу ПНТ як за сценаріями фатальних комбінацій відмов, так із урахуванням багаторівневої працездатності.

РОЗДІЛ 2
РОЗРОБЛЕННЯ СТРУКТУР ТА АНАЛІТИЧНИХ МОДЕЛЕЙ НАДІЙНОСТІ ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ

2.1 Розроблення структур гібридних сенсорних мереж систем моніторингу з використанням літаючих хмарних, граничних та туманних обчислень

2.1.1 Варіанти схем організації та застосування літаючих та наземних хмарних, граничних та туманних обчислень для побудови гібридних сенсорних мереж

У сучасному світі БПЛА розглядають як фундаментальну технологічну базу, що здатна ефективно інтегруватися з концепціями інтернету речей (IoT) для розгортання складних систем моніторингу (СМ) ПНТ. Для того щоб архітектура сенсорних мереж у межах СМ ПНТ була максимально адаптивною, енергоефективною та ресурсоощадною, такі рішення доцільно реалізовувати в тісній комбінації з технологіями літаючих хмарних та літаючих туманних обчислень. Це дає змогу організувати безперервну інтелектуальну взаємодію з обчислювальними ресурсами, які базуються безпосередньо на землі, зокрема з розгалуженою інфраструктурою наземних граничних обчислень.

Завдяки своїй універсальності та можливості швидкого розгортання, БПЛА в подібних архітектурах спроможні виконувати різні функціональні завдання, зокрема:

- відігравати роль мобільних пристроїв, що делегують обчислення на потужніше наземне обладнання;
- виконувати функції підсистеми ЛГО (або ЛХО, ЛТО), яка безпосередньо відповідає за моніторинг кінцевих вузлів (сенсорів) і здатна працювати як ретранслятор, передаючи та обробляючи інформацію між сенсорами й наземною інфраструктурою (наприклад, вузлами граничних обчислень).

Вибір компонентів для архітектури ГСМ базується на аналізі умов її розміщення та особливостей використання відповідних елементів. Порівняльний аналіз технологій ЛХО, ЛГО та ЛТО, проведений на основі сучасних досліджень, дає змогу систематизувати та класифікувати особливості їх застосування. Детальний аналіз кожної технології зведено у три окремі таблиці (2.1, 2.2, 2.3). Характеристики архітектури, переваги та недоліки ЛХО наведено в табл. 2.1.

Таблиця 2.1 − Особливості архітектури, переваги та недоліки літаючих хмарних обчислень

Вид літаючих обчислень	Особливості архітектури	Основні переваги	Основні недоліки
Літаючі хмарні обчислення	Централізована обробка. Швидкий доступ через Інтернет до великої кількості даних.	Масштабованість. Економічна ефективність. Використання надійного TCP/IP протоколу.	Великий час затримки. Обмежена пропускна здатність. Вразливості системи безпеки. Відсутність автономного режиму. Обмежений ресурс батареї. Єдина точка відмови.

Основними архітектурними особливостями ЛХО є централізована обробка даних та використання надійного протоколу TCP/IP. Такі особливості архітектури надають можливість швидкого доступу через Інтернет до великих об’ємів

потрібної інформації. Також архітектура відрізняється високою масштабованістю та економічною ефективністю. Але застосування ЛХО має відповідні недоліки: великий час затримки, обмежена пропускна здатність, вразливість системи безпеки та відсутність режиму автономної роботи. Окрім зазначених недоліків, в таких системах виникає проблема обробки інформації у випадку паралельної передачі інформації великою кількістю пристроїв.

Особливості архітектури, переваги та недоліки ЛГО наведено у таблиці 2.2.

Таблиця 2.2 − Особливості архітектури, переваги та недоліки літаючих граничних обчислень

Вид літаючих обчислень	Особливості архітектури	Основні переваги	Основні недоліки
Літаючі граничні обчислення	Немає потреби у стаціонарній комунікаційній інфраструктурі. Літаючий вузол діє як підсистема комунікації та зв’язку. Літаючий вузол знаходиться ближче до кінцевих пристроїв.	Гнучкість. Масштабованість. Енергоефективність. Здатність працювати з мобільними кінцевими пристроями. Можливість автономного виконання процесів, правил та алгоритмів.	Обмежений ресурс батареї літаючого вузла. Єдина точка відмови.

Головна особливість ЛГО полягає у відсутності потреби мати стаціонарні комунікаційні пристрої. Літаючий вузол знаходиться ближче до кінцевих пристроїв і виступає у ролі системи комунікації. Перевагами технології граничних обчислень є гнучкість використання, масштабованість, енергоефективність, здатність

працювати з мобільними кінцевими пристроями та можливість автономного виконання завдань.

Особливості архітектури, переваги та недоліки ЛТО наведено у таблиці 2.3.

Таблиця 2.3 − Особливості архітектури, переваги та недоліки літаючих туманних обчислень

Вид літаючих обчислень	Особливості архітектури	Основні переваги	Основні недоліки
Літаючі туманні обчислення	Децентралізована обробка. Поширює можливості хмарного середовища до границі мережі.	Гнучкість. Масштабованість. Енергоефективність. Низька затримка передачі даних та кращий взаємозв’язок з кінцевими пристроями. Розширені можливості для застосунків, що працюють у реальному часі.	Обмежений ресурс батареї літаючого вузла. Єдина точка відмови. Дані можуть надсилатися до літаючого вузла складними маршрутами, що збільшує ймовірність їхньої часткової або повної втрати.

Архітектура ЛТО вирізняється децентралізованою обробкою даних, що збільшує можливості використання хмарних послуг до границі мережі. Це забезпечує низьку затримку передачі даних, кращий взаємозв’язок з кінцевими пристроями та надає більші можливості для застосунків, які працюють у режимі реального часу. Головним недоліком архітектури є складна мережева топологія,

через що дані можуть надсилатися до літаючого вузла складними маршрутами, що збільшує ймовірність втрати таких даних.

Спільними недоліками для цих технологій (ЛХО, ЛГО, ЛТО) залишаються обмежений ресурс акумуляторних батарей літаючих вузлів та наявність єдиної точки відмови у разі непрацездатності окремого вузла.

Після проведення аналізу, було виділено три базові варіанти схем організації літаючих обчислень:

– схема організації ЛХО;

– схема організації ЛХО;

– схема організації ЛТО.

Розглянемо схему організації ЛХО. Ця схема (рисунок 2.1) орієнтована на сценарії надзвичайної ситуації. У цьому випадку наземна інфраструктура пошкоджена, а кінцеві пристрої (КП) не мають доступу до глобальної мережі.

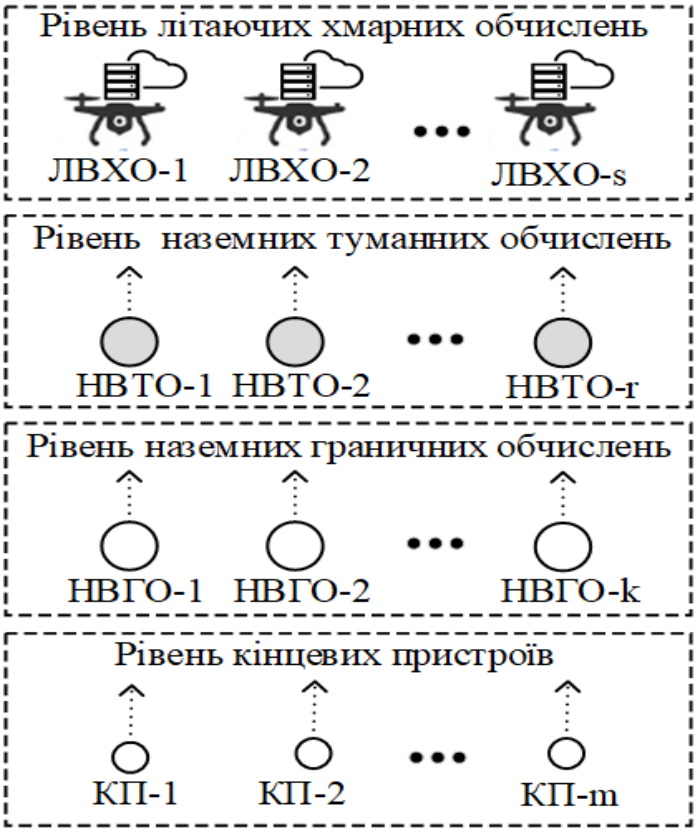

Рисунок 2.1 − Варіант схеми організації літаючих хмарних обчислень

У цій схемі локальні послуги, такі як попереднє розвантаження завдань, надаються на рівні наземних вузлів граничних (НВГО) або туманних (НВТО) обчислень. Глобальні послуги − агрегація даних, безпека системи, аналітика даних − виконує флот БПЛА, що перетворюється на підсистему літаючих хмарних обчислень (ПсЛХО). Окремі БПЛА у цьому випадку функціонують як літаючі вузли хмарних обчислень (ЛВХО).

Далі розглянемо схему організації ЛГО. На запропонованій схемі (рисунок 2.2), флот БПЛА діє як підсистема літаючих граничних обчислень (ПсЛГО), яка знаходиться максимально близько до джерел даних.

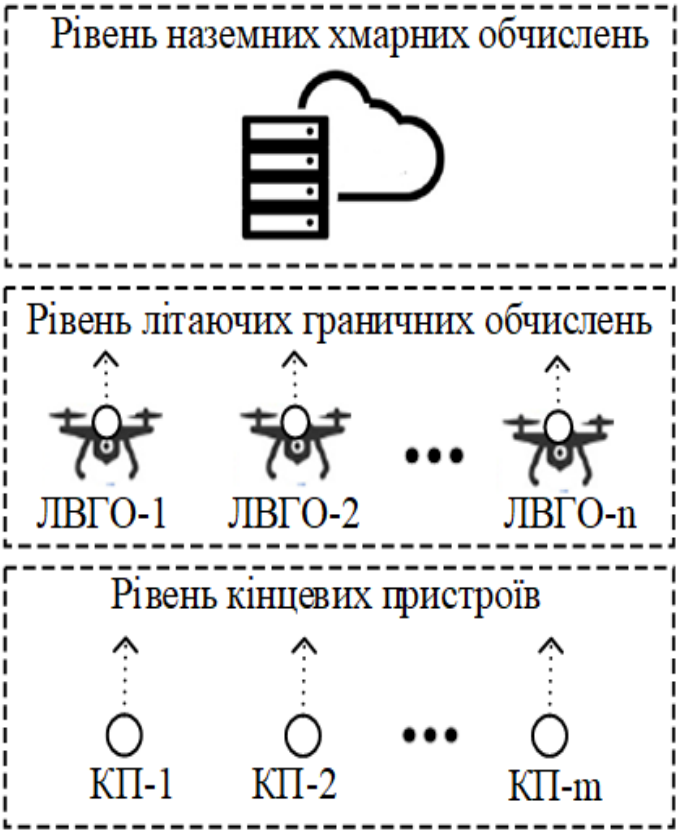

Рисунок 2.2 − Варіант схеми організації літаючих граничних обчислень

Перевагою такої організації є безпосередня обробка даних на борту літаючого вузла граничних обчислень (ЛВГО), що знижує затримку передачі даних та таким чином оптимізує енергоспоживання наземних сенсорів, які витрачають менше потужності для передачі даних до БПЛА.

У разі неможливості виконання завдання за допомогою ПсЛГО, обчислення переводяться на рівень наземних хмарних обчислень (НХО).

Схема організації літаючих туманних обчислень (ЛТО), представлена на рисунку 2.3, передбачає використання флоту БПЛА як підсистеми літаючих туманних обчислень (ПсЛТО).

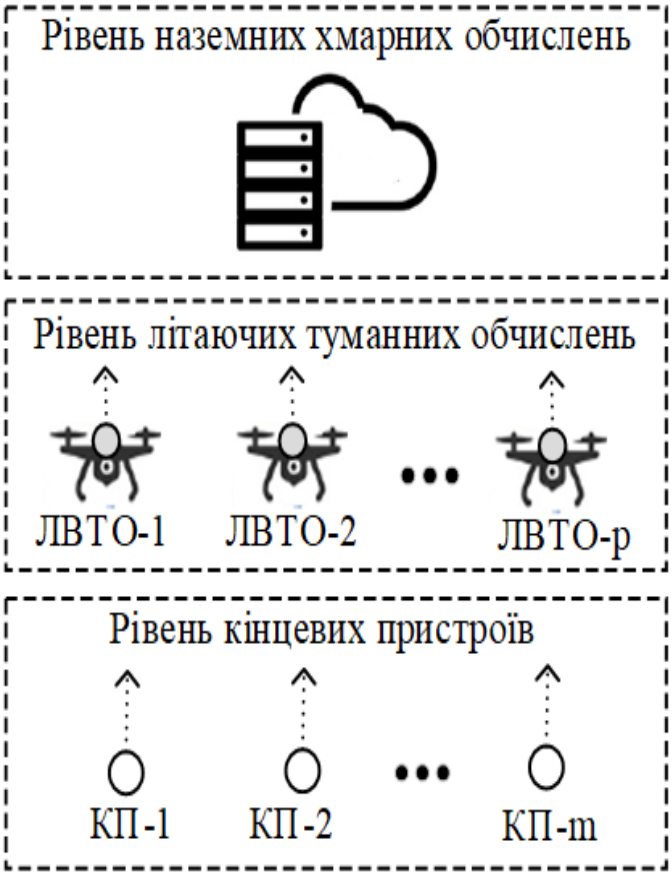

Рисунок 2.3 − Варіант схеми організації літаючих туманних обчислень

БПЛА у ролі літаючих вузлів туманних обчислень (ЛВТО) виступають проміжним інтелектуальним шаром, що поєднує наземні хмарні сервери та кінцеві пристрої. Такий підхід забезпечує достатній об’єм сховища зберігання даних та видає низьку затримку, ці показники є критичними для застосунків, працюючих у режимі реального часу в умовах нестабільного зв’язку.

2.1.2 Архітектура гібридної сенсорної мережі з інтеграцією граничних обчислень та безпілотних літальних апаратів

У цьому підрозділі представлено архітектуру ГСМ, що базується на синергії технологій граничних обчислень та застосуванні БПЛА для моніторингу об’єктів у режимі реального часу. Запропонована багатокомпонентна структура забезпечує виконання повного циклу операцій: збір, інтелектуальне оброблення та комплексний аналіз даних моніторингу. Архітектура побудована за ієрархічним принципом і включає три основні рівні: хмарний, рівень БПЛА та наземний рівень.

Хмарний рівень відповідає за централізоване зберігання великих масивів даних, їх оброблення, візуалізацію отриманих результатів та автоматичне сповіщення про потенційні небезпеки. На цей рівень надходять попередньо опрацьовані дані з нижчих рівнів ієрархії (БПЛА та наземного рівня). Хмарна інфраструктура здійснює їх фінальний аналіз, результати якого стають основою для прийняття стратегічних управлінських рішень. Критично важливою функцією цього рівня є архівація історичних показників роботи системи, що дає змогу виявляти довгострокові тенденції та приховані закономірності. Аналіз ретроспективних даних сприяє точному прогнозуванню майбутніх станів об’єкта моніторингу.

Рівень БПЛА представлений флотом БПЛА, оснащених високопродуктивними бортовими одноплатними комп’ютерами та мультиспектральними сенсорами. Цей рівень забезпечує високу мобільність та адаптивність системи, дозволяючи збирати й первинно фільтрувати дані безпосередньо під час виконання польотних завдань. БПЛА здатні автономно функціонувати в контрольованому просторі, здійснюючи моніторинг у важкодоступних зонах або на великих площах, де розгортання стаціонарної наземної інфраструктури є економічно недоцільним або технічно неможливим через специфіку рельєфу чи умови експлуатації. Обчислювальні потужності бортових систем дозволяють виконувати граничну обробку даних, що мінімізує навантаження на канали зв’язку шляхом передачі лише релевантної та критично важливої інформації.

Третій, наземний рівень, базується на використанні спеціалізованих пристроїв для виконання граничних обчислень (далі — граничні пристрої). Наземні граничні пристрої приймають вхідні потоки даних від рівня БПЛА, після чого здійснюють їх опрацювання із застосуванням алгоритмів машинного навчання або інших сучасних аналітичних методів. Очищена та структурована інформація згодом передається на хмарний рівень для довгострокового зберігання, ретроспективного аналізу та фінальної візуалізації. Перенесення обчислювального навантаження безпосередньо до місця проведення моніторингу надає системі змогу суттєво оптимізувати загальну продуктивність мережевої інфраструктури.

Схематичне зображення запропонованої трирівневої архітектури гібридної сенсорної мережі у складі СМ ПНТ наведено на рисунку 2.4.

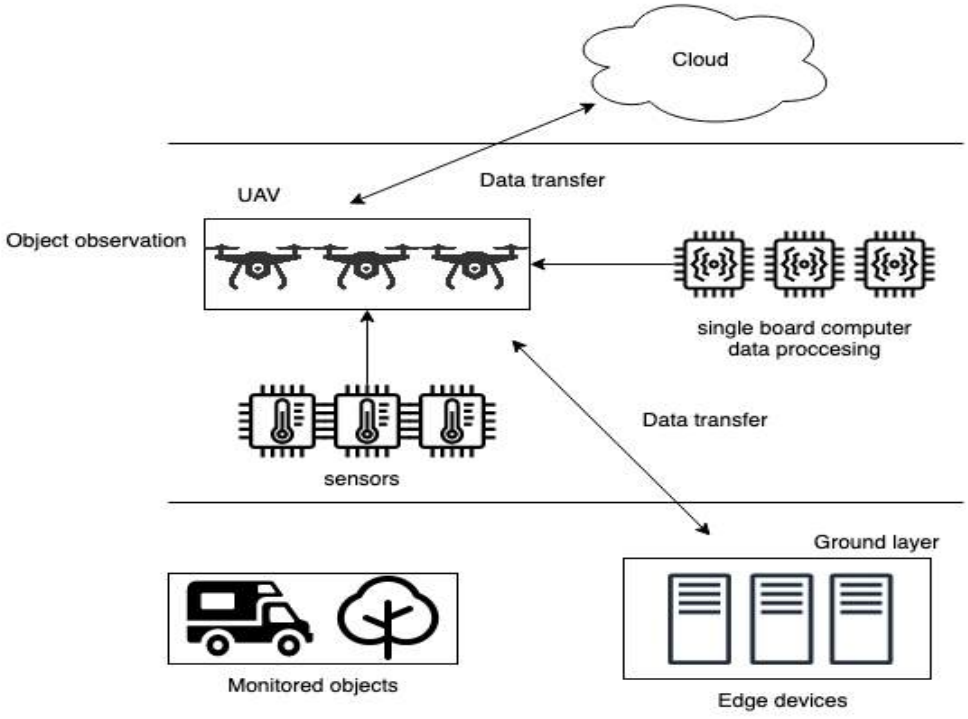

Рисунок 2.4 − Приклад трирівневої архітектури гібридної сенсорної мережі: Cloud − хмарний рівень; UAV − рівень БПЛА; Ground layer − наземний рівень; Data transfer − передавання даних; Object observation − спостереження за об’єктами; single board computer data processing − оброблення даних на одноплатному комп’ютері; sensors − сенсори; Monitored objects − об’єкти моніторингу; Edge devices − граничні пристрої

На наведеному рисунку продемонстрована взаємодія між рівнями: дані від об’єктів моніторингу через сенсори та граничні пристрої надходять до рівня БПЛА, де обробляються і відправляються далі до хмарного рівня для подальшого зберігання та обробки. Така архітектура надає можливість оперативно реагувати на локальні події та проводити глобальну аналітику.

Запропонована архітектура передбачає адаптивність до умов експлуатації. Коли застосування БПЛА є недоцільним (наприклад, через погодні умови, законодавчі обмеження або специфіку об’єкта), архітектура може бути переналаштована у систему з двох рівнів, що складаються з наземного та хмарного рівнів.

У варіанті конфігурації без БПЛА сенсори передають дані на граничні пристрої, які попередньо обробляють інформацію та відправляють її до хмари. Така альтернативна конфігурація зберігає основні переваги граничних обчислень і може використовуватися для різних сценаріїв моніторингу. Відсутність БПЛА дозволяє знизити витрати на впровадження системи та забезпечення її функціонування. Такі зміни зберігають важливість цієї системи через її характеристики продуктивності та стабільності роботи.

На рисунку 2.5 показана спрощена схема взаємодії, де середовище моніторингу обслуговується сенсорами та граничними пристроями, які передають дані на хмару.

Таким чином, така архітектура дозволяє адаптувати систему моніторингу під конкретні завдання та оптимізувати використання ресурсів залежно від вимог та потреб користувачів. Завдяки таким можливостям, як масштабованість, гнучкість та переналаштування, ГСМ здатні адаптуватися до різних умов експлуатації.

Ключовою перевагою подібної архітектури є підвищена надійність сенсорної мережі: у разі збою одного з вузлів, передача даних буде направлена через сусідні робочі вузли, що забезпечує безперервність моніторингу.

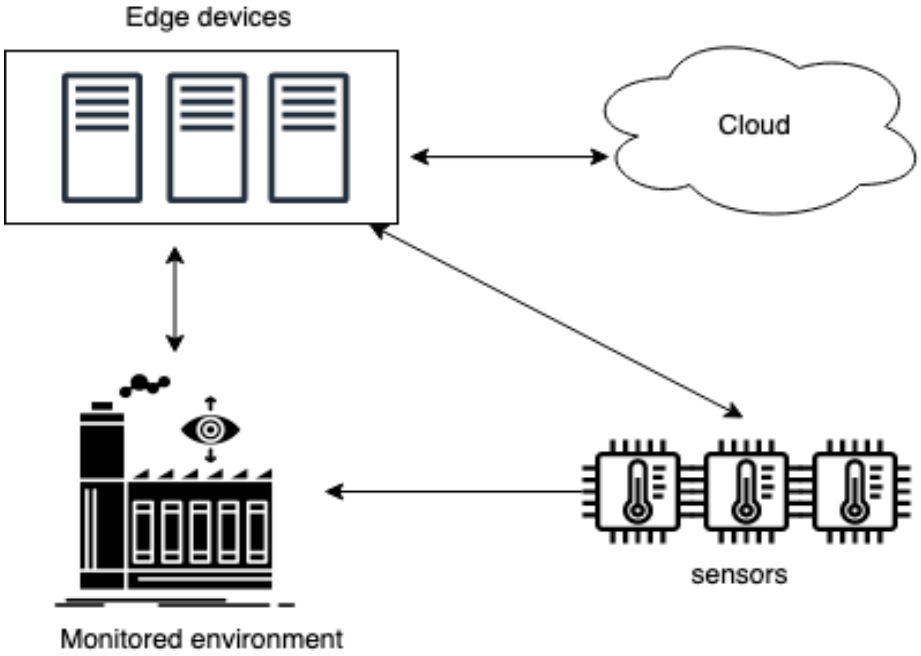

Рисунок 2.5 − Приклад архітектури гібридної сенсорної мережі без рівня БПЛА: Cloud − хмарний рівень; sensors − сенсори; Edge devices − граничні пристрої; Monitored environment − середовище моніторингу

2.1.3 Варіанти застосування літаючих та наземних хмарних, граничних та туманних обчислень компонентами системи моніторингу

Практичну реалізацію розглянутих схем СМ ПНТ покажемо на прикладі СМ потенційно небезпечного об’єкта (ПНО). Запропонована система складається з наступних компонентів: безпосередньо ПНО з об’єктами контролю (як правило, критичні технологічні установки), кризовий центр (КЦ), флот БПЛА, пункт дистанційного пілотування (ПДП) та група зовнішніх експертів (ГЗЕ). На підставі аналізу завдань для кожного компонента запропоновано варіанти застосування хмарних, граничних та туманних обчислень у межах СМ ПНО (таблиця 2.4). Аналіз таблиці 2.4 свідчить, що хмарні обчислення є універсальним підходом: вони використовуються як з мобільними пристроями (через флот БПЛА), так і стаціонарно, спираючись на інфраструктуру ПДП, КЦ та ГЗЕ. Граничні обчислення застосовуються між безпосереднім місцем збору даних (наземна сенсорна мережа на ПНО) та флотом БПЛА, що мінімізує час реакції на інциденти. Запропонована

архітектура туманних обчислень є найбільш спеціалізованою і реалізується виключно літаючим компонентом.

Таблиця 2.4 – Варіант застосування хмарних, граничних та туманних обчислень компонентами СМ ПНО

Види обчислень		Компоненти СМ ПНО				
		ПНО	Флот БПЛА	ПДП	КЦ	ГЗЕ
Хмарні обчислення	літаючі	–	+	–	–	–
	наземні	–	–	+	+	+
Граничні обчислення	літаючі	–	+	–	–	–
	наземні	+	–	–	–	–
Туманні обчислення	літаючі	–	+	–	–	–
	наземні	–	–	–	–	–

Для успішного функціонування ЛХО, ЛГО та ЛТО у складі компонентів СМ ПНО необхідно розгорнути відповідні підсистеми, як показано у таблиці 2.5.

Таблиця 2.5 – Підсистеми у складі компонентів СМ ПНО, створювані для реалізації хмарних, граничних та туманних обчислень

Компонент СМ ПНО	Назва підсистеми
ПНО	ПсНГО−ПНО
Флот БПЛА	ПсЛХО−Ф
	ПсЛГО−Ф
	ПсЛТО−Ф
ПДП	ПсНХО−ПДП
КЦ	ПсНХО−КЦ
ГЗЕ	ПсНХО−ГЗЕ

Аналізуючи таблицю 2.5, ми бачимо, що флот БПЛА є компонентом системи, який має найбільше навантаження. У складі флоту можуть одночасно функціонувати три типи підсистем: літаючих хмарних (ПсЛХО−Ф), граничних

(ПсЛГО−Ф) та туманних (ПсЛТО−Ф) обчислень. Це підкреслює роль БПЛА як ключового елемента гібридної сенсорної мережі за наявності його використання.

Завдяки використанню методів штучного інтелекту (ШІ) та машинного навчання можна суттєво підвищити ефективність роботи згаданих підсистем. Застосування ШІ дозволяє автоматизувати складні процеси управління мережею та обробки даних, оптимізувати розподіл ресурсів і контролювати перевантаження системи. За результатами аналізу сформовано перелік завдань СМ ПНО, що вирішуються за допомогою конкретних методів ШІ, наведених у таблиці 2.6. Зокрема, розглянуто: глибоке навчання (DL − Deep Learning), навчання з підкріпленням (RL − Reinforcement Learning), алгоритм мурашиної колонії (RL-ACO − Reinforcement Learning based on Ant Colony Optimization) глибоке навчання з підкріпленням (DRL − Deep Reinforcement Learning), генетичні алгоритми (GA − Genetic Algorithm), федеративне навчання (FL − Federated Learning) та методи нечіткого виведення (FI − Fuzzy Inference).

Аналіз методів штучного інтелекту (ШІ) дозволяє зробити такі висновки щодо їх застосування в архітектурі СМ ПНО:

1. Навчання з підкріпленням (RL) є універсальним методом, що застосовується всіма підсистемами для розвантаження обчислень та оптимізації розподілу ресурсів.

2. Для задач динамічного розподілу ресурсів доцільно використовувати спеціалізовані методи, такі як RL-ACO, що базуються на алгоритмах мурашиної колонії.

3. Підтримка прийняття рішень у межах кризового центру та групи експертів забезпечується комплексом методів (RL, DRL, GA, DL, FI, FL). Така мультимодальність зумовлена високим рівнем відповідальності цих підсистем та складністю задач, які вони розв'язують.

4. Методи RL є базовими для планування маршрутів БПЛА. Оскільки за планування відповідають саме мобільні (літаючі) підсистеми, це дозволяє адаптувати траєкторії польоту до змін навколишнього середовища в режимі реального часу.

Використання методів ШІ в архітектурі СМ ПНО дозволяє створити адаптивну систему моніторингу. Завдяки інтеграції згаданих підходів мережа функціонує ефективніше в умовах динамічності та високого рівня невизначеності.

Таблиця 2.6 – Завдання, виконувані підсистемами СМ ПНО з використанням різних методів штучного інтелекту

Завдання	Метод ШІ	Підсистеми СМ ПНО						
		ПсЛХО–Ф	ПсЛГО–Ф	ПсЛТО–Ф	ПсНГО–ПНО	ПсНХО–ПДП	ПсНХО–КЦ	ПсНХО–ГЗЕ
Розвантаження обчислень	RL	+	+	+	+	+	+	+
	DRL	+	+	+	+	+	+	+
	GA	+	+	+	+	+	+	+
	DL	+	+	+	+	+	+	+
	FI	+	+	+	+	+	+	+
Розподіл ресурсів	RL	+	–	–	+	+	+	+
	DRL	+	–	–	+	+	+	+
	GA	+	–	–	+	+	+	+
	RL−ACO	+	–	–	+	+	+	+
Підтримка прийняття рішень	RL	+	–	–	–	–	+	+
	DRL	+	–	–	–	–	+	+
	GA	+	–	–	–	–	+	+
	DL	+	–	–	–	–	+	+
	FI	+	–	–	–	–	+	+
	FL	+	–	–	–	–	+	+
Забезпечення безпеки	RL	+	+	+	+	+	+	+
	DRL	+	+	+	+	+	+	+
	GA	+	+	+	+	+	+	+
	DL	+	+	+	+	+	+	+
	FL	+	+	+	+	+	+	+
Планування маршрутів руху БПЛА	RL	+	–	+	–	+	–	–

2.2. Розроблення аналітичних моделей надійності гібридних сенсорних мереж систем моніторингу

2.2.1 Класифікація моделей надійності гібридних сенсорних мереж

Гібридні сенсорні мережі (ГСМ) характеризуються високою адаптивністю до різних умов експлуатації. Перевагою систем моніторингу на основі ГСМ є можливість інтеграції стаціонарних та мобільних компонентів, що суттєво підвищує загальну надійність. У разі виходу з ладу одного з вузлів передача даних перенаправляється через сусідні сегменти мережі. Надійність такої системи визначається комплексом факторів, зокрема: стабільністю апаратного та програмного забезпечення периферійного обладнання, топологією розміщення вузлів, частотою збору та передачі інформації, можливістю відновлення працездатності вузлів та рівнем резервування окремих компонентів.

Нижче наведено класифікацію моделей надійності сенсорних мереж, систематизованих за ознаками відновлюваності та резервування:

– Моделі безвідмовності нерезервованих мереж без відновлення (МБ1). Це базовий клас моделей, що базуються на загальній кількості та інтенсивності відмов окремих сенсорів чи системних компонентів. Критерій відмови всієї мережі при цьому формується без урахування просторового розташування непрацездатних вузлів.

– Моделі безвідмовності сенсорних мереж із резервуванням (МБР2). Враховують дублювання сенсорів, де кожен первинний елемент має резервний аналог, здатний перебрати функції у разі відмови основного.

– Моделі готовності нерезервованих і резервованих мереж із відновленням (МГ1). Ключовою особливістю цих моделей є врахування здатності системи повертатися до працездатного стану завдяки фізичній заміні або ремонту непрацездатних елементів.

– Моделі безвідмовності та готовності з урахуванням деградації (МГД2). Застосовуються для оцінювання систем, здатних до поступового зниження функціональності внаслідок накопичення відмов. Моделі враховують можливість

продовження роботи системи за рахунок залучення додаткових мобільних або стаціонарних підсистем.

– Моделі безвідмовності та готовності з урахуванням топології (МБП3 і МГП3). У цих моделях критерій відмови є складнішим і визначається не лише кількістю непрацездатних вузлів, а й їхнім конкретним розташуванням, що дозволяє ідентифікувати втрату покриття на певних ділянках.

2.2.2 Розроблення аналітичних моделей надійності системи моніторингу на основі гібридної сенсорної мережі

2.2.2.1 Досліджувана структура системи моніторингу на основі гібридної сенсорної мережі

При аналізі СМ, що використовуються для спостереження за міськими складними об’єктами (Urban Complex Objects, UCOs), наприклад, промислові та енергетичні об’єкти, треба правильно формалізувати їх структури.

Досліджувана структура базується на концепції передової повітряної мобільності (Advanced Air Mobility, AAM) та інтегрує технології літаючих сенсорних мереж (Flying Sensor Networks, FSNets) і літаючих мереж граничних обчислень (Flying Edge Networks, FENets).

Загальна схема досліджуваної СМ, адаптована для задач моніторингу міських складних об’єктів, представлена на схемі (рисунок 2.6).

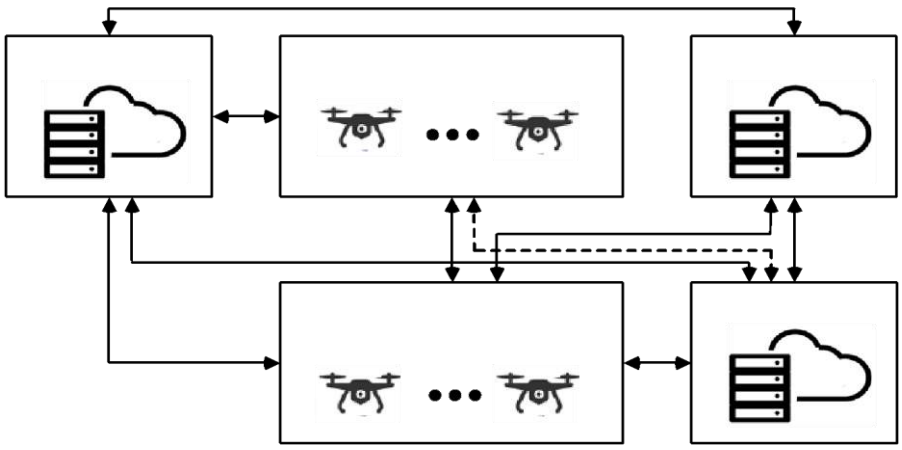

Рисунок 2.6 − Загальна схема системи моніторингу

На рисунку 2.6 зображено, що до складу системи входять такі компоненти:

– флот літаючих сенсорів (Fleet of Flying Sensors, FoFSen) розгорнутий для вимірювання параметрів, що характеризують ступінь забруднення навколишнього середовища та метеорологічні умови (такі сенсори можуть використовуватися замість пошкоджених стаціонарних станцій моніторингу);

– наземна станція управління (Ground Control Station, GCS). Забезпечує керування безпілотним літальним апаратом зовнішніми пілотами (операторами);

– флот літаючих вузлів граничних обчислень (Fleet of Flying Edge Nodes, FoFEN). Розгорнутий для збору інформації від літаючих датчиків, часткової обробки цієї інформації та її передачі до головного кризового центру;

– головний кризовий центр (Main Crisis Centre, MCC). Призначений розробляти заходи щодо запобігання та ліквідації наслідків аварій на об’єкті моніторингу, а також прогнозувати виникнення таких аварій та оцінювати їхні наслідки;

– віртуальний кризовий центр (Virtual Crisis Centre, VCC). Формується групою зовнішніх експертів, які дистанційно спільно з відповідним персоналом кризового центру беруть участь у розробці рішень щодо запобігання та ліквідації наслідків аварій на об’єкті моніторингу.

Алгоритм функціонування системи. При виникненні аварії на міському складному об’єкті БПЛА, що виконують роль літаючих сенсорів та вузлів граничних обчислень, прямують до визначених місць і розгортають відповідні флоти (FoFSeN та FoFEN). Після розгортання FoFSeN передають дані до FoFEN та VCC. FoFEN здійснює попереднє оброблення даних (зберігає результати певних обчислень) і надсилає їх до MCC. Паралельно VCC накопичує дані для аналізу експертною групою.

Важливою особливістю запропонованої структури є наявність механізмів підвищення надійності:

– головний кризовий центр передбачає можливість часткового управління БПЛА у разі відмови наземної станції управління;

– головний кризовий центр має достатньо кваліфікований персонал для автономного прийняття рішень у разі неможливості отримання інформації або рекомендацій від віртуального кризового центру.

Апаратна реалізація літаючих компонентів. Залежно від специфіки моніторингових завдань та часового обмеження їх виконання, у якості літаючих сенсорів або літаючих вузлів граничних обчислень можуть використовуватися різні типи БПЛА. У таблицях 2.7 та 2.8 наведено параметри БПЛА з фіксованим крилом та мультироторного типу, які можуть бути використані у досліджуваній системі.

Таблиця 2.7 – Параметри БПЛА з фіксованим крилом, що можуть використовуватися як FSen/FEN

№ з/п	Назва	Виробник	Тип двигуна	Розмах крил / Діаметр ротора* (м)	Максимальна дальність польоту (км)	Максимальна тривалість польоту (год)	Максимальна злітна маса (кг)
1	Bird-Eye 650D	Israel Aerospace	Внутрішнього згоряння	4.0	150	15	30
2	Bayraktar TB2	Baykar Makina	Внутрішнього згоряння	12.0	150	20	650
3	PD−1 FW VTOL	Ukrspec Systems	Внутрішнього згоряння	4.7*	100	12	45
4	PD−1	Ukrspec Systems	Внутрішнього згоряння	3	85	10	40
5	Scan Eagle	Boeing	Внутрішнього згоряння	3.1	100	22	18

Таблиця 2.8 – Параметри БПЛА мультироторного типу, що можуть використовуватися як FSen/FEN

№ з/п	Назва	Виробник	Тип двигуна	Максимальна дальність польоту (км)	Максимальна тривалість польоту (хв.)	Максимальна злітна маса (кг)
1	DJI Matrice 300 RTK	DJI	Електричний	15	55	3.6
2	DJI Mavic 3	DJI	Електричний	15	55	3.6

Кінець таблиці 2.8

3	T−hawk	FCS DARPA	Внутрішнього згоряння	11	40	6.6
4	Draganfly	Draganfly Drones	Електричний	30	50	30.4
5	KWT−X6L−Q	ALLTECH	Електричний	50	150	2.5
6	DJI Matrice 300 RTK	DJI	Електричний	15	55	3.6

Аналіз характеристик, наведених у таблицях, дозволяє зробити висновок про доцільність використання БПЛА з фіксованим крилом для тривалих місій на великих відстанях (наприклад, моніторинг протяжних периметрів), тоді як БПЛА мультироторного типу є більш ефективними для локальних завдань, що вимагають зависання та маневрування в обмеженому просторі міської забудови.

Описана структура є базовою для подальшого розроблення математичних моделей надійності, оскільки вона визначає логічні зв’язки між компонентами та сценарії їхньої взаємодії, включаючи механізми резервування та деградації функційності.

2.2.2.2 Розроблення та дослідження аналітичних моделей безвідмовності системи моніторингу

Оцінювання показників надійності системи моніторингу виконується на етапі проєктування системи. Такий підхід дозволяє визначити ефективність впровадження розробленої архітектури до її реалізації.

Для побудови математичної моделі використовуються наступні позначення:

$P_\gamma(t)$ − ймовірність безвідмовної роботи (ЙБР) компонента γ, де γ = MS, GCS, FoFSen, FoFEN, MCC, VCC;

t − час виконання місії (операційний час);

λ_δ− інтенсивність відмов δ, де δ = GCS, FSen, FEN, MCC, VCC;

m − кількість літаючих сенсорів у флоті;

n − загальна кількість літаючих вузлів граничних обчислень у флоті;

k − мінімально необхідна кількість працездатних FEN для виконання завдання.

Під час розроблення моделі було прийнято ряд припущень:

1. Елементи СМ характеризуються експоненційним розподілом часу до відмови.
2. Протягом часу виконання місії СМ розглядається як невідновлювана.
3. FoFSen розглядається як система з послідовним з'єднанням елементів (відмова будь-якого FSen призводить до невиконання місії моніторингу в повному обсязі).
4. FoFEN має структуру типу «k-out-of-n». Це означає, що флот складається з n FEN і залишається працездатним доти, доки працездатними є щонайменше $(n-k+1)$ FEN (кількість резервних FEN становить $(n-k)$).

ССН системи моніторингу представлено на рисунку 2.7.

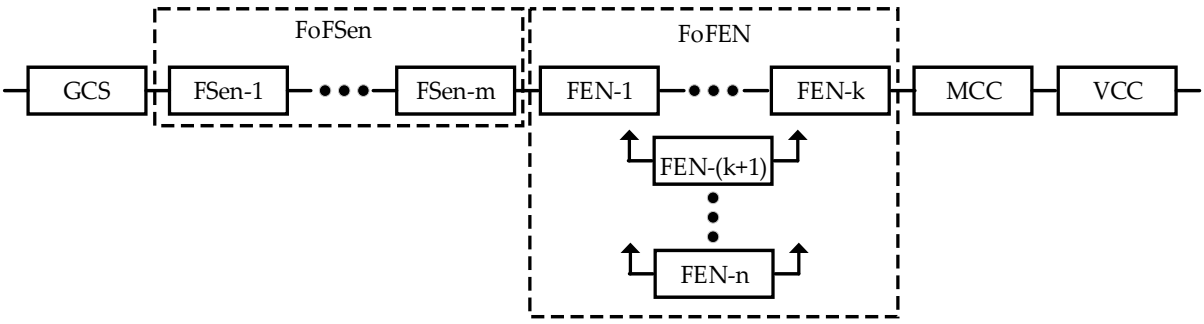

Рисунок 2.7 − Структурна схема надійності системи моніторингу

Відповідно до ССН, математичний вираз для розрахунку ЙБР СМ $P_{MS}(t)$ має вигляд:

$$P_{MS}(t) = P_{GCS}(t)P_{FoFsen}(t)P_{FoFEN}(t)P_{MCC}(t)P_{VCC}(t) \tag{2.1}$$

де:

$$P_{GCS}(t) = e^{-\lambda_{GCS}t}, \tag{2.2}$$

$$P_{FoFSen}(t) = \left[e^{-\lambda_{FSen}t}\right]^m \quad (2.3)$$

$$P_{FoFEN}(t) = \sum_{j=k}^{n} \binom{n}{j} \left[e^{-\lambda_{FEN}t}\right]^j \left[1 - e^{-\lambda_{FEN}t}\right]^{n-j} \quad (2.4)$$

$$P_{MCC}(t) = e^{-\lambda_{MCC}t} \quad (2.5)$$

$$P_{VCC}(t) = e^{-\lambda_{VCC}t} \quad (2.6)$$

З використанням розробленої моделі було проведено серію імітаційних експериментів. В якості вихідних даних використовувалися такі параметри: $m = 21$ (кількість FSen), $n = 9$ (загальна кількість FEN), $k = 7$ (необхідна кількість FEN). Інші параметри, зокрема інтенсивності відмов, змінювалися для дослідження чутливості системи.

Дослідження залежності ЙБР СМ від часу роботи для різних значень інтенсивності відмов FSen (λ_{FSen}) наведено на рисунку 2.8.

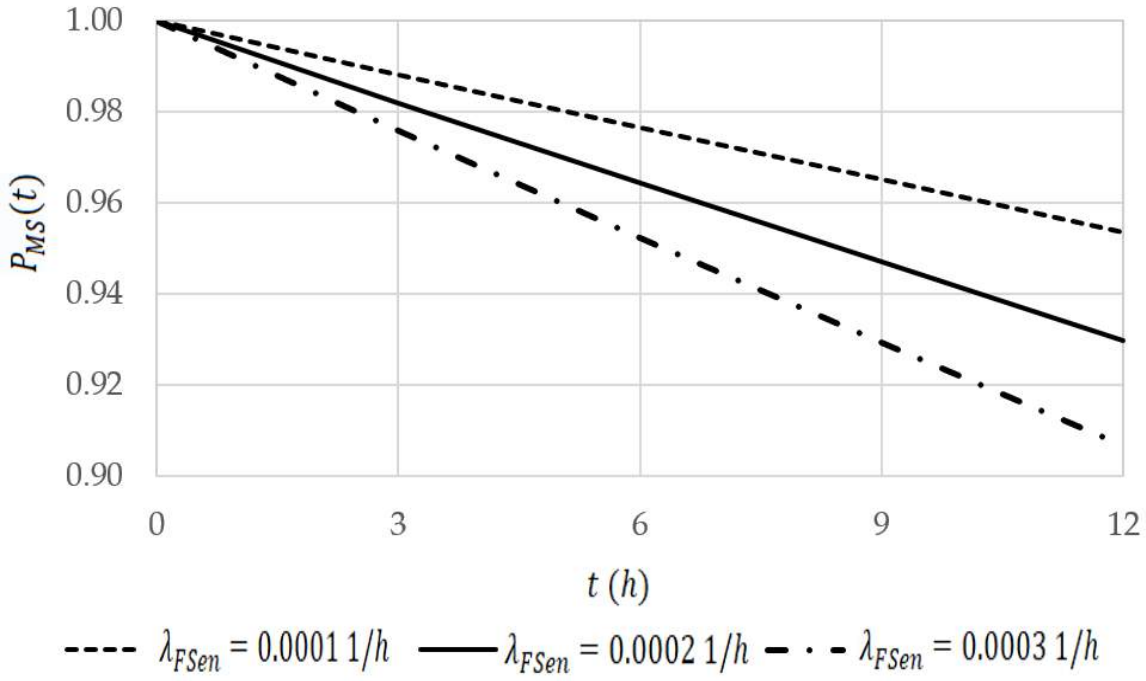

Рисунок 2.8 − Залежність ймовірності безвідмовної роботи системи моніторингу від часу роботи для різних значень інтенсивності відмов FSen

Аналіз отриманих результатів показує, що збільшення часу місії з 0 до 12 годин призводить до зниження ЙБР СМ. Наприклад, при $\lambda_{FSen} = 0.0003$ 1/г ЙБР СМ падає в 1.1 рази (з 1 до 0.90671). Використання FSen (зменшення λ_{FSen} до 0.0001 1/г) більшої надійності дозволяє підвищити ЙБР СМ наприкінці дванадцяти годинної роботи СМ в 1.05 рази.

Аналогічне дослідження було проведено для FEN. Залежність ЙБР СМ від інтенсивності відмов FEN (λ_{FEN}) представлена на рисунку 2.9.

Результати демонструють, що ЙБР СМ є чутливою до відмов FEN. Зменшення інтенсивності відмов λ_{FEN} з 0.005 до 0.001 1/г при $\mathrm{t} = 12$ год призводить до зростання ЙБР СМ в 1.01 рази.

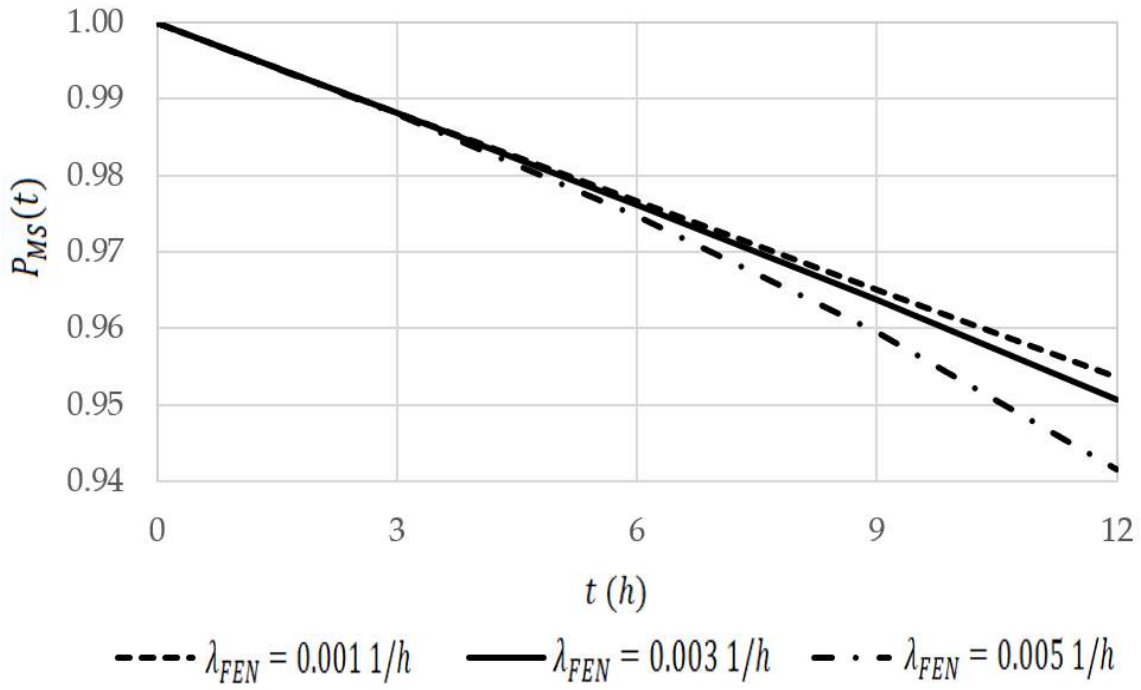

Рисунок 2.9 – Залежність ймовірності безвідмовної роботи системи моніторингу від часу роботи для різних значень інтенсивності відмов FEN

Кількість працездатних FEN безпосередньо впливає на ЙБР системи моніторингу, оскільки цей компонент забезпечує як збір даних із сенсорних вузлів, так і їх часткову обробку, зберігаючи результати проміжних обчислень перед відправленням до МСС. Резервування цих компонентів може суттєво підвищити

надійність системи, тому було проаналізовано вплив кількості резервних FEN у підсистемі граничних обчислень на загальну надійність СМ (рисунок 2.10).

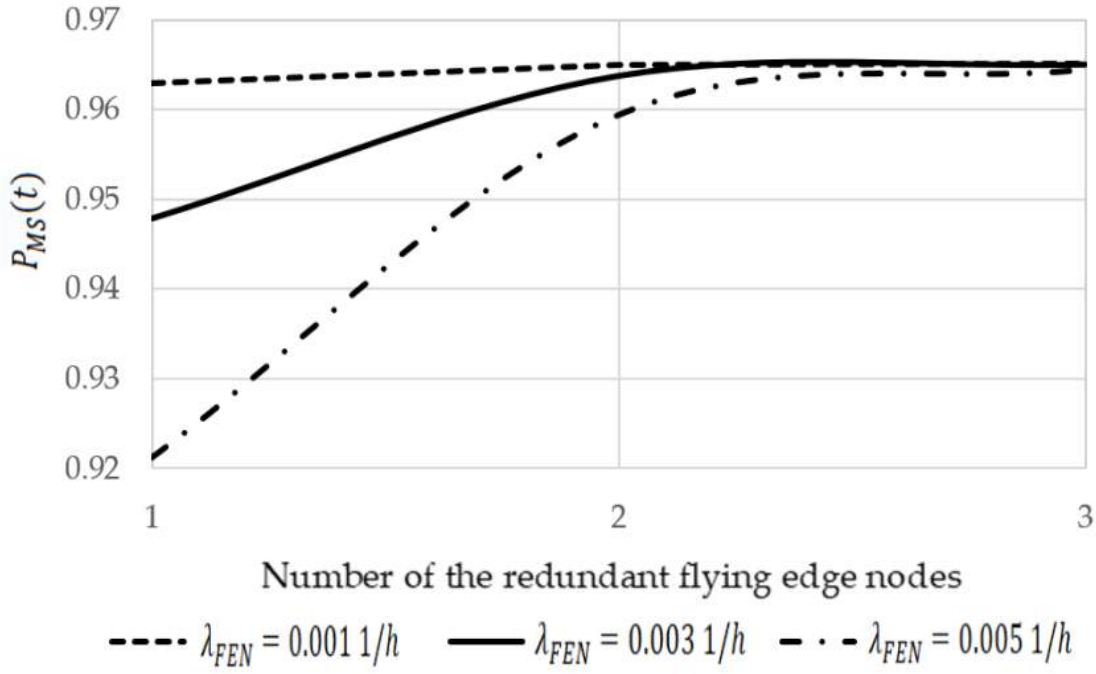

Рисунок 2.10 − Залежність ймовірності безвідмовної роботи системи моніторингу від кількості резервних FEN

Рисунок 2.10 демонструє, що збільшення кількості резервних FEN підвищує ЙБР системи моніторингу. Зокрема, при $\lambda_{FEN} = 0.005$ 1/год додавання резервних вузлів забезпечує зростання ЙБР з 0.92124 до 0.96446 (у 1.05 рази). Найбільш значущий приріст показника спостерігається при впровадженні перших двох резервних FEN, тоді як подальше нарощування їх кількості не призводить до істотного покращення надійності.

Розроблена аналітична модель дозволяє здійснювати кількісне оцінювання надійності СМ на етапі проєктування та обґрунтовувати вимоги до параметрів компонентів і структури флоту БПЛА. Практичне застосування цієї моделі, реалізоване у вигляді спеціалізованого програмного засобу (описаного в розділі 4), дозволяє автоматизувати складні обчислення та своєчасно адаптувати архітектуру гібридної сенсорної мережі до умов реальної експлуатації.

2.2.2.3 Розроблення та дослідження аналітичних моделей надійності системи моніторингу з багаторівневою працездатністю

Функціонування СМ у режимі після аварії характеризується численними несприятливими факторами, що впливають на її працездатність. У цьому випадку доцільно говорити про багаторівневу працездатність СМ, яку можна оцінити за ймовірністю того, що загальна працездатність СМ буде принаймні на заданому рівні. Іншими словами, СМ можна розглядати як систему з багаторівневою працездатністю (СБП). Така система може деградувати від повністю працездатного стану (Рівень 0 (Level 0)) до непрацездатного стану, проходячи через ряд частково працездатних станів (рівні 1, 2, …, *f*).

Деградація стану СМ можлива внаслідок реалізації таких механізмів:

1. У разі відмови віртуального кризового центру (VCC) або наземної станції управління (GCS), їхні функції можуть частково виконуватися головним кризовим центром (MCC).

2. Відмова флоту літаючих сенсорів (FoFSen) або флоту літаючих вузлів граничних обчислень (FoFEN) настає лише після відмови більше ніж α літаючих сенсорів (FSen) або ω літаючих вузлів граничних обчислень (FEN) відповідно.

Введемо наступні позначення:

α − кількість непрацездатних FSen, необхідна для переходу FoFSen з повністю працездатного стану у частково працездатний;

β − кількість основних непрацездатних FEN, необхідна для переходу FoFEN у частково працездатний стан;

ω − загальна кількість непрацездатних FEN, що призводить до деградації FoFEN (де $\omega = n - k + \beta$);

P_{MS_0} − ймовірність перебування СМ у повністю працездатному стані;

$P_{MS\_ij_i}$ − ймовірність перебування СМ у частково працездатному стані j_i на рівні деградації i.

Діаграма рівнів деградації системи моніторингу та відповідні їм стани елементів наведена на рисунку 2.11

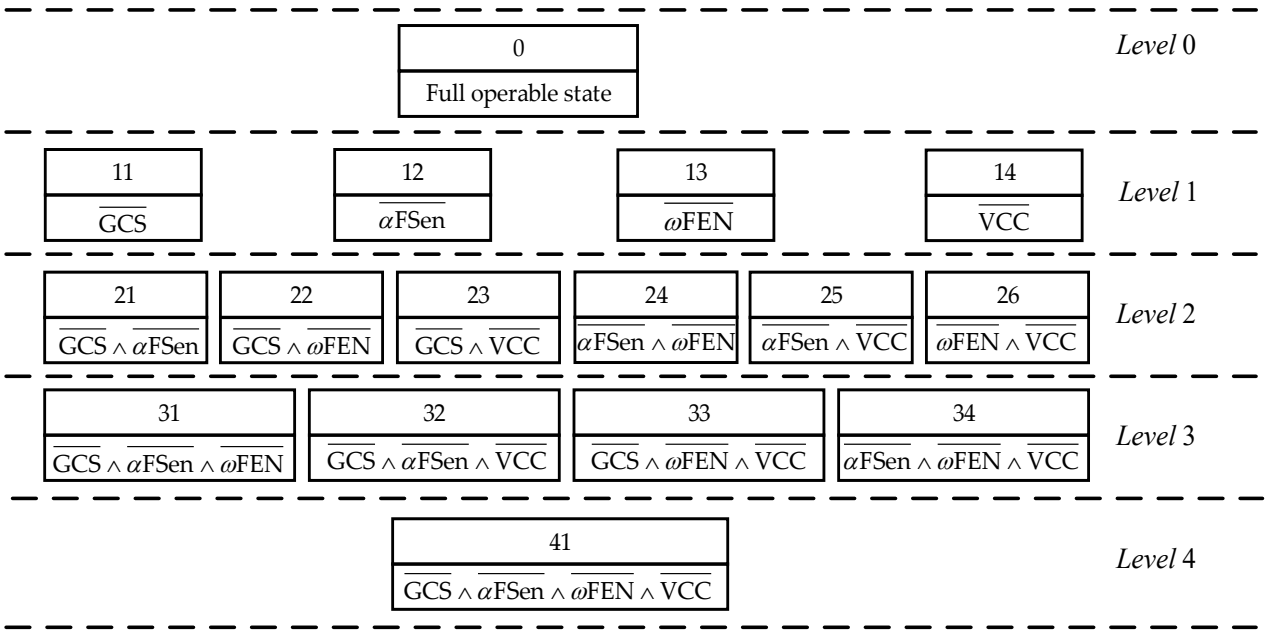

Рисунок 2.11 − Рівні деградації системи моніторингу та відповідні їм елементи, що відмовили

Розрахунок перебування ймовірностей перебування СМ у частково працездатних станах обчислюється системою аналітичних формул. Наприклад, ймовірність перебування СМ у стані, коли GCS та центри працюють, але FoFSen та FoFEN перейшли у режим обмеженої роботи (стан 24), визначається як:

$$P_{MS\_24}(t) = P_{GCS}(t)P_{FoFsen\_L1}(t)P_{FoFEN\_L1}(t)P_{MCC}(t)P_{VCC}(t)\,, \qquad (2.7)$$

де: $P_{FoFsen\_L1}(t) = \left[1 - e^{-\lambda_{FSen}t}\right]^{\alpha}\left[e^{-\lambda_{FSen}t}(t)\right]^{m-\alpha}$ – ймовірність перебування флоту літаючих сенсорів у частково працездатному стані;

$P_{FoFEN\_L1}(t) = \left[1 - e^{-\lambda_{FEN}t}\right]^{n-k+\beta}\left[e^{-\lambda_{FEN}t}\right]^{k-\beta}$ – ймовірність перебування літаючих вузлів граничних обчислень флоту у частково працездатному стані.

Для аналізу станів СМ було обрано сценарій часткової втрати працездатності, що характеризується відмовами FoFSen та FoFEN одночасно. Дослідження залежності ймовірності перебування СМ у частково працездатному стані 24 від часу для різних значень інтенсивності відмов FEN (λ_{FEN}) представлено на рисунку 2.12.

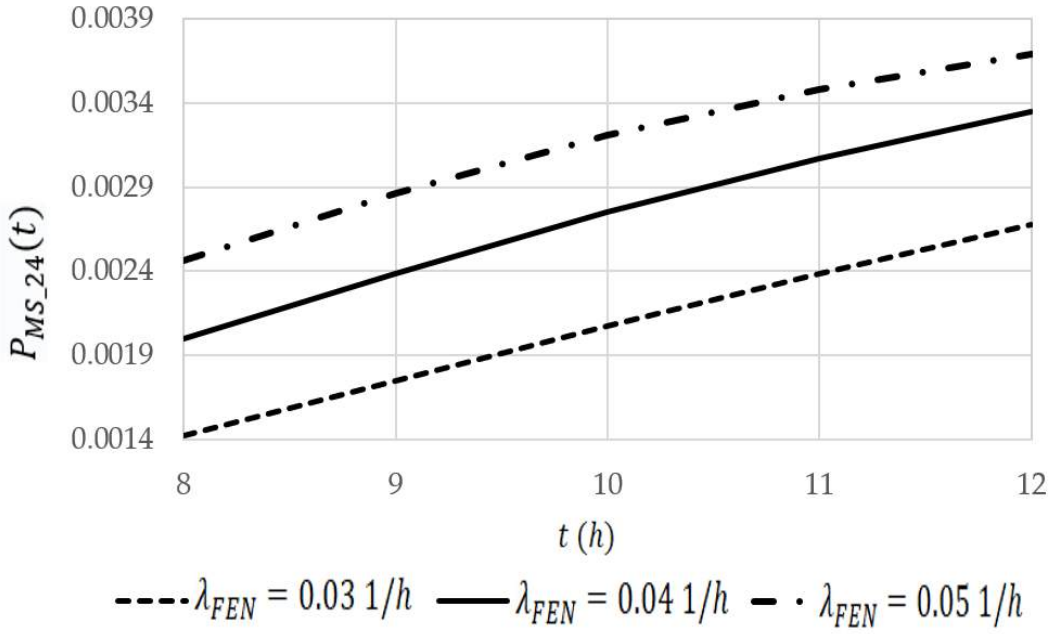

Рисунок 2.12 − Залежність ймовірності перебування системи моніторингу у частково працездатному стані 24 від часу роботи для різних значень інтенсивності відмов FEN

Отримані результати дозволяють зробити висновок, що збільшення часу t з 8 до 12 годин призводить до збільшення ймовірності перебування СМ у частково працездатному стані 24. Зокрема, при $\lambda_{FEN} = 0.05$ 1/год ця ймовірність зростає у 1.5 рази. Використання більш надійних FEN (зменшення λ_{FEN} до 0.03 1/год) дозволяє зменшити ймовірність перебування СМ у частково працездатному стані 24 у 1.38 рази при $t = 12$ год.

Далі було досліджено залежність ймовірності перебування СМ у частково працездатному стані 24 від розміру флоту літаючих сенсорів. Результати дослідження продемонстровані на рисунку 2.13.

Аналізуючи результати, робимо висновок, що збільшення загальної кількості FSen у флоті дозволяє зменшити ймовірність перебування СМ у частково працездатному стані 24. Збільшення кількості сенсорів m з 5 до 7 при $t = 12$ год призводить до зменшення цієї ймовірності у 1.27 рази.

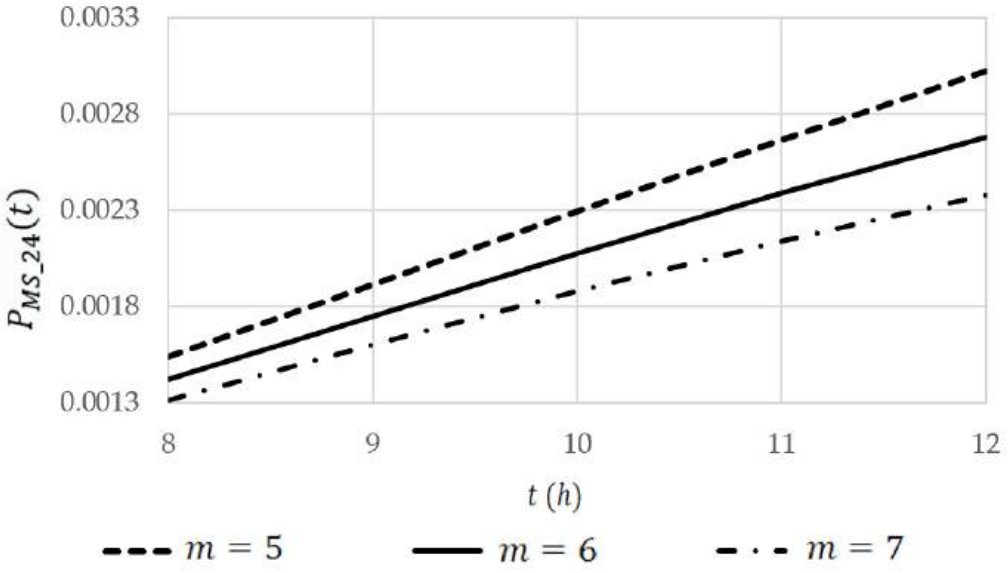

Рисунок 2.13 − Залежність ймовірності перебування системи моніторингу у частково працездатному стані 24 від часу роботи для різної кількості сенсорів

Отже, розроблена модель системи моніторингу з багаторівневою працездатністю дає можливість кількісно оцінити ЙБР та обґрунтувати необхідні рівні резервування в умовах часткових відмов обладнання. У четвертому розділі дисертаційної роботи розглянуто програмний засіб, створений для автоматизованого обчислення показників ЙБР та наочної візуалізації станів системи за умови відмов її окремих компонентів.

2.2.3 Розроблення та дослідження аналітичних моделей надійності наземної сенсорної мережі

2.2.3.1 Критерії відмови і показники безвідмовності

Наземні сенсорні мережі є основним компонентом для систем моніторингу ПНТ. Побудова математичної моделі вимагає чіткого визначення події, яка класифікується як відмова такої мережі. Критерії відмови сенсорної мережі визначаються трьома основними чинниками.

По-перше, розглядається кількісний критерій, який фіксує наявність недопустимої кількості сенсорів, що відмовили (r), незалежно від їхнього просторового розташування в межах області моніторингу. Цей чинник базується на

тому, що загальна втрата інформаційної щільності нижче певного порогу робить роботу мережі неефективною та унеможливлює достовірний аналіз даних.

По-друге, визначальним є просторовий критерій, що описує наявність кластерної відмови. Кластерна відмова трактується як вихід з ладу визначеної кількості суміжних (розташованих поруч) сенсорів. Виникнення такої події унеможливлює здійснення моніторингу на суцільній ділянці простору недопустимого розміру, що має певну геометричну форму. У контексті моніторингу потенційно небезпечних об’єктів утворення таких «сліпих зон» є критичним, оскільки локальні небезпечні явища (наприклад, осередок пожежі або локальний витік хімічної речовини) можуть залишитися невиявленими.

По-третє, враховується критерій відмови інфраструктури, пов’язаний із відмовою периферійного та системного обладнання мережі (наприклад, граничних пристроїв збору даних). У межах консервативного підходу до оцінювання надійності приймається жорстке припущення: будь-яка відмова системного обладнання призводить до повної відмови всієї сенсорної мережі, оскільки порушується маршрутизація даних до хмарного рівня.

Для розроблення аналітичних моделей, що враховують просторовий критерій, необхідно геометрично формалізувати ділянку моніторингу та конфігурацію кластерних відмов. Припускається, що область моніторингу має форму прямокутника. Розміри цього прямокутника задаються в умовних одиницях: довжина n_a та ширина n_b. Зазначені параметри n_a і n_b відповідають кількості сенсорів, що розміщені у відповідних рядках і стовпчиках топологічної ґратки ділянки. Таким чином, фізичні розміри всієї зони контролю визначаються як добуток умовної довжини n_a та ширини n_b на лінійні розміри зони контролю (чутливості) одного окремого сенсора. Відповідно, лінійка з n_b сенсорів повністю покриває одну просторову смугу ділянки, а матриця розмірністю $n_a \times n_b$ сенсорів забезпечує суцільне покриття всієї цільової території моніторингу.

У межах запропонованого підходу критичними для функціонування гібридної мережі вважаються такі кластерні відмови, яким у просторі відповідає

«сліпа» ділянка прямокутної форми. Розміри такого недопустимого кластера визначаються умовною довжиною d_a та шириною d_b $(d_a \times d_b)$. Схему розташування груп сенсорів та просторову параметризацію кластерної відмови наведено на рисунку 2.14.

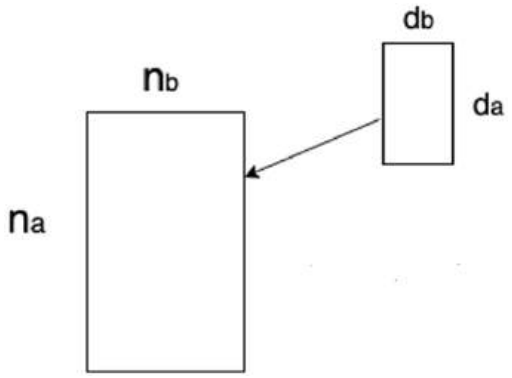

Рисунок 2.14 − Схема розташування груп сенсорів

На рисунку 2.14 проілюстровано матричну топологію розміщення сенсорних вузлів $(n_a \times n_b)$, та окремим елементом виділено прямокутну ділянку критичної групи суміжних непрацездатних сенсорів (кластера відмови) розмірністю $d_a \times d_b$. Формування кластера такого або більшого розміру є ознакою втрати працездатності мережі за просторовою ознакою.

Головним показником, який розраховується у рамках запропонованої аналітичної моделі та враховує основні сформульовані критерії, є ймовірність безвідмовної роботи сенсорної мережі як функція часу *P(t)*. Показник розраховується з урахуванням інтенсивності відмов окремих сенсорів та ймовірності формування просторового критерія відмови (кластер відмов) розміром $d_a \times d_b$ за умови наявності загальної допустимої кількості відмов *r*.

2.2.3.2 Аналітичні моделі надійності наземної сенсорної мережі з урахуванням просторового розташування сенсорів

Для оцінювання надійності сенсорної мережі з урахуванням просторового критерію, який був сформульований у попередньому пункті, необхідно розробити

математичну модель, яка враховує критерій просторового розташування відмов окремих сенсорів. Як було зазначено вище, область моніторингу представляється у вигляді прямокутної ділянки з розмірністю $n_a \times n_b$ сенсорів. Критерієм відмови, що призводить до відмови всієї мережі, вважається утворення кластера непрацездатних сенсорів прямокутної форми з розмірами $d_a \times d_b$ або відмова визначеної кількості сенсорів.

Основним етапом побудови аналітичної моделі є визначення кількості фатальних комбінацій відмов, тобто таких варіантів розташування непрацездатних сенсорів, які утворюють заборонений кластер, що унеможливлює моніторинг на визначеній ділянці.

Для формалізації цього процесу введемо функцію $L(n_a, n_b, d_a, d_b)$, яка визначає загальну кількість комбінацій покриття, що є недопустимими з огляду на фіксовані розміри кластера відмов. За умови, що $d_a \leq n_a$, $d_b \leq n_b$, $d_a < n_b$, $d_b < n_a$, $d_a \neq d_b$, ця функція враховує геометрію ділянки та можливі орієнтації кластера відмов:

$$L(n_a, n_b, d_a, d_b) = (n_a - d_a + 1)(n_b - d_b + 1) + \\ +(n_a - d_b + 1)(n_b - d_a + 1), \tag{2.8}$$

Тоді коефіцієнт структурної надійності сенсорної мережі, який визначається відношенням кількості її можливих працездатних станів за відсутності і наявності відмов сенсорів до загальної кількості можливих станів мережі, обчислюють за такою формулою:

$$K(n_a, n_b, r, d_a, d_b) = \frac{1}{2^{n_a n_b}} \left(\sum_{i=0}^{r-1} C_{n_a n_b}^{i} - L(n_a, n_b, d_a, d_b)\right), \tag{2.9}$$

де: зменшуване у дужках $\sum_{i=0}^{r-1} C_{n_a n_b}^{i}$ враховує першу складову критерію відмов і описує загальну кількість ситуацій з i відмовами в діапазоні від нуля до r-1, яка дорівнює кількості сполучень з $n_a \times n_b$ по i;

від'ємник $L(n_a, n_b, d_a, d_b)$ визначає кількість недопустимих ситуацій з кластерними відмовами (друга складова критерію відмови).

Якщо сторони прямокутника для груп сенсорів є рівними, то маємо наступну формулу для коефіцієнта структурної надійності сенсорної мережі:

$$K(n_a, n_b, r, d_a, d_b) = \frac{1}{2^{n_a n_b}}\left(\sum_{i=0}^{r-1} C_{n_a n_b}^{i} - (n_a - d)(n_b - d)\right). \qquad (2.10)$$

Варто зауважити, що отримані формули описують ситуацію, коли добуток величин d_a і d_b відрізняється від величини *r* на одиницю. По-перше, для загального випадку треба врахувати аспект парності і непарності цих чисел. По-друге, якщо різниця між добутком величин d_a і d_b та *r* перевищує одиницю, вираз для функції *L* буде визначатися сумою, кількість доданків якої залежатиме від цієї різниці.

На основі розробленої моделі для розрахунку коефіцієнта структурної надійності, а також з огляду на прийняті припущення, обмеження та інтенсивність відмов сенсорів λ, сформовано аналітичний вираз для оцінювання ймовірності безвідмовної роботи сенсорної мережі. Ймовірність безвідмовної роботи сенсора $p(t) = e^{-\lambda t}$ є функцією з експоненційним розподілом часу до відмови. Також варто зазначити, що під час розрахунків аналітична модель не враховує вплив зовнішніх факторів, таких як навмисні фізичні руйнування або кібератаки на компоненти системи.

Отже, маємо:

$$P(n_a, n_b, r, d_a, d_b, t) = \sum_{i=0}^{r-1} C_{n_a n_b}^{i} \left(p(t)\right)^{n_a n_b - i}\left(1 - p(t)\right)^{i} - \\ -L(n_a, n_b, d_a, d_b)\left(p(t)\right)^{n_a n_b - d_a d_b}\left(1 - p(t)\right)^{d_a d_b}. \qquad (2.11)$$

Для дослідження розробленої аналітичної моделі було проведено серію експериментів. Об'єктом моделювання обрано ділянку лісового масиву у Малинівському лісництві Харківської області. В межах цього масиву було виділено

квадратну ділянку для розміщення однотипних сенсорів задимлення. Параметри мережі для розрахунку: розмірність ділянки моніторингу n_a= n_b= 5, розміри кластера відмов d_a = d_b = 3, гранична кількість сенсорів до відмови r = 10.

У таблиці 2.9 наведено розрахункові значення ймовірності безвідмовної роботи мережі для різних інтенсивностей відмов λ та часу експлуатації t.

Таблиця 2.9 − Ймовірність безвідмовної роботи сенсорної мережі для різних значень інтенсивності відмов сенсорів і часу роботи

Інтенсивність відмов сенсорів λ, год	Час роботи БСМ t, год	Імовірність безвідмовної роботи БСМ як функція часу $P(t)$
$1\cdot10^{-4}$	100	0.999996
$1\cdot10^{-4}$	1000	0.999948
$1\cdot10^{-4}$	5000	0.451125
$1\cdot10^{-4}$	10000	0.005217
$1\cdot10^{-4}$	50000	$1\cdot10^{-29}$
$1\cdot10^{-5}$	100	0.999999
$1\cdot10^{-5}$	1000	0.999996
$1\cdot10^{-5}$	5000	0.999589
$1\cdot10^{-5}$	10000	0.999948
$1\cdot10^{-5}$	50000	0.451125
$1\cdot10^{-6}$	100	0.999996
$1\cdot10^{-6}$	1000	0.99994
$1\cdot10^{-6}$	5000	0.99992
$1\cdot10^{-6}$	10000	0.99284
$1\cdot10^{-6}$	50000	0.93899

На основі даних таблиці було побудовано графіки залежності ймовірності безвідмовної роботи сенсорної мережі від часу. На рисунку 2.15 представлена залежність ЙБР від часу для різних інтенсивностей відмов $\lambda = 1\cdot10^{-4}$ 1/год, $\lambda = 1\cdot10^{-5}$ 1/год, $\lambda = 1\cdot10^{-6}$ 1/год.

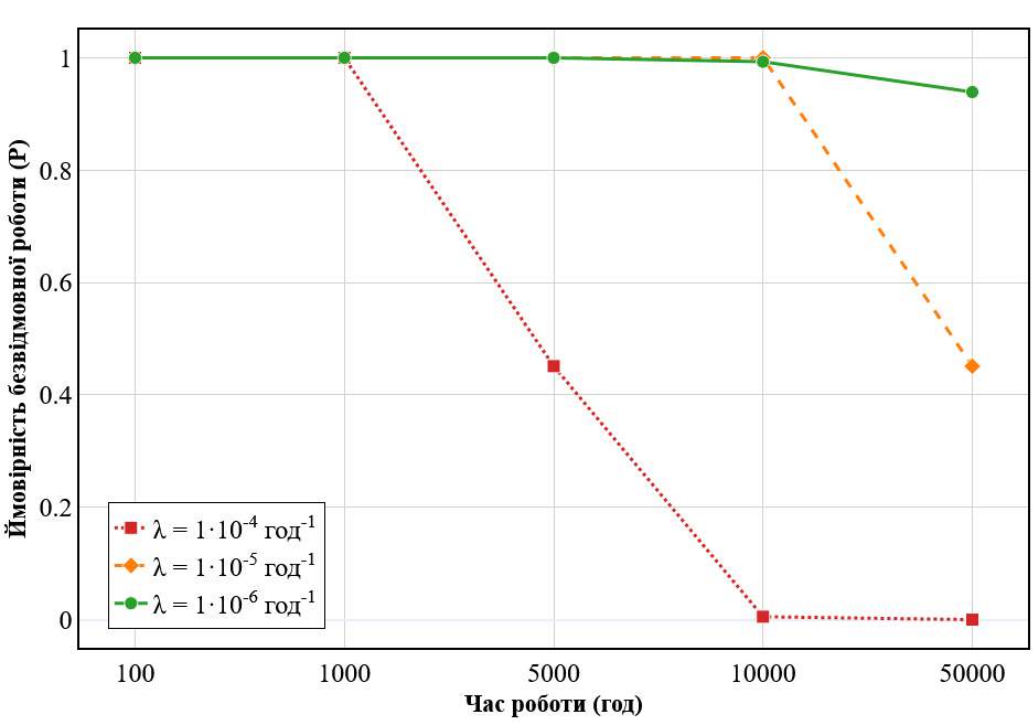

Рисунок 2.15 − Залежність ймовірності безвідмовної роботи сенсорної мережі від часу для різних інтенсивностей відмов сенсорів

Детальний аналіз отриманих результатів дозволяє зробити наступні висновки щодо динаміки деградації мережі у часі:

1. У разі застосування сенсорів з інтенсивністю відмов $\lambda = 1 \cdot 10^{-6}$ 1/год, через 10 000 годин безперервного функціонування мережі ймовірність її безвідмовної роботи зменшується відносно початкового періоду (100 годин) лише у 1.01 рази.

2. Використання сенсорів з інтенсивністю відмов $\lambda = 1 \cdot 10^{-4}$ 1/год призводить до катастрофічного падіння надійності: вже через 5 000 годин роботи ймовірність безвідмовної роботи падає у 2.2 рази, а через 10 000 годин наближається до нуля. Зменшення надійності між 100 та 10 000 годинами для таких сенсорів становить 191.7 рази.

3. Заміна сенсорів з $\lambda = 1 \cdot 10^{-4}$ 1/год на більш надійні аналоги з $\lambda = 1 \cdot 10^{-6}$ 1/год дає змогу суттєво збільшити загальну ймовірність безвідмовної роботи мережі: для 5 000 годин експлуатації показник зростає у 2.2 рази, а для 10 000 годин − у 190.3 рази.

На основі формули (2.11) було розраховано значення ймовірності безвідмовної роботи, що зведені у таблиці 2.10–2.12. За цими даними для різних інтенсивностей відмов окремих сенсорів було побудовано криві залежності ймовірності безвідмовної роботи сенсорної мережі від загальної кількості сенсорів, що відмовили (рис. 2.16–2.18).

Таблиця 2.10 − Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки покриття та недопустимої кількості сенсорів, що відмовили (для $p = 0.85$)

Добуток довжини ділянки моніторингу на її ширину $n_a \times n_b$	Недопустима кількість сенсорів, що відмовили r	Ймовірність безвідмовної роботи БСМ як функція недопустимої кількості сенсорів, що відмовили $P(r)$
64	10	0.920191
64	11	0.961859
64	12	0.983372
64	13	0.993365
64	14	0.997569
81	10	0.760068
81	11	0.854465
81	12	0.918544
81	13	0.957857
81	14	0.979802
100	10	0.516381
100	11	0.646493
100	12	0.758453
100	13	0.845784
100	14	0.907957
121	10	0.274998
121	11	0.391456
121	12	0.515049
121	13	0.634202
121	14	0.739272
144	10	0.112111
144	11	0.182934
144	12	0.273671
144	13	0.379437
144	14	0.492384

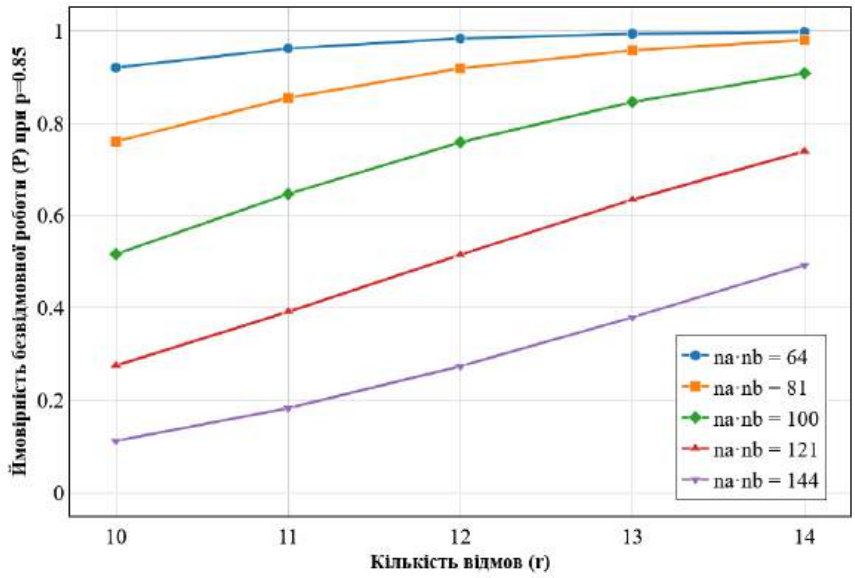

Рисунок 2.16 − Графік залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів (p = 0.85)

Таблиця 2.11 − Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки покриття та недопустимої кількості сенсорів, що відмовили (для p = 0.9)

Добуток довжини ділянки моніторингу на її ширину $n_a \times n_b$	Недопустима кількість сенсорів, що відмовили r	Ймовірність безвідмовної роботи БСМ як функція недопустимої кількості сенсорів, що відмовили $P(r)$
64	10	0.991966
64	11	0.997377
64	12	0.999224
64	13	0.999791
64	14	0.999948
81	10	0.962961
81	11	0.984368
81	12	0.993973
81	13	0.997868
81	14	0.999306
100	10	0.884655
100	11	0.93967
100	12	0.970962
100	13	0.987096
100	14	0.994689
121	10	0.737996
121	11	0.836035
121	12	0.90481

Кінець таблиці 2.11

121	13	0.948637
121	14	0.974183
144	10	0.538526
144	11	0.665276
144	12	0.772616
144	13	0.855321
144	14	0.913701

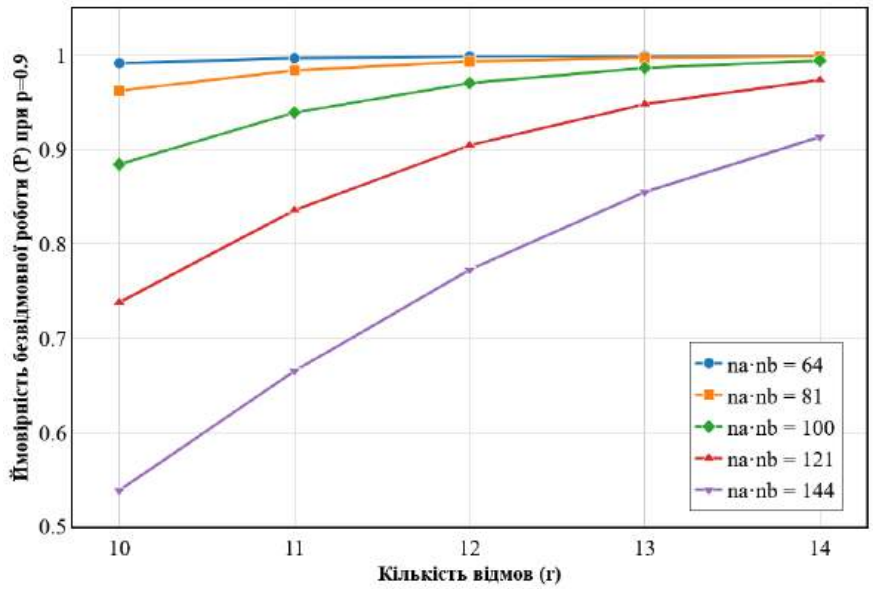

Рисунок 2.17 – Графік залежності ймовірності безвідмовної роботи сенсорної від недопустимої кількості сенсорів, що відмовили (p = 0.9)

Таблиця 2.12 – Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки покриття та недопустимої кількості сенсорів, що відмовили (для p = 0.95)

Добуток довжини ділянки моніторингу на її ширину $n_a \times n_b$	Недопустима кількість сенсорів, що відмовили r	Ймовірність безвідмовної роботи сенсорної мережі як функція недопустимої кількості сенсорів, що відмовили $P(r)$
64	10	0.998763
64	11	0.99969
64	12	0.99993
64	13	0.999986
64	14	0.999997
81	10	0.992872
81	11	0.997679
81	12	0.999312

Кінець таблиці 2.12

81	13	0.999813
81	14	0.999954
100	10	0.971812
100	11	0.988528
100	12	0.995726
100	13	0.998536
100	14	0.999537
121	10	0.917931
121	11	0.959541
121	12	0.98164
121	13	0.992302
121	14	0.997007
144	10	0.814658
144	11	0.892233
144	12	0.94197
144	13	0.970983
144	14	0.986488

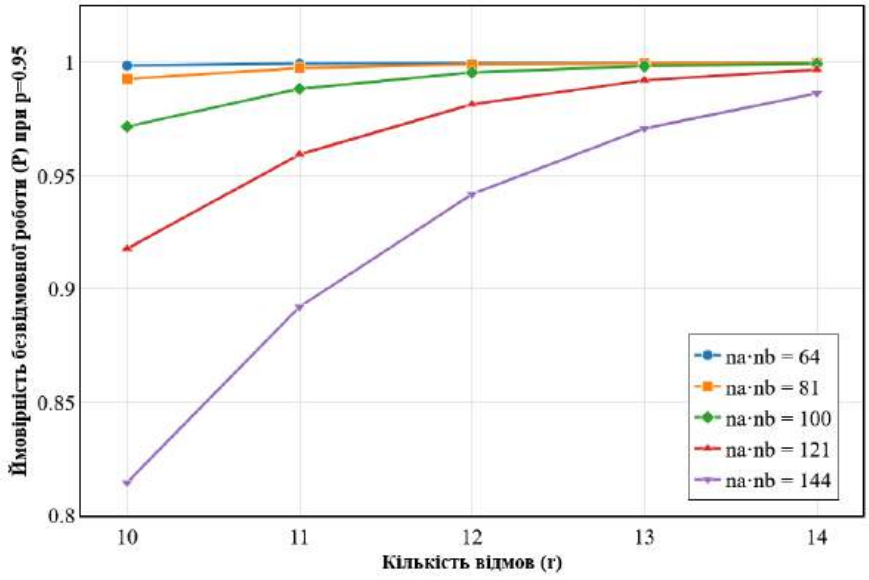

Рисунок 2.18 − Графік залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів, що відмовили (p = 0.95)

Аналіз результатів розрахунків та побудованих графіків дає змогу виявити фундаментальні закономірності проєктування сенсорної мережі:

– для всіх ділянок моніторингу збільшення недопустимої кількості сенсорів, що відмовили, призводить до збільшення ймовірності безвідмовної роботи

сенсорної мережі. Так, наприклад для ділянки розміром $n_a \times n_b$= 121 збільшення кількості таких сенсорів з 10 до 14 зумовлює зростання ймовірності безвідмовної роботи сенсорної мережі у 2.6, 1.3 та 1.1 рази для сенсорів з імовірностями безвідмовної роботи 0.85, 0.9 та 0.95 відповідно;

– за однакової недопустимої кількості сенсорів, що відмовили, менший розмір ділянки моніторингу забезпечує краще значення ймовірності безвідмовної роботи сенсорної мережі. Наприклад тоді, коли таких сенсорів 13, то для ділянки розміром $n_a \times n_b$= 64 ймовірність безвідмовної роботи сенсорної мережі буде у 2.6, 1.2 та 1.1 рази більшою, ніж для ділянки розміром $n_a \times n_b$ 121 у разі використання сенсорів з імовірностями безвідмовної роботи 0.85, 0.9 та 0.95 відповідно.

2.3 Висновки до другого розділу

У розділі розроблено структурні рішення щодо побудови гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій на основі інтеграції літаючих і наземних хмарних, граничних та туманних обчислень. На відміну від традиційних підходів, запропоновані рішення враховують варіативність розміщення обчислювальних ресурсів і функціональний розподіл задач між мобільними та стаціонарними компонентами, що створює методичну основу для побудови адаптивних архітектур моніторингу.

Запропоновано трирівневу архітектуру гібридної сенсорної мережі у складі хмарного, безпілотного та наземного рівнів, яка забезпечує раціональний розподіл функцій збору, попереднього оброблення, передавання, зберігання та аналітичного опрацювання даних. Встановлено, що запропонована архітектура підтримує структурне переналаштування до дворівневої конфігурації без застосування БПЛА, що забезпечує її адаптацію до обмежень експлуатаційного середовища без втрати базових функціональних властивостей.

Обґрунтовано визначальну роль флоту БПЛА як ключового компонента гібридної сенсорної мережі, здатного реалізовувати функції літаючих хмарних,

граничних і туманних обчислень. Показано, що інтеграція методів штучного інтелекту та машинного навчання в підсистеми моніторингу забезпечує підвищення ефективності розвантаження обчислень, розподілу ресурсів, підтримки прийняття рішень, планування маршрутів та забезпечення безпеки функціонування системи.

Сформовано класифікацію моделей надійності гібридних сенсорних мереж, яка охоплює моделі безвідмовності, готовності, резервування, відновлення, деградації та топологічно залежної працездатності. Запропонована класифікація дозволяє системно пов’язати особливості структури мережі, механізми резервування та характер відмов із відповідними підходами до математичного моделювання її надійності.

Розроблено аналітичні моделі безвідмовності та багаторівневої працездатності системи моніторингу на основі гібридної сенсорної мережі, які дають змогу кількісно оцінювати вплив інтенсивностей відмов компонентів, тривалості місії, чисельності флоту БПЛА та рівня резервування вузлів граничних обчислень на інтегральні показники надійності. За результатами моделювання встановлено, що зменшення інтенсивності відмов елементів і введення резервних FEN забезпечують зростання ймовірності безвідмовної роботи системи, а збільшення кількості літаючих сенсорів знижує ймовірність переходу системи до частково працездатних станів.

Розроблено аналітичні моделі надійності наземної сенсорної мережі з урахуванням не лише кількісного, а й просторового критерію відмов, пов’язаного з утворенням кластерів непрацездатних сенсорів. Встановлено, що вирішальний вплив на ймовірність безвідмовної роботи мережі мають інтенсивність відмов сенсорів, розмір ділянки моніторингу та допустима кількість непрацездатних вузлів; при цьому використання більш надійних сенсорів, зменшення площі контролю та підвищення допустимого порогу відмов забезпечують істотне підвищення надійності наземної підсистеми моніторингу.Отримані результати будуть використані для розроблення імітаційних моделей та програмних засобів у наступних розділах роботи.

РОЗДІЛ 3
РОЗРОБЛЕННЯ МАРКОВСЬКИХ ТА ІМІТАЦІЙНИХ МОДЕЛЕЙ НАДІЙНОСТІ НАЗЕМНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ

3.1 Розроблення та дослідження марковських моделей надійності наземних сенсорних мереж систем моніторингу

3.1.1 Методологія побудови марковської моделі готовності наземної сенсорної мережі

У цьому підрозділі представлено дослідження наземних сенсорних мереж (НСМ) з можливістю відновлення працездатності елементів. Для комплексного оцінювання функції готовності таких мереж застосовується методологія стохастичного моделювання їхньої експлуатаційної поведінки. В основу дослідження покладено структурно-автоматний підхід, який виступає фундаментальною методичною базою для побудови адекватної марковської моделі готовності сенсорної мережі. Використання зазначеного підходу дає змогу не лише коректно сформулювати початкові припущення щодо процесів відмов і відновлень, а й детально описати повну множину експлуатаційних станів системи, враховуючи її структурну складність. На основі цього аналізу розробляється граф станів і переходів марковської моделі, що візуалізує динаміку функціонування мережі в часі. Кінцевим етапом моделювання є формування системи лінійних диференціальних рівнянь Колмогорова-Чепмена. Розв’язання цієї системи дозволяє отримати кількісні значення ймовірностей перебування мережі у відповідних працездатних, частково працездатних або непрацездатних станах, що є критично важливим для прогнозування надійності складних інформаційних систем.

Методологія побудови марковської моделі охоплює такі етапи:

Етап 1. Формування вербальної моделі експлуатаційної поведінки сенсорної мережі.

Етап 2. Розроблення графа станів марковської моделі.

Етап 3. Створення марковської моделі сенсорної мережі та її структурно-автоматного подання.

Етап 4. Формування системи диференціальних рівнянь Колмогорова-Чепмена для розрахунку ймовірностей перебування системи у відповідних станах.

Етап 5. Верифікація та валідація марковської моделі.

Вербальна модель є першим етапом методології. Вона описує всі експлуатаційні події (стани), включаючи процеси відновлення сенсорів мережі. Для побудови моделі сенсорної мережі Було прийнято наступні формалізовані припущення та обмеження:

– сенсорна мережа складається з 9 сенсорів та периферійного обладнання, сенсорна мережа має квадратну форму з розмірністю 3x3;

– відмова 3-х сенсорів призводить до відмови системи (простою);

– відмова периферійного обладнання (ПОб) призводить до простою системи;

– система є системою з відновленням. Після ремонту сенсорів система повертається у повністю працездатний стан;

– відмова сенсора визначається моментально. При відмові першого сенсора ремонтна бригада негайно починає виїзд;

– відновлення не є миттєвим, бригаді потрібен час на прибуття та відновлення окремо;

– час очікування бригади однаковий незалежно від кількості відмов сенсорів;

– бригада ремонтує всі відмови за одну процедуру відновлення і система повертається в повністю працездатний стан. При відновлені 1 та 2 сенсорів система не знаходиться у стані простою;

– середній час на відновлення залежить від кількості відмов сенсорів;

– відмова периферії може статися з будь-якого стану, крім стану відновлення;

– відновлення після відмови периферії повертає систему у стан, в якому вона була до відмови. Очікування бригаді не потрібне.

Вербальна модель описується через набір пов’язаних пар подій, що характеризують динаміку системи. Модель показує події і ситуації, які можуть відбутися при роботі сенсорної мереж.

Перша очікувана пара подій: подія 1.1 «початок роботи сенсорної мережі» – подія 1.2 «відмова першого сенсора». Сенсорна мережа працює у штатному режимі з 9-ма справними сенсорами. При відмові першого сенсора система негайно виявляє це та автоматично викликає ремонтну бригаду. Система залишається працездатною.

Друга очікувана пара подій: подія 2.1 «очікування бригади системою з одним непрацездатним сенсором» – подія 2.2 «відмова другого сенсора або прибуття бригади». *Варіант 2.2.1:* Прибуття бригади раніше за другу відмову. Бригада починає ремонт 1 сенсора. *Варіант 2.2.2:* Відмова другого сенсора раніше за прибуття бригади. Залишилося 8 працездатних сенсорів. Система ще працездатна.

Третя очікувана пара подій: подія 3.1 «початок ремонту 1 сенсора» – подія 3.2 «завершення ремонту 1 сенсора». Бригада прибула і ремонтує 1 непрацездатний сенсор. Після завершення ремонту система повертається у повністю працездатний стан.

Четверта очікувана пара подій: подія 4.1 «очікування бригади з двома непрацездатними сенсорами» – подія 4.2 «відмова третього сенсора або прибуття бригади». *Варіант 4.2.1:* Прибуття бригади раніше за третю відмову. Бригада починає ремонт двох сенсорів. *Варіант 4.2.2*: Відмова третього сенсора раніше за прибуття бригади. Система переходить у стан простою (3 відмови). Бригада продовжує їхати.

П’ята очікувана пара подій: подія 5.1 «початок ремонту двох сенсорів» – подія 5.2 «завершення ремонту двох сенсорів». Бригада ремонтує два непрацездатні сенсори.

Шоста очікувана пара подій: подія 6.1 «очікування бригади системою з трьома непрацездатними сенсорами (простій)» – подія 6.2 «прибуття бригади». Система в простої. Після прибуття починається ремонт трьох сенсорів.

Сьома очікувана пара подій: подія 7.1 «початок ремонту трьох сенсорів» – подія 7.2 «завершення ремонту трьох сенсорів». Бригада ремонтує 3 сенсори. Після завершення – повернення в працездатний стан.

Восьма очікувана пара подій: подія 8.1 «відмова периферійного обладнання» – подія 8.2 «відновлення ПОб». Периферійне обладнання може відмовити з будь-якого стану, крім стану ремонту. Відновлення ПОб відбувається без очікування бригади, після чого система повертається у стан, в якому вона була до відмови периферії.

3.1.2 Марковська модель готовності наземної сенсорної мережі

На основі сформованої вербальної моделі експлуатаційної поведінки та прийнятих припущень розроблено дискретно-неперервну марковську модель готовності наземної сенсорної мережі, для побудови якої введено базові показники та параметри, подані у таблиці 3.1.

Таблиця 3.1 – Показники та параметри для марковської моделі готовності сенсорної мережі

λ_v	Інтенсивність відмови сенсора (1/год).
λ_p	Інтенсивність відмови периферійного обладнання (1/год).
T_r	Середнє значення тривалості процедури відновлення сенсора (год).
T_d	Середнє значення тривалості процедури очікування відновлення (год).
T_m	Середнє значення тривалості процедури відновлення ПОб (год).
Pr	Ймовірність успішного завершення ремонту сенсорів (Pr = 1)
Pp	Ймовірність успішного відновлення ПОб (Pp = 1)

Для формування графа станів марковської моделі було сформовано відповідні вектори станів:

V1 *Кількість відмов сенсорів.* V1 ∈ {0, 1, 2, 3};

V1=0 – усі сенсори працездатні;

V1=1 – 1 сенсор відмовив;

V1=2 – 2 сенсори відмовили;

V1=3 – 3 сенсори відмовили (простій за сенсорами);

V2 – *Стан ремонтної бригади.* V2 ∈ {0, 1};

V2=0 – бригада не на місці (або не викликана, або в дорозі);

V2=1 – бригада на місці, виконує ремонт;

V3 – *Стан периферійного обладнання.* V3 ∈ {0, 1};

V3=0 – ПОб працездатне;

V3=1 – ПОб відмовило.

Подальший крок передбачає визначення базових подій (БП), спираючись на попередньо розроблену вербальну модель. Оскільки ця модель слугує фундаментальним джерелом даних і текстовим обґрунтуванням для всіх наступних етапів моделювання та висновків, її зміст необхідно постійно підтримувати в актуальному стані. Згідно з формалізованими парами подій у вербальному описі, статус базової події завжди присвоюється другій події з кожної такої пари.

Для побудови графа станів марковської моделі визначаються БП, сформовані на основі результатів побудови вербальної моделі (таблиця 3.2).

Таблиця 3.2 – Опис базових подій у системі

№	Початок процесу	БП (завершення)	Середня тривалість процедур (год)
1	Робота мережі	Відмова 1-го сенсора (БП1)	1/(9λv)
2	Робота мережі	Відмова 2-го сенсора (БП2)	1/(8λv)
3	Робота мережі	Відмова 3-го сенсора (БП3)	1/(7λv)
4	Очікування бригади	Прибуття бригади (БП4)	Td

Кінець таблиці 3.2

5	Ремонт 1 сенсора	Завершення ремонту (БП5)	Tr
6	Ремонт 2 сенсорів	Завершення ремонту (БП6)	2Tr
7	Ремонт 3 сенсорів	Завершення ремонту (БП7)	3Tr
8	Робота мережі	Відмова ПОб (БП8)	1/λp
9	Простій (ПОб)	Відновленя периферії (БП9)	Tm

Базові події є основним механізмом визначення майбутніх станів системи. Опис цих станів та пов’язаних із ними базових подій, а також аналітичні формули для розрахунку інтенсивностей переходів між станами зведено у граф станів марковської моделі, який винесений у Додаток В. На основі створеного графа станів марковської моделі було побудовано таблицю 3.3 векторів станів.

Таблиця 3.3 – Вектори станів марковської моделі готовності сенсорної мережі

№ стану	V1	V2	V3	Опис
1	0	0	0	S0: Повна працездатність
2	1	0	0	S1: 1 відмова, бригада їде
3	2	0	0	S2: 2 відмови, бригада їде
4	1	1	0	S4: Ремонт 1 сенсора
5	3	0	0	S3: 3 відмови, простій, бригада їде
6	2	1	0	S5: Ремонт 2 сенсорів
7	0	0	1	S7: ПОб відмовила з S0
8	1	0	1	S8: ПОб відмовила з S1
9	2	0	1	S9: ПОб відмовила з S2
10	3	1	0	S6: Ремонт 3 сенсорів
11	3	0	1	S10: ПОб відмовила з S3

Основуючись на отриманих результатах таблиці векторів станів, було сформовано структурно-автоматну модель (САМ) експлуатаційної надійнісної поведінки сенсорної мережі, представлену у таблиці 3.4. САМ описує кожну БП з усіма можливими ситуаціями, логічними виразами, формулами розрахунку інтенсивностей переходів (ФРІП) та правилами модифікації компонента вектору стану (ПМКВС).

Застосування структурно-автоматного підходу дозволяє уникнути прямого ручного синтезу ймовірнісного графа. Завдяки об'єднанню однотипних ситуацій модель стає універсальною: для розширення на більшу кількість можливих відмов достатньо змінити лише одну умову в логічному виразі.

Таблиця 3.4 – Структурно-автоматна модель експлуатаційної надійнісної поведінки сенсорної мережі

БП	Логічний вираз	ФРІП	ПМКВС
БП1: Відмова сенсора	(V1≤2)AND(V2=0)AND(V3=0)	$(9-V1)\lambda_v$	V1:=V1+1
БП2: Прибуття бригади	(V1≥1)AND(V2=0)AND(V3=0)	$\lambda_a=1/T_d$	V2:=1
БП3–5: Відновлення	(V1≥1)AND(V2=1)AND(V3=0)	$\mu_r/V1$, де $\mu_r=1/T_r$	V1:=0 V2:=0
БП6: Відмова ПОб	(V2=0)AND(V3=0)	λ_p	V3:=1
БП7: Відновлення ПОб	(V3=1)	$\mu_p=1/T_m$	V3:=0

Для математичного опису та аналізу системи в неперервному часі застосовується апарат дискретно-неперервних марковських ланцюгів, на основі якого побудовано марковську модель готовності сенсорної мережі у вигляді системи диференціальних рівнянь Колмогорова-Чепмена. Розв'язок цієї системи дає змогу обчислити розподіл ймовірностей перебування досліджуваного об'єкта в кожному з можливих станів. Загальний вигляд системи диференціальних рівнянь формується таким чином:

$$\frac{dP(t)}{dt} = P(t)Q \tag{3.1}$$

Тут *P(t)* виступає як матриця ймовірностей переходів, а її складовий елемент P_{ij}(t) характеризує ймовірність того, що за час t система змінить свій стан з *i* на *j*. *Q* є матрицею переходів марковської моделі (рисунок 3.1), яка кількісно описує інтенсивність переходу зі стану *i* у стан *j*. Розв'язок системи диференціальних рівнянь, а саме розподіл ймовірностей знаходження системи у відповідних станах, слугує базовими даними для розрахунку коефіцієнта готовності (*A*).

Розрахуємо коефіцієнт готовності для системи з 9 сенсорів. Система характеризується п'ятьма працездатними станами:

$$\mathrm{A} = \mathrm{P}(S_0) + \mathrm{P}(S_1) + \mathrm{P}(S_3) + \mathrm{P}(S_4) + \mathrm{P}(S_5) \tag{3.2}$$

$$\mathbf{Q} = \begin{pmatrix}
-(9\lambda_v + \lambda_p) & 9\lambda_v & 0 & 0 & 0 & 0 & 0 & \lambda_p & 0 & 0 & 0 \\
0 & -(8\lambda_v + \lambda_a + \lambda_p) & 8\lambda_v & 0 & \lambda_a & 0 & 0 & 0 & \lambda_p & 0 & 0 \\
0 & 0 & -(7\lambda_v + \lambda_a + \lambda_p) & 7\lambda_v & 0 & \lambda_a & 0 & 0 & 0 & \lambda_p & 0 \\
0 & 0 & 0 & -(\lambda_a + \lambda_p) & 0 & 0 & \lambda_a & 0 & 0 & 0 & \lambda_p \\
\mu_r & 0 & 0 & 0 & -\mu_r & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\mu_r}{2} & 0 & 0 & 0 & 0 & -\frac{\mu_r}{2} & 0 & 0 & 0 & 0 & 0 \\
\frac{\mu_r}{3} & 0 & 0 & 0 & 0 & 0 & -\frac{\mu_r}{3} & 0 & 0 & 0 & 0 \\
\mu_p & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_p & 0 & 0 & 0 \\
0 & \mu_p & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_p & 0 & 0 \\
0 & 0 & \mu_p & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_p & 0 \\
0 & 0 & 0 & \mu_p & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_p
\end{pmatrix}$$

Рисунок 3.1– Матриця інтенсивностей переходів марковської моделі

Відповідно до побудованої CAM генерується система диференціальних рівнянь Колмогорова-Чепмена. Для знаходження розв'язку цієї системи диференціальних рівнянь в обчислювальному середовищі ASNA [65] застосовується метод чисельного інтегрування Рунге-Кутти-Мерсона. З метою гарантування високої точності розрахункових даних було задано такі параметри обчислень: кінцеву межу часового інтервалу моделювання встановлено на рівні

Tk = 3000 годин, тоді як крок інтегрування прийнято рівним Re = 10^{-3}. Для реалізації подальшого порівняльного аналізу було сформовано базовий експлуатаційний сценарій, який забезпечує досягнення стаціонарного значення загального коефіцієнта готовності мережі на рівні A = 0.9754 за наступних заданих вхідних параметрів та індикаторів: λ_v = 0.0013 1/год., λ_p = 0.001 1/год., T_r=12 год., T_d = 20 год., $T_m = 10$ год. Для порівняння з отриманими результатами побудови опорного графа за допомогою методології МЕПІС було створено відповідний граф станів згідно з описом запропонованої системи.

Для порівняння з результатами, отриманими на основі структурно-автоматного підходу, було побудовано графи станів марковської моделі відповідно до опису запропонованої системи. Наведений на рисунку 3.2 граф демонструє узагальнену марковську модель готовності відновлюваної сенсорної мережі розмірності N×N, де N — сторона квадратної ділянки зони покриття моніторингу. На рисунку 3.3 наведено граф станів марковської моделі для системи з дев'яти сенсорів.

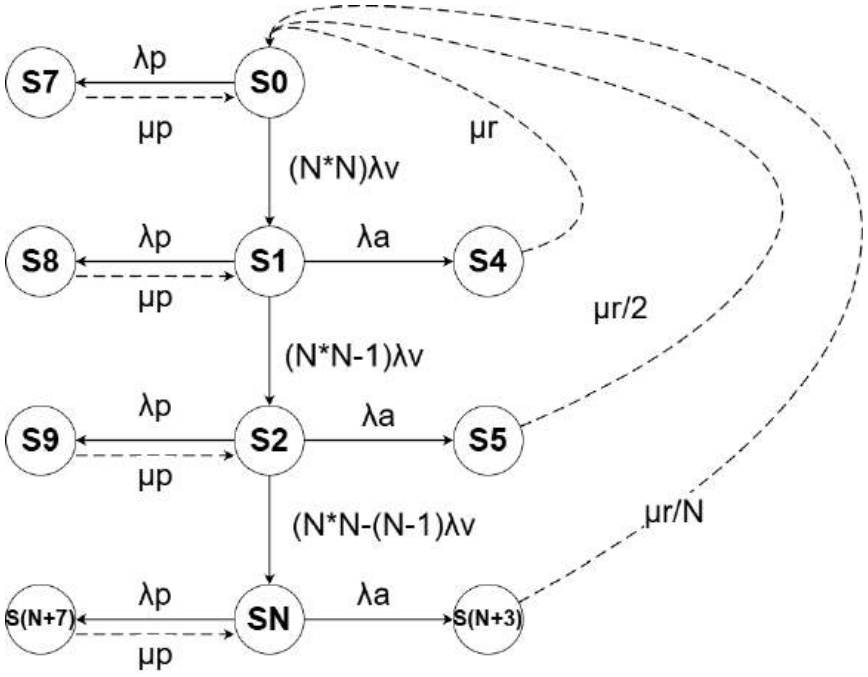

Рисунок 3.2 – Узагальнений граф станів марковської моделі готовності відновлюваної сенсорної мережі для конфігурації N×N

Для проведення кількісних розрахунків узагальнену марковську модель було деталізовано для конкретної конфігурації системи (рисунок 3.3), що складається з дев’яти сенсорів, де відмова трьох сенсорів переводить мережу у стан простою.

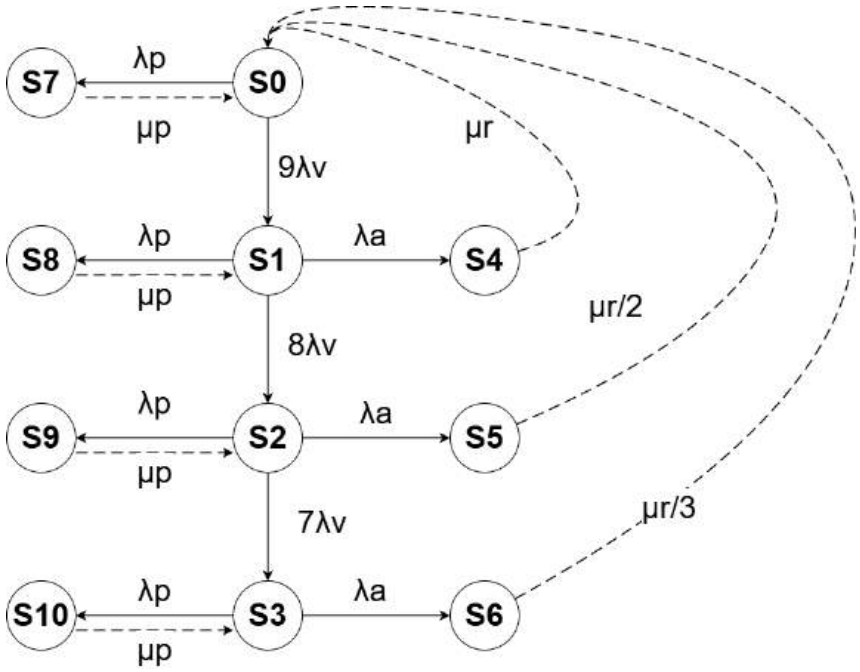

Рисунок 3.3 – Граф станів марковської моделі готовності відновлюваної сенсорної мережі для дев’яти сенсорів за порога відмови 3

Щоб оцінити вплив різних експлуатаційних факторів на загальну готовність мережі, було проведено серію експериментів з варіюванням п’яти критичних параметрів, які впливають на систему. Результати експериментів зведено у таблицю 3.5

Аналізуючи дані таблиці, робимо наступні висновки:

Збільшення інтенсивності відмови ПОб до 0.004 1/год призводить до помірного зниження коефіцієнта готовності з базового рівня 0.9754 до 0.9533, що підтверджує ефективність стратегії постійного відновлення для мінімізації часу простою системи.

Параметр інтенсивності відмови сенсора має критичний вплив на надійність системи, оскільки його зростання з з 0.0013 1/год до 0.004 1/год спричиняє суттєве падіння коефіцієнта готовності до значення 0.8729.

Це пояснюється тим, що сенсори є ключовими компонентами, які визначають коефіцієнт готовності системи. Проте важливо підкреслити: якщо архітектура передбачає надмірність (резервування), то збільшення кількості сенсорів, відмова яких є критичною для системи, призводитиме до зростання показника готовності відносно базових значень.

Параметри очікування відновлення ПОб меншою мірою впливають на загальний стан, оскільки процес його регенерації зазвичай не потребує тривалої підготовки, а інтенсивність відмов ПОб нижча за аналогічний показник для сенсорів. Водночас при використанні високопродуктивних сенсорів із низькою інтенсивністю відмов роль станів ПОб зростає, оскільки цей компонент може вийти з ладу незалежно від інших елементів і спричинити перехід системи у стан простою.

Таблиця 3.5 – Експерименти з валідації моделі

№	Параметр або показник	Базове значення	Базова ймовір-ність	Нове значення	Отримана ймовірність	Коментар
1	T_m	10 год	0.9754	5	0.9811	Незначний вплив на систему, оскільки для відновлення не потрібне додаткове очікування.
				50	0.9323	
				100	0.8834	
2	λ_v	0.0013 1/год	0.9754	0.004	0.8729	Інтенсивність відмови сенсора є одним із основних показників, які впливають на систему.
				0.0009	0.9713	
				0.00001	0.9830	
3	T_d	20 год	0.9754	10	0.9849	Середнє значення тривалості очікування. Має найбільший вплив на готовність системи.
				40	0.9447	
				80	0.8651	
4	T_r	12 год	0.9754	6	0.9783	Середній час тривалості процедури відновлення. Показник суттєво впливає на готовність системи. Час відновлення сенсорів є критичним.
				20	0.9721	
				50	0.9631	
5	λ_p	0.001 1/год	0.9754	0.004	0.9533	На рівні з часом відновлення ПОб впливає на систему незначною мірою.
				0.0009	0.9791	
				0.00001	0.9867	

3.2 Розроблення та дослідження імітаційних моделей надійності наземних сенсорних мереж систем моніторингу

3.2.1 Імітаційна модель надійності бездротових сенсорних мереж з урахуванням фатальних комбінацій множинних відмов сенсорів

Ймовірність безвідмовної роботи (ЙБР) сенсорних мереж є комплексним показником, що залежить від низки факторів. Ключовим параметром, який впливає на ЙБР, є кількість сенсорів, чий вихід із ладу спричиняє відмову всієї системи. Аналіз реальних сценаріїв експлуатації свідчить, що відмова суміжних сенсорів, які утворюють певну послідовність, також призводить до втрати мережею своєї працездатності. Такий тип відмов класифікується як фатальна комбінація непрацездатних сенсорів (ФКНС). Вона спричиняє відмову системи навіть тоді, коли загальна гранична кількість непрацездатних вузлів ще не була досягнута.

У попередніх розділах розглядалися виключно аналітичні моделі оцінювання надійності сенсорних мереж із фіксованою топологією. Однак застосування аналітичних методів для розрахунку ЙБР мереж довільної конфігурації з випадковим характером відмов стає надто складною обчислювальною задачею. Це зумовлено величезним обсягом даних, необхідних для врахування всіх можливих варіацій деградації системи. З огляду на складність аналітичного опису, було обрано метод імітаційного моделювання. Такий підхід дає змогу врахувати основні чинники відмов, як-от: вихід із ладу окремого сенсора або периферійного обладнання, виникнення ФКНС та особливості просторового розташування мережі. Нижче розглянуто процес моделювання мережі з урахуванням ФКНС.

Постановка задачі імітаційного моделювання. Область моніторингу (на прикладі лісового господарства) має довільну форму та рівномірно покрита сенсорною мережею. Основним критерієм відмови мережі є ФКНС – формування критичного кластера відмов із неприпустимої кількості суміжних сенсорів.

Припущення та обмеження моделювання:

1. Територія моніторингу поділяється на ділянки у формі квадратів, довжина сторони яких дорівнює двом радіусам дії сенсора.

2. Бездротова сенсорна мережа (БСМ) вважається непрацездатною при появі визначеної кількості ФКНС заданого розміру. Відмова ПОб на даному етапі моделювання не враховується.

3. Для формування ФКНС квадратна ділянка з непрацездатним сенсором повинна мати хоча б одну спільну сторону з іншою аналогічною ділянкою. Сукупність таких ділянок і утворює фатальну комбінацію.

Приклади геометричної конфігурації фатальних комбінацій для різної кількості непрацездатних сенсорів (двох, трьох та чотирьох) наведено на рисунках 3.4, 3.5 та 3.6 відповідно.

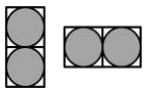

Рисунок 3.4 – Фатальні комбінації двох непрацездатних сенсорів

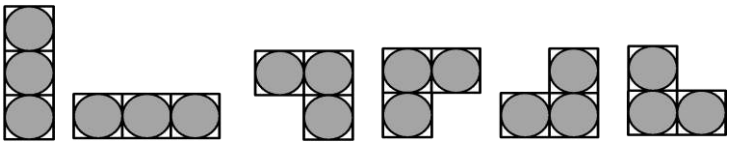

Рисунок 3.5 – Фатальні комбінації трьох непрацездатних сенсорів

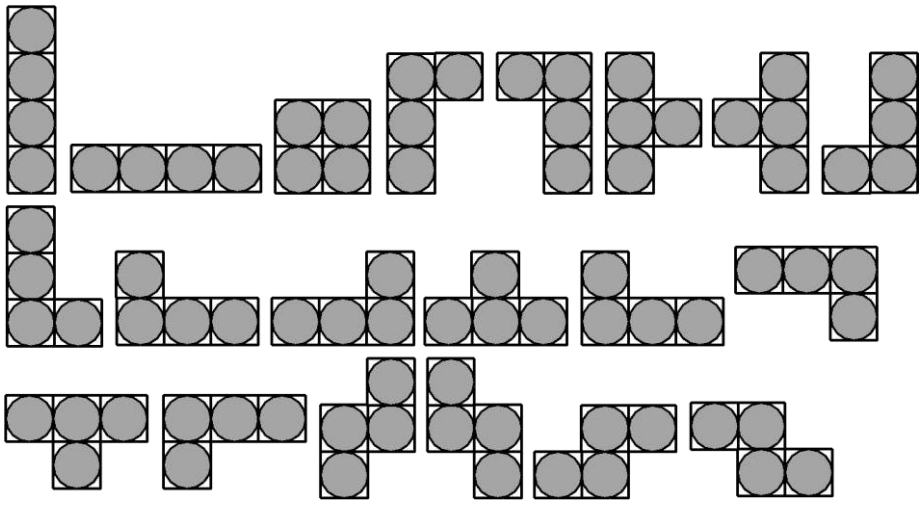

Рисунок 3.6 – Фатальні комбінації чотирьох непрацездатних сенсорів

Наведені рисунки показують, що кластеризація відмов розглядається виключно за умови суміжності сторін квадратних зон відповідальності сенсорів. Запропонована методика імітаційного оцінювання безвідмовності БСМ реалізується у чотири етапи:

Eman 1. Дослідження просторових характеристик зони моніторингу для розрахунку оптимальної кількості та специфікацій сенсорів, що гарантуватимуть повне покриття цільової ділянки.

Eman 2. Формалізація критеріїв відмови. У рамках даного дослідження як основний критерій обрано наявність ФКНС.

Eman 3. Дослідження показників безвідмовності системи методом імітаційного моделювання залежно від розмірності ФКНС. За виявлення ФКНС відповідає алгоритм пошуку у ширину.

Eman 4. Верифікація отриманих результатів безвідмовності БСМ на предмет їхньої відповідності заданим вимогам та рекомендації для підвищення ЙБР.

Для реалізації Етапу 3 було розроблено програмний засіб мовою Python. Він дозволяє генерувати конфігурацію сенсорної мережі для заданої площі довільної форми, імітувати стохастичний процес відмов сенсорів та виявляти наявність ФКНС. Детальний огляд засобу буде продемонстровано у Розділі 4 дисертаційної роботи.

З метою практичної верифікації розробленої імітаційної моделі надійності було обрано мапу реального об’єкта, а саме – лісового масиву Чугуїв – Старий Салтів у Харківській області. Вибір цієї локації зумовлений актуальністю завдань безперервного моніторингу та раннього виявлення лісових пожеж на великих територіях з неоднорідним ландшафтом. У програмному середовищі територію лісового масиву було розділено та покрито сенсорною мережею, що складається з 261 квадратної ділянки. Розмір кожної такої ділянки суворо відповідає зоні покриття одного сенсора, при цьому довжина сторони квадрата дорівнює двом радіусам дії сенсора. На рисунку 3.7 зображено отриману мапу з накладеним покриттям бездротовою сенсорною мережею. На рисунку 3.8 детально проілюстровано проміжний стан системи під час однієї з ітерацій моделювання

просторових відмов. На цьому етапі програмний засіб згенерував множину непрацездатних сенсорів, після чого для аналізу мережі було застосовано алгоритм пошуку в ширину. Алгоритм виявив згенеровані відмови. Стрілками на рисунку позначено ідентифіковані ФКНС, що складаються з двох та чотирьох суміжних вузлів відповідно.

Рисунок 3.7 – Карта покриття сенсорами території лісового масиву

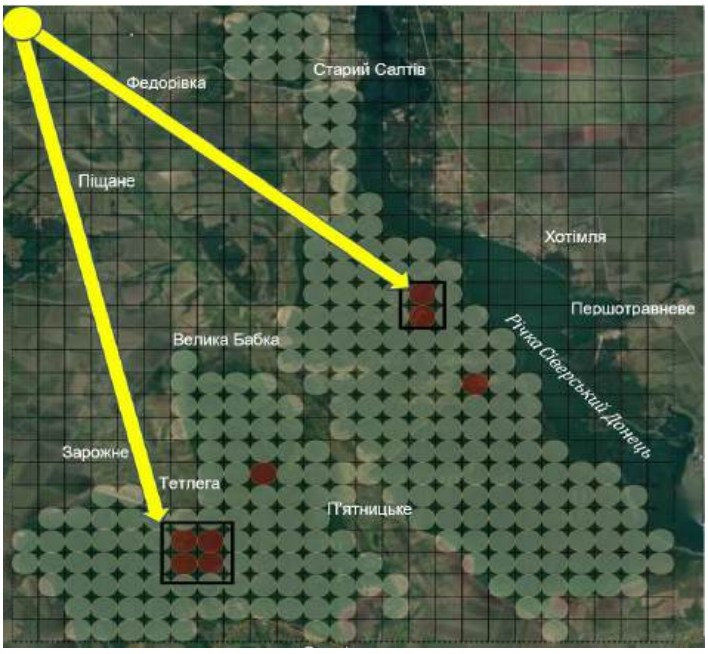

Рисунок 3.8 – Результат генерування відмов сенсорів утвореної БСМ та визначення ФКНС

В ході експериментів [7] було виконано 8 циклів моделювання по 100000 ітерацій у кожному. n_f = 6, 7, 8, 9, 10, 11 та 12 відмов сенсорів БСМ та у кожній ітерації перевірялася наявність та підраховувалася кількість ФКНС з мінімально необхідною кількістю непрацездатних сенсорів, що дорівнює 2, 3, 4 та 5. На підставі отриманих результатів моделювання за формулою (3.3) було обчислено ймовірність відмови БСМ Q_{WSN} та побудовано графік (рис. 3.9) та діаграми (рис. 3.10 та 3.11).

$$Q_{WSN} = \frac{n_{it}\,(N_{fs\_FCFS}^{min})}{N_{it}}, \tag{3.3}$$

де $n_{it}\left(N_{fs_{FCFS}}^{min}\right)$ – кількість ітерацій з мінімально необхідною для відмови БСМ кількістю ФКНС з мінімально необхідної кількістю непрацездатних сенсорів $n_{fs\_FCFS}^{min}$;

N_{it} – кількість ітерацій в циклі моделювання.

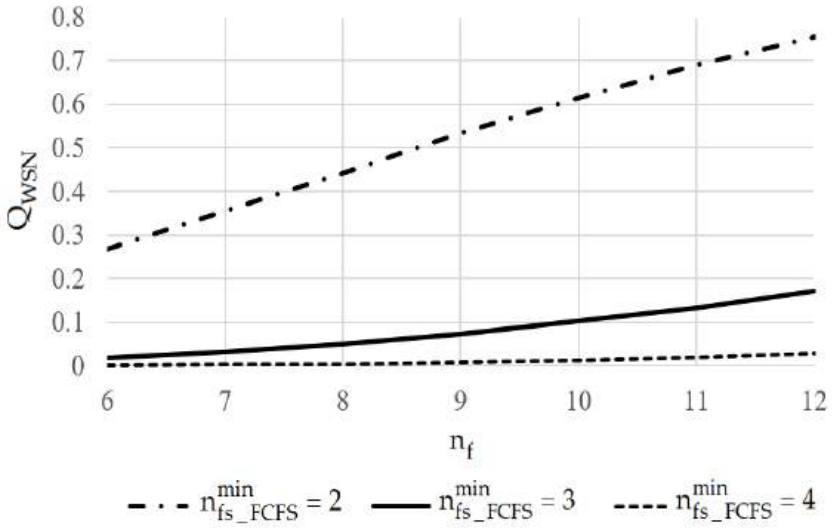

Рисунок 3.9 – Графіки залежності ймовірності відмови БСМ від кількості відмов її сенсорів для різних значень мінімально необхідної кількості непрацездатних сенсорів у складі ФКНС $n_{fs\_FCFS}^{min} = 1$

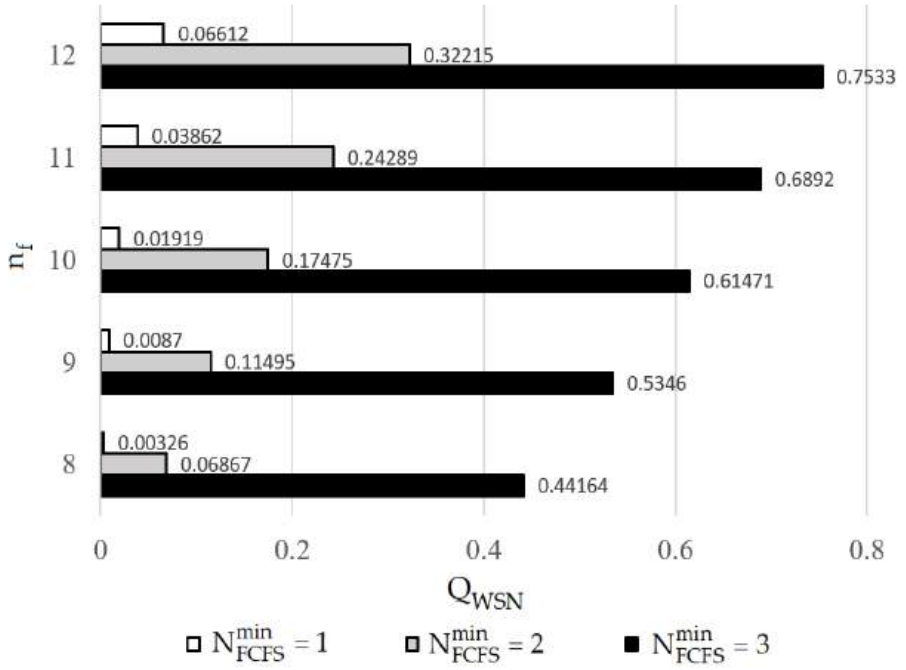

Рисунок 3.10 – Діаграма, що показує залежність ймовірності відмови БСМ від кількості відмов її сенсорів для різної мінімально необхідної для відмови БСМ кількості ФКНС (частина 1) $n_{fs\_FCFS}^{min} = 2$

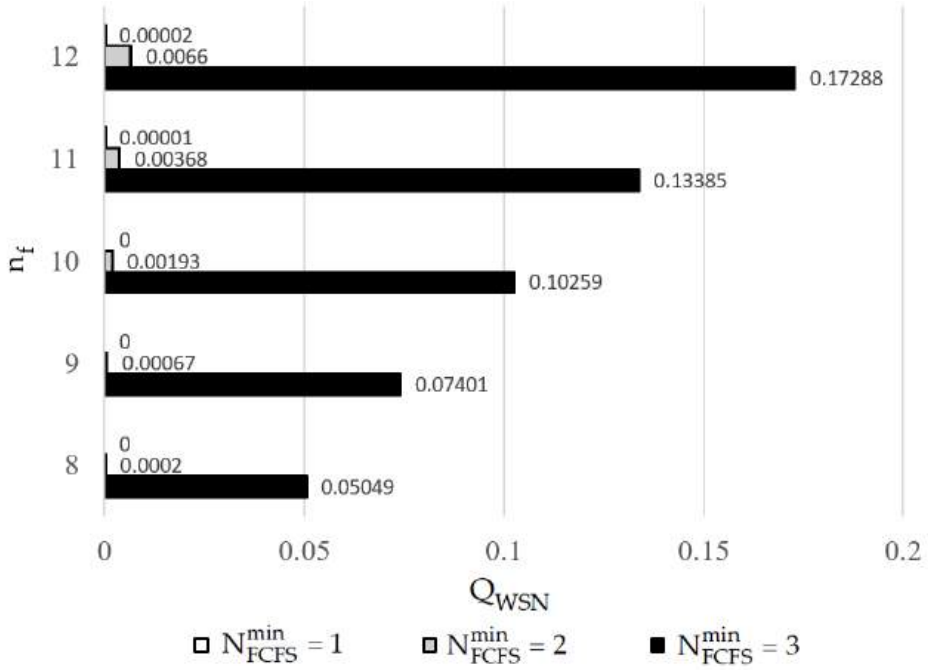

Рисунок 3.11 – Діаграма, що показує залежність ймовірності відмови БСМ від кількості відмов її сенсорів для різної мінімально необхідної для відмови БСМ кількості ФКНС $n_{fs\_FCFS}^{min} = 3$

Аналіз графіків та діаграм, представлених на рис. 3.9-3.11, дає змогу дійти таких висновків:

1. Збільшення загальної кількості непрацездатних сенсорів у системі закономірно збільшує ймовірність відмови всієї БСМ, і ця динаміка прослідковується для всіх розглянутих конфігурацій ФКНС. Так, наприклад, для $n_{fs\_FCFS}^{min} = 2$ збільшення кількості відмов сенсорів з 6 до 12 зумовлює зростання ймовірності відмов БСМ у 2.8 рази (з 0.2680 до 0.7533), тоді як для $n_{fs\_FCFS}^{min} = 3$ та для $n_{fs\_FCFS}^{min} = 4$ це зростання становить 9.2 (з 0.01869 до 0.17288) та 30.1 (з 0.00094 до 0.02826) рази відповідно.

2. Підвищення порогового значення кількості ФКНС, необхідного для відмови всіє мережі, закономірно призводить до суттєвого зниження загальної ймовірності відмови БСМ. Так, наприклад, для $n_{fs\_FCFS}^{min} = 4$ збільшення мінімально необхідної для відмови БСМ кількості ФКНС з 1 до 3 зумовлює зменшення ймовірності відмов БСМ у 135.5, 61.4, 32.0, 17.8 та 11.4 рази для n_f = 8, 9, 10, 11 та 12 відповідно. У випадку $n_{fs\_FCFS}^{min} = 3$ для n_f = 8, 9, 10 ймовірність відмов БСМ дорівнює 0 (див. рис. 9), а для n_f = 11 та 12 набуває близьких до нуля значень.

3.2.2 Імітаційна модель надійності бездротових сенсорних мереж з урахуванням відмов сенсорних вузлів та периферійних компонентів за різними сценаріями

Розглянута у попередньому розділі модель дозволяє моделювати відмову системи у випадку появи ФКНС, але такий підхід відображає тільки один критерій відмови для БСМ. В даному розділі розглянуто логічне продовження, вже запропонованої моделі, це імітаційна модель БСМ з урахуванням відмови системи за наступними критеріями:

– відмова критичної кількості сенсорів, що призводять до відмови системи;

– поява ФКНС, яка унеможливлює повне покриття системи моніторингу;

– критерій периферійного обладнання, відмова якого призводить до повної відмови системи.

З огляду на складність аналітичних розрахунків, при врахуванні усіх описаних критеріїв відмов було розроблено імітаційну модель БСМ для оцінювання ймовірності безвідмовної роботи БСМ. Модель дозволяє відтворити випадкові відмови сенсорів або периферійного обладнання, перевірити мережу на утворення кластерних відмов, враховуючи розміщення БСМ, та отримати показники безвідмовної роботи всієї системи.

Для моделювання відмов окремих сенсорів використовується експоненційний розподіл ймовірностей, що описує раптові відмови з постійною інтенсивністю λ відповідною функцією щільності ймовірностей f:

$$f(t;\lambda) = \lambda e^{-\lambda t}, \quad t \geq 0, \tag{3.4}$$

де: t – час;

λ – інтенсивність відмов.

Для більшої оцінки точності результатів, для ймовірності безвідмовної роботи визначається довірчий інтервал (ДІ):

$$CI = \underline{A} \pm z\frac{s_A}{\sqrt{M}}, \tag{3.5}$$

де: $\bar{A}$ – середнє вибіркове значення ймовірності безвідмовної роботи;

z – критичне значення (z–оцінка) зі стандартного нормального розподілу;

s_A – стандартне відхилення вибірки;

M – розмір вибірки, тобто загальна кількість прогонів симуляції, проведених в експерименті.

Для розташування сенсорів використовується матричне розміщення у вигляді регулярної двовимірної сітки. Кожен сенсор має логічні зв’язки виключно з найближчими сусідами (не більше 4 з’єднань одного сенсора), тобто для утворення ФКНС квадратна ділянка сенсора повинна мати спільну сторону з іншою

такою ділянкою. Діагональні з’єднання між двома сусідніми сенсорами не враховуються.

Процес імітаційного моделювання складається з наступних етапів.

1. Генерація мережі. На основі заданої кількості сенсорів розраховується відповідний крок для сітки з координатами. Генерується матриця сенсорної мережі. Для кожного сенсора формується зв’язок з сусідніми сенсорами, не більше 4 зв’язків відповідно. Формується матриця суміжності.

2. Генерація часу відмов. Для кожного сенсора незалежно генерується випадковий час відмови за експоненційним законом розподілу. Формується відповідний список відмов. Аналогічно генерується час відмови периферійного обладнання t_{periph}. Відповідний список сортується за зростанням.

3. Крок симуляції. На кожному кроці:

– порівнюється час поточної події t_i з часом відмови периферійного обладнання t_{periph} та порівнюється з часом моделювання T_{max}, у випадку коли $t_i \geq t_{periph}$ або $t_i \geq T_{max}$ симуляція на відповідному кроці припиняється;

– кожен крок t_i до списку відмов додаються координати сенсора. Далі йде перевірка кількості відмов сенсорів N_{failed}, якщо кількість $N_{failed} \geq N$, симуляція закінчується;

– запускається перевірка на просторовий критерію відмови алгоритмом пошуку в ширину, якщо знаходиться відповідна послідовність, то фіксується відмова системи.

4. Фінальний крок симуляції: якщо $t_{periph} \geq T_{max}$, фіксується відмова з відповідною позначкою «відмова периферійного обладнання». В іншому випадку, запуск окремої ітерації вважається успішним.

5. Агрегація результатів. У разі досягнення максимального часу моделювання або настання відмови, ітерація завершується, дані записуються у вибірку, після чого запускається наступна ітерація. Після завершення симуляції відбувається розрахунок ЙБР (формула 3.6):

$$R_{wsn} = \frac{i_{scs}}{M} \quad (3.6)$$

де M – загальна кількість ітерацій;

i_{scs} – кількість ітерацій які завершились успішно.

Далі розраховуємо довірчий інтервал для отриманих значень ЙБР.

Для дослідження розробленої моделі було проведено серію експериментів, що дозволили оцінити вплив різних критеріїв відмови та ділянок області моніторингу на показники надійності мережі. Було проведено 10 циклів симуляцій по 100000 ітерацій з використанням таких показників:

– $\lambda = \{10^{-4}, 10^{-5}, 10^{-6}\}$ – інтенсивність відмови сенсора;
– $N = \{50,100,200\}$ – кількість сенсорів у системі;
– $T_{max} = \{100,1000,5000,10000,50000\}$ – час роботи системи;
– $N_{failed} = \{6,8,10\}$ – кількість сенсорів які призводять до відмови;
– $Ad = \{2,3,4\}$ – кількість суміжних сенсорів для утворення ФКНС;
– $CI = 0.90$ – довірчий інтервал.

В рамках дослідження було проведено 4 експерименти, які дозволили оцінити:

1. Вплив інтенсивності відмов сенсорів системи на ЙБР.
2. Вплив ФКНС та розмірності суміжних непрацездатних сенсорів на ЙБР.
3. Вплив геометричної форми просторового розташування сенсорної мережі на ЙБР.
4. Вплив інтенсивності відмов периферійного обладнання на ЙБР.

Експеримент 1. Порівняння впливу інтенсивності відмов на ЙБР системи. Вхідні дані: $N = 100$, $N_{failed} = 10$, $Ad = 3$.

Аналізуючи графік рисунка 3.12, можна зробити висновок, що різниця у використанні сенсорів з різною інтенсивністю відмов є критичною.

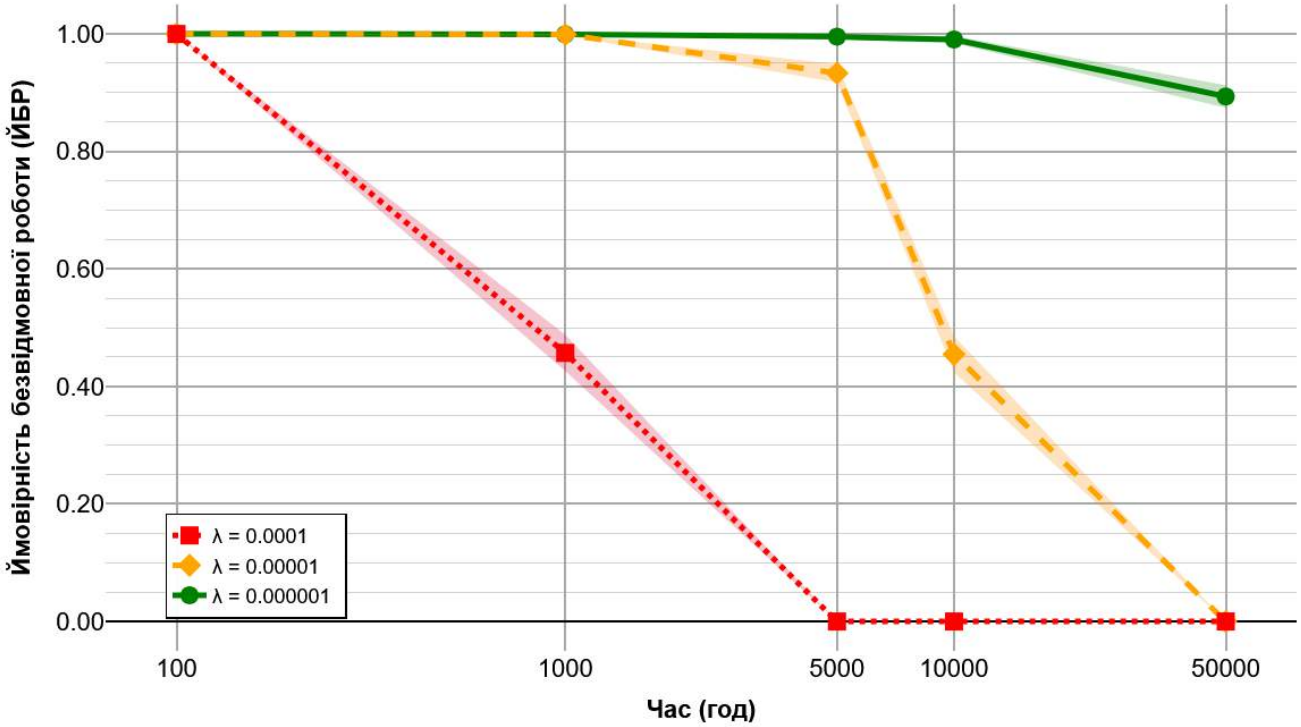

Рисунок 3.12 – Графік ймовірності безвідмовної роботи для різних інтенсивностей відмови сенсорів при $\lambda = \{10^{-4},10^{-5},10^{-6}\}$ 1/год

Таблиця 3.6 – Результати моделювання ймовірності безвідмовної роботи для $\lambda = 10^{-6}$ 1/год, $N = 100$

T_{max}	R_{wsn}	ДІ – верхня	ДІ – нижня
100	0.99989	0.999944551	0.999835449
1000	0.99902	0.999182755	0.998857245
5000	0.99481	0.995183755	0.994436245
10000	0.98977	0.990293406	0.989246594
50000	0.89862	0.900189993	0.897050007

Таблиця 3.7 – Результати моделювання ймовірності безвідмовної роботи для $\lambda = 10^{-5}$ 1/год, $N = 100$

T_{max}	R_{wsn}	ДІ – верхня	ДІ – нижня
100	0.99991	0.99991	0.999860656
1000	0.99854	0.99854	0.998341394
5000	0.94158	0.94158	0.940360048
10000	0.46263	0.46263	0.460036495
50000	0	0	0

Таблиця 3.8 – Результати моделювання ймовірності безвідмовної роботи для $\lambda = 10^{-4}$ 1/год , $N = 100$

T_{max} (год)	R_{wsn}	ДІ – верхня	ДІ – нижня
100	0.99946	0.999580841	0.999339159
1000	0.46919	0.471785837	0.466594163
5000	0	0	0
10000	0	0	0
50000	0	0	0

Аналіз результатів, наведених у таблицях 3.6, 3.7 та 3.8, дозволяє зробити висновок, що інтенсивність відмов сенсорів має критичний вплив на надійність БСМ. Застосування компонентів із $\lambda = 10^{-4}$ 1/год і вище призводить до повної відмови системи вже на позначці 5000 годин (що еквівалентно 208 добам). Отже, використання сенсорів із такою інтенсивністю відмов є недоцільним, якщо очікуваний час безперервної роботи системи перевищує 1000 годин. Порівняння сенсорів з інтенсивностями відмов $\lambda = 10^{-5}$ 1/год та $\lambda = 10^{-6}$ 1/год свідчить про те, що показники ЙБР починають суттєво різнитися на позначці 10 000 годин, де різниця сягає 53%. Обидва типи сенсорів придатні для систем сезонного моніторингу лісових ділянок, проте вибір надійніших вузлів у такому разі може призвести до значного збільшення бюджету на впровадження системи.

Експеримент 2. Вплив ділянки розміщення сенсорів на ЙБР. За допомогою створеного програмного засобу було згенеровано 3 різні ділянки відповідних форм: еліпс, прямокутник та фігура довільної форми (рисунки 3.13–3.15). Вхідні дані: $N = 50$, $N_{failed} = 10$, $\lambda = 10^{-5}$ 1/год.

При генерації сенсорної сітки враховується формат зображення. Тому при візуалізації на широкоформатній мапі відповідний квадрат сенсора може виглядати розтягнутим по ширині, тобто нагадувати прямокутник, але відповідне припущення при візуалізації не впливає на результати моделювання системи.

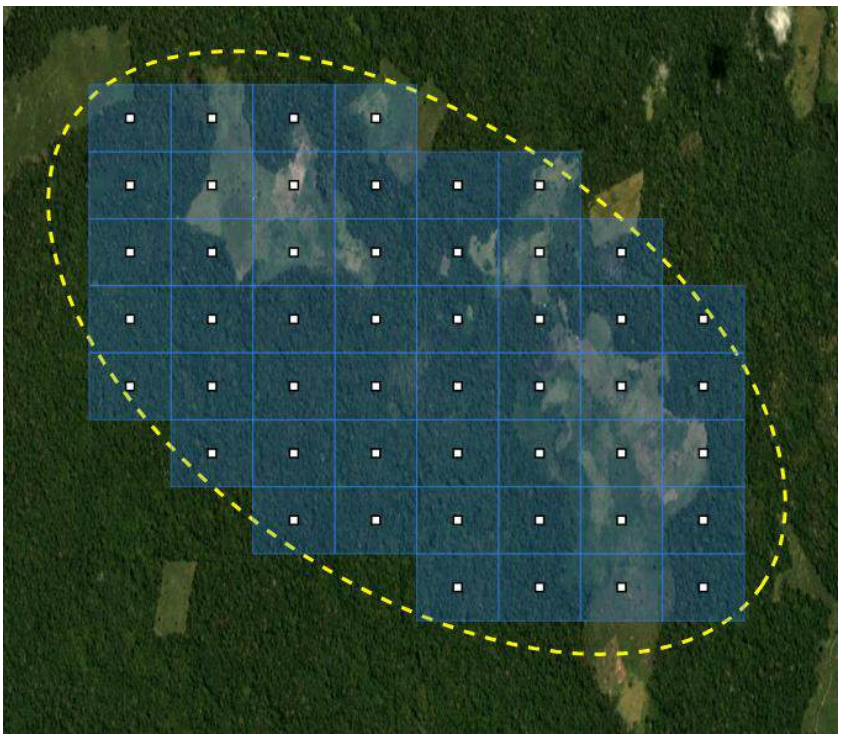

Рисунок 3.13 – Карта сенсорів з площею покриття еліптичної форми з N = 50

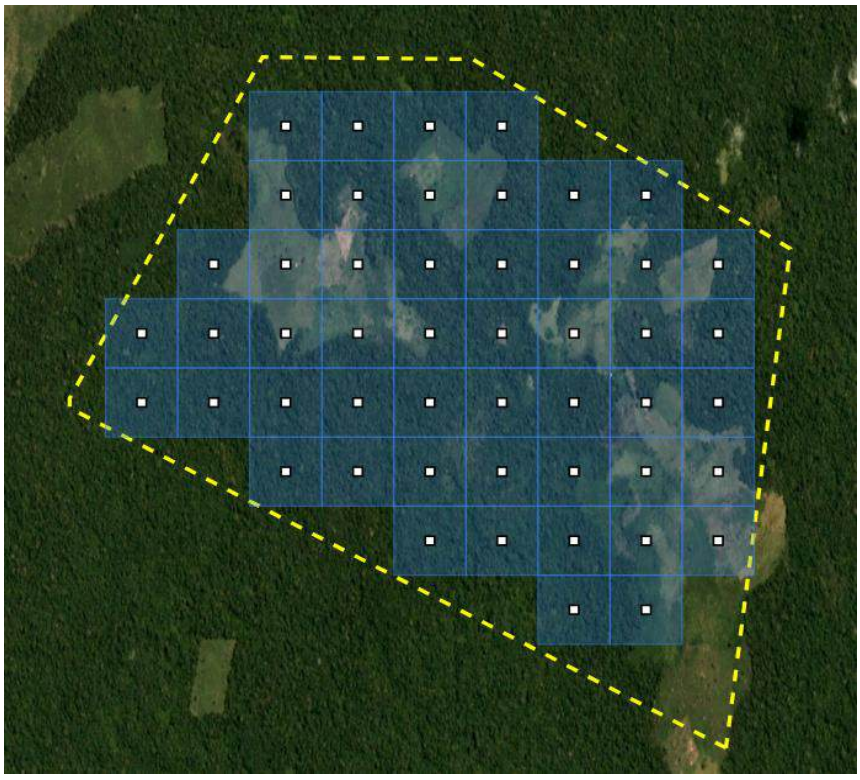

Рисунок 3.14 – Карта сенсорів площею покриття випадкової форми при N = 50

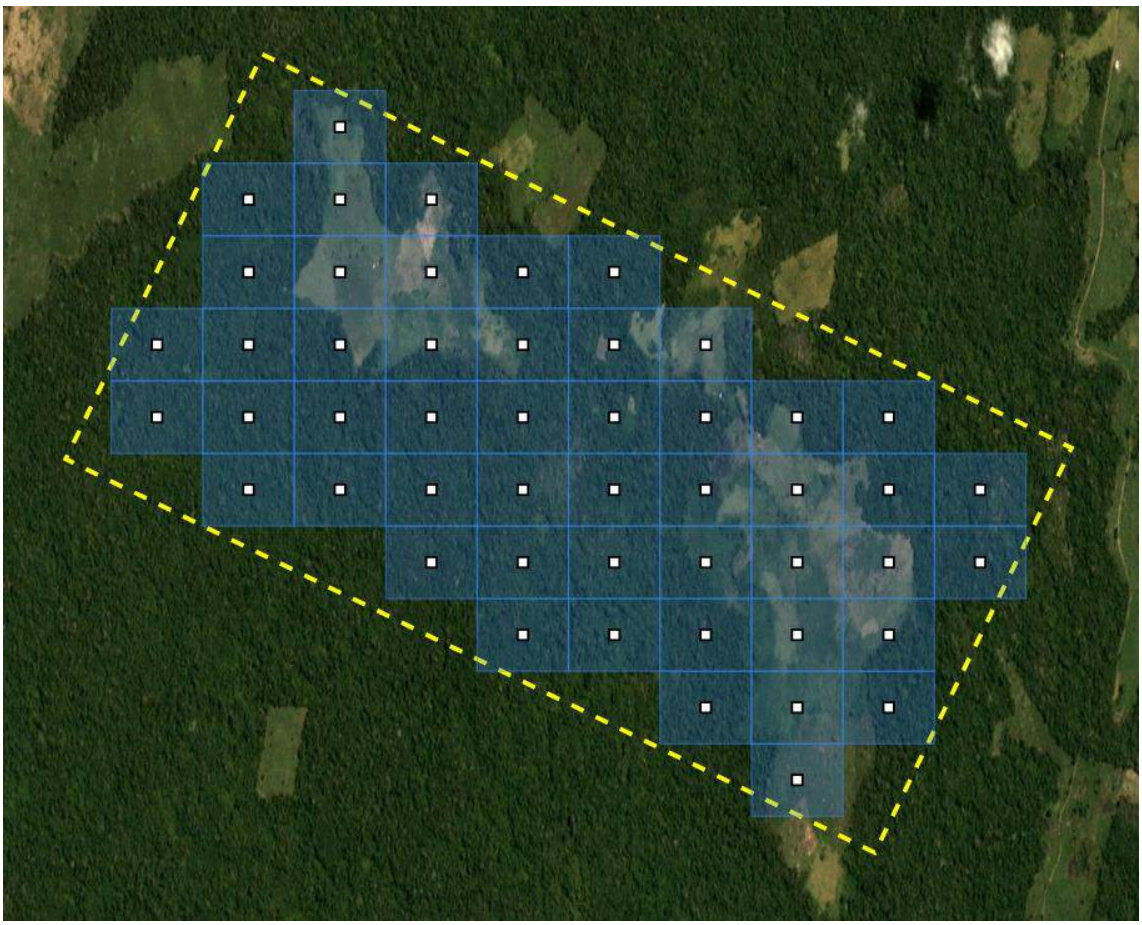

Рисунок 3.15 – Карта сенсорів площею покриття прямокутної форми при N = 50

Відповідною задачею було порівняння впливу геометричної фігури, в якій розміщуються сенсори, на ЙБР при $\lambda = 10^{-5}$1/год та $N = 50$.

На основі даних, наведених у таблиці 3.9 та на рисунку 3.16, проведено порівняльний аналіз надійності мережі залежно від геометричної форми зони моніторингу. Перевагою застосованої моделі є те, що під час проєктування сенсорної мережі та дослідження різних варіацій її розміщення можна безпосередньо враховувати умовний опис реальної ділянки розгортання. На рисунку 3.16 для наочності продемонстровано ймовірність відмови системи.

Проведений аналіз згенерованих зон покриття (прямокутних, еліптичних та довільних багатокутних) показав, що геометрична форма фігури розміщення не здійснює суттєвого впливу на загальні показники системи. При детальному порівнянні ймовірності безвідмовної роботи саме прямокутна ділянка демонструє

дещо вищі показники надійності порівняно з еліптичною та довільною (багатокутною) конфігураціями. Водночас варто відзначити, що саме нерегулярні багатокутні форми найчастіше зустрічаються в реальних умовах проєктування. Ці результати були підтверджені шляхом проведення п’яти симуляцій по 100 000 ітерацій для кожної з досліджуваних фігур.

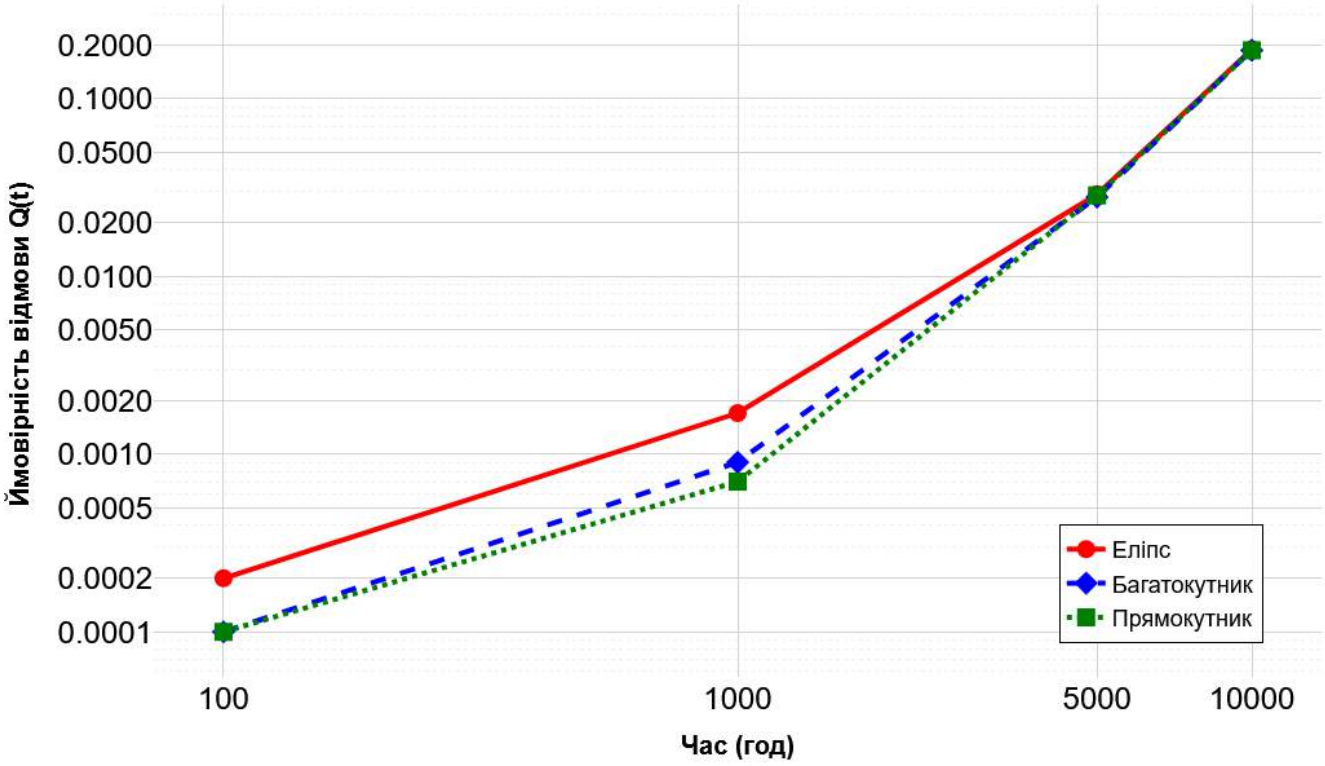

Рисунок 3.16 – Графік результатів моделювання для еліпса, багатокутника та прямокутника

Таблиця 3.9 – Результати моделювання для різних фігур, в яких розміщуються сенсори

Час (год)	R_{wsn} (еліпс)	R_{wsn} (багатокутник)	R_{wsn} (прямокутник)
100	0.9998	0.9999	0.9999
1000	0.9983	0.9991	0.9993
5000	0.9711	0.9721	0.9715
10000	0.8112	0.8132	0.8135

Експеримент 3. Вплив кількості сенсорів у ФКНС. Вхідні дані: $N = 200$, $N_{failed} = 10$, $Ad = \{2,3,4\}$, $\lambda = 10^{-5}$ 1/год.

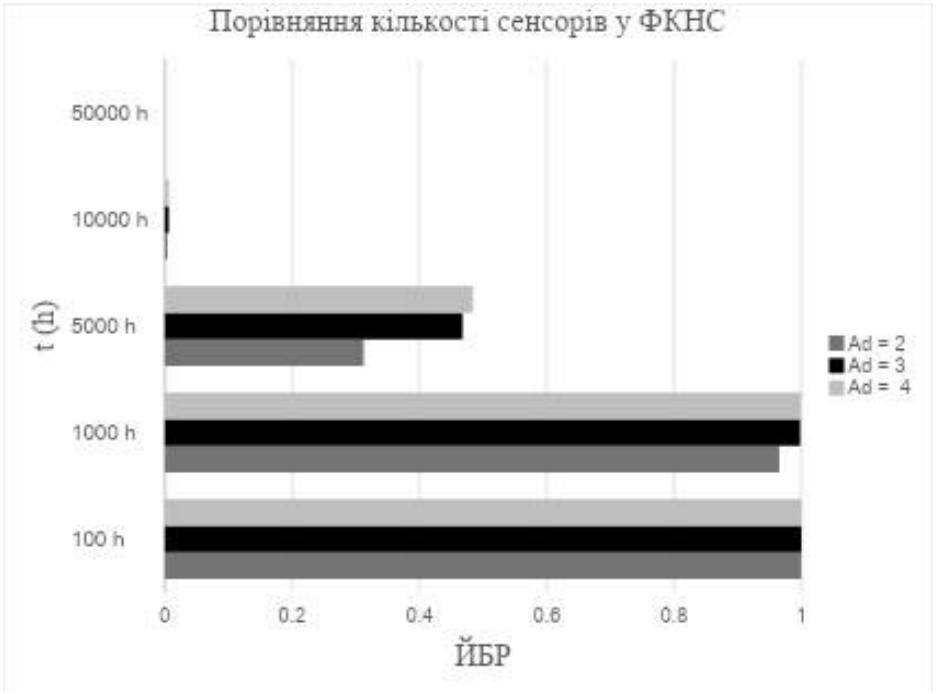

Рисунок 3.17 – Порівняльна гістограма пливу ФКНС на ЙБР сенсорної мережі

Аналіз результатів моделювання, наведених на рисунку 3.17, показує вплив зміни параметра *Ad* (кількості сенсорів у ФКНС) на надійність системи. Виявлено, що при встановленні мінімального значення $Ad = 2$ спостерігається стрімке падіння ЙБР. Зокрема, при збільшенні часу симуляції з 1000 до 5000 годин (при 100 000 ітераціях) кількість відмов суміжних сенсорів зростає більш ніж у 10 разів – з 3369 до 39 103 випадків. При збільшенні критерію до $Ad = 4$ отримано такі результати: зростання часу симуляції з 1000 до 5000 годин призводить до збільшення кількості відмов понад 50 разів, проте абсолютний показник при цьому змінюється лише з 6 до 373 відмов на 100 000 ітерацій. Отже, зміна параметра допустимої кількості суміжних відмов сенсорів критично впливає на ЙБР мережі. Врахування цього критерію під час проєктування БСМ дозволяє суттєво підвищити точність розрахунків імовірності безвідмовної роботи системи. Детальні результати моделювання представлені в таблиці 3.10.

Таблиця 3.10 – Результати моделювання ймовірності безвідмовної роботи для $\lambda = 10^{-5}$1/год, $N = 100$ при зміні розмірності ФКНС

Час (год)	Ad = 2	Ad = 3	Ad = 4
100	0.99959	0.99988	0.9999
1000	0.96517	0.99797	0.99903
5000	0.31239	0.46775	0.48403
10000	0.00391	0.00624	0.00616
50000	0	0	0

Моделювання впливу відмов ПОб здійснюється шляхом зміни інтенсивності відмов такого обладнання λ_{pereph}. Стандартним значенням для нашого моделювання є $\lambda_{pereph} = 10^{-6}$ 1/год. Відповідно, у межах експерименту було оцінено стан системи при зменшенні та збільшенні цього показника. Зокрема, досліджено вплив на систему таких значень: $\lambda_{pereph} = 10^{-4}$ 1/год, $\lambda_{pereph} = 10^{-5}$ 1/год та $\lambda_{pereph} = 10^{-7}$ 1/год. Як продемонстровано на рисунку 3.18, інтенсивність відмов периферійного обладнання прямо впливає на ЙБР системи. При $\lambda_{pereph} = 10^{-4}$ 1/год система починає критично деградувати після 1000 годин експлуатації. Зменшення інтенсивності до $\lambda_{pereph} = 10^{-5}$ 1/год забезпечує стабільнішу роботу системи, водночас подальше зниження показника до $\lambda_{pereph} = 10^{-7}$ 1/год суттєво не підвищує ЙБР. Отже, можна зробити висновок, що для досліджуваної моделі раціональні значення λ_{pereph} знаходяться в діапазоні до $\lambda_{pereph} = 10^{-5}$ 1/год. Оскільки цей параметр має прямий і визначальний вплив на загальну ЙБР, вибір надійної елементної бази для периферійного обладнання є критично важливим етапом проєктування системи моніторингу.

У межах підрозділу розроблено імітаційну модель, яка дозволяє здійснювати моделювання масштабних бездротових сенсорних мереж із використанням методу Монте-Карло. Застосований підхід дає змогу виявляти критичні сценарії відмов та розраховувати ймовірність безвідмовної роботи (ЙБР) систем, для яких використання наявних аналітичних моделей є недоцільним через високу обчислювальну складність, зумовлену значною кількістю сенсорів. Крім того, розроблена модель дозволяє ідентифікувати просторові відмови, виявлення яких за допомогою аналітичного моделювання є складним завданням. Програмно-

архітектурна реалізація імітаційної моделі, зокрема, опис графічного інтерфейсу та структури класів спеціалізованого програмного засобу, детально розглянута у четвертому розділі дисертаційної роботи.

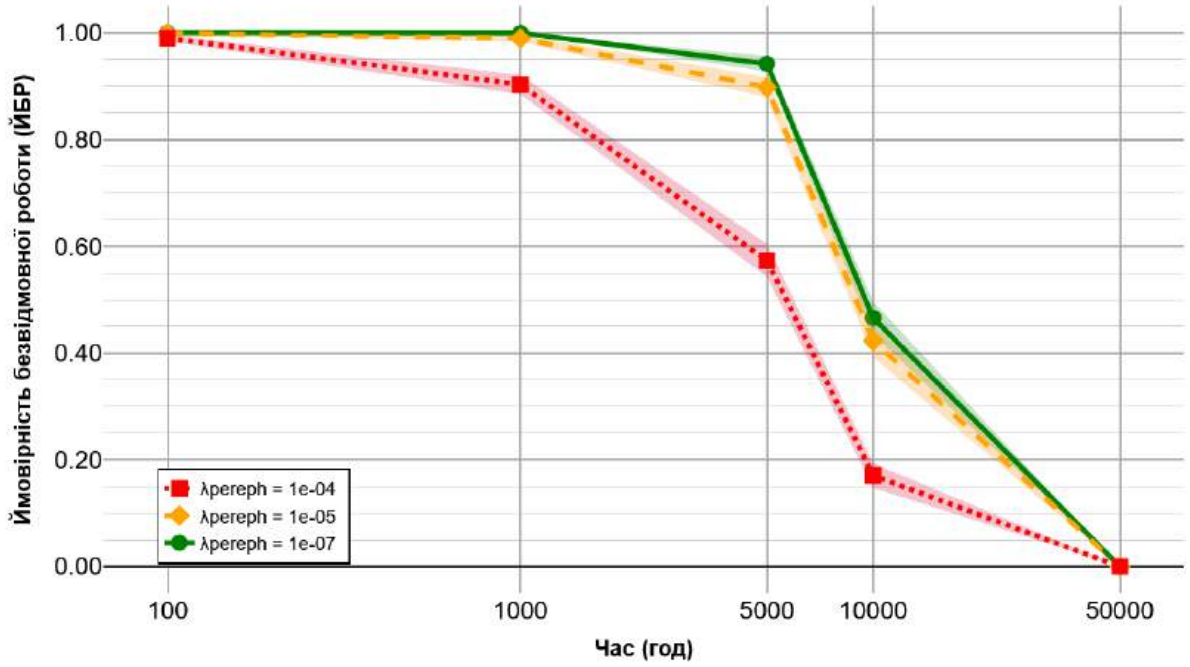

Рисунок 3.18 – Графік порівняння впливу інтенсивності відмов периферійного обладнання для $\lambda = 10^{-5}$ 1/год, $N = 100$

3.3 Висновки до третього розділу

У розділі розроблено методологію оцінювання надійності відновлюваних наземних сенсорних мереж систем моніторингу потенційно небезпечних територій, що ґрунтується на структурно-автоматному підході та використанні апарату дискретно-неперервних марковських ланцюгів. На відміну від спрощених моделей, запропонований підхід враховує стохастичну динаміку відмов сенсорів, відмов периферійного обладнання, процедури відновлення та вплив організації ремонтного обслуговування на готовність системи.

Побудовано марковську модель наземної сенсорної мережі з відновленням, формалізовану через систему векторів станів, структурно-автоматну модель та систему диференціальних рівнянь Колмогорова-Чепмена. Це забезпечило можливість кількісного оцінювання коефіцієнта готовності мережі з урахуванням

переходів між працездатними, частково працездатними станами, а також станами простою та відновлення.

За результатами дослідження марковської моделі встановлено, що визначальний вплив на коефіцієнт готовності наземної сенсорної мережі чинять інтенсивність відмов сенсорів та середній час очікування ремонтної бригади. Доведено, що саме параметри сенсорної підсистеми та організація відновлення формують основний внесок у втрату готовності, тоді як вплив відмов периферійного обладнання є менш істотним за базових умов, але зростає зі збільшенням надійності сенсорних компонентів.

Розроблено імітаційну модель надійності бездротової сенсорної мережі з урахуванням фатальних комбінацій множинних відмов сенсорів, яка дозволяє досліджувати просторово зумовлені сценарії втрати працездатності для мереж довільної конфігурації. На відміну від аналітичних підходів, запропонована модель забезпечує практичну реалізацію оцінювання надійності для великомасштабних мереж із складною геометрією розміщення сенсорів.

У результаті імітаційного моделювання встановлено закономірності впливу кількості непрацездатних сенсорів, параметрів фатальних комбінацій та інтенсивності відмов на ймовірність безвідмовної роботи мережі. Доведено, що зростання кількості відмов сенсорів і зменшення порогу формування фатальних комбінацій призводять до істотного погіршення показників надійності, тоді як геометрична форма ділянки розміщення сенсорів не чинить визначального впливу на інтегральні характеристики безвідмовності.

Розроблено розширену імітаційну модель наземної сенсорної мережі, яка комплексно враховує три критерії відмови: досягнення критичної кількості непрацездатних сенсорів, утворення фатальних комбінацій суміжних відмов та відмову периферійного обладнання. Це дало змогу сформувати науково обґрунтований інструментарій для оцінювання надійності масштабних сенсорних мереж і обґрунтування проєктних рішень щодо вибору параметрів елементної бази, резервування та експлуатаційних режимів систем моніторингу потенційно небезпечних територій.

РОЗДІЛ 4
РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ОЦІНЮВАННЯ НАДІЙНОСТІ ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ТЕРИТОРІЙ. ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

4.1 Програмний засіб для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі

4.1.1 Архітектура програмного засобу для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі

Для автоматизації процесів розрахунку показників надійності, у тому числі для систем моніторингу з багаторівневою працездатністю на основі ГСМ, що пропонує модель, розглянута у підпункті 2.2.2.2, було створено відповідний програмний засіб. Функціональні можливості засобу, окрім аналітичних розрахунків, дозволяють побудувати діаграми ймовірності перебування системи моніторингу в різних частково працездатних станах та створення структурних схем надійності. Інструмент під назвою «Calculation of the main indicators of the reliability and survivability of the monitoring system» було створено для використання інженерами та операторами кризових центрів. Згаданий функціонал інструменту дозволяє ефективно оцінювати показники надійності на етапі проєктування систем моніторингу ПНТ на основі ГСМ.

Програмний засіб можна розділити на три основні компоненти. Ці компоненти забезпечують введення параметрів, їх аналітичну обробку з використання формул з підпункту 2.2.2.2 та подальшу візуалізацію результатів:

1. Графічний інтерфейс користувача. Цей компонент є головним у контексті взаємодії оператора з програмним засобом. Він реалізований у вигляді головної панелі управління, яка містить поля для введення вихідних даних та область відображення результатів розрахунку показника ЙБР.

2. Модуль обробки даних та аналітичних розрахунків. Цей рівень використовує моделі надійності та багаторівневої працездатності для гібридних

сенсорних мереж, розроблені та описані у розділі 2. Розрахункове ядро автоматично обробляє введені конфігураційні дані флотів БПЛА та обчислює ймовірності перебування системи як у стані повної працездатності, так і в частково працездатних станах (станах деградації).

3. Рушій для візуалізації, агрегації та обробки результатів. Цей компонент відповідає за динамічну побудову графічного представлення системи моніторингу. На основі розрахованих даних модуль генерує загальну схему системи, структурні схеми надійності та діаграми рівнів деградації.

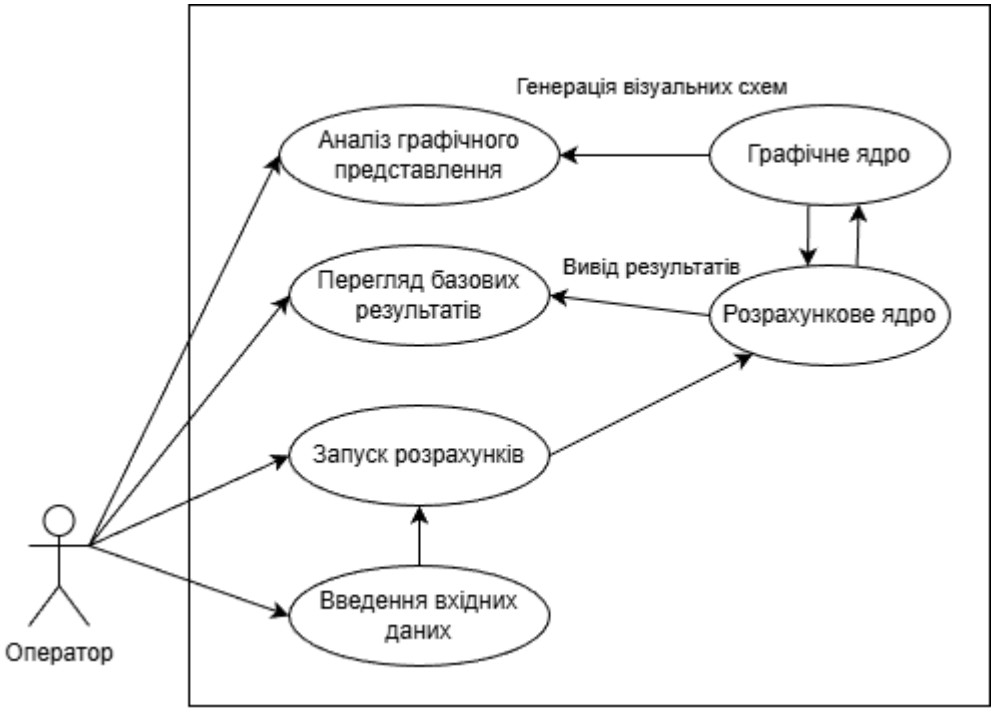

Рисунок 4.1 – Діаграма варіантів використання

На рисунку 4.1 зображено, як оператор кризового центру може взаємодіяти з програмним забезпеченням.

За допомогою панелі управління графічного інтерфейсу оператор здатен налаштовувати систему, вводячи такий набір параметрів:

– загальна кількість літаючих сенсорів (БПЛА);

– загальна кількість літаючих вузлів граничних обчислень;

– кількість основних (робочих) літаючих вузлів граничних обчислень (визначає рівень структурного резервування типу «k-out-of-n»);

– інтенсивність відмов наземної станції управління (1/год);

– інтенсивність відмов літаючого сенсора (1/год);

– інтенсивність відмов літаючого вузла граничних обчислень (1/год);

– інтенсивність відмов головного кризового центру (1/год);

– інтенсивність відмов віртуального кризового центру (1/год);

– загальна кількість непрацездатних літаючих сенсорів, необхідна для переходу флоту літаючих сенсорів з повністю працездатного стану до частково працездатного;

– загальна кількість основних непрацездатних літаючих вузлів граничних обчислень, необхідна для переходу флоту граничних вузлів до частково працездатного стану;

– загальна кількість непрацездатних літаючих вузлів граничних обчислень, що призводить до деградації відповідного флоту;

– операційний час (час виконання місії моніторингу, у годинах).

Взаємодія оператора кризового центра з компонентами ПЗ продемонстровано на діаграмі послідовностей (рисунок 4.2).

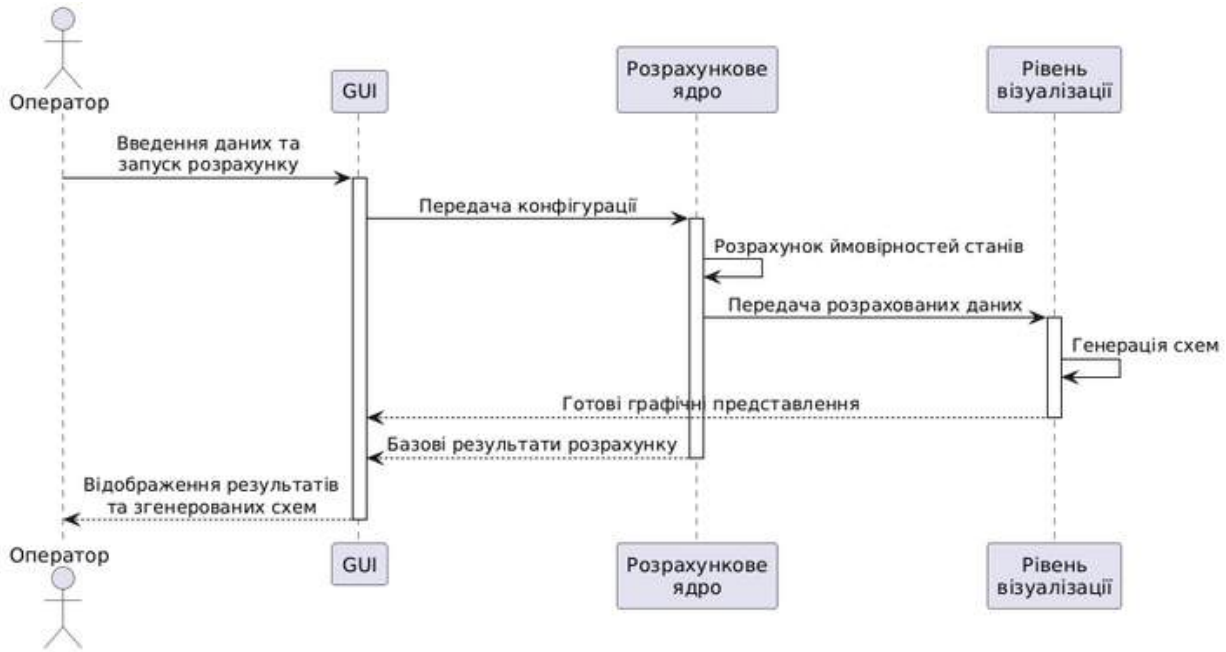

Рисунок 4.2 – Діаграма послідовності

Панель введення вхідних даних та виклику результатів наведено на рисунку 4.3.

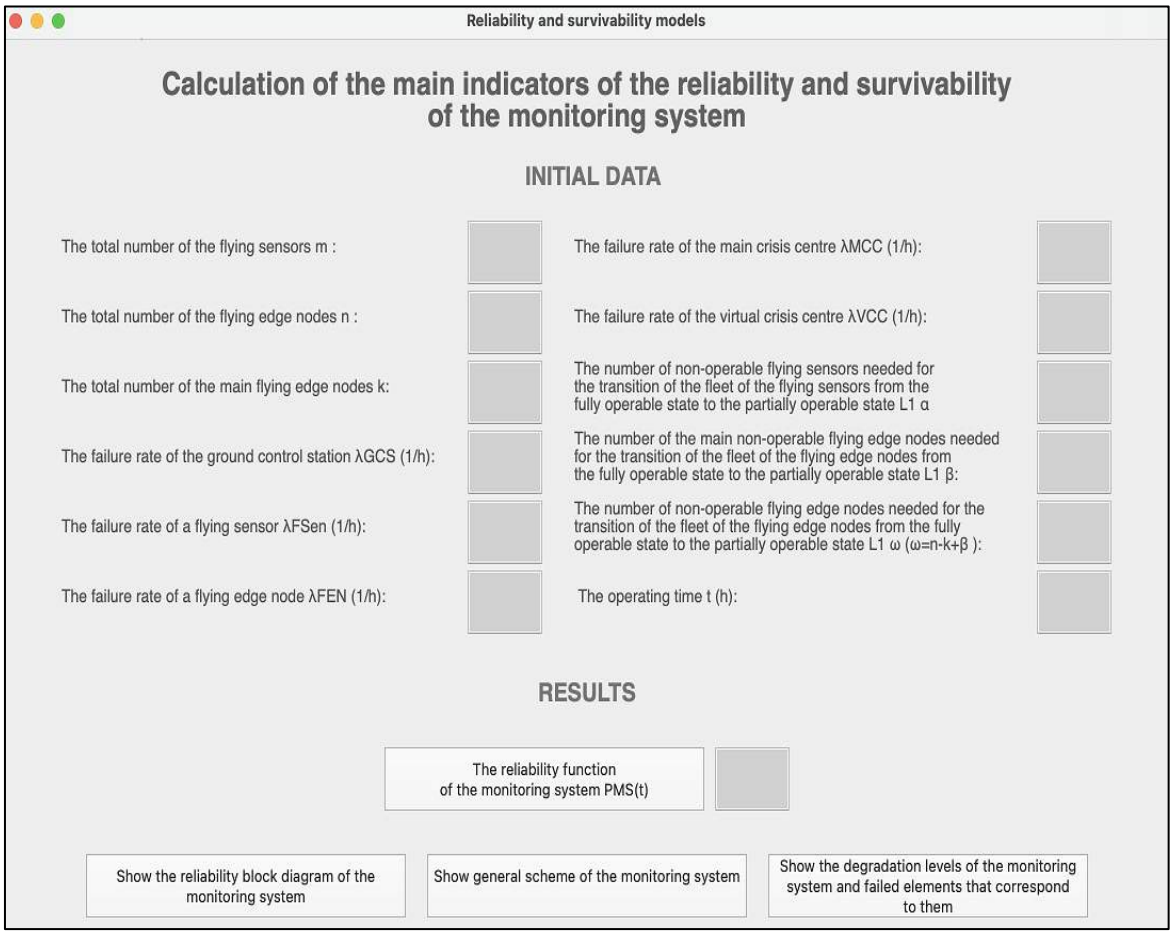

Рисунок 4.3 – Панель для введення вихідних даних і виклику результатів

Логіка роботи програмного засобу побудована таким чином, що після введення всіх необхідних параметрів, модуль аналітичних розрахунків виконує операції для оцінки показників надійності. Результат розрахунку ймовірності безвідмовної роботи системи моніторингу автоматично відображається безпосередньо на головній панелі у вікні «The reliability function of the monitoring system».

Для доступу до функцій візуалізації панель управління інтерфейсу передбачає наявність спеціальних функціональних кнопок:

– кнопка «Show the general scheme of the monitoring system» – ініціює виклик графічного вікна, що містить візуалізовану загальну схему системи моніторингу, адаптовану під обрану кількість компонентів;

– кнопка «Show the reliability block diagram of the monitoring system» – дозволяє оператору переглянути згенеровану структурну схему надійності системи, яка відображає зв’язок між елементами;

– кнопка «Show the degradation levels of the monitoring system and failed elements that correspond to them» – викликає інформаційне вікно, яке містить діаграму рівнів деградації системи. У цьому вікні також виводиться перелік елементів, що відмовили і відповідають кожному з рівнів, та результати розрахунку ймовірностей перебування системи у відповідному частково працездатному стані ij_i (де i – номер рівня деградації, а j_i – номер стану на рівні i).

4.1.2 Особливості застосування програмного засобу для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі

Для демонстрації функціональних можливостей розробленого програмного засобу «Calculation of the main indicators of the reliability and survivability of the monitoring system» розглянемо практичний приклад його застосування. Основною метою інструменту є визначення ймовірності безвідмовної роботи та ймовірностей перебування у станах часткової працездатності, а також автоматична генерація відповідних схем для заданої конфігурації системи.

Перед оператором кризового центру стоїть завдання спроєктувати місію моніторингу з використанням наступних вхідних параметрів системи:

– загальна кількість літаючих сенсорів (БПЛА) = 21;

– загальна кількість літаючих вузлів граничних обчислень = 10;

– кількість основних літаючих вузлів граничних обчислень (необхідних для повноцінного виконання завдання) = 7;

– інтенсивність відмов наземної станції управління (GCS) = 0.00025 1/год;

– інтенсивність відмов літаючого сенсора (FSen) = 0.001 1/год;

– інтенсивність відмов літаючого вузла граничних обчислень (FEN) – 0.005 1/год;

– інтенсивність відмов головного кризового центру (MCC) = 0.00085 1/год;

– інтенсивність відмов віртуального кризового центру (VCC) = 0.00075 1/год;

– порогова кількість непрацездатних літаючих сенсорів для переходу флоту в частково працездатний стан = 1;

– порогова кількість основних непрацездатних літаючих вузлів граничних обчислень для переходу флоту в частково працездатний стан = 1;

– загальна кількість непрацездатних літаючих вузлів граничних обчислень, що призводить до повної деградації підсистеми = 4;

– час виконання місії = 9 годин.

Оператор вводить зазначені параметри у відповідні поля головної панелі управління програмного засобу. Результат заповнення панелі вихідними даними наведено на рисунку 4.4.

На рисунку 4.4 продемонстровано, що після введення всіх необхідних вхідних параметрів програмний засіб автоматично обчислює показник ймовірності безвідмовної роботи всієї системи моніторингу. Результат відображається у нижній частині панелі в спеціальному полі «The reliability function of the monitoring system». Такий підхід дозволяє автоматизувати складні аналітичні обчислення показників надійності систем моніторингу на основі гібридних сенсорних мереж, розглядаючи їх як системи з багаторівневою працездатністю. Для візуального контролю встановленої конфігурації створюється загальна схема архітектури системи шляхом натискання кнопки «Show the general scheme of the monitoring system». Після цього програма самостійно формує загальну схему мережі, наочно відображаючи взаємодію всіх ключових компонентів системи моніторингу. Генерацію загальної схеми системи моніторингу з багаторівневою працездатністю представлено на рисунку 4.5.

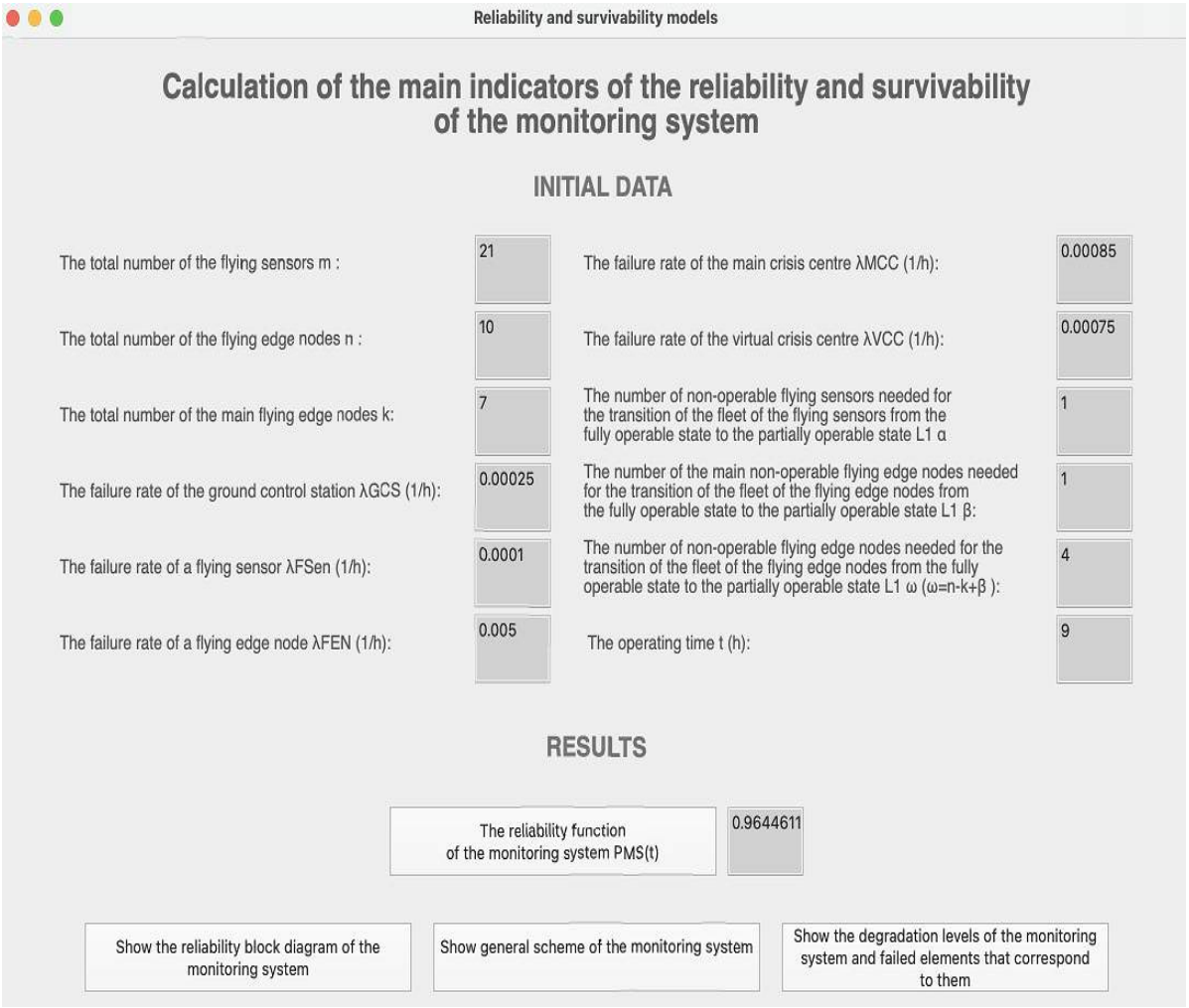

Рисунок 4.4 – Панель після введення початкових даних

Згенерована схема на рисунку 4.5 демонструє взаємодію ключових підсистем MCC, VCC, GCS та відображає введену кількість літаючих вузлів: 21 вузол, які передають дані на 10 літаючих вузлів граничних обчислень.

Наступним кроком є аналіз візуалізації логічних взаємозв’язків компонентів системи. За допомогою кнопки «Show the reliability block diagram of the monitoring system» програмний засіб створює структурну схему надійності.

Рисунок 4.6 показує послідовно-паралельну модель надійності для заданої конфігурації. На схемі видно, що загальна працездатність залежить від наземної станції управління, флоту сенсорів, флоту граничних обчислень, а також кризових центрів. Такий варіант візуалізації дозволяє ідентифікувати критичні компоненти, які можуть найбільше впливати на надійність системи моніторингу та архітектури в цілому.

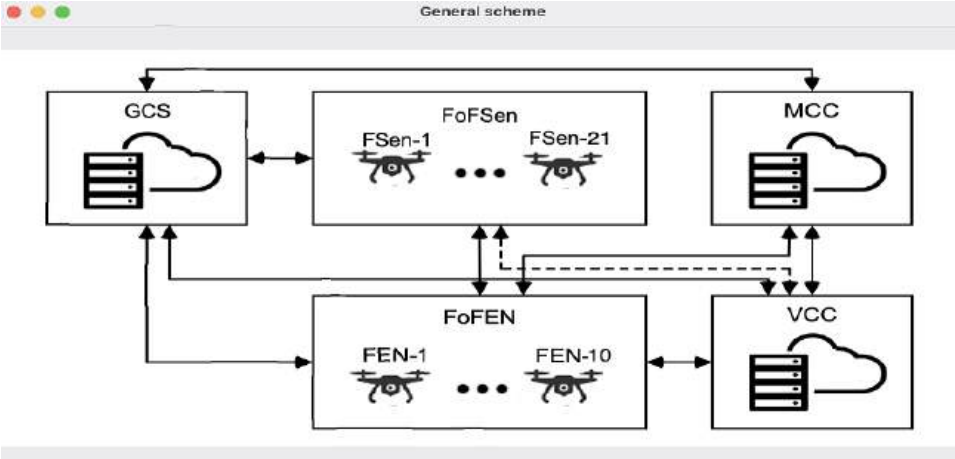

Рисунок 4.5 – Вікно із загальною схемою системи моніторингу

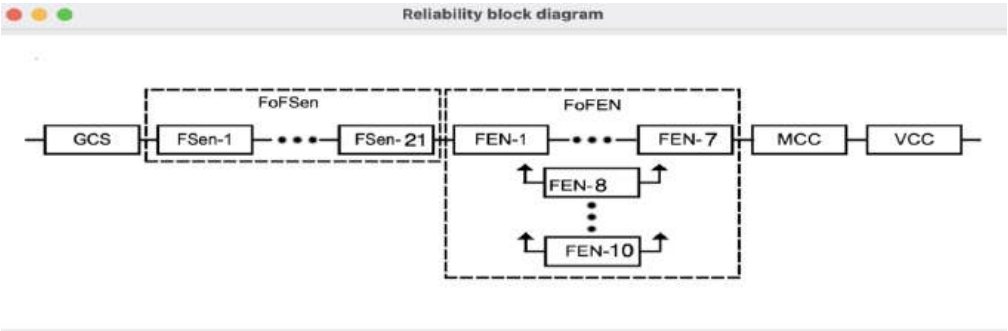

Рисунок 4.6 – Вікно з структурною схемою надійності системи моніторингу

Оскільки система моніторингу на основі ГСМ розглядається як система з багаторівневою працездатністю, є доцільним оцінювання її в умовах часткової деградації. Для цього використовується функція виклику діаграми рівнів деградації через кнопку «Show the degradation levels of the monitoring system and failed elements that correspond to them».

На рисунку 4.7 наведено вікно з результатами розрахунку. Програмне забезпечення автоматично формує таблицю, в якій:

– вказано номери рівнів деградації i (від 0 до 4);

– визначено номери частково працездатних станів ij_i на кожному рівні;

– наведено перелік елементів, відмова яких призводить до переходу системи у відповідний стан (наприклад, стан *12* відповідає частковій відмові флоту літаючих сенсорів);

– розраховано числові значення ймовірності $P_{MS\_ij}(t)$ перебування системи в кожному з цих станів на момент завершення місії.

Аналіз даних, наведених на рисунку 4.7, дозволяє визначити ймовірність, з якою система зможе продовжувати виконання своїх функцій у режимі обмеженої працездатності (наприклад, у разі втрати одного кризового центру або частини мобільних граничних вузлів), що є ключовим показником надійності при моніторингу ПНТ.

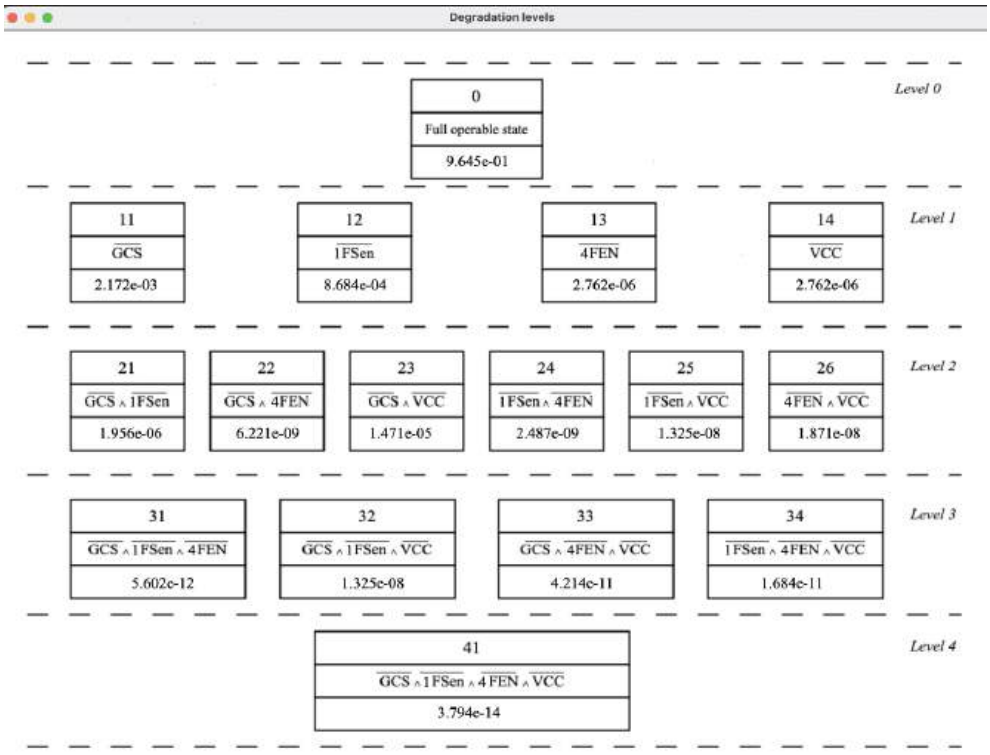

Рисунок 4.7 – Імовірності перебування системи моніторингу в різних частково працездатних станах

Застосування розробленого програмного засобу дозволяє автоматизувати складні аналітичні розрахунки та забезпечити оперативне прийняття рішень щодо оптимальної конфігурації системи моніторингу. Оператор кризового центру має можливість швидко розрахувати ЙБР всієї системи та її стани часткової працездатності для прийняття рішень щодо використання тих чи інших конфігурацій для компонентів систем моніторингу.

4.2 Програмний засіб для оцінювання надійності бездротової сенсорної мережі з урахуванням фатальних комбінацій множинних відмов сенсорів

4.2.1 Архітектура програмного засобу для оцінювання надійності бездротової сенсорної мережі з урахуванням фатальних комбінацій множинних відмов сенсорів

Для автоматизації процесу генерації конфігурацій бездротової сенсорної мережі (БСМ) та оцінювання її надійності шляхом імітаційного моделювання було розроблено спеціалізований програмний засіб мовою Python. Цей інструмент призначений для дослідження ймовірності відмови мережі за умови просторових стохастичних відмов, що призводять до формування фатальних комбінацій непрацездатних сенсорів (ФКНС) на заданій території моніторингу лісових пожеж.

Програмний засіб розроблено за модульним принципом. Такий підхід дозволяє чітко розділити компоненти програмного засобу за їх призначенням, що в подальшому спрощує додавання нових функцій та зміну поведінки існуючих, оскільки зміна окремого модуля не буде безпосередньо впливати на роботу іншого.

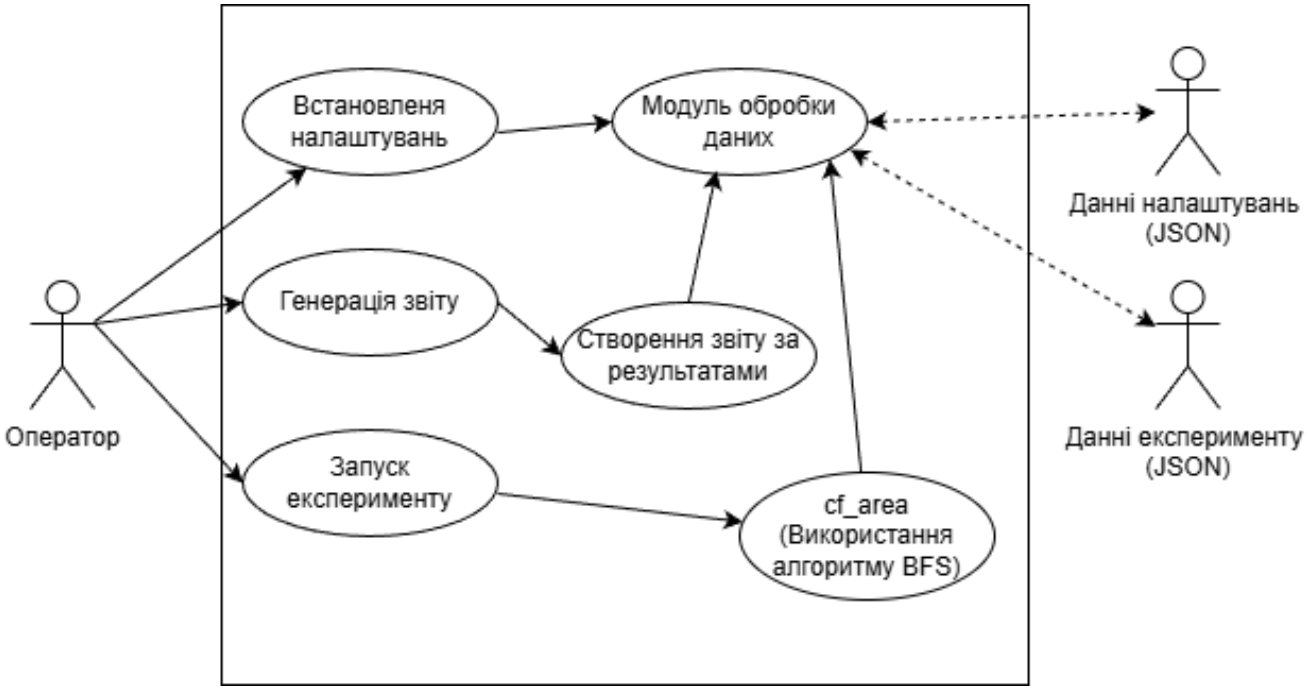

Рисунок 4.8 – Діаграма варіантів використання програмного засобу оцінки впливу ФКНС на надійність системи.

Для візуалізації взаємодії компонентів системи з оператором було розроблено діаграму варіантів використання, представлену на рисунку 4.8.

Для реалізації програмного забезпечення було спроєктовано три відповідні програмні класи:

1. Клас налаштування та обробки відповідає за прийом вхідних даних від користувача або з конфігураційних файлів. Включає модуль обробки даних, який трансформує вхідні параметри конфігурації у формат, зрозумілий для подальшого оброблення програмним засобом. Через цей модуль ми вказуємо мапу для розміщення сенсорів та їх кількість.

2. Клас бізнес-логіки та імітаційного моделювання: основним компонентом цього рівня є розрахунковий модуль cf_area, який виконує основну функцію програмного засобу і генерує випадкові відмови на вказаній мапі. Він відповідає безпосередньо за проведення циклів імітаційного моделювання та використовує алгоритм пошуку в ширину для розпізнавання суміжних непрацездатних сенсорів на визначеній мапі та ідентифікує утворені ФКНС.

3. Клас агрегації даних та звітності: реалізований модулем, який збирає проміжні експериментальні дані з усіх ітерацій, виконує їх агрегацію, проводить розрахунки ймовірності відмови БСМ та формує підсумкові звіти для аналізу.

Базовий функціонал розробленого програмного засобу дозволяє виконувати такі основні дії:

– генерувати карту покриття заданої території лісового господарства сенсорами з урахуванням їх технічних характеристик, де сукупність відповідної кількості сенсорів утворює цільову БСМ;

– задавати фіксовану кількість відмов сенсорів БСМ у межах експерименту, мінімально необхідну кількість суміжних непрацездатних сенсорів для утворення ФКНС, а також загальну кількість ітерацій моделювання;

– генерувати різні комбінації просторового розташування непрацездатних сенсорів БСМ на кожній окремій ітерації;

– підраховувати кількість ітерацій, у яких алгоритмом розпізнавання було згенеровано та підтверджено наявність щонайменше однієї ФКНС заданого розміру.

Для забезпечення гнучкості налаштувань програмного середовища архітектура ПЗ передбачає використання такого набору ключових конфігураційних параметрів:

– X_LEN, Y_LEN – умовні показники розмірності прямокутної фігури, за допомогою яких обчислюється площа фігури, в яку повинен бути вписаний об’єкт моніторингу (територія лісового господарства). Використання умовних одиниць для опису цих показників дозволяє гнучке масштабування моделі.

– MAX_VALUE – загальна кількість сенсорів БСМ, що розгортаються для покриття визначеної території. Це значення програмно корелює з параметрами X_LEN та Y_LEN, оскільки надмірно велика кількість сенсорів може не вміститися в розраховану площу.

– DEFECTS_NUM – кількість сенсорів БСМ із загальної їхньої кількості MAX_VALUE, які переводяться у стан відмови на кожній ітерації моделювання.

– EXP_NUM – кількість ітерацій в одному циклі моделювання, що гарантує достовірність оцінок ймовірності відмови БСМ за вказаним критерієм відмови (наприклад, 100 000 ітерацій).

– SEQUENCE_LENS – масив значень, що визначає послідовність перевірки наявності ФКНС із різною мінімально потрібною кількістю непрацюючих сенсорів. Наприклад, при масиві [2, 3, 4, 5] на кожній ітерації модуль cf_area послідовно перевірятиме наявність кластерів, що складаються з 2, 3, 4 та 5 відмов відповідно.

– REQ_NUM – використовується для генерації відповідної кількості звітів за результатами моделювання.

– DEBUG_MODE – режим виведення поточних значень у консоль або окремий файл. Використовується лише для створення демонстраційних прикладів на різних ітераціях моделювання. Недоцільно використовувати для великої кількості ітерацій.

У процесі використання програмного засобу модуль агрегації результатів генерує JSON файл. Запис результатів експерименту у цьому файлі має такий вигляд: "535: [2,1,0,0]" 6. У цьому записі 535 позначає поточний номер ітерації моделювання, а масив чисел 2, 1, 0, 0 відображає кількість зафіксованих алгоритмом пошуку у ширину ФКНС із мінімально необхідними 2, 3, 4 та 5 непрацездатними сенсорами відповідно.

4.2.2 Особливості застосування програмного засобу для оцінювання надійності бездротової сенсорної мережі з урахуванням фатальних комбінацій множинних відмов сенсорів

Для демонстрації практичних можливостей та верифікації розробленого програмного засобу, архітектуру якого описано у попередньому підрозділі, пропонується розглянути особливості його застосування для розв’язання реальної задачі оцінки надійності БСМ. Метою є оцінювання надійності БСМ, призначеної для моніторингу лісових пожеж на реальному об’єкті моніторингу, з урахуванням ймовірності виникнення фатальних комбінацій непрацездатних сенсорів.

У якості об’єкта дослідження було обрано територію лісового масиву Чугуїв – Старий Салтів у Харківській області. Процес використання програмного засобу для цього сценарію складається з кількох послідовних кроків.

Крок 1. Конфігурація розміщення мережі. На першому етапі за допомогою модуля налаштування здійснюється розрахунок площі лісового господарства. Територія розбивається на регулярну сітку квадратних ділянок, де сторона кожного квадрата дорівнює двом радіусам дії сенсора. Програмний засіб автоматично генерує мапу покриття. Для забезпечення моніторингу обраної ділянки програмний засіб розрахував необхідність розгортання 261 сенсорів.

Крок 2. Налаштування параметрів імітаційного моделювання. Після генерації мапи оператор задає вхідні параметри для розрахункового модуля cf_area (через конфігураційний файл або параметри запуску):

– EXP_NUM=100000 (забезпечення високої статистичної достовірності).

– DEFECTS_NUM – цей параметр задавався ітеративно для серії з 7 циклів експериментів. Послідовно генерувалося 6, 7, 8, 9, 10, 11, 12 відмов сенсорів.

– SEQUENCE_LENS = [2,3,4,5] – масив, що вказує алгоритму пошуку в ширину та необхідність одночасного пошуку в кожній ітерації ФКНС, які складаються з 2, 3, 4 та 5 суміжних непрацездатних сенсорів.

Крок 3. Виконання моделювання та фіксація результатів. На кожній ітерації відбувається симуляція стохастичних відмов DEFECTS_NUM сенсорів і застосовується алгоритм пошуку у ширину. Для кожної ітерації генерується запис у JSON-подібному файлі логування. Наприклад, запис «535: [2,1,0,0]» інформує оператора, що на 535-й ітерації поточної симуляції виявилися два кластери з двох сенсорів, один кластер із трьох сенсорів і жодного більшого кластера. На рисунку 4.9 зображено приклад виводу отриманих результатів симуляції

Крок 4. Агрегація даних та аналіз звітів. Після завершення всіх циклів модуль генерації звітів обробляє масив даних і обчислює ймовірність відмови БСМ Q_{WSN} для кожного сценарію за формулою: відношення кількості ітерацій, де зафіксовано хоча б одну ФКНС заданого розміру N_{fail}, до загальної кількості ітерацій N_{it} = 100 000.

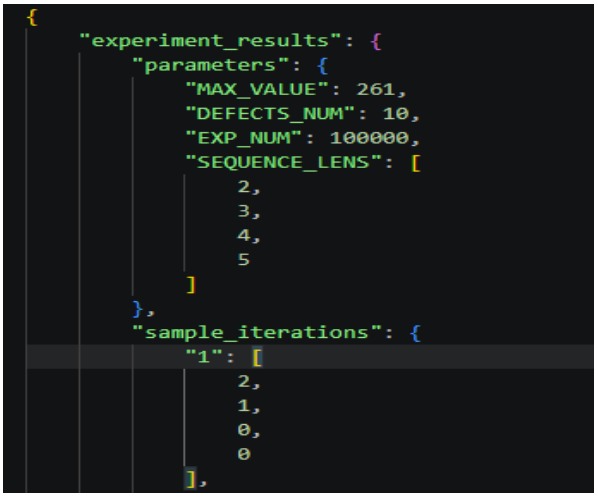

Рисунок 4.9 – Приклад JSON файлу з результатами моделювання

Таким чином, розроблений програмний засіб виступає ефективним інструментом для симуляції утворення та виявлення ФКНС. Він звільняє оператора

від необхідності проведення складних аналітичних розрахунків, автоматизує процес пошуку ФКНС та видає готові статистичні метрики для оцінки надійності спроєктованих БСМ систем моніторингу.

4.3 Програмний засіб для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов

4.3.1 Архітектура програмного засобу для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов

Для комплексного дослідження надійності бездротових сенсорних мереж в умовах стохастичних відмов розроблено спеціалізований програмний засіб «WSNSimulationGUI». На відміну від аналітичних підходів, які стикаються з проблемою складних обчислень при аналізі великих мереж довільної форми, даний інструмент дозволяє фіксувати стохастичну природу відмов сенсорів та периферійного обладнання шляхом множинних ітерацій методом Монте-Карло та подальшої статистичної обробки результатів.

Архітектура розробленого ПЗ побудована за принципом розділення на окремі модульні компоненти. Організацію та взаємодію цих компонентів можна побачити на модульній діаграмі компонентів (рисунок 4.10).

Структурно програмний засіб поділено на три функціональні частини:

1. Графічний інтерфейс користувача (GUI Layer) представлений головним компонентом WSNSimulationGUI. Цей рівень розроблено мовою Python із використанням фреймворку PyQt6. Він забезпечує зручну взаємодію з оператором, прийом параметрів, валідацію вхідних даних та відображення перебігу симуляції під час роботи ПЗ.

2. Модуль для симуляції та розрахунків (Compute Core), який виконує усі функції для імітаційного моделювання: алгоритми генерації мережі, генерація випадкових відмов за експоненційним розподілом часу, а також основний цикл

симуляції, який на кожному кроці згенерованої відмови перевіряє критерії відмови системи, такі як порогові, просторові та периферійні.

3. Система візуалізації та збереження результатів (Storage & Viz). Відповідає за обробку даних після завершення прогонів ітерацій. Завдяки використанню бібліотек NumPy та Pandas модуль розраховує статистичні метрики (ЙБР, стандартне відхилення, довірчі інтервали) та експортує агреговані дані у файли формату Excel. Для візуалізації використовується бібліотека Plotly, яка генерує інтерактивні HTML-графіки. Робота з графами реалізована за допомогою бібліотеки NetworkX.

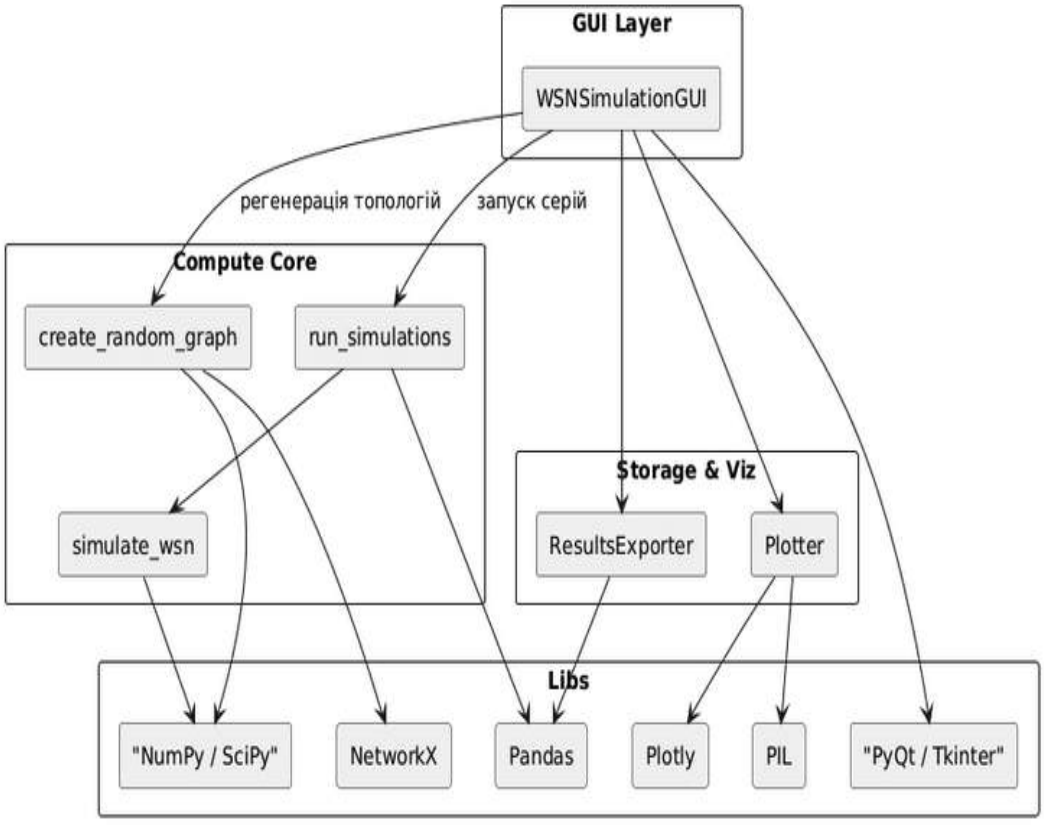

Рисунок 4.10 – Модульна діаграма взаємодії компонентів

Сценарії взаємодії оператора з програмним засобом симуляційного моделювання оцінювання ЙБР БСМ загалом зображені на діаграмі варіантів використання на рисунку 4.11. Вона описує ключові етапи, які ініціює актор-оператор для проведення повного циклу дослідження: від початкового налаштування параметрів моделі до комплексного статистичного аналізу

результатів моделювання. Взаємодія оператора з системою поділяється на три основні етапи:

Етап 1. Конфігурація та введення вхідних даних.

Процес розпочинається із задання системних параметрів експерименту. Оператор через графічний інтерфейс вводить усі необхідні дані

Етап 2. Генерація мережі, запуск та виконання моделювання.

Після налаштування параметрів оператор ініціює генерацію мережі, під час якої програмний засіб будує випадковий геометричний граф розміщення сенсорів у межах заданої ділянки.

Етап 3. Експорт даних та візуальний аналіз результатів.

Завершальним етапом взаємодії є обробка зібраного масиву статистичних даних та аналітична оцінка результатів за допомогою створених візуальних матеріалів.

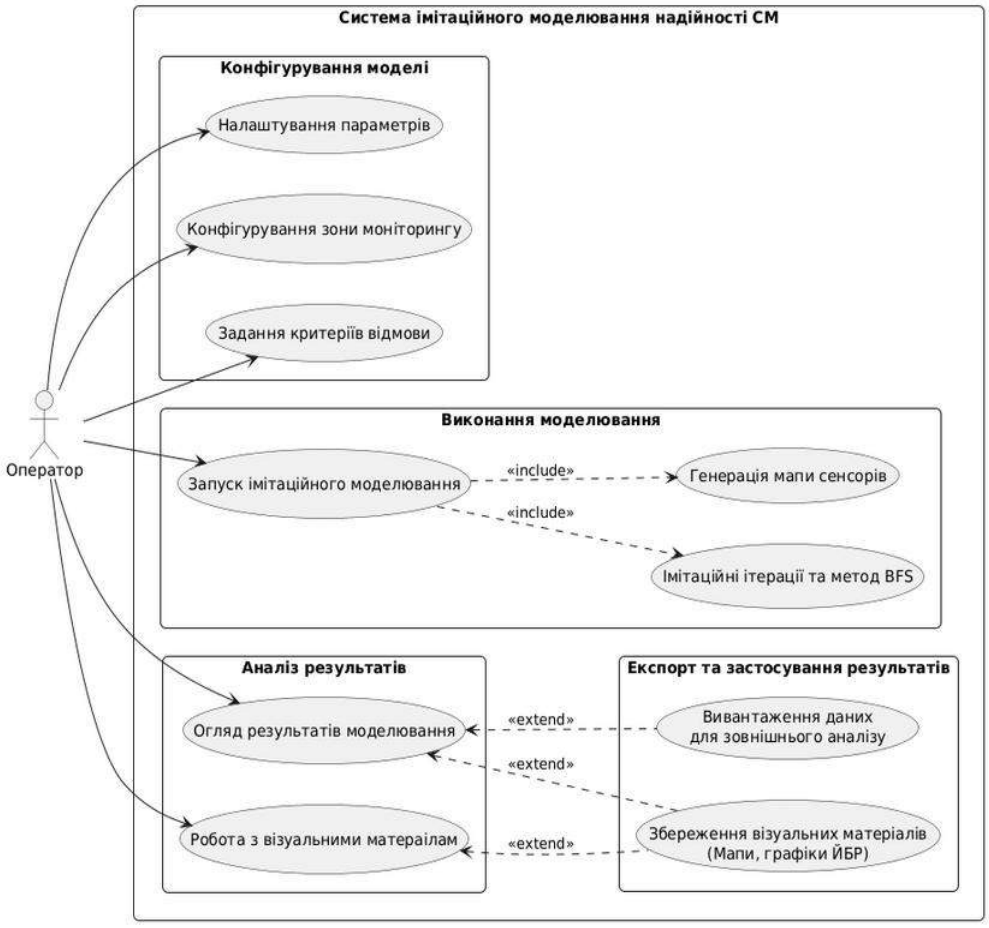

Рисунок 4.11 – Діаграма варіантів використання

Алгоритм роботи імітаційного моделювання з використанням методу Монте-Карло та експоненційного розподілу часу для відмов у сенсорній мережі зображено на рисунку 4.12.

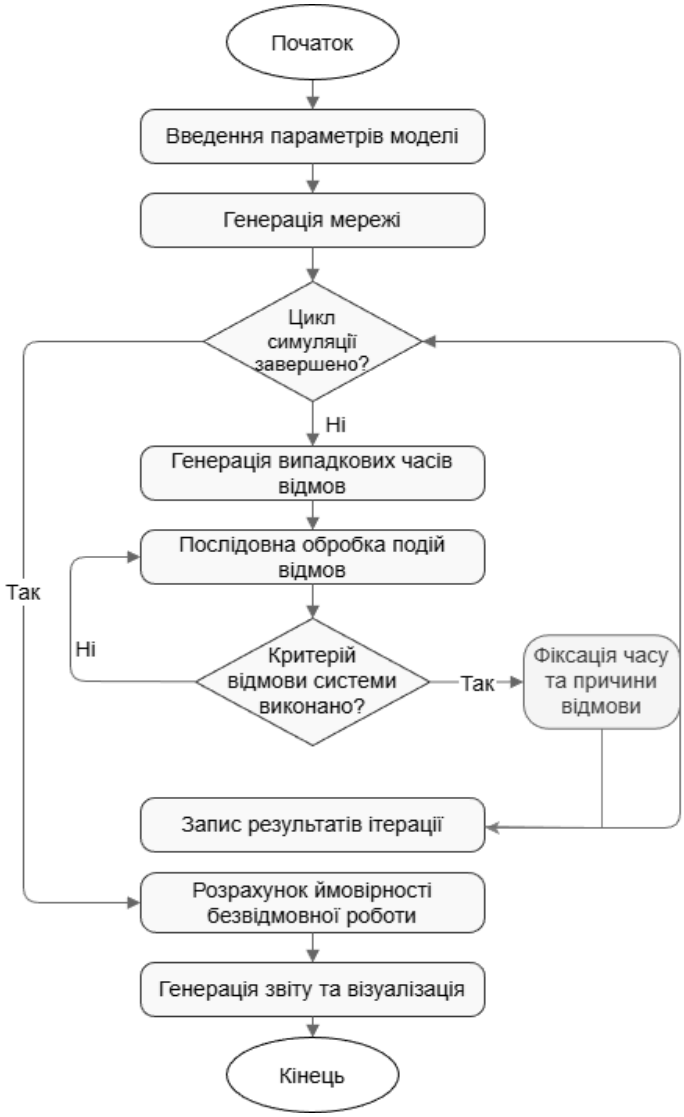

Рисунок 4.12 – Узагальнений алгоритм роботи симуляції ПЗ для стимуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов

Для запуску симуляції оператору потрібно виконати наступні дії: Налаштувати параметри моделювання:

– кількість сенсорів у мережі;

- гранична кількість сенсорів, яка призводить до відмови системи;
- показник для просторового критерія відмови;
- значення для бажаного довірчого інтервалу;
- інтенсивність відмов сенсора;
- інтенсивність відмови периферійного обладнання;
- кількість ітерацій у симуляції;
- часові інтервали, на яких потрібно провести моделювання;
- відповідна мапа для генерації сенсорної мережі.

Після закінчення процесу симуляції оператор, може переглянути отримані результати моделювання, згенеровану мапу сенсорів та графіки ймовірності безвідмовної роботи.

Детальний та покроковий опис роботи алгоритму симуляції, був розглянутий у пункті 3.2.2.

4.3.2 Особливості застосування програмного засобу для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов

Для демонстрації практичних можливостей та алгоритму взаємодії оператора з розробленим програмним засобом, схему якого наведено у попередньому підрозділі, розглянемо повний цикл застосування ПЗ.

Нехай перед оператором стоїть завдання оцінити надійність БСМ для локальної зони потенційно небезпечної території, використовуючи вибірку середнього розміру для пришвидшення розрахунків.

Процес роботи з програмним засобом складається з чотирьох основних етапів.

Етап 1. Ініціалізація та введення параметрів мережі.

Взаємодія оператора із системою розпочинається у головному вікні графічного інтерфейсу, який реалізовано мовою програмування. Приклад такого інтерфейсу з налаштованими параметрами моделювання наведено на рисунку 4.13.

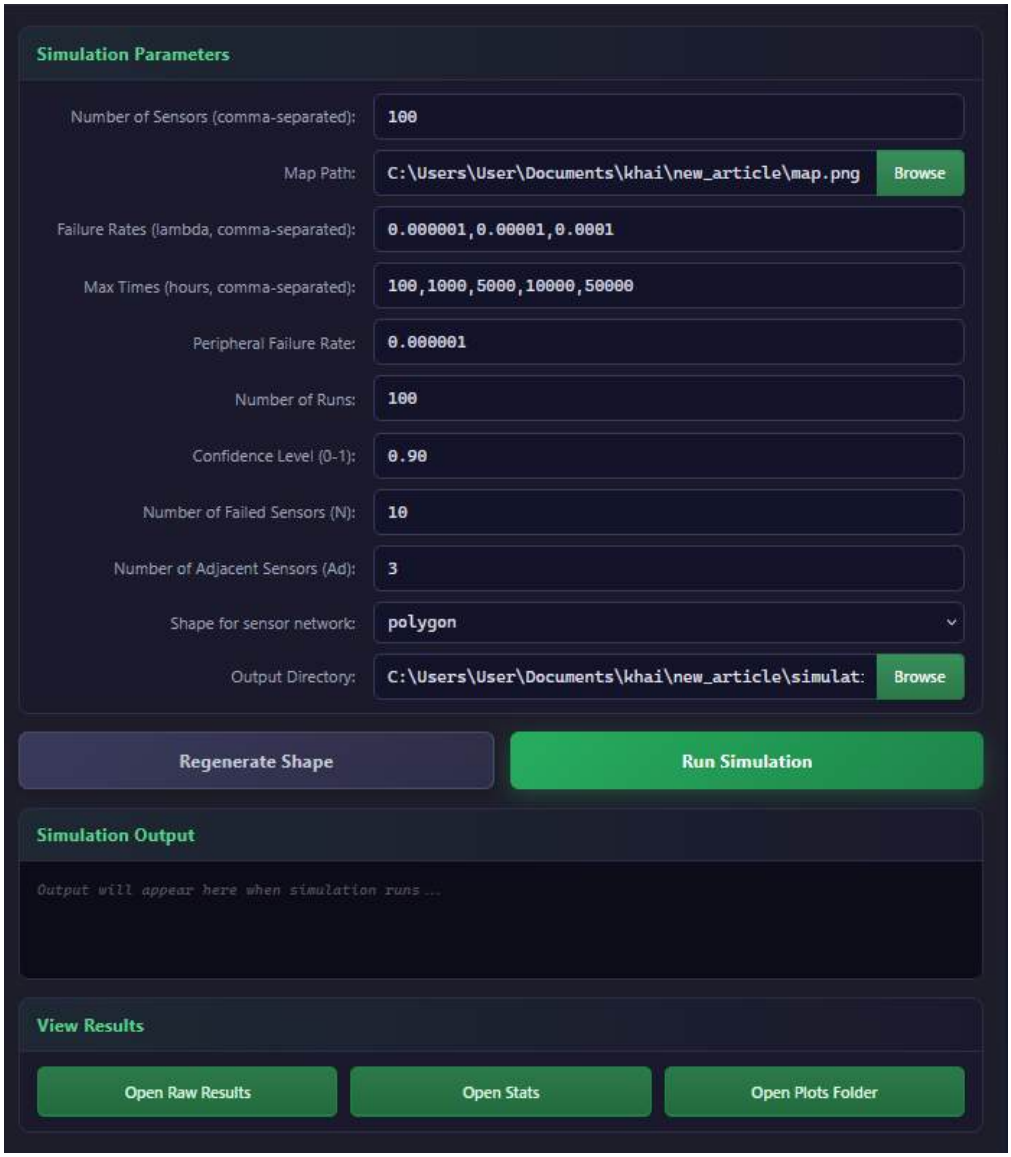

Рисунок 4.13 – Головне вікно програми з налаштованими параметрами

Як видно з рисунка 4.13, інтерфейс користувача складається з кількох логічних блоків:

– Панель введення параметрів: задаються загальна кількість сенсорів, інтенсивності відмов, максимальний час моделювання, порогові та просторові критерії відмов, довірчі інтервали, область розташування сенсорної мережі, а також кількість прогонів для забезпечення статистичної достовірності.

– Елементи керування: представлені кнопками для генерації сенсорної мережі на мапі («Regenerate Shape») та запуску серій симуляцій за встановленою кількістю ітерацій («Run Simulation»).

– Вікно виводу повідомлень (Simulation output): відображає логування подій та виведення результатів.

– Блок доступу до результатів: містить кнопки доступу до Excel-таблиць із даними (Open Raw Results) та статистикою (Open Stats), а також згенеровані інтерактивних HTML-графіків (Open Plots Folder).

Для обраного сценарію оператор вводить нові параметри моделювання: загальна кількість сенсорів $N = 400$, базові інтенсивності відмов $\lambda 1 = 10^{-5}$, $\lambda 2 = 10^{-6}$, $\lambda 3 = 10^{-4}$ максимальний час моделювання $T_{max}= 100000$ годин, кількість прогонів Runs = 100000. $N_{fail} = 40$ − кількість сенсорів які призводять до відмови, Ad=8 – кількість суміжних сенсорів для утворення ФКНС та $\lambda_{pereph} = 10^{-6}$ – інтенсивність відмови периферійного обладнання. Обирається мапа розміщення сенсорної мережі (Map path) та тип фігури в якій вона повинна бути розміщена (Shape of sensor network).

Етап 2. Генерація сенсорної мережі на заданій ділянці. Перед запуском обчислень оператор натискає кнопку «Regenerate Shape». Обчислювальне ядро розміщує 400 сенсорів у заданих межах фігур та відповідно фіксує кількість сенсорів, до яких кожен окремий сенсор є дотичним, не більше 4 зв’язків на 1 сенсор. Після створення мапи її можна переглянути у відповідній директорії за допомогою кнопки «Open Plots Folder», яка відкриває місце зберігання всіх візуальних матеріалів.

Приклад згенерованої сенсорної мережі, розміщеної у прямокутну фігуру на 400 сенсорів, наведено на рисунку 4.14.

Етап 3. Запуск симуляції та моніторинг процесу.

Оператор натискає кнопку «Run Simulation». Програмний засіб послідовно виконує 100000 незалежних прогонів. У вбудованому вікні відображається загальний статус обчислень. Приклад виводу результатів у консольне вікно можна побачити на рисунку 4.15, де зображена загальна кількість успішних ітерацій та кількість відмов за визначеними критеріями.

Рисунок 4.14 – Згенерована карта сенсорів для області при N=400

Max Time Reached	N=10 Sensors Failed	Peripheral Failure	Spatial Failure (BFS, Ad=3)
69654	78489	530	1327

Рисунок 4.15 – Статус обчислень

Етап 4. Автоматизована агрегація даних та аналіз отриманих результатів. Після появи повідомлення про успішне завершення оператор використовує кнопки швидкого доступу «Open Results» та «Open Plots Folder». Підсистема збереження та візуалізації автоматично генерує два типи вихідних даних:

1. Табличні звіти у форматі Excel: файл містить інформацію про кількість відмов різного типу на різних ділянках часу та вкладку зі зведеною статистикою

розрахунку ймовірності безвідмовної роботи. Згенерований файл результатів зображено на рисунку 4.16.

num_sensors	lambda	max_time	reliability_mean	reliability_std	reliability_ci_lower	reliability_ci_upper
400	0,00001	100	0,99983	0,013037362	0,999749194	0,999910806
400	0,00001	1000	0,99903	0,03112987	0,998837056	0,999222944
400	0,00001	5000	0,97738	0,148689464	0,976458419	0,978301581
400	0,00001	10000	0,06716	0,250300142	0,065608633	0,068711367

Рисунок 4.16 – Приклад згенерованих загальних результатів

2. Інтерактивні HTML-графіки: програмний засіб будує графіки ймовірності безвідмовної роботи для різних інтенсивностей відмов та мапи, які можна аналізувати у веб-браузері. На інтерактивних графіках можна побачити зміну ЙБР у часі для визначеної інтенсивності відмов та проаналізувати довірчі інтервали, які зображені спеціальним напівпрозорим виділенням навколо основної лінії графіка. Приклад виводу графіка, згенерованого засобом, зображено на рисунку 4.17.

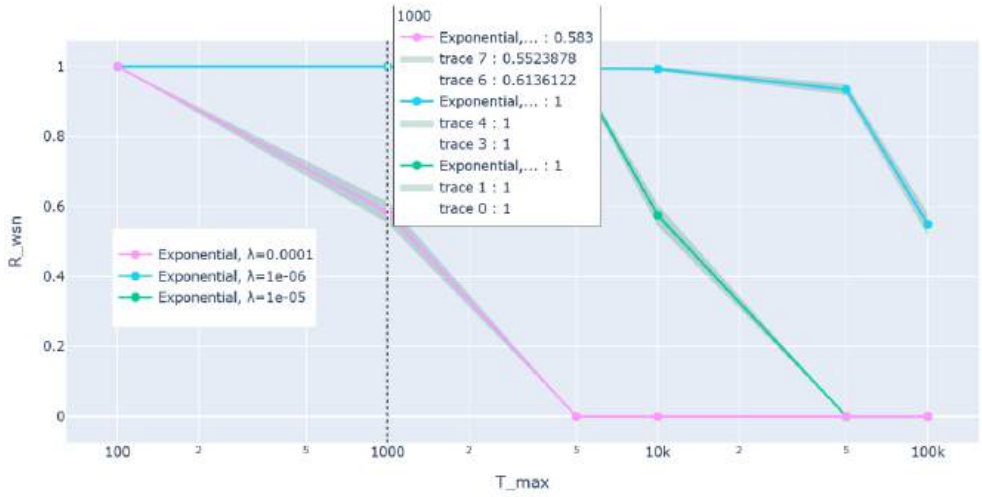

Рисунок 4.17 – Інтерактивні графіки розподілу ймовірності безвідмовної роботи для N=400 з демонстрацією довірчого інтервалу

Для отримання більшої статистичної достовірності результатів симуляції, рекомендується використовувати кількість ітерацій від 10000. Задана кількість ітерацій у 100000 гарантує достатню статистичну достовірність результатів для

розрахунку ймовірності безвідмовної роботи. На рисунках 4.18 та 4.19 видно різницю діапазону довірчого інтервалу для 100 та для 100000.

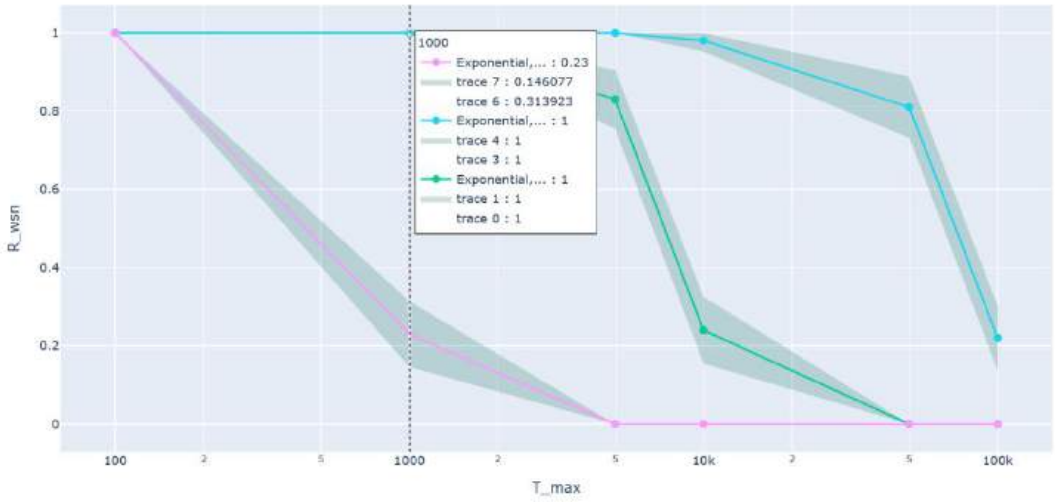

Рисунок 4.18 – Приклад результатів запуску симуляції на 100 ітерацій

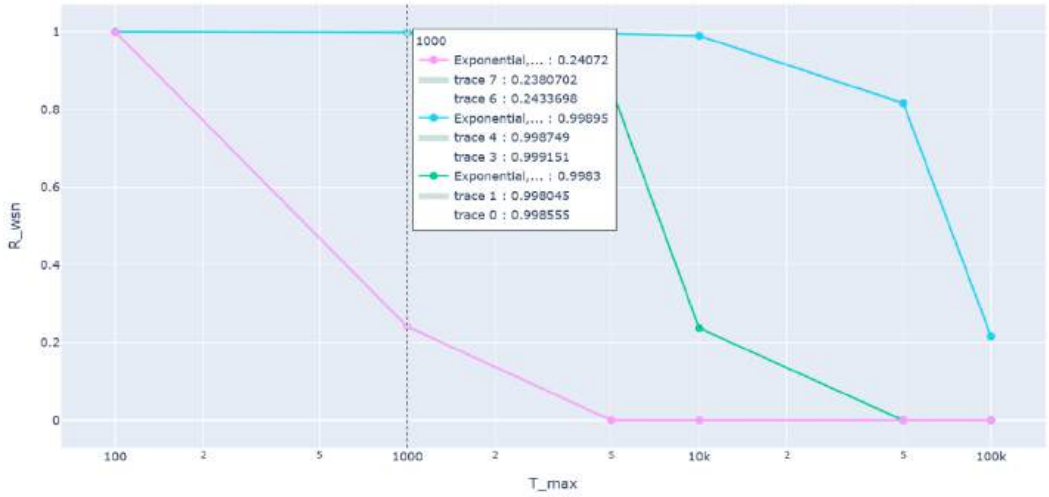

Рисунок 4.19 – Приклад результатів запуску симуляції на 100000 ітерацій

Розроблений програмний засіб дозволяє зручним способом проводити імітаційне моделювання надійності сенсорних мереж. Засіб усуває необхідність ручного написання скриптів для розрахунку відмов, автоматизує формування звітів, візуалізує розміщення сенсорних мереж в межах заданої ділянки моніторингу. Оператор отримує готовий інструмент для моделювання сценаріїв поведінки сенсорної мережі за різних критеріїв відмови, таких як гранична кількість сенсорів, фатальна комбінація несправних сенсорів, або периферійне

обладнання. Це надає можливість на етапі розроблення системи моніторингу спрогнозувати потрібну кількість компонентів мережі та їхню інтенсивність відмов для підвищення надійності сенсорної мережі системи моніторингу.

4.4 Висновки за розділом

У розділі розроблено спеціалізовані програмні засоби для оцінювання надійності гібридних і бездротових сенсорних мереж систем моніторингу потенційно небезпечних територій, які забезпечують практичну реалізацію запропонованих у дисертації аналітичних і імітаційних моделей.

Розроблено архітектуру програмного засобу для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі, що поєднує графічний інтерфейс користувача, модуль аналітичних розрахунків і модуль візуалізації результатів.

Створений програмний засіб для гібридної сенсорної мережі забезпечує автоматизоване обчислення ймовірності безвідмовної роботи, побудову структурних схем надійності та визначення ймовірностей перебування системи у частково працездатних станах для заданої конфігурації компонентів.

Практичним застосуванням розробленого програмного засобу для гібридної сенсорної мережі підтверджено можливість оперативного оцінювання впливу складу флотів БПЛА, параметрів резервування та інтенсивностей відмов компонентів на інтегральні показники надійності системи моніторингу.

Розроблено програмний засіб для оцінювання надійності бездротової сенсорної мережі з урахуванням фатальних комбінацій множинних відмов сенсорів, який забезпечує автоматизовану генерацію конфігурацій мережі, виявлення просторових кластерів відмов та статистичне оцінювання ймовірності відмови мережі.

Розроблено програмний засіб «WSNSimulationGUI» для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов, використання якого довело практичну цінність створеного інструментарію для інженерної підтримки проєктування систем моніторингу потенційно небезпечних територій.

ВИСНОВКИ

1. У дисертації розроблено моделі та програмні засоби оцінювання надійності сенсорних мереж систем моніторингу потенційно небезпечних територій.

2. Вперше запропоновано структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень, які, на відміну від відомих, ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, що дозволяє планувати розподіл ресурсів і забезпечити надійне функціонування системи в умовах деградації мережі.

3. Удосконалено аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території, їхні показники безвідмовності та фатальні комбінації множинних відмов сенсорів за різними критеріями, що дозволяє розраховувати та прогнозувати показники надійності мереж.

4. Отримали подальшого розвитку марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання, що дозволяє розраховувати функції готовності мереж для різних стратегій їх технічного обслуговування.

5. Практичне значення отриманих результатів полягають у доведенні теоретичних положень дисертаційної роботи до конкретних алгоритмів та програмних засобів для планування та розгортання заходів для підвищення надійності сенсорних мереж. Зокрема було розроблено:

– програмний засіб для оцінювання надійності системи моніторингу на основі гібридної сенсорної мережі, який забезпечує автоматизацію розрахунків

аналітичних моделей надійності та візуалізацію станів деградації систем із багаторівневою працездатністю для підтримки рішень інженерів та операторів;

– програмний засіб для оцінювання надійності бездротової сенсорної мережі з урахуванням ФКНС, який дозволяє проводити масові статистичні експерименти (до 100 000 ітерацій) для виявлення просторових відмов та оцінювання надійності мереж складної топології;

– програмний засіб для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов, який призначений для інтерактивного дослідження впливу різних геометричних конфігурацій ділянок (прямокутних, еліптичних, багатокутних) на загальні показники надійності, дозволяючи обрати раціональний варіант розміщення сенсорів.

Результати дисертаційної роботи впроваджено:

– в Українському ордена «Знак пошани» науково-дослідному інституті лісового господарства та агролісомеліорації ім. Г. М. Висоцького Державного агентства лісових ресурсів України та Національної академії наук України. (акт впровадження від 02 квітня 2026).;

– у навчальному процесі Національного аерокосмічного університету «Харківський авіаційний інститут» (акт впровадження від 10 березня 2026);

– при виконанні науково-дослідних проєктів, що виконувалися у Національному аерокосмічному університеті «Харківський авіаційний інститут» (акт впровадження від 09 березня 2026).

7. Подальші дослідження можуть бути спрямовані на:

– розроблення моделей оцінювання надійності, які враховують стохастичний характер накопичення енергії вузлами з відновлюваних джерел та його вплив на інтенсивність відмов і час безперервної роботи сенсорної мережі;

– створення аналітичних методів оцінювання надійності систем, здатних до інтелектуальної зміни топології (наприклад, за допомогою БПЛА) для компенсації відмов наземних компонентів та мінімізації ризику появи критичних сценаріїв втрати покриття.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Скоробогатько С. В., Фесенко Г. В. Перспективи використання літаючих хмарних, граничних та туманних обчислень компонентами системи моніторингу потенційно небезпечних об'єктів. *Системи управління, навігації та зв'язку*. 2022. Вип. 4 (70). С. 145–152. DOI: 10.26906/SUNZ.2022.4.

2. Fesenko H., Illiashenko O., Kharchenko V., Kliushnikov I., Morozova O., Sachenko A., Skorobohatko S. Flying Sensor and Edge Network-Based Advanced Air Mobility Systems: Reliability Analysis and Applications for Urban Monitoring. *Drones*. 2023. Vol. 7, no. 7, article no. 409. P. 1–27. DOI: 10.3390/drones7070409.

3. Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Edge-based Sensors Network for Critical Object Monitoring: Reliability Models Considering the Location of Failed Sensors. *Dependable Systems, Services and Technologies (DESSERT'2023)*: Proc. 13th IEEE Int. Conf., Athens, Greece, Oct. 13–15, 2023. P. 1–7. DOI: 10.1109/DESSERT61349.2023.10416471.

4. Leichenko K., Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Reliability of Sensor Network-Based Systems for Arbitrary Shape Plot Monitoring Considering Multiple Failures. *Dependable Systems, Services and Technologies (DESSERT'2024)*: Proc. 14th IEEE Int. Conf., Athens, Greece, Oct. 11–13, 2024. DOI: 10.1109/DESSERT65323.2024.11122204.

5. Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Architecture and Reliability Models of Hybrid Sensor Networks for Environmental and Emergency Monitoring Systems. *Cybernetics and Systems Analysis*. 2024. Vol. 60, no. 2. P. 293–304. DOI: 10.1007/s10559-024-00670-x

6. Skorobohatko S., Fesenko H., Kharchenko V., Volochiy B. Availability Models of a Recoverable Wireless Sensor Network for Forest Fire Monitoring System. *Reliability Engineering and Computational Intelligence (RECI'2024)*: Proc. 3rd Int. Workshop, Žilina, Slovakia, Nov. 6–8, 2024. P. 13.

7. Leichenko K., Skorobohatko S., Fesenko H., Kharchenko V., Yakovlev S. Assessment of the Reliability of Wireless Sensor Networks for Forest Fire Monitoring

Systems Considering Fatal Combinations of Multiple Sensor Failures. *Cybernetics and Systems Analysis*. 2025. Vol. 61, no. 1. P. 137–147. DOI: 10.1007/s10559-025-00753-3

8. Скоробогатько С., Фесенко Г., Харченко В. Послідовність і програмний засіб для симуляційного оцінювання ймовірності безвідмовної роботи бездротових сенсорних мереж за різних сценаріїв відмов. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. Вип. 4 (84). С 68–80 DOI: 10.31891/2219-9365-2025-84-8.

9. Kassan R., Châtelet E., Soukieh J. Reliability assessment of photovoltaic wireless sensor networks for forest fire propagation detection. *International Journal of Modelling and Simulation*. 2018. Vol. 38, no. 1. P. 50–65. DOI: 10.1080/02286203.2017.1393857.

10. Krishnamoorthy M., Asif M., Kumar P. P., Nuvvula R. S. S., Khan B., Colak I. A design and development of the smart forest alert monitoring system using IoT. *Journal of Sensors*. 2023. Vol. 2023, article no. 8063524. P. 1–12. DOI: 10.1155/2023/8063524.

11. Vikram R., Sinha D., De D., Das A. K. EEFFL: Energy efficient data forwarding for forest fire detection using localization technique in wireless sensor network. *Wireless Networks*. 2020. Vol. 26. P. 5765–5779. DOI: 10.1007/s11276-020-02393-1.

12. Motlagh N. H., Irjala M., Zuniga A., Lagerspetz E., Nurmi P., Flores H., Tarkoma S. Unmanned Aerial Vehicles for Air Pollution Monitoring: A Survey. *IEEE Internet of Things Journal*. 2023. Vol. 10, no. 24. P. 21687–21704. DOI: 10.1109/JIOT.2023.3290508.

13. Woodbridge E., Connor D. T., Verbelen Y., Hine D., Richardson T., Scott T. B. Airborne gamma-ray mapping using fixed-wing vertical take-off and landing (VTOL) uncrewed aerial vehicles. *Frontiers in Robotics and AI*. 2023. Vol. 10, article no. 1137763. DOI: 10.3389/frobt.2023.1137763.

14. Connor D., Martin P. G., Scott T. B. Airborne radiation mapping: Overview and application of current and future aerial systems. *International Journal of Remote Sensing.* 2016. Vol. 37, no. 24. P. 5953–5987. DOI: 10.1080/01431161.2016.1252474.

15. Zaidi S., Atiquzzaman M., Calafate T. Internet of flying things (IoFT): A survey. *Computer Communications*. 2020. Vol. 165. P. 53–74. DOI: 10.1016/j.comcom.2020.10.023.

16. Li J., Xiong X., Yan Y., Yang Y. A Survey of Indoor UAV Obstacle Avoidance Research. *IEEE Access*. 2023. Vol. 11. P. 51861–51891. DOI: 10.1109/ACCESS.2023.3262668.

17. Unlu H. U., Chaikalis D., Tsoukalas A., Tzes A. UAV Indoor Exploration for Fire-Target Detection and Extinguishing. *Journal of Intelligent & Robotic Systems*. 2023. Vol. 107, article no. 25. DOI: 10.1007/s10846-023-01835-0.

18. Xia X., Fattah S., Ali Babar M. A Survey on UAV-Enabled Edge Computing: Resource Management Perspective. *ACM Computing Surveys*. 2024. Vol. 56, no. 3, article no. 78. P. 1–36. DOI: 10.1145/3626566.

19. Kampf R., Soviar J., Bartuška L., Kubina M. Creation of SW for Controlling Unmanned Aerial Systems. *LOGI – Scientific Journal on Transport and Logistics*. 2022. Vol. 13, no. 1. P. 198–209. DOI: 10.2478/logi-2022-0018.

20. Moussa N., Khemiri-Kallel S., El Belrhiti El Alaoui A. Fog-assisted hierarchical data routing strategy for IoT-enabled WSN: Forest fire detection. *Peer-to-Peer Networking and Applications*. 2022. Vol. 15. P. 2307–2325. DOI: 10.1007/s12083-022-01347-y.

21. Devraj, Ram R., Das S. Fog Computing Environment in Flying Ad-hoc Network. *Cloud Computing Enabled Big-Data Analytics in Wireless Ad-hoc Networks*. 2022. P. 31–48. DOI: 10.1201/9781003206453-3.

22. Uddin M. A., Ayaz M., Mansour A., Aggoune el H. M., Sharif Z., Razzak I. Cloud-connected flying edge computing for smart agriculture. *Peer-to-Peer Networking and Applications*. 2021. Vol. 14. P. 3431–3443. DOI: 10.1007/s12083-021-01191-6.

23. Yazid Y., Ez-Zazi I., Guerrero-González A., El Oualkadi A., Arioua M. UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review. *Drones*. 2021. Vol. 5, no. 4, article no. 148. DOI: 10.3390/drones5040148.

24. Iwaszenko S., Kalisz P., Słota M., Rudzki A. Detection of Natural Gas Leakages Using a Laser-Based Methane Sensor and UAV. *Remote Sensing*. 2021. Vol. 13, no. 3, article no. 510. DOI: 10.3390/rs13030510.

25. Yang H. A practical method for connectivity and coverage reliability analysis for linear wireless sensor networks. *Ad Hoc Networks*. 2023. Vol. 146, article no. 103183. DOI: 10.1016/j.adhoc.2023.103183.

26. Ayanoglu M. B., Uysal I. ML Approach to Improve the Costs and Reliability of a Wireless Sensor Network. *Sensors*. 2023. Vol. 23, no. 9, article no. 4303. P. 1–16. DOI: 10.3390/s23094303.

27. Xing L. Reliability Modeling of Wireless Sensor Networks: A Review. *Recent Patents on Engineering*. 2021. Vol. 15, no. 1. P. 3–11. DOI: 10.2174/1872212113666191209091947.

28. Wenzhuo. L., Tang R., Wang W., Zheng Z. An optimal design method for communication topology of wireless sensor networks to implement fully distributed optimal control in IoT-enabled smart buildings. *Applied Energy*. 2023. Vol. 349, article no. 121539. DOI: 10.1016/j.apenergy.2023.121539.

29. Deif D., Gadallah Y. A comprehensive wireless sensor network reliability metric for critical Internet of Things applications. *EURASIP Journal on Wireless Communications and Networking*. 2017. Vol. 2017, article no. 145. P. 1–18. DOI: 10.1186/s13638-017-0930-3.

30. Heidari A., Amiri Z., Jamali M. A. J., Jafari N. Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults. *Concurrency and Computation: Practice and Experience*. 2024. Vol. 36, no. 27, article no. e8252. P. 1–21. DOI: 10.1002/cpe.8252.

31. Nguyen H. A. D., Ha Q. P. Wireless sensor network dependable monitoring for urban air quality. *IEEE Access*. 2022. Vol. 10. P. 40051–40062. DOI: 10.1109/ACCESS.2022.3166904.

32. Adday G. H., Subramaniam S. K., Zukarnain Z. A., Samian N. Fault tolerance structures in wireless sensor networks (WSNs): Survey, classification, and

future directions. *Sensors*. 2022. Vol. 22, no. 16, article no. 6041. P. 1–39. DOI: 10.3390/s22166041.

33. Chakraborty S., Goyal N. K., Mahapatra S., Soh S. Minimal path-based reliability model for wireless sensor networks with multistate nodes. *IEEE Transactions on Reliability*. 2020. Vol. 69, no. 1. P. 382–400. DOI: 10.1109/TR.2019.2954894.

34. Kabashkin I. Reliability of cluster-based nodes in wireless sensor networks of cyber-physical systems. *Procedia Computer Science*. 2019. Vol. 151. P. 313–320. DOI: 10.1016/j.procs.2019.04.044.

35. Munir A., Gordon-Ross A. Markov Modeling of Fault-Tolerant Wireless Sensor Networks. *IEEE International Conference on Computer Communications and Networks (ICCCN'2011)* : Proc. 20th IEEE Int. Conf., Maui, HI, USA, Jul. 31 – Aug. 4, 2011. P. 1–6. DOI: 10.1109/ICCCN.2011.6005768.

36. Yue Y. G., He P. A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions. *Information Fusion*. 2018. Vol. 44. P. 188–204. DOI: 10.1016/j.inffus.2018.03.005.

37. Zonouz A. E., Xing L., Vokkarane V. M., Sun Y. Hybrid wireless sensor networks: A reliability, cost and energy-aware approach. *IET Wireless Sensor Systems*. 2016. Vol. 6, no. 2. P. 42–48. DOI: 10.1049/iet-wss.2014.0131.

38. Yang J., Chen J., Huo Y., Liu Y. A Novel Cluster-Based Wireless Sensor Network Reliability Model. *Journal of Sensors*. 2021. Vol. 2021. Article 8869544. P. 1–13. DOI: 10.1155/2021/8869544.

39. Shakhov V., Migov D., Chen H., Mishchenko P., Koo I. Toward Reliability of Long Wireless Sensor Networks. *IEEE Access*. 2024. Vol. 12. P. 124506–124516. DOI: 10.1109/ACCESS.2024.3454367.

40. Zhu X., Lu Y., Han J., Shi L. Transmission Reliability Evaluation for Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2016. Vol. 12, no. 2. DOI: 10.1155/2016/1346079.

41. Wang N., Tian T., He J., Zhang C., Yang J. Transmission reliability evaluation of wireless sensor networks considering channel capacity randomness and

energy consumption failure. *Reliability Engineering & System Safety*. 2024. Vol. 242, article no. 109769. DOI: 10.1016/j.ress.2023.109769.

42. Ojeda Ruiz F., Mendez D., Fajardo A., Becker M., Ellinger F. A Cross-Layer Approach to Analyzing Energy Consumption and Lifetime of a Wireless Sensor Node. *Journal of Sensor and Actuator Networks*. 2024. Vol. 13, no. 5, article no. 56. P. 1–13. DOI: 10.3390/jsan13050056.

43. Priyadarshi R., Kumar R., Ranjan R., Kumar P. AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks. *Scientific Reports*. 2025. Vol. 15, article no. 3127. P. 1–19. DOI: 10.1038/s41598-025-08677-w.

44. Chowdhury C., Aslam N., Ahmed G., Chattapadhyay S., Neogy S., Zhang L. Novel algorithms for reliability evaluation of remotely deployed wireless sensor networks. *Wireless Personal Communications*. 2018. Vol. 98. P. 1331–1360. DOI: 10.1007/s11277-017-4921-9.

45. Catelani M., Ciani L., Bartolini A., Del Rio C., Guidi G., Patrizi G. Reliability analysis of wireless sensor network for smart farming applications. *Sensors*. 2021. Vol. 21, no. 22, article no. 7683. P 1-16. DOI: 10.3390/s21227683.

46. Mishra P., Dash R. K. A novel method for evaluation of reliability of WSN under different failure models. *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*. 2020. P. 1–6. DOI: 10.1007/s11277-019-06848-3.

47. Arjannikov T., Diemert S., Ganti S., Lampman C. Using Markov chains to model sensor network reliability. *Availability, Reliability and Security (ARES'2017)* : Proc. 12th Int. Conf., Reggio Calabria, Italy, Aug. 29 – Sept. 1, 2017. P. 1–10. DOI: 10.1145/3098954.3098979.

48. Kolisnyk M., Kochkar D., Kharchenko V. Markov model of wireless sensor network availability. *International Journal of Computing*. 2020. Vol. 19, no. 3. P. 491–498. DOI: 10.47839/ijc.19.3.1899.

49. Dogmechi S., Torabi Z., Daneshpour N. An outlier detection method based on the hidden Markov model and copula for wireless sensor networks. *Wireless Networks*. 2024. Vol. 30. P. 4797–4810. DOI: 10.1007/s11276-022-03131-5.

50. Yakovlev S., Kartashov O., Podzeha D. Mathematical models and nonlinear optimization in continuous maximum coverage location problem. *Computation*. 2022. Vol. 10, no. 7, article no. 119. P. 1–15. DOI: 10.3390/computation10070119.

51. Yakovlev S. V. The concept of modeling packing and covering problems using modern computational geometry software. *Cybernetics and Systems Analysis*. 2023. Vol. 59. P. 108–119. DOI: 10.1007/s10559-023-00547-5.

52. Azevedo B. F., Brito T., Lima J. L., Pereira A. I. Optimum sensors allocation for a forest fires monitoring system. *Forests*. 2021. Vol. 21, no. 4, article no. 453. P. 1–13. DOI: 10.3390/f12040453.

53. Yang S. Y., Chen C. F., Zhou K. Q., Ou Y. Coverage optimization of wireless sensor network utilizing an improved CS with multi-strategies. *Scientific Reports*. 2025. Vol. 15, article no. 29668. P. 1–31. DOI: 10.1038/s41598-025-13247-1.

54. Acharya S., Tripathy C. R. A reliable fault-tolerant ANFIS model based data aggregation scheme for wireless sensor networks. *Journal of King Saud University – Computer and Information Sciences*. 2020. Vol. 32, no. 6. P. 741–753. DOI: 10.1016/j.jksuci.2017.11.001.

55. Khalilpour Akram V., Akusta Dagdeviren Z., Dagdeviren O., Challenger M. PINC: pickup non-critical node based k-connectivity restoration in wireless sensor networks. *Sensors*. 2021. Vol. 21, no. 19, article no. 6418. P. 1–16. DOI: 10.3390/s21196418.

56. Zaitseva E., Levashenko V., Mukhamediev R., Brinzei N., Kovalenko A., Symagulov A. Review of Reliability Assessment Methods of Drone Swarm (Fleet) and a New Importance Evaluation Based Method of Drone Swarm Structure Analysis. *Mathematics*. 2023. Vol. 11, no. 11, article no. 2551. P. 1–16. DOI: 10.3390/math11112551.

57. Zaitseva E., Levashenko V., Brinzei N., Kovalenko A., Yelis M., Gopejenko V., Mukhamediev R. Reliability Assessment of UAV Fleets. *Lecture Notes in Electrical Engineering*. 2023. Vol. 965. P. 335–357. DOI: 10.1007/978-3-031-24963-1_19.

58. Qi X., Zhou Y., Liu L. Evaluation of the reliability of UAV swarm for ground combat missions. *Systems Engineering and Electronics*. 2023. Vol. 45, no. 9. P. 2971–2978. DOI: 10.12305/j.issn.1001-506X.2023.09.38.

59. Sun Y., Fesenko H., Kharchenko V., Zhong L., Kliushnikov I., Illiashenko O., Morozova O., Sachenko A. UAV and IoT-Based Systems for the Monitoring of Industrial Facilities Using Digital Twins: Methodology, Reliability Models, and Application. *Sensors*. 2022. Vol. 22, no. 17, article no. 6444. P. 1–31. DOI: 10.3390/s22176444.

60. Varga A., Hornig R. An overview of the OMNeT++ simulation environment. *Simulation Tools and Techniques for Communications, Networks and Systems* : Proc. 1st Int. Conf., Marseille, France, Mar 3–7, 2008. P. 1–10. DOI: 10.4108/ICST.SIMUTOOLS2008.3027.

61. Zárate Ceballos H., Parra Amaris J. E., Jiménez Jiménez H., Romero Rincón D. A., Agudelo Rojas O., Ortiz Triviño J. E. Wireless Network Simulation: A Guide using Ad Hoc Networks and the ns-3 Simulator. New York : Springer, 2021. 219 p. DOI: 10.1007/978-1-4842-6849-0.

62. Ferreira A. M. A., Azevedo L. J. M., Estrella J. C., Delbem A. C. B. Case Studies with the Contiki-NG Simulator to Design Strategies for Sensors' Communication Optimization in an IoT-Fog Ecosystem. *Sensors*. 2023. Vol. 23, no. 4, article no. 2300. . P. 1–18. DOI: 10.3390/s23042300.

63. Ilić D., Marinković D. One Classification and Evaluation Methodology for the WSN Simulators. *Electrical, Electronic and Computing Engineering (IcETRAN'2024)* : Proc. 11th Int. Conf., Niš, Serbia, Jun. 3–6, 2024. P. 1–6. DOI: 10.1109/IcETRAN62308.2024.10645173.

64. Alenezi A., Alhudhaif A., Alnaim N. Advancements and Challenges in IoT Simulators: A Comprehensive Review. *Sensors*. 2024. Vol. 24, no. 5, article no. 1511. P. 1–35. DOI: 10.3390/s24051511.

65. Бобало Ю. Я., Волочій Б. Ю., Лозинський О. Ю., Мандзій Б. А., Озірковський Л. Д., Федасюк Д. В., Щербовських С. В., Яковина В. С. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем: кол. Монографія / Міністерство освіти і науки України, Національний університет "Львівська політехніка". Львів : Видавництво Львівської політехніки, 2013. С 69 –123 .

66. ReliaSoft Corporation. BlockSim System Reliability and Maintainability Analysis Software. URL: https://www.reliasoft.com/products/reliability-analysis/blocksim (date of access: 10.12.2025).

67. Isograph Ltd. Reliability Workbench Software Suite. URL: https://www.isograph.com/software/reliability-workbench/ (date of access: 10.12.2025).

68. Phadke A., Medrano F. A., Sekharan C. N., Chu T. Designing UAV Swarm Experiments: A Simulator Selection and Experiment Design Process. *Sensors*. 2023. Vol. 23, no. 17, article no. 7359. P. 1–26 DOI: 10.3390/s23177359.

69. Al-Mousa A., Sababha B. H., Al-Madi N., Barghouthi A., Younisse R. UTSim: A framework and simulator for UAV air traffic integration, control, and communication. International Journal of Advanced Robotic Systems. 2019. Vol. 16, no. 5. P. 1–12. DOI: 10.1177/1729881419870937.

70. Xie C., Li Y., Zhang T., Zhang C. FANET-Sim: A Simulation Framework for UAV Swarm Communication. *Computer Network Security and Software Engineering (CNSSE'2025)*: Proc. 5th Int. Conf., Qingdao, China, Feb. 21–23, 2025. P. 183–189. DOI: 10.1145/3732365.3732396.

71. Chehida S., Baouya A., Bensalem S., Bozga M. Learning and analysis of sensors behavior in IoT systems using statistical model checking. *Software Quality Journal*. 2022. Vol. 30. P. 367–388. DOI: 10.1007/s11219-021-09559-w.

72. Abdulhamid A., Kabir S., Ghafir I., Lei C. An Overview of Safety and Security Analysis Frameworks for the Internet of Things. *Electronics*. 2023. Vol. 12, no. 14, article no 3086. P. 1–25. DOI: 10.3390/electronics12143086.

73. Thiam F., Mbaye M., Flores M., Wyglinski A. Reliability Evaluation Framework for Centralized Agricultural Internet of Things (Agri-IoT). *International*

Journal of Advanced Computer Science and Applications. 2024. Vol. 15, no. 1. P. 1–8 DOI: 10.14569/IJACSA.2024.0150101.

74. Ergun K., Yu X., Nagesh N., Cherkasova L., Mercati P., Ayoub R., Rosing T. RelIoT: Reliability Simulator for IoT Networks. *Lecture Notes in Computer Science*. 2020. Vol. 12405. P. 63–81. DOI: 10.1007/978-3-030-59615-6_5.

75. Meyer zu Westerhausen S., Raveendran G., Lauth T.-H., Meyer O., Rosemann D., Wawer M. L., Stauß T., Wurst J., Lachmayer R. Reliability Assessment of Wireless Sensor Networks by Strain-Based Region Analysis for Redundancy Estimation in Measurements on the Example of an Aircraft Wing Box. *Sensors*. 2024. Vol. 24, no. 13, article no. 4107. P. 1–26. DOI: 10.3390/s24134107.

76. Aikhuele D. O., Nwosu H. U., Ighravwe D. E. Data-driven model for the evaluation of the reliability of sensors and actuators used in IoT system architecture. *Journal of Reliable Intelligent Environments*. 2023. Vol. 9. P. 135–145. DOI: 10.1007/s40860-022-00179-0.

77. Sabando-Bravo K. E., Navia M., Zambrano-Martinez J. L. Optimizing CO2 Monitoring: Evaluating a Sensor Network Design. *Journal of Sensor and Actuator Networks*. 2025. Vol. 14, no. 5, article no. 93. P. 1–20 DOI: 10.3390/jsan14050093.

78. Adday G. H., Subramaniam S. K., Zukarnain Z. A., Samian N. Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey. *IEEE Access*. 2024. Vol. 12. P. 22938–22977. DOI: 10.1109/ACCESS.2024.3362889.

ДОДАТОК А.

Акти впровадження результатів дисертаційної роботи

ЗАТВЕРДЖУЮ

УКРАЇНСЬКИЙ ОРДЕНА «ЗНАК ПОШАНИ» НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ЛІСОВОГО ГОСПОДАРСТВА ТА АГРОЛІСОМЕЛІОРАЦІЇ ім. Г. М. ВИСОЦЬКОГО ДЕРЖАВНОГО АГЕНТСТВА ЛІСОВИХ РЕСУРСІВ УКРАЇНИ ТА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ (УкрНДІЛГА)

В.о. завідувача відділу новітніх інформаційних технологій, к.е.н., с.н.с.

_____ Анатолій Полупан

« 02 » квітня 2026 року

АКТ

реалізації наукових результатів дисертаційної роботи
Скоробогатька Станіслава Віталійовича,
виконаної на здобуття наукового ступеня доктора філософії .

Комісія у складі: голови комісії — В.о. завідувача відділу новітніх інформаційних технологій, к.е.н., с.н.с. А.В. Полупан; с.н.с. Богомолов В.В.; с.н.с., к.е.н. І.Г. Филиппова, склала даний акт в тому, що при впровадженні моделей та програмних засобів оцінювання надійності сенсорних мереж систем моніторингу було використано наступні наукові результати дослідження Скоробогатька С. В. при тестуванні оновленої версії ГЕОПОРТАЛУ «Ліси країни»: - структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень;

– аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території;

– марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання.

Впровадження результатів дослідження Скоробогатька С. В. надало змогу:

– підвищити точність оцінювання ймовірності безвідмовної роботи систем моніторингу потенційно небезпечних територій;

– підвищити якість планування, розміщення та використання гібридних сенсорних мереж за допомогою аналітичних та імітаційних моделей;

– більш точно оцінювати готовність систем моніторингу потенційно небезпечних територій та планувати їх відновлення та обслуговування.

Голова комісії _____ Анатолій Полупан

Члени комісії: _____ Вадим Богомолов

_____ Ірина Филиппова

Затверджую
Проректор з науково-педагогічної роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
к.т.н., доцент
_____ Андрій ГУМЕННИЙ
«__» _____ 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Скоробогатька Станіслава Віталійовича, виконаної на здобуття наукового ступеня доктора філософії, у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій

Комісія у складі: голови комісії – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія ОДОКІЄНКА, і членів –професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Клайда ФУРМАНОВА, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Дмитра УЗУНА, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. В'ячеслава ДУЖОГО, встановила, що наукові результати, отримані під час досліджень, спрямованих на підвищення повноти множини рішень та точності оцінювання надійності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, а саме:

- структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень, які, на відміну від відомих, ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, що дозволяє

планувати розподіл ресурсів і забезпечити надійне функціонування системи в умовах деградації мережі;

- аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території, їхні показники безвідмовності та фатальні комбінації множинних відмов сенсорів за різними критеріями, що дозволяє розраховувати та прогнозувати показники надійності мереж;
- марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання, що дозволяє розраховувати функції готовності мереж для різних стратегій їх технічного обслуговування,

реалізовані у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій у вигляді:

- лекційного матеріалу і практичних занять з використання моделей та засобів оцінювання та забезпечення надійності, зокрема, моделей гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій відповідно до вимог у навчальній дисципліні «Надійність та відмовостійкість комп'ютерних систем» (4 години).

Це дозволило покращити фундаментальність викладання матеріалу із сучасних парадигм надійності сенсорних мереж, а саме, імітаційних, структурних та надійнісних моделей оцінювання безвідмовності гібридних сенсорних мереж, наочність та практичну спрямованість навчального процесу, якість підготовки фахівців за напрямом комп'ютерної інженерії.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Клайд ФУРМАНОВ

Дмитро УЗУН

В'ячеслав ДУЖИЙ

Затверджую
Проректор з наукової роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
д-р. наук з держ. упр., професор
_____ Світлана ДОМБРОВСЬКА
«09» 03 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Скоробогатька Станіслава Віталійовича,
виконаної на здобуття наукового ступеня доктора філософії,
у науково-дослідних проєктах Національного аерокосмічного університету
«Харківський авіаційний інститут»

Комісія у складі: голови – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія ОДОКІЄНКА і членів – професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, д.т.н. Ольги МОРОЗОВОЇ, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, д.т.н. Ігоря КЛЮШНІКОВА, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Артема ТЕЦЬКОГО, встановила, що наукові результати, а саме:

– структурні та надійнісні моделі гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, що базуються на наземних та літаючих компонентах хмарних, граничних та туманних обчислень, які, на відміну від відомих, ураховують різні варіанти розміщення та взаємодії обчислювальних інтелектуальних ресурсів, а також рівні працездатності компонентів залежно від повноти виконання функцій моніторингу, що дозволяє планувати розподіл ресурсів і забезпечити надійне функціонування системи в умовах деградації мережі;

– удосконалено аналітичні та імітаційні моделі оцінювання безвідмовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують особливості покриття сенсорами контрольованої території, їхні показники безвідмовності та фатальні комбінації множинних відмов сенсорів за різними критеріями, що дозволяє розраховувати та прогнозувати показники надійності мереж;

– отримали подальшого розвитку марковські моделі оцінювання готовності сенсорних мереж систем моніторингу потенційно небезпечних територій, які враховують відмови та варіанти відновлення сенсорів та мережевого обладнання, що дозволяє розраховувати функції готовності мереж для різних стратегій їх технічного обслуговування,

реалізовані у вигляді наукових положень і розробок, використаних при виконанні науково-дослідних проєктів за замовленням Міністерства освіти і науки України:

– «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів» (№ Д/Р 0121U112172, 2021-2023 рр.);

– «Методи, моделі та інформаційні технології підвищення надійності та безпечності складних ІТ-систем на етапах розроблення та впровадження» (№ Д/Р 0121U113842, 2021-2023 рр.);

– «Методологія та інформаційні технології оцінювання та забезпечення безпеки цифрової інфраструктури малих модульних реакторів» (№ Д/Р 0122U000977, 2022-2024 рр.);

– «Методи та засоби виявлення вибухонебезпечних предметів з використанням багатофункційних інтелектуальних систем БПЛА» (№ Д/Р 0123U101992, 2023-2024 рр.);

– «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об'єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час).

Це дозволило підвищити показники надійності і готовності гібридних сенсорних мереж систем моніторингу потенційно небезпечних територій, які досліджувалися в рамках виконання НДР впродовж 2022-2025 рр.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Ольга МОРОЗОВА

Ігор КЛЮШНІКОВ

Артем ТЕЦЬКИЙ

ДОДАТОК Б.
ЛІСТИНГИ КОДІВ ПРОГРАМНИХ ЗАСОБІВ

Програмний засіб для імітаційного моделювання сенсорної мережі

```
import numpy as np

import pandas as pd

import plotly.express as px

import plotly.graph_objects as go

import scipy.stats as stats

import os

from collections import deque

import networkx as nx

from PIL import Image

import base64

import io

from scipy.spatial import ConvexHull

import folium

from folium import plugins

from matplotlib.path import Path


class TextRedirector:

    def __init__(self, text_widget):

        self.text_widget = text_widget


    def write(self, string):
```

```
        self.text_widget.insert('end', string)
        self.text_widget.see('end')
        self.text_widget.update()

    def flush(self):
        pass

def time_to_failure(failure_rate, distribution_type, num_samples=1):
    mean_time = 1 / failure_rate

    if distribution_type == 'exponential':
        samples = np.random.exponential(mean_time, num_samples)
    elif distribution_type == 'normal':
        mu = mean_time
        sigma = mean_time
        a = -mu / sigma
        b = np.inf
        samples = stats.truncnorm.rvs(a, b, loc=mu, scale=sigma, size=num_samples)
    elif distribution_type == 'weibull':
        k = 2
        scale = mean_time / np.sqrt(np.pi)
        samples = scale * np.random.weibull(k, num_samples)
    else:
        raise ValueError(f"Unknown distribution type: {distribution_type}")
```

```
    if not np.all(np.isfinite(samples)) or np.any(samples < 0):
        print(f"Warning: Invalid failure times generated: min={samples.min()}, max={samples.max()},
dist={distribution_type}")
        samples = np.maximum(0, samples)
    return samples


def create_random_graph(num_sensors, radius, figure_type='rectangle'):
    if figure_type == 'random':
        figure_type = np.random.choice(['polygon', 'ellipse', 'rectangle'])

    positions = []

    if figure_type == 'polygon':
        num_vertices = np.random.randint(5, 9)
        angles = np.sort(np.random.uniform(0, 2*np.pi, num_vertices))
        radii = np.random.uniform(0.3, 0.5, num_vertices)
        vertices = np.column_stack([radii * np.cos(angles), radii * np.sin(angles)]) + 0.5
        hull = ConvexHull(vertices)
        vertices = vertices[hull.vertices]
        figure_vertices = np.vstack([vertices, vertices[0]])

        poly_path = Path(vertices)
        min_x, min_y = np.min(vertices, axis=0)
```

```
    max_x, max_y = np.max(vertices, axis=0)

    def is_inside(pt):
        return poly_path.contains_point(pt)

elif figure_type == 'ellipse':
    center = np.array([0.5, 0.5])
    a = np.random.uniform(0.3, 0.5)
    b = np.random.uniform(0.2, a)
    theta = np.random.uniform(0, 2*np.pi)

    t = np.linspace(0, 2*np.pi, 100)
    x_rot = a * np.cos(t) * np.cos(theta) - b * np.sin(t) * np.sin(theta) + center[0]
    y_rot = a * np.cos(t) * np.sin(theta) + b * np.sin(t) * np.cos(theta) + center[1]
    figure_vertices = np.column_stack([x_rot, y_rot])

    min_x, max_x = np.min(x_rot), np.max(x_rot)
    min_y, max_y = np.min(y_rot), np.max(y_rot)

    def is_inside(pt):
        px, py = pt[0] - center[0], pt[1] - center[1]
        px_rot = px * np.cos(-theta) - py * np.sin(-theta)
        py_rot = px * np.sin(-theta) + py * np.cos(-theta)
        return (px_rot / a)**2 + (py_rot / b)**2 <= 1
```

```
    elif figure_type == 'rectangle':
        center = np.array([0.5, 0.5])
        width = np.random.uniform(0.4, 0.8)
        height = np.random.uniform(0.3, 0.6)
        theta = np.random.uniform(0, np.pi/4)

        corners = np.array([[-width/2, -height/2], [width/2, -height/2], [width/2, height/2], [-width/2, height/2]])
        x_rot = corners[:, 0] * np.cos(theta) - corners[:, 1] * np.sin(theta) + center[0]
        y_rot = corners[:, 0] * np.sin(theta) + corners[:, 1] * np.cos(theta) + center[1]
        figure_vertices = np.vstack([np.column_stack([x_rot, y_rot]), [x_rot[0], y_rot[0]]])

        min_x, max_x = np.min(x_rot), np.max(x_rot)
        min_y, max_y = np.min(y_rot), np.max(y_rot)

        def is_inside(pt):
            px, py = pt[0] - center[0], pt[1] - center[1]
            px_rot = px * np.cos(-theta) - py * np.sin(-theta)
            py_rot = px * np.sin(-theta) + py * np.cos(-theta)
            return abs(px_rot) <= width/2 and abs(py_rot) <= height/2

    grid_resolution = int(np.sqrt(num_sensors))
```

```
while True:
    xs = np.linspace(min_x, max_x, grid_resolution)
    ys = np.linspace(min_y, max_y, grid_resolution)

    xv, yv = np.meshgrid(xs, ys)
    grid_points = np.column_stack((xv.ravel(), yv.ravel()))

    positions = [pt for pt in grid_points if is_inside(pt)]

    if len(positions) >= num_sensors:
        break

    grid_resolution += 1

positions = np.array(positions)
centroid = np.mean(positions, axis=0)
distances_to_center = np.linalg.norm(positions - centroid, axis=1)
sorted_indices = np.argsort(distances_to_center)
kept_indices = sorted_indices[:num_sensors]
positions = positions[kept_indices]
positions = positions[np.lexsort((positions[:, 0], positions[:, 1]))]

dx = xs[1] - xs[0] if len(xs) > 1 else 0
dy = ys[1] - ys[0] if len(ys) > 1 else 0
```

```
    neighbor_distance = max(dx, dy) * 1.05

    G = nx.Graph()

    for i in range(num_sensors):
        G.add_node(i, pos=positions[i])

    for i in range(num_sensors):
        for j in range(i + 1, num_sensors):
            dist = np.linalg.norm(positions[i] - positions[j])
            if dist <= neighbor_distance:
                G.add_edge(i, j)

    if not nx.is_connected(G):
        print("Warning: Graph is not connected")

    G.graph['radius'] = round(max(dx, dy), 4)
    return G, positions, figure_vertices, figure_type


def check_spatial_failure_current(G, failure_times, spatial_threshold, current_time):
    for node in G.nodes:
        if failure_times[node] <= current_time:
            failed_neighbors = sum(1 for neighbor in G.neighbors(node) if failure_times[neighbor] <=
current_time)
```

```
            if failed_neighbors >= spatial_threshold - 1:
                return True
    return False


def check_spatial_failure_bfs(G, failed_nodes_set, spatial_threshold):
    visited = set()

    for node in failed_nodes_set:
        if node not in visited:
            queue = deque([node])
            visited.add(node)
            cluster_size = 1

            while queue:
                current = queue.popleft()
                for neighbor in G.neighbors(current):
                    if neighbor in failed_nodes_set and neighbor not in visited:
                        visited.add(neighbor)
                        queue.append(neighbor)
                        cluster_size += 1
                        if cluster_size >= spatial_threshold:
                            return True
    return False
```

```
def simulate_wsn(G, positions, num_sensors, fratio, max_time, peripheral_rate, failure_threshold, spatial_threshold, distribution_type="exponential", spatial_method="spatial", time_step="N/A", figure_type="unknown"):

    sensor_failure_times = np.random.exponential(1 / fratio, num_sensors)

    peripheral_failure_time = np.random.exponential(1 / peripheral_rate)



    sorted_indices = np.argsort(sensor_failure_times)



    failure_time = max_time

    failure_cause = "Max Time Reached"

    failed_nodes = set()



    for failed_count, idx in enumerate(sorted_indices, start=1):

        t = sensor_failure_times[idx]



        if t > max_time or t >= peripheral_failure_time:

            break



        failed_nodes.add(idx)



        if failed_count >= failure_threshold:

            failure_time = t

            failure_cause = f"N={failure_threshold} Sensors Failed"

            break
```

```
    if failed_count >= spatial_threshold:
        if check_spatial_failure_bfs(G, failed_nodes, spatial_threshold):
            failure_time = t
            failure_cause = f"Spatial Failure (BFS, Ad={spatial_threshold})"
            break

if peripheral_failure_time < failure_time and peripheral_failure_time <= max_time:
    failure_time = peripheral_failure_time
    failure_cause = "Peripheral Failure"

reliability = 1.0 if failure_time >= max_time else 0.0

return {
    'num_sensors': num_sensors,
    'lambda': fratio,
    'max_time': max_time,
    'distribution_type': distribution_type,
    'spatial_method': spatial_method,
    'time_step': time_step,
    'radius': G.graph.get('radius', 0.1),
    'figure_type': figure_type,
    'failure_cause': failure_cause,
    'failed_sensors': len(failed_nodes),
    'reliability': reliability,
```

```
        'failure_time': failure_time

    }, sensor_failure_times, peripheral_failure_time


def run_simulations(fratios, times, sensor_counts, peripheral_rate, failure_threshold, spatial_threshold,
num_runs, distribution_types, spatial_method, time_step, graphs, positions_dict, figure_vertices_dict,
figure_types_dict):

    results = []

    viz_data = {}


    for dist_type in distribution_types:

        for num_sensors in sensor_counts:

            G = graphs.get(num_sensors)

            positions = positions_dict.get(num_sensors)

            figure_vertices = figure_vertices_dict.get(num_sensors)

            figure_type = figure_types_dict.get(num_sensors)


            if G is None or positions is None or figure_vertices is None:

                print(f"Error: num_sensors={num_sensors}")

                continue


            for fratio in fratios:

                for max_time in times:

                    print(f"Simulation: dist={dist_type}, num_sensors={num_sensors}, lambda={fratio},
max_time={max_time}, N={failure_threshold}, Ad={spatial_threshold}, method={spatial_method},
radius={G.graph.get('radius', 0.1)}")
```

```
for run_idx in range(num_runs):
    result, sensor_failure_times, peripheral_failure_time = simulate_wsn(
        G=G,
        positions=positions,
        num_sensors=num_sensors,
        fratio=fratio,
        max_time=max_time,
        peripheral_rate=peripheral_rate,
        failure_threshold=failure_threshold,
        spatial_threshold=spatial_threshold,
        distribution_type=dist_type,
        spatial_method=spatial_method,
        time_step=time_step
    )
    results.append(result)

    if run_idx == 0 and (dist_type, num_sensors) not in viz_data:
        viz_data[(dist_type, num_sensors)] = {
            'G': G,
            'positions': positions,
            'figure_vertices': figure_vertices,
            'figure_type': figure_type
        }
```

```
    df = pd.DataFrame(results)
    if df.empty:
        print("Warning: Simulation results were not generated")

    return df, viz_data

def save_results(df, output_path, times):
    output_dir = os.path.dirname(output_path)
    if not os.path.exists(output_dir):
        os.makedirs(output_dir)

    if df.empty:
        return

    max_t = max(times)
    df_filtered = df[df['max_time'] == max_t].copy()

    bins = [0] + sorted(times) + [float('inf')]
    labels = []
    for i in range(len(bins)-1):
        if bins[i+1] == float('inf'):
            labels.append(f"> {bins[i]}")
        else:
            labels.append(f"{bins[i]} - {bins[i+1]}")
```

```
    df_filtered['time_interval'] = pd.cut(df_filtered['failure_time'], bins=bins, labels=labels, right=True)


    pivot = pd.pivot_table(
        df_filtered,
        index=['num_sensors', 'lambda', 'time_interval'],
        columns='failure_cause',
        aggfunc='size',
        fill_value=0
    ).reset_index()


    with pd.ExcelWriter(output_path) as writer:
        pivot.to_excel(writer, sheet_name="Failures_by_Interval", index=False)


def save_summary_stats(df, output_dir, distribution_types, confidence_level, spatial_method):
    if df.empty:
        print("Warning: Cannot compute summary statistics; simulation DataFrame is empty")
        return pd.DataFrame(), {}


    required_columns = ['num_sensors', 'distribution_type', 'lambda', 'max_time', 'reliability',
'spatial_method', 'time_step', 'radius']
    missing_columns = [col for col in required_columns if col not in df.columns]
    if missing_columns:
        print(f"Error: Missing columns in simulation DataFrame: {missing_columns}")
```

```
        return pd.DataFrame(), {}


    try:
        summary = df.groupby(['num_sensors', 'distribution_type', 'lambda', 'max_time', 'spatial_method',
'time_step', 'radius']).agg({
            'reliability': ['mean', 'std', 'count']
        }).reset_index()
    except Exception as e:
        print(f"Error during groupby: {str(e)}")
        return pd.DataFrame(), {}


    summary.columns = ['num_sensors', 'distribution_type', 'lambda', 'max_time', 'spatial_method',
'time_step', 'radius',
                       'reliability_mean', 'reliability_std', 'reliability_count']


    print(f"Summary DataFrame columns: {list(summary.columns)}")


    if summary.empty:
        print("Warning: Summary DataFrame is empty after grouping")
        return pd.DataFrame(), {}


    alpha = 1 - confidence_level
    summary['t_critical'] = summary['reliability_count'].apply(
        lambda x: stats.t.ppf(1 - alpha/2, df=x-1) if x > 1 else 0
    )
```

```
    summary['reliability_se'] = summary['reliability_std'] / np.sqrt(summary['reliability_count'])


    summary['reliability_ci_lower'] = summary['reliability_mean'] - summary['t_critical'] *
summary['reliability_se']

    summary['reliability_ci_upper'] = summary['reliability_mean'] + summary['t_critical'] *
summary['reliability_se']


    summary['reliability_ci_lower'] = summary['reliability_ci_lower'].clip(lower=0, upper=1)

    summary['reliability_ci_upper'] = summary['reliability_ci_upper'].clip(lower=0, upper=1)


    output_columns = ['num_sensors', 'lambda', 'max_time', 'spatial_method', 'time_step', 'radius',

                      'reliability_mean', 'reliability_std', 'reliability_ci_lower', 'reliability_ci_upper']


    summary_files = {}

    for dist_type in distribution_types:

        dist_summary = summary[(summary['distribution_type'] == dist_type) &
(summary['spatial_method'] == spatial_method)]

        if dist_summary.empty:

            print(f"Warning: No summary data for {dist_type} distribution, method={spatial_method}")

            continue

        output_path = os.path.join(output_dir, f'wsn_summary_stats_{dist_type}_{spatial_method}.xlsx')

        at_least_one_sheet = False

        with pd.ExcelWriter(output_path, engine='openpyxl') as writer:

            for num_sensors in sorted(df['num_sensors'].unique()):

                n_summary = dist_summary[dist_summary['num_sensors'] == num_sensors]
```

```
            if not n_summary.empty:
                n_summary = n_summary[output_columns]
                n_summary.to_excel(writer, sheet_name=f'num_sensors={num_sensors}', index=False)
                at_least_one_sheet = True
            else:
                print(f"Warning: No summary data for num_sensors={num_sensors}, dist={dist_type}, method={spatial_method}")
        if at_least_one_sheet:
            summary_files[dist_type] = output_path
        else:
            print(f"Warning: No sheets written for {dist_type}, method={spatial_method}; Excel file not saved")

    return summary, summary_files

def plot_reliability(df, output_dir, distribution_types, spatial_method):
    if df.empty or 'reliability' not in df.columns:
        print(f"Warning: Cannot plot reliability histogram; simulation DataFrame is empty or missing 'reliability'")
        return

    plots_dir = os.path.join(output_dir, 'plots')
    if not os.path.exists(plots_dir):
        os.makedirs(plots_dir)
```

```
    for dist_type in distribution_types:
        dist_df = df[(df['distribution_type'] == dist_type) & (df['spatial_method'] == spatial_method)]
        if dist_df.empty:
            print(f"Warning: No data for {dist_type} distribution, method={spatial_method} in reliability histogram")
            continue
        fig = px.histogram(
            dist_df,
            x='reliability',
            nbins=50,
            histnorm='probability density',
            title=f'Distribution of System Reliability ({dist_type.capitalize()}, {spatial_method.upper()})',
            labels={'reliability': 'reliability', 'count': 'Density'}
        )
        fig.update_layout(
            xaxis_title='Reliability',
            yaxis_title='Density',
            showlegend=False,
            bargap=0.1
        )
        html_file = os.path.join(plots_dir, f'reliability_histogram_{dist_type}_{spatial_method}.html')
        fig.write_html(html_file)
        print(f"Reliability histogram ({dist_type}, {spatial_method}) saved to {html_file}")
```

```
def plot_confidence_intervals(summary, output_dir, sensor_counts, fratios, times, distribution_types, confidence_level, spatial_method):

    if summary.empty or 'reliability_mean' not in summary.columns:

        print("Warning: Cannot plot confidence intervals; summary DataFrame is empty or missing 'reliability_mean'")

        return



    plots_dir = os.path.join(output_dir, 'plots')

    if not os.path.exists(plots_dir):

        os.makedirs(plots_dir)



    for num_sensors in sensor_counts:

        n_summary = summary[(summary['num_sensors'] == num_sensors) & (summary['spatial_method'] == spatial_method)]

        if n_summary.empty:

            print(f"Warning: No summary data for num_sensors={num_sensors}, method={spatial_method} in confidence interval plot")

            continue



        fig = go.Figure()

        for dist_type in distribution_types:

            for fratio in fratios:

                data = n_summary[(n_summary['distribution_type'] == dist_type) & (n_summary['lambda'] == fratio)]

                if data.empty:

                    print(f"Warning: No data for dist={dist_type}, lambda={fratio}, num_sensors={num_sensors}, method={spatial_method} in CI plot")
```

```
    continue
data = data.sort_values('max_time')

fig.add_trace(go.Scatter(
    x=data['max_time'],
    y=data['reliability_ci_upper'],
    mode='lines',
    line=dict(width=0),
    showlegend=False
))

fig.add_trace(go.Scatter(
    x=data['max_time'],
    y=data['reliability_ci_lower'],
    mode='lines',
    line=dict(width=0),
    fill='tonexty',
    fillcolor='rgba(0,100,80,0.2)',
    showlegend=False
))

fig.add_trace(go.Scatter(
    x=data['max_time'],
    y=data['reliability_mean'],
```

```
                mode='lines+markers',
                name=f'{dist_type.capitalize()}, \u03bb={fratio}',
                line=dict(width=2),
                marker=dict(size=8)
            ))

    fig.update_layout(
        title=f'Reliability with {confidence_level*100:.1f}% Confidence Intervals
(num_sensors={num_sensors}, {spatial_method.upper()})',
        xaxis_title='T_max',
        yaxis_title='R_wsn',
        xaxis_type='log',
        showlegend=True,
        hovermode='x unified'
    )
    html_file = os.path.join(plots_dir,
f'reliability_ci_num_sensors{num_sensors}_{spatial_method}.html')
    fig.write_html(html_file)
    print(f"Reliability CI plot for num_sensors={num_sensors}, method={spatial_method} saved to
{html_file}")


def plot_reliability_comparison(summary, output_dir, sensor_counts, distribution_types,
spatial_method):
  if summary.empty or 'reliability_mean' not in summary.columns:
    print("Warning: Cannot plot reliability comparison; summary DataFrame is empty or missing
'reliability_mean'")
```

```
        return


    plots_dir = os.path.join(output_dir, 'plots')

    if not os.path.exists(plots_dir):

        os.makedirs(plots_dir)


    for num_sensors in sensor_counts:

        n_summary = summary[(summary['num_sensors'] == num_sensors) &
(summary['spatial_method'] == spatial_method)]

        if n_summary.empty:

            print(f"Warning: No summary data for num_sensors={num_sensors},
method={spatial_method} in reliability comparison plot")

            continue


        fig = go.Figure()

        for dist_type in distribution_types:

            data = n_summary[n_summary['distribution_type'] == dist_type]

            if data.empty:

                print(f"Warning: No data for dist={dist_type}, num_sensors={num_sensors},
method={spatial_method} in comparison plot")

                continue

            agg_data = data.groupby('max_time')['reliability_mean'].mean().reset_index()

            agg_data = agg_data.sort_values('max_time')


            fig.add_trace(go.Scatter(
```

```
            x=agg_data['max_time'],
            y=agg_data['reliability_mean'],
            mode='lines',
            name=dist_type.capitalize(),
            line=dict(width=2)
        ))

        fig.add_trace(go.Scatter(
            x=agg_data['max_time'],
            y=agg_data['reliability_mean'],
            mode='markers',
            marker=dict(size=8),
            showlegend=False
        ))

    fig.update_layout(
        title=f'Reliability Comparison Across Distributions (num_sensors={num_sensors},
{spatial_method.upper()})',
        xaxis_title='Max Time (Hours)',
        yaxis_title='Mean Reliability',
        xaxis_type='log',
        showlegend=True,
        hovermode='x unified'
    )
```

```
        html_file = os.path.join(plots_dir,
f'reliability_comparison_num_sensors{num_sensors}_{spatial_method}.html')

        fig.write_html(html_file)

        print(f"Reliability comparison plot for num_sensors={num_sensors}, method={spatial_method}
saved to {html_file}")



def plot_sensor_map(viz_data, output_dir, distribution_types, spatial_method, bg_image_path):

    plots_dir = os.path.join(output_dir, 'plots')

    if not os.path.exists(plots_dir):

        os.makedirs(plots_dir)



    default_width = 800

    default_height = 600

    img_width = default_width

    img_height = default_height

    img_str = None



    if bg_image_path and os.path.exists(bg_image_path):

        try:

            img = Image.open(bg_image_path)

            img_width, img_height = img.size

            img_buffer = io.BytesIO()

            img.save(img_buffer, format='PNG')

            img_str = base64.b64encode(img_buffer.getvalue()).decode('utf-8')

            print(f"Map loaded: {img_width}x{img_height} pixels")
```

```
        except Exception as e:
            print(f"Error loading map {bg_image_path}: {e}. Using default dimensions
{img_width}x{img_height}.")


    for dist_type in distribution_types:
        for num_sensors in set(num_s[1] for num_s in viz_data.keys()):
            key = (dist_type, num_sensors)
            if key not in viz_data:
                print(f"Warning: No visualization data for {dist_type}, num_sensors={num_sensors}")
                continue

            data = viz_data[key]
            G = data['G']
            positions = data['positions']
            figure_vertices = data['figure_vertices']
            figure_type = data['figure_type']

            grid_step = G.graph.get('radius', 0.1)
            half_size = grid_step / 2.0

            fig = go.Figure()

            if img_str:
                fig.add_layout_image(
```

```
        dict(
            source=f'{img_str}',
            xref="paper",
            yref="paper",
            x=0,
            y=1,
            sizex=1,
            sizey=1,
            xanchor="left",
            yanchor="top",
            sizing="stretch",
            layer="below"
        )
    )

fig.add_trace(
    go.Scatter(
        x=figure_vertices[:, 0],
        y=1 - figure_vertices[:, 1],
        mode='lines',
        name=f'{figure_type.capitalize()} Boundary',
        line=dict(color='blue', width=2, dash='dash'),
        hoverinfo='none'
    )
```

```
)

unique_x = np.sort(np.unique(np.round(positions[:, 0], 4)))
unique_y = np.sort(np.unique(np.round(positions[:, 1], 4)))

dx = unique_x[1] - unique_x[0] if len(unique_x) > 1 else 0.05
dy = unique_y[1] - unique_y[0] if len(unique_y) > 1 else 0.05

hx, hy = dx / 2.0, dy / 2.0

sq_x = []
sq_y = []

for pos in positions:
    x = pos[0]
    y = 1 - pos[1]

    sq_x.extend([x - hx, x - hx, x + hx, x + hx, x - hx, None])
    sq_y.extend([y - hy, y + hy, y + hy, y - hy, y - hy, None])

fig.add_trace(
    go.Scatter(
        x=sq_x,
        y=sq_y,
```

```
        mode='lines',
        fill='toself',
        fillcolor='rgba(51, 136, 255, 0.15)',
        line=dict(color='rgba(51, 136, 255, 0.4)', width=1),
        name='Coverage Zones',
        hoverinfo='none'
    )
)

x_sensors = [pos[0] for pos in positions]
y_sensors = [1 - pos[1] for pos in positions]

fig.add_trace(
    go.Scatter(
        x=x_sensors,
        y=y_sensors,
        mode='markers',
        name='Sensors',
        marker=dict(
            color='white',
            size=8,
            line=dict(color='black', width=1.5)
        ),
```

```
            text=[f'Sensor {i+1}<br>Adjacency Radius: {grid_step:.3f}" for i in
range(len(positions))],
            hoverinfo='text'
        )
    )

    fig.update_layout(
        title=f'Sensor Map...',
        xaxis=dict(
            title='X',
            range=[0, 1],
            showgrid=False,
            zeroline=False
        ),
        yaxis=dict(
            title='Y',
            range=[0, 1],
            showgrid=False,
            zeroline=False,
            scaleanchor="x",
            scaleratio=1
        ),
        showlegend=True,
        hovermode='closest',
```

```
            width=img_width,
            height=img_height
        )

        html_file = os.path.join(plots_dir,
f'sensor_map_{dist_type}_{spatial_method}_num_sensors{num_sensors}.html')
        fig.write_html(html_file)
print(f"Sensor map plot for {dist_type}, {num_sensors} sensors saved to {html_file} (dimensions:
{img_width}x{img_height})")
```

ДОДАТОК В.

Опорний граф для побудови САМ

Крок	Стан та актуальна БП	Ймовірність переходу	V1	V2	V3	№ стану	Перехід	Інтенсивність
Крок 1: Початковий стан. Усі сенсори справні, бригада на базі, ПОб справне.								
1	—	--	0	0	0	1	--	--
Крок 2: Зі стану 1 (S0) конкурують: відмова сенсора (БП1, 9λv) та відмова ПОб (БП8, λр).								
2	Ст.1, БП1 відмова сенсора	1	1	0	0	2	1→2	9λv
	Ст.1, БП8 відмова *ПОб*	1	0	0	1	7	1→7	λр
Крок 3: Зі стану 2 (S1, 1 відм., бригада їде) конкурують: БП2 (8λv), БП4 (λа), БП8 (λр).								
3	Ст.2, БП2 відмова 2-го сенс.	1	2	0	0	3	2→3	8λv
	Ст.2, БП4 прибуття бригади	1	1	1	0	4	2→4	λа
	Ст.2, БП8 відмова *ПОб*	1	1	0	1	8	2→8	λр
Крок 4: Зі стану 3 (S2, 2 відм., бригада їде) конкурують: БП3 (7λv), БП4 (λа), БП8 (λр).								
4	Ст.3, БП3 відмова 3-го сенс.	1	3	0	0	5	3→5	7λv
	Ст.3, БП4 прибуття бригади	1	2	1	0	6	3→6	λа
	Ст.3, БП8 відмова *ПОб*	1	2	0	1	9	3→9	λр
Крок 5: Зі стану 4 (S4, ремонт 1, працює): під час ремонту відмови неможливі. Тільки БП5 (Pr×μr) → S0.								
5	Ст.4, БП5 ремонт завершено	Pr	0	0	0	1	4→1	Pr×μr
Крок 6: Зі стану 5 (S3, 3 відм., простій, бригада їде) конкурують: БП4 (λа), БП8 (λр).								
6	Ст.5, БП4 прибуття бригади	1	3	1	0	10	5→10	λа
	Ст.5, БП8 відмова *ПОб*	1	3	0	1	11	5→11	λр

Кінець таблиці ДОДАТОК В

Крок 7: Зі стану 6 (S5, ремонт 2, працює): під час ремонту відмови неможливі. Тільки БП6 (Pr×μr/2) → S0.								
7	Ст.6, БП6 ремонт завершено	Pr	0	0	0	1	6→1	Pr×μr/2
Крок 8: Зі стану 7 (S7, ПОб з S0): тільки БП9 (Pp×μp) → S0.								
8	Ст.7, БП9 відновлення *ПОб*	Pp	0	0	0	1	7→1	Pp×μp
Крок 9: Зі стану 8 (S8, ПОб з S1): БП9 (Pp×μp) → стан 2 (S1).								
9	Ст.8, БП9 відновлення *ПОб*	Pp	1	0	0	2	8→2	Pp×μp
Крок 10: Зі стану 9 (S9, ПОб з S2): БП9 (Pp×μp) → стан 3 (S2).								
10	Ст.9, БП9 відновлення *ПОб*	Pp	2	0	0	3	9→3	Pp×μp
Крок 11: Зі стану 10 (S6, ремонт 3, простій): під час ремонту відмови неможливі. БП7 (Pr×μr/3) → S0.								
11	Ст.10, БП7 ремонт завершено	Pr	0	0	0	1	10→1	Pr×μr/3
Крок 12: Зі стану 11 (S10, ПОб з S3): БП9 (Pp×μp) → стан 5 (S3).								
12	Ст.11, БП9 відновлення *ПОб*	Pp	3	0	0	5	11→5	Pp×μp