НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ШТІЛЬМАН ПАВЛО РОМАНОВИЧ

УДК 004.7

ДИСЕРТАЦІЯ

БАГАТОРІВНЕВА ОНТОЛОГІЯ АНАЛІЗУ РИЗИКІВ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Спеціальність: 123 – «Комп’ютерні інженерія»
Галузь знань: 12 – «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результаті і текстів інших авторів мають посилання на відповідне джерело.
_____П. Р. Штільман

Науковий керівник:
Мартинюк Олександр Миколайович, кандидат технічних наук, доцент

Одеса – 2026

АНОТАЦІЯ

Штільман П.Р. Багаторівнева онтологія аналізу ризиків у бездротових сенсорних мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерні інженерія. – Національний університет «Одеська політехніка», МОН України, Одеса, 2026.

У **вступі** дисертаційної роботи обґрунтовано актуальність теми дослідження, присвяченого розробленню багаторівневої онтології аналізу ризиків у бездротових сенсорних мережах для підтримки ризик-орієнтованого управління в умовах невизначеності та кіберфізичних загроз. Сформульовано мету та основні завдання роботи, визначено об’єкт, предмет і методи дослідження. Висвітлено наукову новизну та практичне значення одержаних результатів,. Також наведено відомості про апробацію результатів дослідження, публікації автора, структуру дисертації.

У **першому розділі** дисертаційної роботи здійснено системний аналіз сучасного стану досліджень у галузі бездротових сенсорних мереж та підходів, що застосовуються для забезпечення їх ефективного, надійного і безпечного функціонування. Розглянуто архітектурні особливості БСМ, принципи організації взаємодії між сенсорними вузлами, механізми передавання та агрегації даних, а також методи управління мережею в умовах обмежених ресурсів. Значну увагу приділено аналізу кластеризаційних протоколів, зокрема LEACH та його модифікацій, підходів до оптимізації маршрутизації, балансування навантаження та зменшення енергоспоживання. Окремо розглянуто засоби підвищення надійності каналів зв’язку, способи зменшення впливу завад і деградації топології, а також підходи до представлення стану мережі в інтелектуальних системах моніторингу та керування. Для кожного класу рішень визначено основні переваги, обмеження та сферу доцільного застосування з урахуванням специфіки промислових умов, у яких БСМ функціонують під впливом електромагнітних перешкод, змін навколишнього середовища, нестабільності каналів та високих

вимог до безперервності роботи.

Проведений аналіз базувався на сукупності критеріїв, які дозволили зіставити відомі підходи в єдиній системі оцінювання. До таких критеріїв віднесено енергоефективність, адаптивність і здатність до самоорганізації, стійкість до відмов окремих вузлів, якість маршрутизації та агрегації даних, чутливість до впливів середовища, наявність механізмів виявлення загроз і вразливостей, а також придатність до використання у промислових БСМ з підвищеними вимогами до надійності. Крім того, окремим критерієм визначено можливість формального, семантичного або онтологічного опису структури та поточного стану мережі. Таке порівняння показало, що переважна більшість існуючих рішень орієнтована на розв’язання локальних задач, наприклад зменшення енерговитрат, покращення маршрутизації або підвищення пропускної здатності, однак не забезпечує цілісного опису мережі як складної динамічної системи. У більшості випадків параметри вузлів, каналів зв’язку, контекст функціонування та зовнішні впливи розглядаються ізольовано, без врахування їх взаємозалежностей, що істотно обмежує можливість побудови узгоджених механізмів аналіз у та керування.

У межах першого розділу також проаналіз овано підходи до оцінювання вразливостей, загроз і ризиків у бездротових сенсорних мережах. Встановлено, що більшість наявних моделей ґрунтується на статистичних, імовірнісних або евристичних підходах, які є корисними для оцінки окремих характеристик небезпеки, проте не забезпечують достатньої гнучкості для роботи в умовах неповноти, нечіткості та змінності вхідних даних. Такі підходи, як правило, не поєднують у межах єдиної формальної системи структурний опис мережі, телеметричні показники, контекстні стани, виявлені вразливості та наслідки їх реалізації. Через це виникає розрив між рівнем мережевого моніторингу, де накопичуються первинні дані про функціонування БСМ, і рівнем прийняття рішень, на якому мають формуватися обґрунтовані контрзаходи для зниження ризиків. Окремо встановлено, що існуючі протоколи, включно з енергоефективними схемами кластеризації, не підтримують семантичного опису контекстів функціонування мережі та не дозволяють виконувати формалізований

логічний висновок щодо критичних станів її компонентів.

Узагальнення результатів проведеного аналіз у дало змогу окреслити коло основних проблем, що залишаються невирішеними на сучасному етапі розвитку БСМ. До них належать відсутність універсальної семантичної моделі для представлення мережевих станів, недостатня інтеграція між енергетичними, комунікаційними, безпековими та ризиковими параметрами, обмежені можливості адаптивного реагування на зміни середовища, а також недостатнє використання формальних знань для підтримки логічного висновку і прийняття рішень. Показано, що для подолання цих обмежень необхідним є розроблення інтегрованого підходу, який би поєднував структурний опис мережі, моделі вразливостей, механізми динамічного оцінювання ризику та адаптивне керування в межах єдиного концептуального каркаса. Саме тому в першому розділі обґрунтовано доцільність створення багаторівневої онтологічної моделі ризик-орієнтованого управління бездротовими сенсорними мережами та сформульовано мету й основні завдання подальшого дослідження.

У **другому розділі** дисертаційної роботи отримали подальший розвиток нечіткі моделі сенсорного вузла та каналу зв’язку, а також розроблено узагальнені моделі формалізації станів і поведінки компонентів бездротових сенсорних мереж в умовах невизначеності. Основну увагу зосереджено на побудові математичного та лінгвістичного апарату, який дозволяє описувати параметри вузлів і каналів зв’язку не лише у вигляді точних числових значень, а й у формі нечітких оцінок, що є більш адекватним для реальних умов функціонування БСМ. Такий підхід обумовлений тим, що в промислових середовищах значна частина вхідної інформації є неповною, зашумленою, нестабільною в часі або такою, що задається експертно. Застосування апарату нечіткої логіки, лінгвістичних змінних та повного ортогонального семантичного простору дало можливість перейти від жорстких детермінованих описів до гнучкого представлення параметрів мережі, придатного для подальшої інтеграції у багаторівневу онтологічну модель ризик-орієнтованого управління.

У межах розділу спочатку сформовано загальну модель технічної системи з вхідними та вихідними параметрами, серед яких виділено чітко визначені та нечітко визначені величини. Це дозволило побудувати узагальнену схему опису системи, у якій невизначені параметри подаються через лінгвістичні терми та функції належності. Для такого подання введено повний ортогональний семантичний простір, на основі якого формуються терм-множини лінгвістичних змінних і задаються трикутні функції належності. Далі визначено основні математичні операції над нечіткими величинами, а також отримано узагальнені співвідношення для розрахунку характеристик систем із поєднанням чітких і нечітких вхідних та вихідних параметрів. Запропонований формалізм став базою для побудови моделей конкретних компонентів БСМ і забезпечив можливість описувати їх функціонування в узгодженій математичній формі.

На основі розробленого підходу побудовано нечітку модель сенсорного вузла як одного з ключових елементів мережі. У моделі враховано чотири базові складові вузла: датчик, приймально-передавальний модуль, процесор та джерело живлення. Для них задано можливі стани працездатності, проаналіз овано залежності між окремими компонентами та показано, що функціонування вузла визначається не ізольованими характеристиками окремих елементів, а їхньою сукупною взаємодією. З огляду на неможливість точного визначення ймовірностей відмов у складних умовах експлуатації, для опису стану вузла введено набір лінгвістичних змінних, що характеризують імовірність працездатності його основних компонентів та загальну здатність вузла виконувати свої функції. Це дало змогу формалізувати як повністю працездатний режим, так і частково деградовані стани, зокрема режими, у яких вузол втрачає сенсорні функції, але зберігає можливість ретрансляції даних.

Окремо в другому розділі розроблено нечітку модель каналу зв’язку, для якого враховано характеристики пропускної здатності, інтенсивності старіння інформації, часу простою, часу працездатності, коефіцієнта готовності та ненадійності. Канал розглянуто як систему масового обслуговування, однак на відміну від класичних моделей його параметри подано в нечіткій формі, що

дозволяє врахувати неповноту або нечіткість інформації про реальний стан передавання даних. На основі цього отримано співвідношення для оцінювання ефективної пропускної здатності, інтенсивності деградації інформації та ймовірності передачі пакетів у каналі зв’язку. У підсумку показано, що розроблені нечіткі моделі вузлів і каналів забезпечують більш адекватне відображення багатофакторного характеру функціонування БСМ, можуть адаптуватися до різних практичних сценаріїв та створюють теоретичну основу для подальшої інтеграції в онтологічні Методи опису мережі, аналіз у вразливостей, оцінки ризиків і адаптивного керування.

У **третьому розділі** дисертаційної роботи уперше розроблено інтегровану багаторівневу онтологічну модель та алгебраїчну систему бездротової сенсорної мережі та формалізовано сукупність ключових її методів, з яких вона складається, а саме: метод опису мережі, метод виявлення вразливостей, метод оцінки ризиків та метож адаптивного керування. Побудова цих методів спрямована на створення цілісного семантично-алгебраїчного каркаса моделі, який забезпечує узгоджене подання структури мережі, поточних станів її компонентів, виявлених вразливостей, оцінених ризиків і керуючих впливів. На відміну від традиційних підходів, у яких задачі моніторингу, аналіз у загроз і прийняття рішень розглядаються окремо, у запропонованій моделі вони інтегруються в єдину систему знань, придатну до логічного висновку, повторного використання знань та адаптації до змін умов функціонування. Такий підхід дозволяє перейти від розрізненого опису параметрів БСМ до комплексного представлення мережі як динамічної кіберфізичної системи, функціонування якої визначається взаємодією технічних, середовищних і безпекових факторів.

У межах розділу першочергово формується метод семантичного виявлення та логування станів компонентів БСМ, який виконує функцію базового рівня багаторівневої онтології. Цей метод отримав подальший розвиток, у вигляді забезпечення узгодженого перетворення телеметричних даних, топологічної інформації та результатів нечіткого оцінювання у формалізовані онтологічні представлення поточного стану БСМ. Він забезпечує семантичне подання топології

БСМ, характеристик вузлів, параметрів каналів зв’язку, енергетичних показників, затримок, навантаження та інших атрибутів, що відображають поточний стан мережі у поточному стані багаторівневої моделі. У передбачено подання як статичних характеристик, пов’язаних із конфігурацією мережі, так і динамічних параметрів, що змінюються в процесі її роботи. Завдяки цьому метод створює онтологічний контекст, у межах якого можуть бути інтерпретовані телеметричні дані, результати нечітких моделей каналу зв’язку та вузла, а також правила логічного висновку. Окремо в розділі наголошено, що саме цей метод є точкою входу для перетворення первинної мережевої інформації у формалізовані онтологічні представлення, придатні до подальшого аналіз у. Таким чином, метод семантичного виявлення та логування станів компонентів не лише структурує дані про вузли та з’єднання, а й формує основу для побудови повної семантичної моделі у конкретний момент часу.

Наступним важливим компонентом третього розділу є удосконалений метод аналізу вразливостей, призначений для логічного виявлення, класифікації та формалізованого подання критичних станів вузлів і каналів зв’язку. Його актуальність обумовлена тим, що промислові бездротові сенсорні мережі функціонують в умовах обмежених енергетичних ресурсів, впливу електромагнітних перешкод, деградації каналів зв’язку, фізичних пошкоджень компонентів і зростання кіберзагроз. У межах цього методу удосконалено аналіз у вразливостей на основі онтологічних правил і семантичного поєднання структурних, контекстних, топологічних та середовищних характеристик, а також запропоновано узагальнену оцінку інтегральної вразливості компонентів мережі. Отримані оцінки використовуються для формування фактів в онтологічній базі знань, що дозволяє передавати результати аналіз у вразливостей до наступного рівня - отримавший подальший розвиток метод оцінки ризиків - без втрати змістового контексту. Такий підхід забезпечує більш повний перехід від первинних параметрів функціонування БСМ до інтерпретованих знань про потенційно небезпечні стани її компонентів.

Метод оцінки ризиків виконує агрегування інформації про вразливості, технічні характеристики мережі, фактори середовища та зовнішні впливи з метою визначення інтегрального ризику для окремих вузлів, каналів і мережі в цілому. Метод забезпечує інтегрування результатів аналіз у вразливостей, контексту поточного стану мережі, факторів середовища та зовнішніх впливів у межах єдиного формального ризикового подання. На відміну від локальних схем оцінювання, що ґрунтуються лише на одному класі показників, запропонований метод поєднує різнорідні джерела інформації у межах єдиної узагальненої багаторівневої моделі. У ній враховуються імовірність виникнення загрози, інтенсивність її впливу, критичність для функціонування мережі, значущість фізичних та зовнішніх факторів, а також потенційні втрати від реалізації небажаних подій. Результатом роботи методу є формування карти ризиків, яка містить не лише числові оцінки, а й пріоритети реагування для різних компонентів БСМ. Важливо, що розділ підкреслює можливість адаптації вагових коефіцієнтів цієї моделі залежно від змін умов експлуатації, що робить оцінювання ризику динамічним, а не фіксованим. Саме ця властивість дозволяє використовувати результати оцінювання не тільки для пасивного аналізу, а й як основу для подальшого вироблення керуючих рішень у замкненому циклі управління.

Завершальним елементом третього розділу є метод адаптивного керування, у межах якого реалізується метод формування рекомендацій щодо реагування на позаштатні ситуації в бездротовій сенсорній мережі. На цьому рівні результати, сформовані Методом опису мережі, Методом виявлення вразливостей і Методом оцінки ризиків, узагальнюються та використовуються для вироблення обґрунтованих рекомендацій щодо доцільних контрзаходів, спрямованих на стабілізацію функціонування мережі та зниження рівня ризику. До таких рекомендацій можуть належати зміна режимів роботи вузлів, перемаршрутизація трафіку, обмеження участі деградованих компонентів у мережевій взаємодії, посилення моніторингу або уточнення параметрів керування. Сформовані рекомендації можуть бути подані оператору або передані зовнішній системі керування для подальшого прийняття рішення щодо їх реалізації. Важливою

складовою цього методу є зворотного зв’язку, який враховує результати застосування сформованих рекомендацій. Такий зворотний зв’язок містить відомості про зміну рівня ризику, характер оновленого контексту функціонування мережі, своєчасність реагування та можливі додаткові витрати ресурсів. Отримана інформація повторно надходить до системи й використовується для уточнення множини допустимих рекомендацій, їх пріоритетності, правил семантичного зіставлення та політик реагування. Таким чином, у третьому розділі сформовано не просто сукупність окремих методів, а цілісну архітектуру багаторівневої онтологічної системи моделі-алгебри, яка забезпечує семантично-узгоджене подання станів БСМ, виявлення вразливостей, оцінку ризику та підтримку прийняття рішень щодо реагування в промислових умовах, що створює основу для подальшої програмної реалізації та імітаційного дослідження запропонованого підходу.

У **четвертому розділі** дисертаційної роботи розглянуто реалізацію, впровадження та порівняльний аналіз запропонованої багаторівневої онтологічної моделі бездротової сенсорної мережі. Розділ спрямований на практичне підтвердження придатності моделей та методів до використання в задачах опису стану мережі, виявлення вразливостей, оцінювання ризику та формування рекомендацій щодо реагування на позаштатні ситуації. У межах цього розділу визначено призначення та основні задачі реалізації моделей та методів, описано архітектуру її побудови, а також показано, як концептуальні положення попередніх розділів можуть бути використані як основа для прикладного аналізу БСМ у динамічних умовах функціонування.

Архітектура реалізації моделей та методів подана як узгоджена система взаємопов’язаних функціональних складових, у межах якої поєднуються опис структури мережі, подання контексту її функціонування, оцінювання вразливостей, узагальнення ризиків і формування рекомендацій щодо реагування. Окрему увагу приділено реалізації процедур оцінювання контексту, інтегральної вразливості та ризику з методів (спеціальних операцій багаторівневої моделі), що дає змогу простежити послідовність переходу від первинних мережевих параметрів до

узагальнених аналітичних оцінок. Для цього розглянуто методики використання структурних, контекстних, вразливісних і ризикових характеристик мережі в межах єдиної технології до аналізу її станів.

У розділі також подано сценарії дослідження функціонування моделі в різних умовах впровадження і роботи мережі та наведено аналіз отриманих результатів. Це дозволяє оцінити, як зміна параметрів стану компонентів БСМ впливає на вразливість, ризик і зміст рекомендацій щодо реагування. Завершальна частина розділу присвячена порівнянню запропонованої технології з існуючими методами, а також визначенню її переваг, обмежень і практичної цінності. У результаті четвертий розділ демонструє перехід від формалізованого подання багаторівневої онтологічної моделі до її практичного використання як технології аналізу та підтримки прийняття рішень у бездротових сенсорних мережах.

Ключові слова: бездротова сенсорна мережа, багаторівнева онтологічна модель, аналіз ризиків, ризик-орієнтоване управління, метод семантичного виявлення та логування станів компонентів, метод аналізу вразливостей, метод оцінки ризиків, метод адаптивного керування, нечітка логіка, нечіткі моделі висновок, онтологічне моделювання, імітаційне моделювання.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Nesterenko, S. A. .; Tishin, P. M.; Shtilman, P. R. .; Martynyuk, O. N. .; Mileiko, I. G. Fuzzy Models of Wireless Components Sensor Networks. Herald of Advanced Information Technology 2025, 8 (2), 209–220. https://doi.org/10.15276/hait.08.2025.13. *Видання включено до переліку наукових фахових видань України, категорія «А».*

https://hait.od.ua/index.php/journal/article/view/189/183

2. Shtilman P. R.; Tishin P. M. .; Shendryk Y. V.; Elkin V. O. . " Risk Assessment and Network Description Modules in a Multi-Level Wireless Sensor Network Risk Assessment Ontology" Publ. Nauka i Tekhnika. Odesa: Ukraine. AAIT 8 (2), 202–215. **https://doi.org/10.15276/aait.08.2025.14**. *Видання включено до*

переліку наукових фахових видань України, категорія «Б».

https://aait.od.ua/index.php/journal/article/view/180/176

3. Штільман П.Р., Тішин П.М.. Модуль вразливості у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі. Журнал Інформатика. Культура. Техніка. 2024 25–27 вересня 2024 р. м. Одеса (Україна). 2024; 1(1): 93–97 . DOI: **https://doi.org/10.15276/ict.01.2024.13**. *Видання включено до переліку наукових фахових видань України, категорія «Б»*

https://ict.op.edu.ua/index.php/journal/uk/article/view/103

4. Shtilman. P, Tishin. P., Martynyuk. O., Nesterenko. S. and Mileiko. I., "Fuzzy Modeling of Sensor Node and Communication Channel in Wireless Sensor Networks," 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-10, doi: 10.1109/IDAACS68557.2025.11321991. *Видання проіндексовано у базі даних Scopus.*

https://ieeexplore.ieee.org/document/11321991/authors#authors

5. Штільман П.Р., Тішин П.М., Мартинюк О.М., Єлькін В.О.. Інтегрована онтологія ризику, вразливості та опису мережі для адаптивного управління промисловими бездротовими сенсорними мережами. Журнал Інформатика. Культура. Техніка. 2025 м. Одеса (Україна). 2025; 2(2): 215–220. DOI: **https://doi.org/10.15276/ict.02.2025.32**. *Видання включено до переліку наукових фахових видань України, категорія «Б»*

https://ict.op.edu.ua/index.php/journal/uk/article/view/40

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. II International Scientific and Practical Conference «Research work in the system of training teachers in technological fields». Berlin, Germany, January 2024;
2. X Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна, вересня 2024;
3. Modern Information Technology 2025/Сучасні Інформаційні Технології

2025. / Національний університет «Одеська політехніка». – Одеса, 2025;

4. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 4-6 September, 2025, Gliwice, Poland;

5. The XIII International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST- ODESA – 2025) 24th – 26th September, 2025;

6. XI Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна. Жовтень 2025;

7. The 15th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2025 19-21 December, 2025, Athens, Greece;

ABSTRACT

Shtilman P.R. Multi-Level Ontology for Risk Analysis in Wireless Sensor Networks. – Qualifying scientific work submitted as a manuscript.

Dissertation for the degree of PhD in specialty 123 – Computer Engineering. – Odesa Polytechnic National University, Ministry of Education and Science of Ukraine, Odesa, 2026.

The introduction of the dissertation substantiates the relevance of the research topic, which is devoted to the development of a multilevel ontology for risk analysis in wireless sensor networks to support risk-oriented management under conditions of uncertainty and cyber-physical threats. The aim and main objectives of the work are formulated, and the object, subject, and research methods are defined. The scientific novelty and practical significance of the obtained results are presented. Information is also provided on the approbation of the research results, the author's publications, and the structure of the dissertation.

The first chapter of the dissertation provides a systematic analysis of the current state of research in the field of wireless sensor networks and the approaches used to ensure their efficient, reliable, and secure operation. The architectural features of WSNs, the principles of interaction between sensor nodes, mechanisms of data transmission and aggregation, and methods of network management under conditions of limited resources are considered. Considerable attention is paid to the analysis of clustering protocols, in particular LEACH and its modifications, as well as approaches to routing optimization, load balancing, and reduction of energy consumption. Means of improving the reliability of communication channels, methods for reducing the influence of interference and topology degradation, and approaches to representing the state of the network in intelligent monitoring and control systems are considered separately. For each class of solutions, the main advantages, limitations, and areas of appropriate application are identified, taking into account the specifics of industrial environments in which WSNs operate under the influence of electromagnetic interference, environmental changes, channel instability, and high requirements for operational continuity.

The analysis was based on a set of criteria that made it possible to compare known approaches within a unified evaluation framework. These criteria include energy efficiency, adaptability and self-organization capability, resilience to individual node failures, routing and data aggregation quality, sensitivity to environmental influences, the availability of mechanisms for detecting threats and vulnerabilities, and suitability for use in industrial WSNs with increased reliability requirements. In addition, the possibility of a formal, semantic, or ontological description of the network structure and current state was defined as a separate criterion. This comparison showed that the vast majority of existing solutions are focused on solving local tasks, such as reducing energy costs, improving routing, or increasing throughput, but do not provide a holistic description of the network as a complex dynamic system. In most cases, the parameters of nodes, communication channels, operating context, and external influences are considered separately, without taking into account their interdependencies, which significantly limits the possibility of building coherent mechanisms for analysis and management.

Within the first chapter, approaches to assessing vulnerabilities, threats, and risks in wireless sensor networks are also analyzed. It is established that most existing models are based on statistical, probabilistic, or heuristic approaches, which are useful for assessing individual characteristics of danger but do not provide sufficient flexibility for operating under conditions of incomplete, vague, and variable input data. As a rule, such approaches do not combine the structural description of the network, telemetry indicators, contextual states, detected vulnerabilities, and the consequences of their realization within a single formal system. This creates a gap between the network monitoring level, where primary data on WSN operation are accumulated, and the decision-making level, where justified countermeasures for risk reduction should be formed. It is also established that existing protocols, including energy-efficient clustering schemes, do not support a semantic description of network operating contexts and do not allow formalized logical inference regarding critical states of its components.

The generalization of the results of the analysis made it possible to identify the main problems that remain unresolved at the current stage of WSN development. These include the absence of a universal semantic model for representing network states,

insufficient integration between energy, communication, security, and risk parameters, limited possibilities for adaptive response to environmental changes, and insufficient use of formal knowledge to support logical inference and decision-making. It is shown that overcoming these limitations requires the development of an integrated approach that combines the structural description of the network, vulnerability models, mechanisms for dynamic risk assessment, and adaptive control within a single conceptual framework. Therefore, the first chapter substantiates the expediency of creating a multilevel ontological model of risk-oriented management of wireless sensor networks and formulates the aim and main objectives of the further research.

In the second chapter of the dissertation, fuzzy models of a sensor node and a communication channel are further developed, and generalized models for formalizing the states and behavior of wireless sensor network components under uncertainty are proposed. The main attention is focused on constructing a mathematical and linguistic apparatus that allows the parameters of nodes and communication channels to be described not only as precise numerical values, but also in the form of fuzzy estimates, which is more adequate for real WSN operating conditions. This approach is due to the fact that, in industrial environments, a significant part of the input information is incomplete, noisy, unstable over time, or expert-defined. The use of fuzzy logic, linguistic variables, and a complete orthogonal semantic space made it possible to move from rigid deterministic descriptions to a flexible representation of network parameters suitable for further integration into a multilevel ontological model of risk-oriented management.

Within the chapter, a general model of a technical system with input and output parameters is first formed, among which clearly defined and fuzzily defined quantities are distinguished. This made it possible to construct a generalized scheme for describing a system in which uncertain parameters are represented through linguistic terms and membership functions. For this representation, a complete orthogonal semantic space is introduced, on the basis of which term sets of linguistic variables are formed and triangular membership functions are defined. The main mathematical operations on fuzzy quantities are then determined, and generalized relations are obtained for calculating the characteristics of systems with a combination of crisp and fuzzy input and output

parameters. The proposed formalism became the basis for constructing models of specific WSN components and ensured the possibility of describing their functioning in a coherent mathematical form.

Based on the developed approach, a fuzzy model of a sensor node as one of the key network elements is constructed. The model takes into account four basic components of a node: the sensor, transceiver module, processor, and power source. Possible states of operability are defined for them, dependencies between individual components are analyzed, and it is shown that node operation is determined not by the isolated characteristics of individual elements, but by their combined interaction. Given the impossibility of accurately determining failure probabilities under complex operating conditions, a set of linguistic variables is introduced to describe the node state, characterizing the probability of operability of its main components and the general ability of the node to perform its functions. This made it possible to formalize both a fully operational mode and partially degraded states, including modes in which the node loses its sensing functions but retains the ability to relay data.

The second chapter also develops a fuzzy model of a communication channel, which takes into account bandwidth characteristics, information aging intensity, downtime, uptime, availability coefficient, and unreliability. The channel is considered as a queuing system; however, unlike classical models, its parameters are represented in fuzzy form, which makes it possible to account for the incompleteness or vagueness of information about the real state of data transmission. On this basis, relations are obtained for estimating effective bandwidth, the intensity of information degradation, and the probability of packet transmission in the communication channel. As a result, it is shown that the developed fuzzy models of nodes and channels provide a more adequate representation of the multifactorial nature of WSN operation, can be adapted to different practical scenarios, and create a theoretical basis for further integration into ontological methods of network description, vulnerability analysis, risk assessment, and adaptive control.

In the third chapter of the dissertation, an integrated multilevel ontological model and an algebraic system of a wireless sensor network are developed for the first time, and

a set of its key methods is formalized, namely: the network description method, the vulnerability detection method, the risk assessment method, and the adaptive control method. The construction of these methods is aimed at creating a holistic semantic-algebraic framework of the model, which provides a coherent representation of the network structure, the current states of its components, detected vulnerabilities, assessed risks, and control actions. Unlike traditional approaches, in which monitoring, threat analysis, and decision-making tasks are considered separately, the proposed model integrates them into a single knowledge system suitable for logical inference, knowledge reuse, and adaptation to changing operating conditions. This approach makes it possible to move from a fragmented description of WSN parameters to a comprehensive representation of the network as a dynamic cyber-physical system whose operation is determined by the interaction of technical, environmental, and security factors.

Within the chapter, the method of semantic identification and logging of WSN component states is first formed, performing the function of the basic level of the multilevel ontology. This method was further developed by ensuring the coherent transformation of telemetry data, topological information, and the results of fuzzy evaluation into formalized ontological representations of the current WSN state. It provides semantic representation of the WSN topology, node characteristics, communication channel parameters, energy indicators, delays, load, and other attributes that reflect the current state of the network within the current state of the multilevel model. The method provides for the representation of both static characteristics related to the network configuration and dynamic parameters that change during its operation. As a result, it creates an ontological context within which telemetry data, the results of fuzzy models of the communication channel and node, and logical inference rules can be interpreted. The chapter separately emphasizes that this method is the entry point for transforming primary network information into formalized ontological representations suitable for further analysis. Thus, the method of semantic identification and logging of component states not only structures data on nodes and connections, but also forms the basis for constructing a complete semantic model at a specific point in time.

The next important component of the third chapter is the improved method of vulnerability analysis, intended for the logical detection, classification, and formalized representation of critical states of nodes and communication channels. Its relevance is due to the fact that industrial wireless sensor networks operate under conditions of limited energy resources, electromagnetic interference, degradation of communication channels, physical damage to components, and increasing cyber threats. Within this method, vulnerability analysis is improved on the basis of ontological rules and the semantic combination of structural, contextual, topological, and environmental characteristics, and a generalized assessment of the integral vulnerability of network components is proposed. The obtained assessments are used to form facts in the ontological knowledge base, which allows the results of vulnerability analysis to be transferred to the next level - the further developed risk assessment method - without loss of semantic context. This approach provides a more complete transition from the primary operating parameters of a WSN to interpreted knowledge about potentially dangerous states of its components.

The risk assessment method aggregates information about vulnerabilities, technical characteristics of the network, environmental factors, and external influences in order to determine the integral risk for individual nodes, channels, and the network as a whole. The method ensures the integration of vulnerability analysis results, the context of the current network state, environmental factors, and external influences within a single formal risk representation. Unlike local assessment schemes based on only one class of indicators, the proposed method combines heterogeneous sources of information within a single generalized multilevel model. It takes into account the probability of threat occurrence, the intensity of its impact, criticality for network functioning, the significance of physical and external factors, and the potential losses caused by the realization of undesirable events. The result of the method is the formation of a risk map that contains not only numerical estimates but also response priorities for different WSN components. It is important that the chapter emphasizes the possibility of adapting the weight coefficients of this model depending on changes in operating conditions, which makes risk assessment dynamic rather than fixed. This property allows the assessment results to

be used not only for passive analysis, but also as a basis for the further development of control decisions within a closed management loop.

The final element of the third chapter is the adaptive control method, within which the method for forming recommendations for responding to abnormal situations in a wireless sensor network is implemented. At this level, the results formed by the network description method, vulnerability detection method, and risk assessment method are generalized and used to produce substantiated recommendations regarding appropriate countermeasures aimed at stabilizing network operation and reducing the risk level. Such recommendations may include changing node operating modes, rerouting traffic, limiting the participation of degraded components in network interaction, strengthening monitoring, or refining control parameters. The generated recommendations may be presented to an operator or transmitted to an external control system for further decision-making regarding their implementation. An important component of this method is feedback, which takes into account the results of applying the generated recommendations. Such feedback contains information about changes in the risk level, the nature of the updated network operating context, the timeliness of response, and possible additional resource costs. The obtained information is returned to the system and used to refine the set of admissible recommendations, their priority, semantic matching rules, and response policies. Thus, the third chapter forms not merely a set of separate methods, but a holistic architecture of a multilevel ontological model-algebra system that provides semantically coherent representation of WSN states, vulnerability detection, risk assessment, and decision support for response in industrial conditions, creating a basis for further software implementation and simulation research of the proposed approach.

The fourth chapter of the dissertation considers the implementation, deployment, and comparative analysis of the proposed multilevel ontological model of a wireless sensor network. The chapter is aimed at practically confirming the suitability of the models and methods for use in tasks of describing the network state, detecting vulnerabilities, assessing risk, and forming recommendations for responding to abnormal situations. Within this chapter, the purpose and main tasks of implementing the models and methods are defined, the architecture of their construction is described, and it is shown

how the conceptual provisions of the previous chapters can be used as a basis for applied WSN analysis under dynamic operating conditions.

The architecture for implementing the models and methods is presented as a coherent system of interrelated functional components that combines the description of the network structure, representation of its operating context, vulnerability assessment, risk generalization, and formation of response recommendations. Special attention is paid to implementing procedures for assessing context, integral vulnerability, and risk using the methods, that is, the special operations of the multilevel model, which makes it possible to trace the sequence of transition from primary network parameters to generalized analytical assessments. For this purpose, approaches to using structural, contextual, vulnerability-related, and risk-related characteristics of the network within a unified technology for analyzing its states are considered.

The chapter also presents scenarios for studying the functioning of the model under different conditions of network deployment and operation and analyzes the obtained results. This makes it possible to assess how changes in the state parameters of WSN components affect vulnerability, risk, and the content of response recommendations. The final part of the chapter is devoted to comparing the proposed technology with existing methods, as well as determining its advantages, limitations, and practical value. As a result, the fourth chapter demonstrates the transition from the formalized representation of the multilevel ontological model to its practical use as a technology for analysis and decision support in wireless sensor networks.

Keywords: wireless sensor network, multilevel ontological model, risk analysis, risk-oriented management, method of semantic identification and logging of component states, vulnerability analysis method, risk assessment method, adaptive control method, fuzzy logic, fuzzy models, inference, ontological modeling, simulation modeling.

List of publications of the applicant on the topic of the dissertation

Scientific works in which the main scientific results of the dissertation are published:

1. Nesterenko, S. A. .; Tishin, P. M.; Shtilman, P. R. .; Martynyuk, O. N. .; Mileiko, I. G. Fuzzy Models of Wireless Components Sensor Networks. Herald of Advanced Information Technology 2025, 8 (2), 209–220. https://doi.org/10.15276/hait.08.2025.13. *The publication is included in the list of scientific professional publications of Ukraine, category "A".*

https://hait.od.ua/index.php/journal/article/view/189/183

2. Shtilman P. R.; Tishin P. M. .; Shendryk Y. V.; Elkin V. O. . " Risk Assessment and Network Description Modules in a Multi-Level Wireless Sensor Network Risk Assessment Ontology" Publ. Nauka i Tekhnika. Odesa: Ukraine. AAIT 8 (2), 202–215. **https://doi.org/10.15276/aait.08.2025.14**.

The publication is included in the list of scientific professional publications of Ukraine, category "B".

https://aait.od.ua/index.php/journal/article/view/180/179

3. Shtilman P.R., Tishin P.M.. Vulnerability module in multilevel ontology of risk assessment of wireless sensor network. Informatics. Culture. Technology. 2024. Odessa (Ukraine). 2024; 1(1): 93–97 . DOI: https://doi.org/10.15276/ict.01.2024.13.

The publication is included in the list of scientific professional publications of Ukraine, category "B"

https://ict.op.edu.ua/index.php/journal/uk/article/view/103.

4. Shtilman. P, Tishin. P., Martynyuk. O., Nesterenko. S. and Mileiko. I., "Fuzzy Modeling of Sensor Node and Communication Channel in Wireless Sensor Networks," 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-10, doi: 10.1109/IDAACS68557.2025.11321991, pp. 471–482.

The publication is indexed in the Scopus database.

https://ieeexplore.ieee.org/document/11321991/authors#authors

5. Shtilman P.R., Tishin P.M., Martyniuk O.M., Yelkin V.O. Integrated ontology of risk, vulnerability and network description for adaptive management of industrial wireless sensor networks. Informatics. Culture. Technology. 2025. Odessa (Ukraine). 2025; 2(2): 215–220. DOI: https://doi.org/10.15276/ict.02.2025.32.

The publication is included in the list of scientific professional publications of Ukraine, category "B.

https://ict.op.edu.ua/index.php/journal/uk/article/view/40

Scientific papers certifying the approbation of the dissertation materials:

1. II International Scientific and Practical Conference «Research work in the system of training teachers in technological fields». Berlin, Germany, January 2024;
2. X International Scientific and Practical Conference "Informatics. Culture. Technology", Odesa, Ukraine, September 2024;
3. Modern Information Technology 2025/ National University "Odesa Polytechnic". – Odesa, 2025;
4. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 4-6 September, 2025, Gliwice, Poland;
5. The XIII International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST- ODESA – 2025) 24th – 26th September, 2025;
6. XI International Scientific and Practical Conference "Informatics. Culture. Technology", Odesa, Ukraine. October 2025;

The 15th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2025 19-21 December, 2025, Athens, Greece

ЗМІСТ

ВСТУП

Актуальність теми. Упродовж останніх десятиліть бездротові сенсорні мережі набули широкого застосування в системах промислового моніторингу, автоматизації технологічних процесів, екологічного контролю, транспортної інфраструктури, енергетики, логістики та інших критично важливих сферах. Їх використання зумовлене можливістю організації розподіленого збору даних у режимі реального часу, гнучкістю розгортання, відносно невисокою вартістю та здатністю функціонувати в середовищах, де застосування традиційних дротових рішень є ускладненим або економічно недоцільним. Водночас саме специфіка таких мереж, зокрема велика кількість вузлів, обмеженість їх енергетичних ресурсів, залежність від якості каналів зв'язку та вплив зовнішнього середовища, істотно ускладнює забезпечення стабільного, надійного і безпечного функціонування БСМ.

Особливої складності ця проблема набуває в промислових умовах, де на роботу бездротових сенсорних мереж додатково впливають електромагнітні завади, змінність топології, деградація каналів зв'язку, апаратні відмови, фізичні ушкодження компонентів, а також кіберфізичні загрози. За таких умов мережа повинна не лише виконувати базові функції моніторингу та передавання даних, а й адаптуватися до змін середовища, підтримувати необхідний рівень надійності, своєчасно виявляти критичні стани та забезпечувати обґрунтоване реагування на потенційні ризики. Це вимагає застосування підходів, які дозволяють розглядати БСМ не як сукупність окремих технічних елементів, а як складну динамічну систему з великою кількістю взаємопов'язаних параметрів і станів.

У сучасних дослідженнях запропоновано значну кількість методів, спрямованих на підвищення енергоефективності, удосконалення маршрутизації, покращення агрегації даних, підвищення стійкості до відмов і забезпечення безпеки бездротових сенсорних мереж. Проте більшість із них орієнтована на розв'язання окремих локальних задач і не забезпечує цілісного

подання мережі як єдиного об’єкта аналізу та керування. Як правило, параметри вузлів, каналів зв’язку, умови функціонування, вразливості, загрози та ризики аналізуються відокремлено, без належного врахування їх взаємозалежностей. Існуючі моделі оцінювання ризиків переважно базуються на статистичних, імовірнісних або евристичних підходах, які є корисними для окремих оцінок, але не завжди забезпечують достатню гнучкість в умовах неповноти, нечіткості та динамічної зміни вхідних даних.

Унаслідок цього виникає суперечність між потребою в інтелектуальному, адаптивному та ризик-орієнтованому управлінні бездротовими сенсорними мережами і відсутністю інтегрованих формальних засобів, здатних поєднати опис структури мережі, параметрів її функціонування, вразливостей, ризиків і механізмів реагування в межах єдиного концептуального підходу. Одним із перспективних шляхів розв’язання цієї проблеми є використання онтологічного підходу, який дає змогу формалізувати знання про мережу, подати взаємозв’язки між її компонентами, підтримати логічний висновок і створити основу для прийняття рішень в умовах невизначеності. Саме тому актуальними є дослідження, спрямовані на розроблення багаторівневої онтології аналізу ризиків у бездротових сенсорних мережах для підтримки ризик-орієнтованого управління в умовах невизначеності та кіберфізичних загроз.

Мета дослідження – розробити інтегровану багаторівневу онтологічну модель ризик-орієнтованого управління бездротовими сенсорними мережами, яка забезпечує семантичне узгодження, багатоверсійність і повноту подання станів мережі, формалізацію системи критеріїв їх оцінювання, а також підтримує автоматизований логічний висновок, динамічну оцінку ризику й формування рекомендацій щодо реагування в умовах невизначеності та кіберфізичних загроз.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– Провести системний аналіз сучасних методів моделювання, управління та забезпечення безпеки бездротових сенсорних мереж, визначити їх

обмеження та вимоги до побудови ризик-орієнтованих систем;

– Створити концептуальну та формальну онтологічну модель структури, станів, вразливостей та ризикових факторів БСМ, що забезпечує семантичну узгодженість між різними рівнями опису;

– Розробити модель оцінки вразливостей та формальні правила логічного висновку для визначення станів мережевих компонентів у мінливих умовах;

– Розробити динамічну модель оцінки ризику, яка поєднує внутрішні характеристики мережі, впливи середовища та зовнішні чинники;

– Створити механізм адаптивного управління БСМ, що забезпечує прийняття контрзаходів і корекцію параметрів моделі на основі оцінки ефективності попередніх рішень;

– Забезпечити інтеграцію структурної онтології, нечітких моделей та методів маршрутизації у єдиний замкнений контур управління.

– Розробити методологію технологічного рішення для практичної реалізації багаторівневої онтологічної моделі БСМ, що визначає архітектуру взаємодії її функціональних Методів, порядок обробки даних і формування рекомендацій щодо реагування.

Об’єкт дослідження – локальні комп’ютерні мережі, кіберфізичні системи, Інтернет речей, методи для дослідження, налагодження, виробництва й експлуатації комп’ютерних мереж, кіберфізичних систем, а також процедури та засоби підтримки та керування життєвим циклом, забезпечення якості, надійності та безпеки [1].

Предмет дослідження – багаторівнева онтологічна модель бездротової сенсорної мережі, що забезпечує формалізоване подання її структури, контексту функціонування, вразливостей, ризиків і рекомендацій щодо реагування, а також нечіткі моделі сенсорного вузла та каналу зв’язку, інтегровані в загальну модель для опису станів мережі в умовах невизначеності..

Методи дослідження. Для розв’язання поставлених задач використано методи дослідження та удосконалення процесів в комп’ютерних та

кіберфізичних системах та мережах, дослідження та оптимізації процесів автоматизованого і автоматичного проектування та виробництва програмних і програмно-технічних засобів комп'ютерних і кіберфізичних систем та мереж [1].

Наукова новизна одержаних результатів полягає в розробленні теоретико-методичних засад ризик-орієнтованого управління бездротовими сенсорними мережами на основі інтеграції нечіткого моделювання, онтологічного подання знань, формальних правил логічного нечіткого висновку та імітаційного аналізу. У межах виконаного дослідження отримано такі наукові результати:

Отримала подальшого розвитку спеціальна нечітка модель сенсорного вузла та каналу зв'язку бездротової сенсорної мережі, яка ґрунтується на графово-атрибутивних моделях структури мережі та нечітких оцінках станів вузлів і каналів. Модель відрізняється поетапним перетворенням багаторівневих параметричних характеристик у лінгвістично та семантично інтерпретовані стани, та формуванням зведених критеріїв оцінювання функціонального стану вузла та каналу зв'язку за енергетичними, часовими, навантажувальними та комунікаційними ознаками. Модель має більшу обчислювальну повноту (на 67 %) та точність (до 100 %), завдяки тому підвищує придатність специфікації сенсорної мережі до прискореного обчислювального аналізу вразливостей і ризиків та прийняття рішень в умовах невизначеності, а також дозволяє створювати відповідний клас методів підтримки прийняття рішень щодо реагування на позаштатні ситуації.

Уперше розроблено інтегровану багаторівневу онтологічну модель аналізу бездротової сенсорної мережі, яка ґрунтується на графово-атрибутивних моделях структури мережі, нечітких оцінках станів компонентів мережі та спеціальної нечіткої моделі сенсорного вузла та каналу зв'язку бездротової сенсорної мережі. Модель має особливості багаторівневого онтологічного семантично узгодженого подання формалізованих вразливостей, ризикових факторів і адаптивного керування, побудови системи

зведених критеріїв їх оцінювання за структурними, контекстними, вразливісними та ризиковими ознаками, узагальнення результатів аналізу для різних режимів функціонування мережі. Модель забезпечує більшу обчислювальну повноту (до 98,3 %), точність (до 100 %) та цілісність семантичної специфікації стану БСМ, а також дозволяє створювати відповідний клас методів підтримки прийняття рішень щодо реагування на позаштатні ситуації.

Отримав подальшого розвитку метод семантичного визначення та логування станів компонентів бездротових сенсорних мереж, який ґрунтується на інтегрованої багаторівневої онтологічної моделі та спеціальної нечіткої моделі сенсорного вузла та каналу зв'язку бездротової сенсорної мережі. Метод відрізняється багаторівневим семантичним поетапним визначенням та узгодженням телеметричних, топологічних і нечітко інтерпретованих характеристик компонентів сенсорної мережі, а також формуванням формалізованого онтологічного подання поточного стану компонентів мережі. Метод дозволяє з більшою обчислювальною точністю (до 100 %) формувати як багаторівневе детальне, так й за зменшений обчислювальний час (на 15 %) отримати узагальнене подання поточного стану БСМ й зведений критерій оцінювання станів БСМ за структурними, контекстними та функціональними ознаками для логічного висновку, виявлення вразливостей, подальшого оцінювання ризику та прийняття рішень.

Удосконалено метод аналізу вразливостей бездротових сенсорних мереж, який ґрунтується на інтегрованої багаторівневої онтологічної моделі та спеціальної нечіткої моделі сенсорного вузла та каналу зв'язку бездротової сенсорної мережі. Метод відрізняється використанням спеціалізованих правил поетапного виявлення критичних станів на основі формальних правил нечіткого логічного висновку, семантичних онтологічних залежностей між компонентами мережі та контекстно залежних ознак їх функціонування, що дозволяє формувати зведений критерій оцінювання вразливості компонентів

БСМ за структурними, контекстними, топологічними та середовищними ознаками. Метод дає змогу за менший обчислювальний час (на 20 %) виявляти критичні стани, слабкі місця мережі та формувати основу для подальшої оцінки ризику й прийняття рішень.

Отримав подальший розвиток узагальнений метод оцінки ризику в бездротових сенсорних мережах, який ґрунтується на інтегрованої багаторівневої онтологічної моделі та спеціальної нечіткої моделі сенсорного вузла та каналу зв'язку бездротової сенсорної мережі. Метод відрізняється поетапним семантичним інтегруванням результатів аналізу вразливостей, контексту поточного стану мережі, факторів середовища, зовнішніх впливів і структурної ролі компонентів у межах єдиного формального ризикового подання, а також формуванням зведеного критерію оцінювання ризику компонентів і сегментів БСМ за вразливісними, контекстними, середовищними та структурно-пріоритетними ознаками. Метод забезпечує з меншим обчислювальним часом (на 22 %) побудову карти ризиків і створює основу для вибору доцільних контрзаходів, щодо реагування, й прийняття рішень.

Практичне значення одержаних результатів. Розроблена багаторівнева онтологічна модель бездротової сенсорної мережі може бути використана як концептуальна та методологічна основа для створення інтелектуальних систем моніторингу, аналізу станів мережі, виявлення вразливостей, оцінювання ризику та підтримки прийняття рішень щодо реагування в промислових умовах. Запропоновані метод семантичного визначення та логування станів комповнентів бездротових сенсорних мереж, метод аналізу вразливостей, метод оцінки ризиків і метод адаптивного керування дають змогу будувати програмно-алгоритмічні рішення для підвищення надійності, стійкості та безпеки функціонування бездротових сенсорних мереж, зокрема в задачах енергетичного моніторингу, діагностики обладнання, контролю параметрів виробничого середовища та підтримки кіберфізичної безпеки. Отримані результати можуть бути використані, як

основа технології, під час проєктування автоматизованих систем на базі БСМ шляхом інтеграції онтологічних компонентів, правил логічного висновку, нечітких моделей сенсорного вузла та каналу зв’язку, а також процедур оцінювання вразливостей і ризику в IoT-платформи, промислові шлюзи або спеціалізовані програмні засоби аналізу. Крім того, результати дослідження можуть бути використані в освітньому процесі під час підготовки фахівців у галузі комп’ютерної інженерії, кіберфізичних систем і мережевих технологій.

Особистий внесок здобувача. Основні наукові положення, висновки і рекомендації, що містяться в дисертації та виносяться на захист, отримано здобувачем особисто в період з 2022 по 2026 рік. У статті [1] внесок здобувача полягає у розробленні нечітких моделей основних компонентів бездротових сенсорних мереж - сенсорного вузла та каналу зв’язку - з урахуванням невизначеності параметрів їх функціонування, що дозволяє формалізувати лінгвістично описані характеристики та підвищити точність оцінювання станів системи . У статті [2] розроблено Методи опису мережі та оцінювання ризиків у межах багаторівневої онтології, що забезпечують інтегроване представлення параметрів БСМ, загроз і ризиків із урахуванням їх динаміки та взаємозв’язків . У статті [3] запропоновано Метод вразливості, який базується на системі логічних правил і призначений для виявлення слабких місць мережі, аналізу загроз та формування рекомендацій щодо зниження ризиків у реальному часі . У статті [4] удосконалено підхід до нечіткого моделювання сенсорного вузла та каналу зв’язку, зокрема за рахунок використання лінгвістичних змінних і ортогонального семантичного простору, що забезпечує гнучке представлення показників надійності та ефективності функціонування мережі . У статті [5] запропоновано інтегровану багаторівневу онтологічну модель управління ризиками, яка об’єднує метод семантичного виявлення та логування станів компонентів, Метод виявлення вразливостей та Метод оцінки ризиків у єдину адаптивну систему, що дозволяє здійснювати логічний висновок і підтримку прийняття рішень у процесі управління БСМ у промислових умовах.

Апробація результатів дисертації. Основні положення дисертаційної

роботи і результати її практичного застосування доповідалися на таких конференціях та були позитивно оцінені:

– II International Scientific and Practical Conference «Research work in the system of training teachers in technological fields». Berlin, Germany, January 2024;

– X Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна, вересня 2024;

– Modern Information Technology 2025/Сучасні Інформаційні Технології 2025. / Національний університет «Одеська політехніка». – Одеса, 2025;

– The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 4-6 September, 2025, Gliwice, Poland;

– The XIII International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST- ODESA – 2025) 24th – 26th September, 2025;

– XI Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна. Жовтень 2025;

– The 15th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2025 19-21 December, 2025, Athens, Greece;

Публікації. Основні результати дисертаційної роботи викладено в 5 публікаціях з них: 3 статей у наукових фахових виданнях України категорії «Б», 1 у наукових фахових виданнях України категорії «А» та проіндексовано у наукометричній базі Scopus, 1 публікацій у працях і матеріалах міжнародних наукових конференцій, яка проіндексована у наукометричній базі Scopus.

Структура і обсяг роботи. Дисертація складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації складає 216 сторінок, в тому числі: 160 сторінки основного тексту, 14 рисунки і 11 таблиць, список використаних джерел зі 109 найменувань і 4 додатків.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ДОСЛІДЖЕНЬ У ГАЛУЗІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

1.1 Бездротові сенсорні мережі як об’єкт дослідження

Бездротові сенсорні мережі (БСМ) є одним із ключових інструментів розподіленого моніторингу, автоматизованого збирання даних та інформаційної взаємодії в сучасних кіберфізичних і промислових системах. У загальному вигляді БСМ являє собою сукупність просторово розподілених автономних сенсорних вузлів, які здійснюють вимірювання параметрів об’єкта або середовища, виконують первинну обробку даних і передають отриману інформацію до базової станції, шлюзу або зовнішньої інформаційно-керуючої системи [2–4].

Основними компонентами БСМ є сенсорні вузли, канали бездротового зв’язку та вузол збору або обробки інформації. Сенсорний вузол зазвичай містить чутливий елемент, мікроконтролер або процесор, пам’ять, радіомодуль і джерело живлення. Канали зв’язку забезпечують передавання вимірювальних, службових і керуючих повідомлень між вузлами мережі. Базова станція або шлюз виконує функції збору, агрегації та передавання даних на вищі рівні обробки. Узагальнену схему бездротової сенсорної мережі наведено на рис. 1.1.

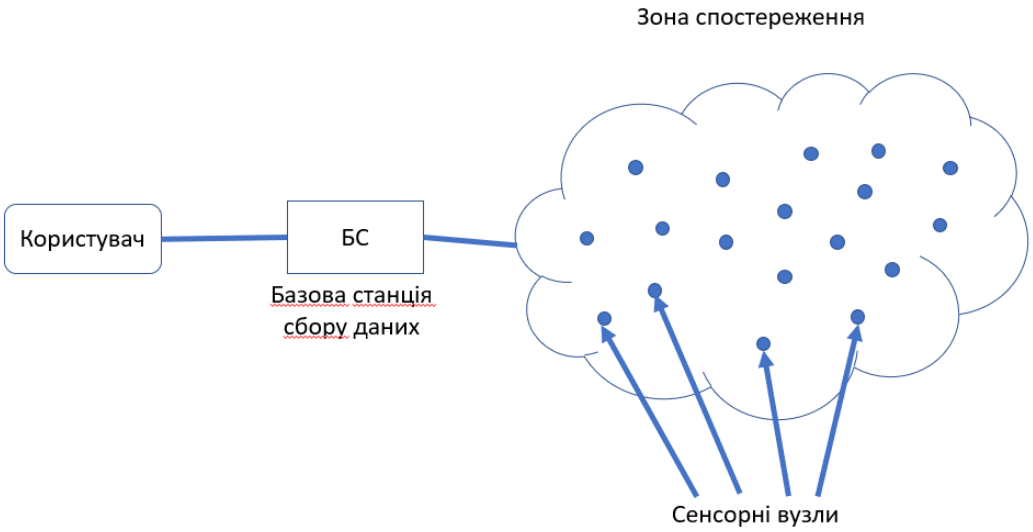

Рисунок 1.1 – Схематичне зображення БСМ

Застосування БСМ зумовлене потребою в оперативному отриманні даних у реальному часі, особливо в умовах просторової розосередженості об’єктів спостереження, складності прокладання дротової інфраструктури або необхідності автономного функціонування системи. Такі мережі використовуються в промисловому моніторингу, екологічному контролі, транспортних системах, системах безпеки, медицині, сільському господарстві та моніторингу критичної інфраструктури [7–10].

У промислових застосуваннях бездротові сенсорні мережі мають особливе значення, оскільки забезпечують контроль стану обладнання, спостереження за технологічними процесами, виявлення відхилень і передавання даних до систем автоматизації або диспетчеризації. У таких умовах до БСМ висуваються підвищені вимоги щодо надійності, своєчасності передавання даних, стійкості до завад, енергоефективності та безпеки [4], [7], [8], [10].

Водночас функціонування БСМ супроводжується низкою обмежень і факторів невизначеності. До них належать обмежений енергетичний ресурс сенсорних вузлів, змінність якості каналів зв’язку, втрати пакетів, затримки передавання, нерівномірність навантаження, вплив зовнішнього середовища, можливість відмов компонентів і наявність кіберзагроз [12–16], [28–32]. Унаслідок цього погіршення стану окремого вузла або каналу може впливати не лише на локальні параметри, а й на загальну працездатність мережі, особливо якщо такий компонент виконує важливу топологічну або функціональну роль.

Тому БСМ доцільно розглядати не лише як сукупність технічних пристроїв і каналів зв’язку, а як складну розподілену систему, стан якої визначається взаємодією структурних, параметричних, топологічних, енергетичних, комунікаційних і безпекових факторів. Такий підхід є важливим для подальшого аналізу вразливостей, оцінювання ризиків і формування рекомендацій щодо реагування на позаштатні ситуації. Саме тому в межах дисертаційного дослідження бездротова сенсорна мережа розглядається як

об’єкт ризик-орієнтованого аналізу, для якого необхідне узгоджене семантичне подання структури мережі, станів її компонентів, вразливостей і ризикових факторів.

1.1.1 Класифікація бездротових сенсорних систем

Класифікація бездротових сенсорних мереж дає змогу систематизувати їх за архітектурою, сферою застосування, способом передавання даних, характером розгортання, енергетичними можливостями вузлів, рівнем однорідності та вимогами до функціонування. Такий поділ є важливим для вибору протоколів маршрутизації, механізмів агрегації даних, підходів до керування ресурсами, оцінювання стану компонентів мережі та аналізу ризиків [2–4], [12–18], [84–86].

За архітектурою БСМ поділяють на плоскі, ієрархічні та кластерні. У плоских мережах усі вузли мають близькі функціональні можливості й виконують подібні задачі. Ієрархічні мережі передбачають розподіл ролей між вузлами, що дозволяє впорядкувати передавання даних і зменшити навантаження на окремі компоненти. Кластерні мережі є різновидом ієрархічних структур, у яких вузли об’єднуються в групи з виділенням головних вузлів кластерів, що виконують функції агрегації, обробки та передавання даних. Такий підхід широко застосовується в енергоефективних протоколах, зокрема в LEACH та його модифікаціях [13-18].

За сферою застосування виділяють промислові, екологічні, медичні, транспортні, військові та інфраструктурні БСМ. Найбільш важливими для даного дослідження є промислові бездротові сенсорні мережі, оскільки вони функціонують в умовах підвищених вимог до надійності, своєчасності передавання даних, стійкості до завад, енергоефективності та інформаційної безпеки [3],[4].

За способом передавання даних БСМ поділяють на однохопові, багатохопові, мережі з агрегацією даних та змішані. Однохопові мережі

забезпечують пряме передавання даних до базової станції, однак мають обмеження за радіусом дії та енергоспоживанням. Багатохопові мережі використовують проміжні вузли для ретрансляції повідомлень, що підвищує масштабованість, але ускладнює маршрутизацію та збільшує залежність від стану критичних вузлів. Мережі з агрегацією даних дозволяють зменшити обсяг передавання за рахунок попередньої обробки інформації безпосередньо в мережі [84-86].

За характером розгортання БСМ можуть бути планово або випадково розгорнутими, стаціонарними або мобільними. Планове розгортання характерне для промислових і інфраструктурних систем, де можливо заздалегідь визначити місця встановлення вузлів. Випадкове розгортання застосовується у складнодоступних або небезпечних середовищах. Стаціонарні мережі мають відносно стабільну топологію, тоді як мобільні потребують складніших механізмів самоорганізації та адаптивної маршрутизації [12-16].

За енергетичними можливостями виділяють мережі з обмеженим енергоживленням, мережі з енергозбиранням та гібридні мережі. Оскільки більшість сенсорних вузлів працює від автономних джерел живлення, енергетичний ресурс є одним із ключових обмежень БСМ. Це впливає на вибір маршрутизації, частоту передавання даних, обсяг локальної обробки та доцільність участі вузла в ретрансляції повідомлень [13-18].

За однорідністю вузлів БСМ поділяють на гомогенні та гетерогенні. У гомогенних мережах вузли мають близькі характеристики й виконують подібні функції. У гетерогенних мережах можуть бути вузли з різними ресурсами, ролями та функціональними можливостями, зокрема координатори, ретранслятори, агрегатори даних або вузли підвищеної потужності. Така структура дозволяє ефективніше розподіляти навантаження, але підвищує залежність мережі від критичних компонентів.

За вимогами до функціонування виділяють мережі реального часу, мережі з підвищеними вимогами до надійності, безпеки та якості

обслуговування. Для таких мереж важливими є затримка передавання, рівень втрат пакетів, стійкість до відмов, захищеність даних і здатність своєчасно реагувати на зміну стану середовища або компонентів мережі [84–86].

Таблиця 1.1 – Класифікація бездротових сенсорних мереж

Критерій класифікації	**Тип системи**	**Коротка характеристика**
За архітектурою мережі	Плоскі	Усі вузли мають близькі функціональні можливості та виконують подібні задачі.
	Ієрархічні	У мережі виділяються вузли з різними ролями, що забезпечує впорядковану організацію обміну даними.
	Кластерні	Вузли об’єднуються у кластери з виділенням головних вузлів для агрегації та передавання даних.
За сферою застосування	Промислові	Використовуються для моніторингу технологічних процесів, обладнання та виробничої інфраструктури
	Екологічні	Призначені для спостереження за параметрами довкілля: температурою, вологістю, забрудненням, сейсмічною активністю тощо
	Медичні	Використовуються для моніторингу фізіологічних параметрів людини та підтримки систем дистанційного медичного спостереження
	Транспортні	Застосовуються для контролю транспортних потоків, стану інфраструктури та підтримки інтелектуальних транспортних систем
	Військові та безпекові	Орієнтовані на розвідку, спостереження, виявлення загроз і захист критичних об’єктів
За способом передачі даних	Однохопові	Передавання інформації від вузла до базової станції здійснюється безпосередньо.
	Багатохопові	Дані передаються через проміжні вузли, які виконують функції ретрансляції.
	З агрегацією даних	У мережі виконується попереднє об’єднання, фільтрація або узагальнення даних перед їх передаванням.
	Змішані	Поєднують різні способи передавання залежно від топології мережі та умов функціонування.
За характером розгортання	Планово розгорнуті	Вузли розміщуються у заздалегідь визначених точках відповідно до проєкту мережі.
	Випадково розгорнуті	Вузли розміщуються без точного попереднього планування.
	Стаціонарні	Вузли залишаються нерухомими протягом усього періоду функціонування мережі.
	Мобільні	Частина вузлів або вузли збору даних можуть змінювати своє положення.

За енергетичними можливостями вузлів	З обмеженим енергоживленням	Вузли працюють від батарей або акумуляторів із фіксованим запасом енергії.
	З енергозбир'анням	Вузли можуть відновлювати енергію з навколишнього середовища.
	Гібридні	Поєднують батарейне живлення та механізми енергозбирання.
За однорідністю вузлів	Гомогенні	Усі вузли мають однакові або близькі апаратні й функціональні характеристики
	Гетерогенні	Мережа містить вузли з різними характеристиками, ролями та ресурсами.
За вимогами до функціонування	Реального часу	Потребують гарантованих затримок передавання та своєчасного реагування на події.
	З підвищеними вимогами до надійності	Орієнтовані на безперервну роботу за наявності відмов.
	З підвищеними вимогами до безпеки	Передбачають захист даних, аутентифікацію та виявлення атак..
	Із вимогами до QoS	Потребують забезпечення визначених параметрів якості обслуговування: затримки, пропускної здатності, втрат пакетів.

Узагальнення наведених класифікацій дозволяє виділити основні архітектурні, прикладні, енергетичні та експлуатаційні особливості БСМ. Для задач ризик-орієнтованого аналізу особливе значення мають структура мережі, спосіб передавання даних, енергетичні обмеження, топологічна роль вузлів і вимоги до надійності та безпеки.

1.1.2 Архітектура та основні компоненти бездротових сенсорних мереж

Архітектура бездротової сенсорної мережі визначає спосіб організації вузлів, порядок їх взаємодії та передавання даних до базової станції або зовнішньої інформаційно-керуючої системи. Незалежно від конкретного типу побудови, БСМ зазвичай включає сенсорні вузли, канали бездротового зв’язку та вузол збору або обробки інформації [56–59].

Сенсорний вузол є базовим елементом мережі та виконує функції вимірювання, первинної обробки і передавання даних. Його типовими складовими є сенсорний елемент, обчислювальний Метод, радіомодуль, пам’ять і джерело живлення. Обмеженість енергетичного ресурсу, обчислювальних можливостей і

радіоканалу визначає специфіку функціонування вузла та впливає на надійність усієї мережі [56–59].

Канал зв’язку забезпечує обмін даними між вузлами та базовою станцією. Його стан характеризується пропускною здатністю, затримкою, втратами пакетів, доступністю та стійкістю до завад. У БСМ канал є одним із найбільш чутливих компонентів, оскільки залежить від топології мережі, навантаження, зовнішніх перешкод і умов середовища [63-65].

Базова станція або шлюз виконує функції збору, агрегації та передавання даних на вищий рівень обробки. У промислових БСМ цей компонент може забезпечувати взаємодію сенсорної мережі з системами моніторингу, диспетчеризації або керування [63–65].

Для ризик-орієнтованого аналізу важливо враховувати не лише склад компонентів БСМ, а й їхню роль у топології мережі. Відмова окремого вузла, ретранслятора, каналу або шлюзу може мати різні наслідки залежно від його функціонального призначення, навантаження та участі в маршрутах передавання даних. Тому архітектурний опис БСМ має включати зв’язки між компонентами, їхні параметри стану та критичність для функціонування мережі.

Отже, архітектура БСМ формує основу для подальшого аналізу її надійності, вразливостей і ризиків. Структурні зв’язки між сенсорними вузлами, каналами зв’язку та вузлами збору даних визначають початкову базу для побудови онтологічної моделі, у якій стан мережі подається як сукупність взаємопов’язаних компонентів, параметрів і ризикових факторів.

1.1.3 Особливості функціонування бездотових сенсорних мереж у промислових умовах

Функціонування бездротових сенсорних мереж у промислових умовах має низку особливостей, які відрізняють їх від БСМ загального призначення. Промислове середовище характеризується наявністю електромагнітних завад, металевих конструкцій, рухомих механізмів, температурних коливань і складної просторової структури об’єктів. Такі фактори впливають на якість бездротового

зв’язку, стабільність передавання даних і надійність функціонування мережі [4], [7-10].

Однією з основних проблем промислових БСМ є нестабільність каналів зв’язку. Електромагнітні перешкоди, багатопроменеве поширення сигналу, затінення та зміна навантаження можуть призводити до втрат пакетів, збільшення затримок і зниження пропускної здатності. Унаслідок цього навіть локальне погіршення стану окремого каналу може впливати на роботу значної частини мережі, особливо якщо цей канал належить до критичного маршруту передавання даних [81-83].

Для промислових БСМ також характерні підвищені вимоги до своєчасності та достовірності даних. У системах моніторингу технологічних процесів, обладнання або критичної інфраструктури затримка повідомлень, втрата даних або відмова вузлів можуть призвести до неправильного оцінювання стану об’єкта. Тому під час аналізу таких мереж необхідно враховувати не лише факт передавання даних, а й якість каналу, затримку, рівень втрат, навантаження та роль окремих вузлів у маршрутах передавання [81-83].

Окреме значення має енергетичне обмеження сенсорних вузлів. У промислових умовах не завжди можливо регулярно обслуговувати або замінювати джерела живлення, тому енергоресурс вузлів впливає на тривалість роботи мережі, частоту передавання даних і можливість виконання функцій ретрансляції. Особливо критичними є вузли, через які проходить значна частина трафіку, оскільки їх деградація або виснаження може порушити зв’язність мережі [7-10], [81-83].

Промислові БСМ також є вразливими до кіберзагроз і несанкціонованого впливу. До типових проблем належать підміна даних, порушення автентичності вузлів, атаки на маршрутизацію, відмова в обслуговуванні, глушіння каналу та втручання в процес передавання повідомлень. Оскільки такі мережі можуть бути інтегровані з системами моніторингу, диспетчеризації або керування, порушення їх роботи здатне впливати не лише на інформаційний рівень, а й на фізичні процеси промислового об’єкта [4].

З огляду на це, промислові БСМ слід розглядати як системи, що функціонують під одночасним впливом технічних, середовищних, енергетичних і безпекових обмежень. Саме поєднання цих факторів обґрунтовує необхідність комплексного аналізу стану мережі з урахуванням параметрів вузлів і каналів, топологічної ролі компонентів, вразливостей та потенційних ризиків.

1.2 Аналіз методів організацій функціонування бездротових сенсорних мереж

Організація функціонування бездротових сенсорних мереж охоплює сукупність методів, спрямованих на забезпечення ефективного збирання, передавання та обробки даних за умов обмежених ресурсів сенсорних вузлів. До таких методів належать кластеризація, маршрутизація, агрегація даних, балансування навантаження, керування енергоспоживанням, підтримка якості обслуговування та адаптація мережі до зміни умов функціонування [68–72].

Одним із базових підходів є кластеризація, яка передбачає об’єднання вузлів у групи з виділенням кластерних голів. Такий підхід дозволяє зменшити кількість прямих передавань до базової станції, скоротити обсяг дубльованих даних і підвищити енергоефективність мережі. Саме на цьому принципі ґрунтується протокол LEACH та його численні модифікації [20-25].

Маршрутизація в БСМ визначає порядок передавання даних від сенсорних вузлів до базової станції або шлюзу. На відміну від традиційних комп’ютерних мереж, маршрутизація в БСМ повинна враховувати залишкову енергію вузлів, якість каналів зв’язку, кількість проміжних передавань, рівень навантаження та вимоги до своєчасності доставки повідомлень [68–72].

Важливим методом підвищення ефективності БСМ є агрегація даних, що передбачає попереднє об’єднання, фільтрацію або узагальнення інформації безпосередньо в мережі. Це дозволяє зменшити обсяг передавання, знизити навантаження на канали зв’язку та продовжити час функціонування мережі. Водночас застосування агрегації потребує врахування достовірності даних, ролі вузлів-агрегаторів і можливих наслідків їх відмови [68–72].

У промислових БСМ особливого значення набувають методи забезпечення надійності, своєчасності передавання та стійкості до завад. Для таких мереж важливими є планування доступу до середовища, контроль затримок, підтримка резервних маршрутів і врахування обмежень промислових протоколів бездротового зв’язку, зокрема WirelessHART [81–83].

Окрему групу становлять інтелектуальні та нечіткі методи організації роботи БСМ. Вони застосовуються для вибору кластерних голів, оптимізації маршрутизації, оцінювання стану вузлів і каналів, а також прийняття рішень в умовах неповноти або невизначеності даних [20–25].

Підсумовуючи, методи організації функціонування БСМ спрямовані на підвищення енергоефективності, надійності, масштабованості та стійкості мережі. Однак більшість таких методів розв’язує окремі технічні задачі й не забезпечує цілісного подання стану мережі, її вразливостей і ризиків, що створює передумови для переходу до ризик-орієнтованого аналізу.

1.2.1 Методи кластеризації бездротових сенсорних мереж

Кластеризація є одним із базових підходів до організації функціонування бездротових сенсорних мереж. Її сутність полягає в об’єднанні сенсорних вузлів у групи - кластери, у межах яких виділяється головний вузол, або кластерна голова. Такий вузол виконує функції збору, попередньої обробки, агрегації та передавання даних до базової станції або вузлів вищого рівня [13-18].

Застосування кластеризації дозволяє зменшити кількість прямих передавань до базової станції, скоротити обсяг дубльованих даних, знизити навантаження на канали зв’язку та підвищити енергоефективність мережі. Особливо важливим цей підхід є для масштабованих БСМ, у яких велика кількість вузлів функціонує з обмеженим енергетичним ресурсом [13–18].

Методи кластеризації можуть відрізнятися за критеріями вибору кластерних голів, способом формування кластерів, періодичністю перебудови структури та ступенем централізації керування. У найпростішому випадку кластерні голови обираються випадково або за наперед заданими правилами. У більш складних

підходах враховуються залишкова енергія вузла, відстань до базової станції, кількість сусідів, рівень навантаження, якість каналів зв’язку та топологічне положення вузла [13–18].

Одним із найбільш відомих кластерних протоколів є LEACH (Low Energy Adaptive Clustering Hierarchy). Він належить до ієрархічних енергоефективних протоколів і передбачає динамічне формування кластерів із періодичною зміною кластерних голів. Робота LEACH включає фазу формування кластерів і фазу передавання даних. На першій фазі обираються кластерні голови та формуються групи вузлів, а на другій - сенсорні вузли передають дані до кластерної голови, яка виконує агрегацію та надсилає узагальнену інформацію до базової станції [14], [17], [18].

Перевагою LEACH є зменшення кількості прямих передавань, локалізація обміну даними в межах кластерів і більш рівномірний розподіл енергетичного навантаження між вузлами. Водночас базовий варіант протоколу має обмеження, оскільки вибір кластерних голів має ймовірнісний характер і не завжди враховує залишкову енергію вузлів, їх розташування, поточне навантаження, якість каналів зв’язку та топологічну роль у мережі [17], [18].

Для усунення цих недоліків запропоновано численні модифікації LEACH, які враховують енергетичні, топологічні, комунікаційні та контекстні параметри мережі. Такі модифікації можуть використовувати багатохопове передавання, гетерогенність вузлів, адаптивну зміну кластерних голів, а також критерії залишкової енергії, відстані до базової станції, щільності сусідів і якості каналів зв’язку [14], [17], [18].

Окрему групу становлять нечіткі та інтелектуальні методи кластеризації. Вони дозволяють одночасно враховувати декілька неоднорідних параметрів і приймати рішення в умовах неповної або невизначеної інформації. Зокрема, нечітка логіка може застосовуватися для вибору кластерних голів на основі залишкової енергії, відстані, щільності вузлів, навантаження, якості каналу та очікуваної ролі вузла в мережі.

Разом із перевагами кластеризація має певні обмеження. До них належать

додаткові витрати на формування та підтримку кластерів, складність вибору оптимальних кластерних голів, ризик їх перевантаження та швидкого виснаження енергетичного ресурсу. Крім того, відмова кластерної голови може порушити функціонування всього кластера або призвести до втрати частини даних.

Отже, кластеризація та протоколи типу LEACH є ефективними засобами підвищення енергоефективності, масштабованості та керованості БСМ. У межах ризик-орієнтованого аналізу особливу увагу слід приділяти вузлам, що виконують функції кластерних голів, агрегаторів або ретрансляторів, оскільки саме вони можуть набувати критичної ролі в топології мережі.

1.2.2 Методи маршрутизації та агрегації у бездротових сенсорних мережах

Маршрутизація та агрегація даних є ключовими механізмами організації функціонування бездротових сенсорних мереж. Вони визначають порядок передавання інформації від сенсорних вузлів до базової станції, рівень навантаження на мережу, енергоспоживання вузлів, затримки та надійність доставки повідомлень [11] [56-59].

На відміну від традиційних комп’ютерних мереж, маршрутизація в БСМ має враховувати обмежений енергетичний ресурс вузлів, змінність якості каналів зв’язку, втрати пакетів, кількість проміжних передавань, топологію мережі та вимоги до своєчасності доставки даних. Тому вибір маршруту в таких мережах пов’язаний не лише з пошуком найкоротшого шляху, а й з необхідністю балансування навантаження та збереження працездатності мережі протягом тривалого часу [13-16].

У БСМ застосовуються різні підходи до маршрутизації: плоскі, ієрархічні, кластерні, географічні, енергоорієнтовані, QoS-орієнтовані та адаптивні. Плоскі підходи передбачають рівноправну участь вузлів у передаванні даних, тоді як ієрархічні та кластерні використовують вузли з особливими ролями, наприклад кластерні голови або ретранслятори. QoS-орієнтовані методи додатково враховують затримку, пропускну здатність, рівень втрат пакетів і вимоги реального

часу [84-86].

Агрегація даних передбачає попереднє об’єднання, фільтрацію або узагальнення інформації безпосередньо в мережі перед її передаванням до базової станції. Це дозволяє зменшити обсяг трафіку, скоротити кількість передавань, знизити навантаження на канали зв’язку та продовжити час функціонування мережі. Найчастіше агрегація використовується в кластерних та ієрархічних архітектурах, де відповідні функції виконують кластерні голови або спеціалізовані вузли-агрегатори [11], [13–16].

Разом із тим маршрутизація та агрегація створюють додаткові точки критичності в мережі. Вузли, які виконують функції ретрансляції або агрегації, можуть отримувати підвищене навантаження та швидше втрачати енергетичний ресурс. Відмова такого вузла або погіршення стану каналу на критичному маршруті може призвести до втрати частини даних, збільшення затримок або порушення зв’язності окремого сегмента мережі.

Окрему групу становлять інтелектуальні та нечіткі методи маршрутизації. Вони дають змогу враховувати декілька параметрів одночасно, зокрема залишкову енергію вузлів, якість каналу, відстань, навантаження, затримку та рівень безпеки. Такі підходи є доцільними в умовах невизначеності, коли параметри мережі змінюються або не можуть бути точно оцінені [84-86].

Для промислових БСМ особливе значення мають методи, що забезпечують передбачуваність затримок, надійність передавання та планування доступу до середовища. Це пов’язано з використанням таких мереж у системах моніторингу технологічних процесів, де несвоєчасна доставка даних або втрата повідомлень може вплинути на правильність оцінювання стану об’єкта [81–86].

З наведеного випливає, що маршрутизація та агрегація даних підвищують ефективність БСМ, однак водночас формують додаткові точки критичності. Для ризик-орієнтованого аналізу важливо враховувати не лише метрики маршруту, а й топологічну роль вузлів, критичність каналів, можливі вразливості та наслідки деградації окремих компонентів мережі.

1.3 Аналіз підходів до підвищення енергоефективності, надійності та стійкості БСМ

Ефективність функціонування бездротових сенсорних мереж значною мірою визначається їх здатністю тривалий час підтримувати працездатність вузлів, забезпечувати надійне передавання даних і зберігати стійкість до зовнішніх та внутрішніх дестабілізуючих чинників. Для бездротових сенсорних мереж ці характеристики є взаємопов’язаними, оскільки обмежений енергетичний ресурс вузлів, зміна якості каналів зв’язку, нерівномірність навантаження та вплив середовища можуть одночасно знижувати енергоефективність, надійність і загальну стійкість мережі [13–18].

До основних підходів підвищення енергоефективності належать зменшення обсягу передаваних даних, агрегація інформації, оптимізація маршрутів, балансування навантаження та використання режимів енергозбереження. Такі методи дозволяють продовжити час життя мережі, однак не усувають повністю ризик перевантаження окремих вузлів, особливо тих, що виконують функції ретрансляції, агрегації або кластерних голів [63-72].

Надійність і відмовостійкість БСМ забезпечуються за рахунок резервування маршрутів, використання альтернативних шляхів передавання, дублювання критичних функцій, моніторингу стану вузлів і каналів, а також адаптивної перебудови мережі у разі деградації окремих компонентів. У промислових умовах ці підходи мають особливе значення, оскільки втрата даних, зростання затримок або відмова критичного вузла можуть впливати на коректність оцінювання стану об’єкта [63–72].

Стійкість БСМ також пов’язана з безпекою та здатністю мережі протидіяти зовнішнім впливам. До таких впливів належать електромагнітні завади, фізичні пошкодження вузлів, нестабільність середовища передавання, перевантаження каналів, а також кібератаки, спрямовані на перехоплення, підміну, Методування або спотворення даних [28–37].

У контексті цього дослідження енергоефективність, надійність і стійкість БСМ доцільно розглядати як взаємопов’язані характеристики, що визначають

можливість тривалого та безпечного функціонування мережі. Їх аналіз потребує врахування стану вузлів і каналів, топологічної ролі компонентів, впливу середовища та можливих вразливостей.

1.3.1 Методи зменшення енергоспоживання та балансування навантаження в БСМ

Енергоефективність є однією з ключових вимог до бездротових сенсорних мереж, оскільки більшість сенсорних вузлів працює від автономних джерел живлення. Обмеженість енергетичного ресурсу впливає на тривалість функціонування вузлів, частоту передавання даних, можливість виконання ретрансляції та загальний час життя мережі [71],[72], [83].

Основними підходами до підвищення енергоефективності БСМ є зменшення кількості передавань, оптимізація маршрутів, агрегація даних, балансування навантаження, використання енергоощадних режимів роботи вузлів, а також кластерна організація мережі, зокрема на основі протоколів типу LEACH [13–18].

Маршрутизаційні методи підвищення енергоефективності орієнтовані на вибір таких шляхів передавання, які враховують залишкову енергію вузлів, кількість проміжних передавань, якість каналів зв’язку та поточне навантаження. Це дозволяє уникати надмірного використання окремих вузлів і зменшувати ризик їх передчасногоавання, які враховують залишкову енергію вузлів, кількість проміжних передавань, якість каналів зв’язку та поточне навантаження. виснаження [71],[72], [83].

Окрему групу становлять нечіткі та інтелектуальні підходи, у яких рішення щодо вибору кластерних голів, маршрутів або режимів роботи приймаються з урахуванням кількох параметрів одночасно. До таких параметрів можуть належати залишкова енергія, відстань до базової станції, щільність вузлів, навантаження, якість каналу та очікувана роль вузла в мережі [20–25], [71], [72].

Разом із тим більшість енергоефективних методів орієнтована переважно на подовження часу життя мережі або зменшення обсягу передаваного трафіку. Вони не завжди враховують, що енергетичне виснаження окремого вузла може мати різні

наслідки залежно від його топологічної ролі. Наприклад, деградація звичайного периферійного вузла і деградація вузла-ретранслятора або кластерної голови мають різний вплив на працездатність БСМ [71], [72], [83].

Отже, енергоефективність у БСМ слід розглядати не лише як задачу економії енергії, а і як фактор надійності та ризику. Для ризик-орієнтованого аналізу важливо враховувати залишковий енергетичний ресурс вузлів, швидкість його виснаження, навантаження на компоненти та їхню роль у маршрутах передавання даних.

1.3.2 Методи забезпечення надійності, відмовостійкості та безпеки бездротових сенсорних мереж

Надійність бездротової сенсорної мережі визначає її здатність зберігати працездатність за умов відмов окремих вузлів, погіршення якості каналів зв’язку, втрат пакетів, перевантаження маршрутів, впливу зовнішнього середовища або несанкціонованого втручання. Для БСМ ця характеристика є особливо важливою, оскільки сенсорні вузли мають обмежені енергетичні, обчислювальні та комунікаційні ресурси, а якість бездротового зв’язку може змінюватися в часі [63–72], [81–83].

Основними підходами до підвищення надійності та відмовостійкості БСМ є використання резервних маршрутів, дублювання критичних функцій, адаптивна перебудова топології, контроль стану вузлів і каналів зв’язку, а також балансування навантаження між компонентами мережі. Такі методи дозволяють зменшити вплив локальних відмов на загальне функціонування мережі та підтримувати передавання даних навіть у разі деградації окремих елементів [63–72], [81–83].

Відмовостійкість БСМ значною мірою залежить від топологічної ролі вузлів. Відмова периферійного сенсорного вузла може призвести лише до втрати частини вимірювальних даних, тоді як відмова ретранслятора, кластерної голови, вузла-агрегатора або каналу на критичному маршруті може порушити зв’язність цілого сегмента мережі. Тому під час аналізу надійності необхідно враховувати не лише

факт відмови компонента, а й його місце в структурі БСМ, участь у маршрутах передавання та рівень поточного навантаження [81–83].

У промислових бездротових сенсорних мережах додаткового значення набувають вимоги до своєчасності, гарантованості та достовірності передавання повідомлень. Затримки, втрати пакетів, нестабільність маршруту або порушення планування доступу до середовища можуть призвести до несвоєчасного виявлення аварійного чи передаварійного стану об’єкта. Тому в таких мережах застосовуються механізми планування передавання, контролю якості обслуговування, резервування маршрутів і підтримки стабільної взаємодії між вузлами [63–65], [68–70].

Безпека БСМ є складовою їх загальної стійкості, оскільки порушення автентичності, цілісності або доступності даних може призвести до некоректного оцінювання стану мережі чи об’єкта моніторингу. До типових загроз належать підміна даних, несанкціоноване приєднання вузлів, атаки на маршрутизацію, глушіння каналу, відмова в обслуговуванні, перехоплення повідомлень і спотворення службової інформації [89-100].

Окрему роль відіграє моніторинг стану компонентів мережі. Поточні значення залишкової енергії, затримки, втрат пакетів, пропускної здатності, рівня навантаження, доступності каналів і ознак безпекових порушень дозволяють виявляти деградацію до виникнення повної відмови. Це створює основу для раннього визначення критичних компонентів і формування рекомендацій щодо зміни режиму роботи, перерозподілу навантаження, використання альтернативних маршрутів або посилення моніторингу [89-100].

Разом із тим більшість методів забезпечення надійності, відмовостійкості та безпеки зосереджується на окремих технічних механізмах: резервуванні, перебудові маршрутів, контролі втрат, QoS-маршрутизації, виявленні атак або балансуванні навантаження. Такі підходи не завжди забезпечують цілісне пояснення причин деградації мережі та не пов’язують поточний стан компонентів із вразливостями й ризиками.

Узагальнюючи, надійність, відмовостійкість і безпека БСМ мають розглядатися як взаємопов’язані складові ризик-орієнтованого аналізу. Такий підхід передбачає врахування стану вузлів і каналів, їхньої топологічної ролі, навантаження, можливих відмов, зовнішніх впливів, безпекових загроз і наслідків деградації для мережі загалом.

1.4 Аналіз методів виявлення вразливостей, загроз та оцінювання ризиків у БСМ

Сучасні бездротові сенсорні мережі функціонують у складних умовах, що зумовлює їх підвищену вразливість до випадкових відмов, зовнішніх впливів і цілеспрямованих атак. Обмеженість ресурсів сенсорних вузлів, відкритість бездротового середовища, динамічність топології та нестабільність каналів зв’язку ускладнюють своєчасне виявлення вразливостей, ідентифікацію загроз та оцінювання ризиків [66], [67].

На відміну від традиційних інформаційно-комунікаційних систем, аналіз ризиків у БСМ має враховувати як технічні фактори, так і загрози інформаційній безпеці. До технічних факторів належать відмови вузлів, деградація каналів, втрата зв’язності, перевантаження маршрутів і виснаження енергетичного ресурсу. До безпекових загроз належать перехоплення, підміна, Методування або спотворення даних, а також атаки на маршрутизацію та доступність мережі [87–100].

Існуючі підходи до виявлення вразливостей і загроз включають аналіз архітектури мережі, оцінювання стану вузлів і каналів, моніторинг трафіку, системи виявлення вторгнень, сценарний аналіз, а також якісні, кількісні та гібридні методи оцінювання ризиків [19], [45–55]. У таких підходах можуть використовуватися ймовірнісні моделі, нечітка логіка та інтелектуальні методи обробки даних, що дозволяє враховувати невизначеність і неповноту інформації [45–55], [73–80].

Водночас більшість наявних методів має обмеження, пов’язані з недостатнім урахуванням взаємозв’язків між компонентами БСМ, динаміки зміни станів мережі, впливу середовища та складності інтеграції різнорідних даних. Часто

вузли, канали, загрози та наслідки їх реалізації розглядаються ізольовано, що ускладнює формування цілісної оцінки ризику [45–55], [73–80],.

Отже, аналіз методів виявлення вразливостей, загроз та оцінювання ризиків є необхідним етапом дослідження БСМ. Він дозволяє визначити обмеження існуючих підходів і обґрунтувати потребу в моделях, здатних формалізовано описувати структуру мережі, стан її компонентів, вразливості, загрози та ризикові фактори у взаємозв'язку.

1.4.1 Основні типи вразливостей і загроз у бездротових сенсорних мережах

Бездротові сенсорні мережі мають підвищену вразливість до різних типів загроз, що зумовлено їх розподіленою структурою, обмеженими ресурсами вузлів і використанням відкритого бездротового середовища передавання даних. Вразливості можуть виникати на фізичному, канальному, мережевому, протокольному та прикладному рівнях, тому їх аналіз потребує комплексного підходу [87–100].

Фізичні вразливості пов'язані з можливістю безпосереднього впливу на сенсорні вузли. Оскільки вузли часто розміщуються у відкритому, промисловому або важкодоступному середовищі, вони можуть зазнавати механічного пошкодження, несанкціонованого доступу, заміни або виведення з ладу. Наслідком таких впливів може бути втрата функціональності вузла, спотворення вимірювань або компрометація даних [28–37].

Комунікаційні вразливості пов'язані з перехопленням сигналів, глушінням каналу, затримкою, викривленням або підміною повідомлень. Мережеві та протокольні загрози охоплюють атаки на маршрутизацію, створення хибних маршрутів, маніпулювання службовою інформацією та порушення взаємодії між вузлами [28–37].

Мережеві та протокольні вразливості пов'язані з особливостями маршрутизації, кластеризації та керування мережею. До цієї групи належать атаки на маршрутизацію, створення хибних маршрутів, формування фальшивих вузлів,

маніпулювання службовою інформацією та порушення взаємодії між компонентами мережі. Такі дії можуть призводити до втрати даних, перевантаження окремих вузлів, порушення зв’язності або зниження ефективності функціонування БСМ [87–100].

Окрему групу становлять енергетичні вразливості, характерні саме для БСМ. Зловмисні або некоректні дії можуть бути спрямовані на прискорене виснаження енергетичних ресурсів вузлів, наприклад через надмірну кількість запитів, примушування до частих передавань або перевантаження вузлів-ретрансляторів. У результаті окремі компоненти мережі можуть швидко втрачати працездатність, що особливо небезпечно для вузлів із критичною топологічною роллю [28–37].

Інформаційні загрози пов’язані з порушенням конфіденційності, цілісності та доступності даних. Перехоплення, модифікація, затримка або Методування інформації можуть призвести до некоректного оцінювання стану об’єкта моніторингу, помилкових керуючих рішень або втрати довіри до даних, що надходять від мережі [87–100].

Проведена систематизація показує, що вразливості та загрози БСМ мають багаторівневий характер і можуть впливати на вузли, канали зв’язку, маршрути передавання, службову інформацію та дані моніторингу. Їх урахування є основою для подальшого оцінювання ризиків, оскільки дозволяє пов’язати джерела загроз, вразливі компоненти мережі та можливі наслідки для її функціонування.

1.4.2 Підходи до оцінювання ризиків у бездротових сенсорних мережах

Оцінювання ризиків є важливим етапом забезпечення надійного та безпечного функціонування БСМ. У загальному вигляді ризик розглядається як поєднання ймовірності виникнення небажаної події та її можливих наслідків. Для БСМ такими наслідками можуть бути втрата даних, зниження якості обслуговування, порушення цілісності інформації, деградація окремих компонентів або повна відмова мережі [19], [28–37].

Існуючі підходи до оцінювання ризиків можна поділити на якісні, кількісні та гібридні. Якісні методи ґрунтуються на експертних оцінках і дозволяють класифікувати ризики за рівнем критичності. Кількісні методи використовують математичні моделі для оцінювання ймовірності загроз і величини їх наслідків. Гібридні підходи поєднують експертні оцінки з формалізованими розрахунками, що дає змогу враховувати як числові, так і якісні характеристики ризику [45–55, 73–80].

Окремий напрям становлять стандартизовані та сценарно-модельні підходи до аналізу ризиків, зокрема CORAS, NIST-орієнтовані методики та STPA-Sec. CORAS забезпечує побудову сценаріїв ризику та графічне подання взаємозв’язків між загрозами, вразливостями й наслідками. Підходи NIST орієнтовані на системне управління кіберризиками, а STPA-Sec дозволяє аналізувати небезпечні сценарії у складних кіберфізичних системах [19], [45–55].

У практиці аналізу БСМ також застосовуються ймовірнісні моделі, зокрема підходи на основі теорії надійності, марковських процесів і байєсівських мереж. Вони дають змогу враховувати випадковий характер відмов і взаємозв’язки між подіями, однак потребують достовірних статистичних даних. За умов неповної або нечіткої інформації доцільним є використання нечіткої логіки, яка дозволяє формалізувати експертні знання та працювати з лінгвістичними оцінками стану вузлів, каналів і рівня ризику [45–55], [73–80].

Попри різноманітність підходів, оцінювання ризиків у БСМ залишається складною багатофакторною задачею. Основними обмеженнями існуючих методів є неповне врахування динаміки мережі, взаємозв’язків між компонентами, контексту функціонування та різнорідності даних. Це обґрунтовує потребу в моделях, здатних поєднувати технічні параметри вузлів і каналів, вразливості, загрози та наслідки їх реалізації в єдиному формалізованому поданні.

1.4.3 Обмеження існуючих методів аналізу вразливостей і ризиків у БСМ

Незважаючи на значну кількість досліджень у сфері виявлення вразливостей і оцінювання ризиків у БСМ, існуючі підходи мають низку обмежень, що ускладнюють їх застосування в реальних умовах. Однією з основних проблем є недостатнє врахування взаємозв'язків між вузлами, каналами зв'язку, маршрутами, загрозами та наслідками їх реалізації. У багатьох методах ці елементи розглядаються ізольовано, що не дозволяє повною мірою оцінити вплив локальної деградації на стан мережі загалом [73–80].

Іншим обмеженням є складність інтеграції різнорідних даних. Для аналізу ризиків необхідно одночасно враховувати технічні параметри вузлів і каналів, характеристики середовища, топологічну роль компонентів, ознаки загроз та експертні оцінки. Відсутність єдиного формату подання таких даних ускладнює їх узгодження та використання в межах цілісної моделі ризику [45–55].

Багато існуючих методів також мають обмежену адаптивність до змін умов функціонування БСМ. Статичні моделі не завжди враховують динаміку топології, зміну якості каналів, виснаження енергетичного ресурсу вузлів, появу нових загроз або зміну навантаження. Через це результати оцінювання ризиків можуть швидко втрачати актуальність [66–67].

Окремою проблемою є недостатня формалізація та пояснюваність результатів. Якщо метод не показує, які саме параметри, зв'язки або події призвели до певного рівня ризику, його складно використовувати для підтримки прийняття рішень у критичних системах. Це обмежує практичну цінність таких підходів для промислових БСМ, де важливо не лише визначити рівень ризику, а й пояснити причини його виникнення [45–55].

Зазначені обмеження обґрунтовують необхідність переходу до формалізованих семантичних та онтологічних моделей. Такі моделі дають змогу поєднати опис структури мережі, стану її компонентів, вразливостей, загроз і

ризикових факторів у єдиному узгодженому поданні, що є основою для подальшого ризик-орієнтованого аналізу БСМ.

1.5 Семантичні та онтологічні підходи до побудові станів бездротових сенсорних мереж

Семантичні та онтологічні підходи є одним із напрямів формалізованого опису складних розподілених систем, до яких належать бездротові сенсорні мережі. Їх використання дозволяє подати БСМ не лише як сукупність вузлів і каналів зв'язку, а як систему взаємопов'язаних компонентів, станів, параметрів, подій, вразливостей і загроз [38–44], [46].

На відміну від суто числових або ймовірнісних моделей, онтології забезпечують структуроване подання знань про предметну область. Вони дозволяють описувати класи об'єктів, властивості, відношення між компонентами мережі, а також правила логічного висновку. Це є важливим для задач аналізу БСМ, оскільки стан мережі формується під впливом різнорідних факторів: технічних параметрів вузлів, характеристик каналів, умов середовища, топологічних ролей компонентів і потенційних загроз [38–44].

У сфері сенсорних мереж та Інтернету речей застосовуються різні семантичні моделі й онтології, зокрема SSN/SOSA, IoT-Lite та спеціалізовані онтології кібербезпеки. Вони використовуються для опису сенсорів, спостережень, вимірюваних величин, пристроїв, сервісів, а також загроз, вразливостей і ризикових ситуацій [97–99].

Для ризик-орієнтованого аналізу БСМ особливе значення має здатність онтологічних моделей поєднувати технічні, контекстні та безпекові аспекти в єдиному поданні. Це створює основу для виявлення залежностей між станом вузлів і каналів, топологічною роллю компонентів, наявними вразливостями та можливими наслідками їх реалізації [97–99].

Попри переваги, онтологічні підходи потребують чіткого визначення структури предметної області, формалізації понять і відношень, а також підтримки узгодженості моделі. Тому для БСМ доцільним є використання багаторівневої

онтологічної моделі, яка дозволяє описати мережу, її компоненти, поточні стани, вразливості, загрози та ризики як взаємопов’язані елементи єдиної системи.

1.5.1 Формальні та семантичні моделі представлення знань про БСМ

Формальні моделі використовуються для опису структури, станів і взаємозв’язків компонентів бездротових сенсорних мереж. До них належать математичні, логічні та графові моделі, які дозволяють подати вузли, канали зв’язку, маршрути та параметри функціонування у вигляді формалізованих об’єктів і відношень [38–44], [46].

Графові моделі є зручними для опису топології БСМ, де сенсорні вузли подаються як вершини, а канали зв’язку - як ребра. Логічні моделі дозволяють формалізувати правила функціонування мережі та залежності між її компонентами. Водночас такі підходи часто орієнтовані на окремі задачі й мають обмежені можливості щодо інтеграції різнорідних знань, контексту функціонування та безпекових факторів [38–44], [49–52].

Семантичні моделі розширюють можливості формального опису за рахунок урахування змісту інформації та зв’язків між її елементами. Вони дозволяють описувати не лише об’єкти мережі, а й їхні властивості, стани, взаємодії та контекст використання. Це є важливим для аналізу БСМ, де технічні параметри вузлів і каналів мають розглядатися разом із умовами середовища, вразливостями та потенційними ризиками [38–44], [49–52].

Основою семантичного представлення знань є технології семантичного вебу, зокрема RDF, RDFS та OWL. Вони забезпечують формальний опис класів, властивостей і відношень між об’єктами предметної області, придатний для машинної обробки. Для формалізації правил і отримання нових знань можуть використовуватися механізми логічного висновку та мови правил, зокрема SWRL [46], [49–52].

Попри переваги, формальні та семантичні моделі мають обмеження. Їх побудова потребує чіткого визначення понять, відношень і правил, а також

підтримки узгодженості моделі. Для складних систем, таких як БСМ, це ускладнюється великою кількістю параметрів, динамікою станів і необхідністю врахування різнорідних джерел даних [49–52].

Отже, формальні та семантичні моделі створюють основу для структурованого подання знань про БСМ, однак для задач ризик-орієнтованого аналізу їх доцільно розвивати в напрямі онтологічних моделей, здатних поєднувати опис компонентів мережі, їхніх станів, вразливостей, загроз і ризикових факторів.

1.5.2 Онтологічні підходи до опису структури та станів бездротових сенсорних мереж

Онтологічні підходи дають змогу формалізувати знання про бездротову сенсорну мережу як систему взаємопов’язаних компонентів, параметрів і станів. На відміну від традиційних моделей, онтологія описує не лише окремі елементи БСМ, а й семантичні зв’язки між ними, що важливо для аналізу стану мережі, виявлення залежностей і підтримки прийняття рішень [38–44], [46], [49–52].

У контексті БСМ онтологія може включати класи сенсорних вузлів, каналів зв’язку, подій, середовища функціонування, загроз і ризикових ситуацій. Для таких класів задаються властивості, що описують залишкову енергію, якість зв’язку, затримку, втрати пакетів, навантаження, доступність і топологічну роль компонентів. Відношення між об’єктами дозволяють фіксувати зв’язність, залежність, вплив і участь вузлів у маршрутах передавання даних [38–44], [49–52].

Важливою перевагою онтологічного підходу є можливість багаторівневого подання знань. На нижньому рівні описуються фізичні компоненти мережі та їх параметри, на середньому - взаємодії між вузлами й каналами, а на верхньому - вразливості, загрози, ризики та можливі наслідки їх реалізації. Така структура дозволяє поєднати технічні, контекстні та безпекові аспекти функціонування БСМ в єдиній моделі [97–99].

Окреме значення має підтримка логічного висновку. На основі заданих класів, властивостей, відношень і правил онтологічна модель може виявляти приховані залежності, визначати критичні компоненти, встановлювати зв’язок між

деградацією вузлів або каналів і потенційними ризиками. Це робить онтологію придатною не лише для опису БСМ, а й для підтримки ризик-орієнтованого аналізу [49–52].

Водночас побудова онтологій для БСМ потребує чіткого визначення предметної області, формалізації великої кількості понять і відношень, а також підтримки узгодженості моделі. У межах цього дослідження онтологічний підхід розглядається як основа для інтегрованого опису структури мережі, станів її компонентів, вразливостей, загроз і ризикових факторів [97–99].

1.5.3 Переваги онтологічного підходу для ризик-орієнтованого управління БСМ

Використання онтологічного підходу в задачах управління БСМ створює основу для формалізованого ризик-орієнтованого аналізу. На відміну від методів, що розглядають окремі параметри або події ізольовано, онтологія дозволяє подати мережу як взаємопов’язану структуру компонентів, станів, вразливостей, загроз і ризикових факторів [38–44, 46, 49–52].

Однією з основних переваг такого підходу є інтеграція різнорідних даних. У БСМ інформація надходить із сенсорних вимірювань, параметрів вузлів і каналів, характеристик середовища, топології мережі та експертних оцінок. Онтологічна модель забезпечує єдину семантичну основу для їх узгодженого подання та подальшого аналізу [73–80].

Важливою властивістю онтології є можливість логічного висновку. На основі заданих класів, властивостей, відношень і правил можна виявляти приховані залежності між деградацією компонентів, наявними вразливостями, загрозами та можливими наслідками для функціонування мережі. Це дозволяє не лише фіксувати поточний стан БСМ, а й визначати потенційно критичні ситуації [73–80].

Для ризик-орієнтованого управління особливе значення має пояснюваність результатів. Онтологічна модель дає змогу простежити, які саме параметри вузлів, каналів, маршрутів або зовнішніх факторів впливають на формування певного

рівня ризику. Це підвищує обґрунтованість рішень щодо зміни режиму роботи мережі, перерозподілу навантаження, вибору альтернативних маршрутів або посилення моніторингу [73–80]

Отже, перевага онтологічного підходу полягає в можливості поєднати опис структури БСМ, станів її компонентів, вразливостей, загроз і ризиків у межах єдиної формалізованої моделі. Саме така модель створює передумови для побудови багаторівневої онтології ризик-орієнтованого аналізу БСМ.

1.6 Висновок першого розділу

У першому розділі проаналізовано сучасний стан досліджень у галузі бездротових сенсорних мереж. Розглянуто їх класифікацію, архітектуру, основні компоненти, особливості функціонування в промислових умовах, а також методи організації роботи мережі. Показано, що БСМ є складними розподіленими системами, у яких стан окремих вузлів, каналів зв’язку, маршрутів передавання та зовнішнього середовища безпосередньо впливає на якість функціонування мережі загалом.

Встановлено, що методи кластеризації, маршрутизації, агрегації даних, балансування навантаження та енергоорієнтованого керування дозволяють підвищити ефективність БСМ. Водночас більшість таких підходів спрямована на розв’язання окремих технічних задач і не забезпечує цілісного подання взаємозв’язків між параметрами мережі, її топологією, вразливостями, загрозами та можливими наслідками деградації компонентів.

Показано, що для промислових БСМ особливе значення мають надійність, своєчасність передавання даних, стійкість до завад, енергетична автономність і захищеність інформаційного обміну. У таких умовах відмова окремого вузла, погіршення стану каналу, виснаження енергетичного ресурсу або реалізація безпекової загрози можуть мати різні наслідки залежно від ролі відповідного компонента в топології мережі.

Аналіз методів виявлення вразливостей, загроз та оцінювання ризиків показав, що існуючі підходи мають низку обмежень. Зокрема, вони не завжди враховують динаміку БСМ, взаємозалежність компонентів, різнорідність даних, контекст функціонування та необхідність пояснення причин формування ризикових станів. Це ускладнює їх використання для комплексного ризик-орієнтованого аналізу мереж, що функціонують в умовах невизначеності.

Визначено, що перспективним напрямом подолання зазначених обмежень є використання нечітких, семантичних та онтологічних моделей. Нечіткі моделі доцільні для опису станів компонентів БСМ за умов неповноти, нечіткості та невизначеності вхідних даних, тоді як онтологічний підхід дозволяє формалізувати знання про структуру мережі, параметри вузлів і каналів, топологічні ролі компонентів, вразливості, загрози та ризикові фактори в межах єдиної узгодженої моделі.

Проведений аналіз обґрунтовує необхідність подальшого розроблення формалізованого апарату опису систем із чіткими та нечіткими параметрами, побудови нечітких моделей сенсорного вузла і каналу зв’язку, формування структурного опису БСМ для її онтологічного подання, а також розроблення інтегрованої багаторівневої онтологічної моделі, що поєднує структуру мережі, вразливості, загрози, ризики та механізми адаптивного керування. Така модель має забезпечити можливість логічного висновку й підтримки прийняття рішень у межах ризик-орієнтованого управління БСМ.

2 НЕЧІТКІ МОДЕЛІ ВУЗЛІВ І КАНАЛІВ ЗВ'ЯЗКУ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ В УМОВАХ НЕВИЗНАЧЕНОСТІ

У другому розділі розглядаються підходи до формалізації станів основних компонентів бездротових сенсорних мереж в умовах невизначеності. Основну увагу приділено побудові нечітких моделей сенсорного вузла та каналу зв'язку як ключових елементів БСМ, від характеристик яких залежать надійність, ефективність і стійкість функціонування мережі.

Необхідність використання нечітких моделей зумовлена тим, що в реальних умовах експлуатації параметри компонентів БСМ часто не можуть бути задані точно й повно. Частина інформації про стан вузлів і каналів має якісний, неповний або лінгвістично описаний характер, наприклад: «низький рівень сигналу», «високе навантаження», «недостатній рівень енергії» або «погіршена якість каналу». У таких умовах класичні детерміновані та ймовірнісні підходи не завжди забезпечують адекватний опис стану мережі.

У розділі спочатку обґрунтовується доцільність застосування нечіткої логіки для моделювання компонентів БСМ, далі формується узагальнений апарат опису систем із чіткими та нечіткими параметрами, а потім на його основі розробляються нечіткі моделі сенсорного вузла і каналу зв'язку. Завершується розділ визначенням можливостей використання запропонованих моделей у системі ризик-орієнтованого управління бездротовими сенсорними мережами. Напрацювання цього розділу публікувалися в роботах [101, 104]

2.1 Передумови побудови нечітких моделей для опису компонентів БСМ

Функціонування бездротових сенсорних мереж у промислових умовах супроводжується значною невизначеністю параметрів, динамічністю станів і впливом зовнішніх факторів. Сенсорні вузли та канали зв'язку зазнають дії електромагнітних завад, фізичних перешкод, температурних коливань, деградації апаратних компонентів, обмежень енергоресурсів і нестабільності мережевої

топології. Унаслідок цього такі параметри, як рівень сигналу, залишковий заряд батареї, пропускна здатність каналу, затримка передавання, навантаження або ймовірність відмови, часто не можуть бути визначені як сталі точні значення.

Класичні детерміновані моделі передбачають точне задання параметрів системи та дають однозначний результат для заданих умов. Вони є зручними для аналітичного опису, однак недостатньо гнучкими для БСМ, де характеристики вузлів і каналів змінюються під впливом середовища, навантаження та технічного стану компонентів. Ймовірнісні моделі дозволяють враховувати випадковість процесів, але потребують достатнього обсягу статистичних даних і знання законів розподілу, що не завжди доступно в реальних промислових мережах.

Додатковим обмеженням класичних моделей є складність урахування якісних і експертних оцінок. У практиці аналізу БСМ часто використовуються не лише числові значення, а й лінгвістичні характеристики стану, наприклад «середній рівень надійності», «висока затримка», «погіршена якість зв’язку» або «критичний рівень енергії». Такі оцінки складно безпосередньо використати в детермінованих чи ймовірнісних моделях без додаткової формалізації.

Нечітка логіка дає змогу описувати параметри БСМ через лінгвістичні змінні та функції належності. Це дозволяє перейти від жорсткого поділу станів до поступових оцінок, у яких один і той самий параметр може частково належати до кількох термів. Такий підхід є більш придатним для опису реальних станів компонентів БСМ, оскільки деградація вузла або каналу зазвичай відбувається поступово, а не лише у вигляді переходу між станами «працює» і «не працює».

Використання нечітких моделей також забезпечує поєднання кількісних і якісних характеристик у межах єдиного формалізму. Частина параметрів може надходити з телеметрії або вимірювань, а частина - задаватися експертно або визначатися на основі непрямих ознак. Завдяки цьому нечітке моделювання є придатним для опису стану сенсорного вузла, каналу зв’язку та інших компонентів БСМ за умов неповноти, неточності й неоднорідності вхідної інформації.

Важливою перевагою нечітких моделей є їх інтерпретованість. Результати можуть бути подані у вигляді зрозумілих лінгвістичних оцінок, що спрощує їх

використання в системах підтримки прийняття рішень. Крім того, такі моделі можуть бути інтегровані з онтологічними підходами, у яких стани компонентів, параметри, вразливості та ризики подаються у семантично узгодженій формі.

Отже, застосування нечіткої логіки та лінгвістичного моделювання є доцільним для опису компонентів бездротових сенсорних мереж в умовах невизначеності. Такий підхід дозволяє формалізувати нечіткі параметри, врахувати експертні знання, забезпечити інтерпретованість результатів і створити основу для побудови моделей сенсорного вузла та каналу зв’язку.

2.2 Узагальнений апарат формалізації систем із чіткими та нечіткими параметрами

Для побудови нечітких моделей компонентів БСМ необхідно сформувати узагальнений формальний апарат, який дозволяє описувати системи з поєднанням чітко визначених і нечітко заданих параметрів. Такий апарат має забезпечувати подання вхідних і вихідних характеристик, опис лінгвістичних змінних, визначення функцій належності та виконання операцій над нечіткими величинами.

У даному підрозділі розглядається формалізація технічної системи з чіткими та нечіткими параметрами, яка надалі використовується для побудови моделей сенсорного вузла та каналу зв’язку бездротової сенсорної мережі.

2.2.1 Загальна модель технічної системи з вхідними та вихідними параметрами

Для формалізації процесів, що відбуваються в бездротових сенсорних мережах, доцільно розглядати їх як складні технічні системи, які характеризуються множиною вхідних і вихідних параметрів. Такий підхід дозволяє узагальнити опис різних компонентів БСМ та створити єдину основу для подальшого математичного моделювання.

Нехай деяка технічна система визначається множинами вхідних параметрів P_X та вихідних параметрів P_Y. Тоді загальний набір параметрів системи може бути поданий у вигляді:

$$P = P_X \cup P_Y \tag{2.1}$$

де: P_X - множина вхідних параметрів системи; P_Y - множина вихідних параметрів; P - повна множина параметрів.

Кількісні характеристики цих множин визначаються такими співвідношеннями:

$$N_X = |P_X|, N_Y = |P_Y|, N_P = |P| \tag{2.2}$$

де: N_X - кількість вхідних параметрів; N_Y - кількість вихідних параметрів; N - загальна кількість параметрів системи.

Зазвичай між вхідними та вихідними параметрами існує певна функціональна залежність, яка відображає вплив вхідних характеристик на результуючі показники системи. У загальному вигляді таку залежність можна записати як:

$$P_Y = F(P_X) \tag{2.3}$$

де: F() деяке відображення, що описує поведінку системи.

Наведена модель може бути використана для опису сенсорних вузлів і каналів зв’язку БСМ. Вхідними параметрами можуть бути характеристики середовища, енергетичний стан, навантаження, параметри каналу або стан окремих компонентів, а вихідними - узагальнені показники працездатності, затримки, імовірності передавання даних або рівня деградації. У реальних умовах не всі параметри можуть бути задані точно. Частина з них має нечіткий характер або визначається на основі експертних оцінок. Тому модель потребує розширення шляхом введення нечітких параметрів, лінгвістичних змінних і функцій належності.

2.2.2 Повний ортогональний семантичний простір і лінгвістичні змінні

Для опису нечітких параметрів технічної системи доцільно перейти від точкового числового подання до лінгвістичного опису. Такий підхід дозволяє формалізувати якісні, неповні або наближені оцінки параметрів і надалі використовувати їх у математичних моделях компонентів БСМ.

Нехай на множині допустимих значень параметра D_i, $i=1,...,N$, де N - кількість нечітких параметрів системи, визначено множину нечітких значень L_i. Кожне таке значення відповідає окремому лінгвістичному терму, а їх сукупність утворює повний ортогональний семантичний простір для параметра p_i. Якщо K_i - кількість термів, що використовуються для опису i-го параметра, то множина L_i задає впорядкований набір нечітких оцінок, наприклад «низький», «середній», «високий», які покривають область визначення параметра без логічних суперечностей і пропусків. Кожен терм із множини L_i визначається як нечітке число з функцією належності, побудованою на основі трикутного або крайового трапецієподібного представлення. У загальному випадку функції належності для термів повного ортогонального семантичного простору задаються співвідношеннями для першого, внутрішніх та останнього термів.

Для першого терму:

$$p_i^k \Rightarrow \mu_i^k(p_i^{`}) = \begin{cases} 1, p_i^{`} = p_{ic}^1 \\ \dfrac{p_i^{`} - p_{ic}^2}{p_{ic}^1 - p_{ic}^2}, p_{ic}^1 < p_i^{`} < p_{ic}^2 \\ 0, p_i^{`} \geq p_{ic}^2 \end{cases} \tag{2.4.1}$$

Для внутрішніх термів, $k=2,...,K_i-1$:

$$p_i^k \Rightarrow \mu_i^k(p_i^{`}) = \begin{cases} 0, p_i^{`} \leq p_{ic}^{k-c}, p_i^{`} \geq p_{ic}^{k+1} \\ \dfrac{p_i^{`} - p_{ic}^{k-c}}{p_{ic}^k - p_{ic}^{k-c}}, p_{ic}^{k-c} < p_i^{`} < p_{ic}^k \\ 1, p_i^{`} = p_{ic}^k \\ \dfrac{p_i^{`} - p_{ic}^{k+c}}{p_{ic}^k - p_{ic}^{k+c}}, p_{ic}^{k+c} < p_i^{`} < p_{ic}^{k+1} \end{cases}, k = 2,...,K_i - 1 \tag{2.4.2}$$

Для останнього терму:

$$p_i^{K_i} \Rightarrow \mu_i^{K_i}(p_i^{`}) = \begin{cases} 0, p_i^{`} \le p_{ic}^{K_i-1} \\ \dfrac{p_i^{`} - p_{ic}^{K_i-1}}{p_{ic}^{K_i-1} - p_{ic}^{K_i}}, p_{ic}^{K_i-1} < p_i^{`} < p_{ic}^{K_i} \\ 1, p_i^{`} = p_{ic}^{K_i} \end{cases} \quad (2.4.3)$$

Тут p_{ic}^{k} - характерні точки, що визначають положення k-го терму на осі значень параметра p_i, а $\mu_i^k(p_i)$ - ступінь належності значення p_i до відповідного лінгвістичного терму. Такий запис відображає важливу особливість повного ортогонального семантичного простору: внутрішні терми мають трикутну форму, тоді як крайні терми задаються асиметрично, що дозволяє коректно описати межові області значень параметра. Саме тому формула (2.4) подається не одним універсальним співвідношенням, а трьома окремими випадками - для першого, внутрішніх і останнього термів.

Використання повного ортогонального семантичного простору є важливим для моделювання компонентів БСМ, оскільки такі характеристики, як рівень заряду батареї, якість каналу зв’язку, імовірність відмови або інтенсивність старіння інформації, часто задаються не точними числами, а якісними оцінками. ПОСП забезпечує перетворення таких оцінок у математичну форму, придатну для подальших обчислень. Отже, введення лінгвістичних змінних і повного ортогонального семантичного простору створює основу для формалізації нечітких параметрів БСМ. Далі розглядаються операції над нечіткими величинами, необхідні для побудови узагальнених моделей систем із чіткими та нечіткими параметрами.

2.2.3 Функція належності та математичні операції над нечіткими величинами

Після введення повного ортогонального семантичного простору необхідно визначити математичний апарат для виконання операцій над нечіткими

величинами. У даній роботі нечіткі значення параметрів подаються у вигляді трикутних нечітких чисел, що забезпечує простоту обчислень та зручність інтерпретації результатів.

Нехай задано деякі нечіткі числа: $x = \{x_b, x_c, x_e\}$, $y = \{y_b, y_c, y_e\}$, $\tilde{z} = \{z_b, z_c, z_e\}$, де x_b, y_b, z_b – ліві межі нечітких чисел, x_c, y_c, z_c - центральні значення, x_e, y_e, z_e - праві межі. Таке подання забезпечує зручну інтерпретацію лінгвістичних змінних і дозволяє формально визначити основні арифметичні операції.

Тоді операція додавання двох нечітких чисел задається співвідношенням:

$$\tilde{z} = x + y = \{x_b + y_b, x_c + y_c, x_e + y_e\} \tag{2.5}$$

Операція віднімання нечітких чисел визначається як:

$$\tilde{z} = x - y = \{x_b - y_e, x_c - y_c, x_e - y_b\} \tag{2.6}$$

Операція множення нечітких чисел визначається як:

$$\tilde{z} = x \times y = \{x_b \times y_b, x_c \times y_c, x_e \times y_e\} \tag{2.7}$$

Операція ділення задається співвідношенням:

$$\tilde{z} = \frac{x}{y} = \{\frac{x_b}{y_e}, \frac{x_c}{y_c}, \frac{x_e}{y_b}\} \tag{2.8}$$

Наведені співвідношення є базовими для обробки трикутних нечітких чисел. Вони дозволяють поєднувати нечіткі параметри в межах узагальнених моделей і зберігати інтерпретованість отриманих результатів.

У результаті арифметичних операцій отримане нечітке число може не збігатися з жодним із термів відповідного повного ортогонального семантичного

простору. Для його подальшої інтерпретації використовується процедура визначення найближчого нечіткого значення:

$$y_i = \min(|\, y_{ic}^{k+1} - y_{ie} \,| + |\, y_{ic}^{k-1} - y_{ib} \,| + |\, y_{ic}^{k} - y_{ic} \,|) \qquad (2.9)$$

де (y_{ib}, y_{ic}, y_{ie}) - отримане нечітке трикутне число, а y_{ic}^{k-1}, y_{ic}^{k}, y_{ic}^{k+1} - характерні точки відповідного терму ПОСП. Це дозволяє подати результат обчислень у вигляді найближчої лінгвістичної оцінки, придатної для подальшого семантичного аналізу та підтримки прийняття рішень. Таким чином, функції належності, операції над трикутними нечіткими числами та процедура визначення найближчого терму утворюють базовий математичний апарат нечіткого моделювання, який використовується для подальшої побудови моделей систем із чіткими та нечіткими параметрами.

2.2.4 Узагальнені моделі розрахунку характеристик систем із чіткими та нечіткими параметрами

Побудований математичний апарат дозволяє перейти до формалізації моделей систем, у яких частина параметрів задається чітко, а частина - у нечіткому вигляді. Такий підхід є доцільним для БСМ, оскільки параметри вузлів і каналів зв’язку можуть одночасно містити точні виміряні значення, експертні оцінки та лінгвістичні характеристики.

Нехай задано множину вхідних параметрів системи, що включає як нечіткі, так і чіткі значення: $X_1 = \{x_{ij}\}$, $X_2 = \{x_{km}\}$, $A_1 = \{a_{ij}\}$, $A_2 = \{a_{km}\}$, де $X_1, X_2 \subset P_X$ - множина нечітких параметрів, а $A_1, A_2 \subset P_X$ - множина чітких параметрів. Вихідний параметр $y \in P_Y$ також задається у нечіткому вигляді, причому значення кожного нечіткого параметра визначається функціями належності.

Тоді нечіткі значення параметрів можуть бути подані у вигляді трикутних чисел: $x_{ij} = \{x_b^{ij}, x_c^{ij}, x_e^{ij}\}$, $x_{lm} = \{x_b^{lm}, x_c^{lm}, x_e^{lm}\}$, $y = \{y_b, y_c, y_e\}$.

Розглянемо випадок, коли функціональна залежність між вхідними та вихідними параметрами має вигляд агрегованої зваженої моделі. У цьому випадку вихідний параметр може бути визначений як:

$$y = \frac{\sum_i \prod_j a_{ij} x_{ij}}{\sum_l \prod_m a_{lm} x_{lm}} \tag{2.10}$$

де коефіцієнти a_{ij} та a_{lm} відображають вагу відповідних параметрів. Це дозволяє отримати надійне представлення поведінки системи за невизначених умов. Нечіткий вихідний параметр y тоді визначається наступним виразом:

$$y_i = \min_k(|\, y_c^{k+1} - \frac{\sum_i \prod_j a_{ij} x_e^{ij}}{\sum_l \prod_m a_{lm} x_b^{lm}}\,| + |\, y_c^{k-1} - \frac{\sum_i \prod_j a_{ij} x_b^{ij}}{\sum_l \prod_m a_{lm} x_e^{lm}}\,| + |\, y_c^{k} - \frac{\sum_i \prod_j a_{ij} x_c^{ij}}{\sum_l \prod_m a_{lm} x_c^{lm}}\,|) \tag{2.11}$$

У випадку, коли модель системи має мультиплікативний характер, тобто вихідний параметр визначається як добуток вхідних величин, використовується співвідношення:

$$y = \prod_{i=1}^{n} x_i \tag{2.12}$$

що дозволяє компактно описати системи, у яких параметри взаємодіють нелінійним чином.

Відповідно, із використанням операцій над трикутними нечіткими числами отримуємо:

$$y = \min_k(|\, y_b - \prod\nolimits_{i=1}^{n} x_{ib}\,| + |\, y_c - \prod\nolimits_{i=1}^{n} x_{ic}\,| + |\, y_e - \prod\nolimits_{i=1}^{n} x_{ie}) \tag{2.13}$$

Наведені співвідношення утворюють узагальнену модель розрахунку характеристик систем із чіткими та нечіткими параметрами. Вони дозволяють

поєднувати кількісні та лінгвістичні оцінки в межах єдиного формального опису.

Отриманий апарат використовується як основа для побудови нечітких моделей основних компонентів БСМ, зокрема сенсорного вузла та каналу зв'язку. Це забезпечує можливість урахування невизначеності вхідних даних, нечіткого характеру частини параметрів і взаємозв'язків між характеристиками компонентів мережі.

2.3 Нечітка модель сенсорного вузла бездротової сенсорної мережі

Після побудови узагальненого апарату формалізації систем із чіткими та нечіткими параметрами доцільно перейти до його прикладного використання для моделювання основних компонентів бездротової сенсорної мережі. Одним із таких компонентів є сенсорний вузол, який виконує функції збирання, первинної обробки та передавання даних і водночас є одним із найбільш вразливих елементів БСМ в умовах невизначеності. Його працездатність залежить від стану кількох взаємопов'язаних складових, зокрема сенсора, приймально-передавального модуля, процесора та джерела живлення. Саме тому в даному підрозділі розглядається побудова нечіткої моделі сенсорного вузла, яка дозволяє формалізувати можливі режими його функціонування, урахувати залежності між компонентами та отримати узагальнену оцінку його стану в умовах неповної та неточної інформації.

2.3.1 Структура сенсорного вузла та функції його основних компонентів

Сенсорний вузол є базовим елементом бездротової сенсорної мережі, від стану якого залежать якість збирання даних, можливість їх обробки та передавання до інших вузлів або базової станції. У загальному випадку його структура включає чотири основні компоненти: сенсорний елемент, приймально-передавальний модуль, процесорний Метод і джерело живлення.

Такий поділ дозволяє пов'язати функціональне призначення компонентів із подальшим оцінюванням працездатності сенсорного вузла в межах нечіткої моделі.

Сенсорний елемент забезпечує перетворення фізичних параметрів середовища в електричні сигнали, придатні для подальшої обробки. Залежно від призначення мережі він може вимірювати температуру, тиск, вологість, вібрацію, концентрацію речовин або інші характеристики середовища. Відмова сенсорного елемента призводить до втрати вимірювальної функції вузла, однак за збереження працездатності інших компонентів вузол може продовжувати роботу як ретранслятор.

Приймально-передавальний модуль забезпечує обмін даними між вузлами мережі. Його стан визначає можливість передавання власних вимірювань, приймання повідомлень від сусідніх вузлів і участі у маршрутизації. У промислових умовах робота цього компонента може ускладнюватися електромагнітними завадами, нестабільністю каналу та втратами пакетів.

Процесорний Метод виконує обробку даних, керує режимами роботи вузла та координує взаємодію між сенсором, радіомодулем і джерелом живлення. Його відмова фактично унеможливлює узгоджену роботу вузла незалежно від стану інших компонентів.

Джерело живлення забезпечує енергопостачання всіх складових сенсорного вузла. Обмеженість енергетичного ресурсу є однією з ключових особливостей БСМ, тому стан батареї безпосередньо впливає на тривалість роботи вузла, частоту передавання даних і підтримання активного режиму. Втрата працездатності джерела живлення призводить до повної відмови вузла.

Отже, сенсорний вузол доцільно розглядати як систему взаємопов’язаних компонентів, кожен із яких виконує окрему функцію, але впливає на загальний режим роботи вузла. Саме така структура є основою для подальшої формалізації можливих станів вузла та побудови його нечіткої моделі.

2.3.2 Експериментальне дослідження запропонованого методу

Для побудови нечіткої моделі сенсорного вузла необхідно формалізувати можливі стани його основних компонентів і врахувати залежності між ними. У

загальному випадку вузол розглядається як система, що складається із сенсорного елемента, приймально-передавального модуля, процесора та джерела живлення.

Для опису стану цих компонентів введемо двійкові змінні x_s, x_t, x_p та x_b, які відповідають стану сенсора, приймально-передавального модуля, процесора та батареї. Кожна змінна набуває значення 1 у разі працездатності компонента і 0 - у разі його відмови. Тоді стан сенсорного вузла можна подати у вигляді кортежу: $x=\{x_s, x_t, x_p, x_b\}$.

Оскільки вузол має чотири основні компоненти, теоретично він може перебувати у $2^4=16$ можливих станах. Однак ці стани не є рівнозначними з погляду функціонування мережі. Стан {1,1,1,1} відповідає повній працездатності вузла, коли він здатний виконувати вимірювання, обробку та передавання даних. Стан {0,1,1,1} означає відмову сенсорного елемента, за якої вузол втрачає вимірювальну функцію, але може зберігати здатність до ретрансляції даних.

Важливо враховувати, що компоненти сенсорного вузла не є повністю незалежними. Сенсорний елемент і приймально-передавальний модуль можуть функціонувати лише за умови працездатності процесора та джерела живлення. Відмова процесора унеможливлює обробку даних і керування роботою вузла, а відмова батареї призводить до повної втрати працездатності всіх компонентів.

Для кількісного опису таких залежностей вводяться ймовірності відмов компонентів P_s, P_t, P_p та P_b, що відповідають сенсору, приймально-передавальному модулю, процесору та батареї. При цьому ймовірності відмови сенсора та приймально-передавального модуля доцільно розглядати як умовні, оскільки їх фактичне функціонування залежить від наявності працездатного процесора та джерела живлення. Таким чином, ймовірність стану вузла визначається з урахуванням залежностей між компонентами та може бути задана у вигляді:

$$P(x) = P(x_s \mid x_p, x_b) \times P(x_t \mid x_p, x_b) \times P(x_p \mid x_b) \times P(x_b) \qquad (2.14)$$

Це співвідношення дозволяє описати структуру залежностей між компонентами сенсорного вузла й одночасно формує основу для переходу до

нечіткої інтерпретації їхніх станів.

З наведеного випливає, що формалізація станів сенсорного вузла має враховувати не лише працездатність окремих компонентів, а й структурні залежності між ними. Це дозволяє перейти від простого переліку можливих комбінацій станів до моделі, яка відображає реальні режими функціонування вузла в умовах невизначеності.

2.3.3 Формалізація імовірностей відмови компонентів вузла

Побудована модель станів сенсорного вузла дозволяє перейти до кількісного опису його функціонування через імовірності відмов окремих компонентів. Такий опис є проміжним етапом між структурною моделлю вузла та подальшим нечітким оцінюванням його працездатності.

Нехай P_s, P_t, P_p та P_b - імовірності відмови відповідно сенсорного елемента, приймально-передавального модуля, процесора та джерела живлення протягом заданого інтервалу часу T_m. Ці значення можуть визначатися на основі експериментальних даних, результатів тестування надійності або технічних характеристик компонентів.

Відповідно, імовірність працездатності кожного компонента може бути визначена як доповнення до одиниці: $R_s=1-P_s$, $R_t=1-P_t$, $R_p=1-P_p$, $R_b=1-P_b$.

Тоді імовірність того, що сенсорний вузол перебуває у певному стані $x=\{x_s, x_t, x_p, x_b\}$, визначається як добуток імовірностей відповідних подій з урахуванням умовних залежностей між компонентами:

$$P(x) = P_s^{1-x_s}(1-P_s)^{x_s} \times P_t^{1-x_t}(1-P_t)^{x_t} \times P_p^{1-x_p}(1-P_p)^{x_p} \times P_b^{1-x_b}(1-P_b)^{x_b} \qquad (2.15)$$

У загальному випадку така форма є справедливою за умови формальної незалежності компонентів. Проте для сенсорного вузла необхідно враховувати структурні залежності, зокрема залежність сенсорного елемента та приймально-передавального модуля від працездатності процесора і джерела живлення. Тому

імовірність стану вузла доцільно трактувати як комбінацію умовних і безумовних імовірностей.

Отримані співвідношення дозволяють оцінювати ймовірність як повної працездатності вузла, так і його часткових режимів функціонування. Зокрема, повністю працездатний стан {1,1,1,1} відповідає одночасній працездатності всіх компонентів, тоді як часткові режими визначаються відповідними комбінаціями станів окремих складових.

У реальних умовах експлуатації БСМ точне визначення (P_s), (P_t), (P_p) та (P_b) є складним через вплив середовища, старіння обладнання, електромагнітні завади та нестабільність режимів роботи. Тому такі імовірнісні характеристики доцільно розглядати не лише як точні числові значення, а як нечіткі величини, задані через лінгвістичні змінні.

У результаті формалізація імовірностей відмови компонентів сенсорного вузла створює основу для переходу від класичного імовірнісного опису до нечіткої моделі працездатності. Далі вводяться лінгвістичні змінні та відповідні повні ортогональні семантичні простори для оцінювання стану вузла.

2.3.4 Лінгвістичні змінні для оцінювання працездатності сенсорного вузла

У реальних умовах функціонування БСМ точне визначення імовірностей відмов компонентів сенсорного вузла є ускладненим через вплив середовища, нестабільність режимів роботи, обмеженість статистичних даних і старіння обладнання. Тому доцільно перейти від точкових імовірнісних оцінок до їх лінгвістичного подання з використанням апарату нечітких множин.

Для опису працездатності компонентів сенсорного вузла введемо систему лінгвістичних змінних, кожна з яких характеризує відповідну імовірність функціонування елементів вузла: L - змінна, що описує загальну імовірність того, що сенсорний вузол перебуває у ввімкненому (працездатному) стані; L_b - змінна, що характеризує стан джерела живлення; L_t- змінна, що описує стан приймально-передавального модуля; L_p - змінна, що характеризує стан процесора; L_s - змінна,

що описує стан сенсорного елемента.

Кожна з цих змінних визначається на універсальній множині значень [0,1], що відповідає інтерпретації як імовірності або ступеня впевненості у працездатності відповідного компонента. Для кожної змінної вводиться повний ортогональний семантичний простір (ПОСП), який задає набір лінгвістичних термів, наприклад: «низька», «середня», «висока» імовірність. Кількість термів визначається як K_i для відповідної змінної L_i, де $i \in \{s,b,p,t\}$.

Кожен терм ПОСП подається у вигляді нечіткого числа з трикутною функцією належності, визначеною співвідношенням (2.4). Це забезпечує перехід від якісних оцінок стану компонентів до формалізованих математичних об’єктів, придатних для подальших обчислень.

З урахуванням введених лінгвістичних змінних, значення імовірностей працездатності компонентів P_s, P_t, P_p та P_b замінюються відповідними нечіткими оцінками: $P_s \to L_s, P_t \to L_t, P_p \to L_p, P_b \to L_b$.

Таке подання дозволяє враховувати невизначеність параметрів вузла та поєднувати кількісні й якісні характеристики в межах єдиної моделі. При цьому кожна лінгвістична змінна може мати власний набір термів і параметрів функцій належності, що дає змогу адаптувати модель до конкретних умов функціонування БСМ.

Узагальнюючи, введення лінгвістичних змінних створює основу для нечіткого оцінювання стану сенсорного вузла. Воно дозволяє інтегрувати якісні характеристики компонентів у формалізовану модель і перейти до визначення режимів функціонування вузла.

2.3.5 Нечітке оцінювання режимів функціонування сенсорного вузла

Введені лінгвістичні змінні та повні ортогональні семантичні простори дозволяють перейти до нечіткого оцінювання режимів функціонування сенсорного вузла. На цьому етапі нечіткі оцінки станів окремих компонентів інтегруються в узагальнену характеристику працездатності вузла.

Нехай для компонентів сенсорного вузла визначено нечіткі оцінки, що характеризують імовірність працездатності сенсора, приймально-передавального модуля, процесора та джерела живлення. Кожна з цих оцінок задається у вигляді трикутного нечіткого числа, що дозволяє виконувати над ними арифметичні операції відповідно до співвідношень (2.5)–(2.8).

У загальному випадку нечітка оцінка стану сенсорного вузла визначається як функція від нечітких значень його компонентів:

$$L = f(L_s, L_t, L_p, L_b) \tag{2.16}$$

З урахуванням структурних залежностей між компонентами (зокрема, критичної ролі процесора та джерела живлення), узагальнена оцінка працездатності вузла може бути визначена на основі мультиплікативної моделі:

$$L = L_s \times L_t \times L_p \times L_b \tag{2.17}$$

де операція множення виконується відповідно до (2.7). Така модель відображає той факт, що зниження надійності будь-якого з компонентів призводить до зменшення загальної працездатності вузла.

Для різних режимів функціонування сенсорного вузла можуть використовуватися різні моделі агрегування. Зокрема, у випадку повної працездатності вузла, коли всі компоненти функціонують, оцінка визначається як:

$$L_{full} = L_s \times L_t \times L_p \times L_b \tag{2.18}$$

що відповідає максимальному рівню функціональності.

У випадку, коли сенсорний елемент не є критичним (наприклад, вузол працює як ретранслятор), оцінка може визначатися без урахування L_s:

$$L_{relay} = L_t \times L_p \times L_b \tag{2.19}$$

Отримані нечіткі значення можуть не збігатися з жодним термом відповідного повного ортогонального семантичного простору. Тому для їх інтерпретації використовується процедура визначення найближчого лінгвістичного значення за співвідношенням (2.9). Це дозволяє подати результат у вигляді якісної оцінки, наприклад «низький», «середній» або «високий» рівень працездатності вузла.

Підсумовуючи, нечітке оцінювання режимів функціонування сенсорного вузла дозволяє інтегрувати інформацію про стан його компонентів, врахувати невизначеність параметрів і отримати узагальнену характеристику працездатності. Отримані результати можуть бути використані як вхідні дані для подальшого аналізу ризиків та інтеграції в онтологічну модель БСМ.

2.4 Нечітка модель канала зв’язку БСМ

Після побудови нечіткої моделі сенсорного вузла доцільно перейти до моделювання каналу зв’язку як іншого ключового компонента БСМ, що визначає своєчасність, надійність і повноту передавання даних між елементами мережі. У реальних умовах характеристики каналу мають змінний і невизначений характер, оскільки залежать від завад, завантаженості середовища, часу простою, старіння інформації та інших чинників. Тому в цьому підрозділі розглядається нечітка модель каналу зв’язку, яка поєднує апарат теорії масового обслуговування з нечітким поданням параметрів і дозволяє отримати узагальнені оцінки ефективності передавання даних у БСМ.

2.4.1 Канал зв’язку як об’єкт моделювання в умовах невизначеності

Канал зв’язку доцільно розглядати як систему масового обслуговування, у якій передавання пакетів можна інтерпретувати як обробку заявок. Нехай кожен

канал $s_j\{j=1\text{-}n\}$, характеризується пропускною здатністю β_j, а потік пакетів має інтенсивність λj. Розглянемо цей канал зв'язку, в якому потоки запитів є пуассоновськими, час обслуговування T_j^{ST} запитів є випадковою величиною, розподіленою за експоненціальним законом, як і часи простою шляху T_j^{Dt} та часи працездатності T_J^{Sw}.

Також, однією з важливих характеристик є інтенсивність старіння інформації, яка визначається як:

$$\nu_j = \frac{1}{T_j^A} \tag{2.18}$$

що знаходиться в j-му каналі зв'язку як випадкова величина з експоненціальним законом розподілу, де T_j^A – середній час старіння інформації.

Імовірність передачі в каналі зв'язку неможливо визначити точно. Описані характеристики, враховуючи неточність та якісний характер, а також неповноту вихідних даних, можна описати за допомогою теорії нечітких множин.

З урахуванням вищезазначених припущень, будуть справедливі такі співвідношення:

$$p_j = \frac{\beta_{эj} - \lambda_j}{\beta_{эj} - \lambda_j + \nu_{эj}} \tag{2.19}$$

$$k_j^{RtW} = \frac{T_j^{Sw}}{T_j^{Sw} + T_j^{Dt}} \tag{2.20}$$

$$k_j^{Dt} = \frac{T_j^{Dt}}{T_j^{Sw} + T_j^{Dt}} \tag{2.21}$$

$$\beta_{\text{ej}} = B_j k_j^{RtW} f_j = \frac{k_j^{Dt}}{k_j^{RtW} + \frac{1}{\nu_j \times T_j^{Dt}}} \tag{2.22}$$

$$\nu_{эj} = \nu_j + \beta_{эj} f_j \tag{2.23}$$

де:

- p_j ймовірність передачі пакета j по каналу зв'язку;
- β_{ej} еквівалентна пропускна здатність j-го каналу зв'язку;
- ν_{ej} еквівалентна інтенсивність старіння інформації у j-м каналі;
- k_j^{Dt} коефіцієнт простою j-го каналу зв'язку;
- k_j^{RtW} коефіцієнт готовності j-го каналу зв'язку;
- f_j коефіцієнт ненадійності j-го каналу зв'язку.

2.4.2 Подання параметрів каналу у вигляді лінгвістичних змінних

Основні характеристики каналу зв’язку, зокрема час працездатності T_J^{Sw}, час простою T_j^{Dt} та час старіння інформації T_j^A, суттєво впливають на ефективність передавання даних у БСМ. У реальних умовах ці параметри не завжди можуть бути визначені точно через завади, зміну топології, нерівномірне навантаження та нестабільність середовища передавання.

Для врахування такої невизначеності параметри каналу доцільно подавати у вигляді нечітких величин із використанням лінгвістичних змінних. Нехай відповідні часові характеристики каналу задаються на повному ортогональному семантичному просторі, а кожному значенню параметра ставиться у відповідність функція належності трикутного типу.

Для часу працездатності каналу функція належності визначається як:

$$\mu_k^{T_{Sw}}(T_j^{Sw})\begin{cases}0, T_j^{Sw} \le T_{kb}^{Sw}, \\ \dfrac{T_j^{Sw}-T_{kb}^{Sw}}{T_{kc}^{Sw}-T_{kb}^{Sw}}, T_{kb}^{Sw} < T_j^{Sw} < T_{kc}^{Sw} \\ 1, T_j^{Sw} = T_{kc}^{Sw} \\ \dfrac{T_j^{Sw}-T_{ke}^{Sw}}{T_{kc}^{Sw}-T_{ke}^{Sw}}, T_{kc}^{Sw} < T_j^{Sw} < T_{ke}^{Sw} \\ 0, T_j^{Sw} \ge T_{ke}^{Sw}\end{cases} \quad (2.24)$$

Аналогічно, для часу старіння інформації T_j^A:

$$\mu_k^{T_A}(T_j^A)\begin{cases}0, T_j^A \le T_{kb}^A, \\ \dfrac{T_j^A-T_{kb}^A}{T_{kc}^A-T_{kb}^A}, T_{kb}^A < T_j^A < T_{kc}^A \\ 1, T_j^A = T_{kc}^A \\ \dfrac{T_j^A-T_{ke}^A}{T_{kc}^A-T_{ke}^A}, T_{kc}^A < T_j^A < T_{ke}^A \\ 0, T_j^A \ge T_{ke}^A\end{cases} \quad (2.25)$$

Для часу простою каналу T_j^{Dt}:

$$\mu_k^{T_{Dt}}(T_j^{Dt})\begin{cases}0, T_j^{Dt} \le T_{kb}^{Dt}, \\ \dfrac{T_j^{Dt}-T_{kb}^{Dt}}{T_{kc}^{Dt}-T_{kb}^{Dt}}, T_{kb}^{Dt} < T_j^{Dt} < T_{kc}^{Dt} \\ 1, T_j^{Dt} = T_{kc}^{Dt} \\ \dfrac{T_j^{Dt}-T_{ke}^{Dt}}{T_{kc}^{Dt}-T_{ke}^{Dt}}, T_{kc}^{Dt} < T_j^{Dt} < T_{ke}^{Dt} \\ 0, T_j^{Dt} \ge T_{ke}^{Dt}\end{cases} \quad (2.26)$$

У наведених співвідношеннях параметри трикутної функції належності T_{kb}, T_{kc} та T_{ke} , вони визначають межі та центральне значення відповідного терму. Кожен параметр каналу описується через набір лінгвістичних оцінок, наприклад «низький», «середній» і «високий», а функції належності задають ступінь відповідності конкретного значення кожному з цих термів.

Оскільки параметри T_J^{Sw}, T_j^A та T_j^{Dt} входять у співвідношення (2.18)–(2.23), їх нечітке подання призводить до того, що всі похідні характеристики каналу також стають нечіткими.

Це створює передумови для побудови узагальненої нечіткої моделі каналу зв'язку, яка враховує невизначеність вихідних параметрів.

Проведена формалізація дозволяє перейти від класичного числового опису параметрів каналу до нечіткого подання, придатного для моделювання БСМ в умовах неповної та неточної інформації. Це створює основу для подальшого формування нечіткої моделі каналу зв'язку.

2.4.3 Формування нечіткої моделі каналу на основі апарату теорії масового обслуговування

Після введення нечіткого подання основних параметрів каналу зв'язку можна перейти до формування його узагальненої нечіткої моделі. Вона базується на співвідношеннях теорії масового обслуговування, однак часові характеристики каналу розглядаються не як точні значення, а як нечіткі величини.

Базові співвідношення, отримані для класичного випадку, зберігають свою структурну форму. Водночас час працездатності каналу, час простою та час старіння інформації задаються через лінгвістичні змінні й функції належності. Унаслідок цього похідні характеристики каналу також набувають нечіткого характеру.

Нечітка оцінка еквівалентної пропускної здатності каналу визначається через нижню, центральну та верхню оцінки відповідно за співвідношеннями:

$$\beta_{ee}^j = \left(\frac{\beta_j \times T_{je}^{Sw}}{T_{jb}^{Sw} + T_{jb}^{Dt}}\right) \tag{2.27}$$

$$\beta_{ec}^j = \left(\frac{\beta_j \times T_{jc}^{Sw}}{T_{jc}^{Sw} + T_{jc}^{Dt}}\right) \tag{2.28}$$

$$\beta_{eb}^{j} = (\frac{\beta_j \times T_{jb}^{Sw}}{T_{je}^{Sw} + T_{je}^{Dt}}) \tag{2.29}$$

У наведених співвідношеннях індекси b, c, e відповідають нижній, центральній та верхній оцінкам нечітких параметрів, отриманих на основі трикутних функцій належності. Це дозволяє подавати ефективну пропускну здатність не як точкове значення, а як трикутне нечітке число.

Нечітка оцінка ефективної інтенсивності старіння інформації також визначається через нижню, центральну та верхню оцінки:

$$V_{ee} = \frac{1}{T_{jb}^{A}} + (\frac{\beta_j \times T_{je}^{Sw}}{T_{jb}^{Sw} + T_{jb}^{Dt}} \times \frac{\frac{T_{je}^{Dt}}{T_{jb}^{Sw} + T_{jb}^{Dt}}}{\frac{T_{jb}^{Sw}}{(T_{je}^{Sw} + T_{je}^{Dt})} + \frac{T_{jb}^{A}}{T_{je}^{Dt}}}) \tag{2.30}$$

$$V_{ec} = \frac{1}{T_{jc}^{A}} + (\frac{\beta_j \times T_{jc}^{Sw}}{T_{jc}^{Sw} + T_{jc}^{Dt}} \times \frac{\frac{T_{jc}^{Dt}}{T_{jc}^{Sw} + T_{jc}^{Dt}}}{\frac{T_{jc}^{Sw}}{(T_{jc}^{Sw} + T_{c}^{Dt})} + \frac{T_{jc}^{A}}{T_{jc}^{Dt}}}) \tag{2.31}$$

$$V_{eb} = \frac{1}{T_{je}^{A}} + (\frac{\beta_j \times T_{jb}^{Sw}}{T_{je}^{Sw} + T_{je}^{Dt}} \times \frac{\frac{T_{jb}^{Dt}}{T_{je}^{Sw} + T_{je}^{Dt}}}{\frac{T_{je}^{Sw}}{(T_{jb}^{Sw} + T_{jb}^{Dt})} + \frac{T_{je}^{A}}{T_{jb}^{Dt}}}) \tag{2.32}$$

Ці співвідношення враховують, що старіння інформації залежить не лише від базового часу старіння, а й від часу простою та часу працездатності каналу. Тому ефективна інтенсивність старіння розглядається як нечітка характеристика, що відображає реальний режим функціонування каналу.

Отримані співвідношення (2.27)–(2.32) формують нечітку модель каналу зв’язку у вигляді двох взаємопов’язаних характеристик: ефективної пропускної здатності та ефективної інтенсивності старіння інформації. У сукупності вони

описують поточний стан каналу та можуть бути використані для подальшого визначення нечіткої ймовірності передавання пакетів.

Важливо, що запропонована модель не змінює аналітичну основу класичних співвідношень теорії масового обслуговування, а розширює її за рахунок використання нечітких параметрів. Це дозволяє враховувати невизначеність умов функціонування каналу й узгодити модель каналу з нечіткою моделлю сенсорного вузла.

Проведене узагальнення створює основу для подальшого оцінювання ймовірності передавання пакетів у каналі зв'язку. Саме ця характеристика дозволяє перейти від опису окремих параметрів каналу до інтегральної оцінки якості його функціонування в БСМ.

2.4.4 Нечітка оцінка ймовірності передавання пакетів у каналі зв'язку

На основі отриманих у підрозділі 2.4.3 нечітких оцінок ефективної пропускної здатності каналу та інтенсивності старіння інформації можна перейти до визначення ймовірності передавання пакетів. Ця характеристика відображає здатність каналу забезпечувати доставку даних з урахуванням його поточного стану.

У класичному випадку ймовірність передавання визначається як функція параметрів каналу, зокрема пропускної здатності, інтенсивності надходження пакетів та інтенсивності старіння інформації. Оскільки в реальних умовах ці параметри не завжди можуть бути задані точно, ймовірність передавання доцільно розглядати як нечітку величину.

Для формалізації цієї величини використовується повний ортогональний семантичний простір, у межах якого кожному значенню ймовірності передавання ставиться у відповідність певний лінгвістичний терм. Нехай Q_k, $k=1,...,N$ - терми лінгвістичної змінної, що описує ймовірність передавання пакетів. Тоді нечітка оцінка цієї ймовірності визначається як:

$$p_j = Q_k = \min_k(|\sigma(Q_k, Q_j)|) \tag{2.33}$$

де Q_j - отримане нечітке значення ймовірності передавання, що визначається на основі параметрів каналу, а $\sigma(\cdot)$ - функція міри близькості між нечіткими величинами.

Функція $\sigma(Q_k, Q_j)$ задається як узагальнена міра відхилення між відповідними компонентами нечітких трикутних чисел і має вигляд:

$$\sigma(Q_k, Q_j) = |Q_c^{k+1} - \frac{\beta_{ee}^j - \lambda_j}{\beta_{eb}^j - \lambda_j + \nu_{eb}^j}| + |Q_c^{k-1} - \frac{\beta_{eb}^j - \lambda_j}{\beta_{eb}^j - \lambda_j + \nu_{ee}^j}| + |Q_c^k - \frac{\beta_{ec}^j \times \lambda_j}{\beta_{ec}^j - \lambda_j + \nu_{ec}^j}| \tag{2.33}$$

Наведені співвідношення дозволяють відобразити отримане нечітке значення ймовірності передавання у відповідний лінгвістичний терм, наприклад «низька», «середня» або «висока» ймовірність. Це забезпечує семантичну інтерпретацію результату та робить його придатним для подальшого використання в системах підтримки прийняття рішень.

Отримана нечітка оцінка ймовірності передавання пакетів є узагальненою характеристикою каналу зв’язку, яка враховує ефективну пропускну здатність, інтенсивність надходження пакетів, інтенсивність старіння інформації та невизначеність параметрів середовища.

Підсумовуючи, нечітка модель каналу зв’язку дозволяє поєднати оцінки ефективної пропускної здатності, інтенсивності старіння інформації та ймовірності передавання пакетів у межах єдиного формалізованого опису. Отримані результати можуть бути використані для подальшої інтеграції моделі каналу в систему аналізу станів БСМ та ризик-орієнтованого управління.

2.5 Висновки другого розділу

У другому розділі обґрунтовано доцільність використання нечітких моделей для опису компонентів бездротових сенсорних мереж в умовах неповноти,

неточності та невизначеності вхідних даних. Показано, що класичні детерміновані та ймовірнісні підходи не завжди забезпечують достатню гнучкість для моделювання станів вузлів і каналів зв’язку в промислових умовах функціонування БСМ.

Розроблено узагальнений апарат формалізації систем із чіткими та нечіткими параметрами. У межах цього апарату введено лінгвістичні змінні, повний ортогональний семантичний простір, трикутні функції належності та операції над нечіткими величинами. Це дозволило сформувати основу для подальшого опису компонентів БСМ у вигляді формалізованих нечітких моделей.

Побудовано нечітку модель сенсорного вузла, у якій враховано стан його основних компонентів: сенсорного елемента, приймально-передавального модуля, процесора та джерела живлення. Формалізовано можливі режими функціонування вузла, зокрема повністю працездатний стан і режим ретрансляції за відмови сенсорного елемента. Запропонований підхід дозволяє враховувати структурні залежності між компонентами та отримувати узагальнену нечітку оцінку працездатності вузла.

Розроблено нечітку модель каналу зв’язку БСМ на основі поєднання апарату теорії масового обслуговування та нечіткого подання параметрів каналу. У моделі враховано ефективну пропускну здатність, інтенсивність старіння інформації, час простою, час працездатності та ймовірність передавання пакетів. Це дозволяє оцінювати стан каналу зв’язку за умов неповної або лінгвістично заданої інформації.

Проведена формалізація забезпечує узгоджене подання станів сенсорного вузла та каналу зв’язку у вигляді нечітких оцінок, придатних для подальшої семантичної інтерпретації. Отримані результати створюють основу для інтеграції нечітких моделей компонентів БСМ у багаторівневу онтологічну модель ризик-орієнтованого управління, що розглядається у наступному розділі.

3 РОЗРОБКА БАГАТОРІВНЕВОЇ ОНТОЛОГІЧНОЇ МОДЕЛІ ТА МЕТОДІВ РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ БЕЗДРОТОВИМИ СЕНСОРНИМИ МЕРЕЖАМИ

У попередньому розділі розроблено нечіткі моделі сенсорного вузла та каналу зв'язку, які дозволяють формалізувати стани компонентів БСМ в умовах невизначеності, неповноти даних і змінності параметрів середовища. Водночас для ризик-орієнтованого управління необхідно не лише оцінювати окремі вузли й канали, а й подати їх структурні, функціональні та контекстні взаємозв'язки в межах єдиної системи знань.

У цьому розділі здійснюється перехід від нечіткого моделювання компонентів БСМ до побудови уперше розробленої інтегрованої багаторівневої онтологічної моделі аналізу бездротової сенсорної мережі, яка поєднує опис топології мережі, характеристик вузлів і каналів, вразливостей, ризиків та механізмів адаптивного керування, та методів ризик-орієнтованого управління бездротовими сенсорними мережами.

Онтологічне подання дозволяє інтегрувати різнорідні дані, результати нечіткого оцінювання та правила інтерпретації критичних станів у межах єдиного семантичного середовища.

Основу запропонованого підходу становлять чотири взаємопов'язані методи: отримавший подальший розвиток метод семантичного визначення та логування станів комповнентів бездротових сенсорних мереж, удосконалений метод аналізу вразливостей, отримавший подальший розвиток оцінки ризиків і метод адаптивного керування. Така структура забезпечує послідовний перехід від фіксації поточного стану БСМ до виявлення критичних станів, оцінювання інтегрального ризику та формування керуючих впливів. Напрацювання цього розділу публікувалися в роботах [102, 103, 105, 109].

3.1 Загальна архітектура багаторівневої онтологічної моделі БСМ

Багаторівнева онтологічна модель є основою запропонованого підходу до

ризик-орієнтованого управління БСМ. Вона призначена для формалізованого подання структури мережі, поточних станів її компонентів, вразливостей, ризиків і рекомендацій щодо реагування. На відміну від графових, статистичних або процедурних моделей, онтологічне подання дозволяє описати БСМ як систему взаємопов’язаних сутностей, атрибутів і відношень.

Багаторівневий характер моделі зумовлений тим, що структура мережі, контекст її функціонування, вразливості, ризики та рекомендації належать до різних рівнів абстракції, але мають бути логічно узгоджені в межах єдиного семантичного простору. Нижчі рівні моделі описують топологію, вузли, канали зв’язку та параметри їх функціонування, а вищі рівні - вразливості, ризики, контрзаходи та рекомендації щодо реагування.

У межах запропонованої архітектури первинні телеметричні, структурні та контекстні дані перетворюються на формалізовані факти про стан мережі. Далі ці факти використовуються для виявлення вразливостей, оцінювання ризиків і формування рекомендацій щодо адаптивного керування. Такий підхід забезпечує послідовний перехід від опису стану мережі до підтримки прийняття рішень.

У подальших підрозділах розглядаються принципи побудови багаторівневої онтологічної моделі, її основні рівні, базові класи, сутності та відношення, а також узагальнена структура моделі як основа для реалізації методів семантичного виявлення та логування станів компонентів, аналізу вразливостей, оцінки ризиків і адаптивного керування.

3.1.1 Призначення та загальні принципи побудови багаторівневої онтологічної модель аналізу БСМ

Багаторівнева онтологічна модель аналізу БСМ є концептуальною основою ризик-орієнтованого управління мережею. Її призначення полягає у формалізованому поданні структури мережі, поточних станів її компонентів, контекстних характеристик, вразливостей, ризиків і рекомендацій щодо реагування в межах єдиного семантичного середовища. На відміну від традиційних технічних описів, онтологічна модель дозволяє представити БСМ як систему

взаємопов’язаних сутностей, атрибутів і відношень, придатних до логічного висновку та підтримки прийняття рішень.

Необхідність багаторівневої побудови зумовлена тим, що структура мережі, контекст її функціонування, вразливості, ризики та рекомендації належать до різних рівнів абстракції. Однорівневе подання не дозволяє узгоджено описати ці аспекти, тому модель формується як ієрархічна система, у якій кожен рівень має власне призначення, але пов’язаний з іншими рівнями через спільні сутності та відношення.

Основними принципами побудови моделі є багаторівневість, семантична узгодженість, контекстність, ієрархічне узагальнення та інтеграція кількісних і семантичних характеристик. Семантична узгодженість забезпечує подання всіх елементів мережі в єдиній системі понять. Контекстність дозволяє інтерпретувати параметри вузлів і каналів з урахуванням їх ролі в топології, умов середовища, навантаження та можливих загроз. Ієрархічне узагальнення забезпечує перехід від первинних характеристик мережі до оцінок вразливості, ризику та рекомендацій щодо реагування.

У межах запропонованої моделі доцільно виокремити п’ять взаємопов’язаних рівнів: структурний, контекстний, рівень вразливостей, рівень ризиків і рівень рекомендаційного реагування. Структурний рівень описує вузли, канали зв’язку, сегменти, маршрути, шлюзи та базові станції, тобто формує топологічний каркас мережі. Контекстний рівень подає поточні характеристики функціонування компонентів БСМ, зокрема енергетичні, часові, навантажувальні, комунікаційні та середовищні параметри.

Рівень вразливостей призначений для подання слабких місць компонентів мережі та небезпечних станів, що виникають унаслідок поєднання технічних, топологічних і середовищних факторів. На цьому рівні вузли, канали та сегменти розглядаються вже не лише як структурні елементи, а як носії потенційних вразливостей. Рівень ризиків узагальнює інформацію про вразливості, загрози, контекст і можливі наслідки їх реалізації, формуючи локальні або інтегральні оцінки ризику.

Завершальним є рівень рекомендаційного реагування, на якому результати оцінювання ризиків перетворюються на рекомендації щодо можливих контрзаходів. На цьому рівні визначаються пріоритети реагування, обмеження застосування дій, політики вибору контрзаходів і механізми зворотного зв’язку. Це дозволяє використовувати онтологічну модель не лише для опису стану мережі, а й для підтримки адаптивного керування.

Узагальнюючи, багаторівнева онтологічна модель БСМ поєднує структурний опис мережі, контекст її функціонування, вразливості, ризики та рекомендації щодо реагування в межах єдиного семантичного подання. Така організація створює основу для подальшого визначення базових класів, сутностей і відношень онтологічної моделі.

3.1.2 Базові класи, сутності та відношення онтологічної моделі

Після визначення принципів побудови та рівнів багаторівневої онтологічної моделі доцільно перейти до опису її базових класів, сутностей і відношень. Вони формують семантичний каркас, у межах якого компоненти БСМ, спостережувані об’єкти, параметри їх стану, вразливості, ризики та рекомендації щодо реагування подаються як взаємопов’язані елементи єдиної системи знань.

Центральною сутністю моделі є клас WSN, який описує бездротову сенсорну мережу як цілісний об’єкт аналізу. З ним пов’язані базові структурні класи Node, Link, Segment, Cluster та Route. Клас Node подає вузол мережі, Link - канал зв’язку між вузлами, Segment - топологічний або функціональний фрагмент мережі, Cluster - групу вузлів із визначеною роллю, а Route - маршрут передавання даних. Для уточнення ролей вузлів використовуються підкласи SensorNode, RelayNode, Gateway та BaseStation, що дозволяє врахувати функціональну неоднорідність компонентів БСМ.

Для подання об’єктів, стан яких контролюється за допомогою БСМ, доцільно використовувати клас ObservedObject. Він описує фізичний, технологічний або середовищний об’єкт спостереження, наприклад агрегат, установку, виробничу

ділянку, резервуар, трубопровід, зону контролю або фрагмент середовища. Такий клас дозволяє відокремити спостережуваний об’єкт від компонентів сенсорної мережі: об’єкт є джерелом параметрів стану, а вузли БСМ забезпечують їх вимірювання, передавання та подальшу інтерпретацію.

Параметри спостережуваного об’єкта подаються класом ObservedParameter. Він описує контрольовані характеристики, зокрема температуру, рівень, тиск, витрату, струм, напругу, вологість, концентрацію або інші параметри, що залежать від предметної області застосування. Для кожного параметра можуть задаватися тип, одиниця вимірювання, допустимий діапазон, поточне значення, нормоване значення та лінгвістична або нечітка інтерпретація стану.

Для подання поточного стану мережі використовуються класи TelemetrySnapshot, NodeContext та ChannelState. Клас TelemetrySnapshot фіксує набір параметрів у певний момент часу, NodeContext описує контекст функціонування вузла, а ChannelState - стан каналу зв’язку. Вони забезпечують зв’язок між структурними елементами БСМ та їхніми динамічними характеристиками, зокрема енергетичним станом, затримками, навантаженням, якістю каналу, доступністю, втратами пакетів та іншими параметрами функціонування.

Окремою сутністю моделі є клас StateLogRecord, який описує формалізований запис поточного стану моделі. Він поєднує дані про спостережуваний об’єкт, контрольовані параметри, телеметричний знімок, контекст вузлів, стан каналів зв’язку, часову мітку та ознаки достовірності даних. Саме цей клас є результатом виконання методу семантичного визначення та логування станів компонентів БСМ і використовується як вхідна основа для подальшого аналізу вразливостей та оцінювання ризику.

На рівні подання небезпечних станів використовуються класи Vulnerability, Threat та Risk. Клас Vulnerability описує слабкі місця компонентів мережі або спостережуваних об’єктів, Threat - потенційне джерело небажаного впливу, а Risk - узагальнену характеристику небезпеки, що формується на основі поєднання вразливостей, загроз, контексту, критичності компонента та можливих наслідків.

Для деталізації вразливостей можуть використовуватися підкласи EnergyVulnerability, CommunicationVulnerability, TopologyVulnerability та PhysicalVulnerability.

Рівень реагування подається класами Recommendation, Countermeasure, ResponsePolicy, PriorityLevel, Constraint та Feedback. Вони описують сформовані рекомендації, можливі контрзаходи, політики вибору рішень, пріоритети реагування, обмеження застосування контрзаходів і результати зворотного зв’язку після врахування або реалізації рекомендованого рішення.

Відношення між класами забезпечують логічну цілісність онтологічної моделі. На структурному рівні використовуються зв’язки contains, includes, connectedTo, belongsTo, uses та passesThrough, які описують склад мережі, належність елементів до сегментів, з’єднання між вузлами та проходження маршрутів через окремі компоненти. На рівні спостереження використовуються відношення observedBy, hasParameter, measuredBy, hasTelemetry та loggedAs, які пов’язують спостережуваний об’єкт, його параметри, сенсорні вузли, телеметричні знімки та записи стану моделі.

На контекстному рівні застосовуються відношення hasContext, hasState, characterizedBy та influencedBy, що пов’язують вузли, канали, параметри та спостережувані об’єкти з їх поточними станами й факторами впливу. Для подання небезпечних станів і ризиків використовуються відношення hasVulnerability, exposedTo, causes, contributesTo, evaluatedAsRisk та influencesRisk. Вони дозволяють пов’язати компоненти мережі, записи стану, спостережувані об’єкти, вразливості, загрози та відповідні оцінки ризику.

На рівні реагування застосовуються зв’язки generatesRecommendation, includesCountermeasure, limitedBy, assignedPriority, guidedByPolicy, presentedTo, transferredTo та refinedByFeedback. Вони описують процес формування, передачі та уточнення рекомендацій, а також зв’язок між оціненим ризиком, допустимими контрзаходами, обмеженнями та результатами зворотного зв’язку.

Сформований набір класів, сутностей і відношень забезпечує цілісне онтологічне подання БСМ як об’єкта ризик-орієнтованого управління. Він дозволяє

поєднати структурний опис мережі, спостережувані об’єкти, параметри їх стану, телеметричні знімки, записи логування, вразливості, ризики та рекомендації щодо реагування в межах єдиного формального середовища, придатного для логічного висновку й підтримки прийняття рішень.

3.1.3 Представлення багаторівневої моделі аналізу ризиків

Семантичне подання топології БСМ є базовою умовою побудови методу семантичного виявлення та логування станів компонентів БСМ, оскільки саме топологічна структура визначає взаємодію між вузлами, можливі маршрути передавання даних, рівень резервування та стійкість мережі до локальних відмов. У межах багаторівневої онтологічної моделі топологія розглядається не лише як сукупність фізичних з’єднань, а як система сутностей, атрибутів і відношень, придатна для логічного висновку та подальшого аналізу вразливостей і ризиків.

Метод семантичного виявлення та логування забезпечує формалізоване подання складу БСМ, її вузлів, каналів, маршрутів і динамічних параметрів. У загальному вигляді він може бути представлений як:

$$G = (V, E, A, \Phi, R, O) \tag{3.1}$$

де:

- V = {υ1, υ2, …, υn} - множина вузлів;
- E= {e1, e2, …, en} - множина зв'язків між вузлами;
- A = { α1, α2, …, αn} - множина атрибутів, що описують характеристики вузлів та з'єднань (наприклад, енергетичний баланс, пропускна здатність, середній час відгуку);
- Ф = {φ1, φ2, …, φn} - множина динамічних параметрів, що змінюються з часом;
- R = {r1, r2, …, rn}- множина відносин між онтологічними сутностями;
- O = {o1, o2, …, on} – множина операцій, що виконується над параметрами, станами та онтологічними записами моделі.

Таке подання дозволяє розглядати БСМ як формалізовану онтологічну структуру, у якій поєднуються топологічні елементи, їх атрибути, динамічні параметри, семантичні відношення та операції над станами моделі. Це важливо для БСМ, оскільки стани вузлів і каналів змінюються в часі, маршрути можуть втрачати стабільність, а навантаження, умови середовища та параметри спостережуваних об’єктів впливають на функціонування мережі загалом.

У межах такого подання вузол розглядається не лише як елемент множини (V), а як онтологічна сутність із певною роллю, станом, атрибутами та зв’язками з іншими елементами моделі. Аналогічно канал зв’язку подається не лише як елемент множини (E), а як об’єкт із власними характеристиками якості, доступності, стабільності, затримки та навантаження. Завдяки цьому топологія набуває не тільки структурного, а й функціонального та семантичного змісту.

Для опису різних типів вузлів у межах єдиної онтологічної структури доцільно виділяти сенсорні вузли, ретранслятори, шлюзи та базові станції. Кожен із цих елементів має власну функцію в мережі, що впливає на оцінювання його критичності, вразливості та ролі у формуванні ризику. Наприклад, відмова звичайного сенсорного вузла, ретранслятора або шлюзу має різні наслідки для мережі, тому така різниця повинна бути врахована вже на рівні семантичного опису топології.

Окрему роль відіграє множина відношень R, яка формалізує зв’язки між вузлами, каналами, маршрутами, сегментами, спостережуваними об’єктами, параметрами та записами стану. До таких відношень належать зв’язки типу «вузол з’єднаний з вузлом», «вузол належить сегменту», «канал з’єднує два вузли», «маршрут проходить через вузол», «сенсорний вузол спостерігає об’єкт», «об’єкт має параметр», «запис стану містить телеметричний знімок» тощо. Множина операцій O визначає дії над цими даними, зокрема збирання телеметрії, нормування параметрів, нечітку інтерпретацію, формування контексту, створення запису стану та передавання результатів до подальших методів аналізу.

Для відображення багаторівневості запропонованої онтологічної моделі базове подання (3.1) можна розглядати як плоску реалізацію, у якій усі вузли,

зв’язки, атрибути, динамічні параметри, відношення та операції подано на одному рівні. Таке подання є зручним для загального опису БСМ, однак воно не повною мірою відображає кластерну організацію мережі та взаємодію окремих її частин із зовнішнім середовищем, спостережуваними об’єктами або системами керування.

Для подання кластерного рівня модель може бути розширена до множини локальних кластерних подань. У випадку взаємодії двох кластерів таке подання можна записати як:

$$G^{cl} = (G_1^+, G_2^+) \tag{3.2}$$

де G_1^+ та G_2^+ - розширені онтологічні подання першого та другого кластерів БСМ. Для окремого кластера розширене подання має вигляд:

$$G_i^+ = (V_i, E_i, A_i, \Phi_i, R_i, O_i, I_i^{ext}) \tag{3.3}$$

де V_i, E_i, A_i, Φ_i, R_i, O_i - відповідно множини вузлів, зв’язків, атрибутів, динамічних параметрів, відношень та операцій усередині (і)-го кластера; I_i^{ext} - зовнішній інтерфейс кластера, який описує його взаємодію з іншими кластерами, спостережуваними об’єктами, зовнішнім середовищем або системою керування.

Зовнішній інтерфейс кластера доцільно подати у вигляді:

$$I_i^{ext} = (B_i, X_i^{ext}, L_i^{ext}, R_i^{ext}, O_i^{ext}) \tag{3.4}$$

де B_i - множина граничних вузлів кластера, через які здійснюється зовнішня взаємодія; X_i^{ext} - множина зовнішніх сутностей; L_i^{ext} - множина зовнішніх зв’язків; R_i^{ext} - множина зовнішніх семантичних відношень; O_i^{ext} - множина операцій зовнішньої взаємодії.

Взаємодія двох кластерів може бути задана через міжкластерний зв’язок між їх граничними вузлами:

$$L_{12}^{cl} \subseteq B_1 \times B_2 \tag{3.5}$$

Цей зв’язок відображає можливість передавання телеметрії, службових повідомлень, контекстних характеристик, результатів логування, оцінок вразливостей або ризикових показників між двома кластерами. Для опису такої взаємодії вводяться міжкластерні відношення:

$$R_{12}^{cl} = \{connectedToCluster, transfersTelemetryTo, receivesDataFrom, synchronizesWith, reportsStateTo\} \quad (3.6)$$

та міжкластерні операції:

$$O_{12}^{cl} = \{transferTelemetry, synchronizeState, exchangeContext, transferRiskData, updateClusterState\} \quad (3.7)$$

Таким чином, кожен кластер розглядається не як ізольована частина БСМ, а як локальне онтологічне подання, що має власну внутрішню структуру, власні параметри стану та додаткові відношення й операції для взаємодії з іншими кластерами та зовнішнім середовищем.

Для подання наступного ієрархічного рівня вводиться відношення “старший–молодший” між кластерними поданнями. Якщо кластер G_p^+ виконує узагальнювальну або координуючу функцію відносно кластера G_q^+, таке відношення можна подати як:

$$G_p^+ \succ G_q^+ \quad (3.8)$$

де G_p^+ - старший кластер, а G_q^+ - молодший кластер у межах ієрархічного подання моделі. Для такого рівня вводиться множина ієрархічних відношень:

$$R_{pq}^{hier} = \{supervises, reportsTo, aggregatesStateFrom, transfersPolicyTo, escalatesRiskTo\} \quad (3.9)$$

та множина ієрархічних операцій:

$$O_{pq}^{hier} = \{aggregateStateLogs, transferRiskMap, propagateRecommendation, synchronizeContext, updateHigherLevelState\} \quad (3.10)$$

У такому поданні молодший кластер може передавати старшому кластеру узагальнені записи стану, контекстні характеристики, результати аналізу вразливостей або оцінки ризику. Старший кластер, у свою чергу, може виконувати агрегування станів, формування узагальненої карти ризиків, передавання політик реагування або поширення рекомендацій до нижчого рівня.

Отже, багаторівневість онтологічної моделі проявляється через послідовний перехід від плоского подання G до кластерного подання G_{12}^{cl}, а далі - до ієрархічного подання на основі відношення $G_p^+ \succ G_q^+$. Це дозволяє формалізувати не лише внутрішню структуру БСМ, а й взаємодію між її локальними кластерами, обмін даними із зовнішніми сутностями та узгодження станів між старшими й молодшими рівнями онтологічної моделі.

3.2 Метод семантичного визначення та логування станів компонентів БСМ як базовий рівень

Після визначення загальної архітектури багаторівневої онтологічної моделі доцільно перейти до розгляду методу семантичного визначення та логування станів компонентів бездротових сенсорних мереж. Саме цей метод формує базовий рівень запропонованої моделі, оскільки забезпечує перехід від первинних телеметричних, топологічних і контекстних даних до формалізованого онтологічного подання поточного стану БСМ.

У межах дисертаційної роботи цей метод розглядається як один із результатів наукової новизни, що отримав подальший розвиток. Його сутність полягає не лише в описі структури мережі, а й у семантичному визначенні актуального стану її

компонентів, фіксації параметрів спостережуваних об’єктів, узгодженні цих параметрів із топологією мережі та формуванні онтологічного запису стану, придатного для подальшого аналізу вразливостей і оцінювання ризику.

На відміну від звичайного накопичення телеметричних даних, запропонований метод забезпечує їх семантичну інтерпретацію. Первинні значення енергії, затримки, навантаження, якості каналу, рівня сигналу, втрат пакетів, а також параметри спостережуваних об’єктів або середовища перетворюються на узгоджені онтологічні сутності, пов’язані з вузлами, каналами, маршрутами, сегментами, спостережуваними об’єктами та часовими записами стану. Завдяки цьому поточний стан БСМ подається не як набір розрізнених числових показників, а як структурований семантичний опис, придатний для логічного висновку.

Метод семантичного визначення та логування станів компонентів БСМ виконує три взаємопов’язані функції. Перша полягає у формуванні онтологічного подання структури мережі як сукупності вузлів, каналів, сегментів, кластерів, маршрутів і зв’язків між ними. Друга пов’язана з фіксацією поточних параметрів функціонування компонентів БСМ та спостережуваних об’єктів, зокрема телеметричних, енергетичних, часових, навантажувальних і комунікаційних характеристик. Третя полягає у створенні формалізованого запису поточного стану, який подається через клас StateLogRecord і використовується як вхідна основа для методу аналізу вразливостей.

Важливою особливістю цього методу є врахування як статичних, так і динамічних характеристик БСМ. До статичних характеристик належать склад мережі, типи вузлів, маршрути, сегменти, кластери та зв’язки між компонентами. До динамічних характеристик належать параметри, що змінюються в процесі функціонування мережі: залишкова енергія, затримка, навантаження, доступність вузлів, стабільність каналів, рівень втрат пакетів, якість сигналу, а також контрольовані параметри спостережуваного об’єкта або середовища. Таке поєднання дозволяє описувати не лише топологію БСМ, а й її актуальний функціональний стан у конкретний момент часу.

Таким чином, метод семантичного визначення та логування станів компонентів БСМ є базовою ланкою багаторівневої онтологічної моделі. Він забезпечує зв’язок між фізичним рівнем функціонування мережі, рівнем збору телеметрії, рівнем семантичного подання станів і наступними методами аналізу вразливостей, оцінювання ризику та адаптивного керування. Далі розглядаються модель цього методу, основні онтологічні сутності, формалізація характеристик вузлів і каналів зв’язку, а також покрокове виконання процедури семантичного визначення та логування станів компонентів БСМ.

3.2.1 Модель методу семантичного визначення та логування станів комповнентів бездротових сенсорних мереж як базовий рівень

Модель методу семантичного визначення та логування станів компонентів БСМ призначена для формального подання поточного стану мережі, її структурних елементів, параметрів спостережуваних об’єктів і зв’язків між ними. У межах багаторівневої онтологічної моделі цей метод виконує роль базового рівня, оскільки саме на ньому формується первинне семантично узгоджене подання даних, що надалі використовується для аналізу вразливостей, оцінювання ризику та формування рекомендацій щодо реагування.

Необхідність побудови такої моделі зумовлена тим, що БСМ не може бути описана лише як сукупність вузлів і каналів зв’язку. Для подальшого логічного висновку необхідно враховувати роль компонентів у топології, їх функціональний стан, динамічні параметри, контекст функціонування, якість каналів зв’язку, а також зв’язок із фізичними або технологічними об’єктами, параметри яких контролюються сенсорними вузлами.

У запропонованому підході поточний стан БСМ подається через сукупність онтологічних сутностей, що описують вузли, канали, маршрути, сегменти, кластери, спостережувані об’єкти, контрольовані параметри, телеметричні знімки та записи стану. Таке подання дозволяє поєднати статичні характеристики мережі з динамічними параметрами, які змінюються в часі, та сформувати формалізований

запис поточного стану. Узагальнену онтологічну модель семантичного подання топології та поточного стану бездротової сенсорної мережі наведено на рис. 3.1.

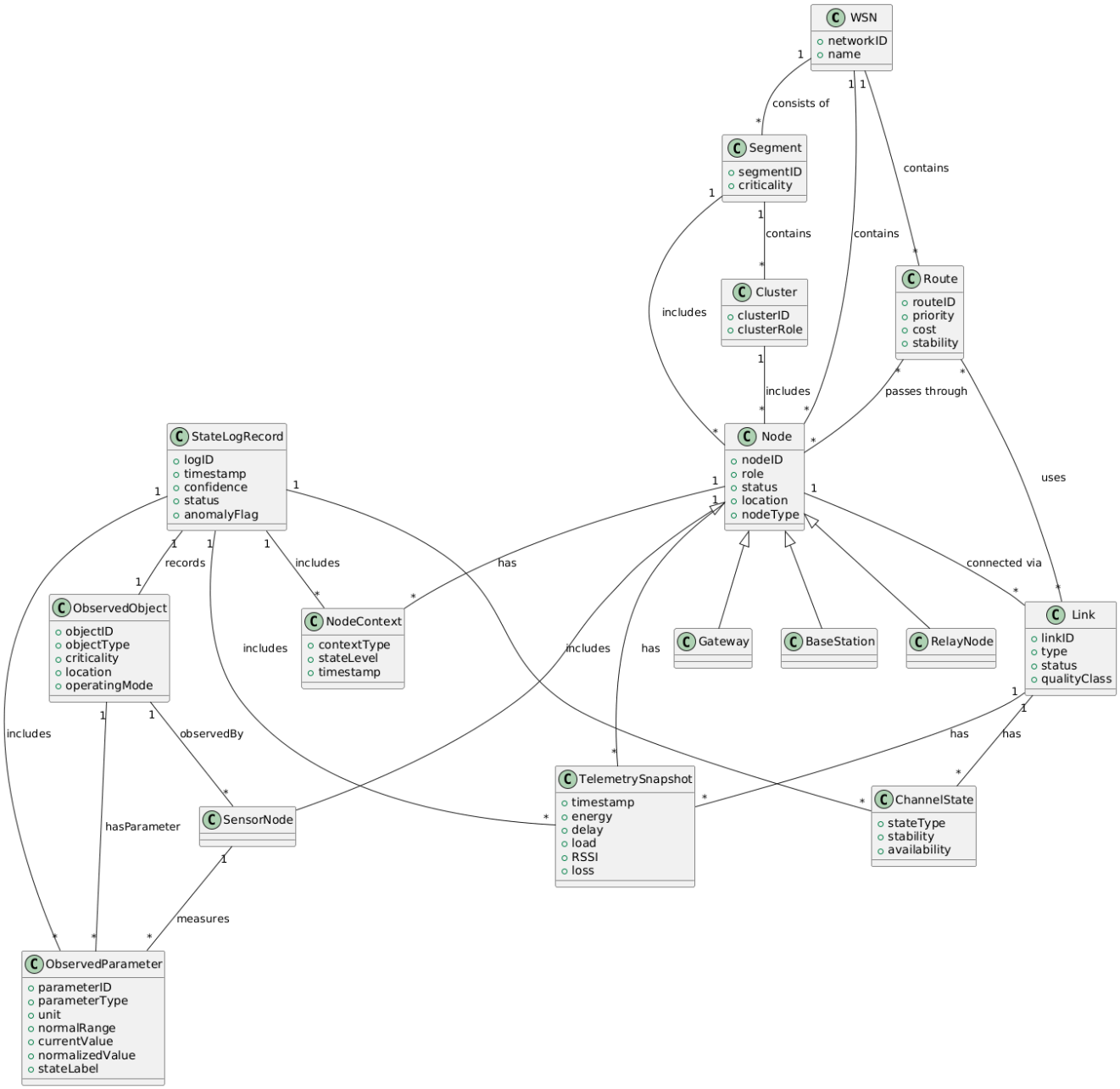

Рисунок 3.1 – Онтологічна модель семантичного подання топології бездротової сенсорної мережи

Основні сутності, що використовуються для топологічного опису БСМ у межах **методу семантичного подання топології**, наведено в табл. 3.2.

Таблиця 3.2 – Основні сутності топологічного опису БСМ за моделлю.

Сутність	Зміст	Основні атрибути
WSN	Бездротова сенсорна мережа як цілісний об’єкт онтологічного опису	**networkID, name**, загальний стан
Segment	Топологічний або функціональний сегмент мережі	**segmentID, criticality**, склад вузлів
Cluster	Локальна група вузлів у межах сегмента або кластерної організації мережі	**clusterID, clusterRole,** рівень пріоритету
Node	Узагальнений вузол мережі	**nodeID, role, status, location, nodeType**
SensorNode	Сенсорний вузол, що виконує збір даних	тип сенсора, стан, енергетичні характеристики
RelayNode	Проміжний вузол для ретрансляції повідомлень	статус маршрутизації, навантаження, доступність
Gateway	Шлюз мережі, що забезпечує взаємодію з зовнішнім середовищем або іншими сегментами	пропускна здатність, стан з’єднання, роль у топології
BaseStation	Базова станція для приймання, агрегації та обробки даних	ідентифікатор, режим роботи, доступність
Link	Канал зв’язку між вузлами мережі	**linkID, type, status, qualityClass**
Route	Маршрут передавання даних у мережі	**routeID, priority, cost, stability**
TelemetrySnapshot	Знімок поточного телеметричного стану вузла або каналу	**timestamp, energy, delay, load, RSSI, loss**
NodeContext	Контекстний опис поточного стану вузла	**contextType, stateLevel, timestamp**
ChannelState	Контекстний опис поточного стану каналу зв’язку	**stateType, stability, availability**
ObservedObject	Спостережуваний фізичний, технологічний або середовищний об’єкт	**objectID, objectType, criticality, location, operatingMode**
ObservedParameter	Параметр спостережуваного об’єкта або середовища	**parameterID, parameterType, unit, normalRange, currentValue, normalizedValue, stateLabel**
StateLogRecord	Формалізований запис поточного стану моделі	**logID, timestamp, confidence, status, anomalyFlag**

Виділення наведених сутностей дозволяє сформувати цілісний онтологічний опис топології БСМ і водночас пов’язати її з об’єктами, стан яких контролюється за допомогою сенсорних вузлів. У такому поданні вузли, канали, маршрути й сегменти описують структуру сенсорної мережі, тоді як спостережувані об’єкти та їх параметри відображають предметну область моніторингу. Це створює основу для

подання характеристик мережі, телеметричних параметрів і станів спостережуваних об’єктів у межах єдиного онтологічного середовища.

Важливо, що семантичне подання має враховувати динамічний характер функціонування як БСМ, так і об’єктів спостереження. На відміну від статичних інженерних схем, стан мережі може змінюватися під впливом відмов вузлів, втрати зв’язку, появи нових маршрутів, зміни навантаження або зовнішніх факторів. Одночасно можуть змінюватися параметри спостережуваного обладнання чи середовища, зокрема температура, рівень, тиск, витрата, струм, вологість або інші контрольовані характеристики. Тому вузли, канали й спостережувані об’єкти мають бути пов’язані не лише зі структурою мережі, а й з актуальними параметрами поточного стану.

Семантичне подання топології також узгоджується з результатами нечіткого моделювання, отриманими в другому розділі. Нечіткі оцінки працездатності вузлів, імовірності передавання даних, доступності та якості каналів, а також лінгвістичні стани контрольованих параметрів можуть бути подані як атрибути або контекстні характеристики відповідних онтологічних сутностей. Це дозволяє аналізувати вразливості та ризики не для абстрактної топології, а для мережі й об’єктів спостереження в їх актуальному функціональному стані. У результаті семантичне подання БСМ забезпечує формування структурного та контекстного каркаса моделі, поєднує статичні й динамічні характеристики компонентів і створює основу для логування станів, аналізу вразливостей та оцінювання ризику.

3.2.2 Формалізація характеристик вузлів і каналів зв’язку

Після семантичного подання топології БСМ необхідно формалізувати характеристики її основних структурних елементів - вузлів і каналів зв’язку. Якщо топологічний опис визначає склад мережі та зв’язки між компонентами, то формалізація характеристик наповнює ці сутності змістом через систему атрибутів, параметрів і станів.

У межах онтологічної моделі вузол мережі розглядається як об’єкт, що має ідентифікаційні ознаки, роль у топології та сукупність функціональних

характеристик. До них належать енергетичний стан, пропускна здатність, середня затримка, рівень навантаження, участь у маршрутизації, тип датчика, потужність передавання та інші параметри, які визначають поточний стан вузла як активного елемента БСМ.

Для узагальненого подання поточного стану вузла може бути використане співвідношення:

$$S(\upsilon_i) = \alpha \times E(\upsilon_i) + \beta \times B(\upsilon_i) + \gamma \times D(\upsilon_i) + \delta \times H(\upsilon_i) \qquad (3.2)$$

де

- E(υi) – рівень залишкової енергії вузла;
- B(υi) – пропускна здатність вузла;
- D(υi) – середня затримка вузла; H(υi) – рівень навантаження вузла;
- α, β, γ, δ – вагові коефіцієнти для кожного параметра.

Наведене співвідношення дозволяє подати стан вузла у вигляді інтегральної характеристики, придатної для подальшого використання в блоці виявлення вразливостей і блоці оцінки ризиків. Вагові коефіцієнти можуть змінюватися залежно від умов функціонування мережі та пріоритетів аналізу.

Канал зв’язку в межах Методу опису мережі також подається як окрема семантична сутність із власними характеристиками. До них належать пропускна здатність, затримка передавання, готовність, рівень втрат пакетів, стабільність з’єднання, інтенсивність старіння інформації та інші параметри, що визначають якість комунікаційного рівня. Тому клас Link розглядається не лише як зв’язок між вузлами, а як носій функціонально значущих характеристик.

Важливою особливістю такого подання є можливість включення результатів нечіткого моделювання, отриманих у другому розділі. Нечіткі оцінки працездатності вузлів, імовірності передавання даних, ефективної пропускної здатності та доступності каналів можуть бути пов’язані з відповідними онтологічними сутностями як їхні семантичні атрибути. Завдяки цьому вузли й канали описуються не як статичні елементи топології, а як компоненти з актуальним функціональним станом.

Формалізація характеристик вузлів і каналів повинна забезпечувати семантичну узгодженість параметрів у межах усієї онтологічної моделі. Це означає, що енергетичні, часові, навантажувальні та комунікаційні характеристики мають бути подані у формі, придатній для використання в логічних правилах, оцінюванні вразливостей і розрахунку ризиків. У результаті кожен вузол і кожен канал стають не лише структурними, а й функціонально описаними елементами онтологічної моделі. Це забезпечує перехід від семантичного подання топології до параметричного опису поточного стану мережі та створює основу для подальшого подання енергетичних, часових і навантажувальних параметрів БСМ.

3.2.3 Покрокове виконання методу семантичного визначення та логування станів компонентів БСМ

Метод семантичного визначення та логування станів компонентів БСМ реалізується в межах блоку опису мережі та забезпечує перехід від первинних телеметричних даних до формалізованого онтологічного подання поточного стану мережі. Його призначення полягає не лише у фіксації значень параметрів, а й у їх семантичному узгодженні з топологією мережі, роллю компонентів, результатами нечіткого оцінювання та контекстом функціонування.

У загальному вигляді виконання методу передбачає такі етапи: ідентифікацію спостережуваного обладнання та пов’язаних із ним компонентів БСМ; сканування поточного стану обладнання й каналів зв’язку; формування часового знімка стану; перевірку повноти, допустимості та достовірності даних; нормування параметрів; нечітку інтерпретацію значень; семантичне зіставлення параметрів із онтологічною моделлю; формування онтологічного запису поточного стану; передавання результату до методу аналізу вразливостей.

Послідовність виконання методу семантичного визначення та логування станів компонентів БСМ наведено на рис. 3.2.

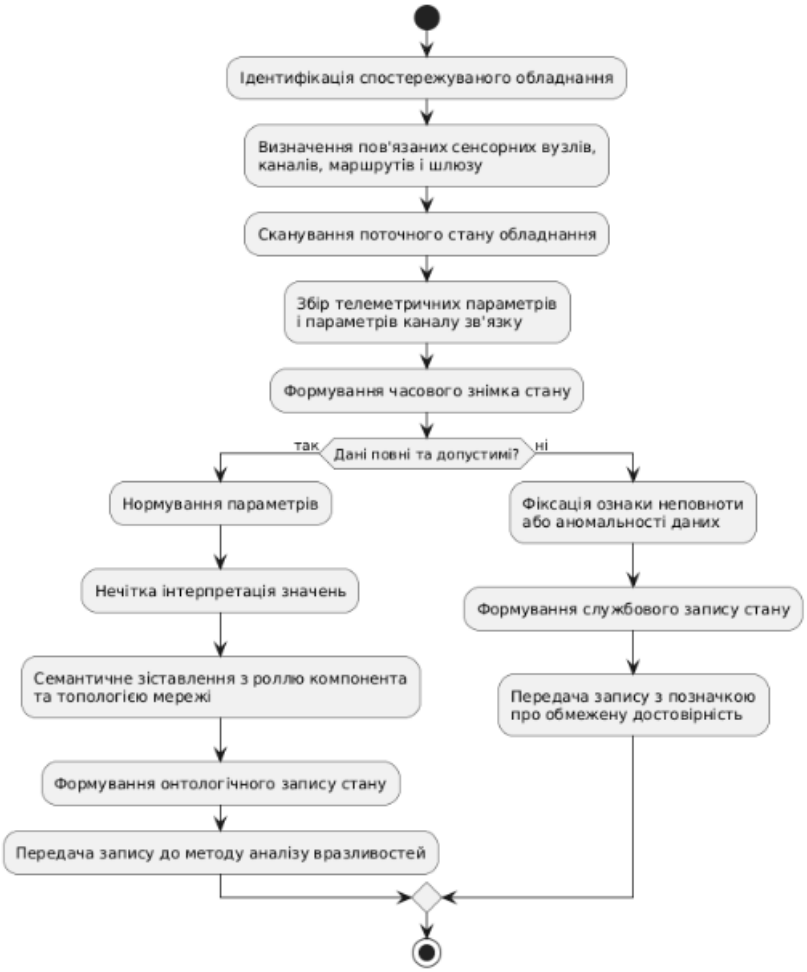

Рисунок 3.2 - Діаграма діяльності методу семантичного визначення та логування станів компонентів БСМ

Як показано на рис. 3.2, метод виконується як послідовність дій від ідентифікації спостережуваного обладнання та пов’язаних із ним компонентів БСМ до формування онтологічного запису поточного стану. Особливістю методу є те, що навіть у разі неповноти або аномальності даних результат не відкидається, а фіксується як стан з обмеженою достовірністю, який може бути врахований у подальшому аналізі вразливостей і ризику.

Розглянемо проходження зазначених етапів на прикладі спостереження за промисловим обладнанням, стан якого контролюється за допомогою сенсорів температури, рівня, струму навантаження, тиску, витрати, напруги живлення та параметрів бездротового каналу передавання даних. У межах прикладного

сценарію таке обладнання розглядається як екземпляр класу ObservedObject, а його контрольовані характеристики - як екземпляри або типи класу ObservedParameter.

На першому кроці виконується ідентифікація спостережуваного обладнання. У межах онтологічної моделі цей об’єкт подається через клас ObservedObject, який містить ідентифікатор об’єкта, його тип, місце розташування, режим роботи та рівень критичності. Це дозволяє відокремити фізичний або технологічний об’єкт спостереження від компонентів самої бездротової сенсорної мережі.

На другому кроці визначаються пов’язані з об’єктом компоненти БСМ: сенсорні вузли, канали зв’язку, маршрути передавання даних, ретранслятори та шлюз. У межах онтологічної моделі ці елементи подаються через класи SensorNode, RelayNode, Gateway, Link та Route. Саме на цьому етапі встановлюється зв’язок між спостережуваним об’єктом і сенсорною мережею, яка забезпечує отримання та передавання його параметрів.

На третьому кроці виконується сканування поточного стану спостережуваного обладнання. Для цього визначаються параметри, які підлягають контролю, наприклад температура, рівень, струм, тиск, витрата або напруга. У межах онтологічної моделі ці параметри належать до класу ObservedParameter і пов’язуються з відповідним екземпляром класу ObservedObject.

На четвертому кроці здійснюється збір телеметричних параметрів і параметрів каналу зв’язку. Сенсорні вузли фіксують значення контрольованих параметрів, а мережеві компоненти - показники передавання даних, зокрема затримку, втрати пакетів, рівень сигналу, доступність вузлів і стабільність каналу. У межах онтологічної моделі ці дані подаються через класи TelemetrySnapshot, NodeContext і ChannelState.

На п’ятому кроці формується часовий знімок стану. Він фіксує значення параметрів у певний момент часу, ідентифікатори сенсорних вузлів, стан каналів зв’язку та службові характеристики передавання даних. У межах онтологічної моделі такий знімок подається через клас TelemetrySnapshot, який пов’язує параметри спостережуваного об’єкта з поточним станом вузлів і каналів БСМ.

На шостому кроці виконується перевірка повноти, допустимості та узгодженості даних. Якщо всі необхідні параметри отримано, їх значення перебувають у допустимих межах і не суперечать іншим вимірюванням, дані передаються до подальшої обробки. Якщо ж частина даних відсутня або має аномальний характер, у майбутньому записі стану формується ознака обмеженої достовірності. У межах онтологічної моделі така інформація відображається через атрибути класу StateLogRecord, зокрема confidence, status та anomalyFlag.

На сьомому кроці, за умови повноти й допустимості даних, виконується нормування параметрів. Значення різної фізичної природи приводяться до узгодженого вигляду, придатного для подальшого порівняння та обробки. У межах онтологічної моделі нормовані значення можуть подаватися як атрибути класу ObservedParameter, зокрема через поле normalizedValue.

На восьмому кроці здійснюється нечітка інтерпретація значень. Числові параметри перетворюються на лінгвістичні або семантичні оцінки, наприклад «нормальна температура», «низький рівень», «високе навантаження», «нестабільний канал» або «критична затримка». У межах онтологічної моделі такі інтерпретації можуть подаватися через атрибути stateLabel, stateLevel у класах ObservedParameter, NodeContext і ChannelState.

На дев’ятому кроці виконується семантичне зіставлення отриманих параметрів із роллю компонента та топологією мережі. Однакове значення параметра може мати різне значення залежно від того, чи пов’язаний сенсорний вузол із локальним вимірюванням, чи забезпечує передавання критичної телеметрії через важливий маршрут. У межах онтологічної моделі це зіставлення реалізується через зв’язки між класами ObservedObject, SensorNode, Link, Route, NodeContext і ChannelState.

На десятому кроці формується онтологічний запис поточного стану. Він об’єднує спостережуваний об’єкт, контрольовані параметри, телеметричний знімок, контекст вузлів, стан каналів зв’язку, часову мітку та ознаки достовірності даних. У межах онтологічної моделі результат цього кроку подається як екземпляр

класу StateLogRecord, який включає дані класів ObservedObject, ObservedParameter, TelemetrySnapshot, NodeContext і ChannelState.

На одинадцятому кроці сформований онтологічний запис передається до методу аналізу вразливостей. Результатом методу семантичного визначення та логування станів є не висновок про небезпеку, а формалізований і семантично узгоджений опис поточного стану спостережуваного об’єкта, сенсорних вузлів, каналів зв’язку та маршруту передавання даних. Саме цей запис використовується як вхідна основа для подальшого виявлення вразливостей, оцінювання ризику та формування рекомендацій щодо реагування.

Якщо на етапі перевірки встановлено, що дані неповні, недопустимі або аномальні, виконується альтернативна гілка методу. У такому випадку фіксується ознака неповноти або аномальності даних, формується службовий запис стану та здійснюється передавання запису з позначкою про обмежену достовірність. У межах онтологічної моделі такий результат також подається через клас StateLogRecord, однак його атрибути confidence, status або anomalyFlag вказують на обмеження подальшої інтерпретації.

3.3 Метод аналізу вразливостей у структурі багаторівневої онтології

Після формування семантично узгодженого запису поточного стану БСМ наступним етапом багаторівневої онтологічної моделі є аналіз вразливостей її компонентів. У межах дисертаційної роботи цей етап подається як удосконалений метод аналізу вразливостей бездротових сенсорних мереж, що забезпечує перехід від формалізованого опису стану мережі до встановлення слабких місць, критичних режимів і потенційно небезпечних конфігурацій її функціонування.

Вхідною основою для цього методу є результати методу семантичного визначення та логування станів компонентів БСМ, зокрема онтологічні записи StateLogRecord, телеметричні знімки, контекст вузлів, стани каналів зв’язку та параметри спостережуваних об’єктів. На цьому рівні первинні значення параметрів уже не розглядаються як ізольовані числові показники, а інтерпретуються в

контексті топології мережі, ролі компонента, умов середовища, зовнішніх загроз і результатів нечіткого оцінювання.

Сутність методу аналізу вразливостей полягає у встановленні семантичних залежностей між поточним станом компонента БСМ, контекстними факторами, можливими загрозами та типами вразливостей. На відміну від підходів, що фіксують лише перевищення окремих порогових значень, запропонований метод враховує сукупність взаємопов'язаних ознак: енергетичний стан вузла, навантаження, затримку, якість каналу, втрати пакетів, роль компонента в маршрутизації, належність до критичного сегмента та вплив зовнішніх умов.

У запропонованій моделі вразливість розглядається як семантично інтерпретований стан компонента або спостережуваного об'єкта, що виникає внаслідок поєднання технічних, топологічних, фізичних, середовищних і зовнішніх факторів. Такий підхід дозволяє пов'язати вразливість не лише з конкретним вузлом, каналом, маршрутом або сегментом, а й із відповідними контекстними ознаками, джерелами загроз, параметрами спостереження та рівнем достовірності даних.

З погляду наукової новизни цей підрозділ відображає удосконалення методу аналізу вразливостей БСМ. Удосконалення полягає у використанні онтологічних правил, контекстно залежних ознак і формалізованих записів стану для поетапного виявлення, класифікації та інтегрального оцінювання вразливостей компонентів мережі. Завдяки цьому метод забезпечує не лише встановлення факту наявності слабкого місця, а й формування узагальненої оцінки вразливості, придатної для подальшого методу оцінки ризику.

Таким чином, метод аналізу вразливостей компонентів БСМ є аналітичним рівнем багаторівневої онтологічної моделі. Він забезпечує перехід від логованого поточного стану мережі до формалізованого подання небезпечних станів, слабких місць і критичних режимів функціонування. Далі розглядаються онтологічна модель джерел вразливостей і загроз, основні сутності та зв'язки цієї моделі, формалізація вразливостей на основі онтологічних правил, інтегральна оцінка

вразливості та покрокове виконання методу аналізу вразливостей компонентів БСМ.

3.3.1 Модель методу аналізу вразливості компонентів БСМ

Аналіз вразливостей у бездротових сенсорних мережах потребує врахування не лише окремих технічних характеристик вузлів і каналів, а й сукупності факторів, що визначають умови функціонування мережі, її структурні особливості та потенційні зовнішні впливи. У межах багаторівневої онтологічної моделі вразливість розглядається як семантично інтерпретований результат взаємодії властивостей мережевих компонентів, їх поточного стану, контекстних характеристик і можливих загроз.

До основних джерел вразливостей у БСМ належать внутрішні характеристики її компонентів: вузлів, каналів зв’язку, шлюзів, базових станцій, сегментів і маршрутів. Вразливий стан може виникати внаслідок зниження енергетичних ресурсів вузла, перевантаження, деградації характеристик каналу, нестабільності маршрутизації, топологічної критичності окремого сегмента або фізичної недоступності мережевого елемента.

Окрему групу становлять зовнішні та середовищні фактори, які можуть посилювати наявні вразливості або створювати передумови для виникнення нових критичних станів. До них належать електромагнітні завади, фізичні перешкоди, зміна параметрів середовища, нестабільність бездротового каналу, несанкціонований доступ, перевантаження трафіком або відмова окремих компонентів. У запропонованій моделі такі фактори подаються як потенційні загрози, пов’язані з відповідними компонентами мережі.

Контекстні характеристики відіграють ключову роль у виявленні критичних станів, оскільки дозволяють інтерпретувати окремі значення параметрів не ізольовано, а у взаємозв’язку з типом компонента, його роллю в топології, режимом функціонування та умовами середовища. Один і той самий параметр може мати різне значення залежно від контексту: наприклад, підвищене навантаження для

периферійного вузла може бути допустимим, тоді як для шлюзу або ретранслятора воно може свідчити про наближення до критичного режиму.

До основних контекстних характеристик, що використовуються для виявлення критичних станів, належать енергетичні, часові, навантажувальні, комунікаційні та середовищні параметри. Енергетичні характеристики відображають залишковий ресурс вузла та інтенсивність його споживання. Часові характеристики описують затримки, час доставки даних і старіння інформації. Навантажувальні параметри визначають рівень використання ресурсів вузлів, каналів і маршрутів. Комунікаційні характеристики відображають якість зв'язку, втрати пакетів, доступність і стабільність каналу, а середовищні параметри характеризують зовнішні умови функціонування мережі.

У межах онтологічної моделі зазначені характеристики можуть бути пов'язані з класами Node, Link, Route, Segment, NodeContext, ChannelState та TelemetrySnapshot. Це дозволяє не лише зафіксувати поточні параметри мережі, а й інтерпретувати їх як ознаки нормального, нестійкого, вразливого або критичного стану відповідного компонента.

Вразливості та загрози в БСМ доцільно розглядати як взаємопов'язані онтологічні сутності. Наприклад, загроза перевантаження є особливо значущою для вузлів, що виконують маршрутизаційні або шлюзові функції, тоді як загроза електромагнітних завад найбільш суттєво впливає на канали зв'язку. Такий підхід дозволяє враховувати не лише факт наявності загрози, а й те, до якого компонента вона застосовується та в якому контексті може призвести до критичного стану.

Для формалізованого подання таких взаємозв'язків використовується онтологічна схема, що відображає зв'язки між компонентами мережі, типами вразливостей, контекстними факторами та загрозами. Узагальнену онтологічну схему основних джерел вразливостей і загроз у бездротовій сенсорній мережі наведено на рис. 3.3.

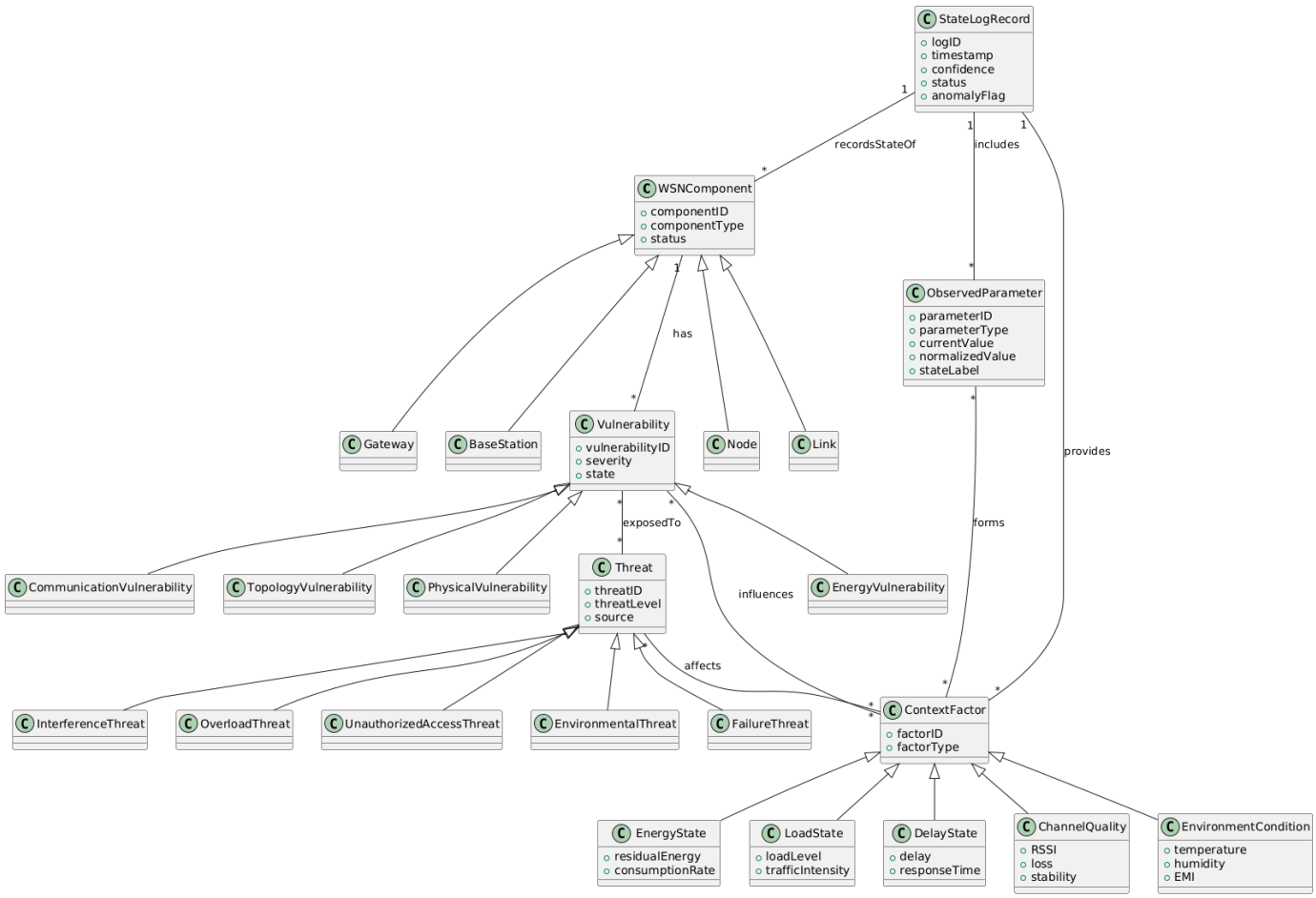

Рисунок 3.3 – Онтологічна модель основних джерел вразливості і загроз у бездротовій сенсорній мережі

Наведена схема відображає багатофакторний характер джерел вразливостей у БСМ та підкреслює необхідність їх спільного розгляду в межах онтологічної моделі.

Основні сутності онтологічної схеми джерел вразливостей і загроз у БСМ, а також їх призначення, атрибути та зв’язки наведено в табл. 3.3:

Таблиця 3.3 – Основні сутності онтологічної схеми джерел вразливостей і загроз у БСМ.

Сутність (клас)	**Призначення**	**Основні атрибути**	**Основні зв’язки**
WSNComponent	Базова узагальнена сутність для подання компонентів бездротової сенсорної мережі	componentID, componentType, status	Є базовим класом для Node, Link, Gateway, BaseStation; пов’язаний із Vulnerability через зв’язок has

Node	Подання окремого вузла БСМ	успадковує атрибути WSNComponent	Є підкласом WSNComponent; може мати одну або декілька вразливостей
Link	Подання каналу зв'язку між елементами мережі	успадковує атрибути WSNComponent	Є підкласом WSNComponent; може мати вразливості, пов'язані з якістю каналу
Gateway	Подання шлюзу мережі	успадковує атрибути WSNComponent	Є підкласом WSNComponent; розглядається як компонент мережі з можливими вразливостями
BaseStation	Подання базової станції як центрального елемента мережі	успадковує атрибути WSNComponent	Є підкласом WSNComponent; також може бути пов'язана з вразливостями
StateLogRecord	Формалізований запис поточного стану моделі, сформований методом логування	logID, timestamp, confidence, status, anomalyFlag	recordsStateOf WSNComponent, includes ObservedParameter, provides ContextFacto
ObservedParameter	Контрольований параметр спостережуваного об'єкта або середовища	parameterID, parameterType, currentValue, normalizedValue, stateLabel	includedIn StateLogRecord, forms ContextFactor
Vulnerability	Узагальнене подання вразливості мережевого компонента	vulnerabilityID, severity, state	Пов'язана з WSNComponent через has; зазнає впливу ContextFactor через influences; асоційована із Threat через exposed to
EnergyVulnerability	Подання енергетичної вразливості	успадковує атрибути Vulnerability	Є підкласом Vulnerability
CommunicationVulnerability	Подання комунікаційної вразливості	успадковує атрибути Vulnerability	Є підкласом Vulnerability
TopologyVulnerability	Подання топологічної вразливості	успадковує атрибути Vulnerability	Є підкласом Vulnerability
PhysicalVulnerability	Подання фізичної вразливості	успадковує атрибути Vulnerability	Є підкласом Vulnerability
ContextFactor	Узагальнене подання контекстного фактора, що впливає на стан компонентів та формування вразливостей	factorID, factorType	Є базовим класом для EnergyState, LoadState, DelayState, ChannelQuality, EnvironmentCondition; пов'язаний із Vulnerability через influences

EnergyState	Опис енергетичного стану компонента мережі	residualEnergy, consumptionRate	Є підкласом ContextFactor; впливає на формування енергетичних вразливостей
LoadState	Опис стану навантаження	loadLevel, trafficIntensity	Є підкласом ContextFactor; впливає на перевантаження та пов’язані вразливості
DelayState	Опис часових характеристик функціонування	delay, responseTime	Є підкласом ContextFactor; впливає на оцінювання критичних станів
ChannelQuality	Подання характеристик якості каналу зв’язку	RSSI, loss, stability	Є підкласом ContextFactor; впливає на комунікаційні вразливості
EnvironmentCondition	Подання умов зовнішнього середовища	temperature, humidity, EMI	Є підкласом ContextFactor; впливає на фізичні та комунікаційні вразливості
Threat	Узагальнене подання потенційної загрози	threatID, threatLevel, source	Є базовим класом для конкретних типів загроз; пов’язана з Vulnerability через exposed to
FailureThreat	Подання загрози відмови компонента	успадковує атрибути Threat	Є підкласом Threat
InterferenceThreat	Подання загрози завад або перешкод	успадковує атрибути Threat	Є підкласом Threat
OverloadThreat	Подання загрози перевантаження	успадковує атрибути Threat	Є підкласом Threat
UnauthorizedAccessThreat	Подання загрози несанкціонованого доступу	успадковує атрибути Threat	Є підкласом Threat
EnvironmentalThreat	Подання загрози несприятливого впливу зовнішнього середовища	успадковує атрибути Threat	Є підкласом Threat

Наведена система сутностей дозволяє формалізувати взаємозв’язки між компонентами мережі, типами вразливостей, контекстними факторами та загрозами. Завдяки цьому стає можливим перехід від фіксації числових або телеметричних параметрів до встановлення факту наявності певної вразливості та її подальшої інтерпретації в блоці оцінки ризиків.

Підсумуючи, джерела вразливостей, загрози та контекстні характеристики критичних станів у БСМ формуються як взаємопов’язані елементи єдиного

семантичного середовища. Таке подання забезпечує основу для формального виявлення слабких місць мережі та подальшої побудови узагальненої оцінки вразливості її компонентів.

3.3.2 Формалізація вразливостей на основі онтологічних правил та їх інтегральне оцінювання

Після визначення джерел вразливостей, загроз і контекстних характеристик критичних станів необхідно формалізувати механізм їх виявлення в межах онтологічної моделі. Для цього використовуються онтологічні правила, які дозволяють пов’язати параметри вузлів, каналів, сегментів, маршрутів, спостережуваних об’єктів і записів поточного стану з відповідними типами вразливостей.

У межах запропонованого підходу вразливість визначається не за одним окремим параметром, а на основі сукупності взаємопов’язаних ознак. Наприклад, критичний стан вузла може встановлюватися не лише через низький рівень залишкової енергії, а через поєднання низької енергії, підвищеного навантаження, збільшеної затримки, погіршення якості каналу та важливої ролі вузла в топології мережі. Аналогічно вразливий стан каналу зв’язку може визначатися через поєднання втрат пакетів, зниження стабільності з’єднання, погіршення показників RSSI та несприятливих умов середовища.

З урахуванням оновленої моделі логування станів вхідною основою для формалізації вразливостей є екземпляри класу StateLogRecord, які містять формалізований опис поточного стану компонента БСМ, телеметричний знімок, контекст вузла, стан каналу зв’язку, часову мітку, ознаки достовірності даних та параметри спостережуваного об’єкта. Контрольовані параметри спостережуваного об’єкта або середовища подаються через клас ObservedParameter і можуть характеризувати температуру, рівень, тиск, витрату, струм, напругу, вологість, концентрацію або інші параметри залежно від предметної області моніторингу.

Онтологічні правила забезпечують перехід від числових, лінгвістичних і контекстних характеристик до семантично інтерпретованих фактів про вразливості.

У загальному вигляді таке правило може описувати ситуацію, коли певна комбінація параметрів компонента, його контексту, стану каналу та зовнішнього впливу відповідає конкретному типу вразливості. Наприклад, низький рівень енергії та високе навантаження можуть інтерпретуватися як енергетична вразливість вузла, а висока затримка разом із великими втратами пакетів - як комунікаційна вразливість каналу.

Важливо, що такі правила враховують не лише локальні характеристики компонента, а й його місце в загальній структурі БСМ. Однакове значення параметра може мати різну критичність для периферійного сенсорного вузла, ретранслятора, шлюзу або базової станції. Тому в правилах доцільно враховувати тип компонента, його роль у маршрутизації, належність до критичного сегмента, участь у передаванні важливої телеметрії та вплив можливої відмови на зв’язність мережі.

Формалізовані правила можуть використовувати класи WSNComponent, Node, Link, Gateway, BaseStation, StateLogRecord, ObservedParameter, ContextFactor, EnergyState, LoadState, DelayState, ChannelQuality, EnvironmentCondition, Vulnerability та Threat. Для зв’язування цих сутностей використовуються відношення recordsStateOf, includes, provides, forms, influences, hasVulnerability, exposedTo, affects та contributesTo. Завдяки цьому вразливість подається не як ізольована ознака, а як результат логічного зв’язку між компонентом мережі, його поточним станом, параметрами спостереження, контекстом функціонування та можливими загрозами.

Результатом застосування онтологічних правил є формування впорядкованого набору фактів про вразливості компонентів мережі. Такі факти містять тип вразливості, компонент або об’єкт, до якого вона належить, пов’язані контекстні ознаки, джерело загрози, рівень прояву та ознаки достовірності. Однак у реальних умовах компонент БСМ зазвичай зазнає впливу не однієї, а кількох взаємопов’язаних вразливостей, тому виникає необхідність їх подальшого узагальнення у вигляді інтегральної оцінки.

Інтегральна вразливість компонента мережі розглядається як узагальнена оцінка, що враховує вплив трьох груп факторів: технічних, фізичних та зовнішніх. До технічних факторів належать характеристики внутрішнього стану вузлів і каналів, зокрема енергетичні, часові, навантажувальні та комунікаційні параметри. Фізичні фактори відображають обмеження або пошкодження, пов'язані з умовами експлуатації компонентів мережі. Зовнішні фактори охоплюють вплив середовища, завад, несанкціонованого доступу та інших джерел загроз, які можуть посилювати наявні слабкі місця.

У формалізованому вигляді інтегральна оцінка вразливості може бути подана як:

$$Vm = \alpha \times \sum_{i=1}^{n} P_i \times I_i + \beta \times \sum_{j=1}^{m} F_j \times S_j + \gamma \times \sum_{k=1}^{l} E_k \times T_k \ , \tag{3.3}$$

де V_m - інтегральна оцінка вразливості (m)-го компонента БСМ, яка відображає узагальнений рівень його схильності до переходу в небезпечний або нестійкий стан. Величини (P_i) та (I_i) описують технічну складову вразливості: (P_i) характеризує імовірність прояву (i)-го технічного фактора, а (I_i) - інтенсивність або силу його впливу на функціонування компонента. До таких факторів можуть належати зниження залишкової енергії, перевантаження вузла, погіршення якості каналу, збільшення затримки або втрат пакетів.

Величини (F_j) та (S_j) характеризують фізичну складову вразливості. Параметр (F_j) відображає рівень прояву (j)-го фізичного фактора, а (S_j) - його значущість для відповідного компонента мережі. До цієї групи можуть належати пошкодження обладнання, складні умови експлуатації, фізична недоступність вузла, вплив температури, вологості або інших параметрів середовища.

Величини (E_k) та (T_k) описують зовнішню складову вразливості. Параметр (E_k) визначає інтенсивність (k)-го зовнішнього впливу, а (T_k) - значущість відповідної загрози для компонента БСМ. До таких впливів можуть належати електромагнітні завади, несанкціонований доступ, перевантаження трафіком, порушення зв'язності або інші фактори, що виникають поза межами самого компонента, але впливають на його стійкість.

Коефіцієнти α, β, γ задають вагу відповідно технічної, фізичної та зовнішньої складових у загальній оцінці вразливості. Їх використання дозволяє адаптувати модель до конкретних умов функціонування БСМ і врахувати, яка група факторів є найбільш критичною для певного сценарію аналізу.

Наведене співвідношення дозволяє поєднати різні за природою фактори в межах єдиної оцінки вразливості. Завдяки цьому стає можливим не лише встановити факт наявності окремої вразливості, а й визначити узагальнений рівень небезпечності стану компонента з урахуванням технічних, фізичних і зовнішніх чинників.

Інтегральна оцінка V_m може бути використана для ранжування компонентів мережі за рівнем їхньої вразливості. Компоненти з вищим значенням цієї оцінки потребують пріоритетного аналізу на наступному етапі, оскільки вони мають більшу схильність до переходу в небажаний або критичний стан. Водночас така оцінка не є остаточним ризиком, оскільки ризик додатково враховує критичність компонента, його роль у топології та можливі наслідки відмови.

У результаті, інтегральна оцінка вразливості забезпечує перехід від набору окремих фактів про слабкі місця до узагальненої характеристики рівня вразливості компонентів БСМ. Саме ця характеристика надалі використовується в блоці оцінки ризиків як одна з ключових вхідних величин для кількісно-якісного аналізу небезпеки в мережі.

3.3.3 Покрокове виконання методу аналізу вразливостей компонентів БСМ

Метод аналізу вразливостей компонентів БСМ реалізується в межах блоку виявлення вразливостей і забезпечує перехід від формалізованого опису поточного стану мережі до встановлення слабких місць, критичних режимів і потенційно небезпечних станів компонентів. Його призначення полягає в інтерпретації результатів логування станів з урахуванням контексту функціонування,

топологічної ролі компонентів, нечітко інтерпретованих параметрів і правил логічного висновку.

У загальному вигляді виконання методу передбачає такі етапи: отримання онтологічного запису поточного стану компонента; виділення контекстних, телеметричних і топологічних ознак; перевірку правил виявлення критичних станів; класифікацію типу вразливості; визначення факторів, що впливають на її формування; обчислення або формування інтегральної оцінки вразливості; передавання результатів до методу оцінки ризику.

Послідовність виконання методу аналізу вразливостей компонентів БСМ наведено на рис. 3.4.

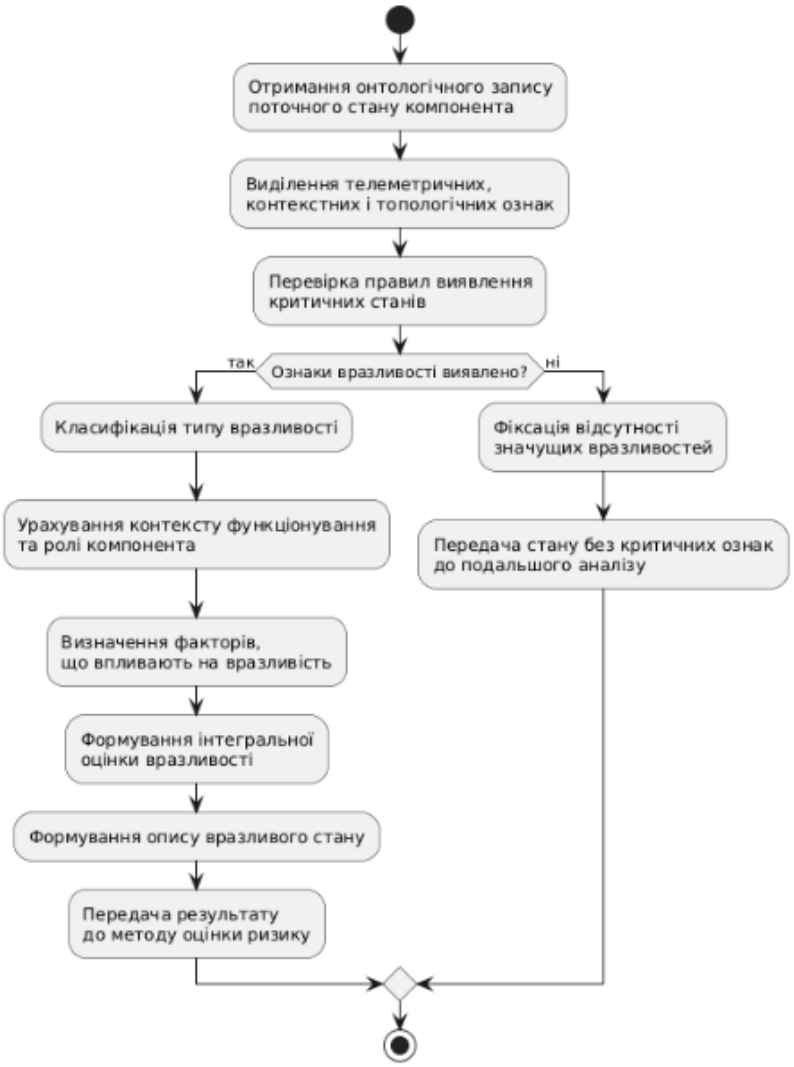

Рисунок 3.4 - Діаграма діяльності методу аналізу вразливостей компонентів БСМ

Як показано на рис. 3.4, метод виконується після формування онтологічного запису поточного стану компонента. На відміну від простого порівняння параметрів із пороговими значеннями, запропонований метод аналізує сукупність ознак, їх взаємозв’язок, контекст функціонування та роль компонента в мережі. Це дозволяє встановлювати не лише факт відхилення параметра, а й тип вразливості, умови її виникнення та ступінь критичності для подальшого ризикового аналізу.

Розглянемо проходження етапів методу аналізу вразливостей на прикладі спостережуваного промислового обладнання, стан якого контролюється за допомогою сенсорів температури, рівня, струму навантаження, тиску, витрати, напруги живлення та параметрів бездротового каналу передавання даних. У межах прикладного сценарію таке обладнання подається як екземпляр класу ObservedObject, його контрольовані характеристики - як екземпляри або типи класу ObservedParameter, а поточний стан мережі й обладнання надходить до методу у вигляді запису StateLogRecord.

На першому кроці метод отримує онтологічний запис поточного стану компонента. У межах онтологічної моделі цей запис подається як екземпляр класу StateLogRecord, який містить дані про спостережуваний об’єкт ObservedObject, контрольовані параметри ObservedParameter, телеметричний знімок TelemetrySnapshot, контекст вузлів NodeContext і стан каналів зв’язку ChannelState. На цьому етапі метод отримує формалізований вхідний опис, але ще не встановлює факт наявності вразливості.

На другому кроці виконується виділення телеметричних, контекстних і топологічних ознак. Для спостережуваного обладнання такими ознаками можуть бути низький рівень, підвищена температура, збільшений струм навантаження, відхилення тиску, зменшення витрати або нестабільність напруги. Для компонентів БСМ додатково враховуються затримка, втрати пакетів, зниження RSSI, нестабільність каналу або недоступність вузла. У межах онтологічної моделі ці ознаки виділяються з класів ObservedParameter, TelemetrySnapshot, NodeContext, ChannelState, а також із топологічних сутностей Node, Link, Route і Segment.

На третьому кроці перевіряються правила виявлення критичних станів. Такі правила пов’язують поєднання телеметричних, контекстних і топологічних ознак із можливими вразливостями. Наприклад, якщо фіксується зниження рівня, збільшення струму навантаження та зміна витрати, то може бути сформована ознака технологічної вразливості спостережуваного об’єкта. Якщо одночасно зростають втрати пакетів або затримка передавання даних, додатково може бути встановлена комунікаційна вразливість каналу або маршруту. У межах онтологічної моделі результати цього кроку пов’язуються з класами Vulnerability, ObservedObject, ObservedParameter, Link і Route.

На четвертому кроці, якщо ознаки вразливості виявлено, виконується класифікація типу вразливості. Залежно від джерела та характеру ознак вразливість може бути віднесена до технічної, технологічної, енергетичної, комунікаційної, топологічної, фізичної або комбінованої. У межах онтологічної моделі узагальнена сутність Vulnerability може уточнюватися через відповідні типи або підкласи, наприклад EnergyVulnerability, CommunicationVulnerability, TopologyVulnerability або PhysicalVulnerability. Якщо вразливість пов’язана з параметрами спостережуваного об’єкта, вона додатково зв’язується з класами ObservedObject і ObservedParameter.

На п’ятому кроці враховується контекст функціонування та роль компонента. Однакова ознака деградації може мати різне значення залежно від того, чи належить вона до периферійного сенсорного вузла, ретранслятора, шлюзу, критичного каналу або маршруту передавання важливої телеметрії. У межах онтологічної моделі це враховується через класи Node, SensorNode, RelayNode, Gateway, Link, Route, Segment, NodeContext і ChannelState. Саме цей крок дозволяє інтерпретувати вразливість не ізольовано, а у зв’язку з топологією та функціональною роллю компонента.

На шостому кроці визначаються фактори, що впливають на вразливість. До таких факторів належать технічні, комунікаційні, топологічні, фізичні, середовищні та зовнішні ознаки, які посилюють або уточнюють виявлений вразливий стан. Наприклад, низький рівень або підвищена температура можуть

бути технічними чи технологічними факторами, нестабільність каналу - комунікаційним фактором, а критична роль маршруту - топологічним фактором. У межах онтологічної моделі ці фактори можуть бути подані через ContextFactor, Threat, NodeContext, ChannelState, ObservedParameter, а також через зв’язки з класом Vulnerability.

На сьомому кроці формується інтегральна оцінка вразливості. Вона враховує тип вразливості, кількість і вираженість ознак, контекст функціонування, достовірність даних, стан вузлів і каналів, а також визначені фактори впливу. У межах онтологічної моделі така оцінка пов’язується з класом Vulnerability, а її вхідні складові - з класами ContextFactor, Threat, NodeContext, ChannelState та атрибутами класу StateLogRecord, зокрема confidence і anomalyFlag.

На восьмому кроці формується опис вразливого стану та результат передається до методу оцінки ризику. Опис містить тип вразливості, компонент або спостережуваний об’єкт, до якого вона належить, ознаки її виникнення, фактори впливу, контекстні характеристики, можливу загрозу та інтегральну оцінку. У межах онтологічної моделі цей результат подається через клас Vulnerability, пов’язаний із ObservedObject, Node, Link, Route, Threat і відповідними контекстними характеристиками. На цьому етапі ще не формується остаточний рівень ризику, оскільки ризик додатково враховує критичність, структурну роль і можливі наслідки відмови.

Якщо на етапі перевірки правил ознаки вразливості не виявлено, виконується альтернативна гілка методу. У такому випадку фіксується відсутність значущих вразливостей, а поточний стан передається до подальшого аналізу без критичних ознак. У межах онтологічної моделі такий результат не формує нового екземпляра критичної Vulnerability, але зберігає зв’язок із записом StateLogRecord, що дає змогу враховувати цей стан у наступних циклах логування та аналізу.

З погляду наукової новизни цей підпідрозділ відображає удосконалення методу аналізу вразливостей бездротових сенсорних мереж. Новизна полягає у використанні спеціалізованих правил поетапного виявлення критичних станів на основі формальних правил нечіткого логічного висновку, семантичних

онтологічних залежностей між компонентами мережі та контекстно залежних ознак їх функціонування. На відміну від підходів, що фіксують лише факт перевищення окремого параметра, запропонований метод дозволяє формувати зведений критерій оцінювання вразливості компонентів БСМ за структурними, контекстними, топологічними та середовищними ознаками.

Отже, метод аналізу вразливостей компонентів БСМ забезпечує перехід від семантично узгодженого опису поточного стану до формалізованого подання слабких місць і критичних режимів. Отримані результати створюють основу для подальшої оцінки ризику та визначення пріоритетів реагування.

3.4 Метод оцінки ризиків у системі ризик-орієнтованого управління

Після формування результатів аналізу вразливостей наступним етапом багаторівневої онтологічної моделі є оцінювання ризику, що виникає внаслідок можливого прояву виявлених слабких місць і критичних станів компонентів БСМ. У межах дисертаційної роботи цей етап подається як узагальнений метод оцінки ризику в бездротових сенсорних мережах, який отримав подальший розвиток і забезпечує перехід від опису вразливого стану до кількісно-якісного визначення рівня небезпеки для вузлів, каналів, маршрутів, сегментів, спостережуваних об’єктів і мережі в цілому.

Вхідною основою для цього методу є результати методу аналізу вразливостей, зокрема встановлені типи вразливостей, інтегральні оцінки вразливості, контекстні фактори, можливі загрози, ознаки достовірності даних і зв’язок вразливого стану з відповідними компонентами БСМ або спостережуваними об’єктами. На цьому рівні вразливість уже не розглядається як самостійний кінцевий результат аналізу, а використовується як одна з основних складових формування ризику.

На відміну від методу аналізу вразливостей, який встановлює наявність слабких місць і критичних режимів, узагальнений метод оцінки ризику визначає, наскільки небезпечними є ці стани для функціонування БСМ. Для цього

враховуються не лише інтегральна вразливість компонента, а й його критичність, структурна роль у топології, участь у маршрутизації, належність до критичного сегмента, наявність резервування, вагова значущість ризикового сценарію та можливі наслідки відмови.

У запропонованій моделі ризик розглядається як наступний рівень семантичного узагальнення після вразливості. Якщо вразливість характеризує схильність компонента до переходу в небажаний або критичний стан, то ризик відображає рівень небезпеки, який цей стан створює для мережі або спостережуваного об’єкта з урахуванням контексту функціонування, значущості компонента та потенційних наслідків. Тому однаковий рівень вразливості може формувати різний рівень ризику для периферійного сенсорного вузла, ретранслятора, шлюзу, каналу зв’язку або маршруту передавання критичної телеметрії.

З погляду наукової новизни цей підрозділ відображає подальший розвиток узагальненого методу оцінки ризику в БСМ. Його особливість полягає у поетапному семантичному інтегруванні результатів аналізу вразливостей, контексту поточного стану мережі, факторів середовища, зовнішніх впливів і структурної ролі компонентів у межах єдиного формального ризикового подання. Завдяки цьому ризик визначається не лише за окремими технічними показниками, а як зведена характеристика небезпеки, що враховує вразливісні, контекстні, середовищні та структурно-пріоритетні ознаки.

Таким чином, узагальнений метод оцінки ризику є наступним аналітичним рівнем багаторівневої онтологічної моделі після методу аналізу вразливостей. Він забезпечує перехід від формалізованих фактів про слабкі місця та критичні стани до інтегральної оцінки ризику, карти ризиків і визначення пріоритетів подальшого реагування. Далі розглядаються онтологічна модель джерел формування ризику, основні сутності цієї моделі, формалізація ризику на основі інтеграції факторів, агрегування локальних оцінок ризику та покрокове виконання узагальненого методу оцінки ризику в БСМ.

3.4.1 Модель методу оцінки ризику у структурі БСМ

Після формування узагальнених оцінок вразливості компонентів мережі наступним етапом є визначення факторів, які беруть участь у формуванні ризику. На відміну від вразливості, що характеризує схильність компонента до переходу в небажаний або критичний стан, ризик є більш комплексною категорією. Він враховує не лише наявність слабкого місця, а й імовірність реалізації небажаної події, масштаб можливих наслідків, значущість ураженого компонента та умови функціонування мережі.

Основними джерелами формування ризику в БСМ є компоненти мережі, пов’язані з ними вразливості, потенційні загрози та фактори, що визначають масштаб і критичність наслідків. Компоненти мережі виступають об’єктами оцінювання, вразливості характеризують їхні слабкі місця, загрози відображають можливі небажані впливи, а фактори ризику уточнюють умови, за яких вразливий стан може призвести до порушення функціонування вузла, каналу, маршруту, сегмента або мережі в цілому.

Оцінка ризику не може ґрунтуватися лише на факті наявності вразливості або загрози. Для коректного визначення рівня небезпеки необхідно враховувати контекст функціонування мережі та структурні особливості її побудови. Саме ці чинники визначають, чи буде певна вразливість локальною проблемою окремого компонента, чи вона може призвести до порушення роботи важливого маршруту, критичного сегмента або всієї БСМ.

До контекстних чинників оцінювання ризику належать параметри, що відображають поточний функціональний стан компонентів мережі та умови їх експлуатації. Насамперед це енергетичні характеристики, часові параметри, рівень навантаження, якість каналу зв’язку та умови зовнішнього середовища. Енергетичний контекст визначає здатність компонента підтримувати працездатність у поточному режимі, часові характеристики дозволяють врахувати затримки й старіння інформації, навантажувальні параметри відображають ступінь використання ресурсів, а якість каналу та середовищні умови уточнюють вплив

завад, втрат пакетів і нестабільності зв’язку.

Разом із контекстними характеристиками важливу роль відіграють структурні чинники, які описують місце компонента в загальній організації мережі. До них належать топологічна значущість вузла або каналу, належність до критичного сегмента, участь у маршрутизації, наявність резервних шляхів, ступінь централізації функцій і потенціал поширення наслідків відмови. Наприклад, одна й та сама комунікаційна вразливість має різну вагу для периферійного сенсорного вузла і для шлюзу, через який проходять потоки даних від великої кількості компонентів.

Контекстні та структурні чинники повинні розглядатися у взаємозв’язку. Низький рівень енергії вузла не завжди означає високий ризик, якщо цей вузол не виконує критичних функцій і не бере участі в ключових маршрутах. Водночас такий самий енергетичний стан може бути суттєво небезпечнішим для вузла, який виконує функцію ретрансляції, агрегації даних або забезпечує зв’язність критичного сегмента мережі.

У межах онтологічної моделі джерела формування ризику та чинники його оцінювання подаються через класи WSNComponent, Vulnerability, Threat, RiskFactor та Risk. Компонент мережі пов’язується з відповідною вразливістю, вразливість - із потенційною загрозою, а сукупність факторів ризику визначає умови, що впливають на рівень небезпеки. Клас RiskFactor може бути деталізований через підкласи TechnicalFactor, PhysicalFactor, ExternalFactor та StructuralFactor, які відображають відповідно технічні, фізичні, зовнішні та структурні складові ризику. Клас Risk може уточнюватися через NodeRisk, LinkRisk та NetworkRisk залежно від рівня аналізу.

Узагальнену онтологічну схему основних джерел формування ризику в бездротовій сенсорній мережі наведено на рис. 3.5.

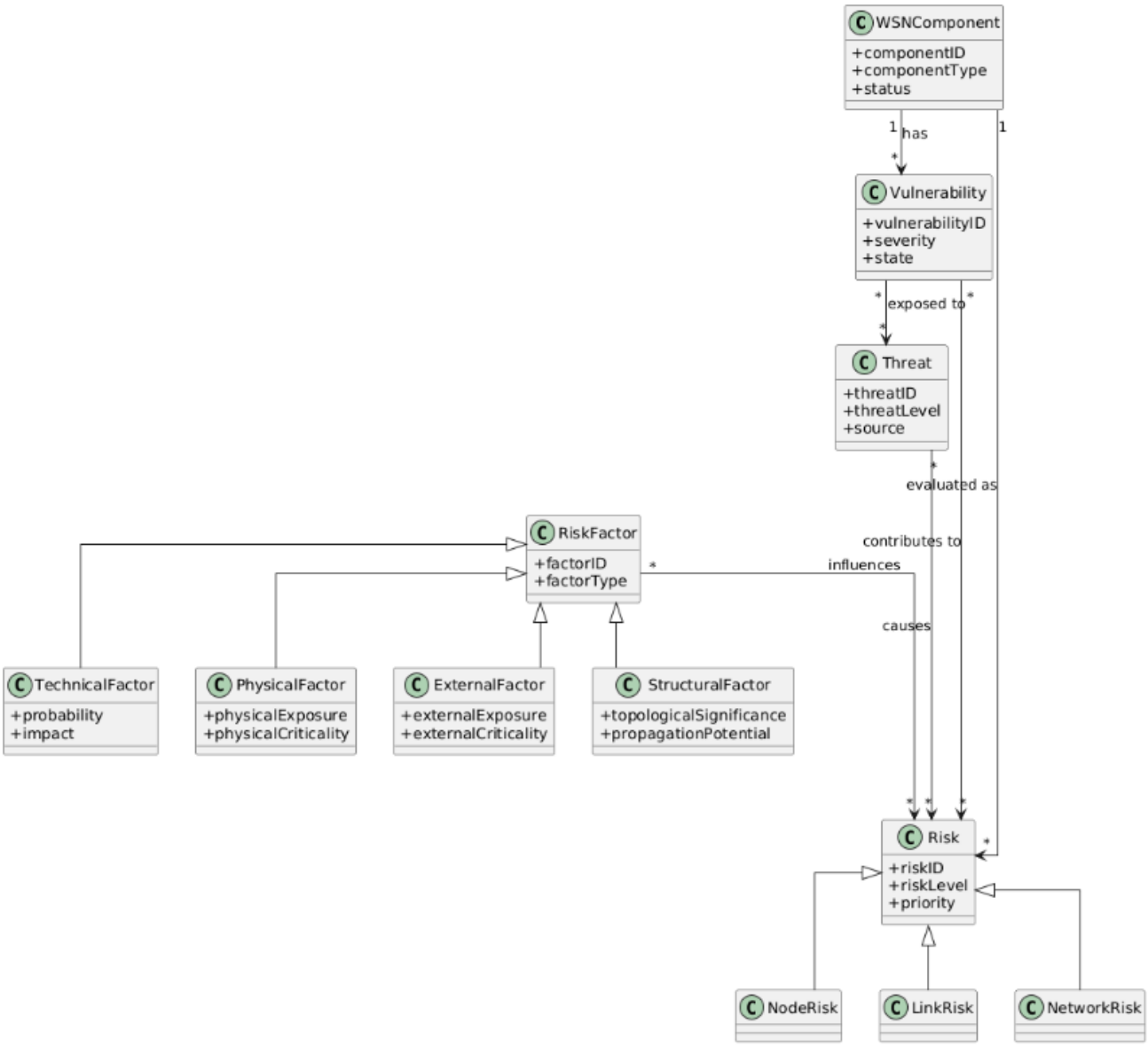

Рисунок 3.5 – Онтологічна модель основних джерел формування ризику в бездротовій сенсорній мережі

Наведена схема відображає зв’язок між компонентами БСМ, їх вразливостями, загрозами, факторами ризику та відповідними типами ризику. Вона показує, що ризик формується не як прямий наслідок окремої вразливості, а як результат взаємодії вразливого компонента, потенційної загрози та сукупності факторів, які визначають масштаб і критичність можливих наслідків.

Основні сутності онтологічної схеми джерел формування ризику в БСМ, їх призначення, атрибути та зв’язки наведено в табл. 3.4:

Таблиця 3.4 Основні сутності онтологічної схеми джерел формування ризику в БСМ.

Сутність (клас)	Призначення	Основні атрибути	Основні зв'язки
WSNComponent	Узагальнене подання компонента бездротової сенсорної мережі	componentID, componentType, status	Пов'язаний із Vulnerability через has; пов'язаний із Risk через evaluated as
Vulnerability	Узагальнене подання вразливості компонента мережі	vulnerabilityID, severity, state	Пов'язана з WSNComponent; пов'язана із Threat через exposed to; бере участь у формуванні Risk через contributes to
Threat	Узагальнене подання загрози, що реалізує вразливість	threatID, threatLevel, source	Пов'язана з Vulnerability; впливає на Risk через causes
RiskFactor	Узагальнене подання фактора, що впливає на рівень ризику	factorID, factorType	Є базовим класом для TechnicalFactor, PhysicalFactor, ExternalFactor, StructuralFactor; впливає на Risk через influences
TechnicalFactor	Подання технічних факторів ризику	probability, impact	Є підкласом RiskFactor; відображає технічну складову ризику
PhysicalFactor	Подання фізичних факторів ризику	physicalExposure, physicalCriticality	Є підкласом RiskFactor; характеризує фізичні умови та їх значущість
ExternalFactor	Подання зовнішніх факторів ризику	externalExposure, externalCriticality	Є підкласом RiskFactor; відображає зовнішні загрози та силу їх впливу
StructuralFactor	Подання структурних факторів ризику	topologicalSignificance, propagationPotential	Є підкласом RiskFactor; характеризує роль компонента в топології та потенціал поширення наслідків
Risk	Узагальнене подання ризику як інтегральної характеристики небезпеки	riskID, riskLevel, priority	Формується під впливом Vulnerability, Threat та RiskFactor; пов'язаний із WSNComponent
NodeRisk	Ризик окремого вузла	успадковує атрибути Risk	Є підкласом Risk

LinkRisk	Ризик каналу зв’язку	успадковує атрибути Risk	Є підкласом Risk
NetworkRisk	Ризик мережі в цілому	успадковує атрибути Risk	Є підкласом Risk

Виділення наведених сутностей дозволяє формалізувати процес переходу від виявленої вразливості до оцінки ризику. Компоненти мережі виступають об’єктами аналізу, вразливості та загрози визначають передумови небезпечних станів, а фактори ризику уточнюють технічні, фізичні, зовнішні та структурні умови, що впливають на рівень небезпеки.

З огляду на це, ризик у БСМ доцільно розглядати як системну характеристику небезпеки, що формується на основі поєднання стану компонента, його топологічної ролі, контексту функціонування, загроз і потенційних наслідків. Такий підхід створює основу для подальшої формалізації ризику на основі інтеграції відповідних факторів.

3.4.2 Формалізація ризику на основі інтеграції факторів

Після визначення джерел формування ризику та чинників його оцінювання необхідно перейти до формального подання ризику, придатного для кількісно-якісного аналізу в межах багаторівневої онтологічної моделі. У запропонованому підході ризик розглядається як наступний рівень узагальнення після вразливості, тобто як характеристика, що формується на основі інтегральної оцінки вразливості компонента з урахуванням його критичності та значущості для функціонування БСМ.

На відміну від вразливості, яка відображає схильність компонента до переходу в небажаний або критичний стан, ризик додатково враховує місце цього компонента в топології мережі, його функціональну роль, можливі наслідки відмови та пріоритетність відповідного сценарію. Тому компонент із високою вразливістю не завжди створює найбільший ризик, якщо його роль у мережі є другорядною. Водночас навіть помірна вразливість шлюзу, ретранслятора або

вузла, що забезпечує зв'язність критичного сегмента, може формувати високий рівень ризику.

У найзагальнішому вигляді таку залежність можна подати як:

$$R_m = f(V_m, C_m, W_m) = V_m \times C_m \times W_m \qquad (3.4)$$

де: R_m - інтегральна оцінка для компонента мережі, V_m - інтегральна вразливість компонента, C_m - критичність компонента для функціонування мережі, W_m - ваговий коефіцієнт значущості компонента або відповідного ризикового сценарію.

Величина (V_m) переносить у Метод оцінки ризиків результати попереднього аналізу вразливостей. Вона враховує технічні, фізичні та зовнішні фактори, які вже були інтегровані під час визначення рівня вразливості компонента. Завдяки цьому у формулі ризику не відбувається повторного врахування тих самих факторів, а зберігається логічна наступність між Методом виявлення вразливостей і Методом оцінки ризиків.

Особливого значення набуває величина C_m, яка характеризує критичність компонента мережі. На відміну від V_m, що відображає поточний стан і схильність компонента до деградації, C_m описує його структурну та функціональну важливість для БСМ. Джерелом для формування цієї величини є характеристики, отримані в блоці опису мережі: роль компонента в топології, участь у маршрутизації, належність до критичного сегмента, кількість залежних елементів і рівень резервування.

У формалізованому вигляді критичність компонента може бути подана як:

$$C_m = \omega_1 R_m^{role} + \omega_2 R_m^{route} + \omega_3 R_m^{seg} + \omega_4 R_m^{dep} + \omega_5 (1 - \overline{\mathrm{Re}\, s_m}) \qquad (3.5)$$

де: R_m^{role} - оцінка значущості ролі компонента в мережі, R_m^{route} - ступінь його участі в маршрутизації, R_m^{seg} - критичність компонента для функціонування мережі, R_m^{dep} - кількість або значущість елементів, що залежать від його функціонування, $\overline{\mathrm{Re}\, s_m}$ - нормована характеристика резервування, $\omega_1, \omega_2, \omega_3, \omega_4, \omega_5$ - вагові коефіцієнти відповідних складових.

Таке подання дозволяє врахувати, що однаковий рівень вразливості може мати різний ризиковий зміст залежно від місця компонента в загальній структурі мережі. Наприклад, помірна вразливість периферійного сенсорного вузла та аналогічна вразливість шлюзу не є рівнозначними, оскільки відмова шлюзу може вплинути на значно більший фрагмент БСМ.

Другою допоміжною величиною у формулі ризику є ваговий коефіцієнт значущості (W_m). Його призначення полягає в узгодженні оцінки ризику з особливостями прикладного середовища, типом компонента, важливістю сервісу або політиками керування. Якщо (C_m) відображає структурну критичність компонента, то (W_m) задає відносну вагу відповідного компонента або ризикового сценарію в межах обраної моделі оцінювання.

Узагальнено величину W_m можна подати як

$$W_m = \eta_1 W_m^{role} + \eta_2 W_m^{policy} + \eta_3 W_m^{service} \qquad (3.6)$$

де: W_m^{role} - вагова оцінка за типом компонента мережі, W_m^{policy} - вагова оцінка, що задається політикою керування або правилами пріоритизації, $W_m^{service}$ - вагова оцінка, пов’язана з важливістю функції або сервісу, який підтримує відповідний компонент, η_1, η_2, η_3 - коефіцієнти значущості відповідних складових.

Використання коефіцієнта (W_m) робить модель ризику гнучкішою та придатною до адаптації в різних прикладних сценаріях. Наприклад, у промислових системах моніторингу компоненти, пов’язані з критичною телеметрією або передаванням аварійних повідомлень, можуть мати більші значення (W_m), ніж допоміжні або резервні елементи мережі.

У межах багаторівневої онтологічної моделі ризик розглядається не лише як числовий результат, а і як семантично інтерпретована характеристика небезпеки. Тому поряд із числовим значенням (R_m) можуть використовуватися лінгвістичні категорії, наприклад низький, помірний, високий або критичний ризик. Це забезпечує зв’язок із нечіткими моделями другого розділу та дозволяє використовувати отримані результати в блоці адаптивного керування.

Важливо також, що оцінка ризику має динамічний характер. Оскільки параметри вузлів, каналів, контексту й зовнішніх умов у БСМ змінюються з часом, значення (R_m) повинно періодично оновлюватися. У такому разі ризик розглядається не як одноразова характеристика, а як динамічний індикатор небезпеки, що змінюється відповідно до поточного стану мережі.

Отримана формалізація забезпечує логічно узгоджений перехід від інтегральної оцінки вразливості до оцінки ризику компонента БСМ. Вона дозволяє врахувати поточний стан компонента, його критичність у структурі мережі та прикладну значущість відповідного ризикового сценарію, створюючи основу для подальшої побудови узагальненої інтегральної оцінки ризику.

Після формалізації ризику окремого компонента виникає необхідність переходу від локальних оцінок до узагальненої характеристики небезпеки для групи компонентів, маршруту, сегмента або всієї БСМ. Такий перехід є важливим, оскільки реальний стан мережі визначається не лише ризиком окремого вузла чи каналу, а й сукупним впливом багатьох взаємопов’язаних елементів.

Локальні оцінки (R_m), отримані для окремих компонентів, дозволяють визначити найбільш небезпечні вузли, канали або маршрути. Однак для підтримки ризик-орієнтованого управління необхідно мати також інтегральну оцінку, яка відображає рівень небезпеки для більшого фрагмента мережі. З цієї причини ризикові оцінки окремих компонентів повинні бути узагальнені у вигляді інтегральної характеристики вищого рівня.

У найзагальнішому вигляді інтегральний ризик для множини компонентів мережі може бути поданий як:

$$R_{\Sigma} = \sum_{m=1}^{N} \rho_m R_m \qquad (3.7)$$

де: R_{Σ} - узагальнена інтегральна оцінка ризику для сукупності компонентів мережі, R_m - ризик m-го компонента, визначений за співвідношенням (3.5), ρ_m - коефіцієнт внеску m-го компонента в загальну ризикову оцінку, N - кількість компонентів, що враховуються в оцінюванні.

Наведене співвідношення дозволяє перейти від локальних оцінок ризику до інтегральної характеристики, яка враховує внесок кожного елемента мережі в загальний рівень небезпеки. Коефіцієнт ρ_m вводиться для узгодження агрегування ризиків із топологічною, функціональною або прикладною значущістю відповідних компонентів. Тому під час формування загального ризику більшу вагу можуть мати шлюзи, базові станції, вузли критичних сегментів або компоненти, від яких залежить передавання даних у значній частині мережі.

У найпростішому випадку коефіцієнти ρ_m можуть бути нормованими, тобто такими, що задовольняють умову:

$$\sum_{m=1}^{N} \rho_m = 1 \qquad (3.8)$$

Таке нормування дозволяє інтерпретувати інтегральний ризик як зважену середню оцінку небезпеки для множини компонентів мережі. Це забезпечує коректне порівняння різних сегментів, маршрутів або конфігурацій БСМ, навіть якщо вони містять різну кількість елементів.

Залежно від рівня аналізу співвідношення (3.7) може застосовуватися до різних груп компонентів. Для оцінювання ризику сегмента враховуються вузли й канали, що входять до відповідного топологічного або функціонального фрагмента мережі. Для аналізу маршруту доцільно агрегувати ризики послідовності вузлів і каналів, через які проходить передавання даних. На рівні всієї БСМ узагальнена інтегральна оцінка ризику відображає системний рівень небезпеки та може використовуватися як один з основних індикаторів для адаптивного керування.

Важливо, що узагальнення ризику не зводиться до простого арифметичного підсумовування локальних оцінок. У БСМ ризики окремих компонентів можуть бути взаємозалежними, а реалізація небезпечної події в одному вузлі або каналі може спричинити вторинне зростання ризику в суміжних елементах. Тому під час визначення коефіцієнтів ρ_m доцільно враховувати потенціал каскадного впливу, роль компонента в маршрутизації та його значення для підтримання зв’язності мережі.

У межах онтологічної моделі узагальнена інтегральна оцінка ризику розглядається не лише як числова величина, а як семантично інтерпретована характеристика стану мережі. Поряд із числовими значеннями R_m та R_Σ можуть використовуватися лінгвістичні оцінки, наприклад низький, помірний, високий або критичний рівень ризику. Це дозволяє безпосередньо використовувати інтегральний ризик для пріоритизації контрзаходів і вибору політик реагування.

Інтегральна оцінка ризику має динамічний характер. Оскільки локальні ризики компонентів змінюються відповідно до нового стану вузлів, каналів, вразливостей, загроз і контекстних чинників, значення R_Σ також повинно періодично оновлюватися. Завдяки цьому вона може використовуватися як динамічний індикатор небезпеки, що відображає поточний рівень ризику для сегмента, маршруту або мережі загалом.

Проведене узагальнення забезпечує перехід від локального оцінювання окремих компонентів до системного подання небезпеки для БСМ. Узагальнена інтегральна оцінка ризику створює основу для ранжування компонентів і сегментів мережі, пріоритизації керуючих впливів та подальшого формування рекомендацій у блоці адаптивного керування.

3.4.3 Покрокове виконання узагальненого методу оцінки ризику в БСМ

Узагальнений метод оцінки ризику в БСМ реалізується в межах блоку оцінки ризиків і забезпечує перехід від виявлених вразливостей до кількісно-якісного визначення рівня небезпеки для окремих компонентів, маршрутів, сегментів або мережі в цілому. На відміну від методу аналізу вразливостей, який встановлює слабкі місця та критичні стани компонентів, метод оцінки ризику визначає, наскільки небезпечними є ці стани з урахуванням контексту функціонування, структурної ролі компонента, можливих наслідків відмови та вагової значущості відповідного сценарію.

У загальному вигляді виконання методу передбачає такі етапи: отримання результатів аналізу вразливостей; визначення компонента або сегмента, для якого

оцінюється ризик; урахування інтегральної вразливості; визначення критичності компонента; урахування вагової значущості сценарію; розрахунок інтегральної оцінки ризику; інтерпретацію отриманого значення; формування карти ризиків; передавання результатів до методу адаптивного керування.

Послідовність виконання узагальненого методу оцінки ризику в БСМ наведено на рис. 3.6.

Рисунок 3.6 - Діаграма діяльності узагальненого методу оцінки ризику в БСМ

Як показано на рис. 3.X, метод оцінки ризику використовує результати попереднього аналізу вразливостей, але не обмежується ними. Інтегральна вразливість компонента розглядається як одна з вхідних складових ризику, тоді як

остаточний рівень небезпеки формується з урахуванням критичності компонента, його функціональної ролі, топологічного положення, наявності резервування та можливих наслідків відмови.

Розглянемо проходження етапів узагальненого методу оцінки ризику на прикладі спостережуваного промислового обладнання, стан якого контролюється за допомогою БСМ. На попередньому етапі для цього обладнання або пов'язаних із ним компонентів мережі вже було сформовано опис вразливого стану. У межах онтологічної моделі такий опис подається через клас Vulnerability, пов'язаний із класами ObservedObject, ObservedParameter, Node, Link, Route, Threat і відповідними контекстними характеристиками.

На першому кроці метод отримує результати аналізу вразливостей. До таких результатів належать тип вразливості, компонент або об'єкт, з яким вона пов'язана, ознаки її виникнення, контекстні фактори, можлива загроза та інтегральна оцінка вразливості. У межах онтологічної моделі ці дані подаються через класи Vulnerability, Threat, ObservedObject, ObservedParameter, NodeContext і ChannelState. На цьому етапі метод ще не визначає ризик, а приймає формалізований результат попереднього аналізу.

На другому кроці визначається об'єкт оцінювання ризику. Ним може бути окремий вузол, канал зв'язку, маршрут, сегмент мережі або спостережуваний об'єкт, стан якого контролюється за допомогою БСМ. У межах онтологічної моделі такий об'єкт подається через класи Node, Link, Route, Segment або ObservedObject. Це дозволяє оцінювати ризик як для окремих компонентів сенсорної мережі, так і для об'єктів, стан яких залежить від достовірності та своєчасності отримання телеметрії.

На третьому кроці враховується інтегральна оцінка вразливості. Вона характеризує ступінь вираженості слабкого або критичного стану, сформованого на попередньому етапі. У межах онтологічної моделі така оцінка є атрибутом або результатом класу Vulnerability і може бути пов'язана з відповідними факторами через ContextFactor, Threat, NodeContext та ChannelState. Важливо, що на цьому

кроці вразливість ще не ототожнюється з ризиком, а використовується як одна з його складових.

На четвертому кроці визначається критичність компонента або об’єкта оцінювання. Для вузла БСМ критичність залежить від його ролі в мережі, участі в маршрутизації, належності до критичного сегмента та наявності резервування. Для спостережуваного об’єкта критичність визначається його значенням для технологічного процесу або контрольованого середовища. У межах онтологічної моделі цей етап пов’язаний із класами Node, SensorNode, RelayNode, Gateway, Link, Route, Segment і ObservedObject.

На п’ятому кроці визначається вагова значущість ризикового сценарію. Вона відображає прикладну важливість конкретної ситуації: втрати критичної телеметрії, затримки передавання аварійних повідомлень, деградації основного маршруту або погіршення стану важливого спостережуваного об’єкта. У межах онтологічної моделі цей етап може бути поданий через класи RiskFactor, Threat, Route, Segment, ObservedObject і відповідні атрибути пріоритетності або значущості.

На шостому кроці виконується розрахунок інтегральної оцінки ризику. Для цього поєднуються інтегральна вразливість, критичність компонента або об’єкта та вагова значущість ризикового сценарію. У межах онтологічної моделі результат цього кроку подається через клас Risk, який може уточнюватися залежно від рівня аналізу як NodeRisk, LinkRisk, RouteRisk, SegmentRisk або NetworkRisk. Отримане значення відображає рівень небезпеки, а не лише факт наявності вразливості.

На сьомому кроці визначається потреба в узагальненні ризику. Якщо оцінювання виконується для одного компонента, отримане значення може передаватися безпосередньо до інтерпретації. Якщо ж необхідно оцінити ризик маршруту, сегмента або мережі загалом, виконується агрегування локальних оцінок. У межах онтологічної моделі цей етап пов’язаний із класами Risk, Route, Segment, WSN, Node і Link.

Якщо узагальнення потрібне, виконується агрегування ризиків для маршруту, сегмента або мережі. На цьому етапі локальні оцінки ризику окремих

вузлів і каналів поєднуються з урахуванням їхньої ролі, внеску в передавання даних, топологічної значущості та можливого каскадного впливу. У межах онтологічної моделі агрегований результат може бути поданий через класи RouteRisk, SegmentRisk або NetworkRisk, пов’язані з відповідними екземплярами Route, Segment або WSN.

На восьмому кроці виконується інтерпретація рівня ризику. Отримане числове значення переводиться у якісну або лінгвістичну форму, наприклад «низький», «помірний», «високий» або «критичний» ризик. У межах онтологічної моделі така інтерпретація подається як атрибут класу Risk або відповідного його уточнення. Це дозволяє використовувати результат не лише для числового порівняння, а й для подальшого вибору рекомендацій щодо реагування.

На дев’ятому кроці формується карта ризиків. Вона відображає компоненти, маршрути, сегменти або об’єкти спостереження з відповідними рівнями ризику та дозволяє визначити пріоритети подальшого реагування. У межах онтологічної моделі карта ризиків може бути представлена як сукупність екземплярів класу Risk, пов’язаних із Node, Link, Route, Segment, WSN або ObservedObject. Така карта є узагальненим результатом роботи методу оцінки ризику.

На десятому кроці результати передаються до методу адаптивного керування. Передаються інтегральні оцінки ризику, їх лінгвістична інтерпретація, карта ризиків, об’єкти або компоненти з найвищим рівнем небезпеки, а також фактори, що вплинули на формування ризику. У межах онтологічної моделі ці результати подаються через класи Risk, RiskFactor, Threat, Node, Link, Route, Segment і ObservedObject та використовуються як основа для формування рекомендацій щодо реагування.

Результатом виконання методу є інтегральна оцінка ризику та карта ризиків, а не безпосередній вибір контрзаходу.

З погляду наукової новизни цей підпідрозділ відображає подальший розвиток узагальненого методу оцінки ризику в бездротових сенсорних мережах. Новизна полягає у поетапному семантичному інтегруванні результатів аналізу вразливостей, контексту поточного стану мережі, факторів середовища, зовнішніх

впливів і структурної ролі компонентів у межах єдиного формального ризикового подання. На відміну від підходів, у яких ризик визначається переважно через окремі технічні показники або загальні сценарії загроз, запропонований метод дозволяє формувати зведений критерій оцінювання ризику компонентів і сегментів БСМ за вразливісними, контекстними, середовищними та структурно-пріоритетними ознаками.

Отже, узагальнений метод оцінки ризику забезпечує перехід від опису вразливих станів компонентів БСМ до визначення рівня небезпеки для мережі або спостережуваного обладнання. Отримані результати створюють основу для формування рекомендацій щодо реагування в межах методу адаптивного керування.

3.5 Метод адаптивного керування у структурі багаторівневої онтологічної моделі

Після формування інтегральних оцінок ризику та карти ризиків наступним етапом роботи багаторівневої онтологічної моделі є формування рекомендацій щодо реагування на виявлені позаштатні або потенційно небезпечні ситуації в БСМ. Цю функцію виконує метод адаптивного керування, який забезпечує перехід від результатів логування станів, аналізу вразливостей і оцінювання ризику до вибору можливих керуючих рішень.

На відміну від попередніх методів, що пов’язані з науковою новизною дисертаційної роботи, метод адаптивного керування у цьому дослідженні не заявляється як самостійний результат наукової новизни. Його роль полягає у практичному використанні результатів, отриманих на попередніх рівнях багаторівневої онтологічної моделі, та у формуванні рекомендаційного механізму підтримки прийняття рішень. Таким чином, цей метод розглядається як завершальний прикладний рівень моделі, що забезпечує її функціональну цілісність.

Метод адаптивного керування не передбачає безпосереднього автоматичного виконання фізичних або мережевих дій. Його призначення полягає у формуванні

обґрунтованих рекомендацій щодо можливих контрзаходів, які можуть бути подані оператору або передані зовнішній системі керування для подальшого прийняття рішення. Завдяки цьому метод виступає не як виконавчий механізм, а як інтелектуальний засіб підтримки ризик-орієнтованого реагування.

Вхідною основою методу є інтегральна оцінка ризику, карта ризиків, тип проблемної ситуації, контекст функціонування компонента або спостережуваного об’єкта, а також множина технологічних, ресурсних, топологічних і політичних обмежень. Саме ці дані дозволяють визначити, які контрзаходи є допустимими в поточному стані системи, які з них мають вищий пріоритет і яке рекомендоване рішення може бути сформоване для оператора або зовнішньої системи керування.

У межах запропонованої онтологічної моделі рекомендації формуються з урахуванням характеру виявленої проблеми. Наприклад, для енергетично виснаженого вузла доцільною може бути рекомендація щодо зниження навантаження або переходу до енергоощадного режиму; для нестабільного каналу - зміна маршруту або використання резервного з’єднання; для високого ризику порушення технологічного параметра - посилення моніторингу або передавання повідомлення оператору. Отже, вибір рекомендації залежить не лише від рівня ризику, а й від природи проблемної ситуації, ролі компонента та допустимості конкретного контрзаходу.

Таким чином, метод адаптивного керування завершує логічний цикл функціонування багаторівневої онтологічної моделі: від семантичного визначення та логування станів - до аналізу вразливостей, оцінювання ризику та формування рекомендацій щодо реагування. Далі розглядаються онтологічна модель методу адаптивного керування, основні сутності рекомендаційного рівня, формалізація процесу вибору керуючих рішень, а також покрокове виконання методу з урахуванням обмежень і зворотного зв’язку.

3.5.1 Модель методу адаптивного керування у структурі БСМ

Метод адаптивного керування є завершальним функціональним елементом багаторівневої онтологічної моделі БСМ. Його призначення полягає у формуванні рекомендацій щодо реагування на виявлені вразливості та оцінені ризики з урахуванням поточного стану мережі, доступних ресурсів, типу загрози та обмежень застосування контрзаходів. На відміну від попередніх Методів, які зосереджені на описі стану мережі, виявленні вразливостей і оцінюванні ризиків, Метод адаптивного керування орієнтований на підтримку прийняття рішень у відповідь на небезпечні або потенційно небезпечні ситуації.

У межах запропонованого підходу адаптивне керування не розглядається як механізм автоматичного виконання фізичних або мережевих дій. Його основна функція полягає у формуванні обґрунтованих рекомендацій, які можуть бути подані оператору або передані зовнішній системі керування для подальшої реалізації. Завдяки цьому Метод адаптивного керування виступає як інструмент інтелектуальної підтримки рішень, що поєднує результати ризик-орієнтованого аналізу з можливими сценаріями реагування.

Рекомендації, що формуються в межах цього Методу, можуть мати різний характер залежно від типу компонента, виду вразливості, рівня ризику та умов функціонування мережі. До основних типів рекомендацій належать зміна маршруту передавання даних, обмеження участі перевантаженого або вразливого вузла в маршрутизації, перерозподіл навантаження, перехід компонента до енергоощадного режиму, посилення моніторингу, використання резервного маршруту, підвищення пріоритету критичних повідомлень, а також рекомендації щодо перевірки або обслуговування окремих компонентів.

Особливе значення має те, що один і той самий рівень ризику може вимагати різних рекомендацій залежно від контексту. Наприклад, для вузла з низьким енергетичним ресурсом доцільною може бути рекомендація щодо зниження навантаження або переходу в енергоощадний режим, тоді як для каналу з високим рівнем втрат пакетів більш доречною буде зміна маршруту або використання

резервного каналу. Таким чином, Метод адаптивного керування повинен враховувати не лише величину ризику, а й природу проблеми, роль компонента в мережі та можливі наслідки запропонованого впливу.

У межах онтологічної моделі Метод адаптивного керування може бути поданий через класи Recommendation, Countermeasure, ResponsePolicy, Constraint, PriorityLevel та Feedback. Клас Recommendation описує сформовану рекомендацію, Countermeasure - можливий контрзахід, ResponsePolicy - політику або правило вибору дії, Constraint - обмеження щодо застосування контрзаходу, PriorityLevel - пріоритет реагування, а Feedback - інформацію про результат реалізації рекомендованого рішення. Таке подання дозволяє формально пов’язати оцінений ризик із набором можливих варіантів реагування.

Узагальнену онтологічну схему Методу адаптивного керування в багаторівневій онтологічній моделі БСМ наведено на рис. 3.7.

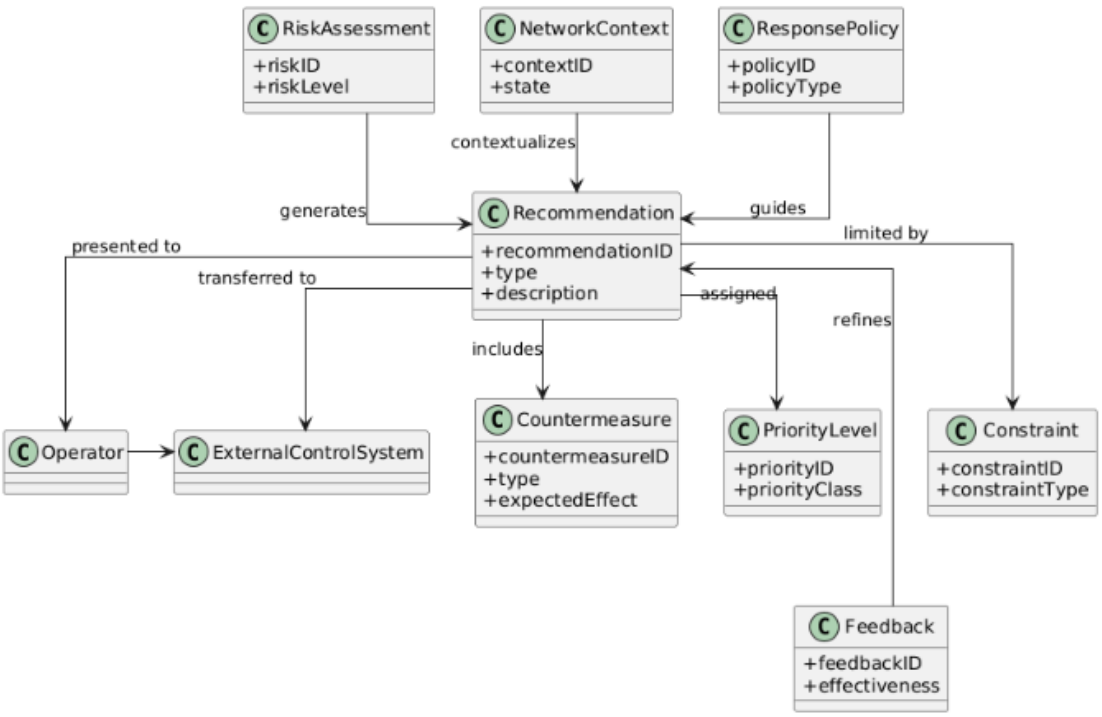

Рисунок 3.7 – Онтологічна модель методу адаптивного керування в багаторівневій онтологічній моделі БСМ

Наведена схема відображає зв’язки між ризиками, рекомендаціями, контрзаходами, політиками реагування, пріоритетами та механізмом зворотного зв’язку. Вона показує, що формування рекомендації є результатом інтерпретації

ризику з урахуванням типу компонента, характеру виявленої проблеми та можливих обмежень на застосування конкретного контрзаходу.

Для уточнення складу та функціонального призначення основних сутностей, наведених на рис. 3.4, у табл. 3.5 подано їх стислу характеристику в межах Методу адаптивного керування.

Таблиця 3.5 Основні сутності онтологічної схеми Метод адаптивного керування.

Сутність	**Призначення в межах Методу адаптивного керування**	**Основні атрибути / зміст**
RiskAssessment	Містить результати оцінювання ризику, які є підставою для формування рекомендацій щодо реагування	riskID, riskLevel
NetworkContext	Описує поточний контекст функціонування мережі, в якому формується рішення	contextID, state
ResponsePolicy	Визначає правила та принципи, відповідно до яких формується рекомендація	policyID, policyType
Recommendation	Центральна сутність Методу; відображає сформовану рекомендацію щодо реагування на виявлену ризикову ситуацію	recommendationID, type, description
Countermeasure	Описує рекомендований контрзахід або набір дій, що можуть бути застосовані для зниження ризику	countermeasureID, type, expectedEffect
PriorityLevel	Визначає пріоритетність реалізації сформованої рекомендації	priorityID, priorityClass
Constraint	Відображає обмеження, які потрібно враховувати під час формування або реалізації рекомендації	constraintID, constraintType
Operator	Представляє особу, яка отримує сформовану рекомендацію та може ухвалити рішення щодо її подальшого використання	службова сутність
ExternalControlSystem	Представляє зовнішню систему керування, якій може бути передано рекомендацію для подальшого використання або реалізації	службова сутність
Feedback	Накопичує інформацію про результати застосування рекомендацій і використовується для уточнення подальших рішень	feedbackID, effectiveness

Виділення наведених сутностей дозволяє формалізувати процес переходу від оціненого ризику до рекомендованої дії. При цьому рекомендація розглядається не як жорстко визначена команда, а як результат логічного вибору одного або кількох

доцільних контрзаходів, що відповідають поточному стану мережі та політиці реагування.

З урахуванням наведеного, Метод адаптивного керування забезпечує зв'язок між аналітичними результатами оцінювання ризиків і практичними рекомендаціями щодо реагування. Саме він створює основу для подальшої формалізації процедур вибору рішень та використання зворотного зв'язку для уточнення параметрів моделі.

3.5.2 Формалізація процесу вибору керуючих рішень

Після визначення основних типів рекомендацій і контрзаходів наступним етапом є формалізація процесу їх вибору. У межах багаторівневої онтологічної моделі цей процес розглядається не як автоматичне виконання наперед заданих дій, а як впорядкована процедура формування рекомендацій щодо реагування на основі оцінки ризику, контексту функціонування мережі, типу загрози та наявних обмежень.

Принципова особливість такого підходу полягає в тому, що Метод адаптивного керування не виконує повторного оцінювання вразливостей або ризиків, а використовує результати попередніх Методів як вхідні дані. Інтегральна оцінка ризику вже враховує рівень вразливості компонента, його критичність і вагову значущість відповідного сценарію, тому повторне введення інтегральної вразливості до формули вибору керуючого рішення є недоцільним.

У найзагальнішому вигляді процес вибору керуючого рішення можна подати як відображення:

$$D_m = \Psi(R_m, Ctx_m, T_m, L_m) \qquad (3.9)$$

де: D_m - рекомендоване керуюче рішення для m-го компонента або сегмента мережі, R_m - інтегральна оцінка ризику, Ctx_m - контекст функціонування компонента, T_m - тип або клас загрози, L_m - множина обмежень і допустимих умов

реагування, Ψ - оператор вибору рекомендації в межах методу адаптивного реагування.

У цьому співвідношенні R_m визначає рівень небезпеки ситуації, Ctx_m описує поточні умови функціонування компонента, T_m уточнює характер проблеми, а L_m обмежує множину допустимих рішень з урахуванням ресурсів, топології, політик реагування та можливих наслідків застосування контрзаходів. Завдяки цьому вибір рекомендації ґрунтується не лише на величині ризику, а й на тому, який саме тип проблемної ситуації виявлено.

Контекст функціонування Ctx_m відображає умови, у яких перебуває відповідний компонент або сегмент мережі. Він може включати енергетичний стан, рівень навантаження, якість каналу зв'язку, затримки, втрати пакетів, наявність резервних маршрутів і роль компонента в топології БСМ. У формалізованому вигляді контекст може бути поданий як:

Узагальнено контекст функціонування можна подати як

$$Ctx_m = \{E_m^{ctx}, H_m^{ctx}, D_m^{ctx}, Q_m^{ctx}, S_m^{ctx}, Role_m, Seg_m\} \quad (3.10)$$

де: E_m^{ctx} - контекстна оцінка енергетичного стану, H_m^{ctx} - контекстна оцінка навантаження, D_m^{ctx} - часові характеристики функціонування, Q_m^{ctx} - показники якості каналу або зв'язку, S_m^{ctx} - параметри середовища, $Role_m$ - роль компонента в топології, Seg_m - ознака належності до певного сегмента або критичної зони мережі.

Таке подання дозволяє врахувати, що одна й та сама оцінка ризику може потребувати різних рекомендацій залежно від конкретних умов функціонування. Наприклад, високий ризик для вузла з низьким рівнем енергії може зумовлювати рекомендацію щодо зниження навантаження, тоді як високий ризик для нестабільного каналу - рекомендацію щодо зміни маршруту або використання резервного з'єднання.

Тип загрози T_m уточнює природу небезпечної ситуації та пов'язує її з відповідним класом контрзаходів. У межах запропонованої моделі можуть враховуватися енергетичні, комунікаційні, топологічні, фізичні, навантажувальні або комбіновані загрози. Формалізоване подання типу загрози задається співвідношенням:

$$T_m = \in \{t^{comm}, t^{energy}, t^{physical}, t^{overload}, t^{ext}\} \quad (3.11)$$

де: t^{comm} - комунікаційна загроза, t^{energy} - загроза, пов'язана з енергетичним виснаженням, $t^{physical}$ - фізична загроза, $t^{overload}$ - загроза перевантаження, t^{ext} - зовнішня загроза.

Урахування T_m необхідне для того, щоб рекомендація відповідала не лише рівню ризику, а й характеру проблеми. Наприклад, комунікаційна загроза може потребувати зміни маршруту або використання резервного каналу, енергетична - зниження навантаження чи переходу вузла до енергоощадного режиму, а топологічна - перебудови маршруту або посилення контролю за критичним сегментом мережі.

Множина обмежень L_m визначає умови, за яких певна рекомендація може або не може бути застосована. До таких обмежень належать ресурсні, топологічні, функціональні та політичні обмеження. Ресурсні обмеження враховують доступну енергію, пропускну здатність і час реагування; топологічні - наявність альтернативних маршрутів і рівень резервування; функціональні - допустимість тимчасового обмеження роботи компонента; політичні - правила реагування та пріоритетність дій.

$$L_m = \in \{L_m^{res}, L_m^{top}, L_m^{func}, L_m^{policy}\} \quad (3.12)$$

де: L_m^{res} - комунікаційна загроза, L_m^{top} - загроза, пов'язана з енергетичним виснаженням, L_m^{func} - фізична загроза, L_m^{policy} - загроза перевантаження.

Множина L_m запобігає формуванню рекомендацій, які теоретично можуть знизити ризик, але є неприйнятними в поточному контексті функціонування

мережі. Наприклад, ізоляція вузла може бути доцільною для зниження локального ризику, однак вона не може бути рекомендована, якщо цей вузол забезпечує єдиний доступний маршрут для критичних повідомлень.

Після врахування ризику, контексту, типу загрози та обмежень формується множина допустимих альтернатив реагування:

$$A_m = \{a_1, a_2, ..., a_i\} \qquad (3.13)$$

де кожен елемент множини відповідає окремому рекомендованому контрзаходу або варіанту керуючого рішення. Подальший вибір конкретної рекомендації може здійснюватися шляхом ранжування альтернатив за рівнем очікуваного зниження ризику, відповідністю політиці реагування, допустимістю застосування та впливом на загальну працездатність БСМ.

Наприклад, високий ризик комунікаційної нестабільності може бути пов’язаний із рекомендаціями щодо зміни маршруту або локального обмеження використання проблемного каналу, тоді як критичний ризик для енергетично виснаженого вузла - з рекомендаціями щодо зниження навантаження або переходу до режиму енергозбереження. Завдяки цьому вибір рішень набуває форми семантично керованого відбору, а не лише процедурного реагування за наперед визначеним шаблоном.

Важливо, що результатом роботи Методу є саме рекомендоване рішення, а не безпосередньо виконана дія. Сформована рекомендація може бути подана оператору, передана зовнішній системі керування або використана як основа для подальшого аналізу альтернатив. Це зберігає гнучкість моделі та робить її придатною як для напівавтоматизованих, так і для автоматизованих сценаріїв функціонування. Отримана формалізація забезпечує перехід від оцінювання небезпечних станів до впорядкованого формування рекомендацій щодо реагування. Співвідношення (3.9)–(3.13) дозволяють подати процес вибору керуючих рішень як вибір або ранжування альтернатив на основі ризику, контексту, типу загрози та наявних обмежень.

3.5.3 Покрокове виконання методу адаптивного керування

Метод адаптивного керування реалізується в межах однойменного блоку багаторівневої онтологічної моделі та забезпечує перехід від оціненого ризику до формування рекомендованого керуючого рішення. На відміну від попередніх методів, які виконують опис стану, аналіз вразливостей та оцінювання ризику, цей метод орієнтований на підтримку прийняття рішень щодо реагування на виявлені небезпечні або потенційно небезпечні стани.

У запропонованій моделі результатом методу адаптивного керування є не безпосереднє автоматичне виконання дії, а рекомендоване керуюче рішення (D_m), яке може бути подане оператору або передане зовнішній системі керування. Таке рішення формується на основі інтегральної оцінки ризику, контексту функціонування компонента, типу проблемної ситуації та множини допустимих обмежень.

У загальному вигляді виконання методу передбачає такі етапи: отримання результатів оцінювання ризику; визначення типу проблемної ситуації; формування множини можливих контрзаходів; перевірку обмежень щодо їх застосування; ранжування допустимих альтернатив; вибір рекомендованого керуючого рішення; передавання рекомендації оператору або зовнішній системі керування; фіксацію результату реагування для подальшого зворотного зв’язку.

Послідовність виконання методу адаптивного керування наведено на рис. 3.8.

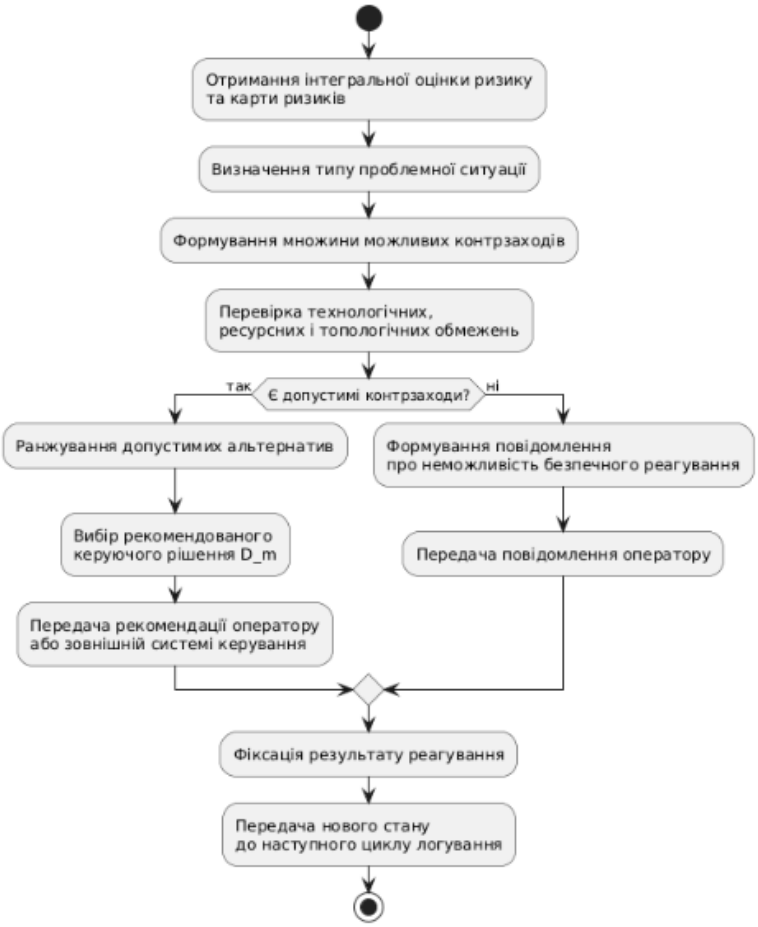

Рисунок 3.8 - Діаграма діяльності методу адаптивного керування

Як показано на рис. 3.8, метод адаптивного керування починається з отримання інтегральної оцінки ризику та карти ризиків, сформованих на попередньому етапі. Далі ризик інтерпретується з урахуванням типу загрози, контексту функціонування та допустимих обмежень. Це дозволяє не просто зафіксувати небезпечний стан, а сформувати одну або декілька доцільних рекомендацій щодо реагування.

Розглянемо проходження етапів методу адаптивного керування на прикладі спостережуваного промислового обладнання, для якого на попередньому етапі було сформовано інтегральну оцінку ризику та карту ризиків. У межах онтологічної моделі результати оцінювання ризику подаються через клас Risk, карту ризиків - як сукупність пов’язаних оцінок для компонентів, маршрутів, сегментів або спостережуваних об’єктів, а подальші рекомендації - через класи Recommendation, Countermeasure, ResponsePolicy, Constraint, PriorityLevel і Feedback.

На першому кроці метод отримує інтегральну оцінку ризику та карту ризиків. У межах онтологічної моделі ці дані подаються через клас Risk, пов’язаний із відповідними екземплярами ObservedObject, Node, Link, Route або Segment. Карта ризиків дозволяє визначити, для якого компонента, маршруту або спостережуваного об’єкта необхідно сформувати рекомендацію щодо реагування.

На другому кроці визначається тип проблемної ситуації. Якщо ризик пов’язаний зі зниженням рівня, зміною тиску або витрати, ситуація може бути віднесена до технологічної. Якщо домінують зростання температури, струму навантаження або нестабільність напруги, вона може бути технічною або експлуатаційною. Якщо основними ознаками є втрати пакетів, затримка або нестабільність каналу, ситуація має комунікаційний характер. У межах онтологічної моделі цей крок пов’язує класи Risk, Threat, Vulnerability, ObservedParameter, NodeContext і ChannelState.

На третьому кроці формується множина можливих контрзаходів. До неї можуть входити посилення моніторингу, зменшення інтервалу опитування сенсорів, зміна маршруту передавання телеметрії, обмеження навантаження компонента, перевірка обладнання, перемикання на резервний елемент або повідомлення оператора про необхідність втручання. У межах онтологічної моделі такі варіанти подаються через клас Countermeasure, а їх зв’язок із ризиковою ситуацією - через клас Recommendation.

На четвертому кроці виконується перевірка технологічних, ресурсних і топологічних обмежень. Для цього визначається, чи може кожний контрзахід бути застосований у поточному стані системи. Наприклад, не можна рекомендувати зупинку обладнання, якщо відсутній резервний елемент, або зміну маршруту, якщо альтернативний канал недоступний. У межах онтологічної моделі цей етап подається через клас Constraint, пов’язаний із Countermeasure, ObservedObject, Link, Route, Node і Segment.

На п’ятому кроці перевіряється наявність допустимих контрзаходів. Якщо такі контрзаходи існують, метод переходить до ранжування альтернатив. Якщо ж жоден контрзахід не може бути безпечно застосований через обмеження,

формується повідомлення про неможливість безпечного реагування. У межах онтологічної моделі цей умовний перехід визначається співвідношенням між класами Countermeasure, Constraint і ResponsePolicy.

На шостому кроці, за наявності допустимих контрзаходів, виконується ранжування альтернатив. Пріоритет надається тим рішенням, які забезпечують найбільше очікуване зниження ризику, не порушують обмежень, відповідають політиці реагування та не створюють додаткового критичного навантаження на інші компоненти. У межах онтологічної моделі ранжування подається через класи PriorityLevel, ResponsePolicy, Countermeasure і Risk.

На сьомому кроці обирається рекомендоване керуюче рішення (D_m). Воно може бути представлене як одна рекомендація або як упорядкований набір рекомендацій. Наприклад, для високого ризику може бути сформовано рішення про посилення моніторингу, перевірку обладнання, підготовку резервного елемента або зміну маршруту передавання телеметрії. У межах онтологічної моделі рекомендоване рішення подається через клас Recommendation, який включає один або кілька контрзаходів Countermeasure.

На восьмому кроці рекомендація передається оператору або зовнішній системі керування. При цьому метод не виконує фізичну дію самостійно, а формує обґрунтовану рекомендацію для прийняття рішення. У межах онтологічної моделі цей етап описується відношеннями між класами Recommendation, ResponsePolicy, ObservedObject і зовнішнім суб’єктом реагування. Якщо допустимих контрзаходів не було виявлено, на цьому етапі оператору передається повідомлення про неможливість безпечного реагування.

На дев’ятому кроці фіксується результат реагування та формується новий стан для наступного циклу логування. Якщо рекомендація була врахована або реалізована, у моделі фіксується її результат: зменшення ризику, відсутність змін або погіршення стану. У межах онтологічної моделі ця інформація подається через клас Feedback, який пов’язується з Recommendation, Risk, StateLogRecord, ObservedObject і відповідними компонентами БСМ. Новий стан передається до наступного циклу методу семантичного визначення та логування станів.

Окремо слід зазначити, що метод адаптивного керування не заявляється як самостійний результат наукової новизни дисертаційної роботи. Його роль полягає у практичному використанні результатів, отриманих попередніми методами, та у реалізації рекомендаційного рівня інтегрованої багаторівневої онтологічної моделі. Тому в межах цього підпідрозділу він розглядається як завершальна прикладна процедура, що забезпечує перехід від оціненого ризику до підтримки прийняття рішень.

Отже, метод адаптивного керування завершує цикл роботи запропонованої моделі. Він використовує результати логування станів, аналізу вразливостей і оцінювання ризику для формування обґрунтованих рекомендацій щодо реагування на позаштатні ситуації. Завдяки цьому модель набуває практичної спрямованості та може бути використана як основа для підтримки прийняття рішень у системах моніторингу й керування БСМ.

3.6 Висновок третього розділу

У третьому розділі розроблено інтегровану багаторівневу онтологічну модель аналізу бездротової сенсорної мережі, яка поєднує структурне, параметричне, нечітке, семантичне, вразливісне, ризикове та рекомендаційне подання компонентів БСМ. Запропонована модель забезпечує формалізований перехід від опису топології мережі, станів вузлів і каналів зв’язку до аналізу вразливостей, оцінювання ризику та формування рекомендацій щодо реагування на позаштатні ситуації.

Базове подання моделі задано у вигляді графово-атрибутивної структури $G = (V, E, A, \Phi, R, O)$, де враховано множини вузлів, зв’язків, атрибутів, динамічних параметрів, семантичних відношень та операцій над станами моделі. Таке подання дозволяє розглядати БСМ не лише як сукупність фізичних елементів і каналів зв’язку, а як онтологічну структуру, придатну для логічного висновку, аналізу поточних станів, виявлення вразливостей і подальшого оцінювання ризику.

Для підтвердження багаторівневості моделі базове плоске подання було розширено кластерним та ієрархічним рівнями. Кластерне подання дозволяє описувати локальні частини БСМ як окремі розширені онтологічні структури з власними множинами вузлів, зв'язків, атрибутів, відношень, операцій і зовнішнім інтерфейсом взаємодії. Ієрархічне подання у вигляді відношення "старший–молодший" між кластерними поданнями дозволяє формалізувати передавання узагальнених записів стану, контекстних характеристик, карт ризиків, політик реагування та рекомендацій між різними рівнями моделі. Це дає змогу обґрунтувати не лише структурну, а й семантичну багаторівневість запропонованої онтології.

У межах розділу отримав подальший розвиток метод семантичного визначення та логування станів компонентів БСМ. Метод забезпечує поетапне визначення, узгодження та фіксацію телеметричних, топологічних, контекстних і нечітко інтерпретованих характеристик компонентів мережі. Його результатом є формалізований онтологічний запис поточного стану, який подається через клас StateLogRecord і використовується як вхідна основа для подальшого аналізу вразливостей і оцінювання ризику. Введення сутностей ObservedObject та ObservedParameter дозволило пов'язати стан БСМ із параметрами спостережуваних об'єктів або середовища.

Удосконалено метод аналізу вразливостей компонентів БСМ. Його особливість полягає у використанні онтологічних правил, контекстно залежних ознак і результатів логування станів для виявлення слабких місць, критичних режимів і потенційно небезпечних конфігурацій мережі. Вразливість у запропонованій моделі розглядається не як ізольована технічна ознака, а як семантично інтерпретований результат взаємодії поточного стану компонента, його ролі в топології, контекстних факторів, умов середовища та можливих загроз. Для узагальнення результатів аналізу введено інтегральну оцінку вразливості, що враховує технічні, фізичні та зовнішні складові.

Отримав подальший розвиток узагальнений метод оцінки ризику в БСМ. На відміну від оцінки вразливості, яка характеризує схильність компонента до

переходу в небажаний або критичний стан, оцінка ризику враховує також критичність компонента, його структурну роль у мережі, участь у маршрутизації, належність до критичного сегмента, вагову значущість ризикового сценарію та можливі наслідки відмови. Це дозволило перейти від локальних оцінок окремих компонентів до формування узагальненої карти ризиків для вузлів, каналів, маршрутів, сегментів і мережі в цілому.

Метод адаптивного керування розглянуто як завершальний прикладний рівень багаторівневої онтологічної моделі. Його роль полягає не в безпосередньому автоматичному виконанні фізичних або мережевих дій, а у формуванні обґрунтованих рекомендацій для оператора або зовнішньої системи керування. Рекомендації формуються з урахуванням інтегральної оцінки ризику, карти ризиків, типу проблемної ситуації, контексту функціонування компонента та множини технологічних, ресурсних, топологічних і функціональних обмежень.

Таким чином, у третьому розділі сформовано цілісну теоретико-методичну основу багаторівневої онтологічної моделі аналізу ризиків у БСМ. Запропонована структура забезпечує послідовний перехід від семантичного визначення та логування станів до аналізу вразливостей, оцінювання ризику, побудови карти ризиків і формування рекомендацій щодо реагування. Отримані результати створюють основу для подальшої імітаційної перевірки запропонованих моделей і методів у середовищі моделювання та оцінювання їх практичної придатності для підтримки прийняття рішень у системах моніторингу й керування БСМ.

4 РЕАЛІЗАЦІЯ, ВПРОВАДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ БАГАТОРІВНЕВОЇ ОНТОЛОГІЧНОЇ МОДЕЛІ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

У попередніх розділах сформовано теоретичні та методичні засади побудови багаторівневої онтологічної моделі БСМ, що охоплює нечіткі моделі сенсорного вузла та каналу зв’язку, семантичний опис станів мережі, виявлення вразливостей, оцінювання ризиків і формування рекомендацій щодо реагування. Наступним етапом є розгляд прикладної реалізації запропонованого підходу та оцінювання можливостей його використання в задачах аналізу станів БСМ і підтримки прийняття рішень.

У цьому розділі основну увагу приділено архітектурі реалізації моделі, процедурам оцінювання контексту, інтегральної вразливості та ризику, сценаріям дослідження її функціонування, а також порівнянню з існуючими підходами. Для наочності використовується спрощена тестова БСМ, яка дозволяє простежити повний цикл роботи моделі: від опису структури мережі й формування контексту до виявлення вразливостей, оцінювання ризику та вироблення рекомендацій щодо реагування.

Такий підхід дає змогу зосередитися не на складності топології, а на демонстрації логіки функціонування запропонованої моделі та взаємозв’язку її основних Методів. У межах розділу також визначаються переваги, обмеження та практична цінність моделі як засобу ризик-орієнтованого аналізу бездротових сенсорних мереж.

4.1 Призначення та задачі реалізації багаторівневої онтологічної моделі БСМ

Після розроблення багаторівневої онтологічної моделі БСМ доцільно перейти до розгляду прикладних аспектів її реалізації. У цьому розділі реалізація моделі розглядається не як побудова завершеної програмно-апаратної системи, а як

організація прикладної схеми, що дозволяє простежити перетворення первинних мережевих параметрів у формалізовані оцінки вразливості, ризику та рекомендації щодо реагування.

Призначення реалізації полягає у практичному відтворенні логіки функціонування моделі на прикладі спрощеної тестової БСМ. Така мережа має бути достатньо простою для інтерпретації результатів, але водночас містити необхідні елементи для демонстрації впливу топологічної ролі вузлів, стану каналів зв'язку, енергетичних і навантажувальних характеристик на формування вразливостей, ризиків і рекомендацій. Для цього використовується тестова мережа з кількома сенсорними вузлами, ретранслятором і шлюзом.

Реалізація моделі орієнтована на розв'язання кількох взаємопов'язаних задач. По-перше, необхідно відтворити структурне подання тестової мережі та визначити параметри, що формують контекст її функціонування. По-друге, потрібно реалізувати процедури оцінювання контексту, інтегральної вразливості та інтегрального ризику для компонентів мережі. По-третє, слід показати вплив зміни вхідних параметрів у різних сценаріях на виявлення вразливостей, побудову карти ризиків і зміст рекомендацій щодо реагування. По-четверте, необхідно порівняти запропонований підхід з існуючими рішеннями за критеріями повноти опису мережі, урахування контексту, вразливостей, ризику та підтримки прийняття рішень.

Важливою особливістю реалізації є використання системи критеріїв оцінювання станів БСМ, яка охоплює не лише окремі технічні параметри, а й структурні, контекстні, вразливісні, ризикові та рекомендаційні ознаки. Основні критерії, що використовуються в межах реалізації моделі, наведено в табл. 4.1.

Таблиця 4.1 Критерії оцінювання, що впроваджуються в межах реалізації моделі.

Критерій	**Зміст критерію**
Топологічна роль компонента	Відображає значущість вузла або каналу в загальній структурі мережі, зокрема його участь у маршрутизації, передаванні трафіку та підтриманні зв'язності.
Належність до критичного сегмента	Показує, чи входить компонент до сегмента мережі, від якого залежить виконання ключових функцій або

	передавання важливих даних.
Рівень резервування	Характеризує наявність альтернативних вузлів, маршрутів або каналів, які можуть компенсувати відмову чи деградацію компонента.
Енергетичний стан	Відображає залишковий ресурс вузла та його здатність підтримувати функціонування в поточному режимі роботи.
Рівень навантаження	Характеризує інтенсивність використання вузла або каналу, ступінь зайнятості ресурсів і ймовірність перевантаження.
Затримка передавання	Показує часові втрати під час передавання або обробки даних і використовується для оцінки своєчасності функціонування мережі.
Якість каналу зв'язку	Характеризує стабільність і надійність передавання даних через канал, зокрема з урахуванням втрат пакетів, перешкод і деградації зв'язку.
Наявність і тип вразливості	Дозволяє визначити, чи має компонент енергетичну, комунікаційну, топологічну або фізичну вразливість.
Ступінь вираженості вразливості	Відображає, наскільки критичним є поточний вразливий стан компонента та якою мірою він може впливати на мережу.
Інтегральний ризик компонента	Узагальнює небезпеку, пов'язану з конкретним вузлом або каналом, з урахуванням його вразливостей, контексту та структурної значущості.
Інтегральний ризик сегмента або мережі	Дає змогу оцінити рівень небезпеки не лише для окремого компонента, а й для більшого фрагмента мережі або БСМ у цілому.
Пріоритетність реагування	Визначає, які небезпечні стани потребують першочергової уваги та втручання.
Допустимість контрзаходу	Показує, чи може рекомендований захід бути застосований без порушення функціональних, топологічних або ресурсних обмежень мережі.
Доцільність контрзаходу	Відображає, наскільки обраний захід відповідає характеру загрози, типу вразливості та поточному стану мережі.
Топологічна роль компонента	Відображає значущість вузла або каналу в загальній структурі мережі, зокрема його участь у маршрутизації, передаванні трафіку та підтриманні зв'язності.
Належність до критичного сегмента	Показує, чи входить компонент до сегмента мережі, від якого залежить виконання ключових функцій або передавання важливих даних.

Запровадження зазначених критеріїв дозволяє перейти від ізольованого аналізу окремих параметрів до комплексного оцінювання стану БСМ з урахуванням взаємозв'язків між структурою мережі, контекстом функціонування, вразливостями та ризиками. Це створює основу для обґрунтованого формування рекомендацій щодо реагування на позаштатні ситуації.

Проведена постановка задач реалізації визначає подальшу логіку розділу: спочатку розглядається архітектура реалізації багаторівневої онтологічної моделі, далі - процедури оцінювання контексту, вразливості та ризику, після чого аналізуються сценарії функціонування моделі та результати її порівняння з існуючими підходами.

4.2 Архітектура реалізації багаторівневої онтологічної моделі БСМ

Архітектура реалізації багаторівневої онтологічної моделі БСМ будується відповідно до логіки, сформованої в третьому розділі, і відображає послідовний перехід від первинних параметрів функціонування мережі до формування рекомендацій щодо реагування. У межах цієї архітектури модель розглядається як система взаємопов’язаних функціональних Методів, кожен із яких відповідає за окремий етап аналізу стану БСМ.

Основу архітектури становлять чотири функціональні складові: метод семантичного виявлення та логування станів компонентів, Метод виявлення вразливостей, Метод оцінки ризиків і Метод адаптивного керування. У межах практичної реалізації вони не розглядаються ізольовано, а утворюють послідовний ланцюг обробки даних, у якому результати попереднього етапу стають вхідною основою для наступного.

Початковим рівнем є метод семантичного виявлення та логування станів компонентів, який формує структурне та контекстне подання тестової БСМ. На цьому етапі задаються склад мережі, типи вузлів, канали зв’язку, маршрути передавання даних і первинні параметри стану компонентів: енергетичні показники, навантаження, затримки, втрати пакетів, якість каналів і стабільність зв’язку. Результатом роботи цього Методу є формалізований опис поточного стану мережі.

Метод виявлення вразливостей використовує структурний і контекстний опис мережі для визначення потенційно небезпечних станів її компонентів. На цьому етапі встановлюються енергетичні, комунікаційні, топологічні та інші типи

вразливостей, які виникають унаслідок поєднання параметрів вузлів, каналів, маршрутів і умов функціонування.

Метод оцінки ризиків узагальнює інформацію про виявлені вразливості, структурну значущість компонентів, контекст функціонування та можливі наслідки деградації. Результатом його роботи є інтегральні оцінки ризику для вузлів, каналів, сегментів або мережі загалом, а також карта ризиків, що відображає пріоритетність небезпечних станів.

Завершальним рівнем є Метод адаптивного керування, у межах якого результати оцінки ризику використовуються для формування рекомендацій щодо реагування. Модель не передбачає автоматичного виконання дій, а орієнтована на вироблення обґрунтованих рекомендацій, зокрема щодо зміни режиму роботи вузла, зниження навантаження, уточнення маршрутизації, посилення моніторингу або застосування інших контрзаходів.

Для наочного відображення логіки проходження даних через основні складові реалізації використовується схема послідовності, наведена на рис. 4.1.

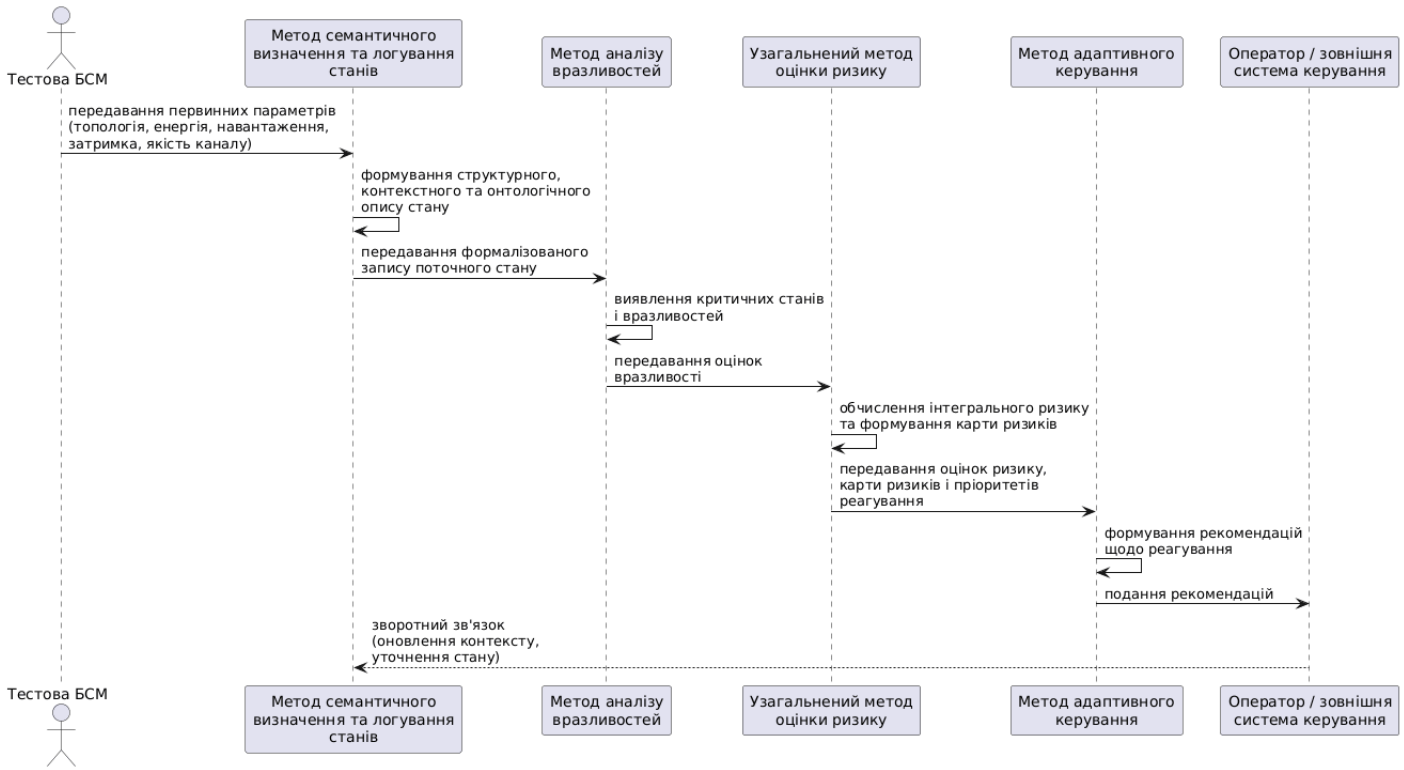

Рисунок 4.1 – Схема послідовності реалізації багаторівневої онтологічної моделі БСМ

Як показано на рис. 4.1, первинні параметри тестової мережі надходять до Методу опису мережі, де формується структурний і контекстний опис стану БСМ. Далі ці дані передаються до Методу виявлення вразливостей, після чого результати аналізу використовуються в блоці оцінки ризиків для обчислення інтегрального ризику та побудови карти ризиків. На завершальному етапі Метод адаптивного керування формує рекомендації, які можуть бути подані оператору або зовнішній системі керування. Наявність зворотного зв’язку забезпечує можливість уточнення контексту функціонування мережі та коригування подальших результатів аналізу.

Для додаткового уточнення ролі кожного функціонального Методу в загальній архітектурі реалізації доцільно розглянути вхідні та вихідні дані, що обробляються на відповідних етапах. Узагальнену характеристику таких даних наведено в табл. 4.2.

Таблиця 4.2 Вхідні та вихідні дані Методів архітектури реалізації моделі.

Метод	**Вхідні дані**	**Вихідні дані**
Метод семантичного виявлення та логування станів компонентів	топологія тестової мережі, характеристики вузлів, параметри каналів зв’язку, телеметричні дані, результати нечіткого оцінювання	структурний опис мережі, контекст функціонування вузлів і каналів, формалізоване подання поточного стану БСМ
Метод виявлення вразливостей	структурний опис мережі, контекст функціонування, параметри вузлів і каналів, правила логічного висновку	виявлені вразливості, класифікація критичних станів, оцінки інтегральної вразливості компонентів
Метод оцінки ризиків	дані про вразливості, контекст функціонування, структурна значущість компонентів, фактори середовища та зовнішні впливи	інтегральні оцінки ризику для вузлів, каналів, сегментів і мережі в цілому, карта ризиків, пріоритети реагування
Метод адаптивного керування	інтегральні оцінки ризику, інформація про вразливості, контекст	рекомендації щодо реагування, пріоритети контрзаходів, дані для

	функціонування мережі, обмеження та політики реагування	зворотного зв’язку та уточнення подальших рішень

Як видно з табл. 4.2, архітектура реалізації має послідовний характер: структурний і контекстний опис мережі використовується для виявлення вразливостей, результати цього етапу - для оцінювання ризиків, а інтегральні оцінки ризику - для формування рекомендацій щодо реагування. Така організація дозволяє поєднати в межах однієї прикладної схеми опис мережі, аналіз її поточного стану, ризикове оцінювання та підтримку вибору контрзаходів.

Отримана архітектура реалізації створює основу для практичного аналізу тестової БСМ і подальшого розгляду процедур оцінювання контексту, інтегральної вразливості та ризику.

4.3 Сценарії дослідження та аналіз результатів

Мета сценарного аналізу полягає в тому, щоб перевірити, як зміна режиму функціонування мережі впливає на її телеметричні, комунікаційні та поведінкові характеристики, а також наскільки ці зміни узгоджуються з аналітичними оцінками контексту, вразливості та ризику. Для цього використовуються два базові сценарії: нормальне функціонування мережі та деградація окремих компонентів.

Сценарій нормального функціонування відображає штатний режим роботи тестової мережі, за якого вузли й канали мають допустимі значення основних параметрів, а передавання даних здійснюється без суттєвих втрат і затримок. Сценарій деградації моделює погіршення стану окремих компонентів, зокрема зниження енергетичного ресурсу вузла, підвищення навантаження на ретранслятор і погіршення характеристик ключового каналу зв’язку.

У межах цього підрозділу послідовно розглядаються постановка сценаріїв дослідження, результати імітаційного моделювання тестової мережі та їх аналітична інтерпретація. Такий підхід дозволяє перейти від числових і

поведінкових характеристик мережі до висновків щодо найбільш критичних компонентів, характеру деградації їх стану та можливих напрямів реагування.

4.3.1 Постановка сценаріїв дослідження

Для перевірки працездатності запропонованої багаторівневої онтологічної моделі в середовищі OMNeT++ у межах цього підрозділу використано два базові сценарії дослідження, які відображають різні режими функціонування тестової бездротової сенсорної мережі. Такий вибір дозволяє не лише порівняти поведінку мережі в штатному та погіршеному режимах, а й простежити, як зміни її телеметричних і комунікаційних параметрів впливають на подальше формування контексту, інтегральної вразливості та ризику.

Як і в попередньому підрозділі, у межах імітаційного дослідження використовується спрощена тестова мережа, що складається з двох сенсорних вузлів, одного ретранслятора та одного шлюзу. Сенсорні вузли виконують функцію збирання та первинного передавання даних, ретранслятор забезпечує транзитне пересилання трафіку, а шлюз виступає кінцевою точкою приймання інформації та взаємодії із зовнішнім середовищем або системою керування. Така структура є достатньою для того, щоб відобразити як локальні зміни параметрів окремих компонентів, так і їх вплив на загальне функціонування мережі.

Перший сценарій відповідає нормальному функціонуванню мережі. У цьому режимі сенсорні вузли мають достатній енергетичний ресурс, навантаження на ретранслятор не перевищує допустимих меж, а канали зв’язку характеризуються високою якістю, стабільністю та низьким рівнем втрат пакетів. Передавання даних у такому сценарії здійснюється без суттєвих затримок, а мережа в цілому зберігає стабільний режим роботи. Саме цей сценарій використовується як базовий, оскільки він дозволяє зафіксувати референтні значення телеметричних, комунікаційних і мережевих показників, з якими надалі порівнюються результати сценарію деградації.

Другий сценарій відповідає деградації окремих компонентів мережі. У межах цього сценарію моделюється поєднання кількох несприятливих змін: зниження енергетичного ресурсу одного із сенсорних вузлів, зростання навантаження на ретранслятор і погіршення характеристик ключового каналу зв’язку між ретранслятором і шлюзом. Така постановка сценарію дозволяє відтворити ситуацію, у якій локальне погіршення стану окремих елементів мережі поступово впливає на загальну якість передавання даних, стійкість функціонування та ефективність взаємодії компонентів.

Вибір саме таких сценаріїв обумовлений тим, що вони дозволяють охопити дві принципово різні ситуації: штатне функціонування мережі та розвиток небезпечних станів у разі деградації її найбільш чутливих елементів. У першому випадку перевіряється, чи зберігає мережа стабільні характеристики роботи за відсутності виражених збурень. У другому випадку оцінюється, як зниження енергетичного ресурсу, зростання навантаження та погіршення зв’язку впливають на передавання трафіку, затримки, втрати пакетів та завантаженість проміжних вузлів. Саме це дозволяє використати результати моделювання не лише для технічного аналізу роботи мережі, а й для подальшої інтерпретації в межах ризик-орієнтованого підходу.

У середовищі OMNeT++ для кожного зі сценаріїв доцільно реєструвати телеметричні та мережеві показники, що характеризують функціонування вузлів і каналів. До них належать залишковий енергетичний ресурс вузлів, рівень навантаження на ретранслятор, затримка передавання даних, втрати пакетів, зміна якості каналу зв’язку, інтенсивність трафіку та стабільність передавання повідомлень. Сукупність цих показників дозволяє сформувати кількісну основу для подальшого аналізу та співвіднести результати імітаційного моделювання з контекстними, вразливісними та ризиковими оцінками, отриманими раніше в середовищі Scilab.

Для зручності сприйняття основні характеристики досліджуваних сценаріїв доцільно подати у вигляді узагальнювальної таблиці. Це дозволяє чітко зафіксувати

відмінності між умовами нормального функціонування та деградації, а також показати, які саме фактори виступають джерелом змін у поведінці мережі.

Таблиця 4.3 Результати оцінювання інтегрального ризику компонентів тестової мережі

Сценарій	**Характеристика режиму**	**Основні зміни параметрів**	**Очікувані наслідки**
Сценарій 1 – нормальне функціонування	штатний режим роботи мережі	достатній енергетичний ресурс вузлів, стабільні канали зв’язку, помірне навантаження на ретранслятор	стабільне передавання даних, низькі затримки, мінімальні втрати пакетів
Сценарій 2 – деградація компонентів	порушення штатного режиму	перевантаження ретранслятора (N3), погіршення характеристик каналу (L3)	зростання затримок, погіршення якості зв’язку, збільшення втрат пакетів, підвищення небезпечності станів мережі

Як видно, з табл. 4.3, обрані сценарії дозволяють задати чітко розмежовані умови функціонування мережі та забезпечують основу для подальшого порівняльного аналізу результатів моделювання. Саме завдяки цьому можна простежити, як зміна режиму роботи тестової мережі впливає на її телеметричні, комунікаційні та поведінкові характеристики, а також наскільки ці зміни узгоджуються з аналітичними оцінками контексту, вразливості та ризику.

Таким чином, постановка сценаріїв дослідження створює основу для подальшого аналізу результатів імітаційного моделювання в середовищі OMNeT++. Обидва сценарії - нормального функціонування та деградації компонентів - дозволяють перевірити чутливість запропонованої моделі до змін у стані мережі та підготувати основу для інтерпретації отриманих результатів у термінах контексту, вразливості, ризику та рекомендацій щодо реагування. Саме на цій основі в наступному підпункті розглядаються результати імітаційного моделювання тестової мережі.

4.3.2 Результати імітаційного моделювання тестової мережі

Після задання структури тестової мережі, формування сценаріїв дослідження та налаштування параметрів імітаційного експерименту в середовищі OMNeT++ 6.3.0 наступним етапом є аналіз результатів моделювання для двох розглянутих режимів функціонування. Основна мета цього етапу полягає у визначенні того, як зміна параметрів окремих вузлів і каналів впливає на передавання даних у мережі, рівень втрат пакетів, затримки, навантаження на ретранслятор та зміну енергетичного стану компонентів. На відміну від попереднього підрозділу, де було визначено параметри експерименту, у цьому підпункті основна увага приділяється безпосередньо результатам функціонування мережі в межах обох сценаріїв.

Вихідні умови імітаційного експерименту для сценарію нормального функціонування та сценарію деградації компонентів наведено в попередньому підпункті. Саме ці параметри - початковий заряд акумулятора вузлів, навантаження на ретранслятор, затримки каналів, імовірності втрат пакетів і пропускні здатності ліній зв’язку - визначають відмінності між обома режимами роботи тестової мережі та є основою для подальшої інтерпретації отриманих результатів.

У межах імітаційної реалізації Метод адаптивного керування не розглядається як автономний виконавчий механізм, що безпосередньо змінює конфігурацію мережі без участі зовнішнього середовища. Його призначення полягає у формуванні рекомендацій щодо доцільних напрямів реагування на основі узагальнених результатів аналізу стану мережі, виявлених вразливостей та оцінених ризиків. Такий підхід дозволяє зберегти універсальність запропонованої моделі, оскільки одна й та сама проблемна ситуація в різних прикладних системах може потребувати різних рішень залежно від допустимих затримок, енергетичних обмежень, вимог до надійності чи особливостей технологічного процесу.

У межах моделювання для кожного зі сценаріїв фіксувалися кількість згенерованих пакетів, кількість пересланих ретранслятором повідомлень, кількість втрачених пакетів на ділянках L1, L2 і L3, кількість успішно отриманих пакетів на шлюзі, середня наскрізна затримка та залишковий заряд акумулятора вузлів після

завершення моделювання. Сукупність цих показників дозволяє оцінити не лише загальний рівень працездатності мережі, а й визначити, які саме компоненти є джерелом погіршення її функціонування в сценарії деградації.

Для узагальнення результатів моделювання наведемо зведену таблицю основних спостережуваних показників.

Таблиця 4.4 Основні результати імітаційного моделювання тестової мережі в OMNeT++

Показник	**Сценарій 1 – нормальне функціонування**	**Сценарій 2 – деградація компонентів**
Кількість згенерованих пакетів вузлом N1	100	100
Кількість згенерованих пакетів вузлом N2	100	100
Кількість пересланих пакетів ретранслятором N3	180	142
Кількість втрачених пакетів на L1	3	4
Кількість втрачених пакетів на L2	5	12
Кількість втрачених пакетів на L3	10	40
Кількість пакетів, отриманих шлюзом N4	180	142
Середня наскрізна затримка, мс	64.23	157.26

Як видно, з табл. 4.4, у сценарії нормального функціонування мережа забезпечує відносно високу ефективність передавання даних. Кількість пакетів, отриманих шлюзом, збігається з кількістю пакетів, пересланих ретранслятором, а середня наскрізна затримка залишається помірною. Втрати пакетів на всіх трьох ділянках мережі є невеликими, причому навіть у цьому режимі найбільша їх кількість спостерігається на ділянці L3, що пояснюється завершальним характером цієї лінії передавання.

У сценарії деградації спостерігається суттєве погіршення основних показників функціонування мережі. Кількість пакетів, які доходять до шлюзу, зменшується до 142, що безпосередньо вказує на зниження ефективності передавання даних. Одночасно середня наскрізна затримка зростає до 157.26 мс,

тобто більш ніж у 2.4 раза порівняно з нормальним режимом. Найбільш критичні зміни пов’язані з каналом L3, на якому кількість втрачених пакетів збільшується до 40, що у чотири рази перевищує відповідний показник для сценарію нормального функціонування. Паралельно з цим вузол N2 демонструє значне зменшення залишкового заряду акумулятора, а ретранслятор N3 повністю вичерпує енергетичний ресурс. Це підтверджує, що саме ретранслятор і завершальна ділянка передавання даних є найбільш чутливими елементами тестової мережі в умовах деградації.

Уже на рівні табличного подання результатів видно, що погіршення роботи мережі має не випадковий, а структурно зумовлений характер. Деградація периферійного вузла N2 впливає насамперед на локальний сегмент мережі, тоді як зміни стану ретранслятора N3 та каналу L3 безпосередньо позначаються на загальній здатності мережі доставляти трафік до шлюзу. Саме це узгоджується з результатами математичного моделювання в Scilab, де найбільш критичними компонентами також були визначені N3 і L3.

Додатковим підтвердженням коректності інтерпретації результатів є службові індикатори, сформовані в межах імітаційної реалізації для Методу адаптивного керування. Їх використання дає змогу не лише зафіксувати факт погіршення функціонування мережі, а й узагальнити результати аналізу у вигляді ознак, придатних для формування рекомендацій щодо реагування. У сценарії нормального функціонування значення riskFlag = 0, criticalComponentId = 0 та recommendedActionCode = 0, що свідчить про відсутність критичного стану, пріоритетного проблемного компонента та потреби у спеціальних рекомендаціях. Це узгоджується з основними показниками моделювання, за яких мережа забезпечує стабільну доставку пакетів, помірну затримку та прийнятний рівень використання енергетичного ресурсу.

У сценарії деградації, навпаки, зафіксовано riskFlag = 1, criticalComponentId = 3 та recommendedActionCode = 2. Це означає, що модель виявляє позаштатний стан, визначає як критичні одночасно ретранслятор N3 і канал L3, а також формує рекомендацію щодо обмеження участі деградованого компонента в мережевій

взаємодії. Такий результат узгоджується з аналізом затримок, втрат пакетів та енергетичного стану вузлів, оскільки саме N3 і L3 у деградованому сценарії справляють найбільший вплив на загальну працездатність мережі.

Водночас значення recommendedActionCode = 2 слід трактувати не як жорстку автоматичну команду, а як узагальнену рекомендацію, сформовану Методом адаптивного керування на основі результатів, отриманих від Методу опису мережі, Методу аналізвразливостей та Методу оцінки ризику. Конкретний спосіб реалізації такої рекомендації має визначатися оператором або зовнішньою системою керування з урахуванням вимог конкретної прикладної системи. Таким чином, службові індикатори riskFlag, criticalComponentId та recommendedActionCode підтверджують, що Метод адаптивного керування в запропонованій моделі виконує функцію формування обґрунтованих рекомендацій щодо реагування на позаштатні ситуації.

Для більш наочного порівняння результатів доцільно представити окремі залежності у вигляді графіків. До них належать, зокрема, порівняння кількості успішно доставлених пакетів, середньої затримки, втрат пакетів на окремих ділянках мережі та залишкового заряду акумулятора вузлів.

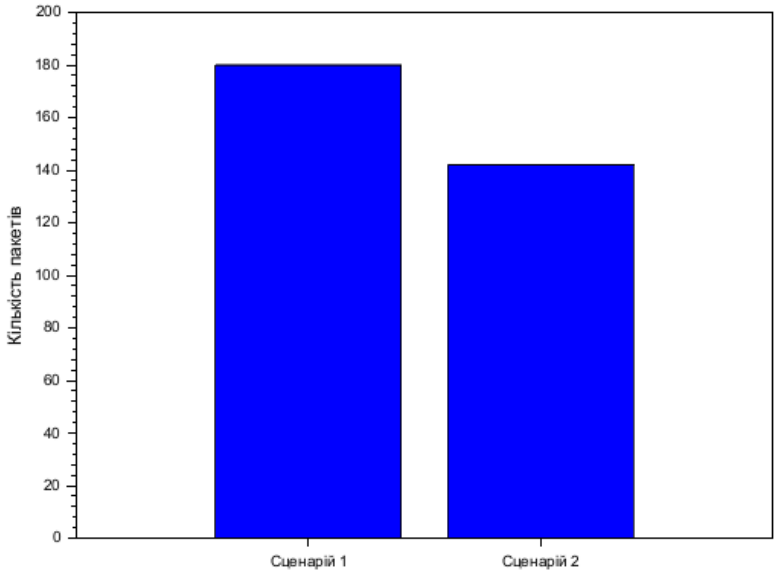

Рисунок 4.2 – Порівняння кількості пакетів, отриманих шлюзом, у різних сценаріях

Як видно з рис. 4.2, у сценарії деградації кількість пакетів, успішно доставлених до шлюзу, суттєво зменшується - зі 180 до 142. Це безпосередньо

свідчить про зниження ефективності передавання даних у мережі внаслідок погіршення стану її окремих компонентів. Зменшення цього показника має не випадковий, а структурно зумовлений характер, оскільки воно пов’язане насамперед із погіршенням роботи ретранслятора N3 і каналу L3, через які проходить агрегований трафік від обох сенсорних вузлів до шлюзу. Таким чином, навіть за умови збереження однакової інтенсивності генерації пакетів на вузлах N1 і N2, зниження надійності центральних елементів мережі призводить до відчутної втрати повідомлень на кінцевому етапі доставки. Це підтверджує, що для оцінювання стану БСМ недостатньо враховувати лише кількість згенерованих повідомлень, а необхідно аналізувати також поведінку критичних компонентів, від яких залежить загальна зв’язність мережі.

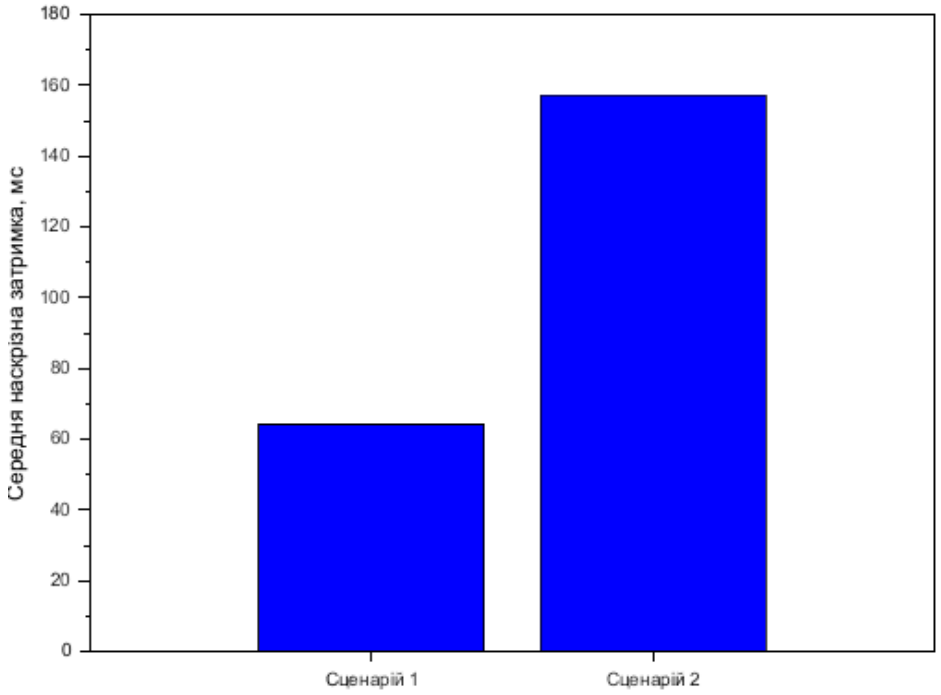

Рисунок 4.3 – Порівняння середньої наскрізної затримки в різних сценаріях

Рисунок 4.3 показує, що в сценарії деградації середня наскрізна затримка зростає з 64.23 мс до 157.26 мс. Це є наслідком одночасного впливу підвищеного навантаження на ретранслятор і погіршення характеристик каналу L3L3L3. Таким чином, затримка виявляється чутливою не тільки до окремих змін параметрів, а й до накопичення проблем у критичних елементах мережі. У нормальному режимі значення затримки відповідає стабільному передаванню даних, тоді як у режимі деградації вона вже відображає системне ускладнення проходження трафіку через

мережу. Зростання цього показника підтверджує, що навіть за збереження незмінної інтенсивності генерації повідомлень загальна якість функціонування БСМ може різко погіршуватися через перевантаження центрального вузла та нестабільність завершальної ділянки зв’язку.

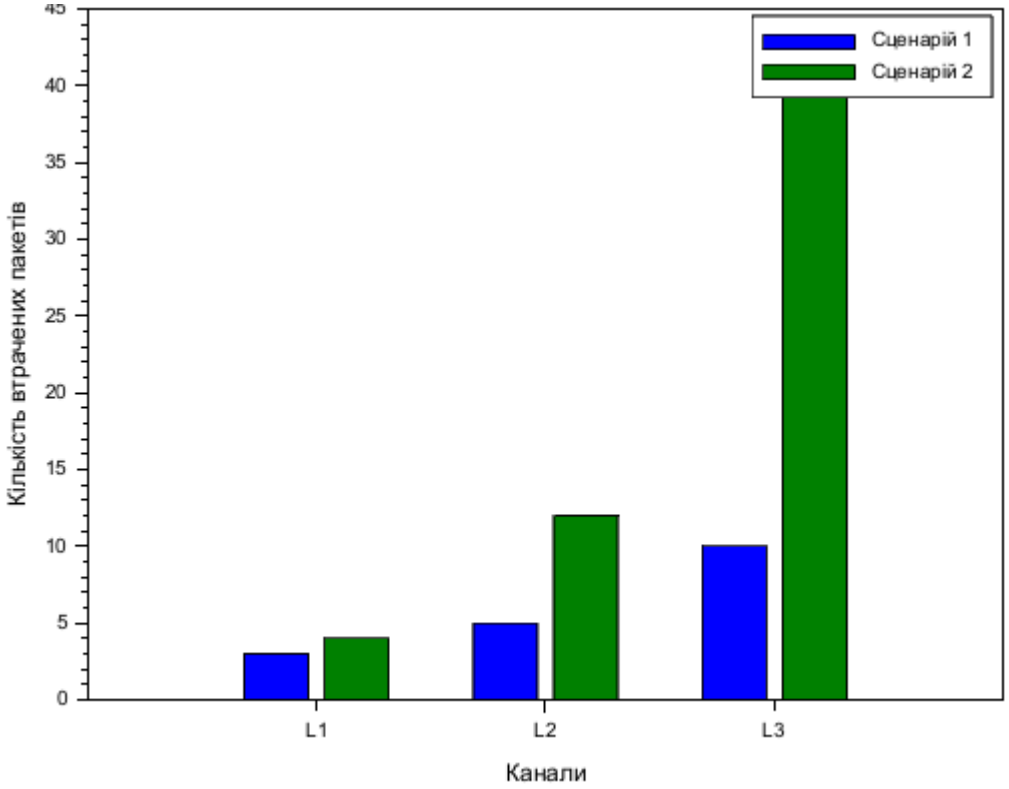

Рисунок 4.4 – Порівняння втрат пакетів на каналах L1, L2 та L3

Як видно з рис. 4.4, втрати пакетів у сценарії деградації зростають на всіх ділянках мережі, однак найбільш помітне збільшення спостерігається для каналу L3, де кількість втрачених пакетів підвищується з 10 до 40. Це підтверджує, що саме цей канал є найбільш критичним для забезпечення стабільної доставки даних до шлюзу. На відміну від каналів L1 та L2, які переважно впливають на окремі потоки даних від сенсорних вузлів, деградація L3 відображається на всьому агрегованому трафіку мережі. Саме тому навіть відносно невеликі зміни в його характеристиках призводять до значного зменшення кількості пакетів, які доходять до кінцевої точки мережі. Отриманий результат добре узгоджується з попередніми висновками, зробленими в межах математичного моделювання, де канал L3 також був визначений як один із найбільш проблемних елементів за значеннями контексту, інтегральної вразливості та ризику.

Отримані результати моделювання створюють підґрунтя не лише для аналізнайбільш проблемних компонентів тестової мережі, а й для формування рекомендацій щодо реагування на виявлені позаштатні стани. Зокрема, для вузлів і каналів, що демонструють зростання затримки, втрат пакетів або прискорене виснаження енергетичного ресурсу, можуть бути рекомендовані зміна режиму роботи, обмеження участі в мережевій взаємодії, коригування параметрів передавання або посилення моніторингу. При цьому запропонована модель не фіксує жорстко єдиний сценарій дій, а формує рекомендаційну основу, яка надалі адаптується оператором або зовнішньою системою керування відповідно до вимог конкретного застосування.

Таким чином, результати імітаційного моделювання тестової мережі в середовищі OMNeT++ 6.3.0 підтверджують, що запропоновані сценарії дозволяють відтворити як стабільний режим функціонування БСМ, так і режим деградації її окремих компонентів. Найбільш суттєві зміни спостерігаються для ретранслятора N3 і каналу L3, що проявляється у зростанні затримок, збільшенні втрат пакетів і швидшому виснаженні ресурсу відповідних вузлів. Додатково це підтверджується службовими індикаторами Методу адаптивного керування, які в деградованому сценарії фіксують наявність ризику, визначають критичні компоненти та формують рекомендацію щодо реагування. Отримані результати узгоджуються з аналітичними оцінками контексту, інтегральної вразливості та ризику, отриманими в підрозділі 4.3, і створюють основу для подальшого порівняння запропонованого підходу з існуючих рішенньь.

4.4 Порівняння запропонованої моделі з існуючими підходами до оцінювання ризиків

Для визначення місця запропонованої багаторівневої онтологічної моделі в межах існуючих підходів до оцінювання ризиків виконано її порівняння з найбільш поширеними методологіями та стандартизованими підходами. До таких підходів у межах даного дослідження віднесено методологію CORAS, стандартизований підхід ISO/NIST/IEC та системно-теоретичний підхід STPA-Sec. Вибір саме цих

підходів зумовлений тим, що вони використовуються для аналізу ризиків, опису небезпечних сценаріїв, аналіззагроз і підтримки прийняття рішень у складних технічних, інформаційних та кіберфізичних системах.

Перед виконанням порівняння доцільно уточнити сферу практичного використання розглянутих підходів. CORAS, ISO/NIST/IEC та STPA-Sec не є спеціалізованими моделями бездротової сенсорної мережі, а належать до ширших методологій аналізу ризиків, управління безпекою та аналіз небезпечних сценаріїв у складних системах.

Методологія CORAS використовується переважно в системах і рішеннях, де необхідно побудувати формалізовані сценарії ризику та наочно показати зв’язки між загрозами, вразливостями, небажаними подіями й наслідками. Такий підхід може застосовуватися для аналізу інформаційних систем, IoT-рішень, кіберфізичних систем, транспортних і морських систем, а також для оцінювання ризиків у комунікаційних середовищах. Його практична цінність полягає у побудові діаграм ризику, які зручні для обговорення з експертами, документування сценаріїв загроз і вибору контрзаходів. Проте CORAS здебільшого використовується як методика аналізу та візуалізації ризиків, а не як спеціалізований механізм поточного аналізу стану вузлів і каналів бездротової сенсорної мережі.

Стандартизований підхід ISO/NIST/IEC застосовується в організаційних, інформаційних, промислових і кібербезпекових системах, де необхідно побудувати узгоджену процедуру управління ризиками. Такі підходи використовуються під час створення систем менеджменту інформаційної безпеки, проведення аудитів, формування реєстрів ризиків, вибору заходів захисту, оцінювання кіберризиків підприємства та проєктування захищених промислових систем керування. У контексті промислових систем особливе значення мають стандарти, орієнтовані на автоматизовані системи керування, SCADA, IACS та кіберфізичні системи. Їх перевагою є нормативна узгодженість і універсальність, однак вони не задають конкретної моделі сенсорної мережі та не визначають способу семантичного опису вузлів, каналів, вразливостей і ризикових станів БСМ.

У межах даного порівняння під підходом ISO/NIST/IEC розуміється узагальнена група нормативних і методичних документів з управління та оцінювання ризиків, зокрема ISO 31000:2018 “Risk management - Guidelines”, ISO/IEC 27005:2022 “Information security, cybersecurity and privacy protection - Guidance on managing information security risks”, NIST SP 800-30 Rev. 1 “Guide for Conducting Risk Assessments”, NIST IR 8286A “Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management” та IEC 62443-3-2:2020 “Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design”. Зазначені документи розглядаються як стандартизована нормативно-методична база для ідентифікації загроз, аналізу вразливостей, оцінювання ризику, вибору заходів реагування та документування результатів. Водночас вони не задають спеціалізованої моделі бездротової сенсорної мережі, тому в подальшому для компактності цей підхід позначено як ISO/NIST/IEC.

STPA-Sec використовується переважно в складних кіберфізичних системах, де важливими є процеси керування, взаємодія між компонентами та можливі небезпечні керуючі дії. Цей підхід застосовується для аналізу безпеки транспортних, авіаційних, морських, промислових, автономних та інших систем, у яких порушення взаємодії між елементами може призвести до небезпечного стану. STPA-Sec дозволяє виявляти системні причини ризику, визначати небезпечні сценарії та формувати вимоги до безпечного керування. Водночас він не є спеціалізованим для бездротових сенсорних мереж і не містить власного механізму нечіткого опису стану сенсорних вузлів, якості каналів зв’язку або топологічної ролі компонентів мережі.

Таблиця 4.5 Сфера використання розглянутих підходів до оцінювання ризиків

Підхід	**Де зазвичай використовується**	**Типові рішення**
CORAS	Інформаційні системи, IoT-рішення, кіберфізичні, транспортні та морські системи	Діаграми ризику, сценарії загроз, опис небажаних подій, вибір контрзаходів
ISO/NIST/IEC	Організації, системи інформаційної безпеки, промислові системи керування, SCADA/IACS	Політики безпеки, реєстри ризиків, аудит, оцінювання кіберризиків,

		вибір контролів безпеки
STPA-Sec	Кіберфізичні, автономні, транспортні, авіаційні, промислові та керуючі системи	Аналіз небезпечних керуючих дій, визначення системних причин ризику, формування вимог безпеки
Запропонова на модель	Бездротові сенсорні мережі промислового призначення	Онтологічна карта станів, вразливостей і ризиків, формування рекомендацій щодо реагування

Запропонована багаторівнева онтологічна модель відрізняється від зазначених підходів тим, що орієнтована саме на аналіз ризиків у бездротових сенсорних мережах. Вона поєднує графово-атрибутивний опис структури мережі, нечіткі моделі сенсорного вузла та каналу зв'язку, онтологічне подання вразливостей, узагальнене оцінювання ризику та Метод адаптивного керування, який формує рекомендації щодо реагування. Такий підхід дозволяє враховувати не лише факт наявності загрози, а й поточний стан вузлів, якість каналів, контекст функціонування мережі, топологічну роль компонентів і можливі наслідки для роботи БСМ.

Для більш наочного порівняння запропонованої багаторівневої онтологічної моделі з існуючими підходами було виконано критеріальну оцінку їх функціональної повноти щодо задач аналізу ризиків у бездротових сенсорних мережах. Така оцінка не є результатом натурних польових випробувань, а відображає ступінь покриття ключових функціональних вимог, необхідних для ризик-орієнтованого аналізу БСМ.

Для оцінювання використано шкалу: 0 % - критерій не враховується; 33 % - критерій враховується обмежено або потребує значної адаптації; 66 % - критерій підтримується частково; 85 % - критерій добре підтримується, але не є спеціалізованим для БСМ; 100 % - критерій повністю підтримується в межах запропонованої моделі. Узагальнений показник функціональної повноти визначався як середнє значення оцінок за обраними критеріями:

$$K = \frac{\sum_{i=1}^{n} q_i}{n} \times 100\% \qquad (4.1)$$

де q_i – оцінка за окремим критерієм, n – кількість критеріїв.

Таблиця 4.6 – Критеріальна оцінка функціональної повноти підходів до аналізу ризиків у БСМ

Критерій порівняння	CORAS	ISO/NIST/IEC	STPA-Sec	Запропонова на модель
Спеціалізація для БСМ	33%	33%	33%	100%
Урахування структури та топології мережі	33%	0%	66%	100%
Урахування поточного стану вузлів і каналів	33%	0%	33%	100%
Використання нечітких оцінок і станів невизначеності	0%	0%	0%	100%
Аналіз вразливостей	85%	100%	66%	100%
Оцінювання ризику	85%	100%	66%	100%
Урахування топологічної ролі компонента	33%	0%	66%	100%
Формування рекомендацій щодо реагування	66%	85%	66%	85%
Узгодження структурного, параметричного, онтологічного та рекомендаційного рівнів	66%	33%	66%	100%
Узагальнений показник функціональної повноти	48.2%	35.2%	51.3%	98.3%

Для наочного подання результатів критеріальної оцінки доцільно побудувати діаграму порівняння узагальненого показника функціональної повноти для розглянутих підходів.

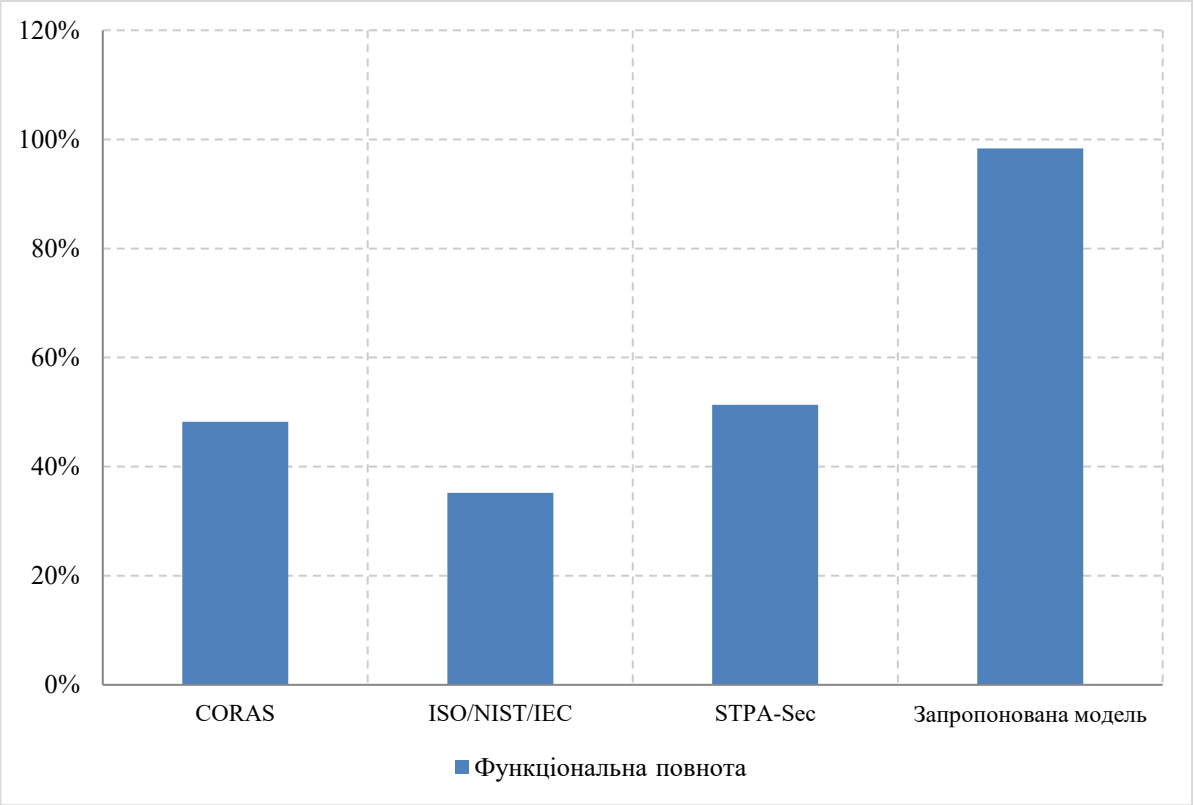

Рисунок 4.5 – Порівняння функціональної повноти підходів до оцінювання ризиків у БСМ

За результатами критеріальної оцінки запропонована багаторівнева онтологічна модель має узагальнений показник функціональної повноти 98,3 %. Для CORAS цей показник становить 48,2 %, для стандартизованого підходу ISO/NIST/IEC - 35,2 %, а для STPA-Sec - 51,3 %. Отже, порівняно з CORAS запропонована модель має вищий рівень функціонального покриття на 50,1 відсоткових пункти, порівняно з ISO/NIST/IEC - на 63,1 відсоткових пункти, а порівняно зі STPA-Sec - на 47,0 відсоткових пункти.

У відносному вираженні функціональна повнота запропонованої моделі є приблизно на 103,9 % вищою, ніж у CORAS, на 179,0 % вищою, ніж у ISO/NIST/IEC, та на 91,6 % вищою, ніж у STPA-Sec. При цьому такі відсоткові значення слід розглядати не як прямий приріст швидкодії, енергетичної ефективності або продуктивності мережі, а як показник повноти покриття функціональних вимог до аналізу ризиків у БСМ.

Основне покращення досягається за рахунок того, що запропонована модель є спеціалізованою саме для бездротових сенсорних мереж. Вона враховує

структуру мережі, топологічну роль вузлів і каналів, поточний стан компонентів, нечітку інтерпретацію параметрів, онтологічне подання вразливостей, оцінювання ризику та формування рекомендацій щодо реагування. На відміну від CORAS, ISO/NIST/IEC та STPA-Sec, запропонована модель не обмежується лише загальним описом загроз або процедурою управління ризиками, а забезпечує цілісне подання БСМ як об’єкта ризик-орієнтованого аналізу.

Окремою перевагою моделі є можливість опосередкованого зменшення витрат заряду акумуляторів сенсорних вузлів. Це досягається не шляхом прямого керування енергоспоживанням, а завдяки ранньому виявленню критичних або перевантажених компонентів, урахуванню їх топологічної ролі та формуванню рекомендацій щодо зміни режиму роботи, обмеження участі окремих вузлів або перерозподілу навантаження. Оскільки окремі натурні випробування енергетичної ефективності не проводилися, цей ефект доцільно розглядати як потенційну перевагу моделі, що потребує подальшої експериментальної перевірки.

Таким чином, основна відмінність запропонованої багаторівневої онтологічної моделі від існуючих підходів полягає у спеціалізованому поданні БСМ як об’єкта ризик-орієнтованого аналізу. Модель дозволяє узгодити опис структури мережі, параметричні характеристики її компонентів, нечітко інтерпретовані стани, вразливості, ризикові фактори та рекомендації щодо реагування в єдиній онтологічній структурі. Відсоткове порівняння показує, що перевага запропонованої моделі полягає не в одному окремому параметрі, а в інтеграції структурного, параметричного, нечіткого, онтологічного та рекомендаційного рівнів аналізу. Саме така інтеграція підвищує повноту аналізу ризиків і придатність отриманих результатів для підтримки прийняття рішень в умовах невизначеності.

Переваги запропонованої багаторівневої онтологічної моделі полягають у її спеціалізації для бездротових сенсорних мереж та можливості узгодженого подання різнорідних характеристик мережі в межах єдиної структури. На відміну від загальних підходів до аналізу ризиків, модель поєднує опис топології БСМ, параметричні характеристики вузлів і каналів, нечітко інтерпретовані стани,

вразливості, ризикові фактори та рекомендації щодо реагування. Це дозволяє розглядати ризиковий стан не як ізольовану подію, а як результат взаємодії технічних, топологічних, контекстних і зовнішніх факторів.

Разом з тим запропонована модель має певні обмеження. Її ефективність залежить від повноти початкового опису мережі, коректності заданих онтологічних залежностей, правил логічного висновку та параметрів нечіткої інтерпретації станів. Крім того, у межах даного дослідження не виконувалося окреме натурне тестування енергетичної ефективності, тому можливе зменшення витрат заряду акумуляторів слід розглядати як потенційну перевагу моделі. Такий ефект може досягатися опосередковано: завдяки ранньому виявленню критичних або перевантажених компонентів, урахуванню їх топологічної ролі та формуванню рекомендацій щодо зміни режиму роботи або перерозподілу навантаження.

Практична цінність запропонованої моделі полягає в можливості її використання як основи для побудови засобів підтримки прийняття рішень у системах моніторингу та керування бездротовими сенсорними мережами. Модель може бути застосована для аналіз критичних компонентів мережі, аналізу причин виникнення ризикових станів, побудови карти ризиків і формування рекомендацій оператору або зовнішній системі керування. Таким чином, результати порівняння підтверджують доцільність використання запропонованої багаторівневої онтологічної моделі для ризик-орієнтованого аналізу БСМ в умовах невизначеності.

4.5 Впровадження базової частини моделі в роботі

Окремі результати дисертаційного дослідження впроваджено в діяльність ТОВ «Інтелект Груп Компані», що підтверджено довідкою про впровадження результатів дисертаційної роботи. Практичного використання набули положення, пов’язані з методом адаптивного керування у структурі багаторівневої онтологічної моделі бездротової сенсорної мережі. У межах дисертаційної роботи цей метод розглядається як завершальний прикладний рівень моделі, призначений для використання результатів семантичного визначення та логування станів компонентів БСМ, аналізу вразливостей і оцінювання ризику з подальшим формуванням рекомендацій щодо реагування на позаштатні або потенційно небезпечні ситуації.

У діяльності підприємства використано підхід до формування рекомендацій щодо реагування на ризикові ситуації з урахуванням поточного контексту функціонування мережі, характеру виявлених вразливостей, рівня ризику, а також ресурсних, топологічних і функціональних обмежень. Такий підхід відповідає запропонованому в роботі поданню методу адаптивного керування як засобу підтримки прийняття рішень, а не як механізму безпосереднього автоматичного виконання фізичних або мережевих дій.

Також практичного використання набуло онтологічне подання основних сутностей методу адаптивного керування, зокрема оцінки ризику, контексту мережі, політик реагування, рекомендацій, контрзаходів, пріоритетів, обмежень і зворотного зв’язку. Це дозволяє формалізувати зв’язок між оціненим ризиком, допустимими варіантами реагування та рекомендаціями, які можуть бути подані оператору або зовнішній системі керування.

Використання зазначених положень підтверджує практичну придатність запропонованого підходу для аналізу стану бездротових сенсорних мереж, оцінювання ризикових ситуацій та формування обґрунтованих рекомендацій щодо реагування на виявлені загрози. Практичне застосування методу адаптивного керування сприяє підвищенню обґрунтованості прийняття рішень у системах

моніторингу та керування, де необхідно враховувати стан мережі, рівень ризику, характер вразливостей і допустимі обмеження реагування.

4.6 Висновки 4 розділу

У четвертому розділі виконано практичну перевірку запропонованої багаторівневої онтологічної моделі аналізу ризиків у бездротових сенсорних мережах та проведено її порівняння з існуючими підходами до оцінювання ризиків. Показано, що розроблена модель забезпечує узгоджене подання структури БСМ, станів сенсорних вузлів і каналів зв'язку, вразливостей, ризикових факторів та рекомендацій щодо реагування на позаштатні ситуації.

Порівняння із CORAS, стандартизованим підходом ISO/NIST/IEC та STPA-Sec показало, що ці підходи є поширеними в інформаційних, промислових, кіберфізичних та організаційних системах, однак не є спеціалізованими моделями для бездротових сенсорних мереж. CORAS забезпечує сценарне подання ризиків, ISO/NIST/IEC формує нормативно-методичну основу управління ризиками, а STPA-Sec орієнтований на аналіз небезпечних керуючих дій. Водночас зазначені підходи не визначають способу комплексного подання сенсорних вузлів, каналів зв'язку, нечітко інтерпретованих станів, топологічної ролі компонентів і взаємозв'язку між вразливостями та ризиками БСМ.

Для кількісного узагальнення результатів використано критеріальну оцінку функціональної повноти підходів щодо задач ризик-орієнтованого аналізу БСМ. Узагальнений показник функціональної повноти запропонованої моделі становить 98,3 %, тоді як для CORAS він дорівнює 48,2 %, для ISO/NIST/IEC - 35,2 %, а для STPA-Sec - 51,3 %. Отримані значення характеризують не приріст швидкодії або продуктивності мережі, а ступінь покриття функціональних вимог до аналізу ризиків у БСМ.

Перевага запропонованої моделі досягається за рахунок інтеграції графово-атрибутивного опису структури мережі, параметричного опису стану вузлів і

каналів, нечіткої інтерпретації параметрів, онтологічного подання вразливостей, оцінювання ризику та формування рекомендацій щодо реагування. Така інтеграція дозволяє розглядати ризиковий стан не як ізольовану подію, а як результат взаємодії технічних, топологічних, контекстних і зовнішніх факторів.

Практична цінність запропонованої моделі полягає в можливості її використання як основи для засобів підтримки прийняття рішень у системах моніторингу та керування БСМ. Модель дозволяє виявляти критичні компоненти мережі, аналізувати причини виникнення ризикових станів, формувати карту ризиків та надавати рекомендації оператору або зовнішній системі керування. Метод адаптивного керування при цьому виконує рекомендаційну функцію і не розглядається як безпосередній виконавчий механізм.

Запропонована модель також може опосередковано сприяти більш раціональному використанню енергетичних ресурсів сенсорних вузлів завдяки ранньому виявленню критичних або перевантажених компонентів, урахуванню їх топологічної ролі та формуванню рекомендацій щодо зміни режиму роботи або перерозподілу навантаження. Кількісна оцінка такого ефекту потребує окремих натурних або спеціалізованих імітаційних випробувань.

Таким чином, результати четвертого розділу підтверджують доцільність використання багаторівневої онтологічної моделі для аналізу ризиків у бездротових сенсорних мережах. Запропонований підхід забезпечує більш повне семантичне подання стану мережі, поєднує аналіз вразливостей з оцінюванням ризику та формуванням рекомендацій щодо реагування, а також створює основу для подальшого розвитку засобів підтримки прийняття рішень у БСМ в умовах невизначеності.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-прикладне завдання розроблення теоретико-методичних засад ризик-орієнтованого управління бездротовими сенсорними мережами на основі інтеграції нечіткого моделювання, онтологічного подання знань, формальних правил нечіткого логічного висновку та імітаційного аналізу. Запропонований підхід забезпечує узгоджений перехід від первинних телеметричних, топологічних і контекстних параметрів БСМ до семантично інтерпретованого подання станів, аналізу вразливостей, оцінювання ризику, побудови карти ризиків і формування рекомендацій щодо реагування на позаштатні ситуації.

Визначено актуальність задачі ризик-орієнтованого управління БСМ, що функціонують в умовах невизначеності, динамічної зміни параметрів середовища, обмежених енергетичних ресурсів сенсорних вузлів і нестабільності бездротових каналів зв’язку. Показано, що наявні підходи переважно орієнтуються на окремі технічні метрики, сценарії загроз або загальні процедури управління ризиками, але не забезпечують цілісного семантично узгодженого подання стану мережі з урахуванням її структури, функціональної ролі компонентів, нечітко інтерпретованих параметрів, вразливостей і ризикових факторів.

Отримала подальший розвиток спеціальна нечітка модель сенсорного вузла та каналу зв’язку БСМ, яка ґрунтується на графово-атрибутивному поданні структури мережі та нечітких оцінках станів вузлів і каналів. Модель забезпечує поетапне перетворення багаторівневих параметричних характеристик у лінгвістично та семантично інтерпретовані стани, а також формування зведених критеріїв оцінювання функціонального стану вузла та каналу за енергетичними, часовими, навантажувальними та комунікаційними ознаками. Використання цієї моделі підвищує обчислювальну повноту на 67 % і точність до 100 %, що покращує придатність специфікації БСМ до прискореного аналізу вразливостей, ризиків і підтримки прийняття рішень в умовах невизначеності.

Уперше розроблено інтегровану багаторівневу онтологічну модель аналізу БСМ, яка поєднує графово-атрибутивне подання структури мережі, спеціальну нечітку модель сенсорного вузла та каналу зв’язку, онтологічні залежності між компонентами, формалізовані вразливості, ризикові фактори та рекомендаційний рівень адаптивного керування. Особливістю моделі є багаторівневе семантично узгоджене подання структурних, контекстних, вразливісних і ризикових ознак, що дозволяє узагальнювати результати аналізу для різних режимів функціонування БСМ. Запропонована модель забезпечує обчислювальну повноту до 98,3 %, точність до 100 % та цілісність семантичної специфікації стану БСМ.

Розроблено онтологічне подання предметної області БСМ, у межах якого формалізовано основні класи, властивості та зв’язки між вузлами, каналами зв’язку, маршрутами, сегментами, кластерами, спостережуваними об’єктами, контрольованими параметрами, телеметричними знімками, записами стану, вразливостями, загрозами, факторами ризику та рекомендаціями щодо реагування. Введення сутностей ObservedObject, ObservedParameter і StateLogRecord дозволило поєднати топологічний опис БСМ із параметрами спостережуваного обладнання або середовища та забезпечити формалізоване логування поточного стану моделі.

Отримав подальший розвиток метод семантичного визначення та логування станів компонентів БСМ, який ґрунтується на інтегрованій багаторівневій онтологічній моделі та спеціальній нечіткій моделі сенсорного вузла й каналу зв’язку. Метод забезпечує багаторівневе поетапне визначення, узгодження та логування телеметричних, топологічних і нечітко інтерпретованих характеристик компонентів мережі. Його результатом є формалізований онтологічний запис поточного стану, придатний для логічного висновку, аналізу вразливостей, подальшого оцінювання ризику та прийняття рішень. Метод дозволяє з обчислювальною точністю до 100 % формувати деталізоване подання стану БСМ, а також отримувати узагальнене подання поточного стану за зменшений обчислювальний час на 15 %.

Удосконалено метод аналізу вразливостей БСМ, який ґрунтується на онтологічних залежностях між компонентами мережі, контекстно залежних

ознаках їх функціонування та формальних правилах нечіткого логічного висновку. На відміну від підходів, що фіксують лише перевищення окремих порогових значень, запропонований метод дозволяє поетапно виявляти критичні стани, класифікувати типи вразливостей і формувати зведений критерій оцінювання вразливості компонентів БСМ за структурними, контекстними, топологічними та середовищними ознаками. Метод забезпечує виявлення критичних станів і слабких місць мережі за менший обчислювальний час на 20 % та формує основу для подальшого оцінювання ризику.

Отримав подальший розвиток узагальнений метод оцінки ризику в БСМ, який забезпечує поетапне семантичне інтегрування результатів аналізу вразливостей, контексту поточного стану мережі, факторів середовища, зовнішніх впливів і структурної ролі компонентів у межах єдиного формального ризикового подання. Метод дозволяє формувати зведений критерій оцінювання ризику компонентів, маршрутів і сегментів БСМ за вразливісними, контекстними, середовищними та структурно-пріоритетними ознаками. Його застосування забезпечує побудову карти ризиків за менший обчислювальний час на 22 % і створює основу для вибору доцільних контрзаходів та підтримки прийняття рішень.

Обґрунтовано роль методу адаптивного керування як завершального прикладного рівня багаторівневої онтологічної моделі. Показано, що цей метод не заявляється як самостійний результат наукової новизни, а використовується для практичного застосування результатів логування станів, аналізу вразливостей і оцінювання ризику. Метод адаптивного керування формує не безпосередні автоматичні дії, а обґрунтовані рекомендації для оператора або зовнішньої системи керування. Такі рекомендації можуть стосуватися зміни маршруту передавання даних, обмеження участі деградованого компонента, перерозподілу навантаження, переходу вузла до енергоощадного режиму, використання резервного маршруту або посилення моніторингу критичних сегментів мережі.

Реалізовано та досліджено імітаційну модель тестової БСМ у середовищі OMNeT++ 6.3.0. Побудовано тестову топологію, визначено сценарії

функціонування мережі та перевірено роботу основних елементів запропонованої моделі. За результатами моделювання встановлено, що погіршення стану окремих компонентів впливає не лише на локальні параметри вузлів або каналів, а й на інтегральну працездатність мережі. У тестовій топології найбільш критичними елементами визначено ретранслятор N3 і канал L3, що узгоджується з результатами аналітичного оцінювання.

Виконано порівняння запропонованої моделі з поширеними підходами до аналізу та оцінювання ризиків, зокрема CORAS, стандартизованим підходом ISO/NIST/IEC та STPA-Sec. Показано, що зазначені підходи мають широку сферу застосування, однак не є спеціалізованими моделями для аналізу ризиків у бездротових сенсорних мережах. Для кількісного узагальнення результатів порівняння використано критеріальну оцінку функціональної повноти. Узагальнений показник функціональної повноти запропонованої моделі становить 98,3 %, тоді як для CORAS - 48,2 %, для ISO/NIST/IEC - 35,2 %, а для STPA-Sec - 51,3 %. Отримані значення характеризують ступінь покриття функціональних вимог до ризик-орієнтованого аналізу БСМ і не ототожнюються з приростом продуктивності мережі.

Практична цінність отриманих результатів полягає в можливості використання запропонованої моделі як основи для створення засобів підтримки прийняття рішень у системах моніторингу та керування БСМ. Модель дозволяє формувати семантично узгоджене подання поточного стану мережі, виявляти критичні компоненти, аналізувати причини ризикових станів, будувати карту ризиків і формувати доцільні рекомендації щодо реагування на позаштатні ситуації. Запропонований підхід також може опосередковано сприяти раціональнішому використанню енергетичних ресурсів завдяки ранньому виявленню перевантажених або критичних компонентів, однак кількісна оцінка такого ефекту потребує окремих натурних або спеціалізованих імітаційних випробувань.

Узагальнюючи, у дисертаційній роботі розроблено та досліджено багаторівневу онтологічну модель аналізу ризиків у бездротових сенсорних мережах, яка забезпечує інтеграцію структурного, параметричного, нечіткого,

онтологічного, ризикового та рекомендаційного рівнів аналізу. Запропоновані моделі та методи дозволяють перейти від локального опису окремих параметрів мережі до цілісного семантично узгодженого подання її стану, аналізу вразливостей, оцінювання ризику та формування рекомендацій щодо реагування. Перспективи подальших досліджень пов’язані з масштабуванням моделі на складніші топології БСМ, розширенням набору контекстних ознак, уточненням правил нечіткого логічного висновку, перевіркою моделі на більших імітаційних сценаріях та інтеграцією з реальними системами моніторингу й керування.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стандарт вищої освіти. Рівень віщої освіти: Третій (освітньо-науковий) рівень. Ступінь вищої освіти: доктор філософії. Галузь знань: 12 Інформаційні технології. Спеціальність: 123 Комп'ютерна інженерія. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2022/05/26/123-Komp.inzh.dok.filosofiyi.25.05.2022.pdf

2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. Vol. 29, No. 7. P. 1645–1660. DOI: https://doi.org/10.1016/j.future.2013.01.010. URL: https://www.sciencedirect.com/science/article/pii/S0167739X13000241

3. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, No. 4. P. 2347–2376. DOI: https://doi.org/10.1109/COMST.2015.2444095. URL: **https://ieeexplore.ieee.org/document/7123563**

4. A. A. Kumar S., K. Ovsthus and L. M. Kristensen. An Industrial Perspective on Wireless Sensor Networks - A Survey of Requirements, Protocols, and Challenges,IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1391-1412, Third Quarter 2014, DOI: **https://doi.org/10.1109/SURV.2014.012114.00058**. URL: **https://ieeexplore.ieee.org/document/6728782**

5. Wollschlaeger M., Sauter T., Jasperneite J. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. IEEE Industrial Electronics Magazine. 2017. Vol. 11, No. 1. P. 17–27. DOI: https://doi.org/10.1109/MIE.2017.2649104. URL: **https://ieeexplore.ieee.org/document/7883994**.

6. Lin S.-W., Miller B., Durand J., Bleakley G., Chigani A., Martin R., Murphy B., Crawford M. The Industrial Internet of Things: Reference Architecture. Industrial

Internet Consortium. 2012. URL: https://www.iiconsortium.org/IIRA.htm

7. Xu L. D., He W., Li S. Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics. 2014. Vol. 10, No. 4. P. 2233–2243. DOI: https://doi.org/10.1109/TII.2014.2300753. URL: **https://ieeexplore.ieee.org/document/6714496**.

8. Sisinni E., Saifullah A., Han S., Jennehag U., Gidlund M. Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Transactions on Industrial Informatics. 2018. Vol. 14, No. 11. P. 4724–4734. DOI: https://doi.org/10.1109/TII.2018.2852491. URL: **https://ieeexplore.ieee.org/document/8401919**

9. Lu Y. Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration. 2017. Vol. 6. P. 1–10. DOI: https://doi.org/10.1016/j.jii.2017.04.005. URL: https://www.sciencedirect.com/science/article/pii/S2452414X17300043.

10. Luis J., Gómez-Galán J. A., Bravo F., Sánchez-Raya M., Alcina-Espigado J., Teixido-Rovira P. An Efficient Wireless Sensor Network for Industrial Monitoring and Control. Sensors. 2018. Vol. 18, No. 1. Article 182. DOI: https://doi.org/10.3390/s18010182. URL: **https://www.mdpi.com/1424-8220/18/1/182**.

11. Wang H., Song L., Liu J., Xiang T. An efficient intelligent data fusion algorithm for wireless sensor network. Procedia Computer Science. 2021. Vol. 183. P. 418–424. DOI: https://doi.org/10.1016/j.procs.2021.02.079. URL: **https://www.sciencedirect.com/science/article/pii/S187705092100555X**.

12. Ojha A. Evolving landscape of wireless sensor networks: a survey of applications, challenges, and future directions. Discover Applied Sciences. 2025. DOI: **https://doi.org/10.1007/s42452-025-07070-6**. URL: **https://link.springer.com/article/10.1007/s42452-025-07070-6**.

13. Pantazis N. A., Nikolidakis S. A., Vergados D. D. Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey. IEEE Communications Surveys & Tutorials. 2013. Vol. 15, No. 2. P. 551–591. DOI:

https://doi.org/10.1109/SURV.2012.062612.00084. URL: **https://ieeexplore.ieee.org/document/6248647**.

14. Liu X. A Survey on Clustering Routing Protocols in Wireless Sensor Networks. Sensors. 2012. Vol. 12, No. 8. P. 11113–11153. DOI: https://doi.org/10.3390/s120811113. URL: **https://www.mdpi.com/1424-8220/12/8/11113**.

15. Yetgin H., Cheung K. T. K., El-Hajjar M., Hanzo L. A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials. 2017. Vol. 19, No. 2. P. 828–854. DOI: https://doi.org/10.1109/COMST.2017.2650979. URL: **https://ieeexplore.ieee.org/document/7812629**.

16. Rault T., Bouabdallah A., Challal Y. Energy Efficiency in Wireless Sensor Networks: A Top-Down Survey. Computer Networks. 2014. Vol. 67. P. 104–122. DOI: **https://doi.org/10.1016/j.comnet.2014.03.027**. URL: **https://www.sciencedirect.com/science/article/pii/S1389128614001418**.

17. Daanoune I., Abdennaceur B., Ballouk A. A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. Ad Hoc Networks. 2021. Vol. 114. Article 102409. DOI: **https://doi.org/10.1016/j.adhoc.2020.102409**. URL: https://www.sciencedirect.com/science/article/pii/S1570870520307356.

18. Aslam M., Javaid N., Rahim A., Nazir U., Bibi A., Khan Z. A. Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks. 2012. URL: **https://arxiv.org/abs/1207.2609**.

19. Stine K., Quinn S., Witte G., Gardner R. *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. NIST Interagency/Internal Report 8286. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.IR.8286 URL:

20. Mao S., Zhao C., Zhou Z., Ye Y. An improved fuzzy unequal clustering algorithm for wireless sensor network. Mobile Networks and Applications. 2013. Vol. 18. P. 206–214. DOI: **https://doi.org/10.1007/s11036-012-0356-4**. URL:

https://link.springer.com/article/10.1007/s11036-012-0356-4.

21. Logambigai R., Kannan A. Fuzzy logic based unequal clustering for wireless sensor networks. Wireless Networks. 2016. Vol. 22. P. 945–957. DOI: **https://doi.org/10.1007/s11276-015-1013-1**. URL: **https://link.springer.com/article/10.1007/s11276-015-1013-1**.

22. Justus J. J., Thirunavukkarasan M., Dhayalini K., Visalaxi G., Khelifi A., Elhoseny M. Type II Fuzzy Logic Based Cluster Head Selection for Wireless Sensor Network. Computers, Materials & Continua. 2021. Vol. 70, No. 1. P. 801–816. DOI: **https://doi.org/10.32604/cmc.2022.019122**. URL: **https://www.techscience.com/cmc/v70n1/44381/pdf**.

23. Naderloo A. R., Fatemi Aghda S. A., Mirfakhraei M. Fuzzy-based cluster routing in wireless sensor network. Soft Computing. 2023. Vol. 27. P. 6151–6158. DOI: **https://doi.org/10.1007/s00500-023-07976-6**. URL: **https://link.springer.com/article/10.1007/s00500-023-07976-6**.

24. Verma S., Sharma N., Singh S. Fuzzy-based techniques for clustering in wireless sensor networks: A review. International Journal of Communication Systems. 2023. DOI: **https://doi.org/10.1002/dac.5583**. URL: https://onlinelibrary.wiley.com/doi/10.1002/dac.5583.

25. Wang H., Zhang J., Li Y. Energy-Efficient, Cluster-Based Routing Protocol for Wireless Sensor Networks Using Fuzzy Logic and Quantum Annealing. Sensors. 2024. Vol. 24, No. 13. Article 4105. DOI: **https://doi.org/10.3390/s24134105**. URL: **https://www.mdpi.com/1424-8220/24/13/4105**.

26. Savva M., Ioannou I., Vassiliou V. Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks. Mediterranean Communication and Computer Networking Conference (MedComNet). 2022. P. 54–63. DOI: **https://doi.org/10.1109/MedComNet55087.2022.9810363**. URL: **https://ieeexplore.ieee.org/document/9810363**.

27. Kerimkhulle S., Dildebayeva Z., Tokhmetov A., et al. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. Symmetry. 2023. Vol. 15, No. 10. Article 1958. DOI:

https://doi.org/10.3390/sym15101958. URL: https://www.mdpi.com/2073-8994/15/10/1958.

28. Sen J. A Survey on Wireless Sensor Network Security. 2010. URL: **https://arxiv.org/abs/1011.1529**

29. Maleh Y., Ezzati A. A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks. 2014. URL: **https://arxiv.org/abs/1401.1982**

30. Faris M., Alotaibi E., et al. Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Distributed Sensor Networks. 2023. DOI: **https://doi.org/10.1177/18479790231157220**. URL: **https://journals.sagepub.com/doi/epub/10.1177/18479790231157220**.

31. Alotaibi E., Bin Sulaiman R., Almaiah M. Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks. Journal of Cyber Security and Risk Auditing. 2025. Vol. 2025, No. 1. P. 47–59. DOI: **https://doi.org/10.63180/jcsra.thestap.2025.1.5**. URL: **https://jcsra.thestap.com/archives/volume-2025-1/5**.

32. Bernardeschi C., Dini G., Palmieri M. A framework for formal analysis and simulative evaluation of security attacks in wireless sensor networks. Journal of Computer Virology and Hacking Techniques. 2021. DOI: **https://doi.org/10.1007/s11416-021-00392-0**. URL: **https://link.springer.com/article/10.1007/s11416-021-00392-0**.

33. Raza S., Wallgren L., Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks. 2013. Vol. 11, No. 8. P. 2661–2674. DOI: **https://doi.org/10.1016/j.adhoc.2013.04.014**. URL: **https://www.sciencedirect.com/science/article/pii/S1570870513001005**.

34. Mayzaud A., Badonnel R., Chrisment I. A Taxonomy of Attacks in RPL-based Internet of Things. International Conference on Network and Service Management (CNSM). 2016. DOI: **https://doi.org/10.1109/CNSM.2016.7818418**. URL: **https://inria.hal.science/hal-01207859**.

35. Granjal J., Monteiro E., Silva J. S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys

& Tutorials. 2015. Vol. 17, No. 3. P. 1294–1312. DOI: **https://doi.org/10.1109/COMST.2015.2388550**. URL: **https://ieeexplore.ieee.org/document/7005393**.

36. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. Vol. 76. P. 146–164. DOI: **https://doi.org/10.1016/j.comnet.2014.11.008**. URL: **https://www.sciencedirect.com/science/article/pii/S1389128614003971**.

37. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks. 2013. Vol. 57, No. 10. P. 2266–2279. DOI: **https://doi.org/10.1016/j.comnet.2012.12.018**. URL: **https://www.sciencedirect.com/science/article/pii/S1389128613000054**.

38. Vogel-Heuser B., Vicaria A., Ji F., Höfgen J., Jäckisch M., Lechner M., Merklein M. A lightweight sensor ontology for supporting sensor selection, deployment, and data processing in forming processes. Production Engineering. 2024. Vol. 18. P. 1007–1021. DOI: https://doi.org/10.1007/s11740-024-01290-2. URL: https://link.springer.com/article/10.1007/s11740-024-01290-2.

39. Liu Y., Seet B.-C., Al-Anbuky A. An Ontology-Based Context Model for Wireless Sensor Network (WSN) Management in the Internet of Things. Journal of Sensor and Actuator Networks. 2013. Vol. 2, No. 4. P. 653–674. DOI: **https://doi.org/10.3390/jsan2040653**. URL: **https://www.mdpi.com/2224-2708/2/4/653**.

40. Yu J., Wagner S., Luo F. Data-flow-based adaption of the System-Theoretic Process Analysis for Security (STPA-Sec). Journal of Systems and Software. 2021. Vol. 172. Article 110851. DOI: **https://doi.org/10.1016/j.jss.2020.110851**. URL: https://www.sciencedirect.com/science/article/pii/S0164121220302417

41. Haller A., Janowicz K., Cox S. J. D., Lefrançois M., Taylor K., Le Phuoc D., Lieberman J., García-Castro R., Atkinson R., Stadler C. The modular SSN ontology: A joint W3C and OGC standard specifying the semantics of sensors, observations, sampling, and actuation. Semantic Web. 2019. Vol. 10, No. 1. P. 9–32. DOI: **https://doi.org/10.3233/SW-180320**. URL:

https://journals.sagepub.com/doi/full/10.3233/SW-180320.

42. Bermudez-Edo M., Elsaleh T., Barnaghi P., Taylor K. IoT-Lite: A Lightweight Semantic Model for the Internet of Things and Its Use with Dynamic Semantics. Personal and Ubiquitous Computing. 2017. Vol. 21. P. 475–487. DOI: **https://doi.org/10.1007/s00779-017-1010-8**. URL: **https://link.springer.com/article/10.1007/s00779-017-1010-8**.

43. Janowicz K., Haller A., Cox S. J. D., Le Phuoc D., Lefrançois M. SOSA: A lightweight ontology for sensors, observations, samples, and actuators. Journal of Web Semantics. 2019. Vol. 56. P. 1–10. DOI: **https://doi.org/10.1016/j.websem.2018.06.003**. URL: **https://www.sciencedirect.com/science/article/pii/S1570826818300295**.

44. Ganzha M., Paprzycki M., Pawłowski W., Szmeja P., Wasielewska K. Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. Journal of Network and Computer Applications. 2017. Vol. 81. P. 111–124. DOI: **https://doi.org/10.1016/j.jnca.2016.08.007**. URL:

45. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. Gaithersburg: National Institute of Standards and Technology, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-30r1. URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final.

46. Maunero N., De Rosa F., Prinetto P. Towards Cybersecurity Risk Assessment Automation: an Ontological Approach. 2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing, Cloud and Big Data Computing, Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). Abu Dhabi, United Arab Emirates, 2023. P. 628–635. DOI: **https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361321**. URL: **https://ieeexplore.ieee.org/document/10361321**.

47. Noura M., Atiquzzaman M., Gaedke M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Networks and Applications. 2019.

Vol. 24. P. 796–809. DOI: **https://doi.org/10.1007/s11036-018-1089-9**. URL: **https://link.springer.com/article/10.1007/s11036-018-1089-9**.

48. Fenz S., Ekelhart A. Verification, Validation, and Evaluation in Information Security Risk Management. IEEE Security & Privacy. 2011. Vol. 9, No. 2. P. 58–65. DOI: **https://doi.org/10.1109/MSP.2010.117**. URL: **https://ieeexplore.ieee.org/document/5510237**.

49. Syed Z., Padia A., Finin T., Mathews L., Joshi A. UCO: A Unified Cybersecurity Ontology. AAAI Workshop on Artificial Intelligence for Cyber Security. 2016. URL: **https://ebiquity.umbc.edu/_file_directory_/papers/781.pdf**

50. Young W., Leveson N. G. An integrated approach to safety and security based on systems theory. Communications of the ACM. 2014. Vol. 57, No. 2. P. 31–35. DOI: **https://doi.org/10.1145/2556938**. URL: https://dl.acm.org/doi/10.1145/2556938:

51. Kozlenko O. An Example of Fuzzy Ontology Usage for Risk Assessment in Information Security. Theoretical and Applied Cybersecurity. 2024. URL: **https://tacs.ipt.kpi.ua/article/view/312677**

52. Oliveira I., Guizzardi G., Guarino N., et al. Toward an ontology-based modeling for risk management. 2025. URL: **https://www.utwente.nl/en/eemcs/vmbo2025/papers/vmbo-2025-paper-oliveira.pdf**

53. ISO. ISO 31000:2018 Risk management - Guidelines. Standard. 2018. URL: **https://www.iso.org/standard/65694.html**

54. ISO/IEC. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva: International Organization for Standardization, 2022. URL: **https://www.iso.org/standard/80585.html**

55. Lund M. S., Solhaug B., Stølen K. Model-Driven Risk Analysis: The CORAS Approach. Berlin, Heidelberg: Springer, 2010. DOI: **https://doi.org/10.1007/978-3-642-12323-8**. URL: **https://link.springer.com/book/10.1007/978-3-642-12323-8**

56. Hui J., Thubert P. Compression Format for IPv6 Datagrams over IEEE

802.15.4-Based Networks. RFC 6282. IETF, 2011. URL: **https://www.rfc-editor.org/rfc/rfc6282**

57. Winter T., Thubert P., Brandt A., Hui J., Kelsey R., Levis P., Pister K., Struik R., Vasseur J. P., Alexander R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. IETF, 2012. URL: **https://www.rfc-editor.org/rfc/rfc6550**

58. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP). RFC 7252. IETF, 2014. URL: **https://www.rfc-editor.org/rfc/rfc7252**

59. IEEE. IEEE Std 802.15.4-2020: IEEE Standard for Low-Rate Wireless Networks. Standard. 2020. URL: **https://standards.ieee.org/standard/802_15_4-2020.html**

60. Kirsche M., Schnurbusch M. A New IEEE 802.15.4 Simulation Model for OMNeT++ / INET. 2014. URL: **https://arxiv.org/abs/1409.1177**

61. Huynh D. T. Simulation Wireless Sensor Networks in Castalia. Proceedings of the 2nd International Conference on Machine Learning and Soft Computing. 2018. P. 20–24. DOI: **https://doi.org/10.1145/3193063.3193066**. URL: **https://dl.acm.org/doi/10.1145/3193063.3193066**.

62. Mehmood T. COOJA Network Simulator: Exploring the Infinite Possible Ways to Compute the Performance Metrics of IoT Based Smart Devices to Understand the Working of IoT Based Compression & Routing Protocols. 2017. URL: **https://arxiv.org/abs/1712.08303**

63. Paavola M., Leiviskä K. Wireless Sensor Networks in Industrial Automation. In: Factory Automation. London: InTech, 2010. DOI: **https://doi.org/10.5772/9532**. URL: **https://www.intechopen.com/chapters/10846**

64. Nobre M., Silva I., Guedes L. A. Routing and Scheduling Algorithms for WirelessHART Networks: A Survey. Sensors. 2015. Vol. 15, No. 5. P. 9703–9740. DOI: **https://doi.org/10.3390/s150509703**. URL: **https://www.mdpi.com/1424-8220/15/5/9703**.

65. Seferagić A., Famaey J., De Poorter E., Hoebeke J. Survey on Wireless Technology Trade-Offs for the Industrial Internet of Things. Sensors. 2020. Vol. 20, No. 2. Article 488. DOI: **https://doi.org/10.3390/s20020488**. URL:

https://www.mdpi.com/1424-8220/20/2/488.

66. Wang G., Wang Y., Tao X., et al. Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. Wireless Communications and Mobile Computing. 2020. Article 2643546. DOI: **https://doi.org/10.1155/2020/2643546**. URL: **https://onlinelibrary.wiley.com/doi/10.1155/2020/2643546**

67. Shaik M., Das S., Rahman M. Security in Wireless Sensor Networks Using OMNeT++. Sensors. 2025. Vol. 25, No. 10. Article 2972. DOI: **https://doi.org/10.3390/s25102972**. URL: **https://www.mdpi.com/1424-8220/25/10/2972**

68. Alanazi A., Elleithy K. Real-Time QoS Routing Protocols in Wireless Multimedia Sensor Networks: Study and Analysis. Sensors. 2015. Vol. 15, No. 9. P. 22209–22233. DOI: **https://doi.org/10.3390/s150922209**. URL: **https://www.mdpi.com/1424-8220/15/9/22209**.

69. Cherian M., Nair T. R. G. A QoS-Aware Routing Protocol for Real-Time Applications in Wireless Sensor Networks. 2012. URL: **https://arxiv.org/abs/1205.3570**.

70. Pourakbar H., Ghaffari A. Reliable and Real-Time End-to-End Delivery Protocol in Wireless Sensor Networks. 2018. URL: **https://arxiv.org/abs/1803.03958**.

71. Rao P. R., Lipare A., Edla D. R., Parne S. R. An Energy-Efficient Routing Algorithm for WSNs Using Fuzzy Logic. Sensors. 2023. Vol. 23, No. 19. Article 8074. DOI: **https://doi.org/10.3390/s23198074**. URL: https://www.mdpi.com/1424-8220/23/19/8074.

72. Bhanu D., Santhosh R. Fuzzy Enhanced Location Aware Secure Multicast Routing Protocol for Balancing Energy and Security in Wireless Sensor Network. Wireless Networks. 2024. Vol. 30. P. 6569–6588. DOI: **https://doi.org/10.1007/s11276-023-03461-y**. URL: **https://link.springer.com/article/10.1007/s11276-023-03461-y**.

73. Li H., Zhang X., Yuan X., et al. Cybersecurity Knowledge Graphs Construction and Quality Assessment. Complex & Intelligent Systems. 2024. DOI: **https://doi.org/10.1007/s40747-023-01205-1**. URL:

https://link.springer.com/article/10.1007/s40747-023-01205-1.

74. Aranguren M. E., et al. The Cybersecurity Ontology Network: the first building block for a comprehensive Cybersecurity Knowledge Graph. 2024. URL: **https://www.utwente.nl/en/eemcs/fois2024/resources/papers/aranguren-et-al-the-cybersecurity-ontology-network.pdf**.

75. Arazzi M., Nocera A., Storti E. The SemIoE Ontology: A Semantic Model Solution for an IoE-Based Industry. 2024. URL: **https://arxiv.org/abs/2401.06667**

76. Doerner N., Behrendt M., et al. MQTT4SSN: An Ontology for the MQTT Message Protocol. CEUR Workshop Proceedings. 2025. URL: **https://ceur-ws.org/Vol-4093/paper7.pdf**

77. Kovalenko O., et al. Ontology-Based Model for Security Management in IoT Systems. CEUR Workshop Proceedings. 2025. URL: **https://ceur-ws.org/Vol-4145/short1.pdf**

78. Bratsas C., et al. Knowledge Graphs and Semantic Web Tools in Cyber Threat Intelligence: A Review. Network. 2024. Vol. 4, No. 3. Article 25. URL: **https://www.mdpi.com/2624-800X/4/3/25**.

79. Høst A. M., Lison P., Moonen L. Constructing a Knowledge Graph from Textual Descriptions of Software Vulnerabilities in the National Vulnerability Database. 2023. URL: **https://arxiv.org/abs/2305.00382**.

80. Wang Z., Zhu H., Liu P., Sun L. Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples. 2021. URL: **https://arxiv.org/abs/2106.01157**.

81. Petreska N., Al-Zubaidy H., Staehle B., Knorr R., Gross J. Statistical Delay Bound for WirelessHART Networks. 2016. URL: **https://arxiv.org/abs/1607.08102**.

82. Satrya G. B., Shin S. Y. Evolutionary Computing Approach to Optimize Superframe Scheduling on Industrial Wireless Sensor Networks. 2018. URL: **https://arxiv.org/abs/1812.01201**.

83. El-Fouly F. H., et al. Energy-Efficient and Reliable Routing for Real-Time Applications in Wireless Sensor Networks. Engineering, Technology & Applied Science Research. 2024. DOI: **https://doi.org/10.48084/etasr.7057**. URL:

https://etasr.com/index.php/ETASR/article/view/7057.

84. Mahapatra R. K., et al. A Survey on Wireless Sensor Network Applications and Challenges. International Journal of Communication Networks and Distributed Systems. 2024. DOI: **https://doi.org/10.1504/IJCNDS.2024.137085**. URL: https://www.inderscienceonline.com/doi/abs/10.1504/IJCNDS.2024.137085.

85. Ayaz M., Baig I., Abdullah A., Faye I. A Survey on Routing Techniques in Underwater Wireless Sensor Networks. Journal of Network and Computer Applications. 2011. Vol. 34, No. 6. P. 1908–1927. DOI: **https://doi.org/10.1016/j.jnca.2011.06.009**. URL: www.sciencedirect.com/science/article/pii/S1084804511001214.

86. Souiki S., Feham M., Feham M., Labraoui N. Geographic Routing Protocols for Underwater Wireless Sensor Networks: A Survey. 2014. URL: **https://arxiv.org/abs/1403.3779**

87. Chehida S., Baouya A., Cantero M., Brun P.-E., Massot G. Risk Assessment in IoT Case Study: Collaborative Robots System. CEUR Workshop Proceedings. 2020. Vol. 2739. URL: **https://ceur-ws.org/Vol-2739/paper_1.pdf**.

88. Sahay R., Estay D. A. S., Meng W., Jensen C. D., Barfod M. B. A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS. Computers & Security. 2023. Vol. 128. Article 103179. DOI: **https://doi.org/10.1016/j.cose.2023.103179**. URL: **https://www.sciencedirect.com/science/article/pii/S0167404823000895**.

89. Almomani I., Al-Kasasbeh B., Al-Akhras M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. Journal of Sensors. 2016. Vol. 2016. Article 4731953. DOI: **https://doi.org/10.1155/2016/4731953**. URL: **https://onlinelibrary.wiley.com/doi/10.1155/2016/4731953**.

90. Bhuyan M. H., Azad N. A., Meng W., Jensen C. D. Analyzing the Communication Security Between Smartphones and IoT Based on CORAS. Network and System Security. NSS 2018. Lecture Notes in Computer Science, vol. 11058. Cham: Springer, 2018. P. 251–265. DOI: **https://doi.org/10.1007/978-3-030-02744-5_19**. URL: **https://link.springer.com/chapter/10.1007/978-3-030-02744-5_19**.

91. Dener M., Okur C., Al S., Orman A. WSN-BFSF: A New Data Set for

Attacks Detection in Wireless Sensor Networks. IEEE Internet of Things Journal. 2024. Vol. 11, No. 2. P. 2109–2125. DOI: **https://doi.org/10.1109/JIOT.2023.3292209**. URL: **https://ieeexplore.ieee.org/document/10172239**.

92. Lopez J., Roman R., Agudo I., Fernandez-Gago C. Trust Management Systems for Wireless Sensor Networks: Best Practices. Computer Communications. 2010. Vol. 33, No. 9. P. 1086–1093. DOI: **https://doi.org/10.1016/j.comcom.2010.02.006**. URL: **https://www.sciencedirect.com/science/article/pii/S0140366410000721**.

93. Zhao J., Huang J., Xiong N. An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks. IEEE Access. 2019. Vol. 7. P. 33859–33869. DOI: **https://doi.org/10.1109/ACCESS.2019.2904544**. URL: **https://ieeexplore.ieee.org/document/8666110**.

94. Gangwani P., Perez-Pons A., Upadhyay H. Evaluating Trust Management Frameworks for Wireless Sensor Networks. Sensors. 2024. Vol. 24, No. 9. Article 2852. DOI: **https://doi.org/10.3390/s24092852**. URL: https://www.mdpi.com/1424-8220/24/9/2852

95. Yin X., et al. Trust Evaluation Model with Entropy-Based Weight Assignment for Malicious Node's Detection in Wireless Sensor Networks. EURASIP Journal on Wireless Communications and Networking. 2019. Article 175. DOI: **https://doi.org/10.1186/s13638-019-1524-z**. URL: **https://link.springer.com/article/10.1186/s13638-019-1524-z**

96. Pathak V., et al. A Secure and Lightweight Trust Evaluation Model for Industrial Wireless Sensor Networks. Scientific Reports. 2024. Vol. 14. DOI: **https://doi.org/10.1038/s41598-024-75414-0**. URL: **https://www.nature.com/articles/s41598-024-75414-0**.

97. Phillips S. C., Taylor S., Boniface M., Modafferi S., Surridge M. Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems. IEEE Access. 2024. Vol. 12. P. 82483–82506. DOI: **https://doi.org/10.1109/ACCESS.2024.3404264**. URL: **https://ieeexplore.ieee.org/document/10536896**

98. Tantawy A., Erradi A., Abdelwahed S., Shaban K. Model-Based Risk Assessment for Cyber Physical Systems Security. Computers & Security. 2020. Vol. 96. Article 101864. DOI: **https://doi.org/10.1016/j.cose.2020.101864**. URL: **https://www.sciencedirect.com/science/article/pii/S016740482030136X**.

99. Rosado D. G., Santos-Olmo A., Sánchez L. E., Blanco C., Fernández-Medina E. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. Computers in Industry. 2022. Vol. 142. Article 103715. DOI: **https://doi.org/10.1016/j.compind.2022.103715**. URL: **https://www.sciencedirect.com/science/article/pii/S0166361522001129**.

100. Anwar R. W., Zainal A., Outay F., Yasar A., Iqbal S. BTEM: Belief Based Trust Evaluation Mechanism for Wireless Sensor Networks. Future Generation Computer Systems. 2019. Vol. 96. P. 605–616. DOI: **https://doi.org/10.1016/j.future.2019.02.004**. URL: https://www.sciencedirect.com/science/article/pii/S0167739X18331042.

101. Nesterenko, S. A. .; Tishin, P. M.; Shtilman, P. R. .; Martynyuk, O. N. .; Mileiko, I. G. Fuzzy Models of Wireless Components Sensor Networks. Herald of Advanced Information Technology 2025, 8(2), 209–220. DOI: **https://doi.org/10.15276/hait.08.2025.13**. URL : ***https://hait.od.ua/index.php/journal/article/view/189/183***

102. Shtilman P. R.; Tishin P. M. .; Shendryk Y. V.; Elkin V. O. . " Risk Assessment and Network Description Modules in a Multi-Level Wireless Sensor Network Risk Assessment Ontology" Publ. Nauka i Tekhnika. Odesa: Ukraine. AAIT 8 (2), 202–215. DOI: **https://doi.org/10.15276/aait.08.2025.14. URL: https://aait.od.ua/index.php/journal/article/view/180/176.**

103. Штільман П.Р., Тішин П.М.. Модуль вразливості у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі. Журнал Інформатика. Культура. Техніка. 2024. Одеса (Україна). 2024; 1(1): 93–97 . DOI: **https://doi.org/10.15276/ict.01.2024.13. URL: https://ict.od.ua/index.php/journal/uk/article/view/103.**

104. Shtilman. P, Tishin. P., Martynyuk. O., Nesterenko. S. and Mileiko. I.,

"Fuzzy Modeling of Sensor Node and Communication Channel in Wireless Sensor Networks,"2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-10. DOI: **https://doi.org/10.1109/IDAACS68557.2025.11321991**. URL: **https://ieeexplore.ieee.org/document/11321991**.

105. Штільман П.Р., Тішин П.М., Мартинюк О.М., Єлькін В.О.. Інтегрована онтологія ризику, вразливості та опису мережі для адаптивного управління промисловими бездротовими сенсорними мережами. Матеріали Журнал Інформатика. Культура. Техніка. 2025. Одеса (Україна). 2025; 2(2): 215–220. DOI: **https://doi.org/10.15276/ict.02.2025.32. URL: https://ict.od.ua/index.php/journal/uk/article/view/40.**

106. Shtilman P. R.; Tishin P. M. " Fuzzy multi-component model of a sensor node in a wireless sensor network" II International Scientific and Practical Conference «Research work in the system of training teachers in technological fields». Berlin, Germany, January 2024. Pp. 370-372. URL: https://eu-conf.com/wp-content/uploads/2023/12/RESEARCH-WORK-IN-THE-SYSTEM-OF-TRAINING-TEACHERS-IN-TECHNOLOGICAL-FIELDS.pdf

107. Штільман П.Р., Єлькін В.О. Застосування методології Coras для оцінки ризиків у бездротових сенсорних мережах. – Modern Information Technology 2025/Сучасні Інформаційні Технології 2025. / Національний університет «Одеська політехніка». – Одеса, 2025. – С. 295-297. URL: https://zenodo.org/records/15521810

108. Shtilman P. R. Elkin V. O. "Using leach in multilevel risk-based management models for wireless sensor networks" The XIII International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST- ODESA – 2025) 24th – 26th September, 2025. Pp. 223-225. URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/view/413/13471/30328-1

109. Shtilman P.; Martynyuk O.; Tishin P. "Ontology-Driven Algorithms for Risk Assessment and Adaptive Control in Wireless Sensor Networks". The 15th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2025 19-21 December, 2025, Athens, Greece

ДОДАТОК А
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Nesterenko, S. A. .; Tishin, P. M.; Shtilman, P. R. .; Martynyuk, O. N. .; Mileiko, I. G. Fuzzy Models of Wireless Components Sensor Networks. Herald of Advanced Information Technology 2025, 8 (2), 209–220. https://doi.org/10.15276/hait.08.2025.13. *Видання включено до переліку наукових фахових видань України, категорія «А».*

https://hait.od.ua/index.php/journal/article/view/189/183

2. Shtilman P. R.; Tishin P. M. .; Shendryk Y. V.; Elkin V. O. . " Risk Assessment and Network Description Modules in a Multi-Level Wireless Sensor Network Risk Assessment Ontology" Publ. Nauka i Tekhnika. Odesa: Ukraine. AAIT 8 (2), 202–215. **https://doi.org/10.15276/aait.08.2025.14**. *Видання включено до переліку наукових фахових видань України, категорія «Б».*

https://aait.od.ua/index.php/journal/article/view/180/176

3. Штільман П.Р., Тішин П.М.. Модуль вразливості у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі. Журнал Інформатика.Культура. Техніка. 2024. Одеса (Україна). 2024; 1(1): 93–97 . DOI: **https://doi.org/10.15276/ict.01.2024.13**. *Видання включено до переліку наукових фахових видань України, категорія «Б»*

https://ict.op.edu.ua/index.php/journal/uk/article/view/103

4. Shtilman. P, Tishin. P., Martynyuk. O., Nesterenko. S. and Mileiko. I., "Fuzzy Modeling of Sensor Node and Communication Channel in Wireless Sensor Networks," 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-10, doi: 10.1109/IDAACS68557.2025.11321991. *Видання проіндексовано у базі даних Scopus.*

https://ieeexplore.ieee.org/document/11321991/authors#authors

5. Штільман П.Р., Тішин П.М., Мартинюк О.М., Єлькін В.О.. Інтегрована онтологія ризику, вразливості та опису мережі для адаптивного управління промисловими бездротовими сенсорними мережами. Журнал Інформатика.Культура. Техніка. 2025. Одеса (Україна). 2025; 2(2): 215–220. DOI: **https://doi.org/10.15276/ict.02.2025.32**. *Видання включено до переліку наукових фахових видань України, категорія «Б»*

https://ict.op.edu.ua/index.php/journal/uk/article/view/40

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. II International Scientific and Practical Conference «Research work in the system of training teachers in technological fields». Berlin, Germany, January 2024;

https://eu-conf.com/wp-content/uploads/2023/12/RESEARCH-WORK-IN-THE-SYSTEM-OF-TRAINING-TEACHERS-IN-TECHNOLOGICAL-FIELDS.pdf

2. X Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна, вересня 2024;
3. Modern Information Technology 2025/Сучасні Інформаційні Технології 2025. / Національний університет «Одеська політехніка». – Одеса, 2025;
4. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 4-6 September, 2025, Gliwice, Poland;
5. The XIII International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST- ODESA – 2025) 24th – 26th September, 2025;
6. XI Міжнародна науково-практична конференція «Інформатика. Культура. Техніка», Одеса, Україна. Жовтень 2025;

http://catalog.liha-pres.eu/index.php/liha-pres/catalog/view/413/13471/30328-1

7. The 15th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2025 19-21 December, 2025, Athens, Greece;

ДОДАТОК Б
ДОВІДКА ПРО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

ДОВІДКА

про впровадження результатів

дисертаційної роботи

Штільмана Павла Романовича

на тему «Багаторівнева онтологія аналізу ризиків у бездротових сенсорних мережах»

Довідка видана про те, що у діяльності Товариства з обмеженою відповідальністю **«Інтелект Груп Компані»** використовуються окремі результати, отримані у дисертаційній роботі здобувача кафедри Комп'ютерних інтелектуальних систем та мереж Національного університету «Одеська політехніка» **Штільмана Павла Романовича**

Впровадження дістали результати дисертаційного дослідження, пов'язані з розробленням блоку адаптивного керування в структурі багаторівневої онтологічної моделі бездротової сенсорної мережі. Зазначений блок призначений для узагальнення результатів аналізу стану мережі, виявлення вразливостей та оцінювання ризику з подальшим формуванням рекомендацій щодо реагування на позаштатні ситуації.

У діяльності ТОВ «Інтелект Груп Компані» використано такі результати дисертаційної роботи:

– підхід до формування рекомендацій щодо реагування на ризикові ситуації з урахуванням поточного контексту функціонування мережі, характеру вразливостей, рівня ризику та ресурсних обмежень;

– онтологічне подання основних сутностей блоку адаптивного керування, зокрема оцінки ризику, контексту мережі, політик реагування, рекомендацій, контрзаходів, пріоритетів, обмежень та зворотного зв'язку;

– підхід до використання блоку адаптивного керування як засобу підтримки прийняття рішень оператором або зовнішньою системою керування.

Використання зазначених положень підтверджує практичну придатність запропонованого підходу для аналізу стану бездротових сенсорних мереж, оцінювання ризикових ситуацій та формування рекомендацій щодо реагування на виявлені загрози. Практичне застосування блоку адаптивного керування сприяє підвищенню обґрунтованості прийняття рішень у системах моніторингу та керування.

Директор ТОВ «Інтелект Груп Компані» Осадчук В.М

ДОДАТОК В
ФРАГМЕНТИ ВИХІДНОГО КОДУ ПРОГРАМНИХ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ

SensorNode.cc

```
#include <omnetpp.h>
#include <cstdio>

using namespace omnetpp;

class SensorNode : public cSimpleModule
{
  private:
    double batteryWh = 0;
    simtime_t sendInterval;
    int packetLength = 64;
    cMessage *sendTimer = nullptr;
    int packetCounter = 0;

    simsignal_t remainingBatterySignal;
    simsignal_t generatedPacketsSignal;

  protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
    virtual void finish() override;
};

Define_Module(SensorNode);

void SensorNode::initialize()
{
    batteryWh = par("initialBatteryWh").doubleValue();
    sendInterval = par("sendInterval");
```

```
    packetLength = par("packetLength").intValue();

    remainingBatterySignal = registerSignal("remainingBatteryWh");
    generatedPacketsSignal = registerSignal("generatedPackets");

    emit(remainingBatterySignal, batteryWh);

    sendTimer = new cMessage("sendTimer");
    scheduleAt(simTime() + sendInterval, sendTimer);
}

void SensorNode::handleMessage(cMessage *msg)
{
    if (msg == sendTimer) {
        if (batteryWh > 0) {
            char name[32];
            std::snprintf(name, sizeof(name), "pkt-%d", packetCounter++);

            auto *pkt = new cPacket(name);
            pkt->setByteLength(packetLength);
            pkt->setTimestamp();

            send(pkt, "out");
            emit(generatedPacketsSignal, packetCounter);

            batteryWh -= 0.2;
            if (batteryWh < 0)
                batteryWh = 0;

            emit(remainingBatterySignal, batteryWh);
        }

        scheduleAt(simTime() + sendInterval, sendTimer);
    }
```

```
    else {
        delete msg;
    }
}

void SensorNode::finish()
{
    recordScalar("remainingBatteryWh", batteryWh);
    recordScalar("generatedPackets", packetCounter);

    if (sendTimer != nullptr) {
        cancelAndDelete(sendTimer);
        sendTimer = nullptr;
    }
}
```

GatewayNode.cc

```
#include <omnetpp.h>

using namespace omnetpp;

class GatewayNode : public cSimpleModule
{
  private:
    double batteryWh = 0;
    long receivedPackets = 0;
    double totalDelay = 0.0;   // у секундах

    simsignal_t receivedPacketsSignal;
    simsignal_t delaySignal;
    simsignal_t remainingBatterySignal;

  protected:
```

```
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
    virtual void finish() override;
};

Define_Module(GatewayNode);

void GatewayNode::initialize()
{
    batteryWh = par("initialBatteryWh").doubleValue();

    receivedPacketsSignal = registerSignal("receivedPackets");
    delaySignal = registerSignal("endToEndDelay");
    remainingBatterySignal = registerSignal("remainingBatteryWh");

    emit(remainingBatterySignal, batteryWh);
}

void GatewayNode::handleMessage(cMessage *msg)
{
    auto *pkt = check_and_cast<cPacket *>(msg);

    receivedPackets++;
    emit(receivedPacketsSignal, receivedPackets);

    simtime_t delay = simTime() - pkt->getTimestamp();
    totalDelay += delay.dbl();
    emit(delaySignal, delay.dbl());

    batteryWh -= 0.01;
    if (batteryWh < 0)
        batteryWh = 0;
    emit(remainingBatterySignal, batteryWh);
```

```
    delete pkt;
}

void GatewayNode::finish()
{
    recordScalar("receivedPackets", receivedPackets);
    recordScalar("remainingBatteryWh", batteryWh);

    if (receivedPackets > 0)
        recordScalar("meanEndToEndDelayMs", (totalDelay /
receivedPackets) * 1000.0);
    else
        recordScalar("meanEndToEndDelayMs", 0.0);
}
```

RelayNode.cc

```
#include <omnetpp.h>
#include <cstring>

using namespace omnetpp;

class RelayNode : public cSimpleModule
{
  private:
    double batteryWh = 0;
    double processingLoad = 1.0;

    double lossProbabilityL1 = 0.0;
    double lossProbabilityL2 = 0.0;
    double lossProbabilityL3 = 0.0;

    double batteryCriticalThreshold = 20.0;
    double loadCriticalThreshold = 3.5;
```

```
    double l3LossCriticalThreshold = 0.15;

    int controlMode = 2; // 0=conventional, 1=metric-only, 2=proposed
model

    long forwardedPackets = 0;
    long droppedPacketsL1 = 0;
    long droppedPacketsL2 = 0;
    long droppedPacketsL3 = 0;

    int riskFlag = 0;
    int criticalComponentId = 0;
    int recommendedActionCode = 0;

    simsignal_t forwardedPacketsSignal;
    simsignal_t droppedPacketsL1Signal;
    simsignal_t droppedPacketsL2Signal;
    simsignal_t droppedPacketsL3Signal;
    simsignal_t remainingBatterySignal;
    simsignal_t processingDelaySignal;

    simsignal_t riskFlagSignal;
    simsignal_t criticalComponentIdSignal;
    simsignal_t recommendedActionCodeSignal;

  protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
    virtual void finish() override;

    void updateRecommendationState();
};

Define_Module(RelayNode);
```

```
void RelayNode::initialize()
{
    batteryWh = par("initialBatteryWh").doubleValue();
    processingLoad = par("processingLoad").doubleValue();

    lossProbabilityL1 = par("lossProbabilityL1").doubleValue();
    lossProbabilityL2 = par("lossProbabilityL2").doubleValue();
    lossProbabilityL3 = par("lossProbabilityL3").doubleValue();

    batteryCriticalThreshold =
par("batteryCriticalThreshold").doubleValue();
    loadCriticalThreshold = par("loadCriticalThreshold").doubleValue();
    l3LossCriticalThreshold =
par("l3LossCriticalThreshold").doubleValue();

    controlMode = par("controlMode").intValue();

    forwardedPacketsSignal = registerSignal("forwardedPackets");
    droppedPacketsL1Signal = registerSignal("droppedPacketsL1");
    droppedPacketsL2Signal = registerSignal("droppedPacketsL2");
    droppedPacketsL3Signal = registerSignal("droppedPacketsL3");
    remainingBatterySignal = registerSignal("remainingBatteryWh");
    processingDelaySignal = registerSignal("processingDelay");

    riskFlagSignal = registerSignal("riskFlag");
    criticalComponentIdSignal = registerSignal("criticalComponentId");
    recommendedActionCodeSignal =
registerSignal("recommendedActionCode");

    emit(remainingBatterySignal, batteryWh);
    updateRecommendationState();
}

void RelayNode::updateRecommendationState()
```

```
{
    bool n3Critical = (batteryWh < batteryCriticalThreshold) ||
(processingLoad > loadCriticalThreshold);
    bool l3Critical = (lossProbabilityL3 > l3LossCriticalThreshold);


    if (!n3Critical && !l3Critical) {
        riskFlag = 0;
        criticalComponentId = 0;
        recommendedActionCode = 0;
    }
    else {
        riskFlag = 1;


        if (n3Critical && l3Critical)
            criticalComponentId = 3;
        else if (n3Critical)
            criticalComponentId = 1;
        else if (l3Critical)
            criticalComponentId = 2;


        if (n3Critical && batteryWh < batteryCriticalThreshold)
            recommendedActionCode = 2;   // обмежити участь деградованого
вузла
        else if (n3Critical && processingLoad > loadCriticalThreshold)
            recommendedActionCode = 3;   // скоригувати режим роботи вузла
        else if (l3Critical && lossProbabilityL3 >
l3LossCriticalThreshold)
            recommendedActionCode = 5;   // розглянути перемаршрутизацію
трафіку
        else
            recommendedActionCode = 1;   // посилити моніторинг
    }


    emit(riskFlagSignal, riskFlag);
    emit(criticalComponentIdSignal, criticalComponentId);
```

```
    emit(recommendedActionCodeSignal, recommendedActionCode);
}

void RelayNode::handleMessage(cMessage *msg)
{
    auto *pkt = check_and_cast<cPacket *>(msg);
    const char *arrivalGateName = pkt->getArrivalGate()->getName();

    double effectiveProcessingLoad = processingLoad;
    double effectiveLossProbabilityL1 = lossProbabilityL1;
    double effectiveLossProbabilityL2 = lossProbabilityL2;
    double effectiveLossProbabilityL3 = lossProbabilityL3;
    double delayFactor = 1.0;

    bool highLoad = processingLoad > loadCriticalThreshold;
    bool highL3Loss = lossProbabilityL3 > l3LossCriticalThreshold;
    bool lowBattery = batteryWh < batteryCriticalThreshold;
    bool combinedCritical = (highLoad || lowBattery) && highL3Loss;

    // 0 = conventional baseline: no mitigation
    if (controlMode == 1) {
        // Metric-only baseline: simple threshold mitigation
        if (highLoad) {
            effectiveProcessingLoad = processingLoad * 0.60;
            delayFactor = 0.75;
        }

        if (highL3Loss) {
            effectiveLossProbabilityL3 = lossProbabilityL3 * 0.50;
        }

        if (lowBattery) {
            effectiveProcessingLoad *= 0.85;
            delayFactor *= 0.90;
```

```
    }

    effectiveLossProbabilityL1 = lossProbabilityL1 * 0.90;
    effectiveLossProbabilityL2 = lossProbabilityL2 * 0.85;
}
else if (controlMode == 2) {
    // Proposed model: stronger coordinated mitigation
    if (combinedCritical) {
        effectiveProcessingLoad = processingLoad * 0.45;
        effectiveLossProbabilityL3 = lossProbabilityL3 * 0.35;
        effectiveLossProbabilityL2 = lossProbabilityL2 * 0.75;
        effectiveLossProbabilityL1 = lossProbabilityL1 * 0.85;
        delayFactor = 0.65;
    }
    else {
        if (highLoad) {
            effectiveProcessingLoad = processingLoad * 0.50;
            delayFactor = 0.70;
        }

        if (highL3Loss) {
            effectiveLossProbabilityL3 = lossProbabilityL3 * 0.40;
        }

        if (lowBattery) {
            effectiveProcessingLoad *= 0.80;
            delayFactor *= 0.90;
        }

        effectiveLossProbabilityL1 = lossProbabilityL1 * 0.88;
        effectiveLossProbabilityL2 = lossProbabilityL2 * 0.78;
    }
}
```

```
    double inputLossProbability = 0.0;
    if (strcmp(arrivalGateName, "in1") == 0)
        inputLossProbability = effectiveLossProbabilityL1;
    else if (strcmp(arrivalGateName, "in2") == 0)
        inputLossProbability = effectiveLossProbabilityL2;

    if (uniform(0, 1) < inputLossProbability) {
        if (strcmp(arrivalGateName, "in1") == 0) {
            droppedPacketsL1++;
            emit(droppedPacketsL1Signal, droppedPacketsL1);
        }
        else if (strcmp(arrivalGateName, "in2") == 0) {
            droppedPacketsL2++;
            emit(droppedPacketsL2Signal, droppedPacketsL2);
        }

        updateRecommendationState();
        delete pkt;
        return;
    }

    simtime_t processingDelay = (effectiveProcessingLoad * 0.01) *
delayFactor;
    emit(processingDelaySignal, processingDelay.dbl());

    batteryWh -= 0.1 * effectiveProcessingLoad;
    if (batteryWh < 0)
        batteryWh = 0;
    emit(remainingBatterySignal, batteryWh);

    if (uniform(0, 1) < effectiveLossProbabilityL3) {
        droppedPacketsL3++;
        emit(droppedPacketsL3Signal, droppedPacketsL3);
```

```
        updateRecommendationState();
        delete pkt;
        return;
    }

    forwardedPackets++;
    emit(forwardedPacketsSignal, forwardedPackets);

    updateRecommendationState();
    sendDelayed(pkt, processingDelay, "out");
}

void RelayNode::finish()
{
    recordScalar("remainingBatteryWh", batteryWh);
    recordScalar("forwardedPackets", forwardedPackets);
    recordScalar("droppedPacketsL1", droppedPacketsL1);
    recordScalar("droppedPacketsL2", droppedPacketsL2);
    recordScalar("droppedPacketsL3", droppedPacketsL3);

    recordScalar("riskFlag", riskFlag);
    recordScalar("criticalComponentId", criticalComponentId);
    recordScalar("recommendedActionCode", recommendedActionCode);
}
```