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