DOI: https://doi.org/10.15276/ict.02.2025.32
УДК 004.7:004.056.5:004.89(045)

Інтегрована онтологія ризику, вразливості та опису мережі для адаптивного управління промисловими бездротовими сенсорними мережами

Штільман Павло Романович[1)]
Аспірнат каф. Комп'ютерні інтелектуальні системи та мережи
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com
Тішин Петро Метталинович[1)]
Канд. фіз.-матем. наук, доцент каф. Комп'ютерних інтелектуальних систем та мереж
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com
Мартинюк Олександр Миколайович[1)]
Канд. техніч. наук, доцент, завідувач каф. Комп'ютерні інтелектуальні системи та мережи
ORCID: https://orcid.org/0000-0003-1461-2000; martynyuk@op.edu.ua
Єлькін Віталій Олександрович[1)]
Аспірнат каф. Комп'ютерні інтелектуальні системи та мережи
ORCID: https://orcid.org/0009-0002-4202-7802; goodideacrew@gmail.com
[1)] Національний університет"Одеська політехніка", пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

У роботі представлено інтегровану онтологічну модель управління ризиками в бездротових сенсорних мережах (БСМ) промислового призначення, що поєднує три взаємопов'язані модулі: опису мережі, оцінки ризиків та вразливості. На відміну від попередніх рішень, кожен із яких розглядав окремий аспект системи, запропонований підхід реалізує їх взаємодію в межах єдиної багаторівневої онтології. Модель базується на формалізованих математичних залежностях і семантичному описі знань у форматі OWL з логічними правилами SWRL, що забезпечує інтеграцію кількісного аналізу з логічним виведенням Система функціонує за адаптивним циклом «моніторинг – виявлення вразливостей – оцінка ризиків – реагування», де результати аналізу мережевих параметрів у реальному часі впливають на вагові коефіцієнти ризику. Додано коефіцієнт адаптації α(t), який враховує зміни стану вузлів та активність контрзаходів. Приклад моделювання для мережі з 50 вузлів показав зниження інтегрального ризику на 20-25 % після кількох ітерацій адаптації. Практична цінність полягає у можливості впровадження моделі як компонента SCADA- або IoT-платформ для підвищення надійності, гнучкості та безпеки БСМ. Результати дослідження створюють основу для побудови самоналаштовуваних інтелектуальних систем управління сенсорними мережами в умовах промислових ризиків.

Ключові слова: багаторівнева онтологія; модуль вразливості; оцінка ризику; адаптивне управління; семантичне моделювання

Вступ. Бездротові сенсорні мережі широко застосовуються в промисловій автоматизації, але їх експлуатація у складних фізичних умовах супроводжується технічними, фізичними та кібератаковими ризиками. Раніше ми формалізували окремі модулі – опису мережі та оцінки ризиків; також розроблено спеціальний модуль вразливості, що аналізує слабкі місця на основі логічних правил. Метою цієї роботи є поєднання цих компонентів в адаптивну онтологічну систему, здатну автоматично коригувати параметри оцінки ризику в реальному часі й ініціювати контрзаходи.

Актуальність. У сучасних умовах цифровізації промисловості ключовим завданням є створення інтелектуальних систем, здатних забезпечувати стабільну роботу бездротових сенсорних мереж (БСМ) за дії різнотипних загроз. Традиційні моделі управління ризиками здебільшого зосереджуються на статистичних або ймовірнісних методах і не враховують складних взаємозв'язків між технічними, інформаційними та організаційними параметрами мережі. Це призводить до того, що навіть при наявності точних даних про стан вузлів система не здатна своєчасно виявляти критичні ризики та адаптуватися до нових умов. Розвиток концепції багаторівневої онтології управління ризиками відкриває можливість створення більш гнучких і самонавчальних систем. Поєднання модулів опису мережі, оцінки ризиків та вразливості у єдиній семантичній структурі дозволяє формалізувати взаємозв'язки між параметрами мережі, подіями та можливими наслідками їх реалізації.

Такий підхід забезпечує побудову логічно цілісної моделі, що підтримує автоматичне виявлення відхилень і динамічне коригування ризикових показників у режимі реального часу. Актуальність дослідження зумовлена потребою у створенні адаптивних систем управління, які здатні інтегрувати кількісні оцінки, логічні правила та контекстні знання в єдиному онтологічному просторі. Це забезпечує підвищення надійності, безпеки та стійкості БСМ у промислових умовах, де помилки в роботі сенсорної мережі можуть призвести до технологічних збоїв або втрати критичних даних.

Мета дослідження – розроблення та формалізація інтегрованої онтологічної моделі управління ризиками у бездротових сенсорних мережах промислового призначення, яка об'єднує модулі опису мережі, оцінки ризиків та вразливості в єдину семантичну структуру. Така модель покликана забезпечити комплексний аналіз технічних, енергетичних і інформаційних параметрів мережі, своєчасне виявлення загроз та реалізацію адаптивного реагування у реальному часі. Реалізація поставленої мети спрямована на підвищення надійності, гнучкості й безпеки БСМ у промислових умовах шляхом інтеграції математичного моделювання з логічним виведенням на основі онтологічного опису знань.

У дослідженні модуля вразливості в багаторівневій онтології оцінки ризиків для бездротових сенсорних мереж (БСМ), представленому в документі, акцент робиться на аналізі слабких місць БСМ у промислових середовищах і пропонується підхід для їх усунення за допомогою логічних правил. Якщо порівнювати це дослідження з іншими статтями зі списку:

У роботі [3] подано системний огляд застосування БСМ в промисловій автоматизації: описано вузли, топології (star/mesh/cluster-tree), енергетичні обмеження, приклад стенду (парогенератор), а також вимоги до протоколів і стандарти (IEEE 802.15.4, ZigBee, WirelessHART), вплив завад і питання мережевого керування в реальному часі. Автор узагальнює класи ISA SP100, виділяє сценарії використання (SCADA, діагностика, періодичний збір, рідкісні події) та розглядає стек протоколів із акцентом на MAC/RT-вимоги й перешкоди в ISM-діапазонах. **Цінність** для нашої роботи полягає в чіткому формулюванні промислових вимог до продуктивності та надійності БСМ, що можна напряму використовувати як набір обмежень/атрибутів у модулі опису мережі та як фактори ризику в онтології. **Обмеження** – оглядовий характер без онтологічної інтеграції, відсутність формальної моделі вразливостей і адаптивної оцінки ризику; також матеріал частково застарілий і не охоплює сучасні підходи (OWL/SWRL, семантичні правила, інтеграцію з модулем ризиків у реальному часі). У роботі [4] проаналізовано ризики та методи захисту, пов'язані з використанням індустріальних сканерів пристроїв у системах SCADA та IIoT. Автори розглядають інструменти Shodan, Nessus, ZMap, оцінюючи їх вплив на безпеку промислових мереж і можливість зловживань для атак. Цінність роботи полягає у систематизації підходів до виявлення вразливостей, що може бути корисним для удосконалення модуля вразливості у БСМ. Обмеження – зосередженість на загальних кіберзагрозах без урахування специфіки сенсорних мереж і енергетичних параметрів вузлів. У роботі [5] представлено фундаментальний аналіз протоколів і архітектур бездротових сенсорних мереж. Автори детально описують шари OSI-моделі, механізми маршрутизації, кластеризації, енергозбереження, а також вплив топології на продуктивність мережі. Розглянуто базові принципи побудови стеку протоколів та їхню роль у забезпеченні QoS, синхронізації та масштабованості. Цінність: робота є класичним теоретичним підґрунтям для формалізації модуля опису мережі в онтологічній моделі оцінки ризиків БСМ. Обмеження: відсутність сучасних аспектів – нечіткої логіки, семантичної інтеграції й ризик-орієнтованого підходу до оцінки стану мережі У роботі [6] запропоновано графову модель для виявлення вразливостей у промислових кіберфізичних системах, що описує взаємозв'язки між сенсорами, контролерами та вузлами. Цінність: формалізований підхід до ідентифікації критичних вузлів можна застосувати у модулі опису мережі та вразливості**.** Обмеження**:** відсутня інтеграція з онтологічними й нечіткими методами оцінки ризику. У

роботі [7] подано огляд застосування методів штучного інтелекту (AI) у системах інфраструктури, включно з енергетичними, транспортними, водними та телекомунікаційними мережами. Автори класифікують підходи за типами навчання (supervised, unsupervised, reinforcement) і відзначають поширення гібридних моделей, таких як ANFIS та нечітка логіка. Особливу увагу приділено ролі AI у прогнозуванні, моніторингу, маршрутизації та забезпеченні безпеки інфраструктурних систем. **Цінність** роботи полягає у міждисциплінарному охопленні AI-підходів і підкресленні потенціалу нечіткої логіки для управління невизначеністю, що безпосередньо узгоджується з концепцією **модулів ризику та вразливостей у БСМ**. **Обмеження** — оглядовий характер без глибокої формалізації семантичних зв'язків між даними, що зменшує придатність моделі для побудови онтологічних структур або реального оцінювання ризиків у динамічних мережах. У роботі [8] проведено систематичний огляд концепції **Agriculture 4.0**, де узагальнено використання технологій Industry 4.0 — IoT, WSN, AI, Big Data, Cloud, Edge/Fog Computing та роботизованих систем — у цифровізації сільського господарства. Автори класифікують напрямки за рівнем зрілості технологій і типом ферм, виділяючи переваги та бар'єри впровадження. **Цінність:** робота демонструє, як цифрові технології формують інтегровані системи моніторингу, що можуть бути адаптовані до моделі **багаторівневої онтології оцінки ризиків БСМ**. **Обмеження:** фокус спрямовано на аграрний сектор без аналізу промислових сенсорних мереж і семантичних механізмів управління ризиками.

Проведений аналіз літератури показав, що сучасні дослідження у сфері бездротових сенсорних мереж охоплюють широкий спектр аспектів — від класичних архітектур і протоколів зв'язку до графових та штучно-інтелектуальних моделей оцінки вразливостей. Виявлено, що більшість робіт зосереджена на структурному, енергетичному та комунікаційному вдосконаленні мереж, тоді як питання семантичної інтеграції, онтологічного представлення ризиків і нечіткого оцінювання залишаються недостатньо дослідженими. Окремі підходи демонструють успішне застосування AI і нечіткої логіки для локального аналізу даних, проте не забезпечують повноцінної взаємодії між рівнями ризиків і структурою мережі. Це підкреслює актуальність створення інтегрованої онтологічної моделі оцінки ризиків у БСМ, яка поєднує формальний опис мережі, модуль вразливостей та механізм динамічного розрахунку ризику на основі логічних і нечітких правил, що дозволить підвищити точність і гнучкість управління безпекою сенсорних систем.

Інтегрована модель управління ризиками у бездротових сенсорних мережах (БСМ) побудована на поєднанні трьох взаємопов'язаних модулів: **опису мережі (NDM)**, **вразливості (VM)** та **оцінки ризиків (RAM)**. Їхня взаємодія реалізована в межах єдиної онтології, яка описує сенсорні вузли, з'єднання, типи загроз і контрзаходи у вигляді семантичних зв'язків між класами *Node, Link, Threat, Vulnerability* та *Risk*.

Модуль опису мережі підтримує графову модель із параметрами вузлів — залишковою енергією, пропускною здатністю, затримками та навантаженням. **Модуль вразливості** аналізує ці дані на основі логічних правил і формує факти про потенційні слабкі місця, наприклад *low_energy_unencrypted* чи *physical_exposure*. **Модуль оцінки ризиків** виконує агрегування отриманої інформації, розраховуючи інтегральний ризиковий показник з урахуванням технічних, фізичних і зовнішніх факторів.

Результати оцінки передаються до **адаптивного шару керування**, який автоматично коригує параметри роботи мережі — маршрутизацію, частоту передачі даних чи ізоляцію вузлів, утворюючи замкнений цикл *«моніторинг → аналіз → оцінка ризику → реагування»*. Онтологічна модель реалізована з використанням OWL та SWRL і може інтегруватися з промисловими платформами SCADA або IoT через протоколи OPC UA чи MQTT.

Інтегрована онтологія управління ризиками в БСМ — демонструє взаємодію модулів NDM, VM та RAM через центральне онтологічне ядро і контур адаптивного зворотного зв'язку.

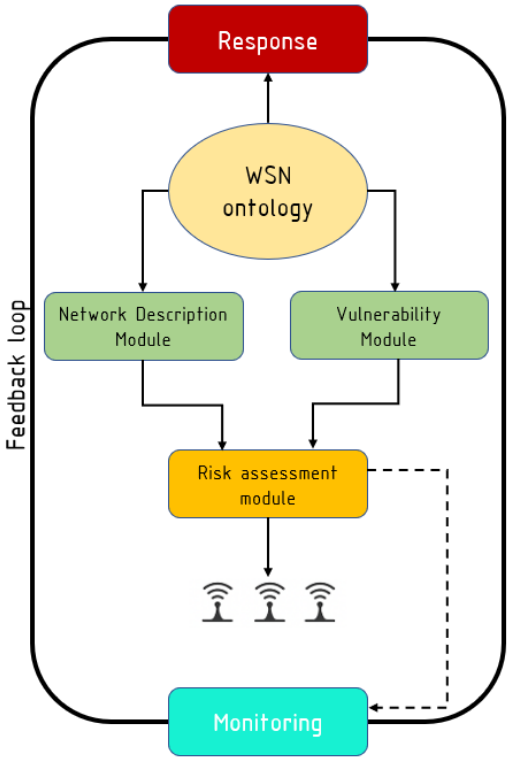

Рисунок. **Інтегрована модель онтології управління ризиками у БСМ**

Ця схема ілюструє архітектуру інтегрованої онтологічної моделі управління ризиками у бездротових сенсорних мережах (БСМ).

У центрі схеми розташовано WSN ontology – семантичне ядро, яке поєднує три функціональні модулі:

- Network Description Module (NDM) – описує топологію та стан мережі;
- Vulnerability Module (VM) – виявляє вразливості на основі логічних правил;
- Risk Assessment Module (RAM) – обчислює інтегральний показник ризику.

Знизу зображено рівень Monitoring, який збирає телеметрію з сенсорних вузлів і передає дані у верхні модулі.

Зверху – блок Response, який реалізує адаптивне реагування: зміну параметрів мережі, ізоляцію вузлів або активацію контрзаходів.

Замкнена стрілка Feedback loop показує зворотний зв'язок між рівнями моніторингу й реагування, що забезпечує безперервний цикл «моніторинг – аналіз – оцінка ризику – реагування» у режимі реального часу

Формалізована модель оцінки ризику в БСМ базується на поєднанні кількісних та логіко-онтологічних механізмів. Основна мета – обчислення інтегрального ризику для окремого вузла або всієї мережі з урахуванням технічних, фізичних та інформаційних факторів, виявлених модулем вразливості.

Інтегральна функція ризику. Сумарний ризик R(t) у момент часу t визначається як зважена сума часткових ризиків із урахуванням коефіцієнтів адаптації:

$$R(t) = \alpha(t)\sum_{i=1}^{n}(P_i(t)\times I_i(t)\times C_i(t)\times W(t)_i) + \lambda(t)\sum_{j=1}^{m}(F_j(t)\times S_j(t)) + \mu(t)\sum_{k=1}^{l}(E_k(t)\times T_k(t)\times M_k(t))$$

де

- $P_i(t)$ – ймовірність настання події або загрози;
- $I_i(t)$ – інтенсивність чи частота її прояву;
- $C_i(t)$ – критичність для конкретного вузла;
- $W_i(t)$ – ваговий коефіцієнт впливу;

- $F_j(t), S_j(t)$ – фізичні фактори середовища (температура, ЕМ-перешкоди, вібрації);
- $E_k(t), T_k(t), M_k(t)$ – енергетичні та мережеві параметри;
- $\alpha(t), \lambda(t), \mu(t)$ – динамічні коефіцієнти, які коригуються адаптивним шаром у відповідь на зміни стану мережі.

Оцінка стану вузла. Для кожного сенсорного вузла υ_i визначається його поточний стан:

$$S(\upsilon_i, t) = \frac{\alpha_E E(\upsilon_i, t) + \beta_B B(\upsilon_i, t) + \gamma_D D(\upsilon_i, t) + \delta_H H(\upsilon_i, t)}{\alpha_E + \beta_B + \gamma_D + \delta_H},$$

де

- E – залишкова енергія;
- B – пропускна здатність;
- D – затримка передачі;
- H – рівень стабільності каналу.

Нормалізоване значення $S(\upsilon_i, t) \in [0,1]$ характеризує працездатність вузла й використовується для уточнення ризику в RAM.

Логічна інтеграція результатів. Онтологічний модуль (OWL + SWRL) формує додаткові знання у вигляді логічних правил:

IF Energy (node)<0.3 AND encryption=false
THEN Vulnerability(node, “low_energy_unencrypted”).

Отримані факти про вразливості додаються до бази знань та автоматично впливають на коефіцієнт адаптації α(t), що зменшує або збільшує загальний ризик.

Адаптивний механізм. Коефіцієнт адаптації α(t) змінюється згідно з ефективністю застосованих контрзаходів:

$$\alpha(t + \Delta t) = \alpha(t) - \eta \frac{\partial R(t)}{\partial C_m}$$

де C_m – набір активних контрзаходів, а η – коефіцієнт швидкості адаптації.

Таким чином формується замкнене коло «моніторинг → аналіз → оцінка → реагування», яке дозволяє системі динамічно знижувати ризик у процесі роботи.

Запропонована інтегрована модель формує теоретичну основу для побудови інтелектуальних систем управління ризиками у бездротових сенсорних мережах. Її структура об’єднує семантичні, логічні та кількісні рівні аналізу, що дозволяє реалізувати повний цикл управління – від збору телеметрії до прийняття рішень у реальному часі. Використання онтологічного підходу забезпечує формалізоване подання знань і підтримує адаптивну взаємодію між модулями оцінки ризиків, опису мережі та вразливості. Це створює умови для подальшої автоматизації процесів виявлення загроз, класифікації інцидентів та узгодження дій у багаторівневих промислових системах.

Висновки. У результаті дослідження було Розроблено концептуальну інтегровану модель управління ризиками у БСМ, яка поєднує онтологічні, логічні та математичні механізми аналізу. Запропонована структура забезпечує взаємодію між модулями опису мережі, вразливості та оцінки ризиків у межах єдиного семантичного простору. Математична формалізація моделі дозволяє враховувати динамічні зміни у стані вузлів і середовища, використовуючи адаптивні коефіцієнти для зниження невизначеності. Онтологічний підхід на основі OWL та SWRL забезпечує гнучкість, масштабованість і логічну узгодженість процесів аналізу ризиків. Отримані результати створюють основу для подальшої розробки прототипу системи підтримки рішень і її інтеграції з промисловими платформами SCADA та IoT.

СПИСОК ЛІТЕРАТУРИ

1. Штільман П. Р., Тішин П. М. «Модуль вразливості у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі». Національний університет «Одеська політехніка». – «Інформатика. Культура. Техніка». 2024; 1: 93–97. DOI: https://doi.org/10.15276/ict.01.2024.04.

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”. AAIT2025. 8(2), 202–215. DOI: https://doi.org/10.15276/aait.08.2025.14.

3. Paavola M., Leivisk K. “Wireless Sensor Networks in Industrial Automation”. *InTech*. 2010. DOI: https://doi.org/10.5772/9532.

4. Borhani M., Gurjot Singh G., Basaez, J., Avgouleas I., Gurtov A. “A critical analysis of the industrial device scanners’ potentials, risks, and preventives”. *Journal of Network and Computer Applications*. 2021; 178: 1–34. DOI: https://doi.org/10.1016/j.jii.2024.100623.

5. Karl H., Willing A. “Protocols and Architectures for Wireless Sensor Networks”. *John Wiley&Sons, Ltd*. 2005.

6. Josbert N. N., Wei M., Wang P., Rafiq A. “A look into smart factory for Industrial IoT driven by SDN technology: A comprehensive survey of taxonomy, architectures, issues and future research orientations “. *Journal of King Saud University – Computer and Information Sciences*”. 2024; 36 (5): 1–43. DOI: https://doi.org/10.1016/j.jksuci.2024.102069.

7. McMillan L., Varga L. “A review of the use of artificial intelligence methods in infrastructure systems”. *Engineering Applications of Artifical Intelligence*. 2022; 116: 1–21. DOI: https://doi.org/10.1016/j.engappai.2022.105472.

8. Abbasi R., Martinez P., Ahmad R. “The digitization of agricultural industry – a systematic literature review on agriculture 4.0”. *Smart Agricultural Technology*. 2022; 2: 1–24. DOI: https://doi.org/10.1016/j.atech.2022.100042.

DOI: https://doi.org/10.15276/ict.02.2025.32
UDC 004.7:004.056.5:004.89(045)

Integrated risk, vulnerability and network description ontology for adaptive management of industrial wireless sensor network

Pavlo R. Shtilman[1)]
PhD student of the Department of Computer Intellectual Systems and Networks
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com
Petr M. Tishyn[1)]
PhD, Associate Professor of the Department of Computer Intellectual Systems and Networks
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com. Scopus Author ID: 57190400970
Oleksandr N. Martynyuk[1)]
PhD, Associate Professor of the Department of Computer Intellectual Systems and Networks
ORCID: http://orcid.org/0000-0003-1461-2000; martynyuk@op.edu.ua. Scopus Author ID: 57103391900
Vitaliy O. Elkin[1)]
PhD student of the Department of Computer Intellectual Systems and Networks
ORCID: https://orcid.org/0009-0002-4202-7802; goodideacrew@gmail.com
[1)] Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, Ukraine

ABSTRACT

This work presents an integrated ontological model of risk management in industrial wireless sensor networks (WSNs), which combines three interconnected modules: network description, risk assessment, and vulnerability. Unlike previous solutions, each of which considered a separate aspect of the system, the proposed approach implements their interaction within a single multi-level ontology. The model is based on formalized mathematical dependencies and semantic knowledge description in OWL format with SWRL logical rules, which provides integration of quantitative analysis with logical inference. The system operates according to the adaptive cycle "monitoring - vulnerability detection - risk assessment - response", where the results of real-time analysis of network parameters affect the risk weight coefficients. An adaptation coefficient α(t) has been added, which takes into account changes in the state of nodes and the activity of countermeasures. A modeling example for a network of 50 nodes showed a reduction in the integral risk by 20–25% after several adaptation iterations. The practical value lies in the possibility of implementing the model as a component of SCADA or IoT platforms to increase the reliability, flexibility and security of BSM. The research results create the basis for building self-configuring intelligent sensor network management systems in conditions of industrial risks.

Keywords: Multi-level ontology; vulnerability module; risk assessment; adaptive control; semantic modeling