**DOI: https://doi.org/10.15276/aait.08.2025.14**
**UDC 004.7:004.056.5:004.94:681.518(045)**

# Risk assessment and network description modules in a multi-level wireless sensor network risk assessment ontology

**Pavel R. Shtilman**[1)]
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com.
**Petr M. Tishin**[1)]
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com.
**Yevhen V. Shendryk**[1)]
ORCID: https://orcid.org/ 0009-0008-9039-810X; e.v.shendrik@op.edu.ua.
**Vitaliy O. Elkin**[1)]
ORCID: https://orcid.org/0009-0002-4202-7802; goodideacrew@gmail.com.
Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, Ukraine

## ABSTRACT

Wireless sensor networks have become widely used in industrial automation systems due to their ease of deployment, flexibility, and cost-effectiveness. They provide real-time monitoring, diagnostics, and control of technological processes without the need for complex cabling infrastructure. However, the operation of wireless sensor networks in production environments is accompanied by risks associated with limited energy resources of nodes, the impact of electromagnetic interference, data transmission delays, the inability to guarantee communication stability, and vulnerability to cyberattacks. These threats are exacerbated in complex environments where equipment is located in hard-to-reach places, and the network has limited bandwidth and variable topology. Such conditions require the construction of multi-level structures for network health analysis, risk assessment, and adaptive management. The aim of the research is to develop two functional modules of a multi-level ontology: a risk assessment module and a network description module, that allow for an integrated analysis of threats, vulnerabilities, and wireless sensor network parameters, taking into account their changing state. The research methodology is based on the construction of formalized mathematical models: the network description is implemented through a graph representation with the parameters of nodes, connections, and their dynamics, while the risk assessment is performed using a multifactor model that takes into account the probability of threats, the level of their impact, the criticality of network components, and external risks. The article presents examples of the application of modules based on typical production scenarios that demonstrate the relationship between the structural description of the network and the dynamic assessment of threats. Information from the network description module is used to calculate risks in real time, while the results of the risk analysis affect the dynamic adjustment of network operation parameters. The scientific novelty of the research lies in the integration of two formalized models within a single ontological system of risk-oriented wireless sensor network management. The practical significance lies in the possibility of implementing the proposed approaches in real industrial conditions to increase the reliability, flexibility, adaptability and information security of sensor networks. The proposed system is the basis for building self-adjusting smart networks capable of independently responding to changes in technical condition, threats and environmental parameters.

**Keywords**: Wireless sensor networks; multi-level ontology; risk analysis; sensor node; threat intensity; threat probability; Supervisory Control and Data Acquisition

***For citation*: 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". *Applied Aspects of Information Technology*. 2025; Vol.8 No.2: 202–215. DOI: https://doi.org/10.15276/aait.08.2025.14**

## INTRODUCTION

In modern conditions of industrialization and automation of production processes, Wireless sensor networks (WSN) play a key role in ensuring monitoring, control and management of various technological processes. They allow receiving and transmitting information in real time, reducing infrastructure costs and ensuring high flexibility and scalability of systems. However, with increasing network complexity and the number of connected devices, the likelihood of risks associated with both technical, cyber and physical threats increase.

To effectively manage such risks, it is necessary to apply multi-level approaches to network status analysis, which allow for a comprehensive assessment of system vulnerabilities, determine the level of potential threats and form adequate response strategies.

Wireless sensor networks are used in a wide range of industries, such as industry, energy, transport and agriculture. Their main functions are:

– monitoring of production processes, ensuring continuous collection of data on the condition of equipment and the environment;

– control of production systems, management of operations based on the received data, which contributes to increasing production efficiency;

– equipment diagnostics, identifying deviations in the operation of systems to prevent malfunctions and breakdowns.

– asset and production operations management, automation of resource management and coordination of actions between different parts of the production complex.

However, despite their effectiveness, WSNs remain vulnerable to a number of threats, including: limited energy resources, physical obstacles, limited bandwidth, and cyber threats. Limited energy resources - most nodes operate on batteries, which limits their autonomous operation, especially in hard-to-reach places. Physical obstacles, electromagnetic interference in an industrial environment can reduce communication quality and interfere with data transmission. Limited bandwidth, in some critical production systems, data transmission delays can be unacceptable. Cyber threats, due to limited computing resources of nodes, the use of complex encryption algorithms becomes difficult, which makes the network vulnerable to attacks.

In this regard, there is a need to develop a comprehensive risk management system for WSN, which would allow to effectively identify, analyze and reduce the impact of potential threats. The integration of the risk assessment module and the network description module into a multi-level ontology creates the prerequisites for creating stable and flexible systems that can adapt to changes in the network in real time and ensure stable operation in conditions of increasing complexity of industrial processes.

## LITERATURE REVIEW

The advantages of WSNs over traditional wired systems include a significant reduction in installation and maintenance costs, as there is no need to lay cable routes. This is especially important for industrial environments with a high level of danger, where the deployment of cable infrastructure can be complicated by aggressive conditions, exposure to high temperatures, humidity, chemicals, mechanical damage or physical obstacles. An additional advantage of WSNs is their flexibility and scalability, which allows for the rapid integration of new nodes and expansion of the system without significant changes to the physical infrastructure of the enterprise. This is critically important for production facilities where it is necessary to quickly adapt the network to changes in equipment configuration or to the expansion of production lines.

The main vulnerabilities of WSN in industrial environments include the limited autonomy of the nodes, since most sensors are powered by batteries. This reduces their operating time and complicates maintenance, especially in hard-to-reach places or critical production areas. Another significant risk factor is electromagnetic interference, which can distort or block signals, especially in dense buildings or environments with a large number of metal structures. Limited bandwidth and data transmission delays can be critical for real-time control systems, such as emergency shutdown systems or precise control of technological processes. Another significant challenge is information security, due to limited computing resources, WSN nodes cannot use complex cryptographic algorithms, which makes them vulnerable to attacks such as traffic interception, node substitution, or malicious code injection.

Despite the mentioned vulnerabilities, WSNs have great potential for application in industrial automation, which is confirmed by numerous studies.

Thus, in article [3] the authors describe the general principles of WSN construction in automated systems, advantages over wired networks, problems of integration with industrial protocols and real examples of applications. However, there is no structured approach to risk analysis or a model for describing the network topology. It is used to justify the relevance of WSN application in industry.

In the article [1], a review of risk identification techniques used in the networked environment of modern global supply chains is conducted. The authors analyzed risk identification approaches in the period 1980-2020, classified them by type and assessed their compliance with the requirements of the network environment. Particular attention is paid to gaps in the technical aspect of the methods and recommendations are made to improve the risk identification process in the context of complex interconnected systems. A useful source for the risk assessment module, helps to classify risk identification methods and identifies shortcomings of classical approaches in the context of network interaction, which is relevant for WSM. Limitations – the source focuses mainly on supply chains, therefore, adaptation of the conclusions to the specifics of wireless sensor networks is required.

In article [4], a method for optimizing delay and energy consumption in WSN for smart grids using clustered reinforcement learning is proposed. The algorithm adapts the transmission power to balance delay and energy consumption, demonstrating a

delay reduction of up to 20.3 %. Useful source for the network description module, shows adaptive optimization of energy consumption and delays in a changing environment. Limitations – does not take into account risks and does not use ontological or semantic formalization.

Article [5] uses a hybrid key management scheme combining cryptographic methods with ontological trust modeling is proposed to improve energy efficiency and reliability in WSNs. The ontological-based trust aware hybrid key management scheme model includes two stages: ensuring confidentiality through encryption and building trust relationships between nodes using ontologies. Experimental results demonstrate improvements in metrics such as trust level communication trust value, throughput, packet delivery ratio, and energy consumption. A valuable resource for extending the risk-based module: considering trust, context, and interactions between nodes using ontologies.

The article [6] proposes an ontological model for risk management and real-time cyber situational awareness. It allows to identify threats, formalize dependencies between assets, vulnerabilities and context, and determine response priorities. Useful source for risk assessment module, demonstrates the application of ontology for dynamic threat analysis. Limitations – the model is focused on IT systems, without taking into account the specifics of industrial WSN.

Article [7] presents a model for describing the technical state of objects using ontology, including diagnostic parameters. Despite the difference in the industry, the approach is relevant for building a network description module. It illustrates the structuring of object parameters in a formalized form.

In article [8], an ontological approach to assessing the risks of digital transformation using the Dempster-Shafer model is proposed. The model takes into account technological, organizational and social risk factors, combining IoT data and expert assessments into a single decision-making system. An important source for the risk assessment module, demonstrates the combination of ontologies, fuzzy data and evidential reasoning for modeling complex dynamic risks in cyber-physical systems. Limitations – the model is focused mainly on the digital transformation of enterprises, without specifying the features of industrial WSN or sensor environments.

The article [9] is devoted to the application of WSN for monitoring and controlling industrial processes. The authors emphasize the advantages of WSN over traditional wired systems: cost reduction due to the elimination of cable connections and increased productivity. Data collection is carried out using analog sensors that transmit information to remote nodes. To ensure the protection of the transmitted information, it is proposed to use the AES encryption algorithm with a 256-bit key, which provides high performance with low power consumption and cost. The article demonstrates the basic integration of WSN in industrial environments with an emphasis on secure data transmission. It can be used to justify the use of encryption modules in data transmission subsystems in WSN.

In the article [10] discusses the architecture of multi-channel WSNs integrated with IoT for monitoring and control in Industry 4.0. Emphasis is placed on big data processing and cloud technologies to ensure efficient power system management. Valuable source for network description module, illustrates practical integration of IoT, Big Data and WSN for industrial tasks in Industry 4.0. Limitations – the paper does not focus on risks or adaptive protection of the system, which reduces its suitability for risk assessment models.).

Paper [11] is focused on increasing the energy efficiency of data collection. Modifications of LEACH-like protocols are proposed. However, risk management or an ontological approach is not considered. It is used to take into account energy indicators in the network structure model.

The article [12] reviews approach to detecting disturbances in intelligent transport systems with an emphasis on the use of ontologies for knowledge formalization and decision-making. The authors analyze existing methods and identify shortcomings in terms of detection accuracy, lack of real-world implementation in developing countries, and lack of ontological support for situation identification. A critical review of typical intelligent transport systems architectures and the prospects for integrating semantic models to improve monitoring reliability are provided. A valuable resource for the network and risk description module, highlights the importance of ontologies in knowledge formalization tasks that can be adapted for industrial BSMs. Limitations – focus on transport systems rather than industrial sensor networks; lack of implemented examples in industry.

In the article [13] presents the construction of an intelligent control platform for electronic vehicle architecture based on an adaptive control algorithm that combines domain control with wireless sensor network technologies. The authors focus on the integration of WSNs for real-time system status

monitoring and adaptive response to changing conditions. Despite the technical depth of the development, the article does not consider formalized risk models or ontological approaches to describe the topology or state of the network. Useful for describing examples of practical implementation of WSNs in complex control systems; complements the applied value of the models presented in the article.

This article [14] proposes architecture of a cloud-based industrial process control platform that combines WSN with cloud technologies for monitoring, storing, processing and detecting anomalies in large industrial data sets. The work implements a multi-layered architecture that includes a data acquisition layer, a cloud-based processing layer (SaaS, PaaS, IaaS) and a control layer with support for critical messages and anomaly detection using a naive Bayesian classifier algorithm. The model is tested in a simulation that demonstrates its effectiveness in reducing latency and energy consumption with high data volumes. Value for the research topic: a scalable WSN-cloud architecture with anomaly detection support is proposed, which is useful for risk-based management in distributed industrial systems. Limitations: the model does not take into account security aspects in the context of threats and vulnerabilities, which is important for a comprehensive risk assessment.

This article [15] proposes a neural model for optimizing energy consumption in WSN for transport applications using multiple-input and multiple-output technology. The authors developed a recurrent neural network with a backpropagation algorithm, improved using a chimp-based optimization algorithm. The system allows for cluster head selection and finding the shortest route, minimizing energy consumption. The effectiveness was confirmed in the NS2 environment by comparing with traditional methods according to the criteria of delay, throughput, energy consumption, packet loss and execution time. Ontological or risk models are not used. Relevant from the point of view of energy optimization, suitable as an example of modern WSN applications, however, it does not cover semantic or ontological modeling, which limits its integration into the context of ontologies.

In the paper [16], innovative approaches to designing an energy-efficient WSN for industrial IoT systems are presented, including the use of SSAIL, MQTT-SN, 6LoWPAN, novelty detection algorithms (NDS) and simulation analysis. Although the paper offers deep optimization of topology and energy consumption, it does not contain a formalized risk model or ontological structure. Valuable for strengthening the network description module: performance, delay, energy parameters.

This paper [17] proposes a power management model for industrial WSNs using dynamic power management. The network nodes go into sleep mode to reduce power consumption, and the dynamic power management with scheduled switching modes system ensures the network lifetime extension. Value for the research topic: The paper demonstrates the practical implementation of dynamic power management algorithms to reduce power consumption in WSNs, which is an important component of the risk assessment module under resource constraints. Limitations: The model focuses mainly on the hardware architecture, rather than on ontological or logical modeling, which limits its application for semantic risk analysis.

Paper [18] Energy-efficient routing using clustering and minimum spanning tree construction is proposed. The energy consumption is significantly reduced and the network uptime is increased. However, risks, network dynamics and vulnerabilities are not considered. It is important for implementing energy analysis policies in the network description module.

In paper [19] an IoT platform using WSN based on the TSCH protocol (IEEE 802.15.4e) is built. The paper focuses on architecture with high throughput and low energy consumption, but does not cover issues of risks or ontological description. It is useful for formulating topological characteristics in the description module.

This article [20] proposes a coverage and connectivity maintenance protocol (CCM-OAL) for wireless sensor networks operating in resource-constrained environments. It uses an optimal adaptive learning (OAL) method, in which each node independently decides on its activity state (active/sleep) to maintain coverage and connectivity while minimizing the number of active nodes. The algorithm is implemented in MATLAB and tested against existing K-CCA and LA-PC methods. The results demonstrate improved network lifetime, coverage ratio, and energy efficiency. A useful source for a network description module in terms of optimizing node structure and activity, but does not include a semantic or ontological approach.

In this article [21] discusses the combination of Named Data Networking and Edge Computing approaches to improve IoT performance in wireless and mobile networks. The proposed architecture includes multiple levels of caching, prefetching, and

adaptive routing that takes into account the type of content and latency. A simulation comparison with traditional IP networks is performed, which demonstrates reduced latency and increased reliability of data delivery. The source is valuable for the network description module, demonstrates the integration of content-oriented routing with edge computing in conditions of mobility and limited resources. Limitations – the model is focused on general IoT scenarios without adaptation to the specifics of industrial WSNs or risk-oriented analysis.

The article [22] proposes a two-stage approach to energy-efficient sensor placement and clustering, taking into account interference, coverage, connectivity, and energy resources. The E-TOPSIS method was used for multi-criteria ranking of positions and selection of cluster heads. Experiments showed improved stability and network uptime compared to other methods (TOPSIS, SAW, Modified LEACH). Valuable for the network description module, provides a formalized approach to node placement. Disadvantages – lack of ontology and risk-based analysis, but semantic extension is possible.

The article [23] systematizes existing approaches to secure routing in WSNs, dividing them into two areas: multipath secure protocols (with division into share / non-share) and trust-based routing (clustered and non-clustered models). Special attention is paid to the role of trust as a flexible security mechanism that works effectively in resource-constrained environments, complementing or replacing cryptographic methods. The article considers methods for assessing trust between nodes, related attacks, computational complexity of algorithms, their strengths and weaknesses. The source is valuable for the risk assessment module: it offers behavioral models of nodes, categorization of attacks, and principles for building trust graphs. Potential application, building a semantic trust model in ontology or integration into dynamic routing mechanisms with adaptation to risk levels and node behavior. Limitations – emphasis on reviewing and comparing existing solutions without implementing a new model.

The article [24] proposes a clustered energy-efficient routing for WSNs based on a hierarchical structure. The main goal is to reduce energy consumption and extend the network lifetime by optimally selecting cluster heads. An improved mechanism for cluster head rotation and routing taking into account the energy characteristics of nodes are proposed. The authors demonstrate the effectiveness of the approach compared to classical protocols based on simulations. However, the paper does not describe trust models, risks, or semantic data integration. It is useful for implementing an energy efficiency module and topology management within the framework of an ontological description of the network.

This article [25] discusses the main aspects of security and the scope of application of wireless sensor networks (WSNs), in particular in the military, medical and industrial sectors. The authors systematize the types of attacks on WSNs (physical, network, logical) and highlight key requirements for data protection: confidentiality, authenticity, integrity and availability. To counter threats, cryptographic methods, encryption and authentication protocols, as well as the use of adaptive secure routing protocols are proposed. A useful source for the risk analysis module - contains a classification of threats, protection measures and an emphasis on a multi-layered approach to WSN security. Limitations - the article is of an overview nature, without specific models or formalized methods for risk assessment.

This article [26] considers a new approach to data collection in WSNs with uneven data distribution, which uses a mobile sink. An energy-efficient receiver motion planning scheme based on data density is proposed, which allows reducing the overall energy consumption of nodes. The model takes into account both the data generation frequency and the location of nodes. The simulation results demonstrate improved network lifetime and reduced latency. At the same time, the article does not use an ontological or risk-based approach. It is valuable for building data collection models in the network description module, taking into account mobility and dynamic load redistribution.

The article [27] presents an efficient retransmission algorithm in multi-hop WSNs that uses two buffers: a node buffer (for SID/Count) and a packet buffer (for the route). After receiving a packet, the node checks whether it has already been processed, and only unique packets are forwarded. This reduces the number of collisions and retransmissions in the network, increasing its stability. The algorithm is implemented on the basis of the CC2530 microcontroller and tested experimentally. Scientific novelty – practical implementation of the traffic unification mechanism in a multi-hop WSN through double buffering. Practical value, increased data transmission efficiency, reduced duplication, and reduced energy consumption. Disadvantages: lack of risk, trust, and

attack assessment models; no ontological or semantic representation is used. Possible application – as part of the description of the data transmission architecture in WSNs in the structural module of the ontology or as an element of routing optimization.

This article [28] reviews existing challenges in WSN security, particularly in the context of limited resources, physical vulnerability, unreliability of the wireless environment, and energy constraints. The authors classify attack types (e.g., sinkhole, Sybil, wormhole), consider secure routing protocols, and analyze their advantages and disadvantages. A detailed analysis of architectural and protocol solutions used in WSNs to mitigate risks is provided. The paper also identifies gaps in current research and suggests directions for future work aimed at improving WSN security. An important source for the risk assessment module, summarizes threat categories, points out limitations of existing solutions, and approaches to building secure WSNs. Relevant for determining security requirements when forming an ontology of risks and vulnerabilities in industrial environments.

The article [29] presents an overview of attacks at different WSN levels (physical, channel, network, transport and application) with examples of typical threats, such as DoS, interception, substitution, data modification. Particular attention is paid to security assessment metrics FPR (False Positive Rate), FNR (False Negative Rate), detection accuracy, bandwidth, latency, power consumption, adaptability. Attack detection approaches (e.g., IDS - intrusion detection systems) and their effectiveness are also analyzed. An important source for the risk assessment module, provides a systematization of attacks and threat detection methods, as well as indicators of the effectiveness of protective protocols. Can be integrated into the WSN threat ontology, with formalization of attack types, input parameters and corresponding network reactions.

The [30] article proposes a model based on Improved Naive Bayesian Kernel Estimation (INBK) for predicting and assessing security risks of data transmission in wireless networks. The model is focused on protecting confidentiality and avoiding information leaks during transmission in local WSNs. The main attention is paid to comparison with other algorithms by the metrics FPR, FNR, accuracy, Recall and F1-score. The accuracy indicators turned out to be higher than 95% compared to other approaches (~75-80 %). The model showed lower energy consumption (18 ms vs. 35 ms) and better efficiency even with an increase in the number of attacking nodes. An important source for formalizing the risk assessment module, in particular regarding computational methods for classification and dynamic response to violations. It can also be used to develop prediction components based on data mining.

Although the reviewed studies cover a wide spectrum of problems in WSNs, including secure routing, trust management, event detection, energy optimization, sensor deployment, and ontology-based threat classification. They remain focused on isolated aspects of system modeling. Most works either emphasize architectural or behavioral layers (e.g., routing, clustering, intrusion detection), or provide semantic models that capture specific attack types or decision-making logic. However, none of the analyzed sources presents a comprehensive framework that unites dynamic network structure representation with a formalized risk assessment process in a single coherent ontological system. The proposed approach fills this research gap by integrating both descriptive and risk-related modules into a multi-level ontology, enabling consistent semantic reasoning across structural, behavioral, and threat domains within industrial WSNs.

## PURPOSE AND OBJECTIVES OF THE STUDY

The aim of this study is to develop and formalize two key components of a multi-level WSN risk assessment ontology: a risk assessment module and a network description module. These modules should increase the efficiency, reliability, and adaptability of WSN in industrial environments where network performance and security are critical.

The research includes the design of a formalized structure of a risk assessment module that allows for the identification, quantification, and prioritization of technical, physical, and external threats. In parallel, a network description module is being developed that models, both structural and dynamic characteristics of the WSN, including the level of node power supply, communication channel bandwidth, delays, and load.

In the process of research, the following tasks are solved:

– to build mathematical models to formalize the functioning of the risk assessment module and the network description module;

– to implement examples that demonstrate the practical use of models for adaptive analysis of threats and network parameters;

– to justify the integration of both modules into a common ontological system for automated risk management in WSN.

The research results are aimed at forming the basis for creating an intelligent sensor network

management system capable of independently adapting to changes in the environment and the level of threats.

## RESEARCH METHODS

The developed approach involves creating a multi-level ontology model as a set of modules, presented in Fig. 1. This schema is the structure of an ontology metamodel related to risk assessment in WSN for industry. The schema uses the following key modules:

– Risk assessment module, performs an assessment of risks associated with network operation;

– Network description module, describes the main parameters and structure of the WSN;

– Vulnerability module, detects vulnerabilities in the system.

The risk assessment module in the WSN is the main module and is the interaction between all three previous modules.

The risk assessment module is a critical component of a multi-layered ontology for WSNs, which allows for the identification, analysis, and quantification of potential threats that may arise during network operation. This module provides a systematic approach to risk management, taking into account a wide range of factors, such as technical failures, physical access to sensor nodes, external cyberattacks, and other threats.

The main functions of the module are:

– risk detection – systematic identification of potential threats through analysis of network parameters and data from monitoring modules;

– assessment of the probability of threat realization – determining the chances of a certain threat occurring, taking into account historical and current operating conditions;

– analysis – an assessment of the possible impact of a realized threat on network functioning, data transfer stability, and overall system efficiency;

– prioritization – identifying the most critical threats that require immediate elimination or minimizing their impact.

Thanks to this module, you can increase the effectiveness of risk management and reduce the likelihood of WSN failures, which is especially important for industrial systems with increased requirements for reliability and safety.

The structural model of the module consists of the following key subsystems:

– Threat detection subsystem, analyzes network data to identify potential threats and deviations from normal operation;

– Probability analysis subsystem, uses historical data and statistical methods to assess the probability of threats;

– Consequence assessment subsystem, model possible outcomes of risk realization, including network failures, data loss, and financial losses;

– Decision-making subsystem, forms a list of priorities to eliminate threats or reduce their impact.

The following complex mathematical model of the module is used to conduct a quantitative risk assessment:

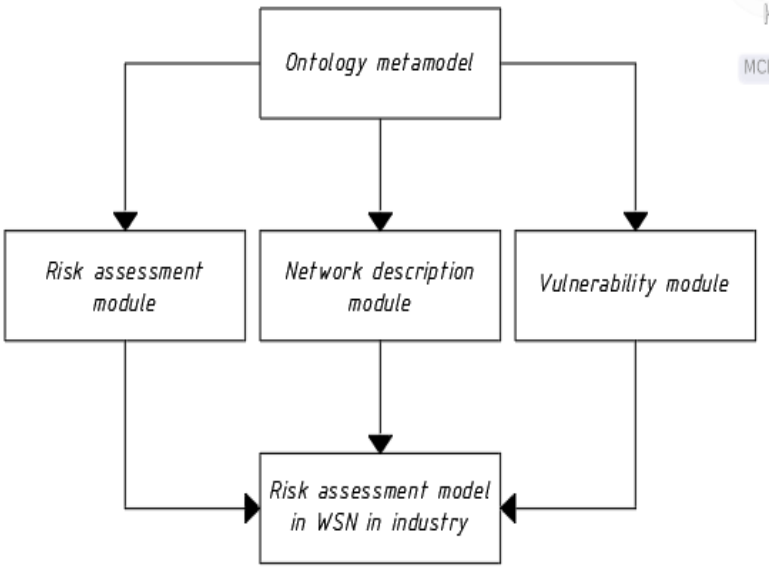


*Fig. 1.* **Multilevel ontology model of risk assessment in wireless sensor networks in industry**
***Source:*** **compiled by the authors**

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

where $R$ is overall risk for the network; $P_i$ is probability of threat $i$ occurring; $I_i$ is intensity of impact of threat $i$; $C_i$ is criticality of the threat for the functioning of the network; $W_i$ is weighting factor that determines the significance of the threat to the system; $F_j$ is level of physical impact of threat $j$; $S_j$ is significance of physical threat $j$; $E_k$ is probability of occurrence of external threat $k$; $T_k$ is level of influence of external threat $k$; $M_k$ is potential losses from threat $k$; λ, μ are coefficients of significance of physical and external threats.

The proposed formula is an integrated model for quantitative risk assessment in a WSN, which takes into account both internal technical and external factors of influence. The formula allows calculating the aggregate risk $R$ for the entire network, adapting the model to changes in the environment or network architecture. It is a key component of the risk assessment module in the ontological management system of the WSN.

The second network description module in the model is the basic component of a multi-level ontology, which is responsible for structuring information about the network topology, characteristics of nodes and connections between them. The main function of the module is to provide a clear description of the current state of the network, including the energy resources of nodes, their location features, bandwidth and stability of connections.

This module allows you to:

– create a complete picture of the network, form a detailed map of nodes and connections between them;

– monitor network status, track changes in real time, including node energy levels, signal delays, and other key parameters;

– optimize network topology, analyze network performance and make changes to improve performance and fault tolerance.

The structural model of the module consists of the following key subsystems:

– node description submodule, records the parameters of each node, such as energy level, sensor type, and transmission power;

– connection description submodule, takes into account the type of connections, their bandwidth, delays, and signal losses;

– network topology submodule, models the physical and logical structure of the network;

– dynamic update submodule, updates network information in real time when the state of nodes changes.

The target function is to minimize the total costs:

$$G = (V, E, A, \Phi),$$

where $V = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes; $E = \{e_1, e_2, \ldots, e_n\}$ is the set of connections between nodes; $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the set of attributes describing the characteristics of nodes and connections (for example, energy balance, throughput, average response time); $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ is the set of dynamic parameters that change in time.

The formula for assessing the state of a node:

$$S(v_i) = \alpha \times E(v_i) + \beta \times B(v_i) + \\ + \gamma \times D(v_i) + \delta \times H(v_i), \quad (2)$$

where $E(v_i)$ is the level of residual energy of the node; $B(v_i)$ is node throughput; $D(v_i)$ is average node delay; $H(v_i)$ is node load level; α, β, γ, δ are weighting factors for each parameter.

A unique feature of the proposed system is its implementation in the form of a multi-level ontology, which acts not only as a formal data model, but also as a logical-semantic structure that combines knowledge about network elements, their properties, relationships and risk factors. Unlike traditional approaches, the ontological model allows for level abstraction, ranging from the physical parameters of nodes and connections to the logical analysis of threats, environmental impact and response priorities. Such a structure supports semantic inference mechanisms, which provides the ability to automatically form decisions based on generalized knowledge and dynamic data. In addition, the ontology acts as an integration platform for combining individual modules (risk assessment, network description, vulnerabilities) into a single system that can be easily scaled and adapted to the specifics of a particular industrial sector.

The interaction between the modules in the proposed multi-level ontology is organized as follows. The network description module forms a semantic representation of the WSN, including node attributes, topological structure, and real-time operational status. This information is transferred to the vulnerability module, which analyzes device characteristics (e.g., battery type, encryption protocols, connectivity), external conditions (e.g., electromagnetic interference, physical access), and

possible attack types (e.g., data interception, jamming, spoofing) using a system of logical rules. These rules allow the identification of weak points and compute cumulative vulnerability scores based on defined parameters and threat models.

Detected vulnerabilities and their attributes – such as type, likelihood, and potential damage – are then passed to the risk assessment module, which integrates this data into the broader ontology-based evaluation of network integrity and operational risk. For example, the presence of unencrypted communication protocols or physically exposed sensor nodes increases the composite risk score calculated by the system. The architecture supports reasoning mechanisms (e.g., OWL+SWRL or custom rule engines) and enables the real-time update of risk status and mitigation strategies.

Technically, the system can be implemented using a combination of OWL (Web Ontology Language) ontologies for structural modeling, SWRL (Semantic Web Rule Language) rules for logic-based inference, and SPARQL queries for extracting critical insights. The modular structure allows seamless integration and communication between components via shared semantic vocabularies and rule-based mechanisms. This layered interaction supports real-time detection of new vulnerabilities and automated decision-making for adaptive responses, such as isolating a vulnerable node or adjusting routing protocols to avoid compromised segments.

## RESEARCH RESULTS

Let's consider an example of using the risk assessment module. Consider a WSN with 100 sensor nodes deployed to monitor temperature and humidity in a large industrial facility. The nodes transmit data to a central server for further analysis. The network operates in an environment with high levels of electromagnetic interference and the risk of physical damage to equipment due to a harsh working environment.

In this simulation, there are the following types of threats:

– technical threat ($R_{tech}$) – transmitter failure due to electromagnetic interference;

– physical threat ($R_{phy}$) – the possibility of damage to the sensor due to physical impact (e.g., impacts or high temperature);

– cyber threat ($R_{cyber}$) – an attempt by a third party to access transmitted data.

Based on this statement, the formula for calculating the overall risk assessment can be divided as follows:

$$R_{tech} = \sum_{i=1}^{n} (P_i \times I_i \times C_i \times W_i) \quad (3)$$

$$R_{phy} = \lambda \sum_{j=1}^{m} (F_j \times S_j) \quad (4)$$

$$R_{cyber} = \mu \sum_{k=1}^{l} (E_k \times T_k \times M_k) \quad (5)$$

The execution of the risk assessment operation looks like this:

Technical risk:

– transmitter failure probability ($P_i$) = 0.3;

– impact intensity ($I_i$) = 0.5;

– criticality of the damaged node for the network ($C_i$) = 0.6;

– threat severity ($W_i$) = 0.8.

According to formula (3), we calculate the $R_{tech}$:

$$R_{tech} = 0.3 \times 0.5 \times 0.6 \times 0.8 = 0.072$$

Physical risk:

– impact or overheating exposure level ($F_j$) = 0.3;

– the significance of the physical threat ($S_j$)= 0.72;

– coefficient of significance ( $\lambda$ ) = 1.

According to formula (4), we calculate the $R_{phy}$:

$$R_{phy} = 1 \times 0.3 \times 0.72 = 0.216$$

Cyber threat:

– attack probability ($E_k$) = 0.05;

– impact level ($T_k$) = 0.9;

– potential loss ($M_k$) = 0.85;

– coefficient of significance ( $\mu$ ) = 1.

According to formula (5), we calculate the $R_{cyber}$:

$$R_{cyber} = 0.05 \times 0.9 \times 0.85 = 0.03825$$

Next, according to formula (1), we calculate the overall risk assessment:

$$R = 0.072 + 0.216 + 0.03825 = 0.32625$$

The greatest contribution to the overall risk is made by technical and physical threats. The model allows for the formalization of mixed risk factors using weighting factors and a combined assessment. Based on the result, the system can recommend:

– placing backup nodes at critical points;

– shielding equipment from interference;

– implementing additional cryptographic means to protect data.

This approach is part of a closed loop: monitoring – assessment – response.

Let's consider an example of using the network description module. In the same network with 100 nodes, some sensors are located in hard-to-reach places, and the amount of data transmitted over the

network increases during peak hours due to frequent data reads. Input parameters for node $\upsilon_i$:

– $E(\upsilon_i)$ residual energy level 60%;
– $B(\upsilon_i)$ transmitter bandwidth 200Kbit/s;
– $D(\upsilon_i)$ average signal delay 150 ms;
– $H(\upsilon_i)$ load level 75 %.

According to formula (2) have the following calculation:

$$S(\upsilon_i) = 0.4 \times 0.6 + 0.3 \times 0.2 +$$

$$+0.2 \times 0.15 + 0.1 \times 0.75 = 0.405$$

The value $S(\upsilon_i)$ = 0.405 indicates the average load level of the node. Nodes with a score below 0.4 are marked as critically loaded and require the following actions:

– redistribute the load by redirecting some of the traffic through other nodes;
– limit data transfer rate if it is not critical;
– suggest replacing the node if its condition steadily deteriorates.

The risk assessment module is aimed at formalizing the processes of identifying, analyzing, and quantifying potential threats, taking into account the probability of their implementation, the level of criticality for the network, and the intensity of their impact. The main task of the module is to ensure timely identification of risks and propose effective measures to eliminate or reduce their impact on the system.

The network description module aims to create a clear structural model of the WSN, which reflects all nodes, their characteristics, connections between them, as well as dynamic changes in the network state over time. The module's task is to provide a complete and up-to-date description of the network topology, its resources and internal connections, which will allow for a more accurate and timely response to changes in the network environment.

Together, these two modules provide the basis for a holistic risk analysis in WSN and allow them to be integrated into a common multi-level ontology designed to improve the reliability, security, and efficiency of the network in industrial operation.

## CONCLUSIONS AND PROSPECTS OF FURTHER REASERCH

Within the framework of this work, two key modules of a multi-level ontology of risk management in WSNs were developed and formalized: a risk assessment module and a network description module. The proposed architecture provides a logically complete model in which formalized knowledge about the topology, resources, and current state of nodes is supplemented by a quantitative assessment of threats, taking into account a set of influence factors. Such integration enables the construction of self-sufficient intelligent decision support systems that operate in real time, which is especially important for industrial critical infrastructure facilities.

The network description module implements a graph-based model of the WSN structure with dynamic parameters such as residual energy, delay, load, and throughput. This module not only serves as a foundation for analytical monitoring and diagnostics, but also acts as a triggering mechanism for recalculating risk levels in response to changes in the state of the network. In turn, the risk assessment module uses semantic relationships and customizable weighting coefficients to calculate the threat level for each node or communication link, considering the likelihood of attack success, the severity of impact, node criticality, and operational conditions.

A bidirectional integration between the two modules ensures that real-time network data influence risk calculations, while the results of the risk assessment inform automated responses, such as routing adaptations, node isolation, prioritization changes, or reconfiguration of communication paths. This creates a closed-loop system of monitoring, analysis, risk evaluation, and mitigation actions with minimal operator involvement.

As a result, the developed system exhibits resilience and adaptability to both internal and external threats. It remains effective under changing environmental conditions or node failures, and is suitable for deployment in industrial systems operating in hard-to-reach or hazardous environments.

Practical implementation aspects include:

– the proposed modules are designed to be compatible with existing SCADA and IoT platforms through ontological interoperability and data exchange interfaces (e.g., via OPC UA or MQTT gateways);
– the system supports heterogeneous sensor networks, incorporating different types of nodes, communication protocols (e.g., ZigBee, LoRa, 6LoWPAN), and traffic profiles. This enhances its universality and scalability for industrial deployments;
– risk metadata and node parameters can be mapped to enterprise-level monitoring dashboards for integration with MES, security information and event management (SIEM), and decision-making systems.

Future research will focus on:

– enhancing the ontology by introducing additional threat scenarios and vulnerability types;

– extending the parameter library to support more node classes, protocol stacks, and communication models;

– refining the inter-module communication protocols with a focus on faster response and reconfiguration cycles;

– developing plug-in components for seamless integration with real-world industrial SCADA and MES platforms.

The proposed model forms a foundation for building a comprehensive intelligent WSN management platform that operates effectively under risk conditions and can be adapted for complex industrial environments.

## REFERENCES

1. Aboutorab, H., Hussain, O. K. Saberi, M., Hussain, F. K. & Chang, E. "A survey on the suitability of risk identification techniques in the current networked environment". *Journal of Network and Computer Applications.* 2021; 178: 102984. https://www.scopus.com/authid/detail.uri?authorId=57201904820. DOI: https://doi.org/10.1016/j.jnca.2021.102984.

2. Shtilman, P. R. & Tishin, P. M. "Vulnerability module in the multi-level ontology of risk assessment for WSNs". *Informatics. Culture. Technology*. 2024; 1: 93-97. DOI: https://doi.org/10.15276/ict.01.2024.04.

3. Duan, Y., Fu, T., Li, L., Pace, P., Aloi, G. & Fortino, G. "AGV-Integrated Noise-Aware Adaptive Clustering for Industrial Wireless Sensor Networks in smart factories". *Ad Hoc Network.* 2025; 177: 103906, https://www.scopus.com/authid/detail.uri?authorId=35755276200.
DOI: https://doi.org/10.1016/j.adhoc.2025.103906.

4. Sun, W., Zhang, L., Lv, Q., Liu, Z., Li, W. & Li, Q. "Dynamic collaborative optimization of end-to-end delay and power consumption in wireless sensor networks for smart distribution grids". *Computer Communications*. 2023; 202: 87–96, https://www.scopus.com/authid/detail.uri?authorId=56585067400. DOI: https://doi.org/10.1016/j.comcom.2023.02.016.

5. Barve, A., Pallavi, R., Deepak, S., Murugan, R., Yadav, D., Singh, A. Kr., Sharma, M. & Shalini, S. "A novel ontological-based trust aware hybrid key management scheme (OTAHKMS) to enhance network lifetime and energy usage in wireless sensor networks (WSNs)". *International Journal of Information Technology*. 2024; 16: 1429–1435. DOI: https://doi.org/10.1007/s41870-023-01696-8.

6. Sanchez-Zas, C., Villagra, V. A., Vega-Barbas, M., Larriva-Novo, X., Moreno, J. I. & Berrocal, J. "Ontology-based approach to real-time risk management and cyber-situational awareness". *Future Generation Computer Systems*. 2023; 141: 462–472, https://www.scopus.com/authid/detail.uri?authorId=57219550778. DOI: https://doi.org/10.1016/j.future.2022.12.006.

7. Tishyn, P. M., Baranova, H. O., Musatov, A. V. & Rakhlinskyi, M. Y. "Development of the ontology model for the technical condition of hydraulic structures". *Herald of Advanced Information Technology*. 2021; 4 (1): 21–34. DOI: https://doi.org/10.15276/hait.01.2021.2.

8. Aishwarya, D., Saranya, S. & Manoharan, S. Q. "Optimizing wireless sensor network routing through memetic algorithms: Enhancing energy efficiency and data reliability". *Procedia Computer Science*. 2023; 230: 150–157, https://www.scopus.com/authid/detail.uri?authorId=55513868500.
DOI: https://doi.org/10.1016/j.procs.2023.12.070.

9. Dharani, N, Krishnan, K. & Mohan, K. V. "Wireless sensor network for industrial monitoring and controlling". *5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. 2021. p. 254–257. DOI: https://doi.org/10.1109/ICICCS51141.2021.9432238.

10. Faheem, M., Fizza, G., Ashraf, M. W., Butt, R. A., Ngadi, A. & Gungor, V. C. "Big Data acquired by Internet of Things-enabled industrial multichannel wireless sensors networks for active monitoring and control in the smart grid Industry 4.0". *Data in Brief*. 2021; 35 (106854): 1–12, https://www.scopus.com/authid/detail.uri?authorId=58648789900.
DOI: https://doi.org/10.1016/j.dib.2021.106854.

11. Alrashidi, M., Nejah, N., Khediri, S. & Kachouri, A. "Energy-Efficiency Clustering and Data Collection for Wireless Sensor Networks in Industry 4.0". *Journal of Ambient Intelligence and Humanized Computing*. 2020. DOI: https://doi.org/10.1007/s12652-020-02146-0.

12. Luther, M. M., Moskalai, N. J., Kaladzavi, G., Tchapi, I., Adamou, A. A. & Kolyang, N. A. "Detection of disturbances in a monitoring system on ITS and usage of ontologies approaches: a critical review and challenges in developing countries". *Procedia Computer Science*. 2023; 224: 250–257,

https://www.scopus.com/authid/detail.uri?authorId=58753894900.
DOI: https://doi.org/10.1016/j.procs.2023.09.034.

13. Hu, Q. & Hu, J. "Construction of an intelligent control platform for electrical and electronic architecture based on adaptive control algorithm combining domain control technology and wireless sensing". *Journal of Combinatorial Mathematics and Combinatorial Computing*. 2025; 127b: 2311–2328. DOI: https://doi.org/10.61091/jcmcc127b-131.

14. Ravindhar, N. V. & Sasikumar, S. "An effective monitoring, storage and analyze on industrial process on cloud big data by data publishing in industrial wireless sensor network". *Measurement: Sensors*. 2022; 24: 100525, https://www.scopus.com/authid/detail.uri?authorId=57210993577.
DOI: https://doi.org/10.1016/j.measen.2022.100525.

15. Ramani, G. & Amarendra, K. "An intelligent recurrent backpropagation neural system for energy optimized wireless sensor based vehicle communication". *Wireless Personal Communications*. 2024; 137 (1): 1–17. DOI: https://doi.org/10.1007/s11277-024-11423-6.

16. Duobienė, S., Simniskis, R. & Raciukaitis, G. "Enabling seamless connectivity: networking innovations in wireless sensor networks for industrial application". *Sensors*. 2024; 24 (15): 4881. DOI: https://doi.org/10.3390/s24154881.

17. Damodaram, D., Godi, R. K., Rajkumar, Divakara Rao, D. V., Glory, K. B. & Somu, K. "Power control management system model using wireless sensor network". *Measurement: Sensors*. 2023; 25: 100639. https://www.scopus.com/authid/detail.uri?authorId=57022221400.
DOI: https://doi.org/10.1016/j.measen.2022.100639.

18. Nasirian, S., Pierleoni, P., Belli, A., Mercuri, M. & Palma, L. "Pizzza: A Joint Sector Shape and Minimum Spanning Tree-Based Clustering Scheme for Energy Efficient Routing in Wireless Sensor Networks". *IEEE Access*. 2023; 11: 68200–68215. DOI: https://doi.org/10.1109/ACCESS.2023.3291915.

19. Mandal, P., Sarkar, H. & Sagarika, K. "Designing an IoT platform using Wireless Sensor Network". *International Journal of Advanced Research in Science, Communication and Technology*. 2024. p. 13–18. DOI: https://doi.org/10.48175/IJARSCT-19302.

20. Meena, N. & Singh, B. "An efficient coverage and connectivity maintenance using optimal adaptive learning in WSNs". *International Journal of Information Technology.* 2023; 15: 4491–4504. DOI: https://doi.org/10.1007/s41870-023-01514-1.

21. Alzabin, L.R., Al-Wesabi, O., Al Hajri, H., Nibras, A., Khudayer, B. H. & Al Lawati H. "Probabilistic detection of indoor events using a wireless sensor network-based mechanism". *Sensors*. 2023; 23 (15): 6918. DOI: https://doi.org/10.3390/s23156918.

22. Chandra, N. & Shetty, D. P. "Multi-attribute decision making approach for energy efficient sensor placement and clustering in wireless sensor networks". *Telecommunication Systems.* 2024; 88 (1). DOI: https://doi.org/10.1007/s11235-024-01250-2

23. Alwakeel, A. M. "Enhancing IoT performance in wireless and mobile networks through named data networking (NDN) and edge computing integration". *Computer Networks.* 2025; 264: 111267, https://www.scopus.com/authid/detail.uri?authorId=57204557471.
DOI: https://doi.org/10.1016/j.comnet.2025.111267.

24. Babiyola, A., Abdus, S. K., Perez de Prado, R. & Parameshchari, B. "An efficient cluster based routing in wireless sensor networks using multiobjective-perturbed learning and mutation strategy based artificial rabbits optimisation". *IET Communications*. 2025; 19 (1). DOI: https://doi.org/10.1049/cmu2.70020.

25. Huanan, Z., Suping, X. & Jiannan, W. "Security and application of wireless sensor network". *Procedia Computer Science*. 2021; 183: 486–492, https://www.scopus.com/authid/detail.uri?authorId=57188864183. DOI: https://doi.org/10.1016/j.procs.2021.02.088.

26. Li, H., Dai, Y., Chen, Q., Dan, L. & Jin, H. "Energy efficient mobile sink driven data collection in wireless sensor network with nonuniform data". *Scientific Reports.* 2024; 14 (1). DOI: https://doi.org/10.1038/s41598-024-79825-x.

27. Chen, S., Cheng, Q. & Wang, J. "Wireless sensor network relay transmitting using dual buffer pools". *Wireless Networks*. 2023; 29 (8): 3617–3623. DOI: https://doi.org/10.1007/s11276-023-03425-2.

28. Mohan, R. G. & Ilavarasan, E. "Security Chalanhes in Wireless Sensor Network: Current Status and Future Trends". *Wireless Personal Communications.* 2024; 139 (2): 1173–1202. DOI: https://doi.org/10.1007/s11277-024-11660-9.

29. Shreyash, A., Alam, J. & Maity, S. “Survey of attacks, detection techniques, and evaluation metrics in wireless sensor networks”. *Advances in Computational Intelligence and Information*. 2024. p. 159–167. DOI: https://doi.org/10.1007/978-981-97-4727-6_16.

30. Huang, B., Yao, H. & Bin Wu, Q. “Prediction and evaluation of wireless network data transmission security risk based on machine learning”. *Wireless Networks*. 2024; 31 (1): 405–416. DOI: https://doi.org/10.1007/s11276-024-03773-7.

**Conflicts of Interest:** The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship or other, which could influence the research and its results presented in this article

Received 08.04.2025
Received after revision 12.06.2025
Accepted 17.06.2025

**DOI: https://doi.org/10.15276/aait.08.2025.14**
**УДК 004.7:004.056.5:004.94:681.518(045)**

# Модуль оцінки ризиків та опису мережі у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі

**Штільман Павло Романович**[1)]
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com
**Тішин Петро Метталинович**[1)]
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com
**Шендрик Євген Валентинович**[1)]
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com
**Єлькін Віталій Олександрович**[1)]
ORCID: https://orcid.org/0009-0002-4202-7802; goodideacrew@gmail.com
[1)] Національний університет“Одеська політехніка”, пр. Шевченка, 1. Одеса, 65044, Україна

## АНОТАЦІЯ

Бездротові сенсорні мережі набули широкого застосування в системах промислової автоматизації завдяки простоті розгортання, гнучкості та економічній ефективності. Вони забезпечують контроль, діагностику та управління технологічними процесами в режимі реального часу без необхідності в складній кабельній інфраструктурі. Проте функціонування бездротові сенсорні мережі у виробничих умовах супроводжується ризиками, пов’язаними з обмеженими енергетичними ресурсами вузлів, впливом електромагнітних завад, затримками передачі даних, неможливістю гарантувати стабільність зв’язку, а також вразливістю до кібератак. Ці загрози посилюються у складних середовищах, де обладнання розміщується у важкодоступних місцях, а мережа має обмежену пропускну здатність та змінну топологію. Такі умови потребують побудови багаторівневих структур для аналізу стану мережі, оцінки ризиків та адаптивного управління. Метою дослідження є розробка двох функціональних модулів багаторівневої онтології – модуля оцінки ризиків і модуля опису мережі, які дозволяють проводити інтегральний аналіз загроз, вразливостей і параметрів бездротові сенсорні мережі з урахуванням їхнього змінного стану. Методологія дослідження базується на побудові формалізованих математичних моделей: опис мережі реалізується через графове подання з параметрами вузлів, з’єднань та їх динаміки, тоді як оцінка ризиків виконується за допомогою багатофакторної моделі, яка враховує ймовірність загроз, рівень їхнього впливу, критичність компонентів мережі та зовнішні ризики. У статті представлено приклади застосування модулів на основі типових виробничих сценаріїв, що демонструють взаємозв’язок між структурним описом мережі та динамічною оцінкою загроз. Інформація з модуля опису мережі використовується для обчислення ризиків у режимі реального часу, тоді як результати аналізу ризиків впливають на динамічне коригування параметрів роботи мережі. Наукова новизна дослідження полягає в інтеграції двох формалізованих моделей в межах єдиної онтологічної системи ризик-орієнтованого управління бездротові сенсорні мережі. Практична значущість полягає у можливості впровадження запропонованих підходів у реальні промислові умови для підвищення надійності, гнучкості, адаптивності та інформаційної безпеки сенсорних мереж. Запропонована система є основою для побудови самоналаштовуваних розумних мереж, здатних самостійно реагувати на зміну технічного стану, загроз і параметрів навколишнього середовища.

**Keywords**: бБездротові сенсорні мережі; багаторівнева онтологія; аналіз ризиків; сенсорний вузол; інтенсивність загрози; ймовірність загрози; система диспетчерського контролю та збору даних

## ABOUT THE AUTHORS

**Pavlo R. Shtilman –** PhD student, Computer Intellectual Systems and Networks Department. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https:// orcid.org/0009-0007-8061-1766, pavel52shtilman62@gmail.com
***Research field*:** Fuzzy Logic; Real-time systems; Wireless sensor networks, Ontology.

**Штільман Павло Романович –** аспірант кафедри Комп'ютерних інтелектуальних систем та мереж. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

**Petr M. Tishin –** Candidate of Physico-Mathematical Sciences, Associate Professor, Computer Intellectual Systems and Networks Department. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https://org/0000-0003-2506-5348, petrmettal@gmail.com
***Research field*:** Fuzzy Logic; Intelligent Systems, Ontology.

**Тішин Петро Метталинович –** кандидат фізико-математичних наук, доцент кафедри Комп'ютерних інтелектуальних систем та мереж. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

**Yevhen V. Shendryk –** Candidate of Engineering Sciences, Associate Professor, Computer Intellectual Systems and Networks Department. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https:// orcid.org/0009-0008-9039-810X, e.v.shendrik@op.edu.ua
***Research field*:** modelling and synthesis of computer systems and networks, real-time systems, algorithmization and programming.

**Шендрик Євген Валентинович –** кандидат технічних наук, доцент кафедри Комп'ютерних інтелектуальних систем та мереж. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

**Vitaliy O. Elkin –** PhD student, Computer Intellectual Systems and Networks Department. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https:// orcid.org/0009-0002-4202-7802, goodideacrew@gmail.com
***Research field*:** Fuzzy Logic; Wireless sensor networks

**Єлькін Віталій Олександрович –** аспірант кафедри Комп'ютерних інтелектуальних систем та мереж. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна