

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова  
праця на правах рукопису

ПІДЛІСНИЙ ЮРІЙ ІВАНОВИЧ

УДК 004.8.5:004.738.5

## ДИСЕРТАЦІЯ

МЕТОДИ ТА МОДЕЛІ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ  
РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІоТ-СЕРЕДОВИЩ

122 – Комп'ютерні науки

12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

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

Підлісний Юрій Іванович

\_\_\_\_\_ підпис

Науковий керівник

Шелест Михайло Євгенович  
доктор технічних наук, професор

Чернігів – 2026

## АНОТАЦІЯ

*Підлісний Юрій Іванович.* Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки». – Національний університет «Чернігівська політехніка», МОН України, м. Чернігів, 2026.

*Актуальність роботи.* Розвиток Інтернету речей (Internet of Things, IoT), кіберфізичних систем, периферійних обчислень і промислового Інтернету речей (Industrial Internet of Things, IIoT) супроводжується ускладненням сучасних інформаційно-комунікаційних систем. IoT-середовища об'єднують пристрої з різним призначенням, обчислювальними можливостями та протоколами взаємодії. Їхній склад, конфігурація і зв'язки між компонентами можуть змінюватися під час експлуатації. Водночас зростає різноманітність кіберзагроз, здатних впливати як на окремі пристрої, так і на роботу середовища загалом.

За таких умов ризик інформаційної безпеки залежить не лише від характеристик загроз і вразливостей. Важливими є функціональна роль пристрою, умови його роботи, зв'язки з іншими компонентами та можливі наслідки порушення їх функціонування. Оцінювання додатково ускладнюється неповнотою вихідних даних і невизначеністю окремих параметрів. Прихована компрометація може залишатися непомітною під час аналізу лише відомих вразливостей та очевидних аномалій.

Аналіз наукових досліджень показав, що класифікація IoT-пристроїв, виявлення вразливостей, аналіз мережевої активності й оцінювання ризиків переважно розглядаються як окремі завдання. Унаслідок цього відомості про характеристики пристрою та поточний стан середовища не завжди узгоджено використовуються під час визначення рівня ризику. Це зумовлює потребу в методах і моделях, які враховують контекст функціонування пристроїв та дають змогу проводити оцінювання за неповних і невизначених даних.

У дисертації розв'язано актуальне наукове завдання, що полягає в розробленні моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконаленні методу оцінювання ризиків інформаційної безпеки IoT-середовищ у процесі аудиту. Під час визначення рівня ризику також враховується попередньо сформований показник ризику прихованої компрометації.

*Метою роботи є розроблення моделі побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням цього профілю, поточного стану безпеки й попередньо сформованого показника ризику прихованої компрометації під час аудиту.*

Для досягнення мети проаналізовано підходи до класифікації IoT-пристроїв, виявлення вразливостей, аналізу аномальної активності та оцінювання ризиків.

Розроблено модель формування контекстно-ризикового профілю пристрою за результатами інтелектуально-контекстної класифікації. Удосконалено метод оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані з урахуванням показника ризику прихованої компрометації BackdoorRisk.

Визначено підхід до побудови інформаційної технології для узгодженого застосування моделі та методу. Запропоновані рішення перевірено з використанням відкритих наборів даних з безпеки IoT і програмно сформованих контекстно-ризикових сценаріїв.

Наукова новизна одержаних результатів полягає в такому:

- *Вперше розроблено модель побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Модель передбачає класифікацію пристрою за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Результати класифікації за кожним критерієм зберігаються*

в профілі без зведення до одного числового показника. Сформований профіль використовується разом із даними про поточний стан безпеки для визначення та інтерпретації параметрів оцінювання ризику.

- *Удосконалено метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані.* Метод передбачає спільне врахування семи вхідних параметрів: критичності активу, рівня загрози, рівня вразливості, можливостей потенційного порушника, імовірності реалізації загрози, тяжкості її наслідків та попередньо сформованого показника ризику прихованої компрометації BackdoorRisk. Параметри, що залежать від контексту, уточнюються з урахуванням профілю пристрою та даних про поточний стан безпеки. Показник BackdoorRisk надходить до системи як окремий вхідний параметр. Функції належності й база нечітких правил дають змогу визначити інтегральний показник RiskLevel та пояснити результат через вхідні параметри і правила виведення.
- *Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ.* На відміну від відокремленого застосування класифікації пристроїв та оцінювання ризиків, підхід передбачає використання контекстно-ризикового профілю пристрою разом із даними про поточний стан безпеки для формування вхідних параметрів нечіткого оцінювання. Це забезпечує узгоджене застосування розробленої моделі й удосконаленого методу, а також оновлення оцінки ризику в разі зміни характеристик пристрою або стану середовища.

На основі зазначеного підходу створено інформаційну технологію оцінювання ризиків інформаційної безпеки IoT-середовищ. У ній передбачено послідовне збирання й опрацювання даних, класифікацію IoT-пристроїв, формування контекстно-ризикових профілів, оцінювання ризиків та підготовку рекомендацій щодо заходів захисту. Результатом оцінювання є показник RiskLevel і відповідна категорія ризику.



*Практичне значення одержаних результатів* полягає у програмній реалізації модуля оцінювання ризиків інформаційної безпеки IoT-середовищ та окремої експериментальної процедури класифікації мережевих подій. Модуль реалізовано в середовищі MATLAB із використанням Fuzzy Logic Toolbox. Він обробляє сім попередньо сформованих вхідних параметрів, виконує нечітке логічне виведення типу Мамдані та визначає показник RiskLevel і відповідну категорію ризику. Експериментальну класифікацію мережевих подій досліджено окремо як засіб одержання відомостей про активність в IoT-середовищі.

*Впровадження результатів.* Результати дисертаційного дослідження впроваджено у практичну діяльність ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС» і ТОВ «АТРІЯ КОМПАНІ» для аналізу стану інформаційної безпеки, оцінювання ризиків та аналізу аномальної мережевої активності. Окремі результати використовуються в освітньому процесі Національного університету «Чернігівська політехніка» під час підготовки фахівців з кібербезпеки та комп'ютерних наук.

Одержані результати дають змогу формувати оцінку ризику з урахуванням характеристик IoT-пристрою, його контекстно-ризикового профілю та поточного стану безпеки. Визначений у роботі підхід до побудови інформаційної технології встановлює порядок спільного застосування розробленої моделі й удосконаленого методу в процесі аудиту IoT-середовищ.

*Ключові слова:* Інтернет речей, IoT-середовище, інформаційна безпека, контекстно-адаптивне оцінювання ризиків, інтелектуально-контекстна класифікація, нечітке логічне виведення, ризик прихованої компрометації, інформаційна технологія, аудит інформаційної безпеки.

## ABSTRACT

*Pidlisnyi Yurii.* Methods and Models for Context-Adaptive Information Security Risk Assessment in IoT Environments. – Qualifying scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 122 – “Computer Science”. – Chernihiv Polytechnic National University, Ministry of Education and Science of Ukraine, Chernihiv, 2026.

*Relevance of the research.* The development of the Internet of Things (IoT), cyber-physical systems, edge computing, and the Industrial Internet of Things (IIoT) is accompanied by increasing complexity in modern information and communication systems. IoT environments bring together devices with different purposes, computing capabilities, and communication protocols. Their composition, configuration, and connections between components may change during operation. At the same time, the range of cyber threats capable of affecting both individual devices and the environment as a whole continues to grow.

Under these conditions, information security risk depends on more than the characteristics of threats and vulnerabilities. The functional role of a device, its operating conditions, its connections with other components, and the possible consequences of disruptions to their operation are also important. Risk assessment is further complicated by incomplete input data and uncertainty in individual parameters. Hidden compromise may remain undetected when analysis is limited to known vulnerabilities and readily observable anomalies.

An analysis of scientific research has shown that IoT device classification, vulnerability detection, network activity analysis, and risk assessment are generally treated as separate tasks. As a result, information about device characteristics and the current state of the environment is not always used consistently when determining the level of risk. This creates a need for methods and models that account for the operating context of devices and enable assessment under conditions of incomplete and uncertain data.

The dissertation addresses the scientific problem of developing and improving methods and models for context-adaptive information security risk assessment in IoT environments during security audits. The proposed solution combines intelligent context-aware device classification, the formation of contextual risk profiles, and fuzzy risk assessment. The risk level is also determined with consideration of a previously calculated hidden compromise risk indicator.

*The aim of the research* is to develop and improve methods and models for context-adaptive information security risk assessment in IoT environments that account for device characteristics, operating conditions, and the current security state and can be used during security audits.

To achieve this aim, approaches to IoT device classification, vulnerability detection, anomalous activity analysis, and risk assessment were analyzed.

A model for forming a device's contextual risk profile based on the results of intelligent context-aware classification was developed. A risk assessment method based on Mamdani fuzzy inference was improved by incorporating the hidden compromise risk indicator, BackdoorRisk

An approach to building an information technology for the coordinated use of the model and method was defined. The proposed solutions were evaluated using open IoT security datasets and programmatically generated contextual risk scenarios.

The scientific novelty of the results is as follows:

- *A model for forming an IoT device's contextual risk profile based on the results of intelligent context-aware classification was developed for the first time.* The model classifies a device according to five criteria: its level of embedded intelligence, security characteristics, interaction architecture, functional context, and the dynamic nature of the environment. The classification results for each criterion are retained in the profile without being reduced to a single numerical value. The resulting profile is used together with data on the current security state to determine and interpret risk assessment parameters.
- *A method for context-adaptive information security risk assessment in IoT environments based on Mamdani fuzzy inference was improved.* The

method jointly considers seven input parameters: asset criticality, threat level, vulnerability level, attacker capability, likelihood of threat occurrence, severity of impact, and the previously calculated hidden compromise risk indicator, BackdoorRisk. Context-dependent parameters are refined using the device profile and data on the current security state. BackdoorRisk is supplied to the system as a separate input parameter. The membership functions and fuzzy rule base make it possible to determine the overall RiskLevel value and explain the result in terms of the input parameters and inference rules.

- *The approach to building an information technology for information security risk assessment in IoT environments was further developed.* The approach uses a device's contextual risk profile together with data on its current security state to form the input parameters for fuzzy risk assessment. This enables the coordinated use of the developed model and the improved method, as well as the reassessment of risk when device characteristics or the state of the environment change.

Based on this approach, an information technology for information security risk assessment in IoT environments was created. It provides for a sequence of data collection and processing, IoT device classification, contextual risk profile formation, risk assessment, and preparation of recommendations on security measures. The assessment produces a RiskLevel value and a corresponding risk category.

*The practical significance of the results* lies in the software implementation of an information security risk assessment module for IoT environments and a separate experimental procedure for classifying network events. The module was implemented in MATLAB using the Fuzzy Logic Toolbox. It processes seven previously calculated input parameters, performs Mamdani fuzzy inference, and determines the RiskLevel value and corresponding risk category. The experimental classification of network events was studied separately as a means of obtaining information about activity in an IoT environment.

*Implementation of the results.* The results of the dissertation research have been implemented in the operations of LUMIERE ELECTRO LLC, ARKADA

FINANCE LLC, and ATRIYA COMPANY LLC for information security analysis, risk assessment, and anomalous network activity analysis. Some of the results are also used in the educational process at Chernihiv Polytechnic National University in the training of cybersecurity and computer science specialists.

The results make it possible to assess risk with consideration of an IoT device's characteristics, its contextual risk profile, and the current security state. The proposed approach to building the information technology establishes a procedure for the combined use of the developed model and improved method during IoT security audits.

*Keywords:* Internet of Things, IoT environment, information security, context-adaptive risk assessment, intelligent context-aware classification, fuzzy inference, hidden compromise risk, information technology, information security audit.

## СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

### Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Pidlisnyi Yuriy, Intelligent-Contextual Model for the Classification of Internet of Things Environments // *[Central Ukrainian Scientific Bulletin Technical Sciences]*. 2025. № 12(43). С. 20–30.  
[https://doi.org/10.32515/2664-262X.2025.12\(43\).1.20-30](https://doi.org/10.32515/2664-262X.2025.12(43).1.20-30).
2. Mariia KAPUSTIAN, Yurii PIDLISNYI, Mykhailo SHELEST, Methods of Hiding Data in Computer Networks: From Classics to IoT and AI // *[Computer systems and information technologies]*. 2025. № 4–3. DOI: <https://doi.org/10.31891/csit-2025-4-3>.
3. Pidlisnyi Yuriy, Fuzzy Logic in IoT Security Risk Assessment: Rule Construction and Implementation // *[Computer Science and Engineering]*. 2025. № 3(41). С. 237–253. DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-237-253](https://doi.org/10.25140/2411-5363-2025-3(41)-237-253).
4. Pidlisnyi Yuriy , Audit of IoT Networks: Assessing Vulnerabilities and Protecting Against Cyber Attacks // *[Computer Science and Engineering]*. 2025. № 1(39). С. 170–183. DOI: [https://doi.org/10.25140/2411-5363-2025-1\(39\)-170-183](https://doi.org/10.25140/2411-5363-2025-1(39)-170-183).
5. Pidlisnyi Yuriy , Possible Ways to Improve Privacy in IoT Networks // *[Central Ukrainian Scientific Bulletin Technical Sciences]*. 2025. № 11(42). С. 46–55. DOI: [https://doi.org/10.32515/2664-262X.2025.11\(42\).1.46-55](https://doi.org/10.32515/2664-262X.2025.11(42).1.46-55).

### Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Підлісний Юрій, Використання алгоритмічних та технічних аспектів кібербезпеки в мережі IoT / Ю.І. Підлісний // Кібербезпека в сучасному світі: актуальні виклики : матеріали конференції. – Одеса, 2024. – С. 63–64.
2. Підлісний Юрій, Технології захисту приватності в мережі IoT / Ю.І. Підлісний// Міжвідомчий міжрегіональний семінар наукової ради НАН України «Технічні засоби захисту інформації». – *[Київ]*, [2025]. С.58-60.

3. Підлісний Юрій, Мультиагентні системи для виявлення та нейтралізації кіберзагроз в IoT / Ю. І. Підлісний // Юність науки – 2025 : матеріали всеукраїнської наукової конференції молодих учених. – Чернігів, 2025. – С. 1124–1125.
4. Підлісний Юрій, Використання NetLogo для моделювання кібератак на IoT-системи / Ю.І. Підлісний // Безпека інформаційних технологій : матеріали XIV Міжнародної науково-технічної конференції (ITSec-2025), 22–24 травня 2025 р. – Тернопіль, 2025. – С. 150–152.
5. Yuriy PIDLISNYI, Mykhailo SHELEST, Detection of Hidden Threats in IoT Systems Based on Kleptaudit and Fuzzy Risk Assessment / Yuriy PIDLISNYI, Mykhailo SHELEST// Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей : матеріали V Міжнародної науково-практичної конференції (TTSIT-2026). – [Київ], 2026. – С. 11–15.
6. Підлісний Юрій, Шелест Михайло, Застосування нечітких продукційних правил для контекстно-довірчого оцінювання кіберризиків у середовищі Інтернету речей/ Ю.І. Підлісний, М.Є. Шелест // Безпека інформаційних технологій : матеріали XV Міжнародної науково-технічної конференції (ITSec-2025), 27–29 травня 2026 р. – Тернопіль, 2026. – С. 29–31.

## ЗМІСТ

|                                                                                                                                             |     |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ВСТУП.....                                                                                                                                  | 15  |
| ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....                                                                                                              | 26  |
| РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІОТ-СЕРЕДОВИЩ.....                                      | 27  |
| 1.1. АНАЛІЗ СУЧАСНОГО СТАНУ НАУКОВОЇ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СЕРЕДОВИЩ ІНТЕРНЕТУ РЕЧЕЙ.....                                      | 28  |
| 1.1.1. Архітектурні засади забезпечення кібербезпеки IoT-середовищ.....                                                                     | 29  |
| 1.1.2. Методи виявлення вразливостей та аналізу кіберзагроз.....                                                                            | 30  |
| 1.1.3. Міжнародні стандарти та методології оцінювання кіберризиків.....                                                                     | 33  |
| 1.1.4. Застосування методів штучного інтелекту в кібербезпеці IoT.....                                                                      | 34  |
| 1.1.5. Узагальнення сучасного стану досліджень та визначення невирішеної наукової задачі.....                                               | 36  |
| 1.2. ПОНЯТТЯ ВРАЗЛИВОСТІ ТА КІБЕРЗАГРОЗИ В ІОТ-СЕРЕДОВИЩАХ.....                                                                             | 38  |
| 1.3. КЛАСИФІКАЦІЯ КІБЕРАТАК НА ІОТ.....                                                                                                     | 40  |
| 1.4. ОСОБЛИВОСТІ ЗАГРОЗ У ДИНАМІЧНИХ ТА ГЕТЕРОГЕННИХ ІОТ-МЕРЕЖАХ.....                                                                       | 43  |
| 1.5. СУЧАСНІ МЕТОДИ МОНІТОРИНГУ ТА АНАЛІЗУ СТАНУ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ.....                                                                 | 45  |
| 1.5.1. Архітектурні підходи до побудови систем виявлення атак.....                                                                          | 46  |
| 1.5.2. Еволюція методів виявлення атак.....                                                                                                 | 47  |
| 1.5.3. Аналіз обмежень сучасних підходів.....                                                                                               | 49  |
| 1.5.4. Практичні аспекти реалізації та оцінювання сучасних методів виявлення атак.....                                                      | 51  |
| 1.6. ЗАГРОЗИ КОНФІДЕНЦІЙНОСТІ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ ІОТ-СЕРЕДОВИЩ.....                                                                     | 53  |
| 1.6.1. Загрози конфіденційності під час оброблення даних у IoT.....                                                                         | 53  |
| 1.6.2. Сучасні методи забезпечення конфіденційності даних.....                                                                              | 55  |
| 1.6.3. Баланс між конфіденційністю, безпекою та ефективністю IoT-систем.....                                                                | 57  |
| 1.7. ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ.....                                                                                                     | 59  |
| Висновки розділу 1.....                                                                                                                     | 61  |
| РОЗДІЛ 2. МОДЕЛЬ ФОРМУВАННЯ КОНТЕКСТНО-РИЗИКОВОГО ПРОФІЛЮ ІОТ-ПРИСТРОЮ ТА МЕТОД ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ..... | 63  |
| 2.1. МОДЕЛЬ ФОРМУВАННЯ КОНТЕКСТНО-РИЗИКОВОГО ПРОФІЛЮ ІОТ-ПРИСТРОЮ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНО-КОНТЕКСТНОЇ КЛАСИФІКАЦІЇ.....                    | 63  |
| 2.1.1. Аналіз сучасних підходів та обмежень класифікації IoT.....                                                                           | 64  |
| 2.1.2. Формування системи критеріїв інтелектуально-контекстної класифікації IoT-пристроїв.....                                              | 65  |
| 2.1.3. Формалізація моделі інтелектуально-контекстної класифікації.....                                                                     | 68  |
| 2.1.4. Порівняльний аналіз традиційних та інтелектуально-контекстних підходів.....                                                          | 71  |
| 2.2. ФОРМАЛІЗАЦІЯ КРИТЕРІЇВ ВРАЗЛИВОСТЕЙ ТА РИЗИКІВ БЕЗПЕКИ.....                                                                            | 73  |
| 2.2.1. Ідентифікація типових вразливостей IoT-середовищ.....                                                                                | 73  |
| 2.2.2. Визначення зв'язку між вразливістю, активом і загрозою.....                                                                          | 75  |
| 2.2.3. Формалізація критеріїв оцінювання ризику згідно з ISO/IEC 27005, EBIOS та ENISA Threat Landscape.....                                | 78  |
| 2.2.4. Побудова структури входних параметрів для моделі нечіткого оцінювання ризиків.....                                                   | 80  |
| 2.3. МЕТОД КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ НА ОСНОВІ НЕЧІТКОГО ЛОГІЧНОГО ВИВЕДЕННЯ.....                                           | 83  |
| 2.3.1. Визначення лінгвістичних змінних та функцій належності.....                                                                          | 84  |
| 2.3.2. Побудова та оптимізація бази нечітких продукційних правил для аудиту безпеки IoT.....                                                | 88  |
| 2.3.3. Програмна реалізація системи нечіткого висновку типу Mamdani.....                                                                    | 92  |
| 2.3.4. Аналіз роботи моделі на тестових сценаріях.....                                                                                      | 95  |
| 2.4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ.....                                           | 98  |
| 2.4.1. Структура інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ.....                              | 98  |
| 2.4.2. Алгоритм функціонування інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ.....                | 101 |
| 2.4.3. Програмна реалізація інформаційної технології.....                                                                                   | 103 |
| Висновки розділу 2.....                                                                                                                     | 104 |
| РОЗДІЛ 3. АРХІТЕКТУРА ТА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ.....           | 107 |



|                                                                                                                                             |            |
|---------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>3.1. ПРИНЦИПИ ПОБУДОВИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ</b>                      | <b>107</b> |
| 3.1.1. <i>Передумови побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ</i>                  | 108        |
| 3.1.2. <i>Порівняльний аналіз підходів до оцінювання ризиків безпеки ІоТ-середовищ</i>                                                      | 108        |
| 3.1.3. <i>Принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ</i>                    | 110        |
| <b>3.2. КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ</b>                              | <b>112</b> |
| 3.2.1. <i>Концептуальна модель інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ</i>                 | 113        |
| 3.2.2. <i>Інформаційно-аналітичний процес функціонування інформаційної технології</i>                                                       | 114        |
| <b>3.3. АРХІТЕКТУРА РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ</b>                 | <b>116</b> |
| 3.3.1. <i>Багаторівнева архітектура ІоТ-середовища для контекстно-адаптивного оцінювання ризиків безпеки</i>                                | 117        |
| 3.3.2. <i>Функціональна архітектура інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ</i>            | 119        |
| 3.3.3. <i>Архітектура інформаційної взаємодії компонентів інформаційної технології</i>                                                      | 123        |
| 3.3.4. <i>Архітектура програмного забезпечення інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ</i> | 124        |
| <b>ВИСНОВКИ РОЗДІЛУ 3</b>                                                                                                                   | <b>127</b> |
| <b>РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА РОЗРОБЛЕНИХ МЕТОДІВ І МОДЕЛЕЙ</b>                                           | <b>129</b> |
| <b>4.1. МЕТОДИКА ЕКСПЕРИМЕНТАЛЬНОЇ ПЕРЕВІРКИ</b>                                                                                            | <b>130</b> |
| 4.1.1. <i>Постановка задач експериментів</i>                                                                                                | 130        |
| 4.1.2. <i>Обґрунтування вибору програмного середовища експериментальних досліджень</i>                                                      | 133        |
| 4.1.3. <i>Опис експериментального ІоТ-середовища</i>                                                                                        | 134        |
| <b>4.2. ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ</b>                                                           | <b>138</b> |
| 4.2.1. <i>Реалізація нечіткої моделі</i>                                                                                                    | 139        |
| 4.2.2. <i>Формування бази продукційних правил</i>                                                                                           | 140        |
| 4.2.3. <i>Валідація програмної реалізації</i>                                                                                               | 142        |
| <b>4.3. ЕКСПЕРИМЕНТАЛЬНЕ ОЦІНЮВАННЯ МЕТОДІВ КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ ПОДІЙ НА ВІДКРИТИХ НАБОРАХ ДАНИХ</b>                                     | <b>145</b> |
| 4.3.1. <i>Опис датасетів</i>                                                                                                                | 146        |
| 4.3.2. <i>Підготовка уніфікованої експериментальної вибірки</i>                                                                             | 148        |
| 4.3.3. <i>Методи та метрики класифікації мережеских подій</i>                                                                               | 150        |
| 4.3.4. <i>Результати класифікації мережеских подій</i>                                                                                      | 151        |
| <b>4.4. ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА МЕТОДУ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ У ЗМОДЕЛЬОВАНОМУ ІОТ-СЕРЕДОВИЩІ</b>                     | <b>152</b> |
| 4.4.1. <i>Формування контекстно-ризикових сценаріїв</i>                                                                                     | 152        |
| 4.4.2. <i>Функціональна перевірка FIS-моделі на контрольних сценаріях</i>                                                                   | 154        |
| 4.4.3. <i>Кількісна валідація FIS-моделі на незалежній сценарній вибірці</i>                                                                | 155        |
| 4.4.4. <i>Порівняння FIS-моделі з базовими моделями оцінювання ризику</i>                                                                   | 156        |
| 4.4.5. <i>Експериментальне оцінювання впливу контекстно-ризикового профілю на формування RiskLevel</i>                                      | 158        |
| 4.4.6. <i>Дослідження впливу параметра BackdoorRisk на формування RiskLevel</i>                                                             | 161        |
| <b>4.5. ОЦІНЮВАННЯ ОБЧИСЛЮВАЛЬНОЇ ЕФЕКТИВНОСТІ ТА СТІЙКОСТІ РОЗРОБЛЕНИХ МЕТОДІВ І МОДЕЛЕЙ</b>                                               | <b>163</b> |
| 4.5.1. <i>Аналіз часових характеристик програмної реалізації</i>                                                                            | 163        |
| 4.5.2. <i>Аналіз масштабованості програмної реалізації</i>                                                                                  | 165        |
| 4.5.3. <i>Аналіз стійкості FIS-моделі до неповноти вхідних даних</i>                                                                        | 166        |
| 4.5.4. <i>Переваги та обмеження розроблених методів і моделей</i>                                                                           | 168        |
| <b>ВИСНОВКИ РОЗДІЛУ 4</b>                                                                                                                   | <b>171</b> |
| <b>ВИСНОВКИ</b>                                                                                                                             | <b>174</b> |
| <b>ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ</b>                                                                                                          | <b>178</b> |
| <b>ДОДАТКИ</b>                                                                                                                              | <b>189</b> |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Додаток А. Список публікацій здобувача за темою дисертації..... | 189 |
| Додаток Б. ....                                                 | 190 |
| Додаток В. ....                                                 | 197 |
| Додаток Г. Акти впровадження та довідки.....                    | 203 |

## ВСТУП

*Актуальність теми дослідження.* Стрімкий розвиток цифрових технологій, широке впровадження концепцій Інтернету речей (Internet of Things, IoT), кіберфізичних систем, промислового Інтернету речей (Industrial Internet of Things, IIoT), хмарних та периферійних обчислень суттєво змінює сучасну інформаційну інфраструктуру. Мережі Інтернету речей інтегрують велику кількість взаємопов'язаних пристроїв, сенсорів, виконавчих механізмів і сервісів, що функціонують у різноманітних сферах – промисловості, енергетиці, транспорті, медицині, критичній інфраструктурі та системах «розумного» міста. Такі середовища характеризуються високою динамічністю, гетерогенністю, масштабованістю та складною структурою інформаційних взаємодій.

Однією з ключових проблем безпеки IoT є складність інтерпретації подій безпеки з урахуванням функціонального контексту пристроїв та їхньої ролі в архітектурі системи. Унаслідок цього однакові за формальними ознаками інциденти можуть мати різний рівень критичності та потребувати різних підходів до реагування. Відсутність механізмів контекстного оцінювання призводить до зниження точності пріоритизації подій і ускладнює прийняття обґрунтованих рішень щодо реагування на загрози.

Поширення IoT-пристроїв супроводжується не лише появою нових можливостей для автоматизації та цифрової трансформації, але й суттєвим розширенням поверхні атак. Поряд із традиційними кіберзагрозами виникають нові їх різновиди, зокрема багаторівневі атаки, атаки на протоколи обміну даними, а також приховані механізми впливу у вигляді бекдорів і клептографічних закладок у прошивках та криптографічних компонентах.

Особливу небезпеку становить те, що такі загрози можуть тривалий час залишатися непоміченими та створювати критичні ризики для промислових, транспортних, медичних та інших кіберфізичних систем.

Складність їх виявлення зумовлена здатністю функціонувати в межах штатної логіки роботи системи без прояву характерних сигнатур або класичних аномалій. За таких умов використання виключно сигнатурного чи поведінкового аналізу часто виявляється недостатнім, що обумовлює необхідність застосування

контекстно-орієнтованих підходів до оцінювання стану безпеки IoT-пристроїв та особливостей їхньої взаємодії в мережі.

Проблемам забезпечення безпеки IoT-середовищ, виявлення вразливостей, аналізу мережевого трафіку та побудови інтелектуальних систем аудиту присвячено значну кількість наукових праць. У дослідженнях A. Al-Fuqaha, M. Ferrag, S. Sicari, R. Hassan, P. Kairouz, M. Gupta, Z. Hou, A. Cortés та інших науковців розглядаються підходи до побудови безпечних IoT-архітектур, використання розподілених обчислень, технологій edge- та fog-computing, а також інтелектуальних методів аналізу даних у середовищах Інтернету речей.

Окремий напрям досліджень пов'язаний із системами виявлення вторгнень (IDS/IPS), що ґрунтуються на сигнатурному та поведінковому аналізі мережевого трафіку. Результати, представлені у працях M. Ferrag, S. Sicari, R. Hassan, M. Gupta та інших авторів, підтверджують ефективність таких підходів під час виявлення відомих типів атак і типових аномалій. Водночас їхня результативність суттєво знижується в умовах динамічної зміни параметрів IoT-середовищ, обмеженості ресурсів кінцевих пристроїв та появи нових, раніше невідомих загроз.

Значного поширення останніми роками набули методи машинного навчання та штучного інтелекту, які використовуються для виявлення аномалій, класифікації IoT-пристроїв і аналізу поведінки мережевого трафіку. Як показано у роботах P. Kairouz, Z. Hou, A. Cortés, M. Gupta та інших дослідників, їх застосування дає змогу підвищити точність виявлення атак і частково автоматизувати процес аналізу даних.

Разом із тим більшість запропонованих рішень характеризується недостатньою інтерпретованістю результатів, високою залежністю від якості навчальних вибірок та обмеженим урахуванням контексту функціонування пристроїв, що ускладнює їх практичне використання в динамічних IoT-середовищах.

Перспективним напрямом є застосування технологій Edge- та Fog-computing, які передбачають перенесення окремих функцій аналізу безпеки ближче до джерел формування даних. Такий підхід дозволяє зменшити затримки під час оброблення інформації та підвищити оперативність реагування на

інциденти. Проте він не забезпечує комплексного оцінювання ризиків та не враховує повною мірою приховані механізми впливу, характерні для гетерогенних IoT-середовищ.

Важливе місце у забезпеченні інформаційної безпеки посідають методології оцінювання ризиків, зокрема CVSS, OCTAVE, EBIOS та ISO/IEC 27005. Зазначені підходи забезпечують формалізацію процесів аналізу вразливостей та оцінювання ризиків, однак переважно орієнтовані на статичні моделі загроз. Унаслідок цього вони недостатньо враховують динамічність IoT-середовищ, невизначеність параметрів мережевої взаємодії, контекст функціонування пристроїв та зміну поведінкових характеристик вузлів системи.

Наявні підходи до виявлення загроз і аналізу безпеки демонструють високу ефективність під час виявлення відомих атак, однак не забезпечують повноцінного оцінювання ризиків у динамічних IoT-середовищах. Основною причиною цього є недостатнє врахування функціонального контексту пристроїв, взаємозв'язків між ними та можливості реалізації прихованих механізмів впливу.

Додаткову складність створює те, що оцінювання ризиків у IoT-середовищах відбувається в умовах невизначеності та неповноти вхідних даних. Такі характеристики, як рівень довіри до пристрою, критичність його функцій, імовірність реалізації загрози чи потенційний вплив інциденту, часто мають якісний або експертний характер і не можуть бути однозначно описані жорсткими числовими межами. Це обмежує можливості традиційних порогових моделей та обумовлює доцільність використання методів нечіткої логіки для формалізації експертних знань і забезпечення інтерпретованого оцінювання ризиків.

Попри значну кількість досліджень у сфері безпеки Інтернету речей, проблема комплексного оцінювання стану безпеки IoT-середовищ залишається актуальною. Насамперед це стосується одночасного врахування функціонального контексту пристроїв, поведінкових і мережевих аномалій, ознак прихованої компрометації та невизначеності параметрів ризику. Існуючі підходи здебільшого розв'язують ці завдання окремо, що обмежує можливості контекстно-адаптивного оцінювання ризиків і знижує обґрунтованість прийняття рішень під час аудиту безпеки.

У зв'язку з цим актуальним науковим завданням є розроблення моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням цього профілю й поточного стану безпеки в процесі аудиту.

На відміну від відомих методів і моделей оцінювання ризиків, запропоновані рішення передбачають використання результатів інтелектуально-контекстної класифікації IoT-пристроїв, сформованих контекстно-ризикових профілів та взаємопов'язаних параметрів критичності активу, рівня загрози, рівня вразливості, можливостей потенційного порушника, імовірності реалізації загрози, тяжкості наслідків і ризику прихованої компрометації. Це забезпечує формування інтегрального показника RiskLevel з урахуванням функціональної ролі пристроїв та умов їх експлуатації.

На основі розробленої моделі формування контекстно-ризикового профілю IoT-пристрою та удосконаленого методу оцінювання ризиків створено інформаційну технологію, яка забезпечує їх узгоджене застосування в межах єдиного інформаційно-аналітичного процесу аудиту IoT-середовищ. Результати оцінювання можуть використовуватися для обґрунтування пріоритетності заходів захисту.

Саме необхідність розв'язання зазначеного наукового завдання визначає актуальність теми дисертаційної роботи.

*Зв'язок роботи з науковими програмами, планами, темами.* Дисертаційну роботу виконано відповідно до основних напрямів наукової діяльності Національного університету «Чернігівська політехніка» та кафедри кібербезпеки та математичного моделювання в межах науково-дослідних робіт, присвячених розробленню методів, моделей та інформаційних технологій забезпечення кібербезпеки інформаційно-комунікаційних систем.

Основні результати дисертаційного дослідження отримано під час виконання науково-дослідних робіт: «Методологія побудови захищеного кіберпростору» (державний реєстраційний номер 0124U004485, 2024–2027 рр.); «Моделі та методи забезпечення безпеки й довіри в кіберпросторі з урахуванням клептографічних загроз» (державний реєстраційний номер 0126U001352, 2026–

2028 pp.); «Методи й моделі забезпечення цілісності даних у каналах керування БпЛА в умовах застосування засобів РЕБ» (державний реєстраційний номер 0125U001728, 2025–2026 pp.).

У межах зазначених науково-дослідних робіт автором розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації, удосконалено метод оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані та розвинуто підхід до побудови інформаційної технології їх узгодженого застосування в процесі аудиту.

Дослідження виконано з урахуванням сучасних міжнародних підходів до управління ризиками інформаційної безпеки та аудиту кібербезпеки, визначених стандартом ISO/IEC 27005, рекомендаціями ENISA Threat Landscape і методологією EBIOS Risk Manager.

*Метою дослідження є розроблення моделі побудови контекстно-ризикового профілю IoT-пристрою та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням характеристик пристрою, поточного стану безпеки й попередньо сформованого показника ризику прихованої компрометації в процесі аудиту.*

Досягнення поставленої мети потребує узгодженого використання відомостей про характеристики IoT-пристроїв, умови їх функціонування та поточний стан безпеки. Це зумовлено гетерогенністю й динамічністю IoT-середовищ, а також невизначеністю окремих параметрів оцінювання ризику. Тому дослідження охоплює формування контекстно-ризикових профілів пристроїв, оцінювання ризиків на їх основі та використання результатів оцінювання під час аудиту інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити такі взаємопов'язані наукові завдання дослідження:

1. Провести аналіз сучасного стану методів і моделей аудиту безпеки IoT-середовищ, виявлення вразливостей, оцінювання ризиків, аналізу аномальної активності та підтримки прийняття рішень, визначити їх переваги, обмеження та невирішені наукові питання.

2. Розробити модель побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища.
3. Удосконалити метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані шляхом формування системи взаємопов'язаних параметрів оцінювання ризику, урахування контекстно-ризикового профілю IoT-пристрою та введення попередньо сформованого показника BackdoorRisk.
4. Розвинути підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ, визначити її архітектуру, склад компонентів, інформаційні потоки та послідовність їх взаємодії в процесі аудиту.
5. Реалізувати програмний прототип ключових компонентів інформаційної технології та провести експериментальну перевірку працездатності й результативності розроблених та удосконалених методів і моделей на основі змодельованих сценаріїв і відкритих наборів даних IoT-безпеки.

*Об'єктом дослідження* є процеси оцінювання ризиків інформаційної безпеки IoT-середовищ під час аудиту в умовах гетерогенності компонентів, динамічності структури й функціонування та невизначеності параметрів середовища.

*Предметом дослідження* є модель побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації, метод оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані з урахуванням попередньо сформованого показника ризику прихованої компрометації, а також підхід до побудови інформаційної технології, що забезпечує їх узгоджене застосування в процесі аудиту.

*Методи дослідження.* Для досягнення поставленої мети використано комплекс взаємопов'язаних методів дослідження.



Методи системного аналізу, теорії складних систем та інформаційного моделювання використано для дослідження процесів аудиту безпеки середовищ Інтернету речей, визначення взаємозв'язків між їх компонентами та формування концептуальних засад контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ.

Методи аналізу ризиків, теорії нечітких множин і нечіткого логічного виведення застосовано під час розроблення та удосконалення моделей і методів контекстно-адаптивного оцінювання ризиків в умовах неповноти та невизначеності вхідних даних.

Методи інтелектуального аналізу даних, контекстного аналізу та аналізу поведінкових характеристик використано для інтелектуально-контекстної класифікації IoT-пристроїв.

Методи математичного та імітаційного моделювання використано для дослідження розроблених моделей і методів, моделювання сценаріїв функціонування IoT-середовищ та експериментальної перевірки запропонованих рішень.

Методи програмного моделювання використано для реалізації розроблених методів і моделей, їх узгодженого застосування в інформаційній технології контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ та створення програмного прототипу.

Для оцінювання результативності розроблених методів і моделей застосовано методи статистичного аналізу та порівняльного оцінювання ефективності.

*Наукова новизна одержаних результатів* полягає в розробленні моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації, удосконаленні методу оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані та подальшому розвитку підходу до побудови інформаційної технології, що забезпечує узгоджене застосування моделі й методу в процесі аудиту.

Вперше:

- *розроблено модель побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації.* Модель передбачає класифікацію пристрою за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Результати класифікації за кожним критерієм зберігаються в профілі без зведення до одного числового показника. Сформований профіль використовується разом із даними про поточний стан безпеки для визначення та інтерпретації параметрів оцінювання ризику.

Удосконалено:

- *метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані.* Метод передбачає спільне врахування семи вхідних параметрів: критичності активу, рівня загрози, рівня вразливості, можливостей потенційного порушника, імовірності реалізації загрози, тяжкості її наслідків та попередньо сформованого показника ризику прихованої компрометації BackdoorRisk. Параметри, що залежать від контексту, уточнюються з урахуванням профілю пристрою та даних про поточний стан безпеки. BackdoorRisk надходить до системи як окремий вхідний параметр. Функції належності й база нечітких правил дають змогу визначити інтегральний показник RiskLevel та пояснити результат через вхідні параметри і правила виведення.

Набуло подальшого розвитку:

- *підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ.* Його особливістю є використання контекстно-ризикових профілів пристроїв разом із даними про поточний стан безпеки для формування вхідних параметрів нечіткого оцінювання ризиків. На цій основі визначено архітектуру технології, склад її компонентів та інформаційні потоки

між ними. У разі зміни характеристик пристрою або стану середовища передбачено оновлення вхідних параметрів і повторне визначення рівня ризику.

*Практичне значення одержаних результатів* полягає у створенні інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ, результати застосування якої можуть використовуватися під час аудиту для обґрунтування пріоритетності заходів захисту. У середовищі MATLAB із використанням Fuzzy Logic Toolbox реалізовано програмний модуль нечіткого оцінювання ризиків. Модуль обробляє сім попередньо сформованих вхідних параметрів, визначає показник RiskLevel і відповідну категорію ризику.

Розроблені методи та моделі можуть бути використані:

- 1) під час проєктування та розвитку систем аудиту безпеки середовищ Інтернету речей;
- 2) у діяльності центрів моніторингу кібербезпеки (SOC) для підтримки процесів оцінювання ризиків та прийняття рішень;
- 3) у процесах оцінювання ризиків та аудиту інформаційної безпеки об'єктів критичної інформаційної інфраструктури;
- 4) під час розроблення програмного забезпечення для оцінювання стану кібербезпеки складних інформаційно-комунікаційних систем;
- 5) у навчальному процесі закладів вищої освіти під час викладання дисциплін, пов'язаних із кібербезпекою, оцінюванням ризиків та безпекою IoT.

Результати дисертаційного дослідження впроваджені у діяльність ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС» та ТОВ «АТРІЯ КОМПАНІ» під час виконання робіт з аудиту безпеки середовищ Інтернету речей, аналізу захищеності мережевої інфраструктури, оцінювання ризиків інформаційної безпеки та виявлення аномальної мережевої активності, що підтверджується відповідними актами впровадження.

Окремі результати використано в освітньому процесі Національного університету «Чернігівська політехніка» під час викладання дисциплін «Безпека ОС» та «Системне програмування».

*Особистий внесок здобувача* полягає у самостійному виконанні всіх основних етапів дисертаційного дослідження, зокрема аналізі сучасного стану проблеми, формуванні наукових засад контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ, розробленні моделі інтелектуально-контекстної класифікації IoT-пристроїв, удосконаленні методу нечіткого оцінювання ризиків та структурно-функціональної організації відповідної інформаційної технології.

Усі наукові результати, що виносяться на захист і сформульовані в дисертації як положення наукової новизни, отримано автором особисто. У наукових працях, опублікованих у співавторстві, автору належать розроблення моделі інтелектуально-контекстної класифікації IoT-пристроїв, удосконалення методу контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ та розроблення структурно-функціональної організації відповідної інформаційної технології.

*Апробація результатів дисертації.* Основні положення та результати дисертаційної роботи доповідалися й обговорювалися на міжнародних та всеукраїнських наукових і науково-практичних конференціях, семінарах та круглих столах, зокрема: XX Міжнародній науково-практичній конференції «Математичне та комп'ютерне моделювання (MODS)» (м.Чернігів, 2025 р.); V Міжнародній науково-практичній конференції «ТТСІТ-2026» (м.Київ, 24–25 березня 2026 р.); Всеукраїнській науковій конференції молодих учених «Юність науки – 2025» (м.Чернігів, 2025 р.); XIV Міжнародній науково-технічній конференції «ITSec-2025» (м. Тернопіль, 2025 р.), XV Міжнародній науково-технічній конференції «ITSec-2026» (м. Тернопіль, 2026 р.). За результатами апробації окремі положення дисертаційної роботи були уточнені та вдосконалені, що знайшло відображення в остаточній редакції дисертації.

*Публікації.* Основні результати дисертації опубліковано у 11 наукових працях, серед яких 5 статей у наукових фахових виданнях України та 6 публікацій у матеріалах наукових конференцій. У публікаціях повною мірою відображено основні наукові результати дисертаційного дослідження.

*Структура та обсяг дисертації.* Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Повний

обсяг дисертації становить 205 сторінки, із них основний текст - 164 сторінки. Робота містить 24 рисунки, 42 таблиці, список використаних джерел із 140 найменувань та 4 додатків.

## ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI -Artificial Intelligence (штучний інтелект)

DDoS - Distributed Denial of Service (розподілена атака типу «відмова в обслуговуванні»);

ENISA - European Union Agency for Cybersecurity (Агентство Європейського Союзу з кібербезпеки);

FIS -Fuzzy Inference System (система нечіткого логічного висновку);

IDS - Intrusion Detection System (система виявлення вторгнень);

IIoT - Industrial Internet of Things (промисловий Інтернет речей);

IoT - Internet of Things (Інтернет речей);

IPS - Intrusion Prevention System (система запобігання вторгненням);

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації);

MATLAB - MATrix LABoratory (середовище математичного моделювання);

MITM - Man-in-the-Middle (атака «людина посередині»);

NIST - National Institute of Standards and Technology (Національний інститут стандартів і технологій США);

SCADA - Supervisory Control and Data Acquisition (система диспетчерського керування та збору даних);

Edge computing - периферійні обчислення;

Fog computing - туманні обчислення;

## **РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІОТ-СЕРЕДОВИЩ**

Розроблення моделі формування контекстно-ризикового профілю ІоТ-пристрою, удосконалення методу оцінювання ризиків інформаційної безпеки ІоТ-середовищ і створення інформаційної технології їх узгодженого застосування потребують аналізу сучасного стану кібербезпеки ІоТ-середовищ.

Незважаючи на значну кількість наукових праць, присвячених окремим аспектам захисту ІоТ-середовищ, розвиток Інтернету речей супроводжується постійним ускладненням архітектури інформаційних систем, збільшенням кількості взаємопов'язаних пристроїв, появою нових сценаріїв їх використання та, відповідно, розширенням спектра потенційних кіберзагроз. Це обумовлює необхідність критичного аналізу сучасних наукових результатів з метою визначення рівня розробленості проблеми, виявлення існуючих обмежень та формування наукових передумов для створення нових підходів до забезпечення кібербезпеки ІоТ-середовищ.

У цьому розділі виконано комплексний аналіз сучасного стану наукових досліджень у сфері забезпечення кібербезпеки Інтернету речей, досліджено міжнародні стандарти та методичні підходи до оцінювання ризиків інформаційної безпеки ІоТ-систем, проаналізовано сучасні види вразливостей, кіберзагроз, а також методи їх виявлення та оцінювання. Проведений аналіз дозволив визначити рівень розробленості наукової проблеми, встановити основні обмеження існуючих підходів, виявити невідомі наукові задачі та сформулювати наукове підґрунтя для розроблення методів і моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки ІоТ-середовищ, що враховують гетерогенність, динамічність, функціональний контекст, невизначеність вхідних даних та ризик прихованої компрометації і становлять предмет подальших розділів дисертаційної роботи.

### **1.1. Аналіз сучасного стану наукової проблеми забезпечення кібербезпеки середовищ Інтернету речей**

Забезпечення кібербезпеки середовищ Інтернету речей належить до найбільш динамічних напрямів сучасних наукових досліджень у галузі інформаційної безпеки. Розвиток концепцій Industry 4.0, Smart City, Smart Grid, Industrial Internet of Things, Connected Healthcare та інших кіберфізичних екосистем супроводжується зростанням кількості взаємопов'язаних пристроїв і розширенням спектра інформаційних взаємодій [1, 2]. Особливості забезпечення кібербезпеки промислових і медичних IoT-систем, а також характерні для них кіберзагрози та вразливості досліджуються в сучасних наукових працях [3, 4].

На відміну від традиційних інформаційно-комунікаційних систем, IoT-середовища характеризуються високим рівнем розподіленості, неоднорідністю апаратних і програмних платформ, обмеженими обчислювальними ресурсами кінцевих пристроїв, використанням спеціалізованих комунікаційних протоколів, динамічністю конфігурації та постійною зміною складу компонентів. У таких умовах рівень кібербезпеки визначається не лише захищеністю окремих пристроїв, а й характером взаємодії між ними, станом мережевої інфраструктури, периферійних вузлів, хмарних сервісів, програмних платформ і механізмів керування.

У сучасних наукових дослідженнях сформувалося декілька основних напрямів забезпечення кібербезпеки IoT-середовищ: побудова безпечних архітектур, виявлення вразливостей програмного й апаратного забезпечення, аналіз і моделювання кіберзагроз, створення систем виявлення атак, оцінювання кіберризиків [5, 6], застосування стандартизованих підходів до аналізу й управління ризиками [7], дослідження актуальних кіберзагроз [8], застосування методів машинного навчання та штучного інтелекту.

Водночас переважна частина відомих підходів орієнтована на розв'язання окремих задач. Архітектурні моделі визначають структуру IoT-систем, засоби сканування виявляють відомі вразливості, системи моніторингу аналізують мережеву активність, методології оцінювання ризиків формалізують потенційні наслідки, а інтелектуальні моделі здійснюють класифікацію подій або виявлення



аномалій. Проте результати застосування цих засобів не завжди поєднуються в межах єдиного інформаційно-аналітичного процесу аудиту кібербезпеки.

Для системного визначення рівня розробленості наукової проблеми доцільно послідовно проаналізувати архітектурні підходи до захисту IoT, методи виявлення вразливостей і атак, міжнародні стандарти та методології оцінювання ризиків, а також можливості застосування штучного інтелекту.

### ***1.1.1. Архітектурні засади забезпечення кібербезпеки IoT-середовищ***

Архітектура IoT-системи визначає принципи взаємодії між кінцевими пристроями, мережевою інфраструктурою, периферійними вузлами, хмарними сервісами та прикладними застосунками [9, 10]. Від способу організації цих компонентів залежать межі довіри, склад поверхні атаки, можливості централізованого контролю та вибір механізмів забезпечення кібербезпеки [11].

Значний внесок у формування сучасного бачення архітектури безпечних IoT-систем зроблено в оглядових дослідженнях, присвячених аналізу моделей побудови Інтернету речей, класифікації загроз та визначенню перспективних засобів захисту. У роботах L. Babun, A. K. Sikder, A. Acar та A. S. Uluagac досліджено особливості захисту корпоративних і промислових IoT-систем, проаналізовано характерні вектори атак та проблеми масштабування засобів безпеки в багаторівневих IoT-екосистемах [12].

Окремий напрям становлять дослідження архітектур Edge Computing, Fog Computing і Cloud Computing. Концептуальні засади використання Fog Computing та перенесення обчислювальних функцій ближче до джерел формування даних розглянуто в роботах [13, 14]. Подальший розвиток цих підходів пов'язаний із використанням периферійних обчислень та інтеграцією Edge-, Fog- і Cloud-рівнів у межах єдиної розподіленої інфраструктури [15, 16]. Перенесення частини функцій оброблення даних із централізованих хмарних платформ на периферійні вузли дає змогу зменшити затримки, підвищити автономність системи та забезпечити оброблення даних у реальному часі. Водночас така децентралізація збільшує кількість потенційних точок компрометації, ускладнює встановлення єдиної політики безпеки та потребує узгодженого моніторингу стану різномірних компонентів.

Багаторівнева організація IoT-систем призводить до виникнення взаємозалежностей між пристроями, периферійними вузлами, мережевою інфраструктурою та хмарними сервісами [17, 18]. Унаслідок цього вразливість або компрометація компонента одного рівня може впливати на функціонування та стан захищеності компонентів інших рівнів [19, 20]. Наприклад, компрометація кінцевого пристрою може використовуватися для формування шкідливого мережевого трафіку, впливу на периферійні вузли або несанкціонованого доступу до хмарних сервісів. Тому оцінювання захищеності лише окремих пристроїв не забезпечує цілісного уявлення про стан кібербезпеки всієї екосистеми.

Отже, сучасні архітектурні підходи достатньо повно описують структуру IoT-середовищ, функції їх компонентів і механізми взаємодії, однак переважно орієнтовані на проєктування систем або захист їх окремих рівнів. Недостатньо дослідженими залишаються питання комплексного врахування міждієвних залежностей, функціонального контексту та взаємозв'язків між різнорідними компонентами IoT-середовища під час оцінювання ризиків інформаційної безпеки. Це зумовлює необхідність розроблення методів і моделей контекстно-адаптивного оцінювання ризиків, здатних враховувати архітектурні та функціональні особливості IoT-середовищ під час формування інтегральної оцінки ризику.

### ***1.1.2. Методи виявлення вразливостей та аналізу кіберзагроз***

Важливим напрямом досліджень є розроблення методів виявлення вразливостей програмного забезпечення, апаратних компонентів, мережевої інфраструктури та комунікаційних протоколів IoT. Сучасні підходи до автоматизованого виявлення вразливостей вбудованих пристроїв та їх програмного забезпечення систематизовано в роботах [21, 22]. Окрему увагу в наукових дослідженнях приділено аналізу прошивок IoT-пристроїв, методам їх дослідження та виявленню потенційно небезпечних компонентів [23, 24].

Статичний аналіз дає змогу досліджувати програмний код або бінарні компоненти без їх виконання. Його використовують для виявлення небезпечних функцій, помилок роботи з пам'яттю, незахищених механізмів автентифікації,

жорстко закодованих облікових даних та інших дефектів [25]. Водночас статичний аналіз не завжди відображає поведінку системи в реальних умовах функціонування.

Динамічний аналіз передбачає спостереження за поведінкою програмного забезпечення під час його виконання. Він дозволяє виявляти помилки, що проявляються лише за певних станів системи, комбінацій вхідних даних або умов взаємодії з іншими компонентами. Його обмеженнями є складність відтворення повного набору сценаріїв і значні часові витрати [26].

Особливе місце в аудиті IoT займає аналіз прошивок. Він дає змогу виявляти небезпечні конфігурації, застарілі бібліотеки, приховані сервіси, незахищені ключі та механізми віддаленого доступу [27, 28]. Окремим напрямом є виявлення помилок і вразливостей, пов'язаних зі структурою та компонентами вбудованого програмного забезпечення IoT-пристроїв [29]. Проте ефективність такого аналізу залежить від доступності образу прошивки, можливості її розпакування, типу процесорної архітектури та наявності засобів емуляції.

Для практичної перевірки захищеності застосовують тестування на проникнення, під час якого моделюються дії потенційного злоумисника. Такий підхід дозволяє перевірити можливість експлуатації виявлених слабких місць, однак здебільшого відображає стан системи лише на момент проведення перевірки.

Інший напрям пов'язаний із системами виявлення вторгнень і запобігання атакам. Такі системи використовують сигнатурний, аномальний або поведінковий аналіз мережевого трафіку та телеметричних даних. Сигнатурні методи ефективно виявляють відомі атаки, але залежать від актуальності бази правил. Аномальні та поведінкові методи здатні виявляти невідомі сценарії впливу, проте можуть характеризуватися підвищеною кількістю хибних спрацювань.

Порівняльну характеристику основних напрямів подано в таблиці 1.1.

*Таблиця 1.1 – Порівняльний аналіз методів виявлення вразливостей і кіберзагроз у IoT-середовищах*

| <b>Метод або напрям</b>           | <b>Об'єкт аналізу</b>                          | <b>Основні можливості</b>                                | <b>Основні обмеження</b>                                         |
|-----------------------------------|------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------|
| Статичний аналіз [25]             | Програмний код, бінарні компоненти             | Виявлення дефектів без виконання програми                | Не враховує фактичну поведінку системи                           |
| Динамічний аналіз [26]            | Програмне забезпечення під час виконання       | Дослідження реальних сценаріїв функціонування            | Складність повного покриття станів системи                       |
| Аналіз прошивок[22,23]            | Вбудоване програмне забезпечення IoT-пристроїв | Виявлення небезпечних конфігурацій, сервісів і бібліотек | Залежність від формату, доступності та можливості емуляції       |
| Автоматизоване сканування [21,28] | Мережеві вузли, сервіси, конфігурації          | Швидке виявлення відомих вразливостей                    | Обмежена ефективність щодо невідомих і логічних вразливостей     |
| Тестування на проникнення [28,29] | IoT-система або її окремі компоненти           | Практична перевірка можливості реалізації атак           | Значна залежність від кваліфікації експерта, дискретний характер |
| Сигнатурні IDS/IPS [20]           | Мережевий трафік і події                       | Висока точність виявлення відомих атак                   | Низька ефективність щодо нових сценаріїв                         |
| Аномальний аналіз[20]             | Поведінка пристроїв і мережевий трафік         | Виявлення невідомих відхилень                            | Хибні спрацювання, залежність від базового профілю               |
| Інтелектуальна класифікація[20]   | Телеметричні та мережеві дані                  | Автоматизація розпізнавання атак                         | Залежність від якості даних і навчальної вибірки                 |

Аналіз наведених методів показує, що кожен із них охоплює певний тип даних або етап перевірки. Статичні та динамічні засоби досліджують програмні компоненти, сканери орієнтуються на відомі вразливості, а IDS/IPS - на мережеві

події. У результаті формується сукупність часткових оцінок, які потребують подальшого зіставлення та узагальнення.

Істотним обмеженням також є орієнтація значної частини засобів на вже відомі вразливості або зафіксовані ознаки атак. Недостатньо розвиненими залишаються механізми встановлення прихованих взаємозв'язків між подіями безпеки, прогнозування розвитку загроз і формування інтегральної оцінки стану захищеності IoT-середовища.

Таким чином, більшість існуючих методів ефективно розв'язує окремі задачі аналізу безпеки, проте результати їх застосування залишаються фрагментованими. Недостатньо дослідженими є питання інтеграції різнорідних результатів аналізу та формування цілісної оцінки стану кібербезпеки IoT-середовища.

### ***1.1.3. Міжнародні стандарти та методології оцінювання кіберризиків***

Поряд із технічними засобами захисту значного розвитку набули стандартизовані підходи до управління кібербезпекою та оцінювання ризиків. Їх призначення полягає у формуванні системних вимог до ідентифікації активів, визначення загроз, оцінювання наслідків, вибору заходів захисту, моніторингу та реагування на інциденти.

Вагомий внесок у розвиток цього напрямку здійснюють NIST, ISO, IEC, ENISA, ETSI та OWASP. Розроблені ними документи визначають загальні принципи управління кібербезпекою, базові можливості захисту IoT-пристроїв, вимоги до промислових і споживчих систем, а також рекомендації щодо тестування програмних компонентів.

Документи сімейства NISTIR 8259 визначають базові можливості кібербезпеки IoT-пристроїв, пов'язані з ідентифікацією, конфігурацією, захистом даних, керуванням доступом, оновленням програмного забезпечення та інформуванням про стан безпеки [30].

Стандарти ISO/IEC серії 27000 орієнтовані на створення систем менеджменту інформаційної безпеки [31]. Серія IEC 62443 визначає вимоги до захисту промислових систем автоматизації та керування, що робить її важливою для Industrial IoT [32]. ETSI EN 303 645 установлює базові положення щодо

безпеки споживчих IoT-пристроїв [33], а матеріали ENISA систематизують актуальні кіберзагрози та підходи до їх аналізу [34].

Поряд зі стандартами застосовуються методології оцінювання ризиків і моделювання загроз. Методологія OCTAVE орієнтована на системне оцінювання інформаційних ризиків організації [35], а EBIOS Risk Manager — на формування та аналіз сценаріїв кіберризиків [36]. Для моделювання загроз застосовують STRIDE [37] та PASTA [38], тоді як підхід Attack Trees дає змогу структуровано представляти можливі сценарії реалізації атак [39].

Зазначені стандарти й методології достатньо повно визначають, що необхідно контролювати під час забезпечення кібербезпеки, однак переважно не встановлюють механізмів інтеграції результатів технічного аналізу, оцінювання ризиків і моніторингу в межах єдиного інтелектуального процесу аудиту. Вони формують вимоги, принципи та контрольні заходи, але не замінюють інформаційну технологію їх практичної реалізації.

Проведений аналіз показує, що міжнародні стандарти визначають вимоги, принципи та процеси забезпечення безпеки, однак практично не регламентують механізми автоматизованої інтеграції результатів технічного аналізу, оцінювання ризиків та інтелектуальної підтримки прийняття рішень під час аудиту IoT-систем.

#### ***1.1.4. Застосування методів штучного інтелекту в кібербезпеці IoT***

Зростання кількості IoT-пристроїв, обсягів телеметричних даних і складності сучасних кібератак обумовило активне застосування методів штучного інтелекту та машинного навчання в задачах кібербезпеки. Такі методи використовують для аналізу мережевого трафіку, виявлення аномалій і класифікації атак [40, 41]. Окремий напрям становить застосування методів машинного навчання для інтелектуального виявлення вторгнень та аналізу подій кібербезпеки [42].

У сучасних дослідженнях застосовують дерева рішень, випадкові ліси, метод опорних векторів, алгоритми кластеризації, штучні нейронні мережі, згорткові та рекурентні мережі, автоенкодери, графові нейронні мережі та методи навчання з підкріпленням [43].

Класичні алгоритми машинного навчання використовують для класифікації мережеских потоків і подій безпеки. Глибокі нейронні мережі дозволяють автоматично виділяти складні ознаки з великих масивів даних, однак потребують значних обсягів якісних навчальних вибірок та обчислювальних ресурсів [44].

Федеративне навчання створює можливість спільного формування моделей без централізованого передавання первинних даних [45]. Це особливо важливо для розподілених IoT-систем, однак породжує проблеми неоднорідності локальних вибірок, захисту оновлень моделей і протидії отруєнню навчання.

Методи Explainable Artificial Intelligence спрямовані на підвищення прозорості результатів інтелектуального аналізу. Для аудиту кібербезпеки пояснюваність має принципове значення, оскільки експерт повинен отримати не лише клас або числову оцінку, а й обґрунтування причин, які вплинули на сформований висновок [46].

Перспективним напрямом є застосування великих мовних моделей для аналізу журналів подій, зіставлення відомостей про вразливості, формування пояснень і підтримки роботи аудитора. Водночас їх використання потребує контролю достовірності результатів, захисту конфіденційних даних, протидії маніпулятивним вхідним даним і перевірки сформованих рекомендацій [47].

Основними обмеженнями інтелектуальних методів у кібербезпеці IoT є:

- залежність від повноти й репрезентативності навчальних даних;
- зниження точності при зміні характеру мережевої активності;
- складність перенесення моделей між різними IoT-середовищами;
- обмежена пояснюваність результатів;
- вразливість до атак на моделі та процес навчання;
- переважна орієнтація на одну задачу або один тип даних.

Отже, методи штучного інтелекту мають значний потенціал для автоматизації аудиту кібербезпеки. Однак сама наявність інтелектуальної моделі не забезпечує комплексного аудиту. Необхідне її включення до інформаційно-аналітичного процесу, який охоплює збирання даних, їх нормалізацію, зіставлення результатів різних методів, оцінювання ризиків, пояснення висновків і підтримку рішень експерта.

Тобто, сучасні методи штучного інтелекту створюють широкі можливості для автоматизації окремих процедур аналізу безпеки, проте їх застосування здебільшого обмежується розв'язанням локальних задач. Формування цілісного інформаційно-аналітичного процесу аудиту із використанням інтелектуальних моделей потребує подальших досліджень.

#### ***1.1.5. Узагальнення сучасного стану досліджень та визначення невирішеної наукової задачі***

Проведений аналіз показав, що в галузі кібербезпеки IoT сформовано значний науковий і методичний доробок. Розроблено архітектурні моделі IoT-систем, методи пошуку вразливостей, засоби моніторингу мережевої активності, системи виявлення атак, методології оцінювання ризиків, міжнародні стандарти та інтелектуальні моделі аналізу даних.

Водночас зазначені напрями переважно розвиваються як відносно самостійні. Архітектурні моделі описують структуру системи, але не забезпечують безперервного оцінювання її стану. Засоби аналізу вразливостей формують локальні результати щодо окремих компонентів. IDS/IPS орієнтовані на виявлення мережевих подій. Методології оцінювання ризиків формалізують сценарії та наслідки, але значною мірою залежать від експертних даних. Інтелектуальні моделі підвищують ефективність окремих операцій, проте не завжди інтегруються в повний цикл аудиту.

Узагальнення результатів аналізу подано в таблиці 1.2.

*Таблиця 1.2 – Узагальнення сучасного стану наукової проблеми забезпечення кібербезпеки IoT*

| <b>Напрямок</b>                | <b>Основні результати</b>                                         | <b>Невирішені питання</b>                                               |
|--------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------|
| Архітектура IoT [19,20]        | Моделі рівнів, компонентів та інформаційних взаємодій             | Аналіз міжрівневих залежностей та їх впливу на загальний стан безпеки   |
| Виявлення вразливостей [24,28] | Засоби статичного, динамічного, мережевого й прошивкового аналізу | Інтеграція різнорідних результатів та виявлення невідомих слабких місць |



|                               |                                                                     |                                                                                          |
|-------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| IDS/IPS і моніторинг [42,44]  | Виявлення відомих атак, аномалій та відхилень поведінки             | Формування цілісної оцінки та прогнозування розвитку загроз                              |
| Оцінювання ризиків [5,7]      | Формалізація активів, загроз, наслідків і заходів захисту           | Автоматизоване оновлення оцінок на основі поточних даних                                 |
| Міжнародні стандарти [6,33]   | Вимоги, процеси та контрольні заходи забезпечення безпеки           | Відсутність єдиного механізму їх технологічної реалізації в аудиті                       |
| Штучний інтелект [40,46]      | Автоматизація класифікації, виявлення аномалій і прогнозування      | Пояснюваність, адаптивність та інтеграція моделей у процес аудиту                        |
| Інтелектуальний аудит [28,41] | Поєднання інформації про архітектуру, вразливості, загрози й ризики | Потреба в цілісній інформаційній технології та формалізованому процесі її функціонування |

Підсумовуючи, невирішена частина наукової проблеми полягає в недостатньому врахуванні контексту функціонування, гетерогенності та динамічності IoT-середовищ під час оцінювання ризиків інформаційної безпеки. Існуючі підходи не повною мірою забезпечують узгоджене врахування характеристик IoT-пристроїв, рівня загроз і вразливостей, критичності активів, імовірності реалізації загроз, можливих наслідків та ознак прихованої компрометації в умовах неповноти й невизначеності вхідних даних.

Отже, актуальним науково-практичним завданням є розроблення та удосконалення методів і моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ, що забезпечують інтелектуально-контекстну класифікацію IoT-пристроїв, формування їх контекстно-ризикових профілів, нечітке оцінювання ризиків та врахування ознак прихованої компрометації.

Розв'язання зазначеного завдання визначає спрямованість подальших досліджень щодо формалізації, розроблення, програмної реалізації та експериментальної перевірки запропонованих методів і моделей.

## 1.2. Поняття вразливості та кіберзагрози в IoT-середовищах

Інтернет речей (Internet of Things, IoT) є одним із ключових напрямів розвитку сучасних інформаційно-комунікаційних технологій, що забезпечує інтеграцію фізичних об'єктів, сенсорів, виконавчих пристроїв і програмних сервісів у єдине цифрове середовище. Стрімке зростання кількості IoT-пристроїв, їх гетерогенність, динамічність топології та тісна інтеграція з фізичними процесами суттєво ускладнюють забезпечення кібербезпеки[17,20]. На відміну від традиційних інформаційних систем, реалізація кібератак у IoT може призводити не лише до компрометації інформаційних ресурсів, а й до порушення функціонування кіберфізичних систем, зокрема промислових, транспортних і медичних[3,4].

### *Поняття вразливості.*

Відповідно до стандарту ISO/IEC 27005:2022, *вразливість* (vulnerability) визначається як слабкість активу або групи активів, яка може бути використана однією чи кількома загрозами[6]. У середовищах Інтернету речей це поняття набуває ширшого трактування, оскільки вразливість пов'язана не лише з технічними недоліками окремих пристроїв, протоколів або програмного забезпечення, а й із можливістю порушення довіри до функціонування всієї системи[20].

Особливості вразливостей IoT-середовищ визначаються специфікою їх побудови та експлуатації. Основними чинниками є обмежені обчислювальні ресурси, відсутність регулярного оновлення програмного забезпечення, використання спрощених або недостатньо захищених протоколів взаємодії та закритість програмних платформ, що ускладнює незалежний аудит їх безпеки[21].

Узагальнену характеристику типових вразливостей IoT-пристроїв, їх проявів і можливих наслідків наведено в таблиці 1.3.

*Таблиця 1.3 – Типові вразливості IoT-пристроїв*

| Категорія             | Приклади                                               | Потенційні наслідки                             |
|-----------------------|--------------------------------------------------------|-------------------------------------------------|
| Ідентифікація [17,20] | Використання паролів за замовчуванням, відсутність MFA | Несанкціонований доступ, перехоплення керування |

|                                |                                                      |                                            |
|--------------------------------|------------------------------------------------------|--------------------------------------------|
| Комунікаційні протоколи[17,20] | Відкриті порти Telnet/HTTP, слабкий захист MQTT/CoAP | Підміна даних, MITM-атаки                  |
| Прошивки та ПЗ[22,28]          | Наявність бекдорів, відсутність OTA-оновлення        | Постійна компрометація пристрою            |
| Апаратний рівень[20,29]        | Side-channel атаки, відсутність захисту пам'яті      | Витік ключів, фізичний контроль над вузлом |

### *Поняття кіберзагрози.*

Згідно з рекомендаціями NIST SP 800-30 та ENISA Threat Landscape, *кіберзагроза* розглядається як потенційна причина небажаного інциденту, здатного завдати шкоди інформаційній системі або організації[7,8]. У середовищах Інтернету речей характер таких загроз істотно ускладнюється, оскільки об'єктом впливу стають не лише інформаційні ресурси, а й фізичні процеси, керовані підключеними пристроями.

До найбільш характерних загроз належать використання IoT-пристроїв у складі ботнетів, несанкціонований збір і аналіз даних сенсорів, атаки на промислові системи керування, а також компрометація медичних і транспортних систем[3,4]. Незалежно від механізму реалізації всі зазначені загрози використовують наявні вразливості компонентів IoT-середовища.

### *Взаємозв'язок понять «загроза – вразливість – ризик».*

Фундаментальним поняттям сучасної кібербезпеки є взаємозв'язок між загрозами, вразливостями та ризиками, який традиційно описується моделлю «Загроза – Вразливість – Ризик» [6] (Рис. 1.1).

У цій моделі загроза є потенційним джерелом негативного впливу, вразливість визначає можливість його реалізації, а ризик характеризує ймовірність і можливі наслідки реалізації загрози через наявну вразливість[6,7].



*Рисунок 1.1 - Модель взаємодії «Загроза – Вразливість – Ризик» у IoT-середовищі*

Для IoT-середовищ наведена модель має ширше практичне трактування. Реалізація ризику може призводити не лише до втрати конфіденційності, цілісності чи доступності інформації, а й до порушення фізичних процесів, прийняття помилкових керуючих рішень та зниження довіри до результатів функціонування всієї системи [20].

Аналіз вразливостей IoT потребує врахування не лише технічних характеристик окремих компонентів, а й їх функціонального контексту та взаємозв'язків у межах системи.

### 1.3. Класифікація кібератак на IoT

Ефективність виявлення вразливостей і протидії кібератакам у середовищах Інтернету речей значною мірою залежить від розуміння механізмів реалізації сучасних загроз. На відміну від традиційних інформаційних систем, де атаки здебільшого спрямовані на окремі програмні або мережеві компоненти, у IoT-середовищах об'єктами впливу стають усі рівні архітектури - від фізичних пристроїв і каналів зв'язку до прикладних сервісів і хмарної інфраструктури[48]. Це обумовлено гетерогенністю IoT-середовищ, використанням різномірних

протоколів взаємодії, ресурсними обмеженнями пристроїв і тісною інтеграцією цифрових та фізичних процесів.

У науковій літературі кібератаки на IoT найчастіше класифікують за рівнем їх реалізації: *мережевим, протокольним, прикладним та апаратним* [48,49]. Такий підхід дає змогу систематизувати джерела загроз, визначити характерні вразливості кожного рівня та обґрунтувати їх виявлення та протидії.

*Мережеві атаки.* Мережевий рівень є одним із найуразливіших елементів IoT-інфраструктури, оскільки забезпечує взаємодію великої кількості пристроїв, що функціонують у відкритих або недостатньо захищених мережах. До найпоширеніших атак цього рівня належать сканування мережі, DDoS-атаки із використанням ботнетів, атаки типу *Man-in-the-Middle*, різні види спуфінгу та атаки на бездротові канали зв'язку [48,49]. Їх наслідками є порушення доступності сервісів, перехоплення або підміна даних і компрометація мережевої взаємодії між компонентами системи.

Протидія мережевим атакам ґрунтується на використанні сегментації мережі, захищених протоколів маршрутизації, механізмів контролю доступу та систем виявлення вторгнень [49]. Ефективність зазначених засобів значною мірою визначається здатністю враховувати контекст функціонування пристроїв і динаміку структури IoT-середовища.

*Протокольні атаки.* Протокольні атаки пов'язані з особливостями реалізації протоколів обміну даними, зокрема MQTT, CoAP, ZigBee, Bluetooth Low Energy та LoRaWAN [49]. Більшість із них створювалися з урахуванням жорстких ресурсних обмежень IoT-пристроїв, що обумовило використання спрощених механізмів автентифікації, авторизації та криптографічного захисту.

У більшості випадків успішна реалізація таких атак пов'язана не зі слабкістю самих специфікацій, а з використанням застарілих версій протоколів, помилками конфігурування або порушенням рекомендацій щодо їх безпечного застосування. Це визначає необхідність постійного контролю конфігурації та оцінювання відповідності використовуваних протоколів сучасним вимогам безпеки.

*Прикладні атаки.* Прикладний рівень охоплює програмне забезпечення IoT-пристроїв, механізми оновлення прошивок, прикладні інтерфейси, хмарні

сервіси та компоненти периферійних обчислень. На цьому рівні реалізуються атаки, пов'язані з компрометацією ланцюгів постачання програмного забезпечення, поширенням шкідливих оновлень, викраденням криптографічних ключів, експлуатацією програмних вразливостей та атаками на моделі штучного інтелекту.

Ключовою особливістю прикладних атак є їх масштабність: компрометація одного програмного компонента або механізму оновлення може спричинити одночасне порушення функціонування великої кількості взаємопов'язаних пристроїв [50].

*Апаратні атаки.* Апаратні атаки використовують фізичні особливості функціонування електронних компонентів. До них належать атаки по побічних каналах, ін'єкція збоїв, експлуатація інтерфейсів налагодження та методи фізичного вилучення інформації з мікросхем пам'яті [51].

Попри необхідність фізичного доступу або спеціалізованого обладнання, наслідки таких атак можуть бути критичними через можливість компрометації криптографічних ключів, обходу механізмів захищеного завантаження та встановлення стійкого контролю над пристроєм. Тому важливими складовими захисту є використання багаторівневих механізмів апаратної безпеки, оцінювання стійкості пристроїв до фізичних впливів і контроль безпеки ланцюга постачання.

Узагальнену класифікацію основних класів кібератак на IoT-середовища наведено на Рис. 1.2.

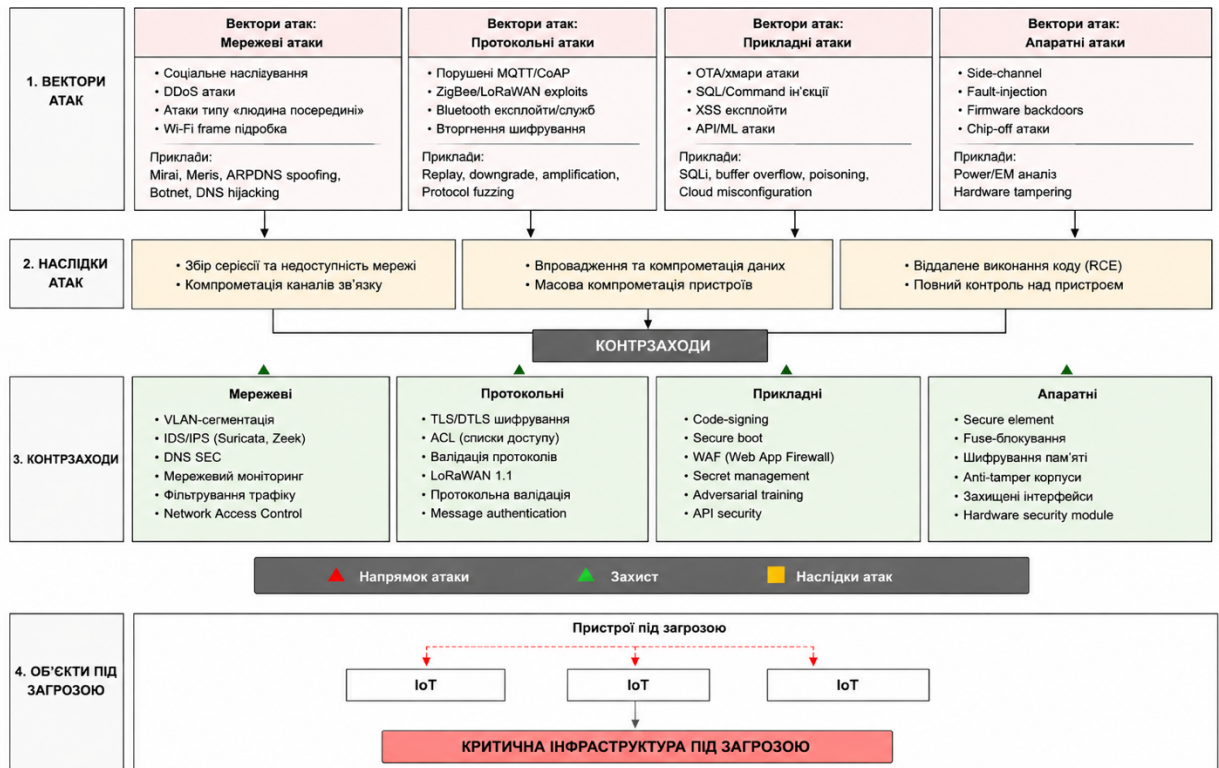


Рисунок 1.2 – Узагальнена схема класифікації кібератак на IoT.

Підсумовуючи, сучасні кібератаки реалізуються на різних рівнях архітектури IoT, що потребує комплексного аналізу їх взаємозалежностей.

#### 1.4. Особливості загроз у динамічних та гетерогенних IoT-мережах

Однією з визначальних особливостей сучасних IoT-середовищ є їх висока динамічність і гетерогенність. На відміну від традиційних інформаційних систем, вони об'єднують пристрої з різними апаратними характеристиками, операційними платформами, мережевими протоколами та моделями взаємодії. Використання технологій 6LoWPAN, RPL, MQTT, CoAP, LoRaWAN, ZigBee, Bluetooth Low Energy, а також периферійних обчислень (*edge computing*) забезпечує масштабованість і гнучкість IoT-мереж, проте водночас формує нові класи вразливостей і суттєво ускладнює забезпечення кібербезпеки таких середовищ [49,52].

Специфіка сучасних загроз у таких середовищах визначається трьома взаємопов'язаними чинниками: *мультипротоковністю, динамічною зміною топології мережі та ресурсними обмеженнями кінцевих пристроїв*[52].

*Мультипротокольність та інтероперабельність.* Використання різнорідних мережевих протоколів і механізмів взаємодії потребує їх узгодження за допомогою шлюзів та сервісів трансляції. На стику різних технологічних стеків виникають додаткові вразливості, пов'язані з помилками перетворення даних, несумісністю політик безпеки та некоректною конфігурацією шлюзів. Такі зони взаємодії різних технологічних стеків ускладнюють централізований контроль безпеки й автоматизоване виявлення аномалій [49,52] .

*Динамічна топологія та мобільність.* Склад IoT-мереж постійно змінюється: пристрої можуть приєднуватися до мережі, залишати її або змінювати свої функції. Унаслідок цього змінюються відносини довіри між вузлами, а ефективність статичних механізмів контролю доступу знижується. Особливу небезпеку становлять атаки на маршрутизацію в мережах LLN, зокрема *sinkhole*, *selective forwarding*, маніпулювання службовими повідомленнями протоколу RPL та інші способи порушення процесів маршрутизації [53] .

*Ресурсні обмеження пристроїв.* Більшість IoT-пристроїв характеризується обмеженими обчислювальними ресурсами, пам'яттю та енергоспоживанням, що обмежує можливість використання складних криптографічних механізмів і алгоритмів аналізу безпеки безпосередньо на кінцевих вузлах. У зв'язку з цим значна частина функцій моніторингу переноситься на периферійні вузли або шлюзи. Перенесення функцій аналізу на периферійні вузли підвищує ефективність оброблення даних, але одночасно збільшує критичність компрометації периферійної інфраструктури, оскільки її порушення може вплинути на значну кількість підключених пристроїв [54].

Сукупний вплив зазначених чинників формує нові класи загроз, характерні саме для динамічних IoT-середовищ. До них належать короточасні маніпуляції ролями вузлів, маршрутизаційні атаки в мережах LLN, а також контекстні атаки, що використовують зміни топології, мобільності або функціонального стану системи для прихованої реалізації шкідливих дій [53,55]. Особливістю таких атак є відсутність явних ознак компрометації окремих пристроїв, тому їх виявлення потребує врахування поточного контексту функціонування мережі та взаємозв'язків між її компонентами [56] .



Узагальнення основних чинників, що визначають специфіку загроз у динамічних і гетерогенних IoT-мережах, наведено в таблиці 1.4.

*Таблиця 1.4 – Особливості загроз у динамічних та гетерогенних IoT-мережах*

| <b>Фактор</b>                                      | <b>Наслідки (тип загроз)</b>                                                                                                                      | <b>Рекомендовані контрзаходи</b>                                                                                                        |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Мультипротокольність / інтероперабельність [52,54] | «Зони перетину» протоколів → логічні слабкі місця, помилки шлюзової трансляції.                                                                   | Уніфіковані політики на gateway; валідація трансляцій; тестування інтеграції; контекстна фільтрація.                                    |
| Динамічна топологія / мобільність [53,55]          | Мінливі відносини довіри → роєві маніпуляції; маршрутизаційні атаки (sinkhole, selective-forwarding, DIO/DAO flooding).                           | Репутаційні критерії вибору маршрутів; hardening RPL (Trickle); локальні IDS/edge-контрзаходи.                                          |
| Обмежені ресурси вузлів [52,54]                    | Неможливість «важких» криптопроцедур на кінці → перенесення ризику на edge; компрометація edge має великий вплив.                                 | Легковагі крипто/аналізи на вузлах; HSM/secure-element для критичних вузлів; сегментація та мінімізація прав.                           |
| Контекстно-залежні атаки [56]                      | Використання змін контексту (join/leave, мобільність, пікові події) для прихованих атак; нетипові появи/зникнення вузлів, зміни профілів трафіку. | Контекстно-орієнтований моніторинг і кореляція метаданих; адаптивні політики доступу; автоматична тимчасова ізоляція підозрілих вузлів. |

За результатами проведеного аналізу, рівень безпеки сучасних IoT-середовищ визначається не лише характеристиками окремих пристроїв, а й сукупністю їх функціональних зв'язків, мережевого контексту, поведінкових особливостей і динаміки зміни рівня довіри між компонентами системи.

Підсумовуючи, динамічність і гетерогенність IoT-середовищ істотно ускладнюють застосування традиційних методів аналізу безпеки.

### **1.5. Сучасні методи моніторингу та аналізу стану безпеки IoT-середовищ**

Розвиток Інтернету речей зумовлює підвищення вимог до методів моніторингу та аналізу стану безпеки. Гетерогенність пристроїв, динамічність топології, обмеженість обчислювальних ресурсів, неповнота даних і постійна поява нових типів кіберзагроз потребують застосування підходів, здатних

забезпечувати своєчасне виявлення подій безпеки та формування даних для подальшого оцінювання ризиків [57, 58].

### ***1.5.1. Архітектурні підходи до побудови систем виявлення атак***

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) залишаються одним із базових засобів виявлення атак у IoT-середовищах. Залежно від організації процесу аналізу інформації розрізняють *централізовані, розподілені та гібридні архітектури IDS*, кожна з яких має власні переваги та обмеження щодо масштабованості, продуктивності, відмовостійкості та ефективності виявлення атак [57,59].

*Централізовані архітектури* - забезпечують високоякісний аналіз завдяки використанню значних обчислювальних ресурсів і централізованому накопиченню інформації. Разом із тим вони характеризуються обмеженою масштабованістю, високим навантаженням на мережеву інфраструктуру та наявністю єдиної точки відмови [59].

*Розподілені архітектури* - виконують аналіз безпосередньо на периферійних вузлах або локальних агентах, що дає змогу зменшити затримки реагування та підвищити стійкість системи до відмов окремих компонентів. Водночас ресурсні обмеження IoT-пристроїв істотно звужують можливості використання складних алгоритмів аналізу, а узгодження результатів між вузлами ускладнює побудову єдиної політики безпеки [60].

*Гібридні архітектури* - поєднують локальне попереднє оброблення інформації на периферійних вузлах із централізованим аналізом на шлюзах або в хмарній інфраструктурі. Такий підхід дає змогу поєднати переваги швидкого локального реагування із можливістю комплексного аналізу, забезпечуючи кращу масштабованість і ефективніше використання обчислювальних ресурсів [61].

Порівняльну характеристику основних архітектурних підходів наведено в Табл. 1.5.

*Таблиця 1.5 – Порівняльна характеристика архітектурних підходів для IoT-середовищ*

| Архітектурний підхід         | Принцип організації                                                            | Основні переваги                                                                                              | Основні обмеження                                                                                     | Доцільність використання під час аудиту безпеки                                                                       |
|------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Централізована</b>        | Аналіз мережевого трафіку виконується центральним вузлом                       | Висока якість аналізу; централізоване керування; простота адміністрування                                     | Єдина точка відмови; обмежена масштабованість; значне навантаження на мережу                          | Забезпечує комплексний аналіз, але має обмежену адаптивність до динамічних змін середовища                            |
| <b>Розподілена</b>           | Аналіз здійснюється безпосередньо на вузлах або локальних агентах              | Висока масштабованість; швидке локальне реагування; відсутність єдиної точки відмови                          | Обмежені обчислювальні ресурси пристроїв; складність координації; неоднорідність політик безпеки      | Забезпечує оперативне локальне виявлення подій, однак потребує узгодження результатів між вузлами                     |
| <b>Гібридна (Edge/Cloud)</b> | Первинний аналіз виконується на edge-вузлах, поглиблений — у gateway або хмарі | Поєднання швидкого реагування та комплексного аналізу; добра масштабованість; ефективне використання ресурсів | Підвищена складність реалізації; необхідність координації між рівнями; залежність від каналів зв'язку | Найбільш придатна для комплексного аудиту завдяки поєднанню локального аналізу та централізованого оцінювання ризиків |

### **1.5.2. Еволюція методів виявлення атак**

Методи виявлення атак у IoT-середовищах пройшли послідовну еволюцію від сигнатурних і поведінкових підходів до методів машинного та глибокого навчання, федеративного навчання й пояснюваного штучного інтелекту. Основні етапи розвитку методів виявлення кібератак у IoT-середовищах наведено на Рис. 1.3.

| КРИТЕРІЇ ОЦІНЮВАННЯ                                                                      | АРХІТЕКТУРНІ ПАРАДИГМИ IDS/IPS                                                                  |                                                                                                 |                                                                                              |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|                                                                                          | 1. Централізована (Network-based)                                                               | 2. Розподілена (On-device)                                                                      | 3. Гібридна (Edge + Cloud)                                                                   |
| 1. Видимість і контекст подій (охоплення та точність контексту)                          | <b>M</b> Широкий огляд мережі, але обмежений контекст пристроїв і стану середовища              | <b>H</b> Глибокий локальний контекст пристрою та середовища, обмежений глобальний огляд         | <b>H</b> Поєднання глобальної видимості та локального контексту, повна картина подій         |
| 2. Шифрування й протоколи (підтримка безпечних протоколів та інспекції)                  | <b>L</b> Складно дешифрувати та аналізувати зашифрований трафік end-to-end                      | <b>H</b> Аналіз на рівні пристрою, підтримка локальних протоколів, але обмежений DPI            | <b>H</b> Аналіз на edge до шифрування та централізований дешифрування для глибокої інспекції |
| 3. Часові характеристики (затримка та швидкодія)                                         | <b>L</b> Затримки передачі даних до центру та кореляції, повільне реагування                    | <b>H</b> Миттєве виявлення і локальне блокування, мінімальні затримки                           | <b>M</b> Швидка реакція на edge, глибока кореляція в хмарі, середня затримка                 |
| 4. Ресурси обмеження (вимоги до обчислювальних і мережевих ресурсів)                     | <b>H</b> Високі ресурси на сервері, мінімальні вимоги до пристроїв, але високі мережеві витрати | <b>L</b> Обмежені обчислення, пам'ять і енергія на пристрої, складно реалізувати складні моделі | <b>M</b> Розвантаження на edge/cloud, оптимальний розподіл ресурсів, помірні вимоги          |
| 5. Керуваність і масштабування (централізоване управління та масштабованість)            | <b>H</b> Централізоване управління та оновлення, проста політика, добра масштабованість         | <b>L</b> Складне оновлення великої кількості пристроїв, різномірність, низька керуваність       | <b>H</b> Централізоване управління з локальною автономією, висока масштабованість            |
| 6. Конфіденційність і комплаєнс (мінімізація передачі даних та відповідність стандартам) | <b>L</b> Передача великих обсягів даних, ризики конфіденційності та комплаєнсу                  | <b>H</b> Дані не покидають пристрій, підтримка локального та federated навчання                 | <b>M</b> Обробка чутливих даних на edge, агрегація в хмарі, баланс приватності та аналітики  |
| 7. Надійність (відмовостійкість і стійкість до збоїв)                                    | <b>L</b> Єдина точка відмови – центр, залежність від мережі, ризики недоступності               | <b>M</b> Стійкість до втрати зв'язку, але залежність від пристрою і швидкого постачання         | <b>H</b> Відмовостійкість за рахунок розподіленої архітектури, резервування на рівнях        |

| ЛЕГЕНДА ОЦІНОК |                                        | ПРИМІТКА                                                                               |  |
|----------------|----------------------------------------|----------------------------------------------------------------------------------------|--|
| <b>H</b>       | Високий рівень відповідності критерію  | Оцінювання виконано відносно вимог гетерогенних IoT-екосистем та задач аудиту безпеки. |  |
| <b>M</b>       | Середній рівень відповідності критерію |                                                                                        |  |
| <b>L</b>       | Низький рівень відповідності критерію  |                                                                                        |  |

Рисунок 1.3 – Еволюція методів виявлення кібератак у IoT-середовищах

Першими широкого застосування набули сигнатурні методи, що ґрунтуються на пошуку відомих шаблонів атак. Їх перевагою є висока точність виявлення відомих загроз, тоді як основним обмеженням залишається низька ефективність щодо нових або модифікованих атак [62].

Подальшого розвитку набули поведінкові та аномальні методи, засновані на виявленні відхилень від нормального функціонування системи. Вони дають змогу виявляти раніше невідомі атаки, проте характеризуються підвищеним рівнем хибнопозитивних спрацювань і потребують адаптації до особливостей конкретного IoT-середовища [62].

Наступний етап пов'язаний із застосуванням методів машинного та глибокого навчання, які забезпечують автоматичне виявлення складних закономірностей у мережевому трафіку та поведінці IoT-пристроїв і підвищують ефективність класифікації кіберзагроз [63].

Подальший розвиток інтелектуальних методів пов'язаний із федеративним навчанням, що дає змогу здійснювати спільне навчання моделей без централізованого передавання вихідних даних, та пояснюваним штучним інтелектом (Explainable Artificial Intelligence, XAI), спрямованим на підвищення

інтерпретованості результатів аналізу та обґрунтованості прийнятих рішень [64–66].

Порівняльний аналіз можливостей сучасних методів виявлення атак щодо роботи в умовах IoT-середовищ наведено в Табл.1.6.

*Таблиця 1.6 - Порівняльна характеристика сучасних методів виявлення атак у IoT-середовищах*

| Метод                             | Відомі атаки | Нові атаки | Урахування контексту | Оцінювання ризику | Підтримка прийняття рішень |
|-----------------------------------|--------------|------------|----------------------|-------------------|----------------------------|
| Сигнатурний аналіз                | ✓            | ✗          | ✗                    | ✗                 | ✗                          |
| Поведінковий та аномальний аналіз | ✓            | ✓          | Δ                    | ✗                 | ✗                          |
| Машинне навчання (ML)             | ✓            | ✓          | Δ                    | ✗                 | Δ                          |
| Глибоке навчання (DL)             | ✓            | ✓          | Δ                    | ✗                 | Δ                          |
| Федеративне навчання (FL)         | ✓            | ✓          | Δ                    | ✗                 | Δ                          |
| Контекстно-орієнтовані підходи    | ✓            | ✓          | ✓                    | Δ                 | Δ                          |

### ***1.5.3. Аналіз обмежень сучасних підходів***

Незважаючи на значний розвиток сучасних методів виявлення атак, їх застосування в IoT-середовищах супроводжується низкою принципових обмежень, зумовлених особливостями побудови та функціонування таких систем.

*По-перше*, більшість існуючих підходів орієнтована на аналіз окремих мережевих подій або поведінкових аномалій без урахування функціонального контексту роботи пристроїв. Унаслідок цього однакові події можуть інтерпретуватися як нормальна поведінка або як ознака атаки залежно від поточного стану системи, що знижує достовірність результатів аналізу[67].

*По-друге*, сучасні IoT-середовища характеризуються високою динамічністю: змінюються склад мережі, ролі пристроїв, маршрути взаємодії та умови функціонування. Це істотно ускладнює побудову статичних моделей

нормальної поведінки та призводить до збільшення кількості хибнопозитивних і хибнонегативних спрацювань [68,69].

*По-третє*, широке використання методів машинного та глибокого навчання обмежується недостатньою інтерпретованістю отриманих результатів. Незважаючи на високу точність класифікації, такі моделі часто не дають можливості пояснити причини прийняття рішення, що знижує рівень довіри експертів до автоматизованих засобів аналізу [66,70]].

Ще одним суттєвим обмеженням є відокремлений розгляд процесів виявлення атак і оцінювання ризиків [71,72]. У більшості існуючих рішень рішення щодо реагування приймаються без комплексного врахування критичності пристроїв, рівня довіри до джерел інформації, поточного стану мережі та можливих наслідків реалізації загроз [73,74].

Важливим фактором також залишаються ресурсні обмеження IoT-пристроїв, які не дозволяють використовувати складні алгоритми аналізу безпосередньо на кінцевих вузлах [75,76]. Крім того, дедалі більшого значення набуває безпека ланцюга постачання моделей і процесів їх оновлення, що потребує контролю цілісності програмних компонентів, аудиту джерел походження моделей та використання захищених механізмів їх розгортання [77,78].

Узагальнення переваг і обмежень сучасних підходів до виявлення атак у IoT-середовищах наведено в Табл. 1.7.

*Таблиця 1.7 – Узагальнення основних переваг і обмежень сучасних підходів до виявлення атак у IoT-середовищах*

| Сучасний підхід             | Основні переваги                                                                  | Основні обмеження                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Сигнатурний аналіз<br>[62]  | Висока точність виявлення відомих атак; низький рівень хибнопозитивних спрацювань | Не виявляє нові та модифіковані атаки; потребує постійного оновлення бази сигнатур                  |
| Поведінковий аналіз<br>[62] | Дає змогу виявляти невідомі атаки та аномалії                                     | Значна кількість хибнопозитивних спрацювань; залежність від коректності моделі нормальної поведінки |

|                                     |                                                                                                                                        |                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Методи машинного навчання [63]      | Адаптивність; автоматичне виявлення складних закономірностей; висока точність класифікації                                             | Потребують репрезентативних навчальних даних; складність перенавчання при зміні середовища |
| Методи глибокого навчання [63]      | Висока ефективність під час аналізу складних залежностей і великих обсягів даних                                                       | Значні обчислювальні витрати; низька інтерпретованість результатів                         |
| Федеративне навчання [64,65]        | Забезпечує навчання без централізованої передачі даних; підвищує конфіденційність                                                      | Складність синхронізації моделей; залежність від якості локального навчання                |
| Контекстно-орієнтовані підходи [67] | Враховують функціональний стан пристроїв, контекст взаємодії та динаміку середовища; забезпечують більш обґрунтоване оцінювання загроз | Висока складність реалізації; потребують інтеграції різномірних джерел інформації          |

Підбиваючи підсумки, жоден із розглянутих підходів окремо не забезпечує одночасного врахування функціонального контексту IoT-пристроїв, динаміки середовища, невизначеності параметрів ризику та підтримки прийняття рішень щодо протидії кібератакам. Це обумовлює необхідність розроблення методів, що поєднують контекстний аналіз, інтелектуальне виявлення аномалій і оцінювання ризиків у межах єдиного процесу аналізу безпеки.

#### ***1.5.4. Практичні аспекти реалізації та оцінювання сучасних методів виявлення атак***

Практичне застосування сучасних методів виявлення атак в Інтернеті речей визначається не лише вибором алгоритмів аналізу, а й можливістю їх ефективної роботи в умовах ресурсних обмежень, динамічності мережевого середовища та інтеграції в існуючу інфраструктуру.

Одним із ключових завдань є зменшення обчислювальних витрат моделей машинного навчання. Для цього застосовують скорочення кількості параметрів, зменшення точності обчислень, квантування, прунінг, а також передачу знань від складніших моделей до компактніших. Такі підходи дозволяють знизити використання пам'яті, енергоспоживання та час оброблення без суттєвого

погіршення точності виявлення атак [79,80]. У багаторівневих IoT-архітектурах поширеним є розподіл функцій аналізу між кінцевими пристроями, периферійними вузлами (edge), шлюзами та хмарною інфраструктурою, що забезпечує раціональне використання ресурсів і скорочує затримки під час прийняття рішень [81,82].

Ефективність сучасних систем виявлення атак оцінюють за сукупністю показників, що характеризують якість класифікації, продуктивність і стійкість функціонування системи. Крім традиційних метрик Precision, Recall, F1 та AUC-ROC, у задачах із незбалансованими вибірками широко використовують AUC-PR, коефіцієнт кореляції Метьюза (MCC), показники калібрування прогнозів, а також характеристики швидкодії, пропускну здатність, часу виявлення та реагування на інциденти [83,84]. Для перевірки робастності моделей оцінюють їх поведінку за зміни профілів трафіку, появи нових типів пристроїв, втрати телеметричних даних і навмисного спотворення інформації [85].

Експериментальні дослідження зазвичай проводять із використанням наборів даних BoT-IoT, TON\_IoT, IoT-23, Edge-IoTset та спеціалізованих засобів моделювання IoT-мереж [86,87].

Не менш важливим аспектом є інтеграція систем виявлення атак у реальну інфраструктуру Інтернету речей. Ефективність їх функціонування значною мірою залежить від узгодженої взаємодії компонентів різних рівнів, використання стандартизованих механізмів обміну телеметрією, захищених процедур автентифікації, централізованого журналювання подій і контролю цілісності програмних компонентів [88,89].

Сучасні підходи також передбачають автоматизацію оновлення моделей і правил безпеки із застосуванням практик DevSecOps та MLOps, що забезпечує підтримку актуального стану системи захисту протягом усього життєвого циклу її експлуатації [90].

Проведений аналіз показує, що сучасні методи виявлення атак поступово переходять від реактивного до інтелектуального підходу.



## **1.6. Загрози конфіденційності та їх вплив на безпеку IoT-середовищ**

Конфіденційність є однією з базових складових інформаційної безпеки IoT-середовищ, оскільки більшість пристроїв Інтернету речей здійснює безперервне збирання, передавання, оброблення та зберігання інформації про фізичні об'єкти, користувачів і технологічні процеси. На відміну від традиційних інформаційних систем, IoT характеризується великою кількістю розподілених вузлів, використанням різномірних протоколів зв'язку, динамічною топологією мережі та інтеграцією з кіберфізичними системами, що істотно ускладнює забезпечення конфіденційності даних та потребує застосування комплексних механізмів їх захисту [90,91].

Особливістю IoT є те, що порушення конфіденційності окремого пристрою створює передумови до розкриття інформації про функціонування всієї системи. Аналіз телеметрії, службових повідомлень, маршрутів передавання даних або характеристик мережевої взаємодії дозволяє зловмиснику відновити структуру мережі, визначити критичні вузли, побудувати профілі користувачів і підготувати цілеспрямовані кібератаки. Таким чином, проблема конфіденційності виходить за межі захисту персональних даних і безпосередньо впливає на загальний рівень безпеки IoT-середовища [92].

У зв'язку з цим аналіз загроз конфіденційності слід розглядати як складову оцінювання безпеки IoT-систем. Виявлення каналів можливого витоку інформації, аналіз інформаційних потоків і визначення потенційних наслідків компрометації даних дозволяють своєчасно ідентифікувати вразливості та оцінити ризики реалізації кібератак.

### ***1.6.1. Загрози конфіденційності під час оброблення даних у IoT***

У IoT-середовищах загрози конфіденційності виникають на всіх етапах життєвого циклу даних - під час їх збирання, передавання, оброблення, зберігання та використання. Це зумовлено великою кількістю взаємопов'язаних пристроїв, відкритістю каналів зв'язку, гетерогенністю протоколів і ресурсними обмеженнями кінцевих вузлів. Унаслідок цього порушення конфіденційності можуть виникати не лише внаслідок безпосереднього доступу до інформації, а й

через аналіз службових даних, особливостей мережевої взаємодії або характеристик функціонування пристроїв [93,94].

На відміну від традиційних інформаційних систем, у середовищах Інтернету речей джерелом конфіденційної інформації є не лише персональні дані користувачів, а й телеметрія, службові повідомлення, параметри роботи сенсорів, характеристики мережевого трафіку, часові параметри передавання повідомлень та інші метадані [94,95]. Навіть за умови використання сучасних криптографічних механізмів аналіз таких даних може дозволити визначити структуру мережі, функціональні ролі окремих вузлів або особливості роботи об'єкта спостереження.

Серйозну загрозу становлять також атаки, пов'язані з профілюванням користувачів, повторною ідентифікацією анонімізованих даних, аналізом поведінкових шаблонів пристроїв і кореляцією інформації, отриманої з різних джерел [93,95]. У кіберфізичних системах результати такого аналізу можуть використовуватися не лише для розкриття конфіденційної інформації, а й для підготовки цілеспрямованих кібератак на критичні компоненти інфраструктури.

Додаткові ризики виникають унаслідок поширення периферійних обчислень (edge computing), хмарних сервісів і розподілених моделей оброблення інформації [91,94]. Багатоетапне передавання даних між різними рівнями інфраструктури збільшує кількість потенційних точок компрометації та ускладнює контроль за їх обробленням. Тому забезпечення конфіденційності повинно охоплювати весь життєвий цикл даних незалежно від місця їх збирання, передавання, зберігання чи аналізу.

Основні загрози конфіденційності під час функціонування IoT-середовищ узагальнено в Табл. 1.8.

*Таблиця 1.8 – Основні загрози конфіденційності під час оброблення даних у IoT-середовищах*

| <b>Етап оброблення даних</b> | <b>Основні загрози</b>                | <b>Потенційні наслідки</b>           | <b>Основні засоби протидії</b> |
|------------------------------|---------------------------------------|--------------------------------------|--------------------------------|
| Збирання даних [73]          | Компрометація сенсорів, підміна даних | Недостовірна інформація, спотворення | Автентифікація пристроїв,      |

|                            |                                                                 |                                                            |                                                                  |
|----------------------------|-----------------------------------------------------------------|------------------------------------------------------------|------------------------------------------------------------------|
|                            |                                                                 | результатів моніторингу                                    | контроль цілісності                                              |
| Передавання даних [74]     | Перехоплення, MITM-атаки, аналіз трафіку                        | Розкриття конфіденційної інформації, підміна повідомлень   | Шифрування каналів зв'язку, захищені протоколи                   |
| Оброблення даних [73,74]   | Несанкціонований доступ, витік інформації                       | Компрометація службових і персональних даних               | Контроль доступу, ізоляція середовищ                             |
| Зберігання даних [73]      | Несанкціоноване копіювання, повторна ідентифікація              | Порушення конфіденційності, витік історичних даних         | Шифрування сховищ, анонімізація                                  |
| Використання даних [71,73] | Профілювання, кореляція інформації, повторне використання даних | Розкриття поведінкових характеристик користувачів і систем | Політики мінімізації даних, контроль доступу, аудит використання |

Аналіз загроз конфіденційності показує, що забезпечення конфіденційності в IoT не може обмежуватися лише використанням криптографічних засобів захисту [91,93]. Ефективне виявлення потенційних вразливостей потребує врахування особливостей оброблення даних, функціонального контексту пристроїв та взаємозв'язків між компонентами системи.

### ***1.6.2. Сучасні методи забезпечення конфіденційності даних***

Забезпечення конфіденційності даних у сучасних IoT-середовищах базується на комплексному використанні криптографічних, організаційних та інтелектуальних методів захисту. Вибір конкретних механізмів визначається архітектурою системи, характером даних, ресурсними можливостями пристроїв і вимогами до рівня безпеки.

Основою забезпечення конфіденційності залишається криптографічний захист, який охоплює симетричне та асиметричне шифрування, механізми автентифікації, управління ключами й захищені протоколи передавання даних [96]. Ці засоби ефективно запобігають несанкціонованому доступу до інформації

під час її передавання та зберігання, проте не усувають загроз, пов'язаних із аналізом метаданих, профілюванням користувачів або кореляцією інформації з різних джерел [91,95].

Для зниження ризику розкриття конфіденційної інформації застосовують методи анонімізації, псевдонімізації та диференційної приватності (*Differential Privacy*), які дозволяють виконувати статистичне оброблення даних без розкриття інформації про окремих користувачів або пристрої [97].

Перспективним напрямом також є федеративне навчання (*Federated Learning*), що забезпечує побудову моделей машинного навчання без централізованого збирання вихідних даних і тим самим зменшує ризик їх компрометації. Водночас ефективність такого підходу залежить від захищеності процесу локального навчання, узгодження моделей та стійкості до спеціалізованих атак [98,99].

Сучасні дослідження дедалі більше орієнтовані на інтеграцію криптографічних механізмів, методів збереження приватності, контекстного аналізу та інтелектуального оцінювання ризиків, що дозволяє підвищити рівень захисту даних і враховувати особливості функціонування IoT-середовищ під час прийняття рішень щодо реагування на загрози [96,98].

Порівняльну характеристику сучасних методів забезпечення конфіденційності наведено в Табл. 1.9.

*Таблиця 1.9 – Порівняльна характеристика сучасних методів забезпечення конфіденційності даних у IoT-середовищах*

| Метод                                   | Основні переваги                               | Основні обмеження                                             | Доцільність використання в IoT         |
|-----------------------------------------|------------------------------------------------|---------------------------------------------------------------|----------------------------------------|
| Криптографічний захист [96]             | Забезпечує конфіденційність і цілісність даних | Не захищає від аналізу метаданих; потребує управління ключами | Базовий механізм захисту інформації    |
| Анонімізація та псевдонімізація [93,95] | Знижує ризик ідентифікації користувачів        | Можлива повторна ідентифікація                                | Захист персональних даних і телеметрії |

|                                                   |                                                                             |                                                          |                                           |
|---------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------|
|                                                   |                                                                             | при кореляції даних                                      |                                           |
| Диференційна приватність [97]                     | Забезпечує конфіденційність під час статистичного аналізу                   | Знижує точність результатів при надмірному рівні захисту | Аналітичні системи та хмарні сервіси      |
| Федеративне навчання [98]                         | Навчання моделей без централізованої передачі даних                         | Складність координації та захисту процесу навчання       | Розподілені IoT- та Edge-середовища       |
| Комплексні контекстно-орієнтовані підходи [67,61] | Поєднання криптографічного захисту, аналізу контексту та оцінювання ризиків | Висока складність реалізації                             | Інтелектуальні системи аудиту безпеки IoT |

Порівняння сучасних методів свідчить про те, що жоден із розглянутих методів окремо не забезпечує комплексного вирішення задачі захисту конфіденційності в умовах гетерогенних і динамічних IoT-середовищ. Ефективне забезпечення безпеки потребує поєднання криптографічного захисту, механізмів збереження приватності, контекстного аналізу та оцінювання ризиків [96-99]. При цьому аналіз порушень конфіденційності має розглядатися не лише як засіб захисту даних, а й як джерело інформації для виявлення потенційних вразливостей і підтримки прийняття рішень щодо протидії кібератакам.

### ***1.6.3. Баланс між конфіденційністю, безпекою та ефективністю IoT-систем***

У сучасних IoT-середовищах забезпечення конфіденційності не може розглядатися ізольовано від вимог інформаційної безпеки та ефективності функціонування системи. Посилення криптографічного захисту, застосування додаткових процедур автентифікації та механізмів збереження приватності підвищують рівень захищеності інформації, однак можуть збільшувати затримки передавання даних, енергоспоживання та обчислювальне навантаження на IoT-пристрої [100].

Особливого значення цей компроміс набуває в системах реального часу, промисловому Інтернеті речей, транспортних і медичних системах, де вибір заходів захисту має здійснюватися з урахуванням функціонального контексту, критичності вузлів, ресурсних обмежень і допустимого рівня ризику.

Міжнародні стандарти та нормативні документи, зокрема ISO/IEC 27001, ISO/IEC 27005, GDPR, ETSI EN 303 645 і концепція *Privacy by Design*, визначають загальні принципи забезпечення конфіденційності та управління ризиками, проте не встановлюють універсального механізму адаптивного вибору заходів захисту для динамічних IoT-середовищ [101, 102]. Це зумовлює необхідність застосування підходів, здатних враховувати поточний стан середовища, функціональний контекст пристроїв та зміну рівня ризику в процесі їх функціонування [103, 104].

Отже, забезпечення конфіденційності в IoT-середовищах потребує узгодження з вимогами безпеки та ефективності функціонування системи з урахуванням її поточного контексту й рівня ризику. Взаємозв'язок між зазначеними складовими наведено на рис. 1.4.



Рисунок 1.4 – Концептуальна схема взаємозв'язку конфіденційності, безпеки та ефективності функціонування IoT-середовища

### 1.7. Постановка задачі дослідження

Проведений аналіз сучасного стану забезпечення інформаційної безпеки IoT-середовищ показав, що наявні методи виявлення кіберзагроз, аналізу вразливостей та оцінювання ризиків переважно орієнтовані на окремі складові процесу забезпечення безпеки. Водночас недостатньо враховуються функціональний контекст IoT-пристроїв, гетерогенність і динамічність середовища, невизначеність вхідних даних та можливість прихованої компрометації.

Особливої актуальності набуває комплексне оцінювання ризиків інформаційної безпеки, що потребує узгодженого врахування характеристик активів, загроз і вразливостей, можливостей потенційного порушника, імовірності реалізації загроз, тяжкості можливих наслідків, функціонального контексту IoT-пристроїв та ознак прихованої компрометації.

Отже, актуальним науковим завданням є розроблення моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням цього профілю й поточного стану безпеки в процесі аудиту.

Розроблена модель формування контекстно-ризикового профілю IoT-пристрою та удосконалений метод оцінювання ризиків становлять основу створеної інформаційної технології. Вона забезпечує їх узгоджене застосування для визначення показника RiskLevel і відповідної категорії ризику, які можуть використовуватися під час аудиту IoT-середовища для обґрунтування пріоритетності заходів захисту.

Для досягнення поставленої мети необхідно вирішити такі взаємопов'язані наукові завдання дослідження:

1. Провести аналіз сучасного стану методів і моделей аудиту безпеки IoT-середовищ, виявлення вразливостей, оцінювання ризиків, аналізу аномальної активності та підтримки прийняття рішень, визначити їх переваги, обмеження та невирішені наукові питання.
2. Розробити модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації за

п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища.

3. Удосконалити метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані шляхом формування системи взаємопов'язаних параметрів оцінювання ризику, урахування контекстно-ризикового профілю IoT-пристрою та введення попередньо сформованого показника BackdoorRisk.
4. Розвинути підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ, визначити її архітектуру, склад компонентів, інформаційні потоки та послідовність їх взаємодії в процесі аудиту.
5. Реалізувати програмний прототип ключових компонентів інформаційної технології та провести експериментальну перевірку працездатності й результативності розроблених та удосконалених методів і моделей на основі змодельованих сценаріїв і відкритих наборів даних IoT-безпеки.

Взаємозв'язок між науковою проблемою, метою, об'єктом і предметом дослідження, поставленими задачами, застосованими методами, одержаними науковими результатами та їх практичною реалізацією узагальнено в логічно-структурній схемі дослідження, наведеній на Рис. 1.5.



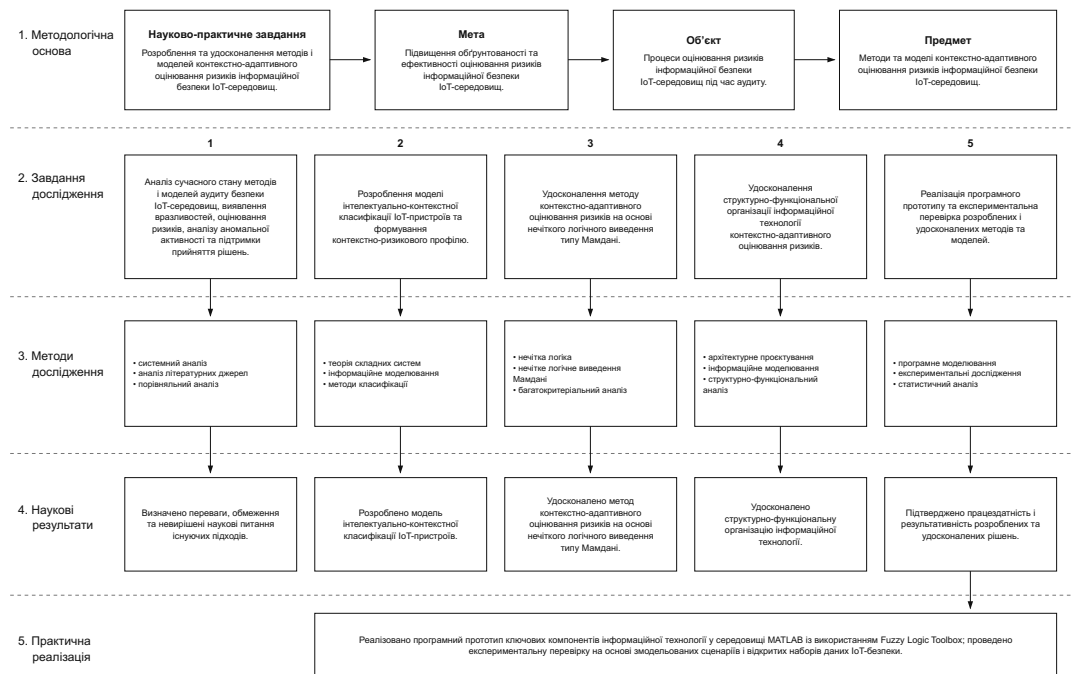


Рисунок 1.5— Структурно-логічна схема дисертаційного дослідження

## Висновки розділу 1

У першому розділі досліджено сучасний стан забезпечення інформаційної безпеки IoT-середовищ, проаналізовано характерні для них кіберзагрози та вразливості, сучасні методи виявлення атак, оцінювання ризиків і забезпечення конфіденційності. Встановлено, що гетерогенність, динамічність, ресурсні обмеження IoT-пристроїв та невизначеність параметрів функціонування ускладнюють комплексне оцінювання стану інформаційної безпеки та потребують урахування контексту функціонування пристроїв під час оцінювання ризиків.

За результатами проведеного дослідження:

1. Встановлено, що характерними особливостями сучасних IoT-середовищ є гетерогенність пристроїв і протоколів, динамічність структури та інформаційних взаємодій, ресурсні обмеження вузлів і невизначеність параметрів функціонування. Зазначені особливості зумовлюють необхідність урахування контексту IoT-пристроїв під час аналізу стану їх інформаційної безпеки.
2. Досліджено сучасні кіберзагрози та вразливості IoT-середовищ і встановлено, що їх вплив на стан безпеки залежить не лише від наявності

окремих вразливостей, а й від критичності активів, можливостей потенційного порушника, імовірності реалізації загроз, тяжкості можливих наслідків та функціонального контексту пристроїв.

3. Проаналізовано сучасні методи виявлення кібератак, оцінювання ризиків і забезпечення конфіденційності даних. Встановлено, що наявні підходи мають обмеження щодо комплексного врахування різномірних параметрів безпеки, функціонального контексту та невизначеності вхідних даних, що обмежує обґрунтованість оцінювання ризиків у гетерогенних і динамічних IoT-середовищах.
4. Обґрунтовано необхідність комплексного врахування характеристик IoT-пристроїв і параметрів ризику, зокрема критичності активів, рівня загроз і вразливостей, можливостей потенційного порушника, імовірності реалізації загроз, тяжкості можливих наслідків, контекстно-ризикового профілю та ризику прихованої компрометації.
5. Визначено передумови для розроблення моделі формування контекстно-ризикового профілю IoT-пристрою та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ. Їх узгоджене застосування в процесі аудиту потребує визначення архітектури інформаційної технології та порядку взаємодії її компонентів.

Отримані результати становлять підґрунтя для розроблення моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації, удосконалення методу оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані та побудови інформаційної технології їх узгодженого застосування, які розглядаються в наступних розділах дисертації.

## **РОЗДІЛ 2.**

### **МОДЕЛЬ ФОРМУВАННЯ КОНТЕКСТНО-РИЗИКОВОГО ПРОФІЛЮ ІОТ-ПРИСТРОЮ ТА МЕТОД ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ**

У цьому розділі розроблено модель формування контекстно-ризикового профілю ІоТ-пристрою за результатами інтелектуально-контекстної класифікації та удосконалено метод оцінювання ризиків інформаційної безпеки ІоТ-середовищ. Розглянуто п'ять критеріїв класифікації пристроїв, порядок формування профілю, структуру вхідних параметрів оцінювання ризику та нечітке логічне виведення типу Мамдані для визначення показника RiskLevel.

На відміну від підходів, у яких характеристики ІоТ-пристроїв, параметри загроз і вразливостей та оцінювання ризиків розглядаються відокремлено, запропонований підхід забезпечує їх узгоджене врахування з урахуванням функціонального контексту, невизначеності вхідних даних і ризику прихованої компрометації. Це створює основу для контекстно-адаптивного оцінювання ризиків інформаційної безпеки в гетерогенних і динамічних ІоТ-середовищах.

#### **2.1. Модель формування контекстно-ризикового профілю ІоТ-пристрою на основі інтелектуально-контекстної класифікації**

Ефективність оцінювання ризиків інформаційної безпеки ІоТ-середовищ значною мірою залежить від повноти врахування характеристик пристроїв та умов їх функціонування. Висока гетерогенність обладнання, різноманітність протоколів взаємодії та динамічність структури ІоТ-середовищ обмежують можливості традиційних класифікаційних підходів щодо формування достатнього інформаційного опису пристроїв для подальшого оцінювання ризиків.

Більшість існуючих підходів до класифікації ІоТ-пристроїв ґрунтується на окремих технологічних або функціональних ознаках, зокрема типі пристрою, архітектурі, протоколах зв'язку та функціональному призначенні. Водночас недостатньо враховуються рівень вбудованого інтелекту, контекст функціонування, поведінкові та безпекові характеристики, що ускладнює формування комплексного представлення пристрою для оцінювання ризиків.

У роботі розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами його інтелектуально-контекстної класифікації. Пристрій класифікується за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Результати класифікації за кожним критерієм зберігаються у профілі без зведення до одного числового показника. Сформований профіль разом із даними про поточний стан безпеки використовується для визначення та інтерпретації параметрів подальшого оцінювання ризику.

### ***2.1.1. Аналіз сучасних підходів та обмежень класифікації IoT***

Існуючі підходи до класифікації IoT-систем переважно орієнтовані на окремі аспекти функціонування мережі. Найчастіше класифікація здійснюється за архітектурою системи, використовуваними протоколами передавання даних, сферою застосування або ресурсними характеристиками пристроїв [105,106]. Найбільш поширеними класифікаційними ознаками є:

- a) *архітектурним рівнем* - поділ на сенсорний, мережевий і прикладний рівні [106];
- b) *типом передавання даних* - використання протоколів MQTT, CoAP, ZigBee, LoRaWAN, NB-IoT, BLE тощо [107];
- c) *галуззю застосування* - промислові (IIoT), транспортні, енергетичні, медичні або побутові системи [108,109];
- d) *ресурсними характеристиками* - енергоспоживання, обчислювальна потужність, пропускну здатність каналів зв'язку [110].

Попри широке використання таких підходів, вони мають низку принципових обмежень. Насамперед вони не враховують рівень вбудованого інтелекту пристроїв, контекст їх функціонування, динамічність зміни структури мережі та практично не інтегруються з процедурами оцінювання ризиків і аудиту безпеки [111,112].

У сучасних дослідженнях спостерігається поступовий перехід до контекстно-орієнтованих моделей класифікації, які враховують автономність пристроїв, рівень їх адаптивності, механізми взаємодії та характеристики інформаційної безпеки [113,114]. Такі моделі значно краще відповідають

потребам сучасних IoT-систем, однак і вони переважно розглядають зазначені характеристики ізольовано, без побудови єдиної багатовимірної моделі [115,116].

Отже, існуючі класифікаційні підходи не забезпечують комплексного врахування технічних, поведінкових, контекстних і безпекових характеристик IoT-пристроїв, необхідних для побудови адаптивних систем аудиту безпеки. Це обумовлює розроблення інтелектуально-контекстної моделі класифікації, яка об'єднує зазначені критерії в єдиному інформаційному просторі та створює основу для подальшого формалізованого оцінювання ризиків.

### ***2.1.2. Формування системи критеріїв інтелектуально-контекстної класифікації IoT-пристроїв***

На основі результатів аналізу, наведених у першому розділі, обґрунтовано необхідність використання багатокритеріальної моделі класифікації IoT-пристроїв. Традиційні підходи, що ґрунтуються переважно на технічних характеристиках або функціональному призначенні пристроїв, не забезпечують достатньої інформаційної основи для контекстно-адаптивного оцінювання ризиків інформаційної безпеки. Таке оцінювання потребує комплексного врахування характеристик, що визначають функціональне призначення IoT-пристрою, особливості його архітектури та поведінки, контекст функціонування, рівень вбудованого інтелекту та безпекові характеристики.

З цією метою запропоновано систему з п'яти взаємопов'язаних критеріїв інтелектуально-контекстної класифікації (Рис.2.1), яка забезпечує формування багатовимірного профілю IoT-пристрою та є основою подальшого оцінювання ризиків.

1. Рівень вбудованого інтелекту (Intelligence Level, I). Характеризує здатність IoT-пристрою автономно обробляти дані, приймати локальні рішення та адаптувати свою поведінку без постійної взаємодії з центральною інфраструктурою[117]. Залежно від функціональних можливостей виділяють:

- пасивні пристрої (збір і передавання даних);
- аналітичні пристрої (локальне оброблення інформації);
- адаптивні пристрої (самонавчання та оптимізація поведінки).

Рівень інтелекту визначає можливість автономного реагування на зміни середовища та впливає на особливості подальшого оцінювання ризиків.

2. Рівень захищеності (Security Level,  $S$ ). Відображає здатність IoT-пристрою протидіяти кіберзагрозам і забезпечувати безпечне функціонування в мережевому середовищі. Основними рівнями є:

- відкритий;
- базово захищений;
- високозахищений.

Оцінювання здійснюється з урахуванням механізмів автентифікації, авторизації, криптографічного захисту та контролю цілісності даних [118].

3. Архітектура взаємодії (Architecture Model,  $A$ ). Характеризує спосіб організації інформаційної взаємодії між компонентами IoT-середовища. Виділяють:

- централізовану;
- децентралізовану;
- гібридну архітектури.

Архітектура визначає особливості реалізації механізмів захисту, масштабованість системи та стійкість до кіберінцидентів [119].

4. Контекст функціонування (Context,  $C_x$ ). Відображає сферу застосування IoT-пристрою та визначає вимоги до безпеки, допустимий рівень ризику і критичність можливих наслідків компрометації. До основних контекстів належать:

- критична інфраструктура;
- Smart City;
- домашні IoT-системи;
- носимі пристрої (Wearable Devices).

Контекст функціонування визначає особливості процедур аналізу стану безпеки та критерії оцінювання ризиків [120].

5. Динамічність середовища (Dynamicsity  $D_y$ ). Характеризує зміну топології мережі, поведінки вузлів та умов функціонування IoT-системи[121]. За цим критерієм виділяють:

- статичні;

- мобільні;
- колективні (Swarm-based IoT) середовища.

Урахування динамічності дозволяє адаптувати процедури моніторингу безпеки та оцінювання ризиків до змін структури IoT-середовища.

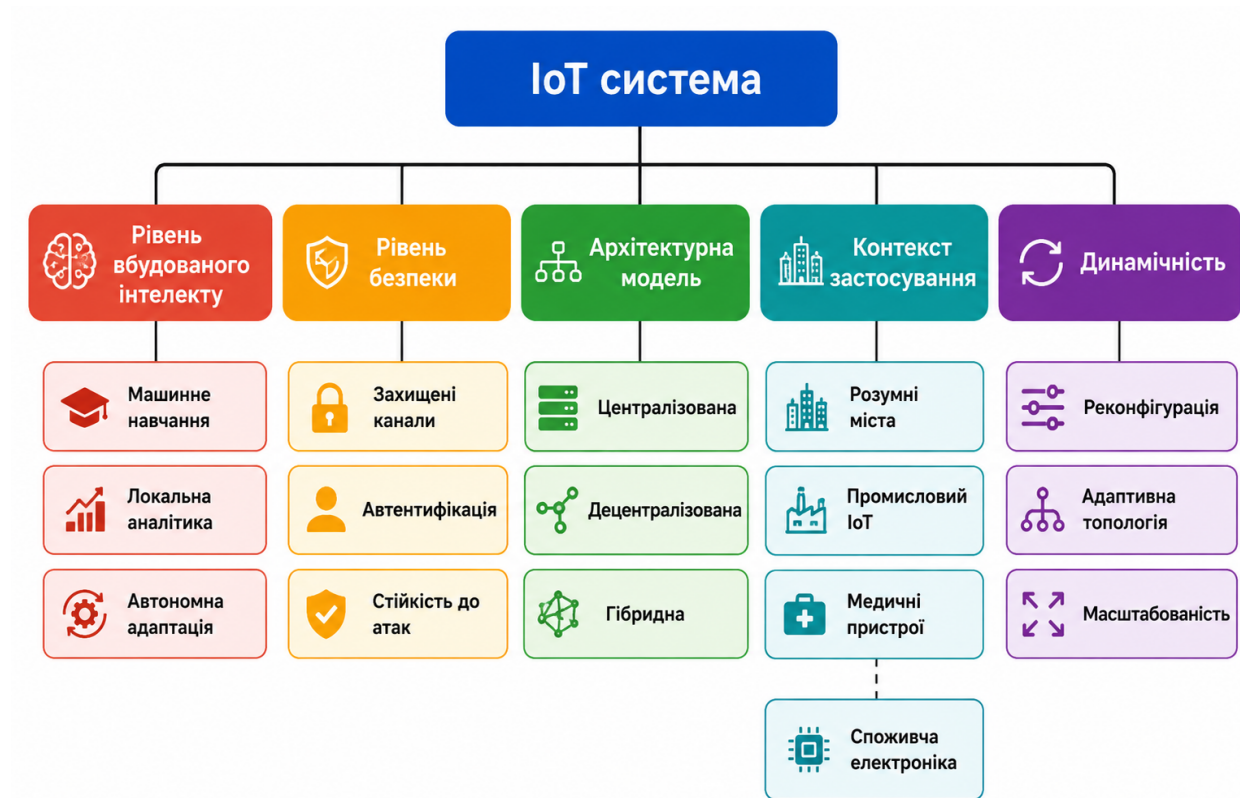


Рисунок 2.1 – Концептуальна схема інтелектуально-контекстної класифікації IoT-пристроїв

Таким чином, запропонована система критеріїв забезпечує комплексний опис IoT-пристроїв за п'ятьма взаємодоповнювальними характеристиками: рівнем інтелекту, захищеності, архітектурою взаємодії, контекстом функціонування та динамічністю середовища. На відміну від традиційних підходів, запропонована класифікація формує єдину інформаційну основу для побудови контекстно-ризикового профілю пристрою, який використовується на наступних етапах формалізації та оцінювання ризиків.

### 2.1.3. Формалізація моделі інтелектуально-контекстної класифікації

Для подальшого використання запропонованої моделі інтелектуально-контекстної класифікації під час оцінювання ризиків необхідно подати її у формалізованому вигляді. Формалізація забезпечує перехід від якісного опису характеристик IoT-пристроїв до структурованого представлення результатів класифікації та створює інформаційну основу для подальшого контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовища.

Для формального подання моделі введемо функцію інтелектуально-контекстної класифікації, результат якої для IoT-пристрою визначається як

$$C(d) = \langle I(d), S(d), A(d), C_x(d), D_y(d) \rangle \quad (2.1)$$

де: -  $C(d)$ - результат інтелектуально-контекстної класифікації IoT-пристрою;

$d$ - IoT-пристрій або підсистема;

- $I(d)$ - рівень вбудованого інтелекту;
- $S(d)$ - рівень безпеки;
- $A(d)$ - архітектура взаємодії;
- $C_x(d)$ - контекст функціонування;
- $D_y(d)$ - рівень динамічності.

З огляду на наведене, кожний IoT-пристрій описується багатовимірним набором характеристик, що відображає рівень вбудованого інтелекту, безпекові характеристики, архітектуру взаємодії, контекст функціонування та динамічність середовища. На відміну від традиційних підходів до класифікації, таке представлення використовується не лише для віднесення пристрою до певної категорії, а й для врахування його особливостей під час подальшого оцінювання ризиків інформаційної безпеки.

Для узгодженого поєднання визначених критеріїв у запропонованій моделі введено оператор семантичної конвергенції  $\Psi$ . Під семантичною конвергенцією розуміється формалізоване перетворення результатів класифікації за визначеними критеріями в структурований контекстно-ризиковий профіль IoT-пристрою зі збереженням змістового значення окремих характеристик.

$$w(d) = \Psi(C(d)) \quad (2.2)$$



де:

- $w(d)$ - інтегрований контекстно-ризиковий профіль IoT-пристрою;
- $\Psi$ - оператор семантичної конвергенції результатів інтелектуально-контекстної класифікації.
- $C(d)$ - результат класифікації IoT-пристрою за сукупністю критеріїв, визначених у (2.1).

Оператор семантичної конвергенції  $\Psi$  не передбачає зведення визначених критеріїв до одного інтегрального числового показника. Його призначення полягає у структурованому об'єднанні результатів класифікації зі збереженням інформації про особливості конкретного IoT-пристрою та контекст його функціонування. Це дає змогу використовувати сформований профіль як інформаційну основу для подальшого контекстно-адаптивного оцінювання ризиків.

Сформований контекстно-ризиковий профіль  $w(d)$  не є окремою вхідною змінною системи нечіткого логічного виведення. Він використовується на етапі формування та контекстної інтерпретації параметрів оцінювання ризику, що забезпечує врахування особливостей конкретного IoT-пристрою та умов його функціонування. Механізм використання контекстно-ризикового профілю під час формування вхідних параметрів моделі оцінювання ризику розглянуто в підрозділі 2.2.4.

Безпосередні вхідні параметри моделі оцінювання ризику для IoT-пристрою подамо у вигляді:

$$\boxed{X(d) = \langle AC(d), TL(d), V(d), CAP(d), L(d), IS(d), BR(d) \rangle} \quad (2.3)$$

де:

- $X(d)$  вектор параметрів оцінювання ризику IoT-пристрою ;
- $AC(d)$  критичність активу (AssetCriticality);
- $TL(d)$  рівень загрози (ThreatLevel);
- $V(d)$  рівень вразливості (Vulnerability);
- $CAP(d)$  можливості потенційного порушника (AttackerCapability);
- $L(d)$ , імовірність реалізації загрози (Likelihood);
- $IS(d)$ , тяжкість можливих наслідків (ImpactSeverity);

- $BR(d)$ ризик прихованої компрометації (BackdoorRisk).

Враховуючи наведене, взаємозв'язок між результатом інтелектуально-контекстної класифікації, сформованим контекстно-ризиковим профілем та параметрами подальшого оцінювання ризику можна подати у вигляді:

$$\boxed{C(d) \xrightarrow{\Psi} w(d) \rightarrow X(d)} \quad (2.4)$$

Наведене подання розмежовує функціональне призначення складових запропонованої моделі:

- $C(d)$ характеризує результат класифікації IoT-пристрою за визначеними критеріями;
- $\Psi$  оператор забезпечує формування інтегрованого контекстно-ризикового профілю;
- сукупність  $X(d)$  визначає параметри, що використовуються на наступному етапі оцінювання ризику.

У межах запропонованої моделі семантична конвергенція реалізує три послідовні операції:

- узгодження різнорідних результатів класифікації в межах профілю конкретного IoT-пристрою;
- їх контекстуалізацію з урахуванням взаємозв'язків між визначеними критеріями;
- ризик-орієнтовану інтерпретацію характеристик для їх подальшого використання під час формування параметрів оцінювання ризику.

Оператор не передбачає арифметичного агрегування критеріїв та не формує інтегрального числового показника.

Тобто, інтелектуально-контекстна класифікація є початковою складовою процесу контекстно-адаптивного оцінювання ризиків. Сформований за допомогою оператора семантичної конвергенції профіль  $w(d)$ забезпечує структуроване представлення характеристик і контексту IoT-пристрою та створює інформаційну основу для формування параметрів подальшого оцінювання ризику.

На Рис. 2.2 наведено структурну схему формування інтегрованого контекстно-ризикового профілю IoT-пристрою та його взаємозв'язку з параметрами оцінювання ризику.

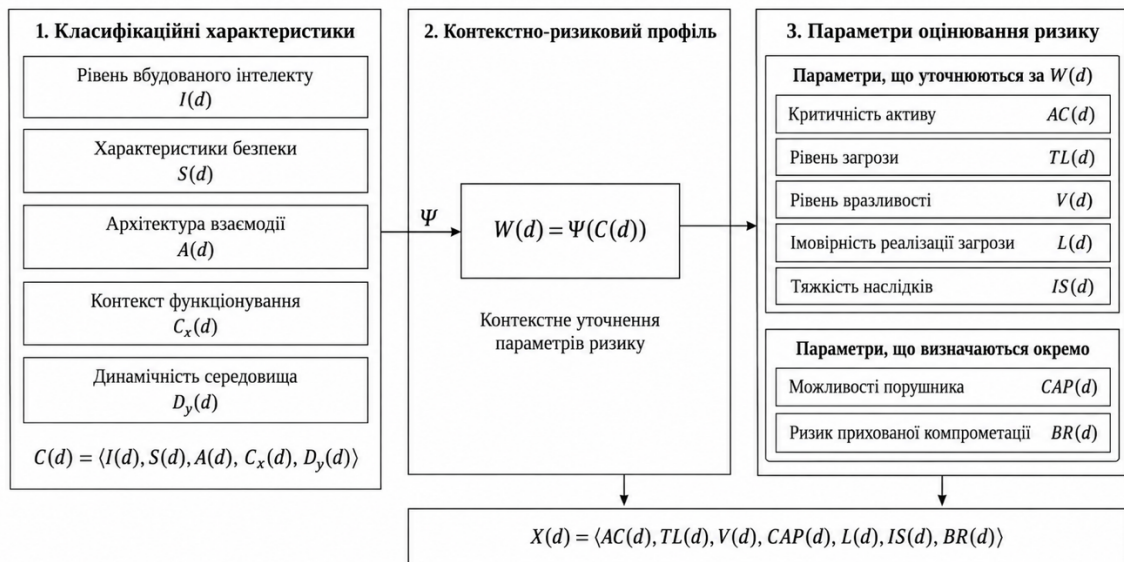


Рисунок 2.2 – Структурна схема формування контекстно-ризикового профілю IoT-пристрою та його взаємозв'язку з параметрами оцінювання ризику

#### 2.1.4. Порівняльний аналіз традиційних та інтелектуально-контекстних підходів

Проведений аналіз показав, що традиційні підходи до класифікації IoT-пристроїв переважно ґрунтуються на статичних технічних і функціональних характеристиках та недостатньо враховують контекст функціонування, рівень вбудованого інтелекту, динамічність середовища й характеристики безпеки пристроїв. Це обмежує можливості їх використання як інформаційної основи для контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ [117, 118, 121, 123].

Запропонована інтелектуально-контекстна модель спрямована на усунення зазначених обмежень шляхом комплексного врахування визначених критеріїв класифікації та формування на їх основі контекстно-ризикового профілю IoT-пристрою. Такий профіль забезпечує структуроване представлення характеристик пристрою та контексту його функціонування і створює

інформаційну основу для подальшого оцінювання ризиків. Порівняльну характеристику традиційних і запропонованого підходів наведено в Табл. 2.1.

*Таблиця 2.1 — Порівняльна характеристика традиційної та інтелектуально-контекстної класифікації IoT-пристроїв*

| <b>Критерій</b>                                | <b>Традиційні підходи</b>                                        | <b>Запропонована модель</b>                                                                                           |
|------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Ознаки класифікації                            | Переважно технічні та функціональні характеристики [112-114,116] | Рівень вбудованого інтелекту, безпека, архітектура взаємодії, контекст функціонування та динамічність                 |
| Урахування рівня вбудованого інтелекту         | Переважно не враховується [112,113]                              | Передбачено                                                                                                           |
| Урахування контексту функціонування            | Обмежене [114,116]                                               | Передбачено                                                                                                           |
| Урахування динамічності середовища             | Обмежене [113,116]                                               | Передбачено                                                                                                           |
| Урахування характеристик безпеки               | Фрагментарне [112-114]                                           | Передбачено                                                                                                           |
| Формування контекстно-ризикового профілю       | Не передбачено [112-114,116]                                     | Передбачено                                                                                                           |
| Зв'язок з оцінюванням ризиків                  | Переважно відсутній або опосередкований [112-114,116]            | Результати класифікації використовуються під час формування та контекстної інтерпретації параметрів оцінювання ризику |
| Використання в інформаційній технології аудиту | Переважно як засіб систематизації пристроїв [112-114]            | Як інформаційна основа для подальшого контекстно-адаптивного оцінювання ризиків                                       |

Проведене порівняння свідчить, що запропонована модель відрізняється від традиційних підходів не лише розширеним складом критеріїв класифікації, а й функціональним використанням її результатів. Сформований контекстно-ризиковий профіль забезпечує структуроване представлення характеристик IoT-пристрою та контексту його функціонування і використовується як інформаційна основа для формування та контекстної інтерпретації параметрів подальшого оцінювання ризиків. Це забезпечує взаємозв'язок процесів класифікації та оцінювання ризиків у межах інформаційної технології інтелектуального аудиту безпеки IoT-середовищ.

## **2.2. Формалізація критеріїв вразливостей та ризиків безпеки**

Після побудови інтелектуально-контекстної моделі класифікації наступним етапом є формалізація критеріїв оцінювання безпеки IoT-середовищ. Метою цього етапу є формалізоване подання вразливостей, загроз і ризиків, придатне для подальшого математичного моделювання. При цьому оцінювання виконується з урахуванням сформованого контекстно-ризикового профілю  $w(d)$ , що забезпечує адаптивний аналіз ризиків залежно від особливостей функціонування IoT-пристрою.

Сформований на попередньому етапі контекстно-ризиковий профіль  $w(d)$  використовується для врахування характеристик конкретного IoT-пристрою та контексту його функціонування під час формування й інтерпретації параметрів оцінювання ризику. Це забезпечує взаємозв'язок між результатами інтелектуально-контекстної класифікації та подальшим контекстно-адаптивним оцінюванням ризиків.

У цьому підрозділі виконано систематизацію типових вразливостей IoT-середовищ, формалізовано взаємозв'язок між активами, загрозами та ризиками, а також визначено множину критеріїв, яка використовується як вхідна інформація для побудови нечіткої моделі оцінювання ризиків.

### **2.2.1. Ідентифікація типових вразливостей IoT-середовищ**

Формалізація процесу оцінювання ризиків передбачає попередню систематизацію типових вразливостей, характерних для різних рівнів IoT-інфраструктури. Аналіз сучасних рекомендацій ENISA Threat Landscape , ISO/IEC 27005 [6,8] та практики побудови систем кіберзахисту показує, що більшість загроз може бути згрупована за чотирма основними категоріями: мережеві, протокольні, програмні та апаратні вразливості.

Мережеві вразливості - пов'язані з недостатнім захистом мережевої інфраструктури, відсутністю сегментації, використанням незахищених каналів передавання даних і слабкими механізмами контролю доступу. Їх експлуатація створює передумови для реалізації атак типу Man-in-the-Middle, DoS/DDoS, перехоплення трафіку та несанкціонованого доступу до ресурсів IoT-середовища [48,49].

Протокольні вразливості - обумовлені особливостями реалізації або обмеженнями протоколів MQTT, CoAP, ZigBee, BLE, LoRaWAN та інших технологій Інтернету речей. Вони можуть призводити до підроблення повідомлень, компрометації каналів обміну даними, несанкціонованого приєднання вузлів до мережі та порушення достовірності інформаційної взаємодії [49].

Програмні вразливості - виникають унаслідок помилок програмної реалізації, використання застарілих бібліотек, відсутності оновлень програмного забезпечення або недотримання принципів безпечного програмування. Такі вразливості використовуються для виконання довільного коду, поширення шкідливого програмного забезпечення, формування ботнетів і компрометації програмних компонентів IoT-систем [50].

Апаратні вразливості - пов'язані з фізичною компрометацією пристроїв, модифікацією мікропрограм, підміною компонентів або порушенням довіри до програмно-апаратної платформи [51]. Особливу небезпеку становлять *клеттографічні вразливості*, що виникають унаслідок навмисного вбудовування прихованих криптографічних механізмів у програмне чи апаратне забезпечення. На відміну від традиційних технічних дефектів, такі механізми можуть залишатися непомітними під час стандартного тестування, але забезпечувати прихований доступ до криптографічних ключів, службової інформації або функцій керування пристроєм [124]. Тому під час оцінювання ризиків безпеки IoT-середовищ необхідно враховувати не лише наявність відомих технічних вразливостей, а й ризики порушення криптографічної довіри та компрометації ланцюга постачання [77,78].

*Таблиця 2.2 – Класифікація типових вразливостей IoT-середовища*

| Категорія | Типові приклади                                                    | Потенційні наслідки            | Механізми протидії                                     |
|-----------|--------------------------------------------------------------------|--------------------------------|--------------------------------------------------------|
| Мережеві  | Відсутність шифрування, відкриті порти, слабка сегментація [48,49] | Перехоплення трафіку, DoS/DDoS | Сегментація мережі (VLAN), IDS/IPS, Zero Trust Network |

|             |                                                                 |                                                 |                                                   |
|-------------|-----------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------|
| Протокольні | Недостатня автентифікація у MQTT, CoAP, ZigBee [49,107]         | Підроблення даних, вставка фальшивих вузлів     | Secure MQTT, DTLS, криптографічна автентифікація  |
| Програмні   | Buffer overflow, SQL-injection, відсутність оновлень [21-24,50] | Виконання шкідливого коду, компрометація систем | Secure coding, OTA updates, sandboxing            |
| Апаратні    | Підміна мікросхем, бекдори у криптомодулях [22,23,51]           | Компрометація криптографічних операцій          | Secure Boot, TPM/TEE, контроль ланцюга постачання |

Проведена систематизація показує, що поряд із традиційними мережевими, протокольними та програмними вразливостями суттєве значення мають апаратні й криптографічні вразливості, пов'язані з порушенням довіри до компонентів IoT-систем. Ідентифіковані вразливості є одним із джерел інформації для подальшого формування параметрів оцінювання ризику  $w(d)$ , при цьому їх значущість розглядається з урахуванням характеристик і контексту функціонування IoT-пристрою, представлених у контекстно-ризиковому профілі.

### **2.2.2. Визначення зв'язку між вразливістю, активом і загрозою**

Побудова моделі оцінювання ризиків безпеки IoT-середовищ базується на формалізації взаємозв'язку між активами, вразливостями та загрозами. Саме взаємодія цих компонентів визначає можливість реалізації кіберінциденту та рівень потенційного ризику.

У межах дослідження актив розглядається як об'єкт, що потребує захисту, вразливість - як слабкість активу або механізмів його захисту, а загроза – як потенційна причина небажаного інциденту, здатного негативно вплинути на актив. Відповідно, наявність вразливості розглядається у взаємозв'язку з активом, для якого вона характерна, та загрозою, здатною її використати.

У загальному вигляді концептуальна залежність між активом, вразливістю та загрозою описується функцією

$$R = f(A, V, T) \quad (2.5)$$

де: -  $R$ - рівень ризику;

- $A$ -актив;
- $V$ - множина вразливостей активу;
- $T$ - множина потенційних загроз;
- $f$  -функціональна залежність, що відображає взаємозв'язок між активом, його вразливостями та потенційними загрозами під час формування ризику.

Співвідношення (2.5) має концептуальний характер і відображає загальну логіку формування ризику. Воно не визначає безпосередній спосіб числового обчислення його рівня, а встановлює взаємозв'язок між основними складовими, характеристики яких надалі конкретизуються через параметри моделі оцінювання ризику.

У запропонованому підході зазначена залежність доповнюється результатами інтелектуально-контекстної класифікації IoT-пристрою. Сформований на попередньому етапі контекстно-ризиковий профіль  $w(d)$ , містить структуровану інформацію про характеристики пристрою та контекст його функціонування і використовується під час подальшої інтерпретації параметрів оцінювання ризику. Це дає змогу розглядати активи, вразливості та загрози з урахуванням особливостей конкретного IoT-пристрою, а не ізольовано від умов його функціонування.

Тобто, концептуальне подання (2.5) та контекстно-ризиковий профіль  $w(d)$  виконують різні, але взаємопов'язані функції: співвідношення (2.5) визначає загальну логіку взаємозв'язку активу, вразливостей і загроз, тоді як  $w(d)$  забезпечує контекстну інформацію про пристрій, необхідну для подальшого формування та інтерпретації параметрів оцінювання ризику.

Для систематизації відповідності між типами активів IoT-середовища, характерними для них вразливостями, можливими загрозами та потенційними наслідками сформовано узагальнення, наведене в Табл. 2.3.



*Таблиця 2.3 –Відповідність типів активів IoT-середовища характерним вразливостям, загрозам та потенційним наслідкам*

| <b>Актив IoT-середовища</b>        | <b>Типові вразливості</b>                                             | <b>Можливі загрози</b>                                                | <b>Потенційні наслідки</b>                         |
|------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------|
| IoT-пристрої (сенсори, контролери) | Відсутність шифрування, слабка автентифікація, відкриті порти [48,49] | Несанкціонований доступ, підміна даних, DoS-атаки                     | Порушення цілісності даних, відмова у сервісі      |
| Комунікаційна мережа               | Недостатня сегментація, вразливості протоколів (MQTT, CoAP) [49,107]  | Перехоплення або модифікація трафіку                                  | Витік або компрометація конфіденційної інформації  |
| Хмарна інфраструктура              | Неправильна конфігурація доступу, SQL/NoSQL-ін'єкції [17,20]          | Захоплення облікових записів, викрадення даних                        | Компрометація сервісів, зниження довіри до системи |
| Мобільні та веб-додатки            | Недоліки авторизації, слабкі паролі, відсутність MFA [20,33]          | Фішинг, brute-force, повторні атаки                                   | Несанкціонований доступ до системи керування IoT   |
| Апаратні модулі безпеки            | Бекдори у мікрокодї, вразливості криптографічних бібліотек [21,22,51] | Експлуатація прихованих механізмів (зокрема криптографічних закладок) | Підрив цілісності криптографічних операцій         |

Наведена відповідність демонструє, що різні типи активів IoT-середовища характеризуються специфічними вразливостями та пов'язаними з ними загрозами, реалізація яких може призводити до різних за характером наслідків. Систематизовані таким чином відомості використовуються як інформаційна основа для подальшого формування параметрів оцінювання ризику.

### ***2.2.3. Формалізація критеріїв оцінювання ризику згідно з ISO/IEC 27005, EBIOS та ENISA Threat Landscape***

Після визначення взаємозв'язків між активами, вразливостями та загрозами необхідно сформувати систему критеріїв, яка забезпечує кількісне оцінювання ризиків безпеки IoT-середовищ. Саме ці критерії надалі використовуються як вхідні параметри нечіткої моделі оцінювання ризиків.

Під час формування системи критеріїв використано положення міжнародного стандарту ISO/IEC 27005 [6], методології EBIOS Risk Manager [36] та рекомендацій ENISA Threat Landscape [8]. Зазначені підходи використовуються як методологічна основа для визначення характеристик активів, загроз, вразливостей, можливостей потенційного порушника, імовірності реалізації загроз та можливих наслідків. З урахуванням специфіки IoT-середовищ систему критеріїв доповнено показником ризику прихованої компрометації.

*Формування системи критеріїв.* Особливості IoT-середовищ зумовлюють необхідність урахування не лише характеристик активів і загроз, а й вразливостей, можливостей потенційного порушника, імовірності реалізації загроз, можливих наслідків та ризику прихованої компрометації. З огляду на це для подальшого оцінювання ризиків визначено сім взаємопов'язаних критеріїв.

1. *Критичність активу(AC)*. Характеризує значущість IoT-пристрою або підсистеми для функціонування всієї інфраструктури. При визначенні критичності враховується не лише інформаційна цінність активу, а й можливі наслідки його компрометації для фізичних процесів [6,8].

2. *Рівень загрози (TL)*. Відображає тип потенційної атаки, її актуальність та відповідність сучасному ландшафту загроз IoT [8].

3. *Рівень вразливості(V)*. Відображає ступінь наявності та значущості слабких місць IoT-пристрою, програмного забезпечення, протоколів або компонентів інфраструктури, які можуть бути використані під час реалізації загрози [6].

4. *Спроможність атакувальника (CAP)*. Оцінює рівень ресурсів, кваліфікації та мотивації потенційного противника відповідно до принципів методології EBIOS Risk Manager [36].

5. *Імовірність реалізації загрози(L)*. Характеризує можливість реалізації визначеної загрози щодо конкретного активу з урахуванням наявних вразливостей та умов функціонування IoT-середовища [6].

6. *Тяжкість можливих наслідків(IS)*. Відображає очікуваний вплив реалізації загрози на конфіденційність, цілісність, доступність інформації, а також на безперервність функціонування фізичних процесів [6,8].

7. *Ризик прихованої компрометації(BR)*. На відміну від наведених критеріїв, є авторським доповненням запропонованої моделі та враховує можливість існування прихованих механізмів впливу (бекдорів, клептографічних модифікацій, компрометації криптографічних модулів), які можуть залишатися непоміченими традиційними засобами аудиту [124].

На відміну від класичних критеріїв, показник BR введено для врахування сценаріїв, у яких компрометація може не проявлятися через традиційні ознаки відомої вразливості або активної атаки. Конкретний порядок формування та інтерпретації цього параметра розглядається на наступних етапах побудови моделі оцінювання ризику.

У подальшому кожний із наведених критеріїв інтерпретується як окрема вхідна лінгвістична змінна нечіткої системи оцінювання ризиків.

*Таблиця 2.4 — Формалізовані критерії оцінювання ризиків інформаційної безпеки IoT-середовищ*

| Критерій                       | Позначення | Методологічна основа | Функціональне призначення                             |
|--------------------------------|------------|----------------------|-------------------------------------------------------|
| Критичність активу             | (AC)       | ISO/IEC 27005, ENISA | Оцінювання значущості активу                          |
| Рівень загрози                 | (TL)       | ISO/IEC 27005, ENISA | Характеристика актуальності та інтенсивності загрози  |
| Рівень вразливості             | (V)        | ISO/IEC 27005        | Характеристика слабких місць активу                   |
| Спроможність атакувальника     | (CAP)      | EBIOS Risk Manager   | Оцінювання можливостей потенційного порушника         |
| Імовірність реалізації загрози | (L)        | ISO/IEC 27005        | Оцінювання можливості реалізації загрози              |
| Тяжкість можливих наслідків    | (IS)       | ISO/IEC 27005, ENISA | Оцінювання потенційного впливу реалізації загрози     |
| Ризик прихованої компрометації | (BR)       | Авторське доповнення | Урахування ризику прихованих механізмів компрометації |

Проведений аналіз показує, що окремо жодна з розглянутих методологій не забезпечує повного врахування особливостей сучасних IoT-середовищ. Стандарт ISO/IEC 27005 визначає загальну структуру управління ризиками, методологія EBIOS деталізує аналіз можливостей атакувальника, тоді як ENISA характеризує актуальний ландшафт кіберзагроз.

У запропонованому підході зазначена система доповнюється показником BackdoorRisk(BR), що дає змогу окремо враховувати ризик прихованої компрометації, пов'язаної з недокументованими функціями, прихованими модифікаціями програмного або апаратного забезпечення та компрометацією критичних компонентів IoT-пристроїв.

Сукупність визначених критеріїв відповідає введеному в підрозділі 2.1.3 вектору параметрів оцінювання ризику  $X(d)$  (2.3).

#### ***2.2.4. Побудова структури вхідних параметрів для моделі нечіткого оцінювання ризиків***

Після формалізації системи критеріїв оцінювання ризику наступним етапом є визначення структури вхідних параметрів та порядку їх формування для подальшого використання в моделі нечіткого оцінювання ризиків. Відповідно до співвідношення (2.3), безпосередні вхідні параметри моделі представлені вектором  $X(d)$ , що містить сім складових:  $AC(d), TL(d), V(d), CAP(d), L(d), IS(d), BR(d)$ .

Особливістю запропонованого підходу є врахування результатів інтелектуально-контекстної класифікації під час формування та інтерпретації зазначених параметрів. На етапі класифікації для IoT-пристрою  $d$  визначається сукупність характеристик, яка за допомогою оператора семантичної конвергенції  $\Psi$  перетворюється у контекстно-ризиковий профіль  $w(d)$ . Сформований профіль містить узгоджене представлення відомостей про рівень вбудованого інтелекту, характеристики безпеки, архітектуру взаємодії, контекст функціонування та динамічність IoT-пристрою.

У межах запропонованої моделі семантична конвергенція  $\Psi$  реалізує узгодження різнорідних результатів класифікації, їх контекстуалізацію та ризик-

орієнтовану інтерпретацію. При цьому оператор не виконує арифметичного агрегування критеріїв, не формує інтегрального числового показника та безпосередньо не визначає значення вхідних параметрів моделі оцінювання ризику. Його результатом є структуроване контекстне представлення характеристик конкретного IoT-пристрою, що використовується на наступному етапі оцінювання.

Для формування значень параметрів вектора  $X(d)$ , крім контекстно-ризикового профілю, використовуються дані про поточний стан безпеки IoT-пристрою та середовища його функціонування. До них належать відомості про значущість активу, виявлені вразливості, актуальні загрози, характеристики потенційного порушника, умови реалізації загроз, можливі наслідки інцидентів та ознаки прихованої компрометації. Сукупність зазначених даних позначимо  $D_{sec}(d)$ .

Загальний інформаційний взаємозв'язок між контекстно-ризиковим профілем, даними про стан безпеки та вхідними параметрами моделі оцінювання ризику подамо у вигляді:

$$\{w(d), D_{sec}(d), \} \rightarrow X(d) \quad (2.6)$$

- $w(d)$  – контекстно-ризиковий профіль IoT-пристрою, сформований на основі результатів інтелектуально-контекстної класифікації;
- $D_{sec}(d)$  – сукупність даних про стан безпеки IoT-пристрою та середовища його функціонування;
- $X(d)$  – вектор вхідних параметрів оцінювання ризику, визначений співвідношенням (2.3).

Співвідношення (2.6) відображає інформаційну залежність між зазначеними складовими, а не окрему розрахункову функцію. Контекстно-ризиковий профіль  $w(d)$  не є додатковим вхідним параметром моделі нечіткого логічного виведення та не збільшує розмірність вектора  $X(d)$ . Його призначення полягає у врахуванні особливостей конкретного IoT-пристрою під час формування та інтерпретації параметрів оцінювання ризику.

Практично це означає:

- функціональне призначення та контекст використання пристрою  $AC(d)$ , враховуються під час визначення критичності активу і тяжкості можливих наслідків  $IS(d)$ ;
- характеристики безпеки та архітектури взаємодії – під час інтерпретації рівня вразливості  $V(d)$ , і рівня загрози  $TL(d)$ ;
- динамічність середовища та особливості функціонування – під час визначення рівня загрози та імовірності її реалізації  $L(d)$ ;
- $CAP(d)$ , формується на основі відомостей про можливості потенційного порушника;  $BR(d)$  – на основі ознак, що можуть свідчити про приховану компрометацію.

Таке представлення дає змогу розмежувати два типи інформації, що використовуються під час оцінювання ризику. Контекстно-ризиковий профіль  $w(d)$  характеризує особливості самого IoT-пристрою та умов його функціонування, тоді  $D_{sec}(d)$ , як відображає дані про поточний стан його безпеки. Їх спільне використання забезпечує формування вхідних параметрів з урахуванням не лише наявних загроз і вразливостей, а й функціональної ролі та контексту конкретного пристрою.

Структуру вхідних параметрів моделі оцінювання ризиків наведено в табл. 2.5.

Таблиця 2.5 – Структура вхідних параметрів моделі нечіткого оцінювання ризиків

| Позначення | Параметр           | Інформаційна основа формування                       | Контекстна інтерпретація                            |
|------------|--------------------|------------------------------------------------------|-----------------------------------------------------|
| (AC)       | AssetCriticality   | Дані про значущість активу                           | Функціональна роль і контекст використання пристрою |
| (TL)       | ThreatLevel        | Дані про актуальні загрози                           | Архітектура, контекст і динамічність середовища     |
| (V)        | Vulnerability      | Дані про виявлені вразливості                        | Характеристики безпеки та архітектури пристрою      |
| (CAP)      | AttackerCapability | Дані про можливості потенційного порушника           | Характер потенційного впливу та об'єкт атаки        |
| (L)        | Likelihood         | Дані про загрози, вразливості та умови їх реалізації | Контекст і динамічність функціонування              |
| (IS)       | ImpactSeverity     | Дані про можливі наслідки інциденту                  | Функціональна роль і значущість пристрою            |

|      |              |                                 |                                              |
|------|--------------|---------------------------------|----------------------------------------------|
| (BR) | BackdoorRisk | Ознаки прихованої компрометації | Характеристики безпеки та поведінки пристрою |
|------|--------------|---------------------------------|----------------------------------------------|

Побудована структура вхідних параметрів забезпечує узгоджений перехід від формалізованої системи критеріїв оцінювання ризику до вхідного інформаційного простору моделі.

При цьому контекстно-ризиковий профіль не є окремим вхідним параметром моделі оцінювання ризику, а використовується для контекстної інтерпретації тих складових, значення яких залежать від функціональної ролі, архітектури, характеристик безпеки та умов функціонування конкретного IoT-пристрою. Подальше подання сформованих параметрів у вигляді лінгвістичних змінних та визначення їх функцій належності розглянуто в підрозділі 2.3.1.

### **2.3. Метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення**

В умовах невизначеності, динамічності та гетерогенності IoT-середовищ оцінювання ризиків ускладнюється неповнотою та контекстною залежністю інформації про загрози, вразливості, можливості потенційного порушника та наслідки інцидентів. За таких умов доцільним є застосування нечіткої логіки, яка дає змогу використовувати лінгвістичні оцінки та враховувати нечіткість меж між рівнями ризику [125–128].

У межах дисертаційного дослідження під методом контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ розуміється впорядкована сукупність процедур подання вхідних параметрів оцінювання ризику у вигляді лінгвістичних змінних, їх фазифікації, застосування бази нечітких продукційних правил, агрегування результатів нечіткого логічного виведення та дефазифікації з формуванням інтегрального показника RiskLevel. Контекстна адаптивність методу забезпечується врахуванням контекстно-ризикового профілю IoT-пристрою під час формування та інтерпретації вхідних параметрів оцінювання ризику.

Контекстна адаптивність запропонованого методу реалізується на рівні інформаційного представлення об'єкта оцінювання. Залежно від функціональної ролі IoT-пристрою, архітектури його взаємодії, характеристик безпеки, контексту функціонування, динамічності середовища та поточного стану

інформаційної безпеки формуються й інтерпретуються значення семи вхідних параметрів оцінювання ризику. Функції належності та база нечітких продукційних правил у межах реалізованої FIS-моделі залишаються фіксованими.

Отже, адаптація полягає не в динамічній зміні математичного апарату нечіткого логічного виведення, а в контекстно залежному формуванні його вхідного інформаційного простору та повторному оцінюванні RiskLevel у разі зміни характеристик пристрою або стану IoT-середовища.

Для реалізації запропонованого методу використано систему нечіткого логічного виведення типу Mamdani, яка забезпечує інтерпретованість правил та можливість формалізації експертних знань [129, 130]. Вхідну основу моделі становить сформований у підрозділі 2.2  $X(d)$  вектор параметрів, що включає критичність активу, рівень загрози, вразливість, спроможність атакувальника, імовірність реалізації загрози, тяжкість можливих наслідків та ризик прихованої компрометації.

### ***2.3.1. Визначення лінгвістичних змінних та функцій належності***

Сформований у підрозділі 2.2 вектор вхідних параметрів  $X(d)$  є інформаційною основою побудови моделі нечіткого оцінювання ризиків. На цьому етапі кожний параметр вектора подається як лінгвістична змінна, для якої визначаються універсум значень, множина лінгвістичних термів та відповідні функції належності [126, 127]. Такий підхід забезпечує перехід від сформованих параметрів оцінювання ризику до їх нечіткого подання та подальшого використання в системі нечіткого логічного виведення.

Для уніфікованого подання параметрів моделі використовується єдиний універсум значень:

$$U = [0; 10] \quad (2.7)$$

що забезпечує узгоджене представлення різномірних параметрів та спрощує подальше визначення функцій належності і програмну реалізацію моделі в середовищі MATLAB Fuzzy Logic Toolbox.



*Формалізація лінгвістичних змінних.* кожна лінгвістична змінна моделі подається у вигляді –

$$L_i = \langle U_i, T_i, \mu_i, R_i, M_i \rangle \quad (2.8)$$

де: -  $U_i$  -універсум значень;

- $T_i$  —-множина лінгвістичних термів;
- $\mu_i(x)$ -множина функцій належності відповідних лінгвістичних термів;
- $R_i$  - правила формування термів;
- $M_i$  -процедура інтерпретації.

Наведена формалізація відповідає класичному визначенню лінгвістичної змінної, запропонованому Л. Заде[126], та використовується як базова модель у системах нечіткого логічного висновку[127,128]. Її застосування забезпечує єдині принципи опису всіх параметрів ризику незалежно від їх фізичної природи.

Відповідно до співвідношення (2.3), модель використовує сім вхідних лінгвістичних змінних:  $AC(d), TL(d), V(d), CAP(d), L(d), IS(d), BR(d)$ , які характеризують відповідно критичність активу, рівень загрози, рівень вразливості, спроможність потенційного порушника, імовірність реалізації загрози, тяжкість можливих наслідків та ризик прихованої компрометації.

*Множина вхідних лінгвістичних змінних.* Відповідно до структури (2.3), сформованої у підрозділі 2.2, модель використовує сім вхідних параметрів. Для змінних критичність активу, рівень загрози, рівень вразливості, спроможність потенційного порушника, імовірність реалізації загрози, тяжкість можливих наслідків та ризик прихованої компрометації використовується трирівнева множина лінгвістичних термів *Low, Medium, High*. Для змінної *AttackerCapability* застосовано терми *Basic, Intermediate, Advanced*, які змістовно характеризують рівень підготовки та технічних можливостей потенційного порушника.

Вихідною лінгвістичною змінною моделі є *RiskLevel*, що характеризує інтегральний рівень ризику. Для неї використано чотири лінгвістичні терми: *Low, Moderate, High, Critical*. Додаткове виділення терма *Critical* дає змогу відокремити сценарії з найвищим рівнем ризику, що потребують першочергового реагування.

*Вибір функцій належності.* З урахуванням вимог інтерпретованості експертами, простоти параметризації, обчислювальної ефективності та

сумісності із середовищем MATLAB Fuzzy Logic Toolbox для більшості змінних використано трикутні функції належності

$$\mu(x) = \text{trimf}(a, b, c) \quad (2.9)$$

які забезпечують плавний лінійний перехід між сусідніми лінгвістичними оцінками та широко застосовуються під час побудови систем нечіткого логічного висновку [131].

Наприклад, для змінної *Threat Level* використовуються функції:

$$\begin{aligned} \text{Low} &= \text{trimf}(0, 0, 4) \\ \text{Medium} &= \text{trimf}(3, 5, 7) \\ \text{High} &= \text{trimf}(6, 10, 10) \end{aligned} \quad (2.10)$$

Для опису крайніх областей універсуму використано трапецієподібні функції належності:

$$\mu(x) = \text{trapmf}(a, b, c, d) \quad (2.11)$$

які забезпечують області насичення та дозволяють коректно моделювати граничні рівні ризику. Зокрема:

$$\text{Critical} = \text{trapmf}(7, 9, 10, 10) \quad (2.12)$$

*Нормування параметрів.* Оскільки початкові показники мають різну фізичну природу та різні діапазони зміни, перед поданням до системи нечіткого висновку всі вони нормуються до єдиного універсуму  $[0; 10]$ . Це забезпечує порівнюваність параметрів, уніфікує процедуру побудови функцій належності та дозволяє використовувати єдину структуру бази знань.

Нормування здійснюється за співвідношенням:

$$\hat{x} = 10 \cdot \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (2.13)$$

де: -  $x$ — початкове значення параметра;

-  $x_{\min}, x_{\max}$ — мінімальне та максимальне значення параметра;

-  $\hat{x}$ — нормоване значення.

Склад лінгвістичних змінних моделі наведено в Табл. 2.6.

Таблиця 2.6 – Склад лінгвістичних змінних моделі нечіткого оцінювання ризиків

| Позначення | Назва змінної      | Лінгвістичні терми            |
|------------|--------------------|-------------------------------|
| (AC)       | AssetCriticality   | Low, Medium, High             |
| (TL)       | ThreatLevel        | Low, Medium, High             |
| (V)        | Vulnerability      | Low, Medium, High             |
| (CAP)      | AttackerCapability | Basic, Intermediate, Advanced |

|      |                |                               |
|------|----------------|-------------------------------|
| (L)  | Likelihood     | Low, Medium, High             |
| (IS) | ImpactSeverity | Low, Medium, High             |
| (BR) | BackdoorRisk   | Low, Medium, High             |
| (R)  | RiskLevel      | Low, Moderate, High, Critical |

Побудована система лінгвістичних змінних забезпечує нечітке подання сформованих входних параметрів  $X(d)$  та створює основу для їх фазифікації і подальшого застосування бази нечітких продукційних правил. Контекстні особливості IoT-пристрою на цьому етапі вже враховані під час попереднього формування та інтерпретації параметрів  $X(d)$ , тому контекстно-ризиковий профіль  $w(d)$  не є окремою входною змінною системи нечіткого логічного виведення.

Послідовність нечіткого подання сформованих входних параметрів моделі наведено на рис. 2.3.



Рисунок 2.3 – Послідовність формування нечіткого подання входних параметрів моделі оцінювання ризику

### 2.3.2. Побудова та оптимізація бази нечітких продукційних правил для аудиту безпеки IoT

Після визначення лінгвістичних змінних і функцій належності наступним етапом є формування бази нечітких продукційних правил, яка визначає логіку взаємозв'язку між вхідними параметрами та інтегральним рівнем ризику *RiskLevel*.

У запропонованій моделі продукційні правила відображають характерні ризикові сценарії IoT-середовищ та взаємозв'язки між критичністю активу, рівнем загрози, рівнем вразливості, спроможністю потенційного порушника, імовірністю реалізації загрози, тяжкістю можливих наслідків і ризиком прихованої компрометації. Контекстні особливості конкретного IoT-пристрою враховуються через значення вхідних параметрів, сформованих та інтерпретованих відповідно до підходу, описаного у підрозділі 2.2.

*Загальна структура нечіткого продукційного правила.*

Нечіткі продукційні правила формуються за класичною схемою Mamdani типу IF–THEN:

$$R_j: IF (A_1 = T_1) \wedge (A_2 = T_2) \wedge \dots \wedge (A_n = T_n) THEN Risk = T_r \quad (2.14)$$

де  $R_j$  -  $j$ -те продукційне правило;  $A_i$ - вхідна лінгвістична змінна;  $T_i$ - відповідний лінгвістичний терм;  $Risk$ - вихідна змінна рівня ризику;  $T_r$ - лінгвістичний терм вихідної змінної.

Умова правила може містити як повну множину вхідних змінних, так і їх змістовно обґрунтовану підмножину. Це дозволяє описувати окремі сценарії аудиту без необхідності включення до кожного правила всіх параметрів моделі. Кожне правило формалізує певний експертний сценарій розвитку кіберінциденту та визначає відповідний рівень ризику.

Ступінь активації правила визначається на основі ступенів належності фактичних значень вхідних параметрів термам, зазначеним у його передумові. За використання операції нечіткої кон'юнкції типу *minimum* ступінь активації  $j$ -го правила визначається як:

$$\alpha_j = \min\{\mu_{T_1}(A_1), \mu_{T_2}(A_2) \dots \mu_{T_n}(A_n)\} \quad (2.15)$$

Тобто, кожне продукційне правило визначає експертно сформований причинно-наслідковий зв'язок між певною комбінацією характеристик ризику та відповідним рівнем RiskLevel, а ступінь його активації залежить від поточних значень вхідних параметрів.

*Принципи формування продукційної бази.*

База нечітких продукційних правил формується з урахуванням таких принципів:

- посилення інтегрального ризику зі зростанням критичності активу та масштабу можливих наслідків;
- непропорційне підвищення ризику за одночасної дії декількох небезпечних факторів;
- урахування рівня підготовки та технічних можливостей потенційного атакувальника;
- підвищена пріоритетність сценаріїв, пов'язаних із прихованою компрометацією, модифікацією прошивок, компонентів і ланцюга постачання;
- адаптація змісту та пріоритетності правил відповідно до контекстно-ризикового профілю IoT-пристрою;
- відсутність логічно суперечливих правил з однаковими передумовами та різними висновками.

Особливістю запропонованої моделі є використання параметра BackdoorRisk, що дає змогу враховувати ризик потенційної прихованої компрометації поряд з іншими характеристиками безпеки. Високе значення цього параметра не розглядається ізольовано як безумовна ознака критичного ризику, а оцінюється у взаємозв'язку з критичністю активу, тяжкістю можливих наслідків та іншими вхідними параметрами.

Такий підхід забезпечує чутливість моделі до сценаріїв, пов'язаних із прихованими механізмами впливу, недокументованими функціями, модифікаціями програмних і апаратних компонентів та іншими ознаками прихованої компрометації.

Приклади характерних продукційних правил наведено в Табл. 2.7.

Таблиця 2.7 – Приклади продукційних правил нечіткої моделі оцінювання ризику

| № | Умова (IF)                                                                             | Висновок (THEN)       |
|---|----------------------------------------------------------------------------------------|-----------------------|
| 1 | Threat Level = High AND Vulnerability Level = High<br>AND Asset Criticality = High     | Risk Level = Critical |
| 2 | Backdoor / Covert Risk = High AND Asset Criticality<br>= High                          | Risk Level = Critical |
| 3 | Backdoor / Covert Risk = High AND Impact Severity =<br>High                            | Risk Level = Critical |
| 4 | Likelihood of Exploitation = High AND Attacker<br>Capability = Advanced                | Risk Level = High     |
| 5 | Asset Criticality = High AND Vulnerability Level =<br>Medium AND Threat Level = Medium | Risk Level = High     |
| 6 | Threat Level = Low AND Vulnerability Level = Low<br>AND Backdoor / Covert Risk = Low   | Risk Level = Low      |

Наведені правила демонструють загальну логіку моделі. Перше правило описує сценарій одночасної високої критичності активу, загрози та вразливості. Друге і третє правила відображають посилений вплив ризику прихованої компрометації у поєднанні з високою критичністю активу або значними наслідками. Четверте правило враховує поєднання високої імовірності експлуатації з розвиненими можливостями атакувальника. Шосте правило визначає сценарій низького ризику за відсутності суттєвих технічних і прихованих загроз.

*Необхідність оптимізації продукційної бази.* У разі побудови повної бази правил їх кількість швидко зростає зі збільшенням числа вхідних змінних і кількості лінгвістичних термів. Максимальна кількість можливих правил визначається як

$$N_{\max} = \prod_{i=1}^m k_i \quad (2.16)$$

де  $m$  — кількість вхідних лінгвістичних змінних;  $k_i$  — кількість термів  $i$ -ї змінної.

Запропонована модель містить сім вхідних змінних. Для шести з них використано по три лінгвістичні терми. Тому максимальна кількість можливих продукцій становить

$$N_{\max} = 3^6 \cdot 3 = 287 \quad (2.17)$$

Формування повної бази з 2187 правил є недоцільним. Значна частина можливих комбінацій відповідає малоймовірним, логічно несумісним або практично неінформативним сценаріям. Крім того, надмірна кількість продукцій ускладнює експертну перевірку бази знань, знижує її інтерпретованість і збільшує обчислювальні витрати.

З метою скорочення продукційної бази у роботі запропоновано метод її експертної оптимізації, спрямований на видалення надлишкових і нереалістичних правил із одночасним збереженням покриття типових та критичних сценаріїв аудиту безпеки IoT [132,133].

*Метод експертної оптимізації продукційної бази.* Експертна оптимізація продукційної бази реалізується як послідовність взаємопов'язаних етапів.

1. Формування початкового простору правил. На основі множини вхідних лінгвістичних змінних формується простір допустимих комбінацій їх термів. На цьому етапі визначається верхня межа кількості правил і формується початкова множина потенційних продукцій.
2. Аналіз досяжності сценаріїв. Із початкової множини видалюються правила, передумови яких відповідають практично нереалістичним, взаємно несумісним або малоймовірним станам IoT-системи.
3. Виявлення надлишкових продукцій. Аналізуються правила з близькими передумовами та однаковими висновками. Надлишкові продукції видалюються або об'єднуються в узагальнені правила без втрати їх основного семантичного змісту.
4. Виділення пріоритетних сценаріїв. Окремо формуються правила для сценаріїв, пов'язаних із високою критичністю активів, значними наслідками, високою імовірністю експлуатації та ризиком прихованої компрометації. Для таких правил можуть установлюватися підвищені вагові коефіцієнти.
5. Перевірка несуперечності бази. Виконується пошук правил з однаковими або еквівалентними передумовами, але різними висновками. Виявлені суперечності усуваються шляхом експертного уточнення умов або зміни ваг правил.

6. Перевірка повноти покриття. Оптимізована база перевіряється щодо наявності правил для типових, граничних і критичних сценаріїв аудиту. Особлива увага приділяється сценаріям високого ризику та прихованої компрометації.

У результаті виконання зазначених етапів формується компактна, інтерпретована та обчислювально ефективна база нечітких продукційних правил, придатна для використання в системі нечіткого висновку Mamdani.

Запропонований метод оптимізації не зводиться лише до механічного скорочення кількості правил. Він є процедурою інтелектуальної формалізації експертних знань, у межах якої визначаються значущі взаємозв'язки між параметрами ризику, усуваються логічно надлишкові продукції та забезпечується покриття критичних сценаріїв. Це створює передумови для адаптації бази знань до різних типів IoT-пристроїв і подальшого її розширення відповідно до появи нових класів кіберзагроз.

### ***2.3.3. Програмна реалізація системи нечіткого висновку типу Mamdani***

Для програмної реалізації розробленої моделі використано середовище MATLAB із пакетом Fuzzy Logic Toolbox та подальшою інтеграцією із Simulink. Такий підхід забезпечує побудову системи нечіткого логічного виведення типу Mamdani, налаштування функцій належності, реалізацію продукційної бази та проведення обчислювальних експериментів для різних сценаріїв функціонування IoT-середовищ.

Використання системи нечіткого висновку типу Mamdani зумовлено її інтерпретованістю, можливістю формалізації експертних знань і прозорим поданням причинно-наслідкових зв'язків між вхідними параметрами та інтегральним рівнем ризику [129]. Загальну архітектуру програмної реалізації наведено на Рис. 2.4.





*Рисунок 2.4 – Архітектура програмної реалізації системи нечіткого оцінювання ризиків у середовищі MATLAB/Simulink.*

Програмна реалізація моделі включає такі основні етапи:

- створення структури системи нечіткого висновку (*Fuzzy Inference System, FIS*);
- визначення множини вхідних і вихідної лінгвістичних змінних;
- налаштування функцій належності;
- завантаження оптимізованої бази нечітких продукційних правил;
- виконання процедури нечіткого висновку Mamdani;
- дефазифікацію результатів;
- передачу інтегральної оцінки ризику до моделей імітаційного моделювання Simulink.

Основою програмної реалізації є система нечіткого висновку, структура якої описується співвідношенням:

$$FIS = \langle X, R, \mu, Bs, Agg, Def \rangle \quad (2.18)$$

де  $X$  - множина вхідних лінгвістичних змінних;

$R$  - вихідна лінгвістична змінна;

$\mu$  - сукупність функцій належності;

$Bs$  - оптимізована база нечітких продукційних правил;

*Agg* - механізм агрегування результатів активованих правил;

*Def* - процедура дефазифікації.

Множина вхідних змінних, функції належності та база продукційних правил відповідають моделі, сформованій у підрозділах 2.3.1–2.3.2. Вихідною змінною системи є *Risk Level*, що характеризує інтегральний рівень ризику інформаційної безпеки IoT-середовища.

*Інтеграція із середовищем MATLAB/Simulink.* Практична реалізація моделі виконана із застосуванням *MATLAB Fuzzy Logic Toolbox*, який забезпечує створення системи нечіткого висновку, налаштування функцій належності, редагування продукційної бази, аналіз поверхонь нечіткого висновку та візуалізацію результатів оцінювання ризиків [134].

Після формування системи нечіткого висновку модель імпортується до блока *Fuzzy Logic Controller* середовища *Simulink*, де використовується як окремий функціональний модуль у складі інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ..

Архітектурно блок нечіткого висновку функціонує як незалежний програмний компонент, що приймає на вході нормалізовані параметри ризику та формує інтегральний показник *Risk Level*, який надалі використовується для підтримки прийняття рішень, вибору заходів захисту та адаптивного налаштування політик безпеки.

Крім використання синтетичних тестових сценаріїв, реалізована модель допускає підключення реальних потоків телеметричних даних від IoT-пристроїв, що забезпечує можливість експериментального дослідження її поведінки за різних умов функціонування та сценаріїв розвитку кіберінцидентів.

Тобто, програмна реалізація системи нечіткого висновку типу *Mamdani* у середовищі *MATLAB/Simulink* забезпечує практичне використання розробленої моделі для інтегрального оцінювання ризиків безпеки IoT-середовищ. Реалізований програмний модуль створює основу для проведення експериментальних досліджень розробленого методу та запропонованої інформаційної технології, результати яких наведено в наступному підрозділі.

### 2.3.4. Аналіз роботи моделі на тестових сценаріях

Для перевірки працездатності, адекватності та інтерпретованості розробленої моделі проведено серію обчислювальних експериментів, що імітують типові сценарії функціонування IoT-середовищ із різними комбінаціями рівнів загроз, вразливостей, наслідків кібератак та ризику прихованої компрометації.

Обчислення виконувалися у середовищі *MATLAB* із використанням розробленої моделі нечіткого висновку *IoT\_Risk\_FIS\_40rules.fis*, реалізованої засобами *MATLAB Fuzzy Logic Toolbox*. Для оцінювання інтегрального рівня ризику використовувався механізм нечіткого висновку типу Mamdani, параметри якого визначено у попередніх підрозділах.

З метою перевірки адекватності роботи моделі сформовано три характерні тестові сценарії, що відповідають низькому, типовому та високому рівням кіберризiku.

Таблиця 2.8 – Результати оцінювання тестових сценаріїв

| Сценарій | Характеристика                                   | Значення Risk Level | Лінгвістична інтерпретація |
|----------|--------------------------------------------------|---------------------|----------------------------|
| 1        | Низький рівень ризику                            | 1.61                | Low                        |
| 2        | Типовий режим функціонування                     | 4.00                | Medium–High                |
| 3        | Високий рівень ризику та прихована компрометація | 7.62                | High–Critical              |

*Сценарій 1 - низький рівень ризику.*

У першому сценарії всі параметри, що характеризують рівень загроз, вразливостей, можливостей атакувальника та ризику прихованої компрометації, набували мінімальних значень.

За результатами нечіткого висновку отримано Risk Level  $\approx 1.61$ , що відповідає області лінгвістичного терма Low.

Отриманий результат підтверджує коректність роботи моделі: за відсутності суттєвих загроз вона не формує завищених оцінок ризику, забезпечуючи низьку ймовірність хибних спрацьовувань.

*Сценарій 2 - типовий режим функціонування.*

У другому сценарії основні параметри ризику набували середніх значень. За результатами моделювання отримано  $RiskLevel \approx 4,00$ , що відповідає проміжній області між лінгвістичними оцінками *Medium* та *High*. Результат демонструє поступове зростання інтегральної оцінки за сукупного підвищення значень вхідних параметрів.

*Сценарій 3 - високий рівень ризику та прихована компрометація.*

У третьому сценарії для параметрів *ThreatLevel*, *Vulnerability*, *AttackerCapability*, *Likelihood* та *ImpactSeverity* задано високі значення, а параметр *BackdoorRisk* характеризував наявність виражених ознак потенційної прихованої компрометації. У результаті отримано  $RiskLevel \approx 7,62$ , що відповідає області між лінгвістичними оцінками *High* та *Critical*.

За результатами моделювання отримано  $Risk Level \approx 7.62$ , що відповідає області між лінгвістичними термами *High* та *Critical*.

Проведені експерименти показали, що збільшення значення параметра *Backdoor Risk* навіть без максимальних значень інших факторів приводить до істотного зростання інтегральної оцінки ризику. Це пояснюється тим, що приховані механізми компрометації можуть тривалий час залишатися непоміченими традиційними засобами моніторингу, створюючи додатковий рівень невизначеності під час оцінювання безпеки IoT-систем.

Отриманий результат демонструє, що параметр *BackdoorRisk* бере участь у формуванні інтегральної оцінки ризику разом з іншими вхідними параметрами. Його підвищене значення у поєднанні з високими значеннями інших факторів активує продукційні правила, орієнтовані на сценарії прихованої компрометації, що приводить до підвищення результуючого значення *RiskLevel*.

*Аналіз поверхонь нечіткого висновку.* Для додаткового дослідження поведінки моделі використовувався інструмент *Surface Viewer*, який входить до складу *MATLAB Fuzzy Logic Toolbox* та забезпечує візуалізацію поверхонь нечіткого висновку.

На Рис. 2.5 наведено приклад поверхні залежності інтегрального рівня ризику від двох найбільш впливових параметрів моделі.

Аналіз поверхні дає змогу простежити характер зміни інтегрального показника *RiskLevel* залежно від комбінації значень вибраних параметрів. Нелінійний характер поверхні зумовлений спільною дією функцій належності та бази нечітких продукційних правил Mamdani. Перехід між окремими областями ризику відбувається поступово, що відповідає принципам нечіткого логічного виведення.

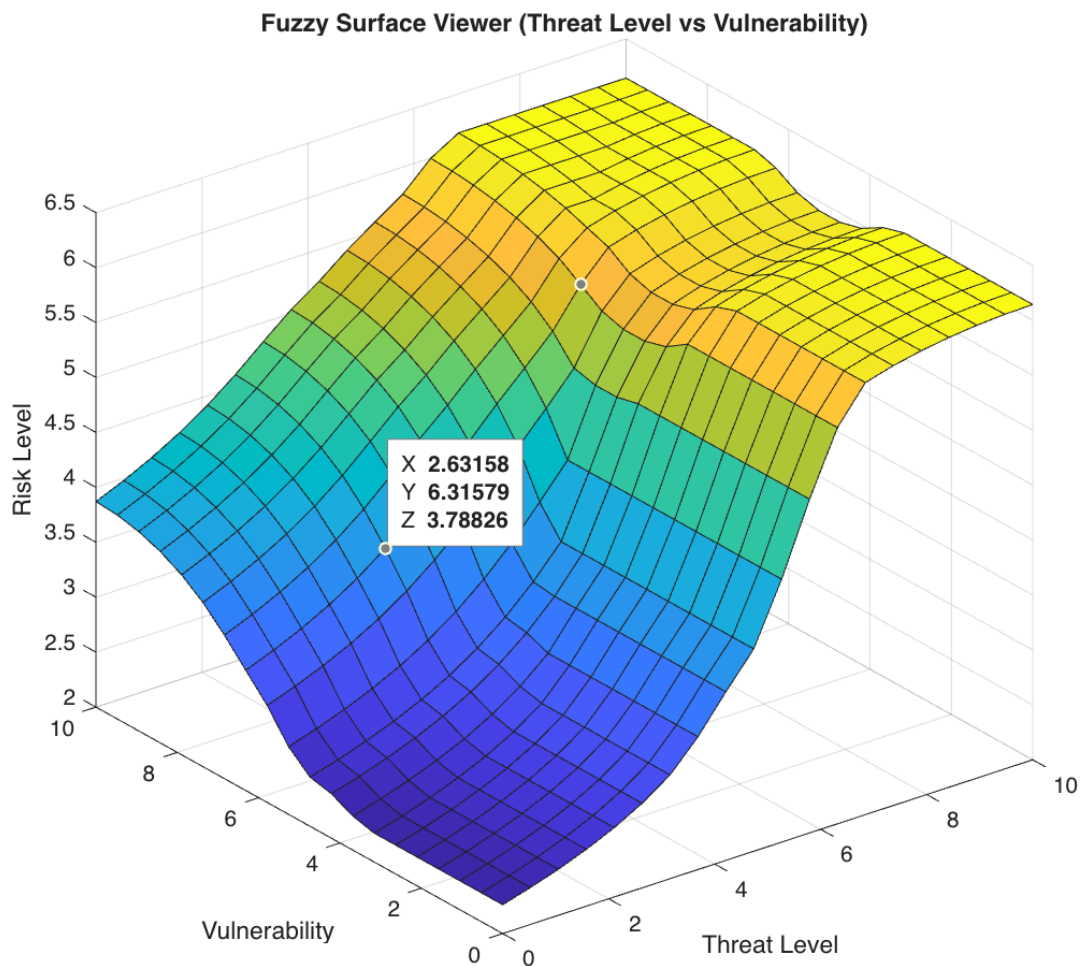


Рисунок 2.5 – Поверхня нечіткої моделі оцінювання ризику, побудована засобами MATLAB Surface Viewer

Проведена перевірка на контрольних сценаріях показала логічно узгоджену реакцію FIS-моделі на зміну вхідних параметрів: низькі значення факторів формують низький рівень *RiskLevel*, їх сукупне підвищення приводить до зростання інтегральної оцінки, а поєднання високих значень основних параметрів з ознаками прихованої компрометації формує високий рівень ризику.

Отримані результати підтверджують функціональну працездатність реалізованої FIS-моделі та можливість її використання для подальшої експериментальної перевірки розробленого методу контекстно-адаптивного оцінювання ризиків.

## **2.4. Інформаційна технологія контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ**

Розроблені у попередніх підрозділах модель інтелектуально-контекстної класифікації IoT-пристроїв, засоби формування контекстно-ризикового профілю та метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу *Mamdani* утворюють методичну основу для побудови інформаційної технології оцінювання ризиків безпеки IoT-середовищ. Їх спільне використання забезпечує послідовний перехід від збору та оброблення даних про IoT-пристрої і стан їх безпеки до формування контекстно-ризикового профілю, визначення вхідних параметрів оцінювання та отримання інтегрального показника рівня ризику.

У межах дисертаційного дослідження запропоновано інформаційну технологію контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ, яка об'єднує розроблені моделі, методи та алгоритми в єдиний інформаційно-аналітичний процес.

Особливістю запропонованої інформаційної технології є використання результатів інтелектуально-контекстної класифікації та сформованого контекстно-ризикового профілю під час формування й інтерпретації параметрів оцінювання ризику, що забезпечує врахування функціональної ролі, характеристик безпеки, архітектури взаємодії, контексту та динамічності функціонування конкретного IoT-пристрою.

Структуру, принципи функціонування та алгоритм роботи запропонованої інформаційної технології розглянуто у наступних підрозділах.

### **2.4.1. Структура інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ**

Запропонована інформаційна технологія контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ побудована за модульним

принципом та об'єднує розроблені моделі, методи й алгоритми в єдиний інформаційно-аналітичний процес. Її функціонування забезпечує послідовний перехід від збору та оброблення даних про IoT-пристрої і стан їх безпеки до формування контекстно-ризикового профілю, визначення вхідних параметрів та отримання інтегральної оцінки ризику.

Структурну основу інформаційної технології становлять три взаємопов'язані функціональні компоненти.

1. *Модель інтелектуально-контекстної класифікації IoT-пристроїв*, за допомогою якої визначаються характеристики пристрою за рівнем вбудованого інтелекту, безпеки, архітектурою взаємодії, контекстом функціонування та динамічністю. Результати класифікації за допомогою оператора семантичної конвергенції перетворюються у контекстно-ризиковий профіль, що використовується для подальшого формування та контекстної інтерпретації параметрів оцінювання ризику.
2. *Механізм формування вхідних параметрів оцінювання ризику*, який поєднує контекстно-ризиковий профіль  $w(d)$  з даними про поточний стан безпеки  $D_{sec}(d)$ , У результаті формується вхідний вектор:
 
$$X(d) = \langle AC(d), TL(d), V(d), CAP(d), L(d), IS(d), BR(d) \rangle$$
 що характеризує критичність активу, рівень загрози, вразливість, можливості потенційного порушника, імовірність реалізації загрози, тяжкість можливих наслідків та ризик прихованої компрометації.
3. *Метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Mamdani*, який забезпечує перетворення сформованих вхідних параметрів у інтегральний показник *RiskLevel*. Нечітке логічне виведення здійснюється з використанням визначених функцій належності та сформованої бази продукційних правил, що забезпечує врахування невизначеності та взаємного впливу факторів ризику.

Враховуючи наведене, функціональний взаємозв'язок основних складових інформаційної технології можна подати у вигляді :

$$C(d) \rightarrow w(d) \rightarrow \{w(d), D_{sec}(d)\} \rightarrow X(d) \rightarrow FIS_{Mamdani} \rightarrow RiskLevel$$

Наведена послідовність відображає перетворення результатів інтелектуально-контекстної класифікації та даних про стан безпеки у формалізовані параметри ризику з подальшим визначенням його інтегрального рівня.

Структурно інформаційна технологія реалізується у вигляді чотирьох взаємопов'язаних рівнів:

- рівень збору та попереднього оброблення даних;
- рівень інтелектуально-контекстної класифікації та аналізу стану безпеки;
- рівень формування параметрів і контекстно-адаптивного оцінювання ризиків;
- рівень підтримки прийняття рішень.

Кожний рівень реалізує визначену частину інформаційно-аналітичного процесу, а їх послідовна взаємодія забезпечує перетворення первинних даних IoT-середовища в інтегральну оцінку ризику та інформацію для підтримки прийняття рішень.

Структурно-функціональну схему запропонованої інформаційної технології наведено на Рис. 2.6.

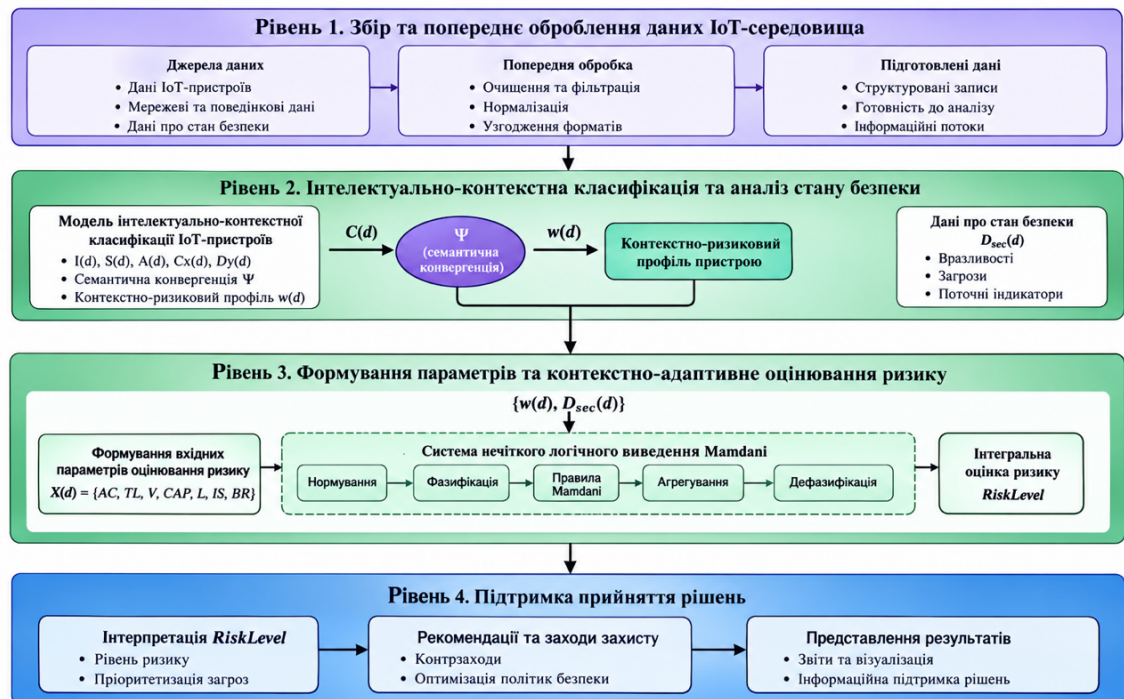


Рисунок 2.6 – Структурно-функціональна схема інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовища



Наведена схема визначає склад і взаємозв'язки основних функціональних компонентів інформаційної технології. Послідовність виконання операцій, формування інформаційних потоків та отримання інтегральної оцінки ризику розглянуто в наступному підрозділі.

#### ***2.4.2. Алгоритм функціонування інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ***

Алгоритм функціонування запропонованої інформаційної технології визначає послідовність процедур перетворення первинних даних IoT-середовища у вхідні параметри оцінювання ризику, їх оброблення засобами нечіткого логічного виведення та формування інтегрального показника RiskLevel. Контекстна адаптивність забезпечується врахуванням характеристик конкретного IoT-пристрою та умов його функціонування під час формування й інтерпретації параметрів оцінювання ризику.

Алгоритм включає сім взаємопов'язаних процедур.

1. *Збір та нормалізація даних.* На початковому етапі здійснюється отримання даних про IoT-пристрої та середовище їх функціонування, зокрема конфігураційних характеристик, мережевої та телеметричної інформації, журналів подій, відомостей про вразливості, оновлення програмного забезпечення, налаштування безпеки та інших доступних показників. Отримані дані очищуються, узгоджуються та приводяться до формату, придатного для подальшого аналізу.
2. *Інтелектуально-контекстна класифікація та формування контекстно-ризикового профілю.* Для кожного IoT-пристрою відповідно до моделі, розробленої у підрозділі 2.1, визначається сукупність класифікаційних характеристик, за допомогою оператора семантичної конвергенції результати класифікації узгоджуються та перетворюються у контекстно-ризиковий профіль. Сформований профіль характеризує особливості конкретного IoT-пристрою та контекст його функціонування і використовується під час подальшого формування та інтерпретації параметрів оцінювання ризику.

3. *Аналіз поточного стану безпеки.* На цьому етапі формується сукупність даних  $D_{sec}(d)$ , що характеризує поточний стан безпеки IoT-пристрою та середовища його функціонування. Аналізуються відомості про виявлені вразливості, актуальні загрози, можливості потенційного порушника, умови реалізації загроз, можливі наслідки інцидентів та ознаки, що можуть свідчити про приховану компрометацію.
4. *Формування входних параметрів оцінювання ризику.* На основі спільного використання контекстно-ризикового профілю та даних про поточний стан безпеки формується вектор входних параметрів
5. *Контекстно-адаптивне оцінювання ризику.* Сформовані параметри приводяться до встановленого діапазону значень і передаються до системи нечіткого логічного виведення типу *Mamdani*. Послідовно виконуються фазифікація входних параметрів, активація сформованої бази нечітких продукційних правил, агрегування результатів та дефазифікація. Результатом є числове значення інтегрального показника *RiskLevel*, що характеризує рівень ризику для досліджуваного IoT-пристрою.
6. *Інтерпретація результатів та підтримка прийняття рішень.* Отримане значення *RiskLevel* інтерпретується відповідно до встановлених рівнів ризику. На його основі здійснюється пріоритизація ризиків та формуються рекомендації щодо вибору відповідних технічних і організаційних заходів захисту.
7. *Актуалізація даних та повторне оцінювання.* У разі надходження нових даних про пристрій, зміни контексту його функціонування або стану безпеки відповідні інформаційні складові актуалізуються. Після цього повторно виконуються необхідні процедури формування контекстно-ризикового профілю, входних параметрів та оцінювання *RiskLevel*. Це забезпечує адаптацію результатів оцінювання до змін характеристик IoT-середовища.

Загальну послідовність виконання процедур запропонованої інформаційної технології наведено на Рис. 2.7.

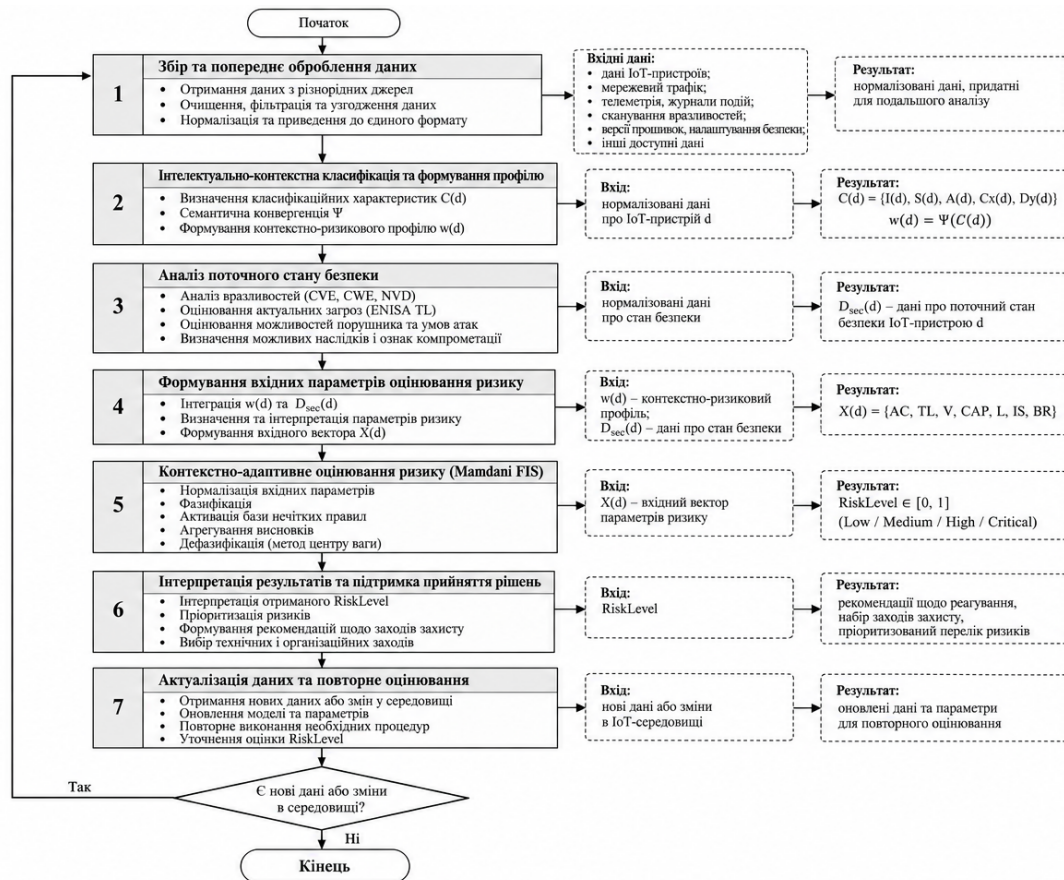


Рисунок 2.7 – Алгоритм функціонування інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Алгоритм функціонування запропонованої інформаційної технології визначає послідовність процедур контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ та реалізує безперервний цикл аналізу. Результати кожного етапу використовуються на наступних етапах оцінювання з урахуванням змін стану та контексту функціонування IoT-середовища.

### 2.4.3. Програмна реалізація інформаційної технології

Для практичного використання розроблених моделей і методу визначено програмні засади реалізації інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ. Її програмна реалізація передбачає модульну взаємодію засобів підготовки вхідних даних, інтелектуально-контекстної класифікації, формування контекстно-ризикових профілів, підготовки параметрів оцінювання ризику та системи нечіткого логічного виведення типу Mamdani.

Центральним аналітичним компонентом є FIS-модель, результатом роботи якої є інтегральний показник *RiskLevel*. Архітектуру програмного забезпечення, склад функціональних компонентів, механізми їх взаємодії та деталі програмної реалізації розглянуто у розділі 3, а результати експериментальної перевірки - у Розділі 4.

## Висновки розділу 2

У другому розділі розглянуто модель інтелектуально-контекстної класифікації IoT-пристроїв і розроблено модель формування контекстно-ризикового профілю за її результатами. Формалізовано критерії класифікації та вхідні параметри оцінювання ризику, удосконалено метод оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані. На основі розробленої моделі формування профілю й удосконаленого методу створено інформаційну технологію, що забезпечує їх узгоджене застосування в процесі аудиту IoT-середовищ.

У результаті проведеного дослідження отримано такі основні результати:

1. Розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Вона передбачає класифікацію пристрою за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Результати класифікації за кожним критерієм зберігаються у профілі без зведення до одного числового показника. Сформований профіль разом із даними про поточний стан безпеки використовується для визначення та інтерпретації параметрів оцінювання ризику.
2. Формалізовано критерії та структуру вхідних параметрів оцінювання ризиків з урахуванням положень ISO/IEC 27005, EBIOS Risk Manager та ENISA Threat Landscape. Визначено взаємозв'язки між активами, вразливостями та загрозами, а також сформовано вектор вхідних параметрів. Значення параметрів формуються на основі даних про поточний стан безпеки з урахуванням контекстно-ризикового профілю IoT-пристрою.

3. Удосконалено метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані шляхом взаємопов'язаного врахування критичності активу, рівня загрози, рівня вразливості, можливостей потенційного порушника, імовірності реалізації загрози, тяжкості її наслідків, контекстно-ризикового профілю IoT-пристрою та попередньо сформованого показника *BackdoorRisk*. Метод передбачає нормування і фазифікацію вхідних параметрів, застосування бази нечітких продукційних правил, агрегування результатів нечіткого логічного виведення та дефазифікацію з формуванням інтегрального показника *RiskLevel*.
4. Сформовано та оптимізовано базу нечітких продукційних правил, що формалізує експертні знання щодо взаємодії параметрів ризику. Замість повного простору з можливих комбінацій сформовано робочу базу з 40 продукційних правил, орієнтованих на покриття типових, граничних і критичних сценаріїв. Це забезпечило збереження інтерпретованості моделі та скорочення обчислювальної складності нечіткого логічного виведення.
5. Сформовано інформаційну технологію контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ, яка об'єднує процедури збору та попереднього оброблення даних, інтелектуально-контекстної класифікації, формування контекстно-ризикового профілю, аналізу поточного стану безпеки, формування вхідних параметрів ризику, нечіткого оцінювання та підтримки прийняття рішень. Визначено її структурно-функціональну організацію та алгоритм функціонування із зворотним зв'язком для повторного оцінювання за зміни даних або контексту IoT-середовища.
6. Реалізовано програмний прототип розроблених рішень у середовищі MATLAB/Simulink із використанням *Fuzzy Logic Toolbox*. Проведене моделювання тестових сценаріїв підтвердило працездатність нечіткої моделі та логічно узгоджену зміну інтегрального показника *RiskLevel* залежно від комбінації вхідних параметрів. Детальну експериментальну

перевірку та кількісне оцінювання ефективності розроблених методів і моделей наведено у розділі 4.

### **РОЗДІЛ 3.**

## **АРХІТЕКТУРА ТА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОНТЕКСТНО-АДАПТИВНОГО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІОТ-СЕРЕДОВИЩ**

Гетерогенність, динамічність і багаторівнева організація ІоТ-середовищ зумовлюють необхідність інтегрованого застосування методів аналізу даних, контекстної класифікації та оцінювання ризиків у межах єдиної інформаційної технології.

У другому розділі розроблено модель інтелектуально-контекстної класифікації ІоТ-пристроїв, формалізовано структуру входних параметрів ризику та розроблено метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Mamdani. Отримані результати становлять методичну основу інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ.

У цьому розділі розглянуто архітектуру, функціональну організацію та механізми реалізації запропонованої інформаційної технології, що забезпечує інтеграцію процедур збору й оброблення даних, інтелектуально-контекстної класифікації, аналізу стану безпеки, формування параметрів ризику, нечіткого оцінювання та підтримки прийняття рішень.

Метою розділу є розроблення архітектури та механізмів реалізації інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ.

### **3.1. Принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІоТ-середовищ**

Розроблені у другому розділі модель інтелектуально-контекстної класифікації ІоТ-пристроїв та метод контекстно-адаптивного оцінювання ризиків визначають методичну основу побудови відповідної інформаційної технології. Для їх інтеграції в єдиний інформаційно-аналітичний процес необхідно визначити принципи організації, взаємодії функціональних компонентів та оброблення інформації з урахуванням особливостей ІоТ-середовищ. Зазначені положення є основою для подальшого формування архітектури та механізмів реалізації запропонованої інформаційної технології.

### ***3.1.1. Передумови побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ***

Сучасні IoT-середовища характеризуються гетерогенністю пристроїв, багаторівневою архітектурою, розподіленим обробленням даних і динамічною взаємодією між фізичними, мережевими, периферійними та хмарними компонентами [31,34]. Зазначені особливості ускладнюють оцінювання ризиків безпеки та зумовлюють необхідність урахування не лише поточного стану захищеності, а й функціонального призначення, архітектури взаємодії та контексту функціонування IoT-пристроїв.

Методологічну основу оцінювання ризиків становлять положення ISO/IEC 27005, NIST SP 800-30, EBIOS Risk Manager та рекомендації ENISA [6,8,36]. Водночас їх застосування в IoT-середовищах потребує врахування динамічності, гетерогенності, різноманітності джерел даних та можливих змін контексту функціонування пристроїв.

У дисертаційній роботі зазначені особливості враховуються шляхом інтеграції інтелектуально-контекстної класифікації IoT-пристроїв, аналізу поточного стану безпеки та контекстно-адаптивного оцінювання ризиків. Це забезпечує формування параметрів ризику з урахуванням контекстно-ризикового профілю пристрою та створює передумови для побудови відповідної інформаційної технології.

### ***3.1.2. Порівняльний аналіз підходів до оцінювання ризиків безпеки IoT-середовищ***

Побудова інформаційної технології потребує визначення підходів, положення яких можуть бути використані для організації оцінювання ризиків безпеки IoT-середовищ. До них належать стандартизовані підходи до управління ризиками, сценарні та експертні методології, галузеві рекомендації щодо безпеки IoT, спеціалізовані моделі технічного аналізу, а також інтелектуальні методи оброблення даних.

Стандарти ISO/IEC 27005 та NIST SP 800-30 визначають загальні принципи і процедури оцінювання ризиків інформаційної безпеки. Методології EBIOS Risk Manager та OCTAVE розширюють ризик-орієнтований підхід за рахунок



сценарного аналізу загроз, критичності активів та можливостей потенційного порушника. Рекомендації *ENISA* та *ETSI* враховують специфічні особливості безпеки IoT-пристроїв і середовищ їх функціонування.

Окрему групу становлять спеціалізовані та інтелектуальні підходи, що використовують дані мережевого трафіку, журнали подій, характеристики пристроїв, методи машинного навчання, нечіткої логіки та поведінкового аналізу. Їх перевагою є можливість автоматизованого оброблення різномірних даних та врахування невизначеності, однак такі рішення переважно орієнтовані на окремі задачі аналізу безпеки.

Узагальнення характеристик розглянутих підходів наведено в табл. 3.1.

*Таблиця 3.1 – Порівняльний аналіз підходів до оцінювання ризиків безпеки IoT-середовищ*

| Група підходів                           | Переваги                                                             | Основні обмеження                                                          | Використання у запропонованій ІТ                      |
|------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------|
| ISO/IEC 27005, NIST SP 800-30            | Системність оцінювання ризиків; формалізація основних етапів         | Потребують адаптації до динамічних IoT-середовищ                           | Методологічна основа оцінювання ризиків               |
| EBIOS RM, OCTAVE                         | Сценарний аналіз; урахування активів, загроз і можливостей порушника | Значна роль експертних оцінок                                              | Формування та інтерпретація ризикових сценаріїв       |
| ENISA, ETSI                              | Урахування специфіки IoT та життєвого циклу пристроїв                | Переважно рекомендаційний характер                                         | Урахування характерних для IoT загроз і вимог безпеки |
| Спеціалізовані моделі технічного аналізу | Аналіз трафіку, подій, стану та поведінки пристроїв                  | Орієнтація на окремі задачі та джерела даних                               | Формування даних про поточний стан безпеки            |
| Інтелектуальні та гібридні методи        | Робота з невизначеними даними; автоматизація; адаптивність           | Залежність від даних і моделей; проблема інтерпретованості окремих методів | Контекстна класифікація та нечітке оцінювання ризиків |

Проведений аналіз показує, що розглянуті підходи вирішують взаємопов'язані, але різні завдання: стандартизовані методології визначають принципи оцінювання ризиків, сценарні підходи забезпечують аналіз загроз і можливостей порушника, галузеві рекомендації враховують специфіку IoT, а спеціалізовані та інтелектуальні методи забезпечують оброблення технічних і контекстних даних. Водночас їх ізольоване застосування не забезпечує

узгодженого використання результатів класифікації IoT-пристроїв, даних про поточний стан безпеки та контекстно-адаптивного оцінювання ризиків.

У запропонованій інформаційній технології зазначені підходи інтегруються відповідно до їх функціонального призначення. Результати інтелектуально-контекстної класифікації та дані про стан безпеки використовуються для формування параметрів ризику, а їх інтегральне оцінювання здійснюється розробленим методом контекстно-адаптивного нечіткого логічного виведення.

### ***3.1.3. Принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ***

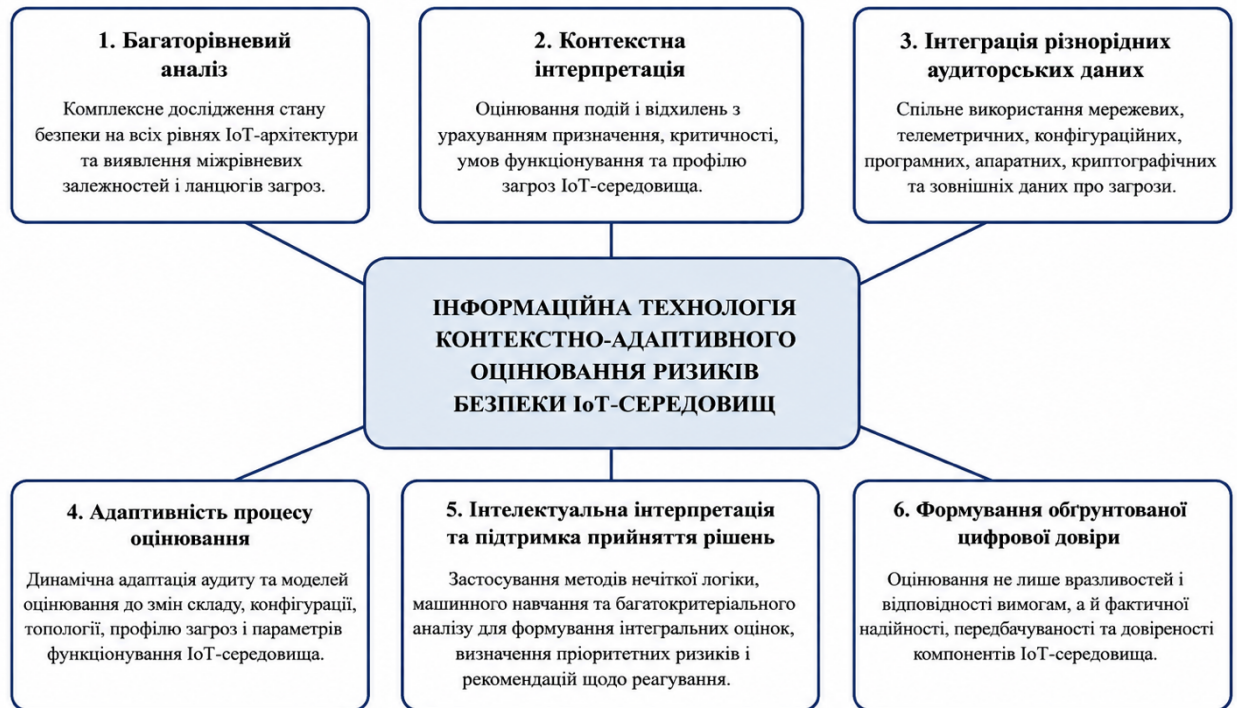
Побудова запропонованої інформаційної технології ґрунтується на сукупності взаємопов'язаних принципів, що визначають організацію оброблення даних, взаємодію функціональних компонентів та формування результатів оцінювання ризиків. З урахуванням особливостей IoT-середовищ і розроблених у другому розділі моделей та методу визначено такі основні принципи.

1. *Принцип багаторівневого аналізу.* Передбачає врахування даних, що характеризують різні рівні IoT-середовища: пристрої, мережеву взаємодію, периферійні та хмарні компоненти. Результати аналізу використовуються у взаємозв'язку, що забезпечує комплексне представлення стану безпеки досліджуваного середовища.
2. *Принцип контекстної інтерпретації.* Оцінювання здійснюється з урахуванням функціонального призначення IoT-пристрою, архітектури його взаємодії, характеристик безпеки, контексту функціонування та динамічності середовища. Реалізація цього принципу забезпечується використанням сформованого контекстно-ризикового профілю під час визначення та інтерпретації параметрів ризику.
3. *Принцип інтеграції різномірних даних.* Інформаційна технологія передбачає спільне використання даних мережевого трафіку, журналів подій, телеметрії, конфігураційних параметрів, відомостей про вразливості, загрози та інших характеристик стану безпеки IoT-пристроїв.

Їх узгоджене використання забезпечує формування вхідних параметрів оцінювання ризику.

4. *Принцип контекстної адаптивності.* Значення та інтерпретація параметрів ризику визначаються з урахуванням особливостей конкретного IoT-пристрою та умов його функціонування. Зміна контексту або даних про стан безпеки приводить до актуалізації вхідних параметрів та повторного визначення інтегрального рівня ризику.
5. *Принцип урахування невизначеності.* Для оброблення неповної, неточної та контекстно залежної інформації використовується апарат нечіткої логіки. Система нечіткого логічного виведення типу Mamdani забезпечує інтеграцію часткових параметрів ризику та формування показника *RiskLevel* на основі сформованої бази продукційних правил.
6. *Принцип підтримки прийняття рішень.* Результати оцінювання ризиків використовуються для визначення пріоритетності виявлених ризиків та формування рекомендацій щодо застосування відповідних заходів захисту. Це забезпечує перехід від отримання інтегральної оцінки *RiskLevel* до її практичного використання під час аналізу стану безпеки IoT-середовища.

Методологічні принципи побудови запропонованої інформаційної технології та їх взаємозв'язок наведено на Рис. 3.2.



*Рисунок 3.2 – Принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІoT-середовищ*

### **3.2. Концепція інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки ІoT-середовищ**

Після визначення передумов і принципів побудови інформаційної технології необхідно сформуванню її загальну концепцію, що визначає призначення, склад основних інформаційних процесів, взаємозв'язки між функціональними компонентами та послідовність перетворення первинних даних у параметри оцінювання ризику й інтегральний показник *RiskLevel*.

У межах дисертаційного дослідження під інформаційною технологією контекстно-адаптивного оцінювання ризиків безпеки ІoT-середовищ розуміється сукупність взаємопов'язаних інформаційних процесів, моделей, методів, алгоритмічних процедур, програмних компонентів і потоків даних, що забезпечують збирання та попереднє оброблення інформації про ІoT-пристрої, інтелектуально-контекстну класифікацію, формування контекстно-ризикового профілю, аналіз поточного стану безпеки, формування вхідних параметрів ризику та їх контекстно-адаптивне оцінювання.

У цьому підрозділі визначено концептуальну організацію інформаційної технології, основні інформаційні потоки та функціональну взаємодію

компонентів, що забезпечують послідовний перехід від первинних даних IoT-середовища до інтегральної оцінки ризику та підтримки прийняття рішень.

### **3.2.1. Концептуальна модель інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ**

Після визначення методологічних засад і принципів побудови інформаційної технології необхідно формалізувати її загальну концепцію. Концептуальна модель визначає склад основних функціональних компонентів, взаємозв'язки між ними та загальну логіку перетворення первинних даних IoT-середовища в інтегральну оцінку ризику.

Функціональну основу інформаційної технології становлять розроблені у другому розділі метод інтелектуально-контекстної класифікації IoT-пристроїв та метод контекстно-адаптивного оцінювання ризиків. Результати класифікації, представлені контекстно-ризиковим профілем, спільно з даними про поточний стан безпеки використовуються для формування вхідних параметрів оцінювання ризику. Їх подальше опрацювання системою нечіткого логічного виведення типу Mamdani забезпечує формування інтегрального показника *RiskLevel*.

На рівні інформаційної технології зазначені процедури реалізуються як взаємопов'язані функціональні компоненти. Первинні дані про характеристики IoT-пристроїв, мережеву активність, загрози, вразливості та стан безпеки надходять до компонентів збору й попереднього оброблення. Після цього результати інтелектуально-контекстної класифікації та аналізу стану безпеки використовуються компонентом контекстно-адаптивного оцінювання ризику, а сформований *RiskLevel* передається до компонента підтримки прийняття рішень.

Важливою властивістю запропонованої концепції є наявність зворотного інформаційного зв'язку. Зміна характеристик пристрою, його контексту функціонування, конфігурації середовища або поточного стану безпеки зумовлює актуалізацію відповідних інформаційних об'єктів та повторне оцінювання ризику. Це забезпечує адаптацію інформаційної технології до динамічних змін IoT-середовища без зміни загальної структури її функціонування.

Підсумовуючи, концептуальна модель інформаційної технології визначає наскрізний інформаційний процес:

*первинні дані → попереднє оброблення → інтелектуально-контекстна класифікація та аналіз стану безпеки → формування параметрів ризику → контекстно-адаптивне оцінювання → RiskLevel → підтримка прийняття рішень.*

Концептуальну модель запропонованої інформаційної технології наведено на рис. 3.3.

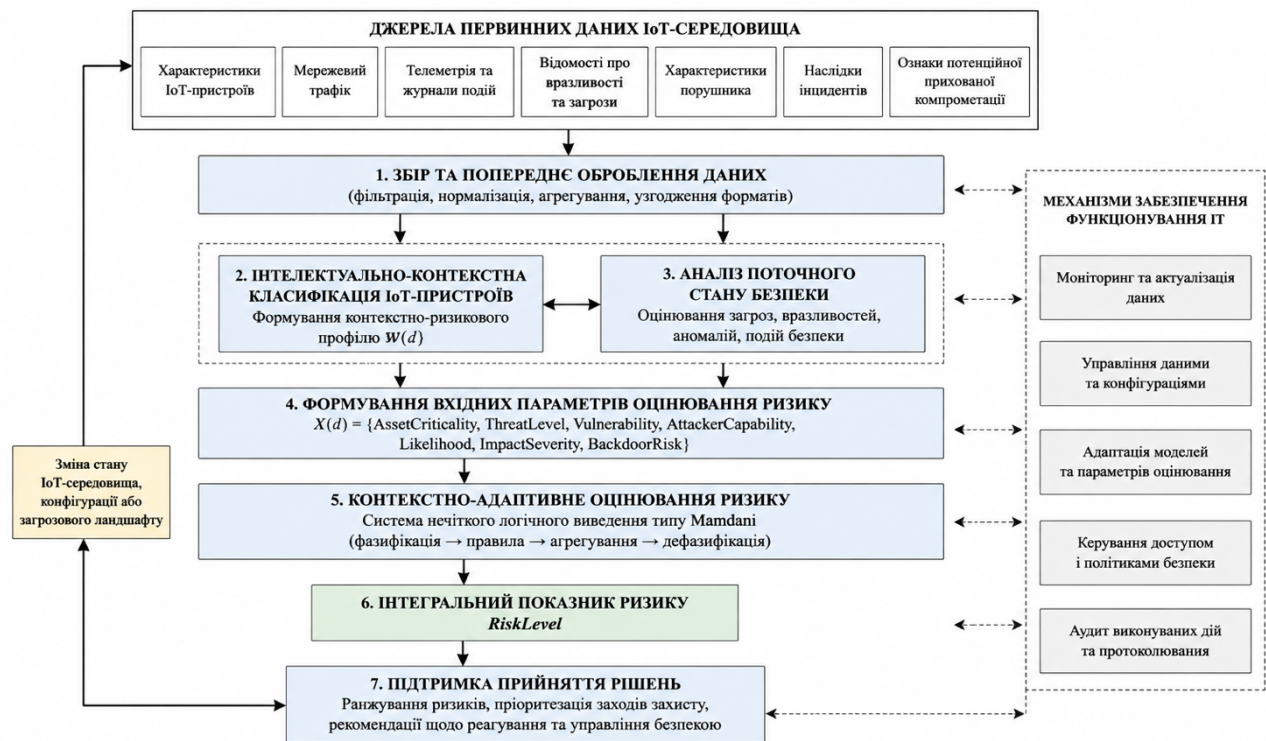


Рисунок 3.3 – Концептуальна модель інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

### 3.2.2. Інформаційно-аналітичний процес функціонування інформаційної технології

Після визначення концептуальної моделі необхідно деталізувати інформаційно-аналітичний процес функціонування запропонованої інформаційної технології. Він забезпечує послідовне перетворення первинних даних IoT-середовища в контекстно-залежні параметри ризику, інтегральний показник *RiskLevel* та результати підтримки прийняття рішень.

Інформаційно-аналітичний процес складається з п'яти взаємопов'язаних етапів:

1. *Збирання та попереднє оброблення даних.* Здійснюється отримання характеристик IoT-пристроїв, мережевого трафіку, телеметрії, журналів подій, відомостей про вразливості, загрози та інші характеристики стану безпеки. Отримані дані проходять фільтрацію, нормалізацію, усунення дублювання та приведення до формату, придатного для подальшого аналізу.
2. *Інтелектуально-контекстна класифікація та аналіз стану безпеки.* На основі підготовлених даних визначаються характеристики IoT-пристроїв і контекст їх функціонування, аналізуються актуальні загрози, вразливості, мережеві та поведінкові ознаки. Результатом є контекстно-ризиковий профіль пристрою та сукупність даних про його поточний стан безпеки.
3. *Формування вхідних параметрів оцінювання ризику.* Результати попередніх етапів використовуються для формування та контекстної інтерпретації параметрів *AssetCriticality*, *ThreatLevel*, *Vulnerability*, *AttackerCapability*, *Likelihood*, *ImpactSeverity* та *BackdoorRisk*. При цьому ознаки потенційної прихованої компрометації враховуються під час формування параметра *BackdoorRisk*.
4. *Контекстно-адаптивне оцінювання ризику.* Сформовані параметри надходять до системи нечіткого логічного виведення типу Mamdani. На основі визначених функцій належності та бази продукційних правил формується інтегральний показник *RiskLevel*, що характеризує рівень ризику безпеки з урахуванням контексту функціонування IoT-пристрою.
5. *Формування результатів та підтримка прийняття рішень.* Отримані значення *RiskLevel* використовуються для ранжування ризиків, визначення пріоритетності реагування та формування рекомендацій щодо застосування відповідних заходів захисту.

Інформаційно-аналітичний процес має адаптивний характер. У разі зміни характеристик IoT-пристроїв, їх контексту функціонування, стану безпеки або актуального профілю загроз здійснюється оновлення вхідних даних і повторне



виконання відповідних етапів оцінювання. Зворотний зв'язок забезпечує актуалізацію результатів відповідно до поточного стану IoT-середовища.

Узагальнену структуру інформаційно-аналітичного процесу наведено на рис. 3.4

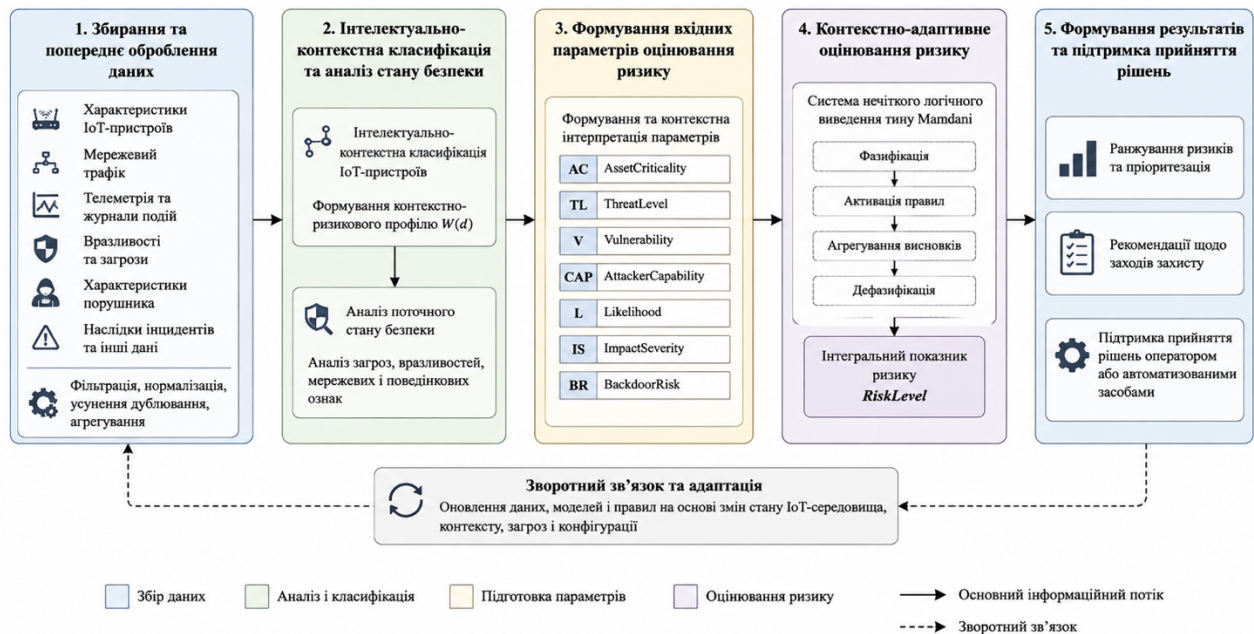


Рисунок 3.4 – Інформаційно-аналітичний процес функціонування інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Узагальнюючи викладене, запропонований інформаційно-аналітичний процес забезпечує послідовне контекстно-адаптивне оцінювання ризиків безпеки та створює основу для розроблення архітектури інформаційної технології й організації взаємодії її функціональних компонентів.

### 3.3. Архітектура реалізації інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Після визначення концептуальної моделі та інформаційно-аналітичного процесу розроблено архітектуру реалізації запропонованої інформаційної технології. Вона визначає склад програмно-функціональних компонентів, механізми їх взаємодії та організацію інформаційних потоків у процесі контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ.

Архітектуру побудовано за модульним принципом, що забезпечує функціональну незалежність компонентів, масштабованість та можливість інтеграції з різними IoT-платформами й засобами кібербезпеки.



Функціональна структура охоплює компоненти збирання та попереднього оброблення даних, інтелектуально-контекстної класифікації, аналізу стану безпеки, формування контекстно-ризикових параметрів, нечіткого оцінювання ризику та підтримки прийняття рішень. У наступних підрозділах розглянуто багаторівневу архітектуру IoT-середовища, функціональну структуру інформаційної технології, інформаційну взаємодію її компонентів та архітектуру програмного забезпечення.

### ***3.3.1. Багаторівнева архітектура IoT-середовища для контекстно-адаптивного оцінювання ризиків безпеки***

Практична реалізація інформаційної технології потребує врахування багаторівневої архітектури IoT-середовища, що поєднує фізичні пристрої, мережеву інфраструктуру, периферійні вузли та хмарні сервіси. Кожний рівень формує власні інформаційні потоки та характеризується специфічними загрозами й вразливостями, що необхідно враховувати під час контекстно-адаптивного оцінювання ризиків безпеки.

Запропонована інформаційна технологія функціонує як надбудова над IoT-інфраструктурою та використовує дані, сформовані на різних рівнях її функціонування. Розподіл процедур збирання, передавання, попереднього оброблення та аналізу даних між рівнями забезпечує можливість застосування технології в гетерогенних і масштабованих IoT-середовищах

Первинне збирання та часткове оброблення даних можуть виконуватися безпосередньо на IoT-пристроях і периферійних вузлах *Edge/Gateway*, тоді як накопичення, інтеграція даних та реалізація основних процедур оцінювання ризиків здійснюються на відповідних централізованих компонентах. Такий розподіл дає змогу зменшити обсяг передавання необроблених даних та забезпечити масштабованість інформаційної технології.

Багаторівневу архітектуру взаємодії IoT-середовища та запропонованої інформаційної технології наведено на Рис. 3.5. Вона охоплює п'ять взаємопов'язаних рівнів: IoT-пристроїв, мережевої інфраструктури, *Edge/Gateway*, хмарної інфраструктури та рівень інформаційної технології контекстно-адаптивного оцінювання ризиків.

1. Рівень IoT-пристроїв охоплює сенсори, контролери, виконавчі пристрої та інші фізичні компоненти, що формують первинні дані про стан і функціонування IoT-середовища: телеметрію, журнали подій, конфігураційні параметри та характеристики програмного й апаратного забезпечення.
2. Мережевий рівень забезпечує інформаційну взаємодію між компонентами IoT-середовища та є джерелом даних про мережевий трафік, з'єднання, використовувані протоколи, події автентифікації та ознаки аномальної мережевої активності.
3. Рівень Edge/Gateway забезпечує локальне збирання, фільтрацію, нормалізацію та агрегування даних перед їх передаванням до централізованих компонентів інформаційної технології.
4. Рівень хмарної інфраструктури забезпечує накопичення й зберігання даних, функціонування IoT-платформ та взаємодію з централізованими засобами їх оброблення й аналізу.
5. Рівень інформаційної технології контекстно-адаптивного оцінювання ризиків реалізує інтелектуально-контекстну класифікацію, аналіз стану безпеки, формування контекстно-ризикових параметрів, нечітке оцінювання ризику та підтримку прийняття рішень.

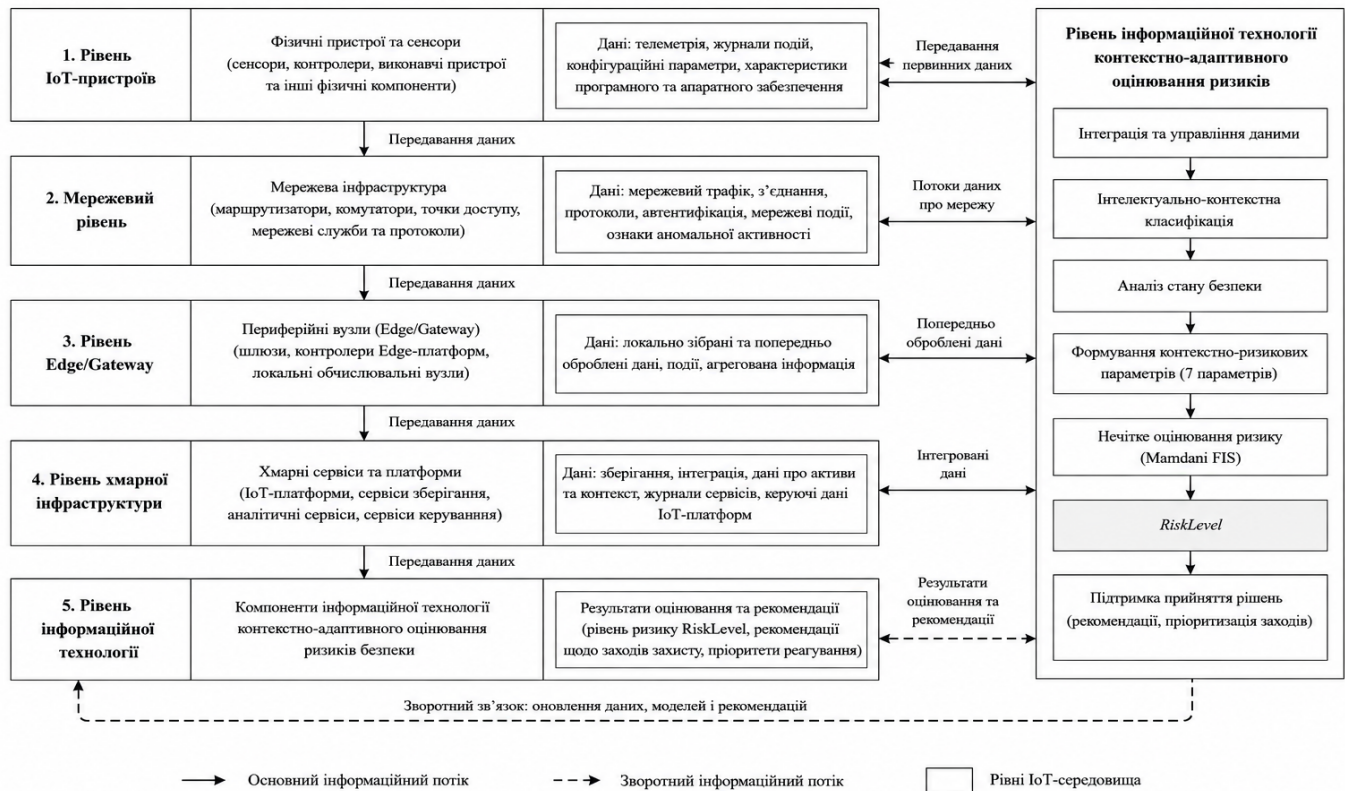


Рисунок 3.5 – Багаторівнева архітектура взаємодії IoT-середовища та інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки

Підсумовуючи, запропонована багаторівнева архітектура визначає рівні формування, передавання й оброблення даних про стан IoT-середовища та створює основу для розміщення програмних і агентних компонентів інформаційної технології, взаємодію яких розглянуто в наступному підрозділі.

### 3.3.2. Функціональна архітектура інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Функціональна архітектура інформаційної технології визначає склад програмно-функціональних компонентів, їх взаємодію та розподіл процедур оброблення даних між різними рівнями IoT-середовища. На відміну від централізованої організації аналізу, запропонована архітектура поєднує розподілене збирання та попереднє опрацювання даних із централізованим контекстно-адаптивним оцінюванням ризиків.

Основними компонентами функціональної архітектури є:

- розподілений рівень інтелектуальних агентів аналізу безпеки;
- інформаційно-аналітичне ядро;

- база знань;
- підсистема підтримки прийняття рішень.

Особливістю запропонованої інформаційної технології є використання розподіленого агентного підходу, за якого збирання, попереднє опрацювання та локальний аналіз даних здійснюються безпосередньо на різних рівнях IoT-середовища. Це забезпечує оперативне виявлення змін стану компонентів, зменшення обсягу даних, що передаються до централізованого інформаційно-аналітичного ядра, та підвищує масштабованість інформаційної технології. Реалізація зазначеного підходу покладається на інтелектуальні агенти аналізу безпеки, які формують розподілений рівень функціональної архітектури.

*Інтелектуальні агенти аналізу безпеки* використовуються для розподіленого отримання та попереднього аналізу даних (Intelligent Security Analysis Agents, ISAA). Під ISAA розуміється автономний програмний компонент інформаційної технології, призначений для збирання, попереднього опрацювання та локального аналізу даних про стан компонентів IoT-середовища, формування аналітичних ознак і передавання результатів до інформаційно-аналітичного ядра.

Залежно від рівня розміщення та функціонального призначення передбачено чотири типи агентів:

- 1) Device ISAA – аналіз параметрів IoT-пристроїв, конфігурацій, прошивок, журналів подій та характеристик криптографічних компонентів;
- 2) Network ISAA – аналіз мережевого трафіку, з'єднань, протоколів, подій автентифікації та ознак аномальної мережевої активності;
- 3) Gateway ISAA – збирання й агрегування даних на рівні Edge/Gateway, контроль міжсегментної взаємодії та локальне виявлення відхилень;
- 4) Cloud ISAA – аналіз журналів хмарних сервісів, API-взаємодій, подій автентифікації, керування доступом та оновленнями.

Такий підхід забезпечує розподілення обчислювального навантаження, зменшення обсягу передавання необроблених даних та можливість локального виявлення значущих змін стану IoT-компонентів.

*Інформаційно-аналітичне ядро* є центральним компонентом архітектури, яке інтегрує результати роботи ISAA та реалізує основні процедури контекстно-адаптивного оцінювання ризиків.

До його функцій належать:

- 1) інтеграція та кореляція даних, отриманих від різних ISAA;
- 2) інтелектуально-контекстна класифікація IoT-пристроїв;
- 3) формування контекстно-ризикових профілів;
- 4) аналіз загроз, вразливостей та ознак прихованої компрометації;
- 5) формування вхідних параметрів моделі оцінювання ризику;
- 6) визначення інтегрального показника засобами нечіткого логічного виведення типу Mamdani.

Результати локального аналізу агентів при цьому не розглядаються ізольовано, а інтегруються з урахуванням взаємозв'язків між пристроями, мережевими сегментами, шлюзами, сервісами та поточним контекстом функціонування IoT-середовища.

*База знань* - забезпечує інформаційну підтримку аналітичних процедур і містить формалізовані експертні знання предметної області, базу нечітких продукційних правил, відомості про загрози та вразливості, характеристики IoT-компонентів, контекстні параметри та критерії інтерпретації отриманих оцінок.

Використання єдиної бази знань забезпечує узгодженість локального та централізованого аналізу, а також можливість актуалізації правил і параметрів відповідно до зміни характеристик IoT-середовища та профілю кіберзагроз.

*Підсистема підтримки прийняття рішень* - використовує сформований показник *RiskLevel*, контекстно-ризиковий профіль і результати аналізу для визначення пріоритетності виявлених ризиків та формування рекомендацій щодо реагування. Залежно від рівня ризику можуть формуватися рекомендації щодо зміни конфігурації, оновлення програмного забезпечення, посилення контролю доступу, ізоляції компонентів, додаткового моніторингу або застосування інших заходів захисту.

Механізм зворотного зв'язку забезпечує передавання результатів прийнятих рішень до інформаційно-аналітичного ядра та агентів ISAA, що дає

змогу актуалізувати контекстно-ризикові профілі й виконувати повторне оцінювання ризику за зміни стану IoT-середовища.

Узагальнену функціональну архітектуру запропонованої інформаційної технології та взаємозв'язки між її основними компонентами наведено на Рис. 3.6.

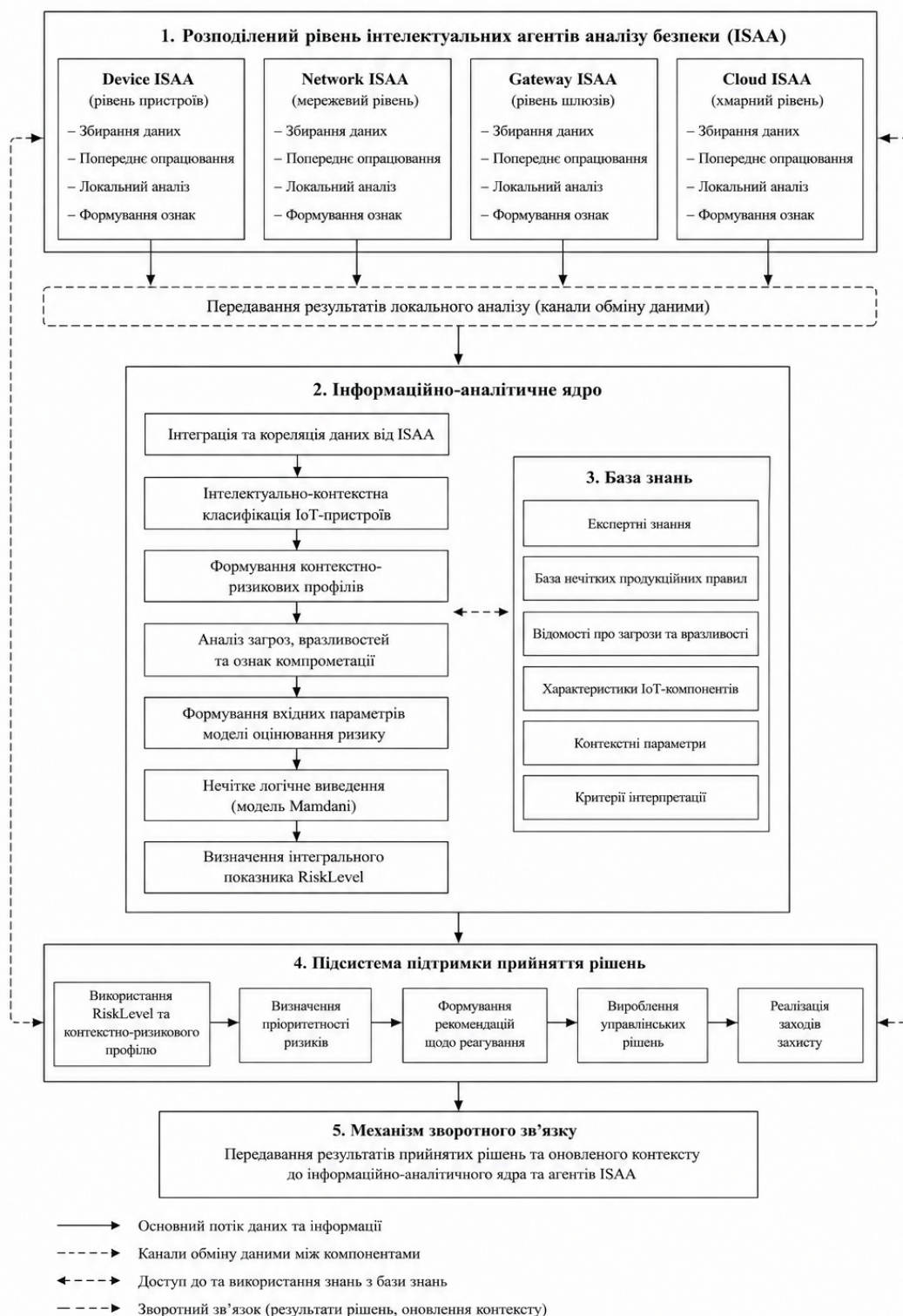


Рисунок 3.6 – Функціональна архітектура інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Підсумовуючи, запропонована функціональна архітектура поєднує розподілений агентний рівень із централізованим інформаційно-аналітичним ядром, базою знань і підсистемою підтримки прийняття рішень. Така організація забезпечує інтеграцію даних із різних рівнів IoT-середовища, формування контекстно-ризикових профілів, контекстно-адаптивне оцінювання ризиків та формування рекомендацій відповідно до поточного стану системи.

### ***3.3.3. Архітектура інформаційної взаємодії компонентів інформаційної технології***

Після визначення функціональної архітектури інформаційної технології необхідно встановити організацію інформаційної взаємодії між її компонентами. Якщо в попередньому підрозділі визначено їх склад і функціональне призначення, то в цьому підрозділі розглядаються інформаційні потоки та послідовність перетворення даних у процесі контекстно-адаптивного оцінювання ризиків безпеки IoT-середовища.

Особливістю запропонованої архітектури є те, що між її компонентами здійснюється не лише передавання даних, а й їх послідовне перетворення. Первинні дані проходять попереднє опрацювання та локальний аналіз на агентному рівні, після чого інтегруються в інформаційно-аналітичному ядрі, використовуються для формування контекстно-ризикових профілів та визначення інтегрального показника *RiskLevel*. Результати оцінювання надходять до підсистеми підтримки прийняття рішень для формування відповідних рекомендацій.

Як наслідок, інформаційна взаємодія компонентів реалізує послідовність *«первинні дані → локально опрацьовані дані → інтегровані дані та контекстно-ризиковий профіль → оцінка ризику → рекомендації»*.

Архітектуру інформаційної взаємодії та основні етапи перетворення даних наведено на Рис. 3.7.



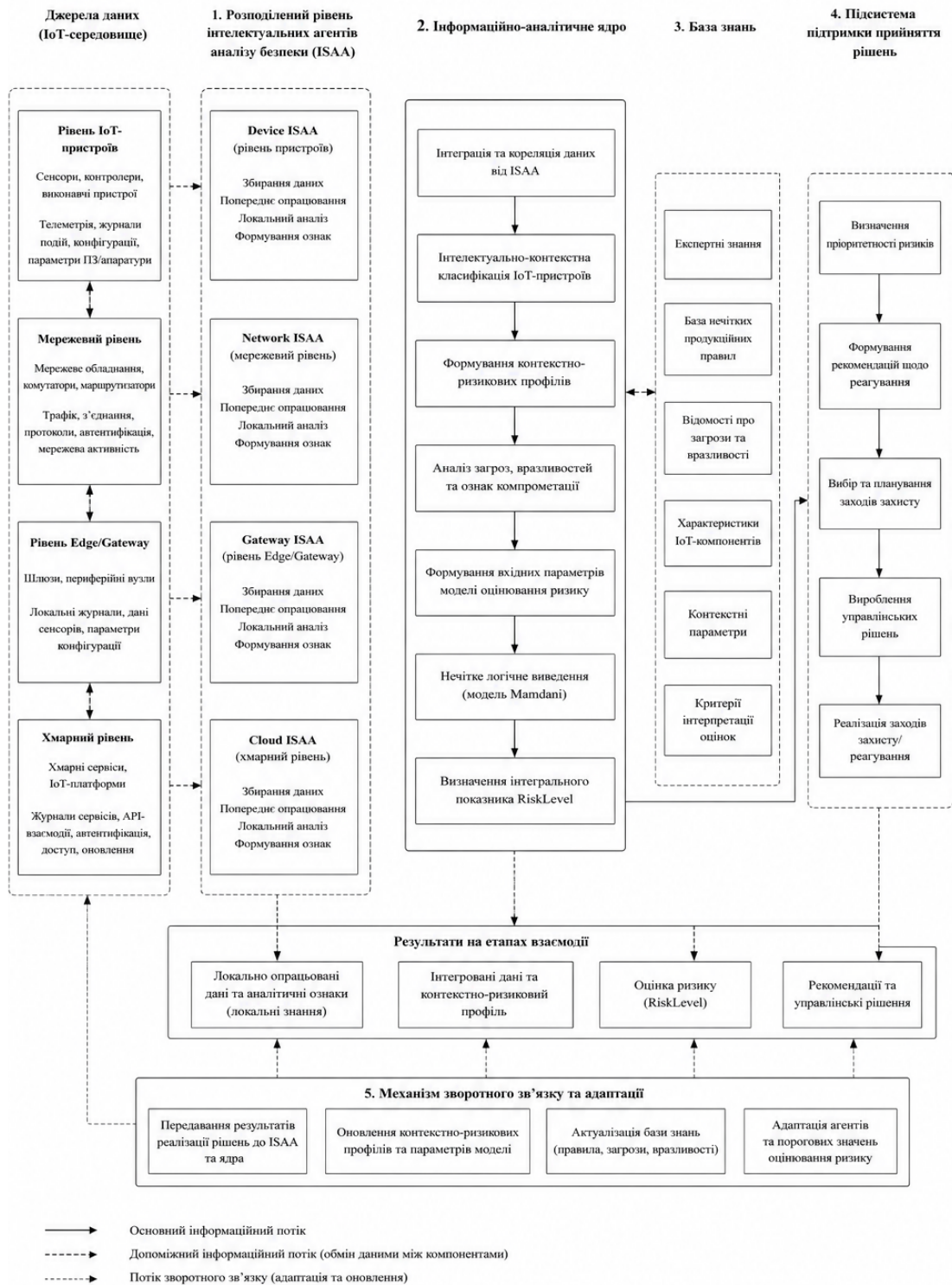


Рисунок 3.7 – Архітектура інформаційної взаємодії компонентів інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

### 3.3.4. Архітектура програмного забезпечення інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ

Після визначення функціональної архітектури та інформаційної взаємодії компонентів необхідно визначити архітектуру програмного забезпечення, що



забезпечує реалізацію основних процедур запропонованої інформаційної технології. Архітектура програмного забезпечення визначає склад програмних підсистем, розподіл функцій між ними та механізми їх взаємодії.

Програмне забезпечення побудовано за модульним принципом, що забезпечує можливість незалежного розвитку окремих компонентів, їх масштабування та адаптації до різних конфігурацій IoT-середовища. Відповідно до функціональної архітектури доцільно виділити чотири взаємопов'язані програмні підсистеми:

1. Підсистему збирання та попереднього опрацювання даних - забезпечує отримання телеметрії, журналів подій, мережових даних, конфігураційних параметрів та інших відомостей про стан компонентів IoT-середовища. На цьому рівні виконуються перевірка, фільтрація, нормалізація, агрегування та приведення отриманих даних до структури, придатної для подальшого аналізу. Розподілене отримання та локальне попереднє опрацювання даних передбачається здійснювати за допомогою агентів ISAA, функціональне призначення яких визначено в підрозділі 3.3.2.
2. Інформаційно-аналітична підсистема є центральним програмним компонентом інформаційної технології. Вона забезпечує інтеграцію даних, інтелектуально-контекстну класифікацію IoT-пристроїв, формування контекстно-ризикових профілів та підготовку вхідних параметрів для оцінювання ризику. Оцінювання здійснюється на основі системи нечіткого логічного виведення типу *Mamdani*, яка використовує параметри *AssetCriticality*, *ThreatLevel*, *Vulnerability*, *AttackerCapability*, *Likelihood*, *ImpactSeverity* та *BackdoorRisk* і формує інтегральний показник *RiskLevel*.
3. Підсистема підтримки прийняття рішень - використовує значення *RiskLevel* та контекстно-ризиковий профіль для інтерпретації результатів оцінювання, визначення пріоритетності ризиків і формування рекомендацій щодо застосування відповідних заходів захисту. Залежно від отриманого рівня ризику можуть формуватися рекомендації щодо додаткового моніторингу, усунення вразливостей, зміни конфігурації,

оновлення програмного забезпечення, посилення контролю доступу або ізоляції окремих компонентів IoT-середовища.

4. Підсистема керування та конфігурування -забезпечує керування параметрами програмних компонентів, конфігурацією джерел даних, базою знань, параметрами моделей та правилами нечіткого висновку. Наявність окремої підсистеми керування забезпечує можливість актуалізації параметрів інформаційної технології відповідно до змін конфігурації та контексту функціонування IoT-середовища.

Узагальнену архітектуру програмного забезпечення та взаємодію її основних підсистем наведено на Рис. 3.8.

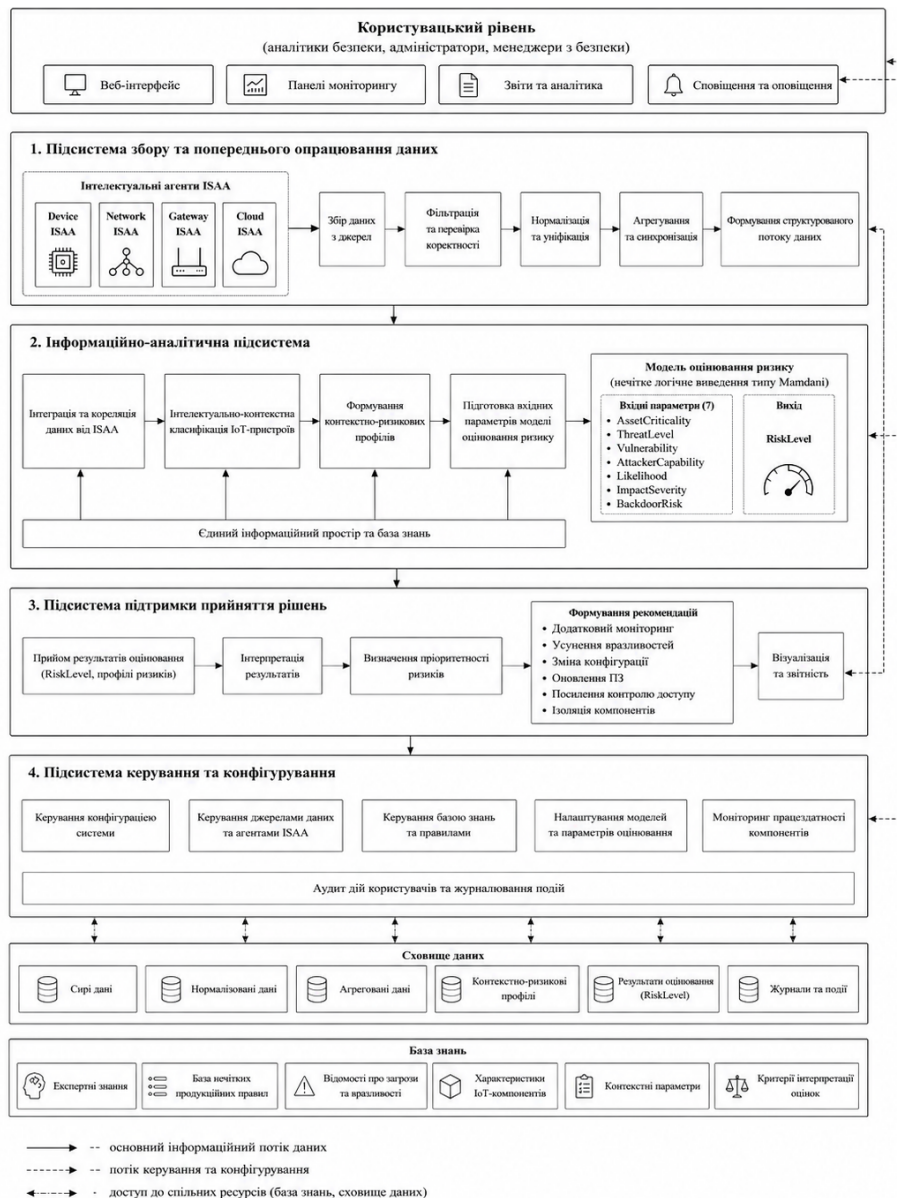


Рисунок 3.8 – Архітектура програмного забезпечення інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовища

Запропонована програмна архітектура забезпечує модульну реалізацію основних процедур інформаційної технології та узгоджує розподілене отримання даних із централізованим контекстно-адаптивним оцінюванням ризиків. Практичну реалізацію та експериментальну перевірку розроблених програмних компонентів наведено у Розділі 4.

### **Висновки розділу 3**

У третьому розділі розроблено архітектурні та програмні засади реалізації інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ. Визначено принципи її побудови, інформаційно-аналітичний процес, багаторівневу та функціональну архітектури, організацію інформаційної взаємодії компонентів і архітектуру програмного забезпечення.

У результаті проведеного дослідження отримано такі основні результати.

1. Сформовано принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ, що визначають вимоги до інтеграції різнорідних даних, урахування контексту функціонування IoT-компонентів, адаптивності процесу оцінювання та підтримки прийняття рішень.
2. Розроблено інформаційно-аналітичний процес функціонування інформаційної технології, що забезпечує послідовне збирання й попереднє опрацювання даних, інтелектуально-контекстну класифікацію IoT-пристроїв, формування контекстно-ризикових профілів і вхідних параметрів, контекстно-адаптивне оцінювання ризиків та формування рекомендацій. Механізм зворотного зв'язку забезпечує повторне оцінювання ризику за зміни стану та контексту функціонування IoT-середовища.
3. Запропоновано багаторівневу та функціональну архітектури інформаційної технології, що поєднують рівні IoT-пристроїв, мережевої інфраструктури, *Edge/Gateway* і хмарної інфраструктури з централізованим інформаційно-аналітичним ядром. Для розподіленого збирання, попереднього опрацювання та локального аналізу даних

запропоновано використання інтелектуальних агентів аналізу безпеки *ISAA* типів *Device ISAA*, *Network ISAA*, *Gateway ISAA* та *Cloud ISAA*.

4. Визначено архітектуру інформаційної взаємодії компонентів інформаційної технології, яка реалізує послідовне перетворення первинних даних у локально опрацьовані та інтегровані дані, контекстно-ризикові профілі, вхідні параметри моделі оцінювання ризику, інтегральний показник *RiskLevel* та рекомендації щодо застосування відповідних заходів захисту.
5. Розроблено модульну архітектуру програмного забезпечення інформаційної технології, що включає підсистеми збирання та попереднього опрацювання даних, інформаційно-аналітичну підсистему, підсистему підтримки прийняття рішень і підсистему керування та конфігурування. Центральним аналітичним компонентом визначено систему нечіткого логічного виведення типу *Mamdani*, яка на основі сформованих контекстно-ризикових параметрів забезпечує визначення інтегрального показника *RiskLevel*.

Отже, у третьому розділі сформовано цілісну архітектуру інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ та визначено взаємодію її основних функціональних і програмних компонентів. Розроблені архітектурні рішення забезпечують інтеграцію результатів інтелектуально-контекстної класифікації, формування контекстно-ризикових профілів і нечіткого оцінювання ризику в межах єдиного інформаційно-аналітичного процесу. Програмну реалізацію та експериментальну перевірку розроблених методів і моделей наведено у четвертому розділі.

## **РОЗДІЛ 4.**

### **ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА РОЗРОБЛЕНИХ МЕТОДІВ І МОДЕЛЕЙ**

У другому розділі розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалено метод оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані. У третьому розділі визначено архітектуру створеної інформаційної технології, склад її компонентів, інформаційні потоки та порядок узгодженого застосування моделі й методу в процесі аудиту. Наступним етапом є програмна реалізація модуля нечіткого оцінювання ризиків та експериментальна перевірка одержаних результатів.

Метою розділу є експериментальна перевірка розроблених і удосконалених методів та моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ, а також оцінювання результатів їх інтегрованого застосування у складі розробленої інформаційної технології. Експериментальні дослідження охоплюють перевірку моделі інтелектуально-контекстної класифікації IoT-пристроїв, методу контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані, методів класифікації мережевих подій та механізму врахування ознак прихованої компрометації під час формування інтегрального показника RiskLevel.

Експериментальні дослідження проведено із застосуванням програмного комплексу, що реалізує розроблені й удосконалені методи та моделі відповідно до архітектури інформаційної технології, сформованої у третьому розділі. Для реалізації експериментів використано середовище MATLAB із пакетом Fuzzy Logic Toolbox, відкриті набори даних BoT-IoT, TON-IoT та Edge-IIoTset, а також окремо сформовані вибірки контекстно-ризикових сценаріїв. Експериментальна перевірка охоплювала функціональну верифікацію нечіткої моделі, оцінювання методів класифікації мережевих подій, сценарну валідацію FIS-моделі, її

порівняння з базовими моделями оцінювання ризику, аналіз часових характеристик та декомпозиційне оцінювання внеску окремих складових.

#### **4.1. Методика експериментальної перевірки**

Методику експериментальної перевірки сформовано відповідно до структури розроблених і удосконалених методів та моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ. Вона передбачає перевірку коректності програмної реалізації нечіткої моделі оцінювання ризиків, експериментальне оцінювання методів класифікації мережевих подій, сценарну валідацію FIS-моделі, порівняння з базовими моделями оцінювання ризику, дослідження часових характеристик та визначення внеску окремих складових у формування показника RiskLevel.

Експериментальні дослідження проведено із застосуванням програмного комплексу, реалізованого відповідно до архітектури інформаційної технології, сформованої у третьому розділі. Для оцінювання методів класифікації мережевих подій використано дані, сформовані на основі відкритих наборів BoT-IoT, TON-IoT та Edge-IoTset. Перевірку FIS-моделі виконано окремо на сформованих вибірках контекстно-ризикових сценаріїв. Результати цих експериментів розглядали окремо, оскільки методи класифікації мережевих подій і FIS-модель мають різні вхідні дані та виконують різні функціональні завдання.

##### ***4.1.1. Постановка задач експериментів***

Експериментальна перевірка спрямована на підтвердження працездатності та оцінювання ефективності розроблених і удосконалених методів та моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ. Окремо досліджено якість класифікації мережевих подій на відкритих наборах даних IoT-безпеки та функціонування нечіткої моделі оцінювання ризиків на сформованих вибірках контекстно-ризикових сценаріїв. Зазначені експерименти виконувалися окремо, оскільки методи класифікації мережевих подій і FIS-модель використовують різні вхідні дані та вирішують різні функціональні задачі.

Експериментальні дослідження охоплювали функціональну перевірку нечіткої моделі, оцінювання методів класифікації мережевих подій, сценарну валідацію FIS-моделі, порівняння з базовими моделями оцінювання ризику, дослідження впливу показника BackdoorRisk та інших складових запропонованого підходу, аналіз часових характеристик програмної реалізації, масштабованості та працездатності за часткової неповноти вхідних даних.

Для досягнення поставленої мети сформульовано такі експериментальні задачі:

- 1) верифікувати коректність програмної реалізації розроблених і удосконалених методів та моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ;
- 2) перевірити функціонування нечіткої моделі оцінювання ризиків шляхом аналізу функцій належності, бази нечітких продукційних правил, поверхонь логічного виведення та результатів контрольних сценаріїв;
- 3) дослідити якість класифікації нормальної та аномальної мережевої активності на відкритих наборах даних IoT-безпеки із застосуванням показників Accuracy, Precision, Recall, F1-score та False Positive Rate;
- 4) провести кількісну валідацію FIS-моделі на незалежній тестовій вибірці контекстно-ризикових сценаріїв;
- 5) порівняти запропоновану FIS-модель із двопараметричною детермінованою та семипараметричною зваженою моделями оцінювання ризику на однаковій сценарній вибірці;
- 6) дослідити вплив показника BackdoorRisk, контекстної класифікації та контекстної адаптації на значення й категорію інтегрального показника RiskLevel;
- 7) оцінити часові характеристики безпосереднього інференсу FIS-моделі та зміну часу виконання повного циклу оброблення даних зі збільшенням кількості модельованих IoT-вузлів;
- 8) здійснити попередню перевірку працездатності програмної реалізації за часткової неповноти вхідних даних;
- 9) перевірити функціонування FIS-моделі під час оцінювання типових сценаріїв кіберзагроз у змодельованому IoT-середовищі.

Для перевірки працездатності та оцінювання ефективності запропонованих рішень сформульовано такі дослідницькі гіпотези:

- 1) методи машинного навчання забезпечують розпізнавання нормальної та аномальної мережевої активності на відкритих наборах даних IoT-безпеки з прийнятними значеннями показників якості класифікації;
- 2) запропонована FIS-модель забезпечує розмежування нормальних і ризикових контекстних сценаріїв шляхом формування інтегрального показника RiskLevel;
- 3) урахування семи контекстно-ризикових параметрів і застосування нечіткого логічного виведення забезпечують вищі показники розмежування нормальних і ризикових сценаріїв порівняно з двопараметричною детермінованою та семипараметричною зваженою моделями в межах сформованої сценарної вибірки;
- 4) показник BackdoorRisk здійснює вимірюваний вплив на значення RiskLevel та підсумкову категорію ризику в сценаріях з ознаками прихованої компрометації;
- 5) контекстна класифікація та контекстна адаптація здійснюють вимірюваний вплив на значення й категорію інтегральної оцінки ризику;
- 6) програмна реалізація FIS-моделі забезпечує формування оцінки ризику з часовими характеристиками, достатніми для її застосування в межах досліджених конфігурацій IoT-середовища;
- 7) FIS-модель зберігає працездатність під час оцінювання типових сценаріїв кіберзагроз і за часткової неповноти вхідних даних після їх попереднього відновлення.

Ефективність розроблених і удосконалених методів та моделей оцінювали на основі статистичних показників класифікації мережевих подій, результатів сценарної валідації FIS-моделі, порівняння з двопараметричною детермінованою та семипараметричною зваженою моделями оцінювання ризику, декомпозиційного експерименту, аналізу часових характеристик і масштабованості, попередньої перевірки працездатності за часткової неповноти



вхідних даних та результатів оцінювання типових сценаріїв кіберзагроз у змодельованому IoT-середовищі.

#### ***4.1.2. Обґрунтування вибору програмного середовища експериментальних досліджень***

Для програмної реалізації та експериментальної перевірки розробленого методу контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ використано середовище MATLAB із пакетом Fuzzy Logic Toolbox. Вибір зазначеного програмного середовища зумовлений необхідністю реалізації нечіткої системи логічного виведення типу Мамдані, формування й налаштування функцій належності, побудови бази нечітких продукційних правил, виконання процедур фазифікації та дефазифікації, а також проведення сценарних і порівняльних експериментів.

Пакет Fuzzy Logic Toolbox забезпечує:

- формалізоване задання вхідних і вихідної лінгвістичних змінних;
- побудову трикутних і трапецієподібних функцій належності;
- формування та модифікацію бази нечітких продукційних правил;
- реалізацію нечіткого логічного виведення типу Мамдані;
- використання центроїдного методу дефазифікації;
- візуалізацію поверхонь нечіткого логічного виведення;
- виконання пакетного оцінювання сформованих контекстно-ризикових сценаріїв;
- аналіз впливу окремих вхідних параметрів на інтегральний показник RiskLevel.

У середовищі MATLAB виконано функціональну перевірку FIS-моделі, аналіз функцій належності та бази нечітких продукційних правил, побудову поверхонь логічного виведення, сценарну валідацію моделі, порівняння з двопараметричною детермінованою та семипараметричною зваженою моделями оцінювання ризику, декомпозиційний експеримент і вимірювання часових характеристик безпосереднього інференсу.

Для оцінювання методів класифікації мережових подій використано програмні засоби машинного навчання та статистичного аналізу, реалізовані в

середовищі MATLAB. Експериментальні дані сформовано на основі відкритих наборів BoT-IoT, TON-IoT та Edge-IIoTset. Попереднє опрацювання даних охоплювало узгодження структури ознак, приведення цільових міток до єдиного подання, нормалізацію числових параметрів і формування навчальної та тестової частин вибірки.

Функціональне призначення використаних програмних засобів наведено в Табл. 4.1.

*Таблиця 4.1 – Програмні засоби експериментальної перевірки*

| Програмний засіб                        | Призначення                                               | Використання в експериментах                                                            |
|-----------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------|
| MATLAB                                  | Підготовка даних, реалізація моделей, статистичний аналіз | Основне середовище проведення експериментів                                             |
| Fuzzy Logic Toolbox                     | Побудова нечіткої системи Мамдані                         | Функції належності, база правил, логічне виведення, дефазифікація, формування RiskLevel |
| Statistics and Machine Learning Toolbox | Реалізація методів класифікації                           | Навчання й оцінювання Random Forest, SVM та інших досліджуваних методів                 |
| Засоби візуалізації MATLAB              | Побудова графіків і поверхонь                             | Аналіз результатів FIS та статистичних показників                                       |

Використання єдиного програмного середовища для реалізації нечіткої моделі, базових моделей оцінювання ризику та методів класифікації мережевих подій забезпечило узгодженість процедур експериментальної перевірки, контроль параметрів моделей і відтворюваність отриманих результатів.

#### **4.1.3. Опис експериментального IoT-середовища**

Для експериментальної перевірки розроблених і удосконалених методів та моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ сформовано програмно змодельоване експериментальне середовище. Його структура відповідає функціональному призначенню компонентів інформаційної технології, визначених у третьому розділі, та забезпечує проведення окремих експериментів із класифікації мережевих подій і нечіткого оцінювання ризиків.

Експериментальне середовище містить два функціонально відокремлені контури:

- 1) контур класифікації мережевих подій, призначений для оцінювання методів розпізнавання нормальної та аномальної мережевої активності на даних, сформованих на основі відкритих наборів BoT-IoT, TON-IoT та Edge-IoTset;
- 2) контур контекстно-адаптивного оцінювання ризиків, призначений для функціональної перевірки, сценарної валідації та порівняльного оцінювання нечіткої моделі типу Мамдані на сформованих вибірках контекстно-ризикових сценаріїв.

Зазначені контури використовують різні структури вхідних даних і виконують різні функціональні задачі. Методи класифікації мережевих подій визначають належність мережевих записів до нормальної або аномальної активності, тоді як FIS-модель формує інтегральний показник RiskLevel на основі семи контекстно-ризикових параметрів. Безпосереднє передавання результатів класифікації мережевих подій на входи FIS-моделі у проведених експериментах не здійснювалося.

У контурі класифікації мережевих подій виконувалися узгодження структури даних, відбір спільних числових ознак, очищення записів, приведення цільових міток до бінарного подання, нормалізація параметрів та стратифікований поділ вибірки на навчальну і тестову частини. Після підготовки даних проводилося навчання та оцінювання досліджуваних методів класифікації за показниками Accuracy, Precision, Recall, F1-score та False Positive Rate.

Контур контекстно-адаптивного оцінювання ризиків реалізовано в середовищі MATLAB із використанням пакета Fuzzy Logic Toolbox. Вхідними параметрами FIS-моделі є AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk, значення яких нормалізовано в діапазоні [0; 10]. Вихідною змінною є інтегральний показник RiskLevel, що також визначається в діапазоні [0; 10].

Для перевірки FIS-моделі сформовано контекстно-ризикові сценарії, які характеризують нормальний стан, мережеву розвідку, DDoS-атаку, витік даних та приховану компрометацію. Значення семи вхідних параметрів генерувалися відповідно до визначених для кожного типу сценарію діапазонів. Показник BackdoorRisk у межах цих експериментів задавався як вхідний параметр

відповідно до характеристик сформованого сценарію. Його автоматичне визначення за первинними мережевими або криптографічними даними не здійснювалося.

Для функціональної перевірки FIS-моделі аналізувалися функції належності, база нечітких продукційних правил, поверхні логічного виведення, монотонність зміни RiskLevel та результати контрольних сценаріїв. Кількісну валідацію виконано на незалежній тестовій частині сформованої сценарної вибірки. Окремо проведено порівняння запропонованої FIS-моделі з двопараметричною детермінованою та семипараметричною зваженою моделями оцінювання ризику.

Для дослідження часових характеристик і масштабованості кількість логічно модельованих IoT-вузлів змінювалася відповідно до конфігурації експерименту. Базові функціональні сценарії відтворювали конфігурації з 10–30 умовними IoT-вузлами, а під час окремого дослідження масштабованості їх кількість збільшувалася до 50, 100, 200 і 500. У цьому експерименті модельовані вузли використовувалися як параметр програмного навантаження, а не як фізичні пристрої, що генерують реальний мережевий трафік.

Узагальнену структуру експериментального середовища наведено на Рис. 4.1.



Рисунок 4.1 – Структура експериментальної перевірки розроблених методів і моделей

Основні параметри експериментального середовища наведено в таблиці 4.2.

Таблиця 4.2 – Основні параметри експериментального середовища

| Параметр                             | Значення                                                                                                   | Призначення                                                                            |
|--------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Тип середовища                       | Програмно змодельоване експериментальне середовище                                                         | Перевірка розроблених і удосконалених методів та моделей                               |
| Експериментальні контури             | Класифікація мережевих подій; FIS-оцінювання ризиків                                                       | Роздільне оцінювання функціонально відмінних компонентів                               |
| Джерела мережевих даних              | BoT-IoT, TON-IoT, Edge-IIoTset                                                                             | Формування уніфікованої вибірки мережевих подій                                        |
| Обсяг уніфікованої мережевої вибірки | 20 527 записів                                                                                             | Навчання і тестування методів класифікації                                             |
| Класи мережевих подій                | Нормальна активність; кіберінцидент                                                                        | Бінарна класифікація мережевих записів                                                 |
| Середовище реалізації FIS            | MATLAB, Fuzzy Logic Toolbox                                                                                | Реалізація нечіткого логічного виведення                                               |
| Тип нечіткої системи                 | Mamdani FIS                                                                                                | Контекстно-адаптивне оцінювання ризиків                                                |
| Кількість вхідних параметрів FIS     | 7                                                                                                          | Формування інтегральної оцінки ризику                                                  |
| Вхідні параметри                     | AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity, BackdoorRisk | Урахування контекстно-ризикових характеристик                                          |
| Діапазон вхідних параметрів          | [0; 10]                                                                                                    | Нормалізований універсум значень                                                       |
| Вихідний показник                    | RiskLevel у діапазоні [0; 10]                                                                              | Інтегральна оцінка ризику                                                              |
| База нечітких правил                 | 40 унікальних правил                                                                                       | Формалізація взаємозв'язків між параметрами                                            |
| Типи контекстно-ризикових сценаріїв  | Нормальний стан, мережева розвідка, DDoS, витік даних, прихована компрометація                             | Сценарна валідація FIS-моделі                                                          |
| Базові моделі оцінювання ризику      | Двопараметрична детермінована; семипараметрична зважена                                                    | Порівняльне оцінювання FIS-моделі                                                      |
| Базова кількість модельованих вузлів | 10–30 умовних IoT-вузлів                                                                                   | Функціональна апробація програмної реалізації                                          |
| Конфігурації масштабованості         | 50, 100, 200 і 500 умовних вузлів                                                                          | Аналіз зміни часу повного циклу оброблення                                             |
| Метрики класифікації                 | Accuracy, Precision, Recall, F1-score, FPR                                                                 | Оцінювання методів класифікації мережевих подій                                        |
| Метрики сценарної валідації FIS      | Accuracy, Precision, Recall, F1-score, FPR, Specificity, ROC-AUC                                           | Оцінювання здатності RiskLevel розмежовувати сформовані нормальні та ризикові сценарії |

Як видно з Табл.4.2, сформоване експериментальне середовище забезпечує роздільне оцінювання методів класифікації мережевих подій і нечіткої моделі контекстно-адаптивного оцінювання ризиків. Використання відкритих наборів даних дає змогу дослідити якість розпізнавання нормальної та аномальної мережевої активності, тоді як сформовані контекстно-ризикові сценарії забезпечують функціональну та кількісну перевірку FIS-моделі. Розмежування зазначених експериментів виключає необґрунтоване подання методів класифікації та FIS як єдиної інтегрованої схеми.

#### **4.2. Програмна реалізація методу контекстно-адаптивного оцінювання ризиків**

У цьому підрозділі наведено особливості програмної реалізації удосконаленого методу контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані. Реалізована нечітка модель забезпечує формування інтегрального показника RiskLevel з урахуванням семи вхідних параметрів: критичності активу AssetCriticality, рівня загрози ThreatLevel, рівня вразливості Vulnerability, можливостей потенційного порушника AttackerCapability, імовірності реалізації загрози Likelihood, тяжкості потенційних наслідків ImpactSeverity та показника ризику прихованої компрометації BackdoorRisk.

Програмну реалізацію виконано в середовищі MATLAB із використанням пакета Fuzzy Logic Toolbox. Зазначений пакет використано для формування вхідних і вихідної лінгвістичних змінних, задання функцій належності, побудови бази нечітких продукційних правил, реалізації логічного виведення типу Мамдані та центроїдної дефазифікації. Засоби MATLAB також застосовано для пакетного оцінювання контекстно-ризикових сценаріїв, побудови поверхонь логічного виведення, перевірки поведінки моделі та кількісного аналізу отриманих результатів.

Реалізована програмна модель забезпечує можливість зміни параметрів функцій належності та бази нечітких продукційних правил, виконання контрольних і сценарних експериментів, аналізу впливу окремих вхідних параметрів на значення RiskLevel та відтворення умов проведених експериментальних досліджень.

#### **4.2.1. Реалізація нечіткої моделі**

Програмну реалізацію нечіткої моделі контекстно-адаптивного оцінювання ризиків виконано у вигляді системи логічного виведення типу Мамдані. Вхідними змінними моделі є критичність активу *AssetCriticality*, рівень загрози *ThreatLevel*, рівень вразливості *Vulnerability*, можливості потенційного порушника *AttackerCapability*, імовірність реалізації загрози *Likelihood*, тяжкість потенційних наслідків *ImpactSeverity* та показник ризику прихованої компрометації *BackdoorRisk*.

Під час функціонування інформаційної технології значення вхідних параметрів мають формуватися на основі контекстно-ризикового профілю IoT-пристрою, відомостей про активи, загрози й вразливості, характеристики потенційного порушника, оцінок імовірності та наслідків, а також наявних ознак прихованої компрометації. У межах проведених сценарних експериментів значення семи вхідних параметрів задавалися відповідно до визначених діапазонів для кожного типу контекстно-ризикового сценарію. Для забезпечення сумісності різнорідних показників усі вхідні параметри подано в нормалізованому універсумі  $[0; 10]$ .

Для змінних *AssetCriticality*, *ThreatLevel*, *Vulnerability*, *Likelihood*, *ImpactSeverity* та *BackdoorRisk* використано по три лінгвістичні терми: Low, Medium і High. Для змінної *AttackerCapability* застосовано терми Basic, Intermediate та Advanced, які характеризують відповідно базовий, проміжний і високий рівні підготовки та технічних можливостей потенційного порушника. Вихідною лінгвістичною змінною є *RiskLevel*, для якої визначено чотири терми: Low, Moderate, High і Critical.

Лінгвістичні терми описано трикутними та трапецієподібними функціями належності. Трикутні функції використано для забезпечення плавних переходів між суміжними лінгвістичними оцінками, а трапецієподібні для подання крайніх областей універсуму та формування зон насичення. Параметри функцій належності визначено на основі експертного подання взаємозв'язків між досліджуваними факторами ризику та формалізації, наведеної в підрозділі 2.3.1.

Процедура формування інтегральної оцінки охоплює фазифікацію вхідних значень, визначення ступенів активації нечітких продукційних правил,

агрегування результатів логічного виведення та дефазифікацію вихідної змінної. Для отримання числового значення RiskLevel використано центроїдний метод дефазифікації. Результатом роботи моделі є чітке значення RiskLevel у діапазоні  $[0; 10]$ , яке характеризує інтегральний рівень ризику інформаційної безпеки IoT-пристрою або досліджуваного сценарію.

Для практичної інтерпретації числового значення RiskLevel встановлено такі інтервали:

- *низький ризик* - від 0 до 2,5 включно;
- *помірний ризик* - понад 2,5 до 5,0 включно;
- *підвищений ризик* - понад 5,0 до 7,0 включно;
- *критичний ризик* - понад 7,0 до 10,0 включно.

Підсумкову категорію ризику визначають за дефазифікованим числовим значенням RiskLevel відповідно до встановлених інтервалів. Максимальний ступінь належності отриманого значення окремому терму вихідної змінної для визначення підсумкової категорії не використовується. Такий підхід забезпечує однозначну інтерпретацію результатів моделі під час сценарної валідації та порівняльного оцінювання.

#### **4.2.2. Формування бази продукційних правил**

Базу нечітких продукційних правил реалізовано засобами MATLAB Fuzzy Logic Toolbox у вигляді набору правил типу IF–THEN, які визначають взаємозв'язок між лінгвістичними оцінками вхідних параметрів та відповідним термом вихідної змінної RiskLevel. Продукційні правила формалізують експертно визначену логіку контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ.

Інформаційну основу бази правил становлять сім вхідних лінгвістичних змінних: AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk. Кожне правило описує характерне поєднання факторів ризику та визначає відповідний лінгвістичний рівень вихідної змінної RiskLevel.

Умова окремого правила може містити повну множину вхідних змінних або їх змістовно обґрунтовану підмножину. Використання підмножин дає змогу



формалізувати сценарії, у яких результируючий рівень ризику переважно визначається окремою комбінацією найбільш значущих факторів. Вхідні змінні, не зазначені в умові такого правила, не впливають на ступінь його активації.

Узагальнений приклад реалізованого правила має вигляд:

*IF AssetCriticality = High AND ThreatLevel = High AND Vulnerability = High THEN RiskLevel = Critical.*

Наведене правило визначає критичний рівень ризику за одночасно високих значень критичності активу, рівня загрози та вразливості. Значення *AttackerCapability*, *Likelihood*, *ImpactSeverity* і *BackdoorRisk* у передумові цього правила не задаються та не враховуються під час визначення ступеня його активації. В інших правилах зазначені параметри використовуються окремо або у взаємозв'язку з іншими факторами ризику.

Для визначення ступеня активації правил з умовами, поєднаними оператором AND, використано операцію нечіткої кон'юнкції *minimum*. Ступінь активації кожного правила визначається мінімальним ступенем належності фактичних значень вхідних параметрів відповідним лінгвістичним термам, зазначеним у його передумові.

Повний комбінаторний простір для семи вхідних змінних із трьома лінгвістичними термами для кожної змінної містить 2187 можливих комбінацій. Використання повної бази правил є недоцільним через значну кількість малоімовірних, надлишкових або практично неінформативних сценаріїв. Тому в програмній реалізації використано оптимізовану базу, що містить 40 унікальних нечітких продукційних правил.

Правила сформовано відповідно до принципів посилення ризику зі зростанням критичності активу, рівня загрози, вразливості, можливостей потенційного порушника, імовірності реалізації загрози та тяжкості наслідків. Окремі правила враховують підвищений ризик прихованої компрометації у взаємозв'язку з іншими контекстно-ризиковими параметрами. Високе значення *BackdoorRisk* при цьому не розглядається як автоматичне підтвердження наявності прихованої компрометації, а використовується як один із факторів формування інтегрального показника *RiskLevel*.

Реалізація бази правил у MATLAB Fuzzy Logic Toolbox забезпечує автоматичне визначення ступенів їх активації, агрегування результатів нечіткого логічного виведення та подальшу дефазифікацію вихідної змінної. Програмне подання правил також забезпечує можливість їх перегляду, коригування та розширення відповідно до зміни характеристик IoT-середовища і складу врахованих кіберзагроз.

#### ***4.2.3. Валідація програмної реалізації***

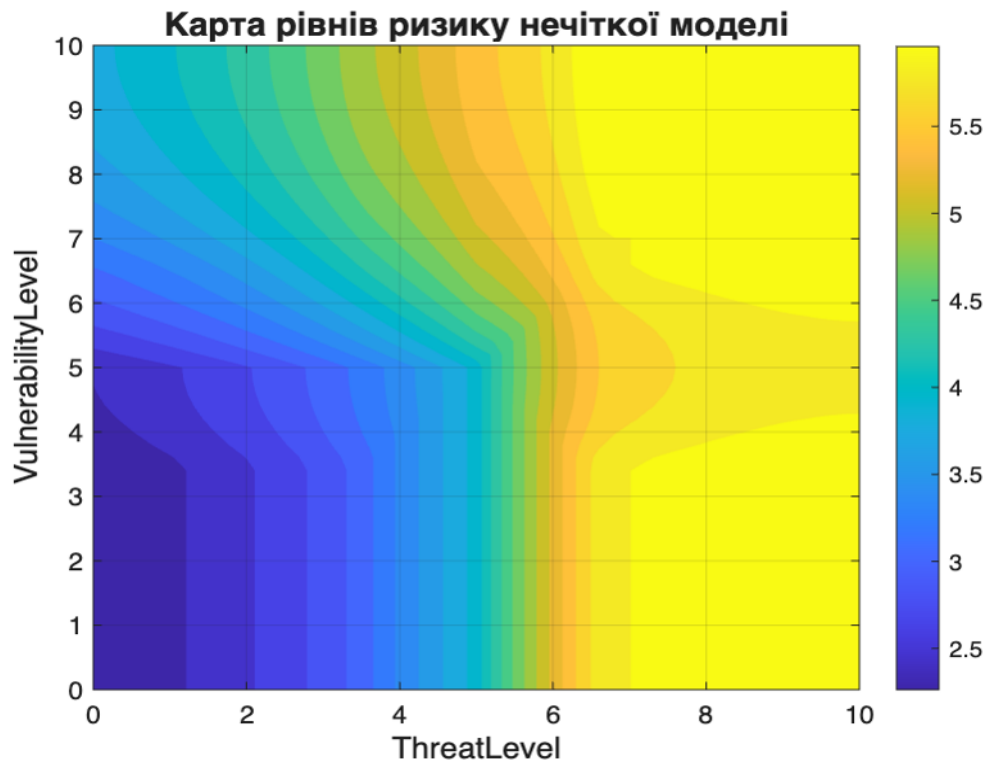
Після програмної реалізації нечіткої моделі та формування бази продукційних правил проведено функціональну перевірку логіки її роботи. Метою цього етапу було підтвердження коректності активації нечітких продукційних правил, узгодженості зміни інтегрального показника RiskLevel зі зміною вхідних параметрів та відповідності отриманих результатів логіки сформованої бази знань.

Перевірку виконано в середовищі MATLAB із використанням засобів Rule Viewer та Surface Viewer пакета Fuzzy Logic Toolbox. Rule Viewer застосовано для аналізу процесу фазифікації вхідних значень, ступенів активації продукційних правил та формування вихідної нечіткої множини. Surface Viewer використано для побудови двовимірних зрізів поверхні нечіткого логічного виведення й дослідження взаємного впливу окремих вхідних параметрів на значення RiskLevel.

На першому етапі перевірено активацію продукційних правил для контрольних комбінацій семи вхідних параметрів. Аналіз показав, що зміна вхідних значень приводить до активації відповідних правил та формування числового значення RiskLevel згідно із закладеною логікою бази знань. Таким чином підтверджено коректність програмної реалізації процедур фазифікації, нечіткого логічного виведення, агрегування результатів активованих правил і центроїдної дефазифікації.

Для візуального аналізу поведінки моделі побудовано двовимірний зріз поверхні RiskLevel залежно від значень ThreatLevel і Vulnerability. Під час побудови поверхні значення інших п'яти вхідних параметрів - AssetCriticality, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk - було зафіксовано

на рівні 5. Значення ThreatLevel і Vulnerability змінювалися в межах нормалізованого універсуму  $[0; 10]$ . Результати аналізу наведено на Рис. 4.2.



*Рисунок 4.2 – Двовимірний зріз поверхні RiskLevel залежно від ThreatLevel і Vulnerability за фіксованих значень інших вхідних параметрів*

Отримана поверхня має нелінійний характер, що зумовлено формою функцій належності, одночасною активацією декількох продукційних правил та агрегуванням результатів нечіткого логічного виведення. Зі збільшенням ThreatLevel і Vulnerability значення RiskLevel загалом зростає. Найбільш виражена зміна спостерігається приблизно в діапазоні ThreatLevel від 5 до 6, де відбувається перехід між областями активації суміжних лінгвістичних термів і продукційних правил.

За дослідженої конфігурації значення RiskLevel змінюється приблизно від 2,3 до 6,1. Відповідно до встановлених інтервалів інтерпретації цей діапазон охоплює низьку, помірну та частину підвищеної категорії ризику. Критична категорія на наведеному зрізі не формується, оскільки інші п'ять вхідних параметрів зафіксовано на середньому рівні. Наведений рисунок характеризує поведінку моделі за вибраної конфігурації та не відображає повністю семивимірний простір нечіткого логічного виведення.

Додатково проведено покомпонентну перевірку монотонності FIS-моделі для опорної конфігурації. У межах цієї перевірки значення шести вхідних параметрів фіксувалися на рівні 5, а значення сьомого параметра послідовно змінювалося від 0 до 10 із кроком 0,1. Перевірку по чергово виконано для AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk. Для кожного вхідного параметра проаналізовано 101 значення.

Критерієм покомпонентної монотонності була відсутність зниження RiskLevel зі збільшенням значення досліджуваного вхідного параметра за незмінних значень інших шести параметрів. Горизонтальні ділянки залежностей, на яких збільшення вхідного параметра не спричиняє зміни RiskLevel, не розглядалися як порушення монотонності. Результати перевірки наведено на Рис. 4.3.

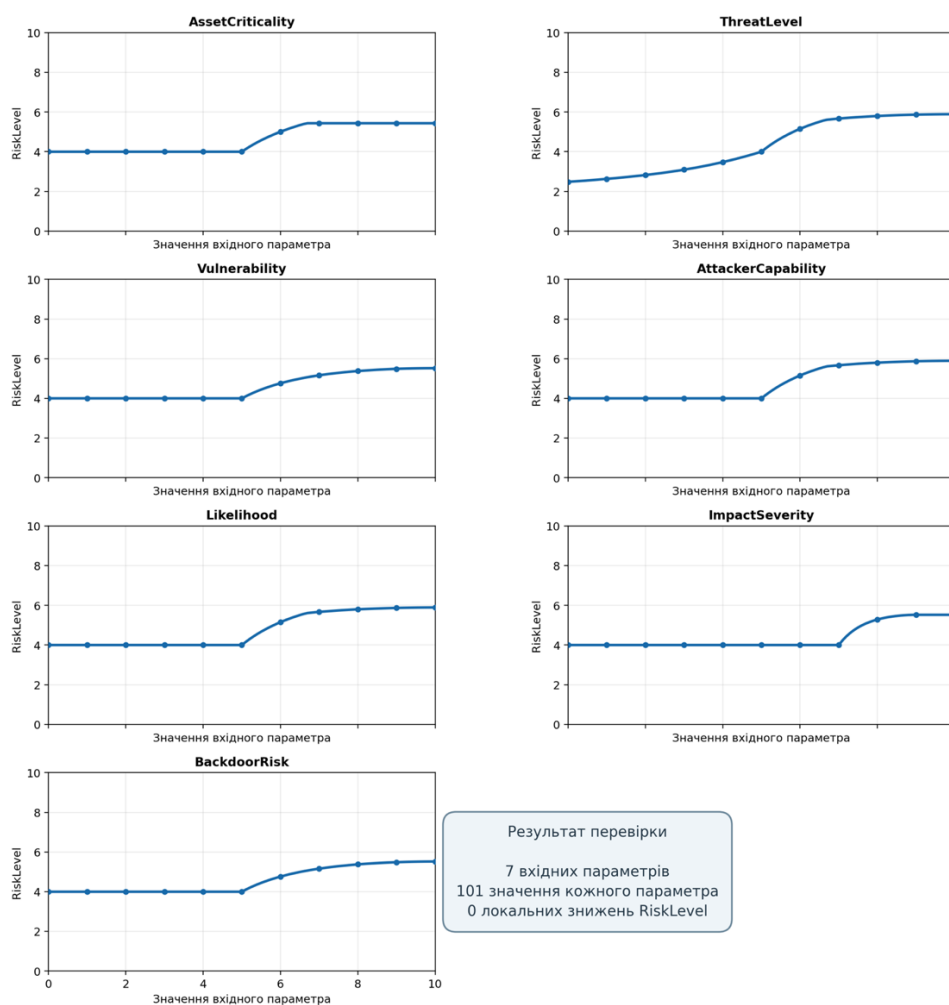


Рисунок 4.3 – Покомпонентна перевірка монотонності FIS-моделі для опорної конфігурації

Отримані залежності показали, що для дослідженої опорної конфігурації збільшення кожного із семи вхідних параметрів не спричиняє зменшення інтегрального показника RiskLevel. У межах 707 виконаних оцінювань, що відповідають 101 значенню для кожного із семи параметрів, локальних знижень RiskLevel не виявлено.

Наявність горизонтальних ділянок на окремих графіках пояснюється тим, що зміна одного параметра в певному діапазоні не завжди приводить до активації додаткових продукційних правил або зміни домінуючої області агрегованої вихідної нечіткої множини. Після переходу значення параметра до іншої області функцій належності активуються додаткові правила, що приводить до подальшого збільшення RiskLevel.

Результати покомпонентної перевірки підтверджують монотонний характер реакції FIS-моделі за всіма сімома входами для дослідженої опорної конфігурації. Водночас отриманий результат не розглядається як доказ глобальної монотонності моделі в усьому семивимірному просторі вхідних параметрів, оскільки інші шість входів під час кожної перевірки фіксувалися на рівні 5.

Проведена функціональна перевірка підтвердила коректність програмної реалізації нечіткої моделі, узгодженість її реакції з логікою сформованої бази знань та можливість використання для контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ. Подальше кількісне оцінювання FIS-моделі на незалежній тестовій вибірці контекстно-ризикових сценаріїв наведено в наступних підрозділах.

#### **4.3. Експериментальне оцінювання методів класифікації мережевих подій на відкритих наборах даних**

Для експериментального оцінювання методів класифікації мережевих подій проведено дослідження з використанням відкритих наборів даних IoT-безпеки. Метою експерименту було визначення здатності досліджуваних методів машинного навчання розпізнавати нормальну та аномальну мережеву активність і порівняння отриманих результатів за визначеними статистичними показниками.

Як джерела мережевих даних використано відкриті набори BoT-IoT, TON-IoT та Edge-IoTset, що містять записи нормального функціонування IoT-компонентів і різних типів кібератак. Використання декількох наборів даних дало змогу сформувати експериментальну вибірку, яка охоплює різні типи мережевої активності та сценарії кіберінцидентів.

Підготовка експериментальних даних охоплювала очищення записів, узгодження структури ознак, приведення цільових міток до єдиного подання, нормалізацію числових параметрів та формування навчальної і тестової частин вибірки. Для оцінювання методів класифікації використано показники Accuracy, Precision, Recall, F1-score та False Positive Rate. Додатково для Accuracy визначено 95% довірчі інтервали, а стабільність результатів на навчальній частині перевірено із застосуванням п'ятикратної крос-валідації.

Експеримент із класифікації мережевих подій проведено окремо від сценарної валідації FIS-моделі. Результати методів машинного навчання не передавалися на входи нечіткої моделі та не використовувалися для автоматичного формування параметрів AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity або BackdoorRisk. Кількісне оцінювання FIS-моделі на сформованих контекстно-ризикових сценаріях наведено окремо в підрозділі 4.5.

#### **4.3.1. Опис датасетів**

Для експериментального оцінювання методів класифікації мережевих подій використано відкриті набори даних, що містять записи нормальної та аномальної активності IoT- та IoT-середовищ. Застосування відкритих наборів даних забезпечує можливість відтворення процедур підготовки експериментальної вибірки, порівняння досліджуваних методів за однаковими показниками та зіставлення отриманих результатів із результатами інших досліджень.

Відкриті набори даних використовувалися виключно для формування вибірки мережевих подій і порівняльного оцінювання методів їх класифікації. Вони не застосовувалися для безпосереднього формування семи вхідних параметрів FIS-моделі, а результати класифікації мережевих записів не

передавалися до нечіткої системи оцінювання ризиків. Сценарну валідацію FIS-моделі проведено окремо на сформованих вибірках контекстно-ризикових сценаріїв.

У межах дослідження використано три відкриті набори даних IoT-безпеки: Edge-IoTset [87], BoT-IoT [138] та TON-IoT [139]. Вибір цих наборів зумовлений наявністю в них нормальної мережевої активності, різних класів кібератак, числових характеристик мережевих з'єднань та цільових міток, необхідних для навчання й тестування методів класифікації.

Набір даних BoT-IoT сформовано в лабораторному мережевому середовищі UNSW Canberra. Він містить нормальний мережевий трафік і ботнет-активність, зокрема DoS- і DDoS-атаки, мережеву розвідку, сканування, кейлогінг та витік даних. Записи набору представлені у форматах PCAP, Argus і CSV та містять мітки категорій і підкатегорій атак.

Набір даних TON-IoT сформовано в експериментальному середовищі, що відтворює взаємодію IoT-, PoT-, хмарних і периферійних компонентів. Він поєднує мережевий трафік, телеметричні дані IoT-пристроїв і журнали операційних систем. Набір містить нормальну активність та різні типи кібератак, зокрема сканування, DoS- і DDoS-атаки, ін'єкційні атаки, активність бекдорів, ransomware та атаки на вебзастосунки.

Набір даних Edge-IoTset орієнтований на оцінювання засобів виявлення атак у середовищах IoT, PoT та периферійних обчислень. Його сформовано з використанням багаторівневого експериментального стенда, що містив IoT-пристрої, сенсори, мережеві протоколи, хмарні й периферійні компоненти. Набір охоплює DoS- і DDoS-атаки, збирання інформації, атаки типу «людина посередині», ін'єкційні атаки та шкідливу активність.

Первинні набори даних відрізняються структурою ознак, форматами записів, складом класів і співвідношенням нормальної та аномальної активності. Тому вони не об'єднувалися безпосередньо в початковому вигляді. Перед формуванням експериментальної вибірки виконано відбір спільних числових ознак, приведення цільових міток до єдиного подання, очищення даних і нормалізацію параметрів. Категоріальні та службові ознаки, які не мали

однозначної відповідності між наборами, до уніфікованого вектора ознак не включалися.

Основні характеристики використаних наборів даних наведено в таблиці 4.3.

*Таблиця 4.3 – Характеристики використаних наборів даних*

| Набір даних | Тип середовища            | Характер даних                                                 | Основні типи атак                                                             | Використання в дослідженні                                          | Джерело |
|-------------|---------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------|---------|
| Edge-IoTset | IoT, PoT, Edge            | Мережевий трафік, журнали, системні та ресурсні характеристики | DoS/DDoS, збирання інформації, MITM, ін'єкційні атаки, шкідлива активність    | Формування вибірки мережевих подій і відбір спільних числових ознак | [87]    |
| BoT-IoT     | Лабораторна IoT-мережа    | Мережеві потоки, PCAP, Argus, CSV                              | DoS/DDoS, мережева розвідка, сканування, кейлогінг, витік даних               | Формування вибірки нормальної та аномальної мережевої активності    | [138]   |
| TON-IoT     | IoT, PoT, Cloud, Edge/Fog | Мережевий трафік, телеметрія, журнали операційних систем       | Сканування, DoS/DDoS, backdoor, injection, ransomware, атаки на вебзастосунки | Формування уніфікованої мережевої вибірки за спільними ознаками     | [139]   |

Як видно з таблиці 4.3, використані набори даних охоплюють різні типи IoT- та PoT-середовищ і містять різноманітні види нормальної та аномальної мережевої активності. Це створює інформаційну основу для порівняльного оцінювання методів класифікації мережевих подій. Водночас усі три набори сформовано в лабораторних або програмно змодельованих середовищах, тому отримані результати характеризують працездатність досліджуваних методів на відкритих експериментальних даних і не розглядаються як повна перевірка в умовах реальної промислової експлуатації.

#### **4.3.2. Підготовка уніфікованої експериментальної вибірки**

Перед проведенням експериментального оцінювання методів класифікації мережевих подій виконано попереднє опрацювання даних, отриманих із наборів BoT-IoT, TON-IoT та Edge-IoTset. Необхідність цього етапу зумовлена відмінностями у структурі ознак, форматах подання даних, системах цільових



міток і співвідношенні класів нормальної та аномальної активності у вихідних наборах [87,138,139].

На першому етапі виконано очищення даних від дублікатів, записів із некоректними значеннями та прикладів, які не могли бути однозначно приведені до спільної структури. Категоріальні й службові ознаки, що не мали однозначної відповідності між використаними наборами, до уніфікованого вектора ознак не включалися.

Після очищення даних відібрано спільні числові ознаки, які характеризують мережеві з'єднання та можуть бути узгоджено представлені для записів із різних наборів. Цільові мітки приведено до бінарного подання: нормальна активність і кіберінцидент. До класу кіберінцидентів віднесено записи різних типів аномальної та атакуючої мережевої активності, наявні у вихідних наборах даних.

У результаті попереднього опрацювання сформовано уніфіковану експериментальну вибірку обсягом 20 527 записів. Із них 11 773 записи відповідають нормальній мережевій активності, а 8754 - кіберінцидентам. Таким чином, частка нормальної активності становить приблизно 57,35%, а частка кіберінцидентів - 42,65%.

Штучне вирівнювання кількості записів двох класів у підсумковій вибірці не проводилося. Для збереження співвідношення класів під час формування навчальної та тестової частин застосовано стратифікований поділ у співвідношенні 80/20. Навчальна частина містила 16 422 записи, тестова - 4105 записів.

Параметри нормалізації числових ознак визначалися за навчальною частиною вибірки, після чого ті самі параметри застосовувалися до тестових даних. Такий порядок запобігає використанню інформації з тестової частини під час підготовки навчальних даних. Тестова вибірка не використовувалася для навчання моделей або визначення параметрів нормалізації.

Розподіл записів між класами та частинами експериментальної вибірки наведено в Табл. 4.4.

Таблиця 4.4 – Розподіл записів у сформованій експериментальній вибірці

| Клас мережевої активності | Загальна кількість | Навчальна частина | Тестова частина |
|---------------------------|--------------------|-------------------|-----------------|
| Нормальна активність      | 11 773             | 9418              | 2355            |
| Кіберінцидент             | 8754               | 7004              | 1750            |
| Разом                     | 20 527             | 16 422            | 4105            |

Для оцінювання стабільності результатів на навчальній частині вибірки застосовано п'ятикратну стратифіковану крос-валідацію. Остаточні показники Accuracy, Precision, Recall, F1-score та False Positive Rate визначалися на незалежній тестовій частині, яка містила 4105 записів.

Сформована уніфікована вибірка забезпечує однакові умови навчання та тестування всіх досліджуваних методів класифікації мережевих подій. Збереження співвідношення класів, роздільне визначення параметрів нормалізації та використання незалежної тестової частини підвищують обґрунтованість порівняльного оцінювання отриманих результатів.

#### 4.3.3. Методи та метрики класифікації мережевих подій

Для експериментального оцінювання класифікації мережевих подій використано п'ять методів машинного навчання: Random Forest, Support Vector Machine з ядром RBF, Gradient Boosting, XGBoost та багатошарову нейронну мережу. Для Random Forest використано 200 дерев, для Gradient Boosting і XGBoost - по 200 оцінювачів із коефіцієнтом швидкості навчання 0,1. Нейронна мережа містила два приховані шари з 32 і 16 нейронами.

Задачу сформульовано як бінарну класифікацію: нормальна мережева активність відповідала негативному класу, а кіберінциденти - позитивному. Налаштування та проміжне оцінювання моделей виконано на навчальній частині даних із застосуванням п'ятикратної стратифікованої крос-валідації. Незалежна тестова вибірка обсягом 4105 записів не використовувалася під час навчання та налаштування моделей і застосовувалася виключно для підсумкового оцінювання.

Результативність методів оцінювалася за показниками Accuracy, Precision, Recall, F1-score та False Positive Rate (FPR). Для Accuracy додатково визначено 95-відсотковий довірчий інтервал. Використання єдиної навчальної та тестової

вибірок і однакового набору метрик забезпечило коректність порівняння досліджуваних методів класифікації.

#### **4.3.4. Результати класифікації мережевих подій**

За результатами експериментального дослідження отримано кількісні показники класифікації мережевих подій на незалежній тестовій вибірці. Оцінювання проведено для методів Random Forest, Support Vector Machine, Gradient Boosting, XGBoost та багатошарової нейронної мережі. Результати наведено в таблиці 4.5.

*Таблиця 4.5 – Результати класифікації мережевих подій*

| Метод             | Accuracy | Precision | Recall | F1-score | FPR    | 5-fold CV Accuracy |
|-------------------|----------|-----------|--------|----------|--------|--------------------|
| Random Forest     | 0,9462   | 0,9479    | 0,9246 | 0,9361   | 0,0378 | 0,9428             |
| SVM               | 0,8443   | 0,8807    | 0,7343 | 0,8009   | 0,0739 | 0,8413             |
| Gradient Boosting | 0,9413   | 0,9510    | 0,9091 | 0,9296   | 0,0348 | 0,9388             |
| Neural Network    | 0,8716   | 0,8651    | 0,8280 | 0,8461   | 0,0960 | 0,8606             |
| XGBoost           | 0,9481   | 0,9661    | 0,9103 | 0,9374   | 0,0238 | 0,9414             |

Найвище точкове значення Accuracy отримано для XGBoost - 0,9481. Цей метод також забезпечив найвищі значення Precision - 0,9661 і F1-score - 0,9374, а також найнижче значення FPR - 0,0238. Водночас найвище значення Recall продемонстрував Random Forest - 0,9246.

Для Accuracy додатково визначено 95-відсоткові довірчі інтервали: Random Forest - [0,9393; 0,9531], SVM - [0,8333; 0,8554], Gradient Boosting - [0,9341; 0,9485], Neural Network - [0,8614; 0,8819], XGBoost - [0,9413; 0,9549].

Довірчі інтервали XGBoost, Random Forest і Gradient Boosting частково перекриваються. Тому XGBoost має найвище точкове значення Accuracy, однак без проведення додаткового статистичного тестування отримані результати не підтверджують його статистично значущої переваги над Random Forest і Gradient Boosting.

Значення Accuracy, отримані під час п'ятикратної стратифікованої крос-валідації, загалом узгоджуються з результатами незалежної тестової вибірки. Це свідчить про відсутність суттєвого погіршення якості класифікації під час переходу від навчальних даних до незалежної тестової частини.

Отримані результати підтверджують можливість застосування досліджуваних методів машинного навчання для розпізнавання нормальної активності та кіберінцидентів у мережевих даних IoT-середовищ. Найвищі сукупні показники в межах сформованої експериментальної вибірки отримано для XGBoost і Random Forest.

#### **4.4. Експериментальна перевірка методу контекстно-адаптивного оцінювання ризиків у змодельованому IoT-середовищі**

Після перевірки програмної реалізації FIS-моделі та експериментального оцінювання методів класифікації мережевих подій проведено сценарну перевірку удосконаленого методу контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ.

Метою цього етапу було дослідження здатності FIS-моделі формувати диференційовані значення інтегрального показника RiskLevel за різних комбінацій контекстно-ризикових параметрів, кількісне оцінювання результативності моделі на незалежній тестовій вибірці та її порівняння з базовими моделями оцінювання ризику.

Експериментальна перевірка охоплювала формування вибірки контекстно-ризикових сценаріїв, визначення порогових значень моделей на валідаційній частині, остаточне оцінювання на незалежній тестовій частині, порівняння FIS із двопараметричною детермінованою та семипараметричною зваженою моделями, а також дослідження впливу сценарної варіативності параметра BackdoorRisk на формування RiskLevel.

##### **4.4.1. Формування контекстно-ризикових сценаріїв**

Для кількісної експериментальної перевірки сформовано 100 000 контекстно-ризикових сценаріїв функціонування IoT-середовища.

Кожний сценарій задавався вектором семи вхідних параметрів FIS-моделі:

$$X(d) = \langle AC(d), TL(d), V(d), CAP(d), L(d), IS(d), BR(d) \rangle$$

Значення всіх параметрів формувалися в межах нормалізованого універсуму [0; 10]. До вибірки включено п'ять класів сценаріїв: нормальне функціонування, мережева розвідка, DoS/DDoS-атака, витік даних і прихована компрометація. Для кожного класу сформовано по 20 000 сценаріїв.

Діапазони генерації параметрів визначено відповідно до змісту модельованих станів. У межах установлених діапазонів значення генерувалися за рівномірним розподілом. Для забезпечення відтворюваності використано фіксоване початкове значення генератора псевдовипадкових чисел `seed = 20260822`. Діапазони параметрів наведено в Табл. 4.6.

*Таблиця 4.6 – Діапазони формування контекстно-ризикових сценаріїв*

| Клас сценарію            | Asset Criticality | Threat Level | Vulnerability | Attacker Capability | Likelihood | Impact Severity | Backdoor Risk |
|--------------------------|-------------------|--------------|---------------|---------------------|------------|-----------------|---------------|
| Нормальне функціонування | 0–5               | 0–4          | 0–4           | 0–4                 | 0–4        | 0–4             | 0–3           |
| Мережева розвідка        | 2–7               | 4–8          | 3–7           | 3–7                 | 3–7        | 1–5             | 0–3           |
| DoS/DDoS                 | 4–9               | 6–10         | 3–7           | 4–8                 | 6–10       | 5–9             | 0–4           |
| Витік даних              | 5–10              | 5–9          | 6–10          | 5–9                 | 5–9        | 6–10            | 2–6           |
| Прихована компрометація  | 5–10              | 5–9          | 5–9           | 6–10                | 5–9        | 6–10            | 7–10          |

Для відтворення нормальних станів критичних IoT-компонентів у 55 % сценаріїв нормального функціонування значення `AssetCriticality` додатково задавалося в діапазоні [7,10], а `AttackerCapability` - у діапазоні [4,8]. Такий підхід враховує, що висока критичність пристрою або можливості потенційного порушника самі по собі не означають наявності актуальної кіберзагрози за низьких значень `ThreatLevel`, `Vulnerability`, `Likelihood`, `ImpactSeverity` та `BackdoorRisk`. Водночас це дає змогу перевірити здатність моделей урахувувати спільний, а не ізольований вплив параметрів.

Сформовану вибірку стратифіковано розділено на дві частини:

- 1) валідаційну - 60 000 сценаріїв, по 12 000 кожного класу;
- 2) незалежну тестову - 40 000 сценаріїв, по 8000 кожного класу.

Після приведення цільових міток до бінарного подання тестова частина містила 8000 сценаріїв нормального функціонування та 32 000 ризикових сценаріїв. Валідаційна частина використовувалася виключно для визначення порогових значень моделей, а тестова - для остаточного обчислення показників їх результативності.

#### 4.4.2. Функціональна перевірка FIS-моделі на контрольних сценаріях

Перед проведенням кількісного оцінювання здійснено функціональну перевірку FIS-моделі на чотирьох контрольних сценаріях. Метою перевірки було встановлення відповідності сформованих значень RiskLevel змісту заданих комбінацій факторів ризику.

У кожному сценарії задавалися конкретні значення семи вхідних параметрів, після чого засобами нечіткого логічного виведення типу Мамдані визначалося дефазифіковане значення RiskLevel. Результати наведено в таблиці 4.7.

Таблиця 4.7 – Результати оцінювання ризику для контрольних сценаріїв

| Сценарій                | AssetCriticality | ThreatLevel | Vulnerability | Attacker Capability | Likelihood | ImpactSeverity | BackdoorRisk | RiskLevel | Категорія ризику |
|-------------------------|------------------|-------------|---------------|---------------------|------------|----------------|--------------|-----------|------------------|
| Мережева розвідка       | 4                | 5           | 5             | 4                   | 4          | 3              | 1            | 3,4633    | Помірний         |
| DoS/DDoS-атака          | 7                | 8           | 5             | 6                   | 8          | 7              | 2            | 6,6807    | Підвищений       |
| Витік даних             | 8                | 7           | 8             | 7                   | 7          | 8              | 4            | 6,5360    | Підвищений       |
| Прихована компрометація | 9                | 8           | 8             | 8                   | 8          | 9              | 9            | 7,4453    | Критичний        |

Для сценарію мережевої розвідки отримано RiskLevel = 3,4633, що відповідає помірній категорії ризику. Для сценаріїв DoS/DDoS та витоку даних одержано відповідно 6,6807 і 6,5360, що належать до підвищеної категорії. Найвище значення RiskLevel = 7,4453 сформовано для сценарію прихованої компрометації, який характеризувався високими значеннями більшості вхідних параметрів, зокрема BackdoorRisk = 9.

Отримані результати підтвердили здатність FIS-моделі диференціювати контрольні сценарії відповідно до сукупного впливу заданих факторів. Водночас зазначена перевірка характеризує реакцію моделі на попередньо сформоване значення BackdoorRisk і не підтверджує автоматичного виявлення прихованої компрометації за первинними мережевими або криптографічними даними.

#### 4.4.3. Кількісна валідація FIS-моделі на незалежній сценарній вибірці

Для кількісної валідації FIS-моделі значення RiskLevel обчислено для всіх 100 000 сформованих сценаріїв. Порогове значення для розмежування нормальних і ризикових станів визначалося на валідаційній вибірці за критерієм максимізації F1-міри.

За результатами валідації встановлено порогове значення:

$$RiskLevel=3,7244.$$

Сценарій відносився до ризикового класу, якщо сформоване значення RiskLevel було не меншим за визначений поріг. Після встановлення порога остаточне оцінювання виконано на незалежній тестовій частині без додаткового коригування параметрів FIS.

Матрицю помилок наведено в Табл. 4.8.

Таблиця 4.8 – Матриця помилок FIS-моделі на незалежній тестовій вибірці

| Фактичний клас           | Визначено як нормальний | Визначено як ризиковий | Разом  |
|--------------------------|-------------------------|------------------------|--------|
| Нормальне функціонування | 7374                    | 626                    | 8000   |
| Ризиковий сценарій       | 527                     | 31 473                 | 32 000 |
| Разом                    | 7901                    | 32 099                 | 40 000 |

FIS-модель правильно визначила 31 473 ризикові та 7374 нормальні сценарії. Кількість хибнопозитивних результатів становила 626, а хибнонегативних - 527.

Наведені результати свідчать, що FIS-модель характеризується високою чутливістю до сформованих ризикових сценаріїв: частка пропущених ризикових станів становила 1,647 %. Водночас 7,825 % сценаріїв нормального функціонування було помилково віднесено до ризикового класу. Отримане співвідношення помилок свідчить про вищу чутливість моделі до ризикових станів порівняно зі здатністю розпізнавати нормальні сценарії. Для задач оцінювання ризиків інформаційної безпеки така властивість є прийнятною, оскільки наслідки пропуску потенційно небезпечного стану можуть бути суттєвішими за наслідки додаткової перевірки хибнопозитивного результату.

Розраховані за матрицею помилок показники наведено в Табл. 4.9.

Таблиця 4.9 – Результати кількісної валідації FIS-моделі

| Показник                        | Значення             |
|---------------------------------|----------------------|
| Порогове значення RiskLevel     | 3,7244               |
| Accuracy                        | 0,971175             |
| 95 % довірчий інтервал Accuracy | [0,969535; 0,972815] |
| Precision                       | 0,980498             |
| Recall                          | 0,983531             |
| F1-міра                         | 0,982012             |
| FPR                             | 0,078250             |
| Specificity                     | 0,921750             |

Загальна точність FIS-моделі становила 0,971175, а F1-міра - 0,982012. Значення Recall = 0,983531 свідчить про правильне визначення більшості ризикових сценаріїв. Значення Specificity = 0,921750 показує, що модель правильно віднесла до нормального класу 92,175 % сценаріїв нормального функціонування.

Вищий порівняно з часткою хибнонегативних результатів рівень FPR пояснюється включенням до нормального класу сценаріїв із високими значеннями AssetCriticality та AttackerCapability за одночасно низьких значень інших факторів ризику. Такі сценарії навмисно сформовано для перевірки поведінки моделі за умов часткового перетину контекстних характеристик нормального та ризикового класів.

Отримані результати підтверджують працездатність FIS-моделі та її здатність диференціювати нормальні й ризикові контекстні стани IoT-середовища на незалежній сценарній вибірці. Подальше оцінювання передбачає порівняння запропонованої FIS-моделі з базовими моделями оцінювання ризику за однакових експериментальних умов.

#### 4.4.4. Порівняння FIS-моделі з базовими моделями оцінювання ризику

Для порівняльного оцінювання використано двопараметричну детерміновану модель та семипараметричну зважену модель.

Двопараметрична детермінована модель формувала оцінку як середнє значення параметрів Likelihood та ImpactSeverity.

Семипараметрична зважена модель використовувала ті самі сім вхідних параметрів, що й FIS, але об'єднувала їх шляхом лінійної згортки з однаковими ваговими коефіцієнтами.



Для забезпечення коректності порівняння всі три моделі оцінювалися на однакових сценаріях. Поріг кожної моделі окремо визначався на спільній валідаційній вибірці за максимальним значенням F1-міри. Остаточні показники обчислювалися на одній незалежній тестовій вибірці обсягом 40 000 сценаріїв.

Результати порівняльного оцінювання наведено в таблиці 4.10.

*Таблиця 4.10 – Результати порівняння моделей оцінювання ризику*

| Модель                        | Поріг         | Accuracy        | Precision       | Recall          | F1-міра         | FPR             | Specificity     |
|-------------------------------|---------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Двопараметрична детермінована | 2,8927        | 0,947825        | 0,962835        | 0,972313        | 0,967550        | 0,150125        | 0,849875        |
| Семипараметрична зважена      | 3,7008        | 0,952500        | 0,966060        | 0,974875        | 0,970447        | 0,137000        | 0,863000        |
| <b>Запропонована FIS</b>      | <b>3,7244</b> | <b>0,971175</b> | <b>0,980498</b> | <b>0,983531</b> | <b>0,982012</b> | <b>0,078250</b> | <b>0,921750</b> |

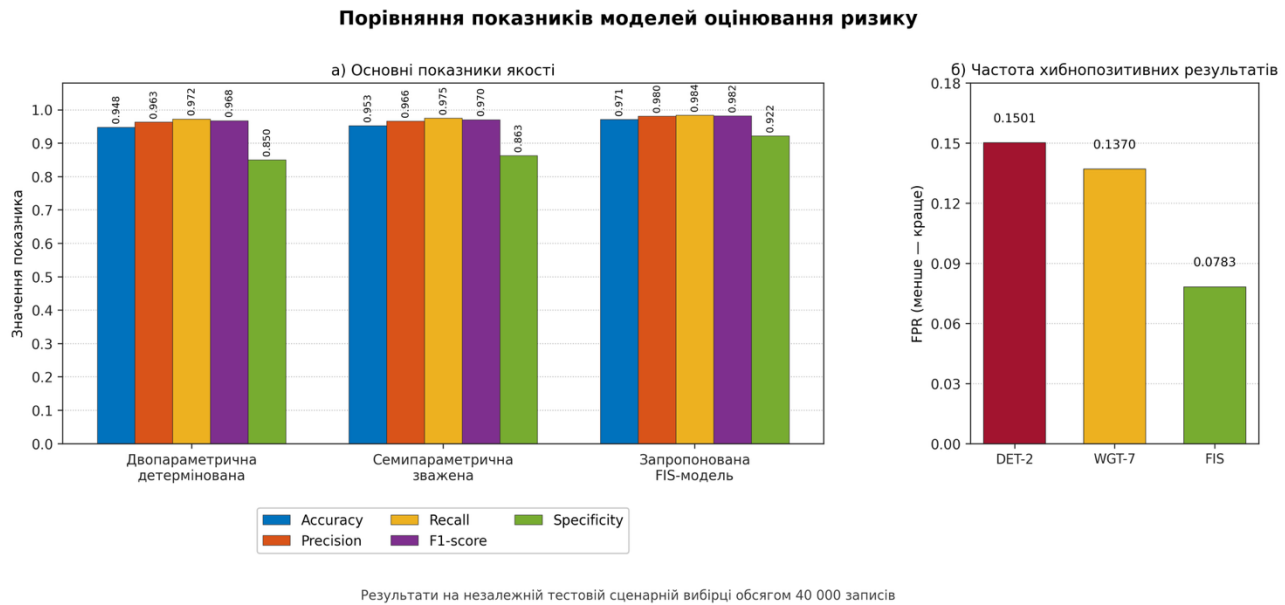
Порівняно з двопараметричною моделлю використання FIS забезпечило підвищення Accurasy на 0,023350, або 2,335 відсоткового пункта, та F1-міри на 0,014462. Значення FPR зменшилося з 0,150125 до 0,078250.

Порівняно із семипараметричною зваженою моделлю Accuracy запропонованої FIS зросла на 0,018675, F1-міра - на 0,011565, а FPR зменшився на 0,058750. Specificity зросла з 0,863000 до 0,921750.

Оскільки FIS і семипараметрична зважена модель використовували однакові вхідні параметри та оцінювалися на тих самих сценаріях, установлена різниця характеризує вплив способу агрегування параметрів. На відміну від лінійної згортки, FIS використовує функції належності та продукційні правила, що дає змогу враховувати спільну дію факторів і нелінійні переходи між рівнями ризику.

Одержані результати підтверджують перевагу FIS над дослідженими базовими моделями в межах сформованої сценарної вибірки. Водночас вони не повинні інтерпретуватися як універсальна перевага нечіткого підходу для всіх можливих IoT-середовищ, оскільки результат залежить від складу сценаріїв, параметрів функцій належності та сформованої бази правил.

Для наочного представлення результатів порівняння на Рис 4.4 наведено основні показники якості трьох моделей оцінювання ризику. Частоту хибнопозитивних результатів FPR подано окремо, оскільки зменшення цього показника відповідає підвищенню якості моделі.



*Рисунок 4.4 – Порівняння показників моделей оцінювання ризику*

#### **4.4.5. Експериментальне оцінювання впливу контекстно-ризикового профілю на формування RiskLevel**

Для кількісного оцінювання впливу контекстно-ризикового профілю на формування інтегрального показника RiskLevel проведено порівняльний експеримент із кількома конфігураціями FIS-моделі. Основне порівняння здійснювалося між запропонованою моделлю, у якій використовувалися контекстно уточнені значення вхідних параметрів, і контрольною конфігурацією без такого уточнення.

Результат інтелектуально-контекстної класифікації пристрою  $d$  відповідно до (2.1) подано у вигляді:

$$K(d) = \langle I(d), S(d), A(d), C_x(d), D_y(d) \rangle$$

де  $I(d)$  - рівень вбудованого інтелекту;  $S(d)$  - характеристики безпеки;  $A(d)$  - архітектура взаємодії;  $C_x(d)$  - контекст функціонування;  $D_y(d)$  - динамічність середовища.

Контекстно-ризиковий профіль пристрою згідно з (2.2) формується оператором семантичної конвергенції:

$$w(d) = \Psi(I(d), S(d), A(d), C_x(d), D_y(d))$$

де  $w(d)$  — контекстно-ризиковий профіль пристрою;  $\Psi$  — оператор семантичної конвергенції результатів класифікації.

У запропонованій FIS-моделі вхідний вектор формувався з урахуванням контекстно-ризикового профілю:

$$X^{\text{ctx}}(d) = \langle AC^{\text{ctx}}(d), TL^{\text{ctx}}(d), V^{\text{ctx}}(d), CAP(d), L^{\text{ctx}}(d), IS^{\text{ctx}}(d), BR(d) \rangle$$

Тут  $AC$  - критичність активу;  $TL$  - рівень загрози;  $V$  - рівень уразливості;  $CAP$  - можливості потенційного порушника;  $L$  - імовірність реалізації загрози;  $IS$  - тяжкість можливих наслідків;  $BR$  - ризик прихованої компрометації. Контекстно-ризиковий профіль використовувався для уточнення параметрів  $AC$ ,  $TL$ ,  $V$ ,  $L$  та  $IS$ . Значення  $CAP$  і  $BR$  в усіх конфігураціях залишалися незмінними.

У контрольній конфігурації контекстну варіативність п'яти параметрів було усунуто шляхом їх одночасної фіксації на рівні 5, що відповідає центру нормалізованого універсуму  $[0; 10]$ :

$$X^0(d) = \langle 5, 5, 5, CAP(d), 5, 5, BR(d) \rangle$$

Для визначення внеску окремих параметрів додатково сформовано п'ять проміжних конфігурацій, у кожній із яких на рівні 5 по чергово фіксувався один параметр: *AssetCriticality*, *ThreatLevel*, *Vulnerability*, *Likelihood* або *ImpactSeverity*. Функції належності, база нечітких продукційних правил, механізми агрегації та дефазифікації в усіх конфігураціях залишалися незмінними. Отже, відмінності результатів характеризують вплив контекстного уточнення вхідних параметрів, а не зміну структури FIS-моделі.

Експеримент виконано на сценарній вибірці зі 100 000 записів. Структура класів, діапазони параметрів і правила формування сценаріїв відповідали умовам, визначеним у підрозділі 4.4.1. Вибірку було стратифіковано розподілено на валідаційну частину обсягом 60 000 сценаріїв і незалежну тестову частину обсягом 40 000 сценаріїв.

Порогове значення для кожної конфігурації окремо визначалося на валідаційній частині за критерієм максимізації F1-міри. Остаточне оцінювання проводилося на незалежній тестовій частині. Результати наведено в табл. 4.12.

Таблиця 4.12 — Результати порівняння запропонованої FIS-моделі з контрольними конфігураціями

| Конфігурація FIS                                          | Поріг  | Accuracy | Precision | Recall   | F1-міра  | FPR      | Specificity |
|-----------------------------------------------------------|--------|----------|-----------|----------|----------|----------|-------------|
| Запропонована FIS-модель із контекстно-ризиковим профілем | 3,7244 | 0,971175 | 0,980498  | 0,983531 | 0,982012 | 0,078250 | 0,921750    |
| Без уточнення AC                                          | 3,8198 | 0,969225 | 0,982439  | 0,979031 | 0,980732 | 0,070000 | 0,930000    |
| Без уточнення TL                                          | 3,8339 | 0,932200 | 0,964918  | 0,949781 | 0,957290 | 0,138125 | 0,861875    |
| Без уточнення V                                           | 3,8674 | 0,949675 | 0,962377  | 0,975219 | 0,968755 | 0,152500 | 0,847500    |
| Без уточнення L                                           | 3,6477 | 0,960225 | 0,968566  | 0,982156 | 0,975314 | 0,127500 | 0,872500    |
| Без уточнення IS                                          | 4,5588 | 0,952650 | 0,974559  | 0,966031 | 0,970276 | 0,100875 | 0,899125    |
| Контрольна FIS без контекстного уточнення                 | 4,0000 | 0,800000 | 0,800000  | 1,000000 | 0,888889 | 1,000000 | 0,000000    |

Порівняно з контрольною конфігурацією без контекстного уточнення запропонована FIS-модель із контекстно-ризиковим профілем забезпечила підвищення Accuracy з 0,800000 до 0,971175, тобто на 0,171175, або на 17,12 відсоткового пункту. Значення Precision зросло з 0,800000 до 0,980498, F1-міри - з 0,888889 до 0,982012, а Specificity - з 0,000000 до 0,921750.

Частота хибнопозитивних результатів зменшилася з 1,000000 до 0,078250, тобто на 0,921750, що відповідає відносному скороченню FPR на 92,18 %.

Значення Recall контрольної конфігурації становило 1,000000, оскільки після одночасної фіксації п'яти контекстно залежних параметрів усі тестові сценарії було віднесено до ризикового класу. Тому ця конфігурація не пропускала ризикових сценаріїв, однак повністю втратила здатність розпізнавати нормальні стани, що підтверджується значеннями Specificity = 0 та FPR = 1. Запропонована модель забезпечила більш збалансоване розпізнавання нормальних і ризикових сценаріїв: за Recall = 0,983531 значення Specificity досягло 0,921750.

Для оцінювання внеску окремих параметрів проаналізовано результати їх почергової фіксації на нейтральному рівні. Найістотніше зниження результативності спостерігалось за відсутності контекстного уточнення ThreatLevel, Vulnerability та ImpactSeverity. Значення F1-міри для цих

конфігурацій становило відповідно 0,957290, 0,968755 та 0,970276 порівняно з 0,982012 для запропонованої моделі.

Менший вплив за показником F1-міри встановлено для AssetCriticality та Likelihood: після усунення їх контекстного уточнення отримано відповідно 0,980732 та 0,975314. Водночас для конфігурації без уточнення AssetCriticality зафіксовано нижче значення FPR - 0,070000 проти 0,078250 для повної моделі. Це свідчить, що внесок окремого параметра доцільно оцінювати за сукупністю показників, а не лише за частотою хибнопозитивних результатів.

Одночасне усунення контекстного уточнення п'яти параметрів призвело до зниження Accuracy до 0,800000, Precision - до 0,800000, F1-міри - до 0,888889 та Specificity - до 0. За таких умов контрольна конфігурація класифікувала всі сценарії як ризикові, тому її Recall дорівнював 1,000000, а FPR - 1,000000. Отриманий результат підтверджує сукупний вплив контекстно-ризикового профілю на формування RiskLevel.

Отже, порівняно з контрольною FIS без контекстного уточнення запропонована модель підвищила Accuracy на 17,12 відсоткового пункта, Precision - на 0,180498, F1-міру - на 0,093123 і Specificity - на 0,921750. Частота хибнопозитивних результатів зменшилася на 92,18 %. Отримані результати підтверджують доцільність використання контекстно-ризикового профілю для уточнення вхідних параметрів під час формування інтегрального показника RiskLevel.

#### ***4.4.6. Дослідження впливу параметра BackdoorRisk на формування RiskLevel***

Для кількісного оцінювання впливу параметра BackdoorRisk проведено додатковий контрольний експеримент на сформованій вибірці контекстно-ризикових сценаріїв. Метою експерименту було визначення зміни інтегрального показника RiskLevel та показників якості FIS-моделі за умови усунення сценарної варіативності BackdoorRisk.

У повній конфігурації FIS значення BackdoorRisk задавалося відповідно до характеристик кожного сформованого сценарію. У контрольній конфігурації значення цього параметра для всіх сценаріїв фіксувалося на рівні 5, що

відповідає центру нормалізованого універсуму  $[0; 10]$ . Значення інших шести вхідних параметрів, структура функцій належності та база нечітких продукційних правил залишалися незмінними.

Фіксація BackdoorRisk на центральному рівні використана замість установлення його значення на нижній межі універсуму. Значення BackdoorRisk = 0 характеризує відсутність або мінімальний рівень ризику прихованої компрометації, а не виключення інформаційного впливу цього параметра. Використання постійного центрального значення усуває відмінності BackdoorRisk між сценаріями та дає змогу оцінити вплив його сценарної варіативності на результат нечіткого логічного виведення.

Для повної та контрольної конфігурацій порогові значення окремо визначалися на спільній валідаційній вибірці за критерієм максимізації F1-міри. Остаточне оцінювання проводилося на одній незалежній тестовій вибірці обсягом 40 000 сценаріїв, з яких 8000 відповідали нормальному функціонуванню, а 32 000 - ризиковим станам. Така організація експерименту забезпечила однакові умови порівняння двох конфігурацій FIS.

Результати контрольного експерименту наведено в Табл. 4.13.

*Таблиця 4.13 – Результати оцінювання впливу параметра BackdoorRisk*

| Конфігурація FIS                                | Попіг  | Accuracy | Precision | Recall   | F1-міра  | FPR      | Specificity |
|-------------------------------------------------|--------|----------|-----------|----------|----------|----------|-------------|
| Повна FIS зі сценарними значеннями BackdoorRisk | 3,7244 | 0,971175 | 0,980498  | 0,983531 | 0,982012 | 0,078250 | 0,921750    |
| FIS із фіксованим BackdoorRisk = 5              | 3,8296 | 0,968300 | 0,977324  | 0,983188 | 0,980247 | 0,091250 | 0,908750    |

Фіксація BackdoorRisk на центральному рівні спричинила зменшення Accuracy з 0,971175 до 0,968300, F1-міри - з 0,982012 до 0,980247, а Specificity - з 0,921750 до 0,908750. Водночас значення FPR збільшилося з 0,078250 до 0,091250. Значення Recall змінилося несуттєво - з 0,983531 до 0,983188.

Додатково виконано попарне порівняння значень RiskLevel, отриманих повною та контрольною конфігураціями для тих самих тестових сценаріїв. Середня абсолютна зміна RiskLevel становила 0,1482, а максимальна абсолютна зміна - 1,8532. Зміна підсумкової категорії ризику спостерігалася у 7,7025 % тестових сценаріїв.

Отримані результати підтверджують, що використання індивідуальних сценарних значень BackdoorRisk здійснює вимірюваний вплив на формування інтегрального показника RiskLevel. У межах сформованої сценарної вибірки врахування варіативності BackdoorRisk забезпечило незначне підвищення загальної точності та F1-міри, а також зменшення частоти хибнопозитивних результатів.

Водночас установлена зміна показників характеризує лише досліджену сценарну вибірку та сформовану базу нечітких продукційних правил. Результати експерименту не підтверджують автоматичного визначення BackdoorRisk за первинними мережевими, поведінковими або криптографічними індикаторами. У проведеному дослідженні BackdoorRisk розглядався як попередньо сформований числовий параметр, що надходить на вхід FIS-моделі.

#### **4.5. Оцінювання обчислювальної ефективності та стійкості розроблених методів і моделей**

Після експериментального оцінювання якості класифікації мережових подій та валідації методу контекстно-адаптивного оцінювання ризиків проведено дослідження обчислювальних характеристик і стійкості їх програмної реалізації. Метою цього етапу є визначення часових витрат безпосереднього інференсу, характеру зміни часу оброблення зі збільшенням обсягу вхідних даних, а також оцінювання працездатності програмної реалізації за часткової неповноти вхідних параметрів.

Оцінювання виконано за трьома напрямками: вимірювання часу формування результату окремими програмними компонентами, дослідження масштабованості зі збільшенням кількості модельованих IoT-вузлів та аналіз впливу неповноти вхідних даних на формування показника RiskLevel. Отримані результати характеризують конкретну програмну реалізацію та умови проведення експерименту, тому не розглядаються як апаратно-незалежні оцінки обчислювальної складності розроблених методів.

##### ***4.5.1. Аналіз часових характеристик програмної реалізації***

Для оцінювання часових характеристик програмної реалізації виміряно тривалість безпосереднього логічного виведення (інференсу) FIS-моделі, Random Forest та SVM. Етапи завантаження моделей, попереднього оброблення

даних, нормалізації ознак і навчання класифікаторів під час вимірювання не враховувалися.

Перед початком експерименту здійснювався програмний прогрів моделей. Для кожної програмної реалізації формувався пакет із 1000 вхідних записів відповідної структури, який оброблявся протягом 100 повторних запусків. За результатами вимірювань визначалися середній час, медіана та 95-й процентиль тривалості інференсу в перерахунку на один запис.

Експеримент виконано в середовищі MATLAB Online. Отримані результати наведено в Табл. 4.14.

*Таблиця 4.14 – Часові характеристики інференсу досліджуваних моделей*

| Метод                        | Середній час,<br>мс/запис | Медіана,<br>мс/запис | p95,<br>мс/запис |
|------------------------------|---------------------------|----------------------|------------------|
| Запропонована FIS-<br>модель | 0,0543                    | 0,0535               | 0,0614           |
| Random Forest                | 0,1939                    | 0,1913               | 0,2129           |
| SVM                          | 0,0326                    | 0,0321               | 0,0406           |

Як свідчать результати Табл. 4.14, середній час формування інтегральної оцінки RiskLevel за допомогою FIS-моделі становив 0,0543 мс на один сценарій. Медіана часу інференсу дорівнювала 0,0535 мс, а 95-й процентиль - 0,0614 мс. Невелика різниця між середнім значенням і медіаною свідчить про відсутність значних одиничних затримок у межах проведених повторних запусків.

Середній час інференсу Random Forest становив 0,1939 мс на один запис, що перевищує відповідний показник FIS-моделі. Для SVM отримано найменший середній час - 0,0326 мс на один запис. Значення 95-го процентилля для всіх досліджуваних реалізацій незначно перевищували відповідні середні значення, що вказує на відносну стабільність часу виконання в межах експерименту.

Наведені часові показники не слід розглядати як пряме порівняння алгоритмічної ефективності FIS, Random Forest і SVM, оскільки ці моделі виконують різні функції та використовують вхідні дані різної структури. Методи Random Forest і SVM здійснюють класифікацію мережевих подій, тоді як FIS-модель формує інтегральний показник ризику за сімома контекстно-ризиковими параметрами.

Отримані результати характеризують конкретні програмні реалізації та умови виконання в MATLAB Online. Вони не є апаратно-незалежною оцінкою



обчислювальної складності моделей. Водночас час інференсу FIS-моделі підтверджує можливість оперативного формування показника RiskLevel після отримання й підготовки необхідних вхідних параметрів.

#### **4.5.2. Аналіз масштабованості програмної реалізації**

Для оцінювання масштабованості програмної реалізації досліджено зміну часу виконання програмного циклу зі збільшенням кількості модельованих IoT-вузлів. Кількість одночасно оброблюваних вузлів послідовно збільшувалася від 50 до 500.

На відміну від експерименту, наведеного в підпункті 4.5.1, у цьому випадку вимірювався не час безпосереднього інференсу для одного запису, а загальний час пакетного оброблення заданої кількості модельованих вузлів. Він включав формування вхідних структур, виконання передбачених програмною реалізацією операцій оброблення та формування результатів оцінювання.

Для кожної конфігурації виконувалася однакова послідовність програмних операцій і визначався середній час оброблення. Результати експерименту наведено в Табл. 4.15.

*Таблиця 4.15 – Залежність часу оброблення від кількості модельованих IoT-вузлів*

| <b>Кількість IoT-вузлів</b> | <b>Середній час оброблення, мс</b> | <b>Середній час на один вузол, мс</b> |
|-----------------------------|------------------------------------|---------------------------------------|
| 50                          | 43                                 | 0,860                                 |
| 100                         | 47                                 | 0,470                                 |
| 200                         | 52                                 | 0,260                                 |
| 500                         | 61                                 | 0,122                                 |

Як видно з Табл. 4.15, зі збільшенням кількості модельованих IoT-вузлів від 50 до 500 середній час виконання програмного циклу збільшився з 43 до 61 мс. Абсолютне збільшення становило 18 мс, а відносне - приблизно 41,9 % за десятикратного збільшення кількості вузлів.

Зменшення середнього часу в перерахунку на один вузол із 0,860 до 0,122 мс пояснюється наявністю постійних початкових витрат програмного циклу та пакетним характером оброблення. Частина службових операцій виконується один раз для всього пакета, тому зі збільшенням його розміру ці витрати розподіляються між більшою кількістю модельованих вузлів.

У межах досліджених конфігурацій збільшення часу виконання мало поступовий характер. За десятикратного збільшення кількості модельованих вузлів середній час пакетного оброблення збільшився приблизно на 41,9 %, що свідчить про відсутність різкого зростання часових витрат у дослідженому діапазоні.

Отримані результати підтверджують працездатність програмної реалізації під час пакетного оброблення від 50 до 500 модельованих IoT-вузлів. Водночас вони характеризують лише використане програмне середовище, спосіб пакетної обробки та досліджений діапазон навантаження. Тому результати не слід інтерпретувати як підтвердження необмеженої масштабованості або як апаратно-незалежну характеристику розроблених методів.

#### **4.5.3. Аналіз стійкості FIS-моделі до неповноти вхідних даних**

Для реальних IoT-середовищ характерними є тимчасова недоступність окремих джерел даних, втрата частини телеметричної інформації, неповнота журналів подій і неможливість визначення окремих контекстно-ризикових параметрів. Унаслідок цього програмна реалізація методу має забезпечувати коректне оброблення частково неповних вхідних даних.

Експеримент проведено на 10 000 контрольних комбінаціях семи вхідних параметрів: AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk. Значення параметрів формувалися в межах нормалізованого універсуму  $[0; 10]$ .

Для кожної контрольної комбінації спочатку визначалося базове значення RiskLevel за повного вхідного вектора. Після цього з вхідної матриці випадково вилучалося відповідно 5, 10, 20 і 30 % значень. Для кожного рівня неповноти вилучалася точно визначена частка із загальної кількості 70 000 значень. Випадкові маски формувалися за вкладеним принципом, тому сукупність пропусків для меншого рівня неповноти входила до сукупності пропусків наступного рівня.

Пропущені значення відновлювалися за медіаною відповідного вхідного параметра, визначеною на повній контрольній вибірці. Медіанне відновлення обрано через його меншу чутливість до граничних значень порівняно із середнім арифметичним.

Після відновлення даних для кожної комбінації повторно обчислювалося значення RiskLevel. Отриманий результат порівнювався з базовою оцінкою, сформованою за повного вхідного вектора. Для кожного рівня неповноти визначалися середня абсолютна зміна RiskLevel, максимальна абсолютна зміна RiskLevel та частка комбінацій, у яких відбувся перехід до іншої категорії ризику. Результати експерименту наведено в таблиці 4.16.

*Таблиця 4.16 – Вплив неповноти вхідних даних на результати FIS-моделі*

| <b>Частка пропущених значень</b> | <b>Середня абсолютна зміна RiskLevel</b> | <b>Максимальна зміна RiskLevel</b> | <b>Зміна категорії ризику, %</b> |
|----------------------------------|------------------------------------------|------------------------------------|----------------------------------|
| 5 %                              | 0,128                                    | 4,554                              | 5,36                             |
| 10 %                             | 0,238                                    | 5,175                              | 10,02                            |
| 20 %                             | 0,425                                    | 5,205                              | 17,97                            |
| 30 %                             | 0,577                                    | 5,335                              | 23,96                            |

Як видно з таблиці 4.16, збільшення частки пропущених значень супроводжується послідовним зростанням середньої абсолютної зміни RiskLevel. За відсутності 5 % значень середнє відхилення становило 0,128, а категорія ризику змінилася у 5,36 % контрольних комбінацій. За збільшення частки пропущених значень до 10 % середня зміна RiskLevel зросла до 0,238, а частка змінених категорій - до 10,02 %.

За відсутності 20 % значень середня абсолютна зміна RiskLevel становила 0,425, а перехід до іншої категорії ризику відбувся у 17,97 % комбінацій. За максимального досліджуваного рівня неповноти 30 % середня зміна RiskLevel досягла 0,577, а категорія ризику змінилася у 23,96 % випадків.

Максимальні відхилення RiskLevel істотно перевищували середні значення. Це свідчить про наявність окремих комбінацій, особливо чутливих до втрати певних вхідних параметрів. Така поведінка пояснюється нелінійним характером нечіткого логічного виведення: відновлення окремого значення медіаною може змінити ступені належності, склад активованих продукційних правил і підсумкову категорію ризику.

Отримані результати підтверджують, що медіанне відновлення забезпечує технічну можливість формування RiskLevel за часткової неповноти вхідного вектора. Водночас зі збільшенням частки пропущених значень відхилення від оцінки, отриманої за повними даними, закономірно зростає. Тому результати,

сформовані за значної неповноти вхідних параметрів, доцільно супроводжувати ознакою зниженої достовірності та рекомендацією щодо уточнення відсутніх даних.

Наведені показники характеризують рівномірно сформовані контрольні комбінації в межах універсуму  $[0; 10]$  і не є результатами перевірки на реальних потоках даних IoT-пристроїв. Дослідження впливу структурованих пропусків і застосування альтернативних методів відновлення даних становить напрям подальшого розвитку програмної реалізації.

#### ***4.5.4. Переваги та обмеження розроблених методів і моделей***

За результатами програмної реалізації та експериментальної перевірки визначено основні переваги й обмеження розробленої моделі побудови контекстно-ризикового профілю IoT-пристрою та удосконаленого методу оцінювання ризиків інформаційної безпеки IoT-середовищ.

До основних переваг належать:

1. Комплексне врахування факторів ризику. FIS-модель використовує сім взаємопов'язаних параметрів: AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk. Це забезпечує ширше представлення стану безпеки порівняно з моделями, що використовують лише імовірність реалізації загрози та тяжкість потенційних наслідків.
2. Врахування контексту функціонування IoT-пристрою. Використання контекстно-ризикового профілю дає змогу враховувати функціональну роль, критичність, характеристики безпеки та умови експлуатації пристрою під час формування вхідних параметрів оцінювання ризику.
3. Врахування ризику прихованої компрометації. Введення параметра BackdoorRisk розширює склад факторів ризику та дає змогу включати до інтегральної оцінки попередньо сформовану характеристику ризику прихованої компрометації. За результатами декомпозиційного експерименту виключення цього параметра

спричинило зміну категорії ризику у 11,96 % контрольних комбінацій.

4. Урахування невизначеності вхідних параметрів. Застосування функцій належності забезпечує плавні переходи між низькими, середніми та високими рівнями факторів ризику й усуває необхідність використання виключно жорстких порогових залежностей.
5. Нелінійне агрегування параметрів. На відміну від семипараметричної зваженої моделі, FIS ураховує не лише значення окремих параметрів, а й характер їх поєднання за допомогою бази нечітких продукційних правил. На незалежній тестовій сценарній вибірці обсягом 40 000 сценаріїв запропонована FIS-модель забезпечила  $Assurasy = 0,971175$ ,  $F1\text{-}міру = 0,982012$  та  $FPR = 0,078250$ . Для семипараметричної зваженої моделі відповідні показники становили 0,952500, 0,970447 та 0,137000. Отримані результати підтверджують перевагу нелінійного нечіткого агрегування над лінійною згорткою з однаковими ваговими коефіцієнтами в межах сформованої сценарної вибірки.
6. Інтерпретованість результатів. Формування RiskLevel можна простежити через ступені належності вхідних значень, активовані правила та результати дефазифікації. Це забезпечує можливість змістового пояснення сформованої оцінки ризику.
7. Можливість оброблення неповних даних. Застосування медіанного відновлення забезпечило формування RiskLevel за часткової відсутності вхідних значень. За 5 % пропусків середня абсолютна зміна RiskLevel становила 0,128, а зміна категорії ризику відбулася у 5,36 % контрольних комбінацій.

Разом із визначеними перевагами розроблені методи й моделі мають низку обмежень.

1. Експертне формування функцій належності та бази правил. Параметри функцій належності й продукційні правила визначено на основі експертних оцінок і змістової інтерпретації факторів ризику.

Тому перенесення моделі до іншого IoT-середовища може потребувати додаткового налаштування.

2. Попереднє формування BackdoorRisk. FIS-модель ураховує задане значення BackdoorRisk, але не виконує автоматичного виявлення бекдорів або прихованої компрометації за первинними мережевими чи криптографічними даними.
3. Якість оцінювання ризику залежить від коректності визначення, нормалізації та масштабування вхідних параметрів. Помилки на етапі підготовки даних можуть негативно впливати на результати нечіткого логічного виведення.
4. Кількісну валідацію FIS-моделі проведено на сформованих контекстно-ризикових сценаріях. Тому подальшого дослідження потребує її застосування на тривалих послідовностях даних, отриманих під час функціонування реальних гетерогенних IoT-середовищ.
5. Проведена перевірка часових характеристик відображає особливості конкретної програмної реалізації в середовищі MATLAB Online і не є апаратно-незалежною оцінкою обчислювальної складності моделі.

Отже, розроблені методи та моделі забезпечують інтерпретоване контекстно-адаптивне оцінювання ризиків з урахуванням розширеної сукупності факторів і невизначеності вхідних параметрів. Водночас їх практичне впровадження потребує налаштування для конкретного IoT-середовища, формалізованого визначення вхідних параметрів та подальшої перевірки на реальних потоках даних і в умовах тривалої експлуатації.

## Висновки розділу 4

У четвертому розділі здійснено програмну реалізацію та експериментальну перевірку ключових компонентів запропонованої інформаційної технології, зокрема ризикового FIS-модуля й окремого контуру класифікації мережевих подій. Проведені експерименти дали змогу перевірити працездатність програмного модуля нечіткого оцінювання ризиків та оцінити вплив контекстно-ризикового профілю і показника BackdoorRisk на визначення рівня ризику інформаційної безпеки IoT-середовищ.

За результатами проведеного дослідження отримано такі основні результати:

1. У середовищі MATLAB із використанням Fuzzy Logic Toolbox реалізовано FIS-модель типу Мамдані, яка містить сім вхідних параметрів, вихідну змінну RiskLevel та базу із 40 унікальних продукційних правил. Функціональна перевірка спрацьовування правил, поверхонь логічного виведення та покомпонентної монотонності для опорної конфігурації підтвердила коректність програмної реалізації моделі.
2. Проведено експериментальне оцінювання методів класифікації мережевих подій на уніфікованій вибірці, сформованій на основі відкритих наборів даних VoT-IoT, TON\_IoT та Edge-IIoTset. Вибірка містила 20 527 записів, із яких 4105 утворювали незалежну тестову частину. Найвище точкове значення Accuracy отримано для XGBoost - 0,9481. Цей метод також забезпечив Precision = 0,9661, F1-miry = 0,9374 та найнижче значення FPR = 0,0238. Найвище значення Recall продемонстрував Random Forest - 0,9246.
3. Функціональна перевірка FIS-моделі на контрольних сценаріях підтвердила її здатність диференціювати стани з різною сукупністю факторів ризику. Для сценарію мережевої розвідки отримано RiskLevel = 3,4633, для DoS/DDoS-атаки - 6,6807, для витоку даних - 6,5360, а для прихованої компрометації - 7,4453. Отримані значення відповідають установленим помірній, підвищеній та критичній категоріям ризику.
4. Кількісну валідацію FIS-моделі виконано на сценарній вибірці зі 100 000 записів, стратифіковано розподілений на валідаційну та незалежну тестову

частини у співвідношенні 60/40. На тестовій частині обсягом 40 000 сценаріїв за порогового значення RiskLevel = 3,7244 отримано Accuracy = 0,971175, Precision = 0,980498, Recall = 0,983531, F1-міру = 0,982012 та Specificity = 0,921750. Частка хибнопозитивних результатів становила 0,078250. Значення Accuracy перебувало в межах 95 % довірчого інтервалу [0,969535; 0,972815].

5. Порівняльне оцінювання FIS-моделі, двопараметричної детермінованої та семипараметричної зваженої моделей проведено на однаковій незалежній тестовій вибірці з 40 000 сценаріїв. Запропонована FIS-модель забезпечила Accuracy = 0,971175, F1-міру = 0,982012 та FPR = 0,078250. Для семипараметричної зваженої моделі відповідні показники становили 0,952500, 0,970447 та 0,137000. Отже, Accuracy FIS-моделі була вищою на 0,018675, F1-міра - на 0,011565, а FPR - нижчим на 0,058750. Оскільки обидві моделі використовували однакові сім вхідних параметрів, отримані результати характеризують перевагу нечіткого логічного виведення над лінійним агрегуванням з однаковими ваговими коефіцієнтами в межах сформованої сценарної вибірки.
6. Проведено експериментальне оцінювання впливу контекстно-ризикового профілю на формування RiskLevel. Запропонована FIS-модель із контекстним уточненням параметрів AssetCriticality, ThreatLevel, Vulnerability, Likelihood та ImpactSeverity забезпечила Accuracy = 0,971175, Precision = 0,980498, Recall = 0,983531, F1-міру = 0,982012, FPR = 0,078250 і Specificity = 0,921750. Порівняно з контрольною конфігурацією Accuracy запропонованої моделі була вищою на 0,171175, або на 17,12 відсоткового пункту, Precision - на 0,180498, F1-міра - на 0,093123, а Specificity - на 0,921750. Відносне зменшення FPR становило 92,18 %. За результатами почергового усунення контекстного уточнення окремих параметрів найбільше зниження F1-міри встановлено для ThreatLevel, Vulnerability та ImpactSeverity. Отримані результати підтверджують вимірюваний вплив контекстно-ризикового профілю на результативність формування RiskLevel у межах сформованої сценарної вибірки.



7. Досліджено вплив сценарної варіативності BackdoorRisk на формування RiskLevel. У контрольній конфігурації значення BackdoorRisk для всіх сценаріїв фіксувалося на центральному рівні 5 за незмінних значень інших шести вхідних параметрів. Порівняно з повною FIS значення Accuracy зменшилося з 0,971175 до 0,968300, F1-міри — з 0,982012 до 0,980247, а FPR збільшилося з 0,078250 до 0,091250. Середня абсолютна зміна RiskLevel становила 0,1482, максимальна — 1,8532, а зміна категорії ризику спостерігалася у 7,7025 % тестових сценаріїв. Отримані результати підтвердили вимірюваний вплив сценарних значень BackdoorRisk на формування інтегральної оцінки ризику, але не характеризують здатність системи автоматично визначати цей параметр за первинними мережевими або криптографічними індикаторами.
8. Середній час безпосереднього логічного виведення FIS-моделі становив 0,0543 мс на один сценарій, медіана - 0,0535 мс, а 95-й перцентиль - 0,0614 мс. Зі збільшенням кількості модельованих IoT-вузлів від 50 до 500 середній час пакетного оброблення збільшився з 43 до 61 мс, тобто приблизно на 41,9 % за десятикратного зростання кількості вузлів.
9. Дослідження неповноти вхідних даних показало, що медіанне відновлення забезпечує можливість формування RiskLevel за часткової відсутності параметрів, однак зі збільшенням частки пропусків відхилення результату зростає. За 5 % пропусків середня абсолютна зміна RiskLevel становила 0,128, а категорія ризику змінилася у 5,36 % комбінацій. За 30 % пропусків ці показники збільшилися відповідно до 0,577 та 23,96 %.

Отримані результати підтвердили працездатність програмного модуля нечіткого оцінювання ризиків та показали вплив контекстного уточнення вхідних параметрів і показника BackdoorRisk на значення RiskLevel.

Кількісну перевірку FIS-моделі проведено на програмно сформованих контекстно-ризикових сценаріях; її роботу на реальних потоках даних IoT-середовища не перевіряли. Подальші дослідження доцільно спрямувати на апробацію технології в реальних IoT-інфраструктурах, автоматизоване визначення семи вхідних параметрів та оцінювання результатів за різних умов експлуатації.

## ВИСНОВКИ

У дисертаційній роботі розв'язано актуальне наукове завдання розроблення моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ у процесі аудиту. На основі розробленої моделі й удосконаленого методу створено інформаційну технологію їх узгодженого застосування.

У результаті проведених досліджень отримано такі основні наукові та практичні результати.

1. Проаналізовано сучасні методи виявлення вразливостей, класифікації мережевих подій, оцінювання ризиків та аудиту інформаційної безпеки IoT-середовищ. З'ясовано, що наявні підходи не повною мірою враховують функціональний контекст пристроїв, взаємозалежність факторів ризику, динамічні зміни середовища, а також неповноту й невизначеність даних. Виявлені обмеження визначили потребу в розробленні методів і моделей, здатних адаптувати процес оцінювання ризиків до умов функціонування конкретного IoT-середовища.
2. Вперше розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Модель передбачає врахування п'яти критеріїв: рівня вбудованого інтелекту пристрою, характеристик його безпеки, архітектури взаємодії, функціонального контексту й динамічності середовища. Поєднання цих характеристик дає змогу узгоджувати різномірні результати класифікації без втрати їхнього змістового значення. На основі отриманих даних формується контекстно-ризиковий профіль IoT-пристрою, який надалі використовується для визначення та контекстної інтерпретації параметрів оцінювання ризику.
3. Удосконалено метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ, побудований на основі

нечіткого логічного виведення типу Мамдані. Під час оцінювання спільно враховуються критичність активу, рівень загрози, рівень вразливості, можливості потенційного порушника, імовірність реалізації загрози, тяжкість її наслідків і попередньо сформований показник BackdoorRisk. Застосування нечіткого виведення дає можливість відтворювати нелінійні взаємозв'язки між зазначеними параметрами та визначати інтегральний показник RiskLevel за неповних або невизначених вхідних даних. Водночас результат оцінювання залишається доступним для змістової інтерпретації.

4. Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ. Він передбачає використання контекстно-ризикового профілю пристрою разом із даними про поточний стан безпеки для формування вхідних параметрів нечіткого оцінювання. На основі цього підходу створено інформаційну технологію, визначено її багаторівневу архітектуру, склад функціональних компонентів, інформаційні потоки та послідовність їх взаємодії в процесі аудиту. Технологія забезпечує узгоджене застосування моделі формування профілю й методу оцінювання ризиків, а також передбачає повторне визначення рівня ризику в разі зміни характеристик пристрою або стану середовища.
5. Розроблено програмний прототип ризикового модуля в середовищі MATLAB із використанням Fuzzy Logic Toolbox. Реалізована FIS-модель типу Мамдані охоплює сім вхідних змінних, вихідну змінну RiskLevel та базу з 40 унікальних продукційних правил. Коректність реалізації перевірено шляхом аналізу спрацьовування правил, поверхонь нечіткого виведення та покомпонентної монотонності моделі для опорної конфігурації.
6. Проведено експериментальне оцінювання методів класифікації мережеских подій на уніфікованій вибірці, сформованій із даних BoT-IoT, TON\_IoT та Edge-IIoTset. На незалежній тестовій частині, що містила 4105 записів, метод XGBoost продемонстрував Accuracy = 0,9481, F1-міру = 0,9374 та FPR = 0,0238. Окремо виконано перевірку

FIS-моделі на незалежній вибірці з 40 000 контекстно-ризикових сценаріїв. Для цієї вибірки отримано Accuracy = 0,971175, F1-міру = 0,982012 та FPR = 0,078250. Порівняно із семипараметричною зваженою моделлю значення Accuracy зросло на 0,018675, F1-міри - на 0,011565, тоді як FPR зменшився на 0,058750.

7. Проведено експериментальне оцінювання впливу контекстно-ризикового профілю на формування RiskLevel. Запропонована FIS-модель із контекстним уточненням параметрів AssetCriticality, ThreatLevel, Vulnerability, Likelihood та ImpactSeverity забезпечила Accuracy = 0,971175, Precision = 0,980498, Recall = 0,983531, F1-міру = 0,982012, FPR = 0,078250 і Specificity = 0,921750. Порівняно з контрольною конфігурацією Accuracy запропонованої моделі була вищою на 0,171175, або на 17,12 відсоткового пункта, Precision - на 0,180498, F1-міра - на 0,093123, а Specificity - на 0,921750. Відносне зменшення FPR становило 92,18 %. За результатами почергового усунення контекстного уточнення окремих параметрів найбільше зниження F1-міри встановлено для ThreatLevel, Vulnerability та ImpactSeverity. Отримані результати підтверджують вимірюваний вплив контекстно-ризикового профілю на результативність формування RiskLevel у межах сформованої сценарної вибірки.
8. Експериментально встановлено вплив сценарної варіативності BackdoorRisk на значення RiskLevel. У разі фіксації BackdoorRisk на рівні 5 категорія ризику змінилася у 7,7025 % тестових сценаріїв, а FPR збільшився з 0,078250 до 0,091250. Середній час виконання нечіткого логічного виведення становив 0,0543 мс для одного запису. Додатково досліджено роботу моделі за наявності пропущених даних. За частки пропущених значень 30 % та застосування медіанного заміщення середня абсолютна зміна RiskLevel дорівнювала 0,577, а зміну категорії ризику зафіксовано у 23,96 % контрольних комбінацій.

Отримані результати підтверджують виконання поставлених завдань. Розроблена модель забезпечує формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Удосконалений метод використовує профіль разом із даними про поточний стан безпеки для уточнення залежних від контексту вхідних параметрів і враховує попередньо сформований показник BackdoorRisk як окремий вхід FIS.

Експериментальні результати засвідчили перевагу запропонованої FIS-моделі над семипараметричною зваженою моделлю в досліджених сценаріях, а також вплив контекстного уточнення параметрів і зміни BackdoorRisk на показник RiskLevel.

Створена інформаційна технологія визначає порядок узгодженого застосування моделі й методу під час аудиту IoT-середовищ. Отримані оцінки ризику можуть використовуватися для обґрунтування пріоритетності заходів захисту.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1]. IoT Analytics, *State of IoT Summer 2024: Number of connected IoT devices growing 13% to 18.8 billion globally, with forecast to reach ~40 billion by 2030*. [Online]. Available: <https://iot-analytics.com/number-connected-iot-devices/>
- [2]. TechJury, *How Many IoT Devices Are There in 2025?* [Online]. Available: <https://techjury.net/industry-analysis/iot/>
- [3]. Article “Industrial IoT, Cyber Threats, and Standards Landscape”, L. L. Dhirani et al., *PMC / NCBI*, 2021 — аналіз ризиків та загроз для промислових IoT-систем. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8200965/>
- [4]. S. Madanian et al., *Health IoT Threats: Survey of Risks and Vulnerabilities*, MDPI, 2024 - про загрози в IoT в медичній сфері. [Online]. Available: <https://www.mdpi.com/1999-5903/16/11/389>
- [5]. M. Waqdan, *Security risk assessment in IoT environments: A taxonomy*, ScienceDirect, 2025 — методологія оцінювання ризику для IoT-середовищ. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404825001452>
- [6]. SO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on information security risk management*. International Organization for Standardization, Geneva, 2022. [Online]. Available: <https://www.iso.org/standard/80585.html>
- [7]. NIST, *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, 2012. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-30r1>
- [8]. ENISA, *ENISA Threat Landscape 2022*. European Union Agency for Cybersecurity, Heraklion, 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
- [9]. S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, *Computer Networks*, vol. 76, pp. 146–164, 2015. [Online]. Available: <https://doi.org/10.1016/j.comnet.2014.11.008>
- [10]. Z. Yan, P. Zhang, A. V. Vasilakos, “A survey on trust management for Internet of Things”, *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014. [Online]. Available: <https://doi.org/10.1016/j.jnca.2014.01.014>
- [11]. European Union Agency for Cybersecurity. *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*. Heraklion: ENISA, 2017. URL: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

- [12]. Puche Rondon L., Babun L., Aris A., Akkaya K., Uluagac A. S. Survey on Enterprise Internet-of-Things Systems (E-IoT): A Security Perspective // *Ad Hoc Networks*. 2021. Vol. 122. Article 102728. DOI: 10.1016/j.adhoc.2021.102728.
- [13]. Bonomi F., Milito R., Zhu J., Addepalli S. Fog Computing and Its Role in the Internet of Things // *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (MCC'12)*. New York : ACM, 2012. P. 13–16. DOI: 10.1145/2342509.2342513.
- [14]. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges // *IEEE Internet of Things Journal*. 2016. Vol. 3, No. 5. P. 637–646. DOI: 10.1109/JIOT.2016.2579198.
- [15]. Satyanarayanan M., Bahl P., Caceres R., Davies N. The Case for VM-Based Cloudlets in Mobile Computing // *IEEE Pervasive Computing*. 2009. Vol. 8, No. 4. P. 14–23. DOI: 10.1109/MPRV.2009.82.
- [16]. Yousefpour A., Fung C., Nguyen T. et al. All One Needs to Know about Fog Computing and Related Edge Computing Paradigms: A Complete Survey // *Journal of Systems Architecture*. 2019. Vol. 98. P. 289–330. DOI: 10.1016/j.sysarc.2019.02.009
- [17]. Babun L., Denney K., Celik Z. B., McDaniel P., Uluagac A. S. *A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives* // *Computer Networks*. 2021. Vol. 192. Article 108040. DOI: 10.1016/j.comnet.2021.108040.
- [18]. Kong L., Tan J., Huang J., Chen G., Wang S., Jin X., Zeng P., Khan M., Das S. K. *Edge-Computing-Driven Internet of Things: A Survey* // *ACM Computing Surveys*. 2022. Vol. 55, No. 8. Article 174. DOI: 10.1145/3555308.
- [19]. Fazeldehkordi E., Grønli T.-M. *A Survey of Security Architectures for Edge Computing-Based IoT* // *IoT*. 2022. Vol. 3, No. 3. P. 332–365. DOI: 10.3390/iot3030019.
- [20]. Adam M., Hammoudeh M., Alrawashdeh R., Alsulaimy B. *A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems* // *IEEE Access*. 2024. Vol. 12. P. 57128–57149. DOI: 10.1109/ACCESS.2024.3382709.
- [21]. Mbarek A., Abbes T., Hanachi C., Ben Abdallah H. *Automatic Vulnerability Detection in Embedded Devices and Firmware: Survey and Layered Taxonomies* // *ACM Computing Surveys*. 2022. Vol. 54, No. 2. Article 36. DOI: 10.1145/3432893.
- [22]. Nadir I., Mahmood H., Asadullah G. *A Taxonomy of IoT Firmware Security and Principal Firmware Analysis Techniques* // *International Journal of Critical Infrastructure Protection*. 2022. Vol. 38. Article 100552. DOI: 10.1016/j.ijcip.2022.100552.
- [23]. Ul Haq S., Singh Y., Sharma A., Gupta R., Gupta D. et al. *A Survey on IoT and Embedded Device Firmware Security: Architecture, Extraction*

- Techniques, and Vulnerability Analysis Frameworks // Discover Internet of Things*. 2023. Vol. 3. Article 17. DOI: 10.1007/s43926-023-00045-2.
- [24]. Feng X. T., Zhu X. G., Han Q.-L., Zhou W., Wen S., Xiang Y. *Detecting Vulnerability on IoT Device Firmware: A Survey // IEEE/CAA Journal of Automatica Sinica*. 2023. Vol. 10, No. 1. P. 25–41. DOI: 10.1109/JAS.2022.105860.
- [25]. Delaitre A., Stivalet B., Black P. E., Okun V., Ribeiro A., Cohen T. S. SATE V Report: Ten Years of Static Analysis Tool Expositions. NIST Special Publication 500-326. Gaithersburg: National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.SP.500-326.
- [26]. Wright C., Moeglein W. A., Bagchi S., Kulkarni M., Clements A. A. Challenges in Firmware Re-Hosting, Emulation, and Analysis. *ACM Computing Surveys*. 2021. Vol. 54, No. 1. Art. 5. P. 1–36. DOI: 10.1145/3423167.
- [27]. Costin A., Zaddach J., Francillon A., Balzarotti D. A Large-Scale Analysis of the Security of Embedded Firmwares. *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*. San Diego: USENIX Association, 2014. P. 95–110. ISBN 978-1-931971-15-7.
- [28]. Bakhshi T., Ghita B., Kuzminykh I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors*. 2024. Vol. 24, No. 2. Art. 708. DOI: 10.3390/s24020708.
- [29]. Zhou X., Wang P., Zhou L., Xun P., Lu K. A Survey of the Security Analysis of Embedded Devices. *Sensors*. 2023. Vol. 23, No. 22. Art. 9221. DOI: 10.3390/s23229221.
- [30]. National Institute of Standards and Technology. *NISTIR 8259 Series* [Electronic resource]. Gaithersburg, MD : NIST. URL: <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>
- [31]. ISO. *ISO/IEC 27000 family — Information security management systems*. Geneva : International Organization for Standardization. URL: <https://www.iso.org/isoiec-27001-information-security.html>
- [32]. International Electrotechnical Commission. *IEC 62443 series – Security for industrial automation and control systems (IACS)*. Geneva : IEC. URL: <https://www.iec.ch/standards-development/iec-62443>
- [33]. European Telecommunications Standards Institute. *ETSI EN 303 645 V2.1.1 (2020-06). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. Sophia Antipolis : ETSI, 2020.
- [34]. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*. Luxembourg : Publications Office of the European Union, 2023. 134 p. DOI: 10.2824/782573.
- [35]. Caralli R. A., Stevens J. F., Young L. R., Wilson W. R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Pittsburgh, PA : Carnegie Mellon University, Software Engineering Institute, 2007. 56 p. CMU/SEI-2007-TR-012. DOI: 10.1184/R1/6574790.v1.



- [36]. Agence nationale de la sécurité des systèmes d'information (ANSSI). *EBIOS Risk Manager: Le guide*. Paris : ANSSI, 2024. URL: <https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm>
- [37]. Shostack A. *Threat Modeling: Designing for Security*. Indianapolis : Wiley, 2014. 408 p. ISBN 978-1-118-80999-0.
- [38]. UcedaVélez T., Morana M. M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (PASTA)*. Hoboken : John Wiley & Sons, 2015. 624 p. ISBN 978-1-118-96971-7.
- [39]. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. 2nd ed. Indianapolis : Wiley Publishing, 2015. 432 p. ISBN 978-1-119-09729-7.
- [40]. Almseidin M., Alzubi J. A., Kovács L. та ін. Artificial Intelligence and Machine Learning for Cybersecurity in IoT: A Survey // *Sensors*. 2022. Vol. 22, No. 12. Art. 4414. DOI: 10.3390/s22124414.
- [41]. Sarker I. H. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions // *SN Computer Science*. 2024. Vol. 5. Art. 146. DOI: 10.1007/s42979-024-02638-9.
- [42]. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, No. 2. P. 1153–1176. DOI: 10.1109/COMST.2015.2494502.
- [43]. Ahanger T. A., Aljumah A., Atiquzzaman M. State-of-the-art Survey of Artificial Intelligent Techniques for IoT Security // *Computer Networks*. 2022. Vol. 206. Art. 108771. DOI: 10.1016/j.comnet.2022.108771.
- [44]. Lansky J., Ali S., Mohammadi M., Majeed M. K., Karim S. H. T., Rashidi S., Hosseinzadeh M., Rahmani A. M. Deep Learning-Based Intrusion Detection Systems: A Systematic Review. *IEEE Access*. 2021. Vol. 9. P. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.
- [45]. Nguyen D. C., Ding M., Pathirana P. N., Seneviratne A., Li J., Niyato D. Federated Learning for Internet of Things: A Comprehensive Survey // *IEEE Communications Surveys & Tutorials*. 2021. Vol. 23, No. 3. P. 1622–1658. DOI: 10.1109/COMST.2021.3075439.
- [46]. Hanif S., Ilyas M., Urooj S., Kim H. Explainable Artificial Intelligence for Cybersecurity: A Systematic Literature Review // *IEEE Access*. 2024. Vol. 12. P. 24792–24824. DOI: 10.1109/ACCESS.2024.3362680.
- [47]. Hasanov I., Virtanen S., Hakkala A., Isoaho J. Application of Large Language Models in Cybersecurity: A Systematic Literature Review // *IEEE Access*. 2024. Vol. 12. P. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.
- [48]. Mishra N., Pandya S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review // *IEEE Access*. 2021. Vol. 9. P. 59353–59377. DOI: 10.1109/ACCESS.2021.3073408.
- [49]. Dritsas E., Trigka M. A Survey on Cybersecurity in IoT // *Future Internet*. 2025. Vol. 17, No. 1. Art. 30. DOI: 10.3390/fi17010030.

- [50]. Kumari N. S., Vimala H. S., Pruthvi C. N., Shreyas J. Holistic Survey on Security in IoT Application Layer: Attacks, Protocols, and Applications // IEEE Access. 2024. Vol. 12. P. 186957–187014. DOI: 10.1109/ACCESS.2024.3462170.
- [51]. Kaur S., Singh B., Kaur H. Stratification of Hardware Attacks: Side Channel Attacks and Fault Injection Techniques // SN Computer Science. 2021. Vol. 2, No. 3. Art. 183. DOI: 10.1007/s42979-021-00562-3
- [52]. Gkonis P., Giannopoulos A., Trakadas P., Masip-Bruin X., D’Andria F. A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues // Future Internet. 2023. Vol. 15, No. 12. Art. 383. DOI: 10.3390/fi15120383.
- [53]. Tsao T., Alexander R., Dohler M., Daza V., Lozano A., Richardson M. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). RFC 7416. IETF, 2015. DOI: 10.17487/RFC7416
- [54]. Bormann C., Ersue M., Keranen A. Terminology for Constrained-Node Networks. RFC 7228. IETF, 2014.
- [55]. Alsukayti I. S., Alreshoodi M. RPL-Based IoT Networks under Simple and Complex Routing Security Attacks: An Experimental Study. Applied Sciences. 2023. Vol. 13, No. 8. Art. 4878. DOI: 10.3390/app13084878.
- [56]. Nitish A., Hanumanthappa J., Krinkin K. On-device context-aware misuse detection framework for heterogeneous IoT edge // Applied Intelligence. 2023. Vol. 53. P. 14792–14818. DOI: 10.1007/s10489-022-04039-5
- [57]. Zarpelão B. B., Miani R. S., Kawakani C. T., de Alvarenga S. C. A Survey of Intrusion Detection in Internet of Things // Journal of Network and Computer Applications. 2017. Vol. 84. P. 25–37. DOI: 10.1016/j.jnca.2017.02.009
- [58]. Al-Garadi M. A., Mohamed A., Al-Ali A. K., Du X., Ali I., Guizani M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 3. P. 1646–1685. DOI: 10.1109/COMST.2020.2988293
- [59]. Butun I., Morgera S. D., Sankar R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks // IEEE Communications Surveys & Tutorials. 2014. Vol. 16, No. 1. P. 266–282. DOI: 10.1109/SURV.2013.050113.00191
- [60]. Raza S., Wallgren L., Voigt T. SVELTE: Real-time Intrusion Detection in the Internet of Things // Ad Hoc Networks. 2013. Vol. 11, No. 8. P. 2661–2674. DOI: 10.1016/j.adhoc.2013.04.014
- [61]. Roman R., Lopez J., Mambo M. Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges // Future Generation Computer Systems. 2018. Vol. 78. P. 680–698. DOI: 10.1016/j.future.2016.11.009
- [62]. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. Cybersecurity. 2019. Vol. 2. Art. 20. DOI: 10.1186/s42400-019-0038-7.
- [63]. da Costa K. A. P., Papa J. P., Lisboa C. O., Munoz R., de Albuquerque V. H. C. Internet of Things: A Survey on Machine Learning-Based Intrusion

- Detection Approaches // *Computer Networks*. 2019. Vol. 151. P. 147–157. DOI: 10.1016/j.comnet.2019.01.023
- [64]. Lim W. Y. B., Luong N. C., Hoang D. T., Jiao Y., Liang Y.-C., Yang Q., Niyato D., Miao C. Federated Learning in Mobile Edge Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22, No. 3. P. 2031–2063. DOI: 10.1109/COMST.2020.2986024.
  - [65]. Arisdakessian S., Wahab O. A., Mourad A., Otrók H. A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions // *IEEE Internet of Things Journal*. 2022.
  - [66]. Neupane S., Ables J., Anderson W., Mittal S., Rahimi S., Banicescu I. Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities // *IEEE Access*. 2022. Vol. 10. P. 112392–112415
  - [67]. Rieger P., Chilese M., Mohamed R., Miettinen M., Fereidooni H., Sadeghi A.-R. ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks. *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim: USENIX Association, 2023. P. 4301–4318. ISBN 978-1-939133-37-3.
  - [68]. Gama J., Žliobaitė I., Bifet A., Pechenizkiy M., Bouchachia A. A Survey on Concept Drift Adaptation // *ACM Computing Surveys*. 2014. Vol. 46, No. 4. Art. 44. DOI: 10.1145/2523813
  - [69]. Bifet A., Gavaldà R. Learning from Time-Changing Data with Adaptive Windowing // *Proceedings of the 2007 SIAM International Conference on Data Mining*. 2007. P. 443–448. DOI: 10.1137/1.9781611972771.42
  - [70]. Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions // *Advances in Neural Information Processing Systems*. 2017. Vol. 30. P. 4765–4774
  - [71]. AlSalem T. S., Almaiah M. A., Lutfi A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics*. 2023. Vol. 12, No. 18. Art. 3958. DOI: 10.3390/electronics12183958.
  - [72]. Brancati F., Mongelli D., Mariotti F., Lollini P. A Cybersecurity Risk Assessment Methodology for Industrial Automation Control Systems. *International Journal of Information Security*. 2025. Vol. 24, No. 2. Art. 76. DOI: 10.1007/s10207-025-00990-9.
  - [73]. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. NIST SP 800-213A. 2021. DOI: 10.6028/NIST.SP.800-213A
  - [74]. Stouffer K., Pease M., Tang C., et al. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. 2023. DOI: 10.6028/NIST.SP.800-82r3.
  - [75]. Warden P., Situnayake D. TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. Sebastopol: O'Reilly Media, 2019.

- [76]. Blalock D., Ortiz J. G., Frankle J., Gutttag J. What is the State of Neural Network Pruning? 2020. arXiv:2003.03033
- [77]. National Institute of Standards and Technology. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST SP 800-218. 2022. DOI: 10.6028/NIST.SP.800-218.
- [78]. SLSA Community. Supply-chain Levels for Software Artifacts (SLSA) Framework. Version 1.0. 2023.
- [79]. Han S., Mao H., Dally W. J. Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. ICLR Workshop, 2016.
- [80]. Hinton G., Vinyals O., Dean J. Distilling the Knowledge in a Neural Network. NIPS Deep Learning and Representation Learning Workshop, 2015
- [81]. Zhou Z., Chen X., Li E., Zeng L., Luo K., Zhang J. Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. Proceedings of the IEEE. 2019. Vol. 107, No. 8. P. 1738–1762. DOI: 10.1109/JPROC.2019.2918951.
- [82]. Alrawais A., Alhothaily A., Hu C., Cheng X. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing. 2017. Vol. 21, No. 2. P. 34–42. DOI: 10.1109/MIC.2017.37.
- [83]. Saito T., Rehmsmeier M. The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets. PLOS ONE. 2015. Vol. 10, No. 3. Art. e0118432. DOI: 10.1371/journal.pone.0118432.
- [84]. Chicco D., Jurman G. The Advantages of the Matthews Correlation Coefficient over F1 Score and Accuracy in Binary Classification Evaluation. BMC Genomics. 2020. Vol. 21. Art. 6. DOI: 10.1186/s12864-019-6413-7.
- [85]. Guo C., Pleiss G., Sun Y., Weinberger K. Q. On Calibration of Modern Neural Networks. Proceedings of the 34th International Conference on Machine Learning. 2017. Vol. 70. P. 1321–1330.
- [86]. Moustafa N. A New Distributed Architecture for Evaluating AI-Based Security Systems at the Edge: Network TON\_IoT Datasets. Sustainable Cities and Society. 2021. Vol. 72. Art. 102994. DOI: 10.1016/j.scs.2021.102994.
- [87]. Ferrag M. A., Friha O., Hamouda D., Maglaras L., Janicke H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning // IEEE Access. 2022. Vol. 10. P. 40281–40306. DOI: 10.1109/ACCESS.2022.3165809.
- [88]. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST SP 800-213. 2021. DOI: 10.6028/NIST.SP.800-213.
- [89]. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. NIST Interagency or Internal Report 8259A. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.IR.8259A.

- [90]. N. Moustafa, "TON\_IoT Telemetry and Network Datasets for the Internet of Things (IoT)," *IEEE Access*, vol. 9, pp. 31277–31293, 2021. [Online]. Available: <https://ieeexplore.ieee.org/document/9354555>
- [91]. S. García, A. Parmisano, A. Zunino, "IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic," Stratosphere Laboratory Report, 2020. [Online]. Available: <https://www.stratosphereips.org/datasets-iot23>
- [92]. Neto E. C. P., Dadkhah S., Ferreira R., Zohourian A., Lu R., Ghorbani A. A. CICIOT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors*. 2023. Vol. 23, No. 13. Art. 5941. DOI: 10.3390/s23135941.
- [93]. De Marco G., Loia V., Karimipour H., Siano P. Assessing Insider Attacks and Privacy Leakage in Managed IoT Systems for Residential Prosumers // *Energies*. 2021. Vol. 14, No. 9. Art. 2385. DOI: 10.3390/en14092385
- [94]. Ibbett A. An Examination of Real-World Data Leakage from IoT Devices: doctoral thesis. Australia: Charles Sturt University, 2022. 207 p.
- [95]. Safi M., Dadkhah S., Shoeleh F., Mahdikhani H., Molyneaux H., Ghorbani A. A. A Survey on IoT Profiling, Fingerprinting, and Identification. *ACM Transactions on Internet of Things*. 2022. Vol. 3, No. 4. P. 1–39. DOI: 10.1145/3539736.
- [96]. Al-Kuwari S., Li X. Lightweight Encryption Schemes for the Internet of Things: Survey and Future Directions // *IEEE Access*. 2022. Vol. 10. P. 54532–54557
- [97]. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy // *Foundations and Trends in Theoretical Computer Science*. 2014
- [98]. Kairouz P. et al. Advances and Open Problems in Federated Learning // *Foundations and Trends in Machine Learning*. 2021.
- [99]. Yang Q., Liu Y., Chen T., Tong Y. Federated Machine Learning: Concept and Applications // *ACM Transactions on Intelligent Systems and Technology*. 2019. Vol. 10, No. 2. P. 1–19.
- [100]. Khan W. Z., Rehman M. H., Zeb A. et al. Balancing Security and Performance Trade-offs in the Internet of Things: A Comprehensive Survey // *Future Generation Computer Systems*. 2022. Vol. 128. P. 275–290.
- [101]. Regulation (EU) 2016/679 ... General Data Protection Regulation (GDPR). Official Journal of the European Union
- [102]. ISO/IEC 27018:2019 — Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO.
- [103]. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Official Journal of the European Union. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>
- [104]. UK Department for Digital, Culture, Media and Sport. Code of Practice for Consumer IoT Security. London, 2018

- [105]. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. 2013. Vol. 29(7). P. 1645–1660. DOI: 10.1016/j.future.2013.01.010
- [106]. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. *Computer Networks*. 2010. Vol. 54(15). P. 2787–2805. DOI: 10.1016/j.comnet.2010.05.010
- [107]. Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *IEEE International Systems Engineering Symposium (ISSE)*. 2017. P. 1–7. DOI: 10.1109/SysEng.2017.8088251
- [108]. Whitmore A., Agarwal A., Da Xu L. The Internet of Things — A survey of topics and trends. *Information Systems Frontiers*. 2015. Vol. 17(2). P. 261–274. DOI: 10.1007/s10796-014-9489-2
- [109]. Li S., Da Xu L., Zhao S. The Internet of Things: A survey. *Information Systems Frontiers*. 2015. Vol. 17(2). P. 243–259. DOI: 10.1007/s10796-014-9492-7
- [110]. Khan R., Khan S. U., Zaheer R., Khan S. Future Internet: The Internet of Things architecture, possible applications and key challenges. *IEEE 10th International Conference on Frontiers of Information Technology (FIT)*. 2012. P. 257–260. DOI: 10.1109/FIT.2012.53
- [111]. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*. 2014. Vol. 16(1). P. 414–454. DOI: 10.1109/SURV.2013.042313.00197
- [112]. Gil D., Ferrández A., Mora-Mora H., Peral J. Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services. *Sensors*. 2016. Vol. 16, No. 7. Art. 1069. DOI: 10.3390/s16071069.
- [113]. Lee I., Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*. 2015. Vol. 58(4). P. 431–440. DOI: 10.1016/j.bushor.2015.03.008
- [114]. Madakam S., Ramaswamy R., Tripathi S. Internet of Things (IoT): A literature review. *Journal of Computer and Communications*. 2015. Vol. 3(5). P. 164–173. DOI: 10.4236/jcc.2015.35021
- [115]. Mahmoud R., Yousuf T., Aloul F., Zualkernan I. Internet of Things (IoT) security: A survey. *IEEE Internet of Things World Forum (IoTWF)*. 2015. P. 245–252. DOI: 10.1109/IoTWF.2015.7389096.
- [116]. Hossain M., Fotouhi M., Hasan R. Towards an analysis of security issues, challenges, and open problems in the Internet of Things. *IEEE SERVICES*. 2015. P. 21–28. DOI: 10.1109/SERVICES.2015.12
- [117]. Chang Z., Liu S., Xiong X., Cai Z., Tu G. A Survey of Recent Advances in Edge-Computing-Powered Artificial Intelligence of Things. *IEEE Internet of Things Journal*. 2021. Vol. 8, No. 18. P. 13849–13875. DOI: 10.1109/JIOT.2021.3088875.

- [118]. Ferrag M. A., Friha O., Kantarci B., Tihanyi N., Cordeiro L., Debbah M., Hamouda D., Al-Hawawreh M., Choo K.-K. R. Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses. *IEEE Communications Surveys & Tutorials*. 2023. Vol. 25, No. 4. P. 2654–2713. DOI: 10.1109/COMST.2023.3317242.
- [119]. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17(4). P. 2347–2376. DOI: 10.1109/COMST.2015.2444095
- [120]. Sylla T., Chalouf M. A., Krief F., Samaké K. Context-Aware Security in the Internet of Things: A Survey. *International Journal of Autonomous and Adaptive Communications Systems*. 2021. Vol. 14, No. 3. P. 231–263. DOI: 10.1504/IJAACS.2021.117808.
- [121]. Ambrosin M., Conti M., Lazzeretti R., Rabbani M. M., Ranise S. PADS: Practical Attestation for Highly Dynamic Swarm Topologies. *Proceedings of the 2018 International Workshop on Secure Internet of Things (SIoT)*. Barcelona: IEEE, 2018. P. 18–27. DOI: 10.1109/SIoT.2018.00009.
- [122]. Klir G. J., Yuan B. *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Englewood Cliffs: Prentice Hall, 1995. 592 p.
- [123]. Ross T. J. *Fuzzy Logic with Engineering Applications*. 3rd ed. Chichester: John Wiley & Sons, 2010. 585 p.
- [124]. Young A., Yung M. Kleptography: Using Cryptography Against Cryptography // *Advances in Cryptology — EUROCRYPT '97*. Lecture Notes in Computer Science. Vol. 1233. Berlin: Springer, 1997. P. 62–74. DOI: 10.1007/3-540-69053-0\_6.
- [125]. Mashaleh A. S., Ibrahim N. F. B., Alauthman M., Almseidin M., Gawanmeh A. IoT Smart Devices Risk Assessment Model Using Fuzzy Logic and PSO. *Computers, Materials & Continua*. 2024. Vol. 78, No. 2. P. 2245–2267. DOI: 10.32604/cmc.2023.047323.
- [126]. Zadeh L. A. The concept of a linguistic variable and its application to approximate reasoning—I. *Information Sciences*. 1975. Vol. 8, No. 3. P. 199–249. DOI: 10.1016/0020-0255(75)90036-5
- [127]. Zimmermann H.-J. *Fuzzy Set Theory—and Its Applications*. 4th ed. Dordrecht: Springer, 2001. 514 p. DOI: 10.1007/978-94-010-0646-0.
- [128]. Barlybayev A., Turginbayeva A. Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering*. 2025. Vol. 4, No. 4. P. 570–580. DOI: 10.47852/bonviewJCCE52024683.
- [129]. Mamdani E. H., Assilian S. An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies*. 1975. Vol. 7, No. 1. P. 1–13. DOI: 10.1016/S0020-7373(75)80002-2.
- [130]. Stojkoska B.L.R., Trivodaliev K.V. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 2017, vol. 140, pp. 1454–1464. DOI: 10.1016/j.jclepro.2016.10.006

- [131]. Pedrycz W. Why Triangular Membership Functions? Fuzzy Sets and Systems. 1994. Vol. 64, No. 1. P. 21–30. DOI: 10.1016/0165-0114(94)90003-5.
- [132]. Guillaume S. Designing Fuzzy Inference Systems from Data: An Interpretability-Oriented Review. IEEE Transactions on Fuzzy Systems. 2001. Vol. 9, No. 3. P. 426–443. DOI: 10.1109/91.928739.
- [133]. Gegov A. Rule Base Reduction Methods for Fuzzy Systems. Complexity Management in Fuzzy Systems: A Rule Base Compression Approach. Studies in Fuzziness and Soft Computing. Berlin: Springer, 2007. Vol. 211. P. 17–31. DOI: 10.1007/978-3-540-38885-2\_3.
- [134]. Gegov A., Gobalakrishnan N., Sanders D. Rule base compression in fuzzy systems by filtration of non-monotonic rules. Journal of Intelligent & Fuzzy Systems. 2014. Vol. 27, No. 4. DOI: 10.3233/IFS-141169
- [135]. The MathWorks, Inc. Fuzzy Logic Toolbox™ User's Guide. Natick, MA: The MathWorks, Inc., 2025.
- [136]. National Institute of Standards and Technology. National Vulnerability Database (NVD). NIST. URL: <https://nvd.nist.gov/>
- [137]. The MITRE Corporation. Common Weakness Enumeration (CWE). URL: <https://cwe.mitre.org/>
- [138]. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset // *Future Generation Computer Systems*. – 2019. – Vol. 100. – P. 779–796. – DOI: 10.1016/j.future.2019.05.041.
- [139]. Moustafa N. TON\_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems // *IEEE Access*. – 2020. – Vol. 8. – P. 165130–165150. – DOI: 10.1109/ACCESS.2020.3022862.
- [140]. ITU-T. Overview of the Internet of Things. Recommendation ITU-T Y.2060. — Geneva: International Telecommunication Union, 2012. — [Online]. Available: <https://www.itu.int/rec/T-REC-Y.2060>



## ДОДАТКИ

### Додаток А. Список публікацій здобувача за темою дисертації

1. Pidlisnyi Yuriy, Intelligent-Contextual Model for the Classification of Internet of Things Environments // *[Central Ukrainian Scientific Bulletin Technical Sciences]*. 2025. № 12(43). С. 20–30.  
[https://DOI: 10.32515/2664-262X.2025.12\(43\).1.20-30](https://doi.org/10.32515/2664-262X.2025.12(43).1.20-30).
2. Mariia KAPUSTIAN, Yurii PIDLISNYI, Mykhailo SHELEST, Methods of Hiding Data in Computer Networks: From Classics to IoT and AI // *[Computer systems and information technologies]*. 2025. № 4–3. DOI: <https://doi.org/10.31891/csit-2025-4-3>.
3. Pidlisnyi Yuriy, Fuzzy Logic in IoT Security Risk Assessment: Rule Construction and Implementation // *[Computer Science and Engineering]*. 2025. № 3(41). С. 237–253. DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-237-253](https://doi.org/10.25140/2411-5363-2025-3(41)-237-253).
4. Pidlisnyi Yuriy , Audit of IoT Networks: Assessing Vulnerabilities and Protecting Against Cyber Attacks // *[Computer Science and Engineering]*. 2025. № 1(39). С. 170–183. DOI: [https://doi.org/10.25140/2411-5363-2025-1\(39\)-170-183](https://doi.org/10.25140/2411-5363-2025-1(39)-170-183).
5. Pidlisnyi Yuriy , Possible Ways to Improve Privacy in IoT Networks // *[Central Ukrainian Scientific Bulletin Technical Sciences]*. 2025. № 11(42). С. 46–55. DOI: [https://doi.org/10.32515/2664-262X.2025.11\(42\).1.46-55](https://doi.org/10.32515/2664-262X.2025.11(42).1.46-55).

## Додаток Б.

Таблиця Б.1 – Репрезентативний фрагмент мережевого датасету TON IoT.

| №  | src_ip | src_port | dst_ip         | dst_port | proto | service | duration    | src_bytes | dst_bytes | conn_state | src_pkts | dst_pkts | label | type       |
|----|--------|----------|----------------|----------|-------|---------|-------------|-----------|-----------|------------|----------|----------|-------|------------|
| 1  |        | 4444     | 192.168.1.193  | 49178    | tcp   | -       | 290.371539  | 101568    | 2592      | OTH        | 108      | 31       | 1     | backdoor   |
| 2  |        | 49180    | 192.168.1.37   | 8080     | tcp   | -       | 0.000102    | 0         | 0         | REJ        | 1        | 1        | 1     | backdoor   |
| 3  |        | 49180    | 192.168.1.37   | 8080     | tcp   | -       | 0.000148    | 0         | 0         | REJ        | 1        | 1        | 1     | backdoor   |
| 4  |        | 49180    | 192.168.1.37   | 8080     | tcp   | -       | 0.000113    | 0         | 0         | REJ        | 1        | 1        | 1     | backdoor   |
| 5  |        | 49180    | 192.168.1.37   | 8080     | tcp   | -       | 0.00013     | 0         | 0         | REJ        | 1        | 1        | 1     | backdoor   |
| 6  |        | 39180    | 18.184.104.180 | 8080     | tcp   | -       | 1123.254189 | 1286281   | 749633    | SF         | 4015     | 1923     | 1     | ddos       |
| 7  |        | 39182    | 18.184.104.180 | 8080     | tcp   | -       | 1123.257114 | 1343869   | 784744    | SF         | 3978     | 2028     | 1     | ddos       |
| 8  |        | 39184    | 18.184.104.180 | 8080     | tcp   | -       | 1123.276244 | 1197748   | 701307    | SF         | 3766     | 1729     | 1     | ddos       |
| 9  |        | 39186    | 18.184.104.180 | 8080     | tcp   | -       | 1123.262629 | 1305914   | 762793    | SF         | 3967     | 1941     | 1     | ddos       |
| 10 |        | 39188    | 18.184.104.180 | 8080     | tcp   | -       | 1123.279137 | 1219202   | 712529    | SF         | 3744     | 1782     | 1     | ddos       |
| 11 |        | 34684    | 101.119.11.17  | 80       | tcp   | -       | 172.941797  | 865       | 1152      | SF         | 25       | 21       | 1     | injection  |
| 12 |        | 38524    | 192.168.1.1    | 53       | udp   | dns     | 0.00562     | 44        | 44        | SF         | 2        | 2        | 1     | injection  |
| 13 |        | 42075    | 192.168.1.1    | 53       | udp   | dns     | 0.00313     | 52        | 52        | SF         | 2        | 2        | 1     | injection  |
| 14 |        | 43803    | 192.168.1.1    | 53       | udp   | dns     | 0.007465    | 44        | 44        | SF         | 2        | 2        | 1     | injection  |
| 15 |        | 45736    | 192.168.1.1    | 53       | udp   | dns     | 0.005039    | 44        | 44        | SF         | 2        | 2        | 1     | injection  |
| 16 |        | 33966    | 101.119.11.17  | 80       | tcp   | http    | 118.154006  | 576       | 768       | SF         | 19       | 16       | 1     | password   |
| 17 |        | 36490    | 192.168.1.1    | 53       | udp   | dns     | 0.015741    | 84        | 424       | SF         | 2        | 2        | 1     | password   |
| 18 |        | 37814    | 192.168.1.195  | 80       | tcp   | http    | 7.761997    | 446       | 205       | SF         | 5        | 4        | 1     | password   |
| 19 |        | 43331    | 192.168.1.1    | 53       | udp   | dns     | 0.015047    | 42        | 200       | SF         | 1        | 1        | 1     | password   |
| 20 |        | 37242    | 34.230.157.88  | 443      | tcp   | -       | 0           | 0         | 0         | OTH        | 0        | 1        | 1     | ransomware |

|    |  |       |               |       |     |     |          |   |     |     |   |   |   |            |
|----|--|-------|---------------|-------|-----|-----|----------|---|-----|-----|---|---|---|------------|
| 21 |  | 37242 | 34.230.157.88 | 443   | tcp | -   | 0        | 0 | 0   | OTH | 0 | 1 | 1 | ransomware |
| 22 |  | 37242 | 34.230.157.88 | 443   | tcp | -   | 0        | 0 | 0   | OTH | 1 | 0 | 1 | ransomware |
| 23 |  | 37242 | 34.230.157.88 | 443   | tcp | -   | 0        | 0 | 0   | OTH | 1 | 0 | 1 | ransomware |
| 24 |  | 42908 | 192.168.1.103 | 2046  | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | scanning   |
| 25 |  | 42908 | 192.168.1.250 | 7435  | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | scanning   |
| 26 |  | 42908 | 192.168.1.46  | 1641  | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | scanning   |
| 27 |  | 42909 | 192.168.1.103 | 2046  | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | scanning   |
| 28 |  | 33108 | 176.28.50.165 | 80    | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | xss        |
| 29 |  | 33114 | 176.28.50.165 | 80    | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | xss        |
| 30 |  | 33118 | 176.28.50.165 | 80    | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | xss        |
| 31 |  | 33122 | 176.28.50.165 | 80    | tcp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 1 | xss        |
| 32 |  | 47260 | 192.168.1.255 | 15600 | udp | -   | 0        | 0 | 0   | S0  | 1 | 0 | 0 | normal     |
| 33 |  | 1880  | 192.168.1.152 | 51782 | tcp | -   | 0        | 0 | 0   | OTH | 0 | 0 | 0 | normal     |
| 34 |  | 34296 | 192.168.1.152 | 10502 | tcp | -   | 0        | 0 | 0   | OTH | 0 | 0 | 0 | normal     |
| 35 |  | 46608 | 192.168.1.190 | 53    | udp | dns | 0.000549 | 0 | 298 | SHR | 0 | 2 | 0 | normal     |

Примітка. Наведено реальні записи з файлу train\_test\_network.csv. Для представлення всіх класів атак відібрано 40 записів: Backdoor – 5, DoS – 5, DDoS – 5, Injection – 5, Password – 4, Ransomware – 4, Scanning – 4, XSS – 4, Normal – 4.

**Таблиця Б.2 – Опис атрибутів мережевого датасету TON\_IoT**

| Позначення | Опис                                                                          |
|------------|-------------------------------------------------------------------------------|
| src_ip     | IP-адреса вузла-джерела мережевого з'єднання.                                 |
| src_port   | Порт вузла-джерела.                                                           |
| dst_ip     | IP-адреса вузла-призначення.                                                  |
| dst_port   | Порт вузла-призначення.                                                       |
| proto      | Протокол транспортного рівня (TCP, UDP, ICMP тощо).                           |
| service    | Мережевий сервіс або прикладний протокол, що використовувався під час сеансу. |
| duration   | Тривалість мережевого з'єднання, с.                                           |
| src_bytes  | Кількість байтів, переданих від вузла-джерела.                                |
| dst_bytes  | Кількість байтів, отриманих вузлом-призначення.                               |
| conn_state | Стан мережевого з'єднання після завершення сеансу.                            |
| src_pkts   | Кількість пакетів, переданих від вузла-джерела.                               |

|                 |                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>dst_pkts</b> | Кількість пакетів, отриманих вузлом-призначення.                                                                               |
| <b>label</b>    | Мітка класу: <b>0</b> – нормальний трафік; <b>1</b> – мережевий трафік, що відповідає кібератаці.                              |
| <b>type</b>     | Тип мережевого трафіку або категорія кібератаки (Normal, Backdoor, DoS, DDoS, Injection, Password, Ransomware, Scanning, XSS). |

**Таблиця Б.3** – Лінгвістичні змінні моделі нечіткого оцінювання ризиків IoT-безпеки

| Позначення | Назва лінгвістичної змінної                             | Тип змінної | Універсум значень | Лінгвістичні терми            | Тип функцій належності      |
|------------|---------------------------------------------------------|-------------|-------------------|-------------------------------|-----------------------------|
| (A_c)      | Критичність активу (Asset Criticality)                  | вхідна      | [0; 10]           | Low, Medium, High             | трикутні                    |
| (T_l)      | Рівень загрози (Threat Level)                           | вхідна      | [0; 10]           | Low, Medium, High             | трикутні                    |
| (V_l)      | Рівень вразливості (Vulnerability Level)                | вхідна      | [0; 10]           | Low, Medium, High             | трикутні                    |
| (A_{cp})   | Спроможність атакувальника (Attacker Capability)        | вхідна      | [0; 10]           | Basic, Intermediate, Advanced | трикутні                    |
| (L_e)      | Імовірність експлуатації (Likelihood of Exploitation)   | вхідна      | [0; 10]           | Low, Medium, High             | трикутні                    |
| (I_s)      | Масштаб наслідків інциденту (Impact Severity)           | вхідна      | [0; 10]           | Low, Medium, High, Critical   | трикутні та трапецієподібні |
| (B_r)      | Ризик прихованої компрометації (Backdoor / Covert Risk) | вхідна      | [0; 10]           | Low, Medium, High             | трикутні                    |
| (R)        | Інтегральний рівень ризику (Risk Level)                 | Вихідна     | [0; 10]           | Low, Medium, High, Critical   | трикутні та трапецієподібні |

**Примітка.** Для всіх змінних використано уніфікований універсум значень [0; 10]. Для опису проміжних рівнів застосовано трикутні функції належності, а для крайніх значень змінних  $I_s$  та  $R$  — трапецієподібні функції належності. Для змінної  $A_{cp}$  використано терми *Basic*, *Intermediate* та *Advanced*, які характеризують рівень підготовки й технічні можливості потенційного атакувальника.

**Таблиця Б.4** – Основні параметри нечіткої системи логічного висновку Mamdani

| Параметр                              | Значення             | Характеристика                                                                                                                                             |
|---------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Назва нечіткої системи                | IoT_Risk_FIS_40rules | Ідентифікатор реалізованої FIS-моделі оцінювання ризику                                                                                                    |
| Тип нечіткої системи                  | Mamdani              | Формування вихідного результату на основі нечітких продукційних правил                                                                                     |
| Версія формату FIS                    | 2.0                  | Версія структури файлу нечіткої системи                                                                                                                    |
| Кількість вхідних змінних             | 7                    | Критичність активу, рівень загрози, вразливість, спроможність атакувальника, імовірність експлуатації, масштаб наслідків та ризик прихованої компрометації |
| Кількість вихідних змінних            | 1                    | Інтегральний рівень ризику<br>RiskLevel                                                                                                                    |
| Універсум вхідних змінних             | [0; 10]              | Єдиний нормований діапазон значень усіх вхідних параметрів                                                                                                 |
| Універсум вихідної змінної            | [0; 10]              | Діапазон інтегральної оцінки ризику                                                                                                                        |
| Кількість термів вхідних змінних      | 22                   | Для шести змінних використано по 3 терми, для ImpactSeverity — 4 терми                                                                                     |
| Кількість термів вихідної змінної     | 4                    | Low, Medium, High, Critical                                                                                                                                |
| Загальна кількість функцій належності | 26                   | 22 функції для вхідних змінних і 4 — для вихідної                                                                                                          |
| Типи функцій належності               | trimf, trapmf        | Трикутні та трапецієподібні функції належності                                                                                                             |
| Метод нечіткої кон'юнкції AND         | min                  | Мінімум ступенів належності умов правила                                                                                                                   |
| Метод нечіткої диз'юнкції OR          | max                  | Максимум ступенів належності альтернативних умов                                                                                                           |
| Метод імплікації                      | min                  | Обмеження вихідної функції належності ступенем активації правила                                                                                           |
| Метод агрегації                       | max                  | Об'єднання вихідних нечітких множин активованих правил                                                                                                     |
| Метод дефазифікації                   | centroid             | Визначення чіткого значення ризику методом центра ваги                                                                                                     |
| Кількість записів правил у FIS-файлі  | 40                   | Загальна кількість рядків у секції [Rules]                                                                                                                 |
| Вага правил                           | 1                    | Для всіх правил використано однакову вагу                                                                                                                  |
| Тип логічного зв'язку в правилах      | AND                  | У правилах застосовано кон'юнкцію умов                                                                                                                     |

**Таблиця Б.5 – Параметри функцій належності нечіткої моделі оцінювання ризику**

| Змінна             | Лінгвістичний терм | Тип функції | Параметри   |
|--------------------|--------------------|-------------|-------------|
| AssetCriticality   | Low                | trimf       | [0 0 5]     |
|                    | Medium             | trimf       | [2 5 8]     |
|                    | High               | trimf       | [5 10 10]   |
| ThreatLevel        | Low                | trimf       | [0 0 5]     |
|                    | Medium             | trimf       | [2 5 8]     |
|                    | High               | trimf       | [5 10 10]   |
| Vulnerability      | Low                | trimf       | [0 0 5]     |
|                    | Medium             | trimf       | [2 5 8]     |
|                    | High               | trimf       | [5 10 10]   |
| AttackerCapability | Basic              | trimf       | [0 0 5]     |
|                    | Intermediate       | trimf       | [2 5 8]     |
|                    | Advanced           | trimf       | [5 10 10]   |
| Likelihood         | Low                | trimf       | [0 0 5]     |
|                    | Medium             | trimf       | [2 5 8]     |
|                    | High               | trimf       | [5 10 10]   |
| ImpactSeverity     | Low                | trapmf      | [0 0 2 4]   |
|                    | Medium             | trimf       | [2 4 6]     |
|                    | High               | trimf       | [4 7 9]     |
|                    | Critical           | trapmf      | [7 9 10 10] |
| BackdoorRisk       | Low                | trimf       | [0 0 5]     |
|                    | Medium             | trimf       | [2 5 8]     |
|                    | High               | trimf       | [5 10 10]   |
| RiskLevel          | Low                | trapmf      | [0 0 2 4]   |
|                    | Medium             | trimf       | [2 4 6]     |
|                    | High               | trimf       | [4 7 9]     |
|                    | Critical           | trapmf      | [7 9 10 10] |

Параметри функцій належності визначають форму та положення відповідних нечітких множин у нормованому діапазоні [0; 10]. Для більшості вхідних змінних використано три трикутні функції належності, що відповідають низькому, середньому та високому рівням. Для змінних *ImpactSeverity* та *RiskLevel* крайні терми *Low* і *Critical* описано трапецієподібними функціями належності, що забезпечує коректне представлення граничних значень відповідних параметрів

**Таблиця Б.6 – Повна база продукційних правил нечіткої моделі оцінювання ризику**

| № | Продукційне правило                                                                                        |
|---|------------------------------------------------------------------------------------------------------------|
| 1 | IF ThreatLevel = High AND Vulnerability = High AND AttackerCapability = Advanced THEN RiskLevel = Critical |
| 2 | IF AssetCriticality = High AND ThreatLevel = Medium AND Likelihood = High THEN RiskLevel = High            |
| 3 | IF Vulnerability = Medium AND BackdoorRisk = High THEN RiskLevel = High                                    |

|    |                                                                                                |
|----|------------------------------------------------------------------------------------------------|
| 4  | IF ThreatLevel = Low AND AttackerCapability = Basic THEN RiskLevel = Low                       |
| 5  | IF Likelihood = Medium AND ImpactSeverity = Critical THEN RiskLevel = High                     |
| 6  | IF ThreatLevel = Medium AND Vulnerability = Low AND BackdoorRisk = Low THEN RiskLevel = Medium |
| 7  | IF ThreatLevel = High AND Likelihood = High THEN RiskLevel = High                              |
| 8  | IF ThreatLevel = High AND ImpactSeverity = High THEN RiskLevel = Critical                      |
| 9  | IF Vulnerability = High AND Likelihood = Medium THEN RiskLevel = High                          |
| 10 | IF Vulnerability = Medium AND AttackerCapability = Advanced THEN RiskLevel = High              |
| 11 | IF ThreatLevel = Medium AND Likelihood = Low THEN RiskLevel = Medium                           |
| 12 | IF ThreatLevel = Medium AND ImpactSeverity = Medium THEN RiskLevel = Medium                    |
| 13 | IF AttackerCapability = Advanced AND BackdoorRisk = High THEN RiskLevel = Critical             |
| 14 | IF ThreatLevel = High AND BackdoorRisk = Medium THEN RiskLevel = High                          |
| 15 | IF Vulnerability = Low AND BackdoorRisk = Low THEN RiskLevel = Low                             |
| 16 | IF ThreatLevel = High AND BackdoorRisk = High THEN RiskLevel = Critical                        |
| 17 | IF Vulnerability = High AND ImpactSeverity = Medium THEN RiskLevel = High                      |
| 18 | IF Likelihood = Low AND ImpactSeverity = Low THEN RiskLevel = Low                              |
| 19 | IF ThreatLevel = Medium AND AttackerCapability = Intermediate THEN RiskLevel = Medium          |
| 20 | IF ThreatLevel = High AND ImpactSeverity = Critical THEN RiskLevel = Critical                  |
| 21 | IF Likelihood = High AND BackdoorRisk = High THEN RiskLevel = Critical                         |
| 22 | IF Vulnerability = Low AND AttackerCapability = Basic THEN RiskLevel = Low                     |
| 23 | IF Vulnerability = Medium AND Likelihood = High THEN RiskLevel = High                          |
| 24 | IF AssetCriticality = Medium AND ThreatLevel = High THEN RiskLevel = High                      |
| 25 | IF AssetCriticality = High AND ImpactSeverity = High THEN RiskLevel = Critical                 |
| 26 | IF ThreatLevel = High AND Likelihood = Medium THEN RiskLevel = High                            |
| 27 | IF ThreatLevel = Low AND Likelihood = High THEN RiskLevel = Medium                             |
| 28 | IF ImpactSeverity = Critical AND BackdoorRisk = Medium THEN RiskLevel = High                   |

|    |                                                                                      |
|----|--------------------------------------------------------------------------------------|
| 29 | IF ThreatLevel = Medium AND AttackerCapability = Advanced THEN RiskLevel = High      |
| 30 | IF ThreatLevel = Low AND AttackerCapability = Intermediate THEN RiskLevel = Low      |
| 31 | IF ThreatLevel = Medium AND Vulnerability = Medium THEN RiskLevel = Medium           |
| 32 | IF Likelihood = High AND ImpactSeverity = High THEN RiskLevel = Critical             |
| 33 | IF Vulnerability = Low AND BackdoorRisk = High THEN RiskLevel = Medium               |
| 34 | IF AssetCriticality = Low AND ThreatLevel = High THEN RiskLevel = Medium             |
| 35 | IF AssetCriticality = Medium AND Vulnerability = Medium THEN RiskLevel = Medium      |
| 36 | IF AssetCriticality = Medium AND BackdoorRisk = High THEN RiskLevel = High           |
| 37 | IF ThreatLevel = Medium AND AttackerCapability = Basic THEN RiskLevel = Medium       |
| 38 | IF AttackerCapability = Advanced AND ImpactSeverity = High THEN RiskLevel = Critical |
| 39 | IF Likelihood = Medium AND ImpactSeverity = Medium THEN RiskLevel = Medium           |
| 40 | IF ImpactSeverity = Medium AND BackdoorRisk = Medium THEN RiskLevel = Medium         |

**Примітка.** Умови, що не зазначені в окремому продукційному правилі, не обмежують значення відповідної вхідної змінної. Для всіх продукційних правил встановлено ваговий коефіцієнт 1. За наявності декількох передумов їх поєднання здійснюється логічною операцією AND. Вхідні змінні, не зазначені в передумові правила, не обмежують його спрацьовування. База містить 40 унікальних продукційних правил.

Наведена база продукційних правил визначає взаємозв'язки між лінгвістичними значеннями вхідних параметрів та інтегральним рівнем ризику. Правила охоплюють характерні комбінації параметрів, що відповідають низькому, середньому, високому та критичному рівням ризику. Повний опис правил разом із параметрами функцій належності забезпечує можливість відтворення розробленої нечіткої моделі.



## Додаток В.

*Таблиця В.1 – Функціональні компоненти інформаційної технології контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ*

| Функціональний компонент                                        | Основне призначення                                                                                                                                               | Вхідні дані                                                                                                                                         | Результат функціонування                                                                                |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Компонент збирання та попереднього оброблення даних             | Збирання, очищення, нормалізація та узгодження даних про IoT-пристрої й стан їх інформаційної безпеки                                                             | Конфігураційні характеристики IoT-пристроїв, мережевий трафік, телеметричні дані, журнали подій, відомості про загрози та вразливості               | Підготовлений і нормалізований набір даних для подальшого аналізу                                       |
| Компонент інтелектуально-контекстної класифікації IoT-пристроїв | Класифікація IoT-пристроїв за рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища | Технічні, функціональні, архітектурні, контекстні та безпекові характеристики IoT-пристрою                                                          | Результати інтелектуально-контекстної класифікації IoT-пристрою                                         |
| Компонент формування контекстно-ризикового профілю              | Узгоджене поєднання різнорідних результатів класифікації за допомогою оператора семантичної конвергенції                                                          | Результати інтелектуально-контекстної класифікації IoT-пристрою                                                                                     | Структурований контекстно-ризиковий профіль IoT-пристрою                                                |
| Компонент аналізу поточного стану інформаційної безпеки         | Аналіз відомостей про активи, актуальні загрози, вразливості, можливості потенційного порушника, умови реалізації загроз і можливі наслідки інцидентів            | Результати аналізу мережевої активності, відомості про вразливості та загрози, журнали подій, дані про активи й умови функціонування IoT-середовища | Сукупність показників, що характеризують поточний стан інформаційної безпеки IoT-пристрою та середовища |

**Примітка.** Інформаційна технологія побудована за модульним принципом і забезпечує послідовне перетворення первинних даних про IoT-пристрої та стан їх інформаційної безпеки в контекстно-ризиковий профіль, вектор вхідних параметрів, інтегральний показник RiskLevel і рекомендації щодо пріоритетності заходів захисту. Програмно реалізовано та експериментально перевірено ризиковий модуль на основі нечіткого логічного виведення типу Мамдані. У межах проведеної експериментальної перевірки BackdoorRisk використовувався як попередньо сформований вхідний параметр; його автоматичне визначення за первинними мережевими, поведінковими або криптографічними індикаторами не здійснювалося.

**Таблиця В.2 – Інформаційні потоки між функціональними модулями запропонованої інформаційної технології**

| Джерело інформаційного потоку                                             | Приймач інформаційного потоку                                   | Зміст інформаційного потоку                                                                                                                                    | Призначення інформаційного потоку                                                                                                       |
|---------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Джерела аудиторських даних                                                | Компонент збирання та попереднього оброблення даних             | Конфігураційні характеристики IoT-пристроїв, мережевий трафік, телеметричні дані, журнали подій, відомості про загрози та вразливості                          | Формування первинної інформаційної основи для подальшого аналізу стану інформаційної безпеки                                            |
| Компонент збирання та попереднього оброблення даних                       | Компонент інтелектуально-контекстної класифікації IoT-пристроїв | Очищені, нормалізовані та узгоджені технічні, функціональні, архітектурні, контекстні й безпекові характеристики пристроїв                                     | Виконання інтелектуально-контекстної класифікації IoT-пристроїв                                                                         |
| Компонент інтелектуально-контекстної класифікації IoT-пристроїв           | Компонент формування контекстно-ризикового профілю              | Результати класифікації за рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища | Узгоджене поєднання різномірних характеристик пристрою за допомогою оператора семантичної конвергенції                                  |
| Компонент формування контекстно-ризикового профілю                        | Компонент формування вхідних параметрів оцінювання ризику       | Структурований контекстно-ризиковий профіль IoT-пристрою                                                                                                       | Контекстне коригування та нормалізація параметрів нечіткої моделі оцінювання ризику                                                     |
| Компонент аналізу поточного стану інформаційної безпеки                   | Компонент формування вхідних параметрів оцінювання ризику       | Відомості про активи, загрози, вразливості, можливості потенційного порушника, імовірність реалізації загроз, можливі наслідки та аномальну активність         | Формування актуальних значень параметрів AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood та ImpactSeverity |
| Джерело попередньо сформованого показника ризику прихованої компрометації | Компонент формування вхідних параметрів оцінювання ризику       | Числове значення показника BackdoorRisk у діапазоні [0; 10]                                                                                                    | Урахування ризику прихованої компрометації як окремого вхідного параметра нечіткої моделі                                               |
| Компонент формування вхідних параметрів оцінювання ризику                 | Ризиковий модуль на основі нечіткого логічного виведення        | Нормалізований вектор AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk                             | Виконання нечіткого логічного виведення типу Мамдані й обчислення інтегрального показника ризику                                        |
| Ризиковий модуль на основі нечіткого логічного виведення                  | Компонент інтерпретації результатів і формування рекомендацій   | Дефазифіковане значення RiskLevel у діапазоні [0; 10] та відомості про активовані продукційні правила                                                          | Визначення категорії ризику та обґрунтування результату оцінювання                                                                      |
| Компонент інтерпретації результатів і формування рекомендацій             | Компонент підтримки прийняття рішень і звітності                | Категорія ризику, пріоритетність виявлених ризиків та рекомендовані технічні й організаційні заходи захисту                                                    | Формування результатів аудиту та підтримка прийняття рішень                                                                             |

**Примітка.** Інформаційні потоки між функціональними модулями забезпечують послідовне оброблення вхідних даних: від первинної класифікації IoT-пристроїв і аналізу мережевого трафіку до формування інтегральної оцінки ризику та підготовки рекомендацій щодо підвищення рівня інформаційної безпеки.

**Таблиця В.3 – Основні інформаційні об'єкти, що використовуються в запропонованій інформаційній технології**

| Інформаційний об'єкт                               | Джерело формування                                                                          | Основний вміст                                                                                                                                                               | Модуль-одержувач                                                                                             |
|----------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Первинні аудиторські дані                          | IoT-пристрої, мережеві шлюзи, журнали подій та джерела відомостей про загрози й вразливості | Конфігураційні характеристики пристроїв, мережевий трафік, телеметричні дані, події безпеки, відомості про активи, загрози та вразливості                                    | Компонент збирання та попереднього оброблення даних                                                          |
| Підготовлений набір даних                          | Компонент збирання та попереднього оброблення даних                                         | Очищені, нормалізовані та узгоджені технічні, функціональні, архітектурні, контекстні й безпекові характеристики IoT-пристроїв                                               | Компонент інтелектуально-контекстної класифікації та компонент аналізу поточного стану інформаційної безпеки |
| Результати інтелектуально-контекстної класифікації | Компонент інтелектуально-контекстної класифікації IoT-пристроїв                             | Оцінки рівня вбудованого інтелекту, характеристик безпеки, архітектури взаємодії, функціонального контексту та динамічності середовища                                       | Компонент формування контекстно-ризикового профілю                                                           |
| Контекстно-ризиковий профіль IoT-пристрою          | Компонент формування контекстно-ризикового профілю                                          | Структуроване поєднання функціональних, архітектурних, контекстних і безпекових характеристик пристрою, сформоване за допомогою оператора семантичної конвергенції           | Компонент формування вхідних параметрів оцінювання ризику та компонент інтерпретації результатів             |
| Показники поточного стану інформаційної безпеки    | Компонент аналізу поточного стану інформаційної безпеки                                     | Відомості про критичність активу, рівень загрози, вразливість, можливості потенційного порушника, імовірність реалізації загрози, тяжкість наслідків та аномальну активність | Компонент формування вхідних параметрів оцінювання ризику                                                    |
| Показник ризику прихованої компрометації           | Зовнішнє джерело або попередня аналітична процедура формування BackdoorRisk                 | Попередньо сформоване числове значення BackdoorRisk у діапазоні [0; 10]                                                                                                      | Компонент формування вхідних параметрів оцінювання ризику                                                    |
| Вектор вхідних параметрів нечіткої моделі          | Компонент формування вхідних параметрів оцінювання ризику                                   | Нормалізовані значення AssetCriticality, ThreatLevel, Vulnerability, AttackerCapability, Likelihood, ImpactSeverity та BackdoorRisk у діапазоні [0; 10]                      | Ризиковий модуль на основі нечіткого логічного виведення                                                     |

|                                 |                                                                       |                                                                                                                                                           |                                                                          |
|---------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Інтегральний показник ризику    | Ризиковий модуль на основі нечіткого логічного виведення типу Мамдані | Дефазифіковане значення RiskLevel у діапазоні [0; 10] та відомості про активовані продукційні правила                                                     | Компонент інтерпретації результатів і формування рекомендацій            |
| Результати інтерпретації ризику | Компонент інтерпретації результатів і формування рекомендацій         | Категорія ризику, пріоритетність виявлених ризиків та рекомендовані технічні й організаційні заходи захисту                                               | Компонент підтримки прийняття рішень і звітності                         |
| Звіт про результати аудиту      | Компонент підтримки прийняття рішень і звітності                      | Контекстно-ризиковий профіль, показники поточного стану безпеки, значення RiskLevel, категорія ризику та рекомендації щодо пріоритетності заходів захисту | Адміністратор інформаційної безпеки, аудитор або інша уповноважена особа |

**Примітка.** Інформаційні об'єкти є логічними одиницями даних, що циркулюють між функціональними модулями інформаційної технології. Вони забезпечують послідовне перетворення первинної інформації про стан IoT-середовища в інтегральну оцінку ризику та рекомендації щодо підвищення рівня інформаційної безпеки.

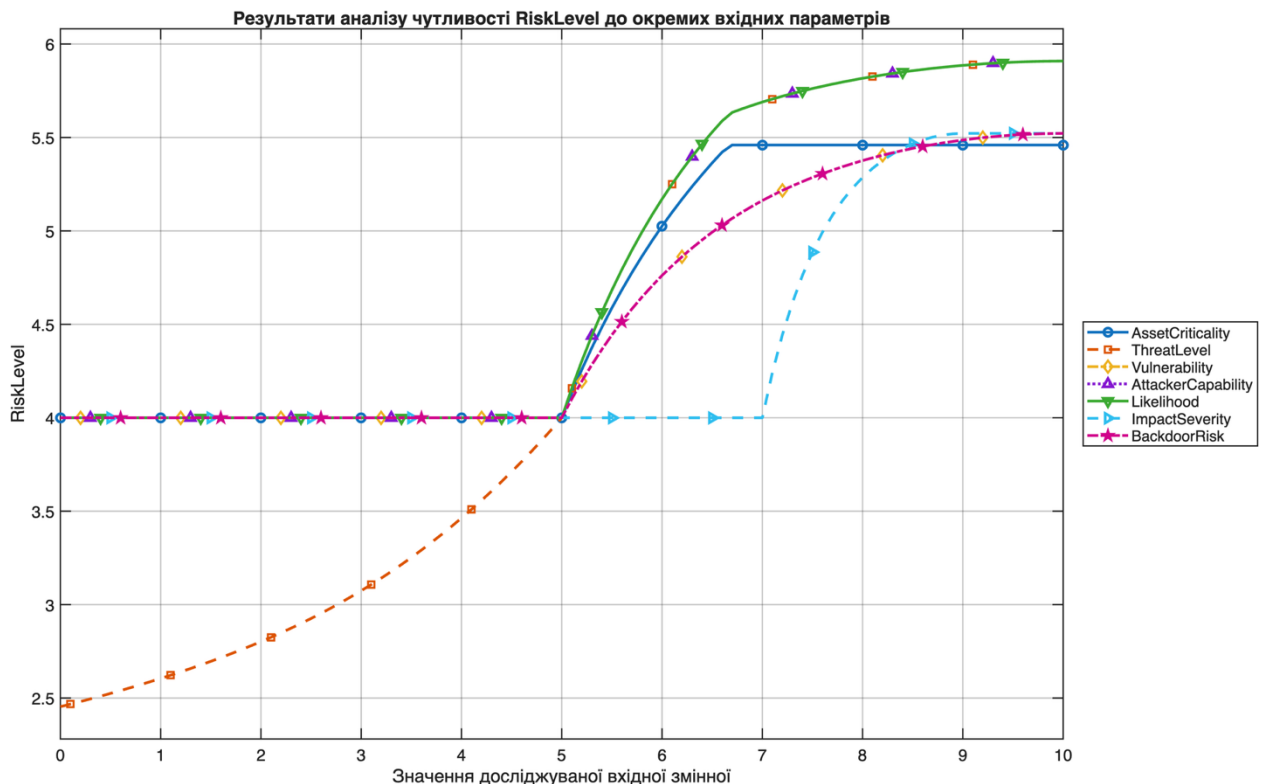
**Таблиця В.4** – Параметри програмно-експериментального середовища

| Компонент                                           | Характеристика                                                        |
|-----------------------------------------------------|-----------------------------------------------------------------------|
| Середовище програмної реалізації                    | MATLAB                                                                |
| Засоби нечіткого моделювання                        | MATLAB Fuzzy Logic Toolbox                                            |
| Тип нечіткої системи                                | Mamdani FIS                                                           |
| Метод дефазифікації                                 | Центроїдний метод                                                     |
| Відкриті набори даних                               | BoT-IoT, TON_IoT, Edge-IIoTset                                        |
| Обсяг уніфікованої вибірки мережевих подій          | 20 527 записів                                                        |
| Обсяг незалежної тестової частини мережевої вибірки | 4105 записів                                                          |
| Методи класифікації мережевих подій                 | Random Forest, SVM, Gradient Boosting, XGBoost, нейронна мережа       |
| Кількість вхідних змінних FIS                       | 7                                                                     |
| Кількість вихідних змінних FIS                      | 1 - RiskLevel                                                         |
| Діапазон значень вхідних і вихідної змінних         | [0; 10]                                                               |
| Кількість унікальних продукційних правил            | 40                                                                    |
| Базові моделі оцінювання ризику                     | Двопараметрична детермінована та семипараметрична зважена моделі      |
| Обсяг сценарної вибірки для кількісної валідації    | 100 000 сценаріїв, із яких 40 000 становили незалежну тестову частину |



|    |                                        |    |   |   |   |   |    |    |            |          |
|----|----------------------------------------|----|---|---|---|---|----|----|------------|----------|
| 17 | Високий Backdoor Risk                  | 5  | 5 | 4 | 5 | 5 | 6  | 10 | 5,52<br>20 | Високий  |
| 18 | Висока загроза, низька вразливість     | 5  | 9 | 2 | 8 | 8 | 7  | 2  | 5,45<br>17 | Високий  |
| 19 | Низька загроза, критичний вплив        | 5  | 2 | 5 | 4 | 4 | 10 | 3  | 4,21<br>49 | Середній |
| 20 | Висока критичність, низька ймовірність | 10 | 3 | 4 | 3 | 2 | 8  | 2  | 4,96<br>21 | Середній |

**Примітка.** Значення інтегрального показника Risk Level отримано шляхом обчислення за допомогою розробленої нечіткої системи логічного висновку Mamdani (evalfis) для 20 репрезентативних тестових сценаріїв. Усі результати перебувають у допустимому діапазоні  $[0;10]$ , що підтверджує коректність роботи моделі.



**Рисунок Б.1** — Покомпонентний аналіз чутливості вихідної змінної RiskLevel до зміни окремих вхідних параметрів нечіткої моделі оцінювання ризику.

**Примітка.** Під час побудови графіка кожна вхідна змінна змінювалася окремо в діапазоні від 0 до 10, тоді як решта вхідних параметрів були зафіксовані на середньому рівні (5).



**Додаток Г. Акти впровадження та довідки**

Товариство з обмеженою відповідальністю  
«ЛЮМ'ЕР ЕЛЕКТРО»

02094, м.Київ, вул. Вісхозна, 17  
Тел. (097)160-84-07, e-mail: r.onoprienko@lightcraft.com.ua  
П/р UAЕ33510050000025030566/97 Баче ПАТ "ЛЮМ'ЕР ЕЛЕКТРО", м.Київ  
ІП# 413153976533

**ДОВІДКА ПРО ВПРОВАДЖЕННЯ**

наукових результатів дисертаційної роботи Підлісного Юрія Івановича на тему  
«Методи виявлення вразливостей та протидія кібератакам в мережі Інтернету  
речей», представлена на здобуття вченого ступеня доктора філософії зі  
спеціальності 122 – «Комп'ютерні науки».

Запропоновані в дисертаційній роботі методи виявлення вразливостей та протидії  
кібератакам у мережах Інтернету речей були використані під час аналізу стану  
інформаційної безпеки мережевої інфраструктури підприємства та оцінювання  
захищеності підключених мережевих пристроїв.

Впровадження результатів дослідження дозволило:

- 1) провести інвентаризацію та аналіз безпеки пристроїв Інтернету речей, що використовуються в інформаційній інфраструктурі підприємства;
- 2) виявити потенційно небезпечні конфігурації та вразливості мережевого обладнання;
- 3) визначити найбільш імовірні сценарії реалізації кібератак на IoT-пристрої та мережеві сервіси;
- 4) здійснити оцінювання ризиків інформаційної безпеки та пріоритетності заходів захисту;
- 5) розробити комплекс рекомендацій щодо підвищення стійкості інформаційної інфраструктури до сучасних кіберзагроз.

Використання результатів дисертаційної роботи сприяло підвищенню рівня захищеності інформаційних ресурсів підприємства, зниженню ризиків несанкціонованого доступу та вдосконаленню процесів забезпечення кібербезпеки.

З повагою,

Директор



Р.М. Онопрієнко



ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ  
"АРКАДА ФІНАНС"

01033, м. Київ, вулиця Іллі Еренбурга, будинок 5, офіс 26  
ЄДРПОУ 40096154

№ 77 від 08.06.2026 року

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Підлісного Юрія Івановича на тему  
«Методи виявлення вразливостей та протидія кібератакам в мережі Інтернету  
речей», представлена на здобуття вченого ступеня доктора філософії зі  
спеціальності 122 – «Комп'ютерні науки».

У результаті впровадження наукових розробок, присвячених виявленню  
вразливостей та протидії кібератакам у мережах Інтернету речей, було застосовано  
методи аудиту безпеки IoT-середовища, моделі оцінювання ризиків на основі  
нечіткої логіки та засоби виявлення аномалій мережевого трафіку.

Запропоновані методи дозволили:

- 1) здійснити комплексний аудит безпеки пристроїв Інтернету речей;
- 2) виявити критичні вразливості та потенційні канали реалізації кібератак;
- 3) оцінити рівень ризику інформаційної безпеки IoT-середовища з урахуванням контексту функціонування пристроїв;
- 4) підвищити ефективність виявлення аномальної активності та кіберінцидентів;
- 5) сформулювати рекомендації щодо посилення захисту IoT-інфраструктури та зменшення ризиків кіберзагроз.

Використання результатів дисертаційної роботи сприяло підвищенню рівня  
інформаційної безпеки та стійкості мережі Інтернету речей до сучасних кібератак.

Директор



О.В.Дьошина



## ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "АТРІЯ КОМПАНІ"

вул.Саксаганського, будинок 74Б, офіс 11, місто Київ, 01032  
ЄДРПОУ 39562990

08.06.2026 № 43

### ДОВІДКА ПРО ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Підлісного Юрія Івановича на тему «Методи виявлення вразливостей та протидія кібератакам в мережі Інтернету речей», представлена на здобуття вченого ступеня доктора філософії зі спеціальності 122 – «Комп'ютерні науки».

Результати дисертаційного дослідження, присвяченого розробці методів виявлення вразливостей та протидії кібератакам у мережах Інтернету речей (IoT), були використані під час аналізу стану інформаційної безпеки мережевої інфраструктури підприємства.

Запропоновані автором методи дозволили:

- 1) здійснити аудит IoT-пристроїв та виявити потенційні вразливості інформаційної інфраструктури;
- 2) підвищити рівень виявлення аномальної мережевої активності та ознак кібератак;
- 3) провести оцінювання ризиків інформаційної безпеки з урахуванням особливостей функціонування IoT-пристроїв;
- 4) сформулювати рекомендації щодо підвищення рівня захищеності мережевої інфраструктури підприємства.

Отримані результати сприяли підвищенню ефективності заходів із забезпечення кібербезпеки та захисту інформаційних ресурсів підприємства.

Директор



Володимир ПЕТУХОВ