

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова праця  
на правах рукопису

ТРУНОВ ОЛЕКСІЙ ІГОРОВИЧ

УДК 004.056:004.89:656.07

## ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ  
ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТРАНСПОРТНО-  
ЛОГІСТИЧНОГО ЦЕНТРУ

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.

Трунов Трунов Олексій Ігорович

Науковий керівник



Дорош Марія Сергіївна  
доктор технічних наук, професор

Чернігів – 2026

## АНОТАЦІЯ

*Трунов О. І.* Інформаційна технологія підтримки прийняття рішень при забезпеченні інформаційної безпеки транспортно-логістичного центру. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю F3 (122) «Комп'ютерні науки» (F (12) – Інформаційні технології). – Національний університет «Чернігівська політехніка», МОН України, Чернігів, 2026.

В роботі вирішено актуальне наукове завдання розробки інформаційної технології комплексної оцінки ризиків інформаційної безпеки, яка враховує параметри та специфічні риси діяльності транспортно-логістичних центрів (ТЛЦ). Розроблені моделі та методи дозволяють інтегрувати сильні сторони існуючих підходів, адаптувати існуючі технології до специфіки галузі, враховувати системні взаємозв'язки та забезпечувати підвищення ефективності в реальних умовах функціонування ТЛЦ.

*Метою* дисертаційного дослідження є підвищення ефективності підтримки прийняття рішень при забезпеченні інформаційної безпеки ТЛЦ шляхом поєднання методів експертної аналітики та використання гнучких адаптивних нейронечітких систем.

*Об'єктом* дослідження є інформаційні процеси управління інформаційною безпекою та підтримки прийняття рішень у транспортно-логістичних системах.

*Предметом* дослідження є моделі, методи та інформаційні технології оцінювання ризиків ІБ, на основі нечіткої логіки та нейромережевих технологій.

Для проведення дослідження були застосовані метод системного аналізу; теорія нечітких множин; метод аналізу ієрархій у нечіткій постановці (Fuzzy АНР); методи обчислювального інтелекту (нейронечіткі мережі ANFIS); методи функціонального та об'єктно-орієнтованого моделювання (IDEF0, DFD, UML); методи алгоритмічної оптимізації (алгоритм Rete); методи математичної статистики та регресійного аналізу.

У вступі обґрунтовано актуальність теми дисертації, визначено мету,

об'єкт, предмет та завдання дослідження. Сформульовано наукову новизну та практичне значення отриманих результатів. Наведено відомості щодо зв'язку роботи з науковими програмами кафедри. Визначено, що в умовах повномасштабної війни та повоєнного відновлення України ТЛЦ є стратегічними об'єктами критичної інфраструктури. Діджиталізація та конвергенція інформаційних (ІТ) та операційних (ОТ) технологій перетворюють їх на пріоритетні цілі для кіберзагроз. Встановлено, що ефективне управління ІБ ТЛЦ ускладнюється критичною інформаційною невизначеністю. Існуючі методи оцінки ризиків часто є фрагментарними, не враховують специфіки ТЛЦ та нечіткість інформації.

*У першому розділі* дисертаційної роботи проведено аналіз ТЛЦ як об'єкта критичної інфраструктури, що мають стратегічне значення для забезпечення національної безпеки. Проаналізовано специфічні бізнес-процеси, архітектуру ІС ТЛЦ та сформовано модель загроз і вразливостей. Доведено, що конвергенція інформаційних та операційних технологій у ТЛЦ створює нові класи кіберзагроз, з якими класичні методи оцінювання ризиків не справляються через високий рівень невизначеності та динамічність процесів. Обґрунтовано необхідність розробки нової інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ, здатної функціонувати в умовах дефіциту ретроспективних даних. Сформульовано завдання дослідження щодо створення інтелектуальних моделей оцінки стану рівня ІБ ТЛЦ.

*У другому розділі* розглянуто концептуальну модель інтегрального оцінювання рівня ризику ІБ ТЛЦ. Вона включає експертну нечітку модель стратегічного аналізу, що базується на трирівневій ієрархії факторів з урахуванням удосконаленого методу нечіткого аналізу ієрархій (Fuzzy ANP) та рівня впевненості експерта. Для проведення стратегічного аналізу запропоновано використання удосконаленої матриці Дж. Х. Вілсона, що, на відміну від класичної, має нечіткі координати з осями рівень ризику та рівень впевненості експертів і є інструментом для вибору стратегії захисту. Розроблена адаптивна нейронечітка модель оцінювання інтегрального рівня ризику ІБ ТЛЦ, яка

базується на системі висновків ANFIS з поліноміальною функцією другого ступеня та вирішує проблему функціонування системи за відсутності ретроспективної вибірки даних із подальшою параметричною оптимізацією моделі засобами нейромережевого навчання. Сформульовано задачу умовної оптимізації керованих факторів захисту на основі символічного аналізу градієнтів, що дозволило здійснити теоретичну інтерпретацію елементів поліноміальної моделі як показників чутливості інтегрального ризику до управлінських впливів.

*У третьому розділі* виконано функціональне моделювання інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ (IDEF0, DFD, IDEF3) та побудовано сценарії взаємодії користувачів за допомогою UML-діаграм. Обґрунтовано використання чотирирівневої багатокомпонентної сервіс-орієнтованої архітектури системи. Описано програмну реалізацію її ключових компонентів: модулів фазифікації, удосконаленого Fuzzy АНР, автоматизованої генерації еталонної бази знань, оптимізації виведення (Rete) та адаптивного ядра ANFIS.

*У четвертому розділі* проведено практичну апробацію та імітаційне моделювання розробленої інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ. На основі 3072 прецедентів підтверджено високу точність нейронечіткої моделі ( $RMSE = 0,0017$ ,  $Accuracy = 95,2\%$ ). Обґрунтовано, що рівень витрат на створення і експлуатацію системи ІБ та рівень культури ІБ мають суттєво вищий коефіцієнт впливу на зниження ризику, ніж технічне переоснащення. Це підтверджує, що розвиток компетенцій персоналу є базовою умовою інформаційної безпеки ТЛЦ. Доведено ефективність методу редукції правил та алгоритму Rete. Для задач експертної оцінки рекомендовано застосовувати базу правил, обсяг якої не перевищує 729. Це забезпечує похибку  $< 1\%$  при мінімальних витратах часу. Для стратегічного планування доцільно застосовувати повну конфігурацію (понад 3000 правил). Розроблено кросплатформний вебзастосунок «SecureFuzzy» із сервіс-орієнтованою архітектурою яка поєднує автономні програмні модулі для забезпечення стратегічного управління ризиками ІБ ТЛЦ та формування сценаріїв захисту.

Наукова новизна полягає у розробці трирівневої ієрархічної моделі класифікації факторів впливу на рівень ризику ІБ ТЛЦ, яка дозволяє системно структурувати та враховувати взаємозалежність різнорідних чинників, специфічних для кіберфізичних систем. Уперше запропоновано концептуальну модель інтегрального оцінювання ризику ІБ, яка базується на інтеграції експертної нечіткої оцінки та адаптивної нейронечіткої системи висновків (ANFIS) з поліноміальною функцією другого порядку, що забезпечує підвищення точності оцінки у динамічному середовищі, та підтримку прийняття рішень з ІБ ТЛЦ. Удосконалено метод Fuzzy АНР, що забезпечує математичну повноту пріоритизації чинників без втрати експертних переваг. Застосування дворівневого алгоритму Rete в архітектурі ІС ППР дозволило суттєво підвищити швидкість аналізу, забезпечуючи підтримку прийняття рішень у режимі реального часу.

Практичне значення роботи полягає у розробці нової інформаційної технології підтримки прийняття рішень, що забезпечує підвищення інформаційної безпеки логістичної інфраструктури ТЛЦ. Технологія дозволяє проводити комплексну оцінку ризиків ІБ, формувати оптимальні стратегії захисту та ефективно пріоритезувати інвестиції в безпеку. Практична реалізація результатів дослідження втілена у комп'ютерній програмі «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів». Вона є інструментом для ІТ-фахівців, що дозволяє автоматизувати аналітичні процедури та підвищувати інформаційну безпеку інформаційних систем ТЛЦ. Розроблений на її основі вебзастосунок «SecureFuzzy» забезпечує підтримку прийняття рішень на етапах стратегічного аналізу ризиків та вибору контрзаходів, що дозволяє компенсувати дефіцит кваліфікованих аналітиків у логістичній галузі.

*Ключові слова:* інформаційна технологія, інформаційна безпека, кібербезпека, транспортно-логістичний центр, система підтримки прийняття рішень, ризик інформаційної безпеки, нечітка логіка, Fuzzy АНР, ANFIS, прескриптивна оптимізація, кіберфізичні системи, сервіс-орієнтована

архитектура.

## ABSTRACT

*Trunov, O. I.* Information Technology for Decision Support in Ensuring Information Security at a Transport and Logistics Center. – Qualifying scientific thesis in manuscript form.

Doctoral dissertation for the degree of Doctor of Philosophy in the specialty F3 (122) «Computer Science» (F (12) – Information Technology). – Chernihiv Polytechnic National University, Ministry of Education and Science of Ukraine, Chernihiv, 2026.

The work addresses the pressing scientific challenge of developing information technology for a comprehensive assessment of information security risks, taking into account the parameters and specific characteristics of the operations of transport and logistics centers (TLCs). The developed models and methods allow for integrating the strengths of existing approaches, adapting existing technologies to the specifics of the industry, accounting for systemic interrelationships, and ensuring increased efficiency under real-world operating conditions of TLCs.

*The aim of* this dissertation research is to improve the effectiveness of decision-making support in ensuring the information security of TLCs by combining expert analytics methods with the use of flexible adaptive neuro-fuzzy systems.

*The object of the study* is the information processes of information security management and decision-making support in transport and logistics systems.

*The subject of the study* is models, methods, and information technologies for assessing information security risks based on fuzzy logic and neural network technologies.

The following methods were used to conduct the research: the method of system analysis; the theory of fuzzy sets; the method of hierarchical analysis in a fuzzy setting (Fuzzy AHP); computational intelligence methods (ANFIS neural networks); functional and object-oriented modeling methods (IDEF0, DFD, UML); algorithmic optimization methods (Rete algorithm); and methods of mathematical statistics and regression analysis.

The introduction justifies the relevance of the dissertation topic and defines the purpose, object, subject, and research objectives. The scientific novelty and practical significance of the obtained results are formulated. Information regarding the connection of the work with the department's research programs is provided. It is determined that, in the context of full-scale war and Ukraine's post-war recovery, logistics centers are strategic critical infrastructure facilities. The digitization and convergence of information (IT) and operational (OT) technologies transform them into priority targets for cyber threats. It has been established that effective information security management of TLCs is complicated by critical information uncertainty. Existing risk assessment methods are often fragmented, do not account for the specifics of TLCs, and fail to address the ambiguity of information.

*The first chapter* of the dissertation analyzes data centers as critical infrastructure objects of strategic importance for ensuring national security. It examines specific business processes and the information security architecture of data centers and develops a model of threats and vulnerabilities. It is demonstrated that the convergence of information and operational technologies in the TLC creates new classes of cyber threats that classical risk assessment methods cannot handle due to the high level of uncertainty and the dynamic nature of the processes. The necessity of developing a new information technology for decision support in ensuring the information security of the TLC, capable of functioning under conditions of a shortage of retrospective data, is substantiated. Research tasks regarding the creation of intelligent models for assessing the state of the TLC's information security level are formulated.

*The second chapter* examines a conceptual model for the integrated assessment of the information security risk level of the TLC. It includes an expert fuzzy model of strategic analysis based on a three-level hierarchy of factors, taking into account the improved Fuzzy AHP method and the expert's level of confidence. For conducting strategic analysis, the use of an improved J. H. Wilson matrix is proposed, which, unlike the classical one, has fuzzy coordinates with axes representing risk level and expert confidence level and serves as a tool for selecting a protection strategy. An adaptive

neuro-fuzzy model for assessing the integral level of information security risk in the TLC has been developed, based on an adaptive neuro-fuzzy inference system (ANFIS) with a second-degree polynomial function, which solves the problem of system operation in the absence of retrospective data samples, followed by parametric optimization of the model using neural network training. The problem of conditional optimization of controllable security factors was formulated based on symbolic gradient analysis, which allowed for a theoretical interpretation of the elements of the polynomial model as indicators of the sensitivity of the integral risk to management influences.

*In the third chapter*, functional modeling of the information technology for decision support in ensuring the information security of the TLC (IDEF0, DFD, IDEF3) was performed, and user interaction scenarios were constructed using UML diagrams. The use of a multi-component service-oriented system architecture was justified. The software implementation of its key components is described: the phasing modules, the improved Fuzzy AHP, the automated generation of a reference knowledge base, inference optimization (Rete), and the adaptive ANFIS core.

*Chapter 4* presents the practical testing and simulation modeling of the developed information technology for decision support in ensuring information security at the Trade and Logistics Center. Based on 3,072 cases, the high accuracy of the neuro-fuzzy model was confirmed ( $RMSE = 0.0017$ ,  $Accuracy = 95.2\%$ ). It is substantiated that the level of costs for creating and operating an information security system and the level of information security culture have a significantly higher impact on risk reduction than technical re-equipment. This confirms that the development of personnel competencies is a fundamental condition for the cyber resilience of the TLC. The effectiveness of the rule reduction method and the Rete algorithm has been demonstrated. For expert assessment tasks, it is recommended to apply a rule base with a size not exceeding 729. This ensures an error rate below 1% with minimal time requirements. For strategic planning, it is advisable to use the full configuration (over 3,000 rules). A cross-platform web application “SecureFuzzy” has been developed with a service-oriented architecture that combines autonomous software modules to ensure strategic management of TLC



information security risks and the formation of protection plans.

The scientific novelty lies in the development of a three-level hierarchical model for classifying factors influencing the level of information security risk in cyber-physical systems, which allows for the systematic structuring and consideration of the interdependence of diverse factors specific to cyber-physical systems. For the first time, a conceptual model for the integrated assessment of information security risk has been proposed, based on the integration of expert fuzzy evaluation and an adaptive neuro-fuzzy inference system (ANFIS) with a second-order polynomial function, which ensures increased assessment accuracy in a dynamic environment, and supports decision-making regarding the information security of the logistics center. The Fuzzy AHP method has been improved, ensuring the mathematical completeness of factor prioritization without losing expert preferences. The application of the two-level Rete algorithm in the architecture of the decision-making support system has significantly increased the speed of analysis, ensuring real-time decision-making support.

The practical significance of this work lies in the development of a new information technology for decision support that enhances the cyber resilience of TLC logistics infrastructure. The technology enables a comprehensive assessment of information security risks, the formulation of optimal protection strategies, and the effective prioritization of security investments. The practical implementation of the research results is embodied in the computer program. It serves as a tool for IT specialists, enabling the automation of analytical procedures and enhancing the cyber resilience of TLC information systems. The “SecureFuzzy” web application, developed on this basis, supports decision-making during the stages of strategic risk analysis and the selection of countermeasures, thereby helping to address the shortage of qualified analysts in the logistics industry.

*Keywords:* information technology, information security, cybersecurity, transport and logistics center, decision support system, information security risk, fuzzy logic, Fuzzy AHP, ANFIS, prescriptive optimization, cyber-physical systems, service-oriented architecture.

## СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

### Наукові публікації, в яких опубліковані основні результати дисертації

1. Modeling of the Information Security Risk of a Transport and Logistics Center Based on Fuzzy Analytic Hierarchy Process / O. Trunov, I. Skiter, M. Dorosh, E. Trunova, M. Voitsekhovska // Mathematical Modeling and Simulation of Systems. MODS 2023. – Cham : Springer, 2024. – Vol. 1091. – P. 306–322. – (Lecture Notes in Networks and Systems). – DOI: [https://doi.org/10.1007/978-3-031-67348-1\\_23](https://doi.org/10.1007/978-3-031-67348-1_23).
2. Simulation of Strategies for Providing Information Security of the Transport and Logistics Center Based on Fuzzy Logic Methods / O. Trunov, M. Dorosh, I. Skiter, E. Trunova, M. Voitsekhovska // Mathematical Modeling and Simulation of Systems. MODS 2024. – Cham : Springer, 2025. – Vol. 1391. – P. 262–281. – (Lecture Notes in Networks and Systems). – DOI: [https://doi.org/10.1007/978-3-031-90735-7\\_21](https://doi.org/10.1007/978-3-031-90735-7_21).
3. Трунов О. Систематизація підходів до оцінки ризиків інформаційної безпеки транспортно-логістичних центрів / О. Трунов, М. Дорош // Технічні науки та технології. – 2025. – № 2(40). – С. 207–220. – DOI: [https://doi.org/10.25140/2411-5363-2025-2\(40\)-207-220](https://doi.org/10.25140/2411-5363-2025-2(40)-207-220).
4. Гребенник А. Алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту / А. Гребенник, О. Трунов // Технічні науки та технології. – 2025. – № 3(41). – С. 158–168. – DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-158-168](https://doi.org/10.25140/2411-5363-2025-3(41)-158-168).
5. Трунов О. І. Архітектура інтелектуальної системи підтримки прийняття рішень для управління інформаційною безпекою транспортно-логістичних центрів / О. І. Трунов, М. С. Дорош // Наука і техніка сьогодні. Серія «Техніка». – 2025. – № 11(52). – С. 2804–2817. – DOI: [https://doi.org/10.52058/2786-6025-2025-11\(52\)-2804-2817](https://doi.org/10.52058/2786-6025-2025-11(52)-2804-2817).

### Наукові праці, які додатково відображають результати дисертації

1. Strategic analysis in the selection of sites for NPP construction based on fuzzy

logic methods / I. Skiter, V. V. Derenhovskyi, O. V. Mykhailov, Ye. A. Menshenin, O. B. Savchuk, O. I. Trunov // Nuclear Power and the Environment. – 2024. – Vol. 31 (3). – P. 12–22. – DOI: <https://doi.org/10.31717/2311-8253.24.3.2>.

2. Свідоцтво про реєстрацію авторського права на твір. Комп'ютерна програма «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів» / О. І. Трунов, М. С. Дорош; авторські майнові права належать Нац. ун-ту «Чернігівська політехніка». – № 143390; дата реєстрації 23.02.2026.

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

1. Дослідження потреб ключових стейкхолдерів для удосконалення логістичних операцій прикордонних регіонів в умовах воєнного часу : аналіт. звіт / В. Маргасова, М. Дорош, А. Дука, А. Приступа, О. Сакун, К. Гнедіна, О. Трунов. – Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2025. – 45 с. – DOI: [https://doi.org/10.54929/analytical\\_report-2025-01](https://doi.org/10.54929/analytical_report-2025-01).
2. Трунов О. І., Дорош М. С. Системи забезпечення інформаційної безпеки для транспортно-логістичних центрів // Математичне та імітаційне моделювання систем. МОДС 2022 : тези доповідей Сімнадцятої міжнар. наук.-практ. конф. (14–16 листоп. 2022 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 7–10. – URL: <http://ir.stu.cn.ua/handle/123456789/26927>.
3. Трунов О. І. Загальна концепція фрактального детектора телекомунікаційного трафіка // Новітні технології у науковій діяльності і навчальному процесі : зб. тез доп. Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених (м. Чернігів, 19–20 квіт. 2023 р.). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 114–116. – URL: <http://ir.stu.cn.ua/handle/123456789/27778>.

4. Trunov O., Dorosh M., Lytvyn S. Ensuring information security when working remotely // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 23) : зб. матеріалів VIII Міжнар. конф. (27–28 квіт. 2023, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 109–113. – URL: <http://ir.stu.cn.ua/handle/123456789/29075>.
5. Трунов О. І., Дорош М. С. Прогнозування рівня ризику інформаційної безпеки транспортно-логістичного центру // Математичне та імітаційне моделювання систем. МОДС 2023 : тези доповідей Вісімнадцятої міжнар. конф. (13–15 листоп. 2023 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 60–65. – URL: <http://ir.stu.cn.ua/handle/123456789/29144>.
6. Trunov O. I. Information and analytical system for management of logistics operations for restoration of border regions // Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства : зб. тез доп. XIV Міжнар. наук.-практ. конф. студентів, аспірантів і молодих вчених (м. Чернігів, 24–26 квіт. 2024 р.). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 1162–1163. – URL: <http://ir.stu.cn.ua/handle/123456789/30262>.
7. Trunov O., Dorosh M., Lytvyn S. Methods of detecting intrusions to computer networks transport and logistics industry // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 24) : зб. матеріалів VIII Міжнар. конф. (27–28 квіт. 2024, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 132–135. – URL: <http://ir.stu.cn.ua/handle/123456789/30881>.
8. Трунов О. І., Дорош М. С. Генетичний алгоритм в логістиці: оптимізація маршрутів // Математичне та імітаційне моделювання систем. МОДС 2024 : тези доповідей Дев'ятнадцятої міжнар. наук.-практ. конф. (11–13 листоп. 2024 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 64–67. – URL: <https://ir.stu.cn.ua/handle/123456789/31373>.

9. Трунов О. І., Суботін І. Л. Розробка сучасної інформаційної системи забезпечення волонтерської діяльності // Математичне та імітаційне моделювання систем. МОДС 2024 : тези доповідей Дев'ятнадцятої міжнар. наук.-практ. конф. (11–13 листоп. 2024 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 57–60. – URL: <https://ir.stu.cn.ua/handle/123456789/31373>.
10. Trunov O. I. Decision support system for ensuring information security of a transport and logistics center // Юність науки – 2025 : зб. тез доп. XIV Міжнар. наук.-практ. конф. студентів, аспірантів і молодих вчених (м. Чернігів, 23–25 квіт. 2025 р.). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 1162–1163. – URL: <http://ir.stu.cn.ua/handle/123456789/32545>.
11. Trunov O., Dorosh M. Ensuring information security in the transportation of nuclear // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 25) : зб. матеріалів X Міжнар. конф. (25–26; 29–30 квіт. 2025, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 109–113. – URL: <https://ir.stu.cn.ua/handle/123456789/33540>.
12. Dorosh M., Trunov O., Sharovara O. Indirect impact factors in assessing information security risks of logistics operations in border regions // Управління проєктами у розвитку суспільства : зб. матеріалів XXII Міжнар. наук.-практ. конф. (м. Київ, 23 трав. 2025 р.). – Київ : КНУБА, 2025. – С. 20–23. – URL: <https://er.chdtu.edu.ua/bitstream/ChSTU/4632/1/%D0%A2%D0%B5%D0%B7%D0%B8%20%D0%9A%D0%B8%D1%96%CC%88%D0%B2-2023.pdf>.
13. Туревський Д., Трунов О. Автоматизація генерації повної бази нечітких правил для моделі оцінки ризиків ІБ // Математичне та імітаційне моделювання систем. МОДС 2025 : тези доповідей Двадцятої міжнар. конф. (10–12 листоп. 2025 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 64–67. – URL: <https://ir.stu.cn.ua/handle/123456789/33857>.

## ЗМІСТ

АНОТАЦІЯ.....	2
ABSTRACT.....	6
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	16
ВСТУП.....	17
РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТРАНСПОРТНО- ЛОГІСТИЧНОГО ЦЕНТРУ .....	24
1.1. Транспортно-логістичний центр як складний об'єкт інформатизації та захисту.....	24
1.2. Сучасні підходи до оцінки рівня інформаційної безпеки .....	37
1.3. Проблема невизначеності в задачах оцінки стану інформаційної безпеки ТЛЦ.....	46
1.4. Аналіз існуючих моделей оцінки ризиків ІБ .....	48
1.5. Постановка задачі дослідження .....	52
Висновки до розділу 1 .....	55
РОЗДІЛ 2. МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТРАНСПОРТНО-ЛОГІСТИЧНОГО ЦЕНТРУ .....	57
2.1. Концептуальна модель інтегрального оцінювання рівня ризику ІБ ТЛЦ ...	57
2.2. Експертна нечітка модель стратегічного аналізу факторів ризику ІБ ТЛЦ	64
2.3. Адаптивна нейронечітка модель оцінювання інтегрального рівня ризику ІБ ТЛЦ.....	88
2.4. Оптимізація та стратегічне управління ризиками ІБ ТЛЦ .....	96
Висновки до розділу 2 .....	102
РОЗДІЛ 3. ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІБ ТЛЦ.....	104
3.1. Функціональне моделювання процесів підтримки прийняття рішень .....	104
3.2. Моделювання сценаріїв взаємодії користувачів мовою UML .....	111
3.3. Обґрунтування та розробка архітектури інформаційної технології .....	116
3.4. Програмна реалізація компонентів інформаційної технології підтримки	

прийняття рішень при забезпеченні ІБ ТЛЦ.....	123
Висновки до розділу 3 .....	144
РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ВЕРИФІКАЦІЯ АДАПТИВНОЇ НЕЙРОНЕЧІТКОЇ МОДЕЛІ .....	146
4.1. Експериментальна верифікація та структурний аналіз моделі.....	146
4.2. Аналіз архітектурної масштабованості та обчислювальної ефективності	156
4.3. Дослідження адаптивних властивостей системи в умовах зміни стратегічних пріоритетів.....	159
4.4. Прескриптивна аналітика та оптимізація стратегій захисту.....	169
4.5. Програмна реалізація інформаційної технології підтримки прийняття рішень.....	171
Висновків до розділу 4 .....	177
ВИСНОВКИ .....	179
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	181
ДОДАТКИ .....	198

## ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ANFIS (Adaptive Neuro-Fuzzy Inference System) – адаптивна нейронечітка система висновків

APT (Advanced Persistent Threat) – розвинена стала загроза

ERP (Enterprise Resource Planning) – планування ресурсів підприємства

ICS (Industrial Control Systems) – промислові системи управління

IDS (Intrusion Detection System) – система виявлення вторгнень

IoT (Internet of Things) – інтернет речей

IPS (Intrusion Prevention System) – система запобігання вторгненням

IT (Information Technology) – інформаційні технології

OT (Operational Technology) – операційні технології

SCADA (Supervisory Control and Data Acquisition) – диспетчерське управління та збір даних

SIEM (Security Information and Event Management) – управління інформацією та подіями безпеки

TMS (Transport Management System) – система управління транспортом

WMS (Warehouse Management System) – система управління складом

БД – база даних

БЗ – база знань

ЖЦ – життєвий цикл

ІБ – інформаційна безпека

ІТ ППР – інформаційна технологія підтримки прийняття рішень

ПЗ – програмне забезпечення

СППР – система підтримки прийняття рішень

ТЛЦ – транспортно-логістичний центр



## ВСТУП

**Актуальність теми дослідження.** В умовах глобалізації та сучасних геополітичних викликів транспортно-логістичні центри (ТЛЦ) це не просто ключові вузли економіки, а й стратегічні об'єкти критичної інфраструктури. Їхня роль набуває особливої ваги в контексті повномасштабної війни в Україні, де вони забезпечують життєво важливі функції: постачання для сил оборони, доставку гуманітарної допомоги, підтримку економічної стійкості тилу та функціонування експортно-імпортних операцій. Водночас ТЛЦ є невід'ємною складовою післявоєнного відновлення територій, забезпечуючи логістику для відбудови інфраструктури та реінтеграції економіки постраждалих регіонів.

Діджиталізація сучасних ТЛЦ перетворює їх на інтегровані інформаційні системи, що робить їх пріоритетною ціллю для кіберзагроз, активність яких значно посилюється в умовах війни. Атаки на ІС ТЛЦ, включаючи програми-вимагачі, злам систем управління (ІТ/ОТ), атаки на ланцюги поставок та витік даних, можуть призвести до повного паралічу логістичних операцій, підриваючи не лише економіку, а й національну безпеку і обороноздатність. Забезпечення ІБ ТЛЦ стає критично важливим елементом не тільки для їхньої поточної діяльності, але й для сталого розвитку країни та її здатності до ефективного відновлення.

Управління ІБ ТЛЦ ускладнюється високим ступенем невизначеності, що загострюється в умовах війни (неповнота даних, нечіткість експертних оцінок, цілеспрямовані атаки державних акторів). Існуючі методи оцінки ризиків часто є фрагментарними, неадаптованими до специфіки ІТ/ОТ-конвергенції в ТЛЦ та погано враховують нечіткість інформації. Це створює значні труднощі у прийнятті обґрунтованих рішень щодо захисту.

Застосування інтелектуальних підходів, зокрема теорії нечітких множин та нейронечітких систем, дозволяє адекватно моделювати та обробляти цю невизначеність. Розробка ІТ ППР, яка б комплексно здійснювала стратегічний аналіз в специфічних умовах функціонування ТЛЦ (включаючи воєнний стан та

завдання відновлення), є актуальним науковим завданням, що має важливе значення для безпеки, стійкості та сталого розвитку України.

Загальні аспекти інформаційної безпеки та кіберзахисту ґрунтовно досліджені у працях В. Л. Бурячка, В. Б. Толубка, В. О. Хорошка та Б. Шнайєра (B. Schneier). Специфіка оцінювання ризиків у транспортно-логістичній галузі та розробки галузевих систем підтримки прийняття рішень висвітлена у роботах Ю. О. Васютинської, О. Мельниченка, Б. Гюнеша (B. Gunes), П. Болата (P. Bolat) та Л. Ляна (L. Liang).

Питання інтелектуалізації процесів захисту на основі апарату нечіткої логіки, експертних систем та нейромережових моделей (ANFIS) опрацьовані у дослідженнях О. Кочеткова, І. Карпович, О. Гладка, а також В. Соколова (V. Sokolov), Б. Гіти (B. Ghita) та Ц. Танга (J. Tang). Методологічне підґрунтя багатокритеріального аналізу (Fuzzy AHP, Fuzzy SAW) для пріоритизації ризиків закладено Д. Чангом (D. Y. Chang), Дж. Баклі (J. J. Buckley), А. Нассером (A. Nasser) та А. Ганіним (A. A. Ganin). Використання моделей стратегічного аналізу (зокрема матриці Дж. Х. Вілсона) як інструменту інтерпретації результатів моделювання та планування інвестицій у безпеку досліджували Р. Гоел (R. Goel), А. Кумар (A. Kumar) та Ч. З. Ту (C. Z. Tu). Удосконалення підходів до інтеграції нечітких оцінок ризику (Fuzzy AHP, ANFIS) та інструментів стратегічного аналізу є актуальним питанням, що потенційно дозволить покращити якість прийняття управлінських рішень в ІБ.

Отже, актуальним науковим завданням є розробка нової, комплексної та адаптованої методики оцінки ризиків ІБ, спеціально призначеної для ТЛЦ. Вона має інтегрувати сильні сторони існуючих підходів, але водночас бути адаптованою до специфіки галузі, враховувати системні взаємозв'язки та бути більш ефективною в реальних умовах функціонування ТЛЦ.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційна робота виконана в рамках державного проєкту прикладного дослідження «Розробка інформаційно-аналітичної системи управління

логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки» № 0124U000696 та відповідно до плану науково-дослідної роботи Національного університету «Чернігівська політехніка» – «Системний аналіз інформаційних процесів управління логістичною діяльністю» (№0124U003344).

**Мета і завдання дослідження.** *Метою* дисертаційного дослідження є підвищення ефективності підтримки прийняття рішень при забезпеченні інформаційної безпеки ТЛЦ шляхом поєднання методів експертної аналітики та використання гнучких адаптивних нейронечітких систем.

Для досягнення поставленої мети були сформульовані наступні завдання дослідження:

1. Проаналізувати специфіку ТЛЦ як об'єктів критичної інфраструктури, класифікувати загрози ІБ з урахуванням воєнних ризиків, дослідити існуючі підходи до оцінки ризиків та обґрунтувати доцільність розробки ІТ ППР при забезпеченні безпеки в умовах високої невизначеності.

2. Розробити ієрархічну модель факторів ризику ІБ ТЛЦ та метод їх пріоритизації на основі вдосконаленого алгоритму Fuzzy АНР, що забезпечить усунення проблеми нульових ваг та математичну повноту експертних оцінок.

3. Розробити адаптивну нейронечітку модель оцінювання інтегрального рівня ризику ІБ ТЛЦ на основі інтеграції виводу Mamdani (для автоматичного формування початкової бази знань) та системи ANFIS з поліноміальною апроксимацією, що забезпечить високу швидкодію обчислень у режимі реального часу.

4. Розробити архітектуру та реалізувати інформаційну технологію, що інтегрує розроблені моделі та включає модулі оцінки ризику, оптимізації керованих факторів для досягнення цільового рівня безпеки та стратегічного аналізу ефективності заходів.

5. Провести експериментальне дослідження розробленої інформаційної технології для перевірки узгодженості експертних оцінок, валідації моделі оцінки

ризиків та апробації функціональних можливостей системи в контексті типових сценаріїв для ТЛЦ.

*Об'єктом дослідження* є інформаційні процеси управління інформаційною безпекою та підтримки прийняття рішень у транспортно-логістичних системах.

*Предметом дослідження* є моделі, методи та інформаційні технології оцінювання ризиків ІБ, на основі нечіткої логіки та нейромережових технологій.

**Методи дослідження.** Метод системного аналізу, теорія нечітких множин, метод аналізу ієрархій у нечіткій постановці (Fuzzy AHP), методи обчислювального інтелекту (нейронечіткі мережі ANFIS), методи функціонального та об'єктно-орієнтованого моделювання (IDEF0, DFD, UML), методи алгоритмічної оптимізації (алгоритм Rete), методи математичної статистики та регресійного аналізу.

#### **Наукова новизна одержаних результатів:**

Вперше розроблено:

- трирівнева ієрархічна модель класифікації факторів, що впливають на рівень ризику ІБ ТЛЦ, яка дозволяє системно структурувати та враховувати взаємозалежність різнорідних чинників, специфічних для кіберфізичних систем транспортно-логістичних центрів;
- модель інтегрального оцінювання ризику інформаційної безпеки, яка базується на інтеграції експертної нечіткої оцінки та адаптивної нейронечіткої системи висновків (ANFIS) з поліноміальною функцією другого порядку, що забезпечує підвищення точності оцінки у динамічному середовищі, та підтримку прийняття рішень з ІБ ТЛЦ.

Удосконалено:

- метод Fuzzy AHP для пріоритезації факторів ризику ІБ ТЛЦ, що дозволяє більш точно враховувати нечіткі експертні оцінки при визначенні важливості чинників і, на відміну від існуючих, містить поєднання підходів Чанга та Баклі із введенням коефіцієнта впевненості експерта, що дозволяє підвищувати об'єктивність оцінювання.

Набуло подальшого розвитку:

- метод обробки правил нечіткого виводу за рахунок дворівневого застосування алгоритму Rete в архітектурі адаптивної нейронечіткої системи висновків, що дозволяє збільшити швидкість обчислення при оцінці ризиків ІБ.

**Практичне значення отриманих результатів** полягає в тому, що комплекс запропонованих наукових підходів формує нову інформаційну технологію підтримки прийняття рішень при забезпеченні ІБ ТЛЦ. Це надає змогу забезпечувати суттєве підвищення інформаційної безпеки логістичної інфраструктури, що є критично важливим для національної безпеки, сталого економічного розвитку та ефективного відновлення країни в умовах сучасних викликів. Технологія дозволяє проводити комплексну оцінку ризику ІБ, підтримувати прийняття рішень щодо вибору оптимальних стратегій захисту та пріоритезувати інвестиції в заходи безпеки.

Розроблена комп'ютерна програма «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів» (Свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму) № 143390 від 23 лютого 2026 р.) надає практичний інструмент ІТ-фахівцям ТЛЦ для проведення регулярного моніторингу та підвищення інформаційної безпеки критичних інформаційних систем.

Розроблений вебзастосунок «SecureFuzzy» для підтримки прийняття рішень автоматизує управління ІБ на етапах стратегічного аналізу та оцінювання ризиків ІБ, прийняття рішень, щодо вибору контрзаходів. Впровадження системи дозволяє компенсувати дефіцит кваліфікованих аналітиків у невеликих логістичних центрах.

**Результати дисертаційного дослідження впроваджені:**

- в ТОВ «СІБЕРТРАНС» при розробці трирівневої моделі класифікації загроз, адаптації нейронечіткої системи ANFIS до реальних даних підприємства та використанні результатів моделювання для формування оптимального вектора контрзаходів, що дозволило підвищити рівень інформаційної безпеки

транспортно-логістичного центру за рахунок досягнення точності розпізнавання загроз (акт про впровадження наукових результатів № 26/03 від 26.03.2026 р.).

- при виконанні державного проекту прикладного дослідження «Розробка інформаційно-аналітичної системи управління логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки» № 0124U000696. Зокрема, у межах зазначеного проекту було впроваджено адаптивну нейронечітку модель для оперативного моніторингу станів транспортно-логістичних центрів в умовах високої невизначеності, що дозволило підвищити стійкість управління логістичними процесами при відновленні інфраструктури. Використання методів штучного інтелекту забезпечило можливість автоматизації аналізу ризиків та дозволило здійснювати прескриптивну оптимізацію захисних заходів відповідно до стратегічних пріоритетів національної безпеки (довідка про впровадження № 202/08-512 від 24.03.2026 р.).
- в освітній процес Національного університету «Чернігівська політехніка» на кафедрі інформаційних технологій та програмної інженерії. Зокрема, матеріали роботи використано при розробці та викладанні навчальних дисциплін: «Операційні системи. Частина 1», «Системи штучного інтелекту», «Кодування та захист інформації», «Системи захисту обчислювальних мереж», «Моделювання, аналіз та інструментальні засоби інформаційної безпеки» для здобувачів ступенів бакалавра та магістра зі спеціальності F2 (121) «Інженерія програмного забезпечення». Також результати дисертації включено до змісту дисципліни «Моделі та методи інформаційної безпеки інженерії програмного забезпечення» для підготовки аспірантів за цією ж спеціальністю (довідка про впровадження № 202/08-518 від 23.03.2026 р.).

**Особистий внесок здобувача.** Наукові результати, викладені у дисертаційній роботі, отримані автором особисто. У наукових працях, опублікованих у співавторстві, для дисертаційного дослідження використано

лише ті ідеї, концептуальні положення та обчислювальні алгоритми, що є результатом самостійної наукової діяльності автора.

**Апробація результатів дисертації.** Основні положення дисертаційного дослідження доповідались та обговорювались на: Міжнародній науково-практичній конференції «Математичне та імітаційне моделювання систем. МОДС» (Чернігів, 2022, 2023, 2024, 2025); Всеукраїнській науково-практичній конференції «Новітні технології у науковій діяльності і освітньому процесі» (Чернігів, 2023); Міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO)» (Славутич, 2023, 2024, 2025); Міжнародній науково-практичній конференції «Юність науки» (Чернігів, 2024, 2025); Міжнародній науково-практичній конференції «Управління проєктами у розвитку суспільства. Тема: «Управління проєктами післявоєнної розбудови України»» (Київ, 2025).

**Публікації.** За темою дисертаційного дослідження з викладом основного матеріалу було опубліковано 19 наукових праць, серед них 5 статей у наукових фахових виданнях України (із них 2 статті опубліковано у виданнях, що індексуються у міжнародних наукометричних базах Scopus та Web of Science), 1 свідоцтво про реєстрацію авторського права на комп'ютерну програму, 14 праць апробаційного характеру (тези доповідей на міжнародних та всеукраїнських науково-практичних конференціях).

**Структура та обсяг роботи.** Дисертаційна робота складається з переліку умовних скорочень, вступу, 4 розділів, висновків, списку використаних джерел з 134 найменувань та 6 додатків на 51 сторінці. Обсяг роботи становить 248 сторінок, основний текст – 164 сторінки, 51 рисунок, 36 таблиць.

## **РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТРАНСПОРТНО- ЛОГІСТИЧНОГО ЦЕНТРУ**

### **1.1. Транспортно-логістичний центр як складний об'єкт інформатизації та захисту**

Транспортно-логістичні центри є основними системоутворюючими елементами транспортно-логістичних систем, що забезпечують скоординовану взаємодію всіх учасників, а також інтеграцію транспортних, товаро-матеріальних, сервісних, інформаційних та фінансових потоків [1], [2]. Єврокомісія визначає ТЛЦ як певну територію, на якій усі види діяльності, пов'язані з транспортуванням, логістикою та дистрибуцією товарів, здійснюються різними операторами [3].

Для більш точного академічного аналізу, ТЛЦ визначається як багатофункціональний інфраструктурний комплекс та спеціалізована економічна зона, що об'єднує на єдиній території сукупність незалежних логістичних, транспортних, митних та допоміжних компаній, а також обов'язковий вантажний термінал з метою оптимізації та розподілу вантажних потоків [4].

З точки зору інформаційних технологій ТЛЦ будемо розглядати як складну кіберфізичну систему, де ефективність управління вантажопотоками безпосередньо залежить від цілісності та доступності даних у системах WMS та TMS.

Сучасний ТЛЦ виконує функції транспортно-розподільчого логістичного комплексу з широким спектром надання послуг (рис. 1.1). Це комплекс інженерно-технічних споруд розміщений у вузлах транспортної мережі, із сучасним технологічним обладнанням, що інтегрує логістичні, митні, фінансові та сервісні модулі.



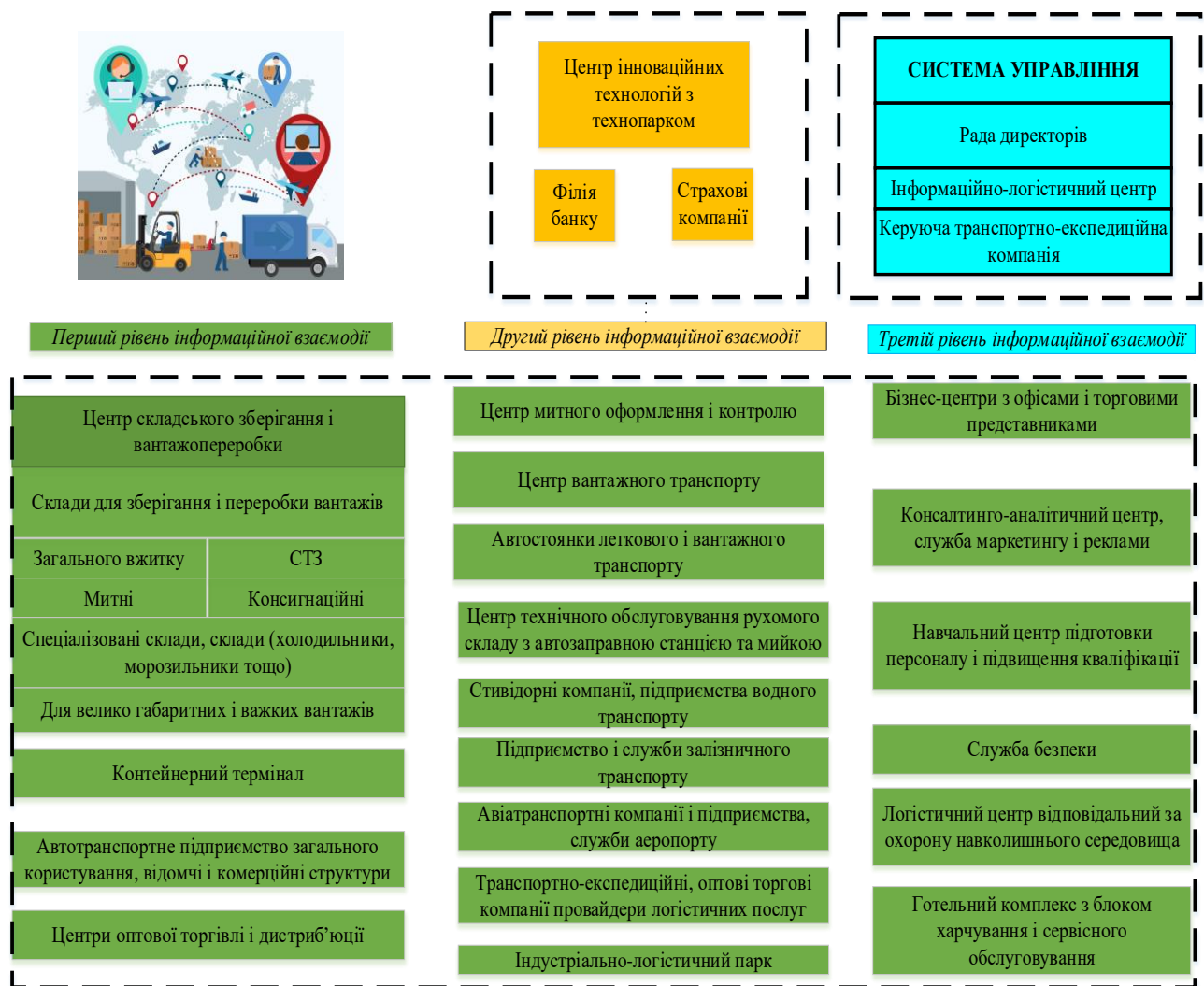


Рисунок 1.1 – Функціональна структура ТЛЦ з урахуванням рівнів інформаційної взаємодії

Кожен з функціональних елементів структури ТЛЦ має відповідний рівень інформаційної взаємодії [5].

*Перший рівень* – поточної робочої оперативної інформації. Це повторювана, передбачувана інформація, що часто оновлюється:

- заявки (прямі та форвардні);
- рахунки до вкладів та розрахунків;
- бухгалтерський облік;
- отримання довідок тощо.

*Другий рівень* – оперативної тактичної інформації, де аналогічні категорії

інформації групуються у функціональні одиниці, що дозволяє забезпечити:

- створення логічно замкнутої інформаційної картини кожного елементарного процесу;
- керування діловими операціями;
- визначення ступеня контролю достовірності інформації.

*Третій рівень* – стратегічної інформації. Містить відомості для керівництва, які дозволяють здійснювати довгострокове планування бізнес-процесів, що відбуваються в інформаційному просторі, та розробляти політику впливу на них.

Ефективне функціонування сучасного ТЛЦ неможливе без глибокої інформатизації ключових бізнес-процесів. Цифрова трансформація охоплює всі етапи логістичного ланцюга, від планування до аналітики. Основні компоненти та цифрові інновації, що формують архітектуру інформаційної системи ТЛЦ, та їхні основні функції представлені в табл. 1.1.

Таблиця 1.1 – Основні компоненти та цифрові інновації, що формують архітектуру ІС ТЛЦ, та їхні основні функції

Компонент ІС ТЛЦ	Функціональне призначення та вплив на бізнес-процеси
Системи управління маршрутизацією (внутрішні та міжнародні)	Оптимізація часу та собівартості транспортування. Ефективне призначення завдань водіям для дотримання графіків доставки. Побудова оптимальних маршрутів для складних мультимодальних схем.
Телематичні системи моніторингу (GPS/GPRS)	Надання даних про місцезнаходження та стан транспорту в реальному часі. Мінімізація ризиків затримок та збоїв у логістичному процесі.
Системи управління ресурсами (Складом/Транспортом)	Забезпечення раціонального розподілу вантажних місць у транспортних засобах. Зниження транспортних витрат через мінімізацію втрат корисного простору.
Системи бізнес-аналітики (BI Systems)	Аналіз ефективності експлуатації автопарку. Підвищення точності калькуляції та розрахунку експлуатаційних витрат.
Системи стратегічного аналізу	Моделювання та розробка довгострокових стратегій розвитку. Адаптація маршрутної мережі до змін ринкових умов.

Як видно з табл. 1.1 критична інфраструктура ТЛЦ глибоко залежить від коректної та безперебійної роботи цих інтегрованих цифрових систем. Кожна з цих інновацій є як інструментом підвищення ефективності, так і потенційним об'єктом захисту та вектором для кібератак.

Компрометація «Системи планування маршрутів» або «GPS/GPRS-моніторингу» може призвести до зриву поставок, фізичної втрати чи перехоплення вантажів. В умовах воєнних дій це створює пряму загрозу для доставки військової та гуманітарної допомоги.

Злам «Системи оптимізації завантаження» може спричинити фінансові збитки та операційний хаос на складах.

Несанкціоноване втручання в «Аналітичні системи» або «Систему стратегічного планування» може спотворити дані для прийняття управлінських рішень, що призведе до невірних стратегій розвитку.

Отже, глибока інформатизація бізнес-процесів ТЛЦ та конвергенція ІТ/ОТ-систем формують складну поверхню атаки, що підкреслює гостру актуальність розробки спеціалізованої інформаційної технології підтримки прийняття рішень. Оцінка рівня захищеності такого складного об'єкта неможлива без врахування надійності кожного окремого механізму захисту.

Спираючись на аналіз напрямків діяльності ТЛЦ, можна деталізувати ключові бізнес-процеси та їх ІС-компоненти, що обробляють критичні дані (табл. 1.2).

Таблиця 1.2 – Аналіз ключових бізнес-процесів ТЛЦ, їх інформаційних систем та критичних даних

Напрямок діяльності	Процеси	Системи та технології	Критичні дані
1. Управління складом	Приймання, розміщення, крос-докінг, управління запасами, комплектація (pick-by-voice/light/vision), відвантаження.	WMS, IoT, RFID, AS/RS, AGV.	Точні операційні дані про запаси, локації, замовлення, терміни придатності. Компрометація WMS може зупинити операції складу.
2. Управління транспортуванням	Планування маршрутів, відстеження вантажів (вкл. митний е-документообіг), управління автопарком, доставка «останньої милі».	TMS, телематика (GPS/IoT), мобільні додатки, API з біржами.	Конфіденційні логістичні дані: маршрути, графіки, клієнти, водії. Несанкціонована модифікація даних може призвести до крадіжки.
3. Управління ланцюгами	Прогнозування попиту, автоматизація	Платформи SCM, AI/ML для	Стратегічна комерційна інформація: постачальники,

Напрямок діяльності	Процеси	Системи та технології	Критичні дані
поставок	замовлень, забезпечення наскрізної видимості (end-to-end visibility) ланцюга.	прогнозування, EDI, API з постачальниками, IoT.	ціни, обсяги, контракти.
4. Клієнтський сервіс та внутрішні операції	Надання клієнтам доступу до даних (замовлення, відстеження), внутрішній документообіг, управління фінансами та персоналом.	Онлайн-портали, мобільні додатки, CRM, чат-боти (AI), СЕД, хмарні сервіси.	Персональні дані клієнтів, комерційна інформація (замовлення, платежі), внутрішня конфіденційна інформація (фінанси, дані співробітників).

Компоненти описані в таблиці 1.1 формують складну кіберфізичну систему, в якій відбувається глибока конвергенція IT/OT. Наприклад, команда з WMS (IT) безпосередньо ініціює фізичний рух на складі через AGV або AS/RS (OT). Ця тісна взаємодія між цифровим та фізичним рівнями створює специфічні вектори атак, адже компрометація IT-системи (наприклад, TMS) може призвести до несанкціонованих фізичних дій (зміна маршруту, помилкове завантаження тощо).

Окрім внутрішньої інтеграції, архітектура ІС ТЛЦ характеризується високим ступенем зовнішньої інтеграції. Вона нерозривно пов'язана з інформаційними системами десятків та сотень третіх сторін:

- партнери та постачальники (обмін даними через EDI та API в межах SCM);
- державні органи (інтеграція з митними службами для електронного декларування);
- фінансові установи (обмін даними з банками).

Ця розподілена архітектура означає, що периметр безпеки ТЛЦ є розмитим, а ризики ланцюга поставок (SCRM) стають одними з найбільш критичних, оскільки атака на менш захищеного партнера може надати прямий доступ до ключових систем ТЛЦ [6].

Актуальність дослідження ТЛЦ як критичних вузлів підтверджується аналізом динаміки вантажних перевезень в Україні за 2023–2024 роки [7], [8] (рис. 1.2).

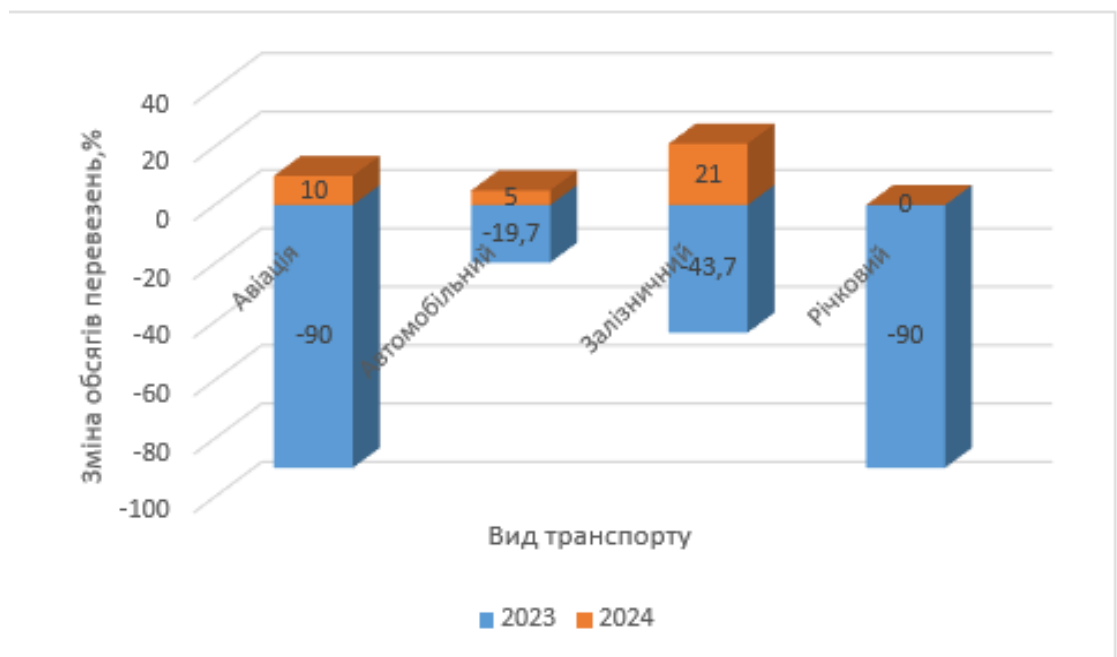


Рисунок 1.2 – Динаміка обсягів перевезень в Україні за 2023–2024 роки за видами транспорту

Воєнний стан призвів до докорінної трансформації транспортної системи. Діаграма демонструє, що після критичного спаду у 2023 році, спричиненого безпековими ризиками та блокуванням кордонів, 2024 рік став періодом адаптації та відновлення для ключових видів транспорту. Залізничний транспорт, як основа логістичної безпеки країни, продемонстрував зростання на 21%, взявши на себе основний тягар експортно-імпортних операцій. Водночас авіаційні та річкові перевезення залишаються на мінімальному рівні через закритий повітряний простір та мінну небезпеку.

Така нерівномірність розвитку створює асиметричні ризики для ТЛЦ:

- ТЛЦ залізничного та автомобільного профілю зазнають пікових навантажень, що робить їхні інформаційні системи критичними мішенями для кібератак спрямованих на зрив логістики;
- ТЛЦ авіаційного та морського профілю функціонують в режимі консервації або обмеженої дієздатності, де пріоритетом стає фізичне збереження інфраструктури та даних для майбутнього відновлення.

В контексті ІБ, особливо в період воєнних дій та післявоєнного відновлення, неможливо аналізувати ТЛЦ як монолітний об'єкт. Класичні класифікації, хоч і є ґрунтовними, але орієнтовані на операційну діяльність у мирний час. Вони не враховують стратегічні та кіберфізичні загрози, що є ключовими для нашого дослідження [9].

З огляду на це, пропонується багатовимірна класифікація ТЛЦ, яка розширює загальноприйняті таксономії новими класифікаційними ознаками, що є критично важливими для аналізу ризиків ІБ у логістичних системах (Додаток В). Визначальними для оцінки стану ІБ ТЛЦ є:

1. Геостратегічна ознака. Це фундамент для оцінки рівня ІБ, оскільки в умовах воєнного стану територіальне розташування визначає інтенсивність та характер атак. Західні ТЛЦ фокусуються на забезпеченні цілісності даних у ланцюгах міжнародних поставок. Основним ризиком є АРТ-атаки на митні ІТ-системи. Форпостні ТЛЦ (зокрема прикордоння Чернігівської області) характеризуються гібридною моделлю загроз. Забезпечення ІБ вимагає протидії засобам РЕБ, що блокують GPS-моніторинг, та захисту локальної інфраструктури від фізичних диверсій. Прифронтові ТЛЦ – пріоритетом є відмовостійкість, тобто здатність системи до миттєвого відновлення даних після кіберкінетичних ударів.

2. Технологічна модальність. Ознака визначає технологічну складність об'єкта та ступінь кіберфізичної конвергенції. Мультимодальні ТЛЦ вимагають захисту гетерогенних мереж, що інтегрують дані різних видів транспорту [10], [11]. Інтермодальні ТЛЦ мають найвищий рівень ризику через глибоку інтеграцію ІТ-систем з операційними технологіями. Тут компрометація цифрового коду може призвести до фізичних аварій роботизованого обладнання (на кшталт кранів, AGV-роботів) [12].

3. Інфраструктурний масштаб. Ознака визначає ієрархічне положення вузла у логістичній мережі (від міжнародних хабів до малих периферійних вузлів) та потенційний обсяг каскадних наслідків у разі успішної атаки. Глобальні хаби є цілями для державних акторів через масштабний вплив на національну економіку.

Периферійні прикордонні вузли є стратегічно важливими для транскордонної логістики. У них спостерігається брак ресурсів на захист ІБ, що створює загрозу проникнення в централізовані державні та корпоративні мережі через їх менш захищені канали.

На сьогодні спостерігається тенденція до створення малих спеціалізованих ТЛЦ на прикордонних територіях, що є стратегічно виправданим як з логістичних, так і з безпекових позицій. Обмеження спектра послуг та потужності окремого вузла зменшують поверхню кібератак та мінімізують вплив на національну логістичну мережу у разі компрометації об'єкта. Таким чином, децентралізація інфраструктури ТЛЦ виступає архітектурним рішенням у сфері безпеки, спрямованим на підвищення загальної стійкості системи.

Для проведення дослідження обрано регіональні прифронтові мультимодальні ТЛЦ, що обумовлено їх критичною роллю у забезпеченні транскордонної логістики та у задачах повоєнного відновлення територій.

Проведений аналіз потреб ключових стейкхолдерів прикордонних регіонів виявив гострий дефіцит інструментів забезпечення ІБ адаптованих до умов ресурсної обмеженості та високої невизначеності [13].

Аналіз інформаційних потоків ТЛЦ представлений на рисунку 1.3 ілюструє високий ступінь інтеграції бізнес-систем (CRM, ERP) та операційних технологій (GPS, WMS, АСУ перевізників).

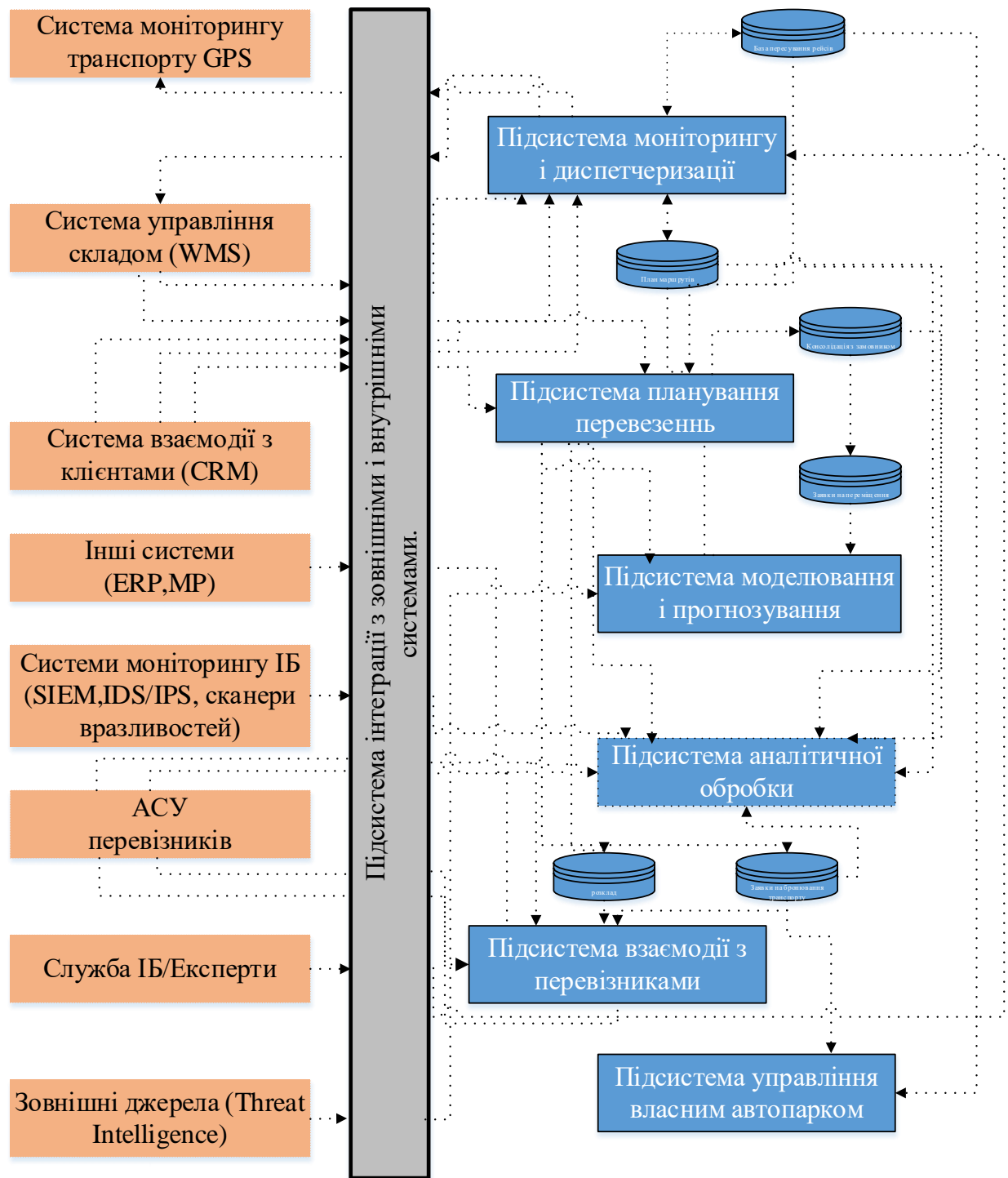


Рисунок 1.3 – Модель інформаційної взаємодії в системі ТЛЦ як об'єкта захисту

При цьому представлена модель ілюструє фундаментальну проблему архітектурного розриву.

З лівого боку моделі представлені джерела, які формують повний спектр даних: чітко структуровані операційні метрики (GPS-координати, статуси WMS),



метрики специфічної природи – події безпеки (SIEM), індикатори компрометації та нечіткі експертні оцінки.

Права частина моделі це функціональні блоки ІС ТЛЦ. Вона вказує на те, що існуючі підсистеми (планування, диспетчеризації) спроектовані виключно для обробки детермінованих логістичних даних і нездатні сприймати стохастичну природу даних ІБ та працювати з невизначеністю.

Фактично, критично важливі для захисту потоки від SIEM та експертів ігноруються на рівні прийняття рішень, оскільки в діючих ІС ТЛЦ відсутній модуль для їх семантичної обробки та агрегації.

Таким чином, відсутність у стандартній архітектурі єдиного центру консолідації, здатного поєднати «жорстку» логіку операційних процесів з «м'якими» обчисленнями ризиків безпеки, унеможливорює адекватну реакцію на інциденти. В умовах конвергенції ІТ/ОТ систем та розмитого периметра це робить ТЛЦ вразливим до специфічних кіберкінетичних атак, які маскуються під легітимні операційні процеси.

Виявлений розрив обґрунтовує необхідність розробки нової ІТ ППР. Перш ніж створювати механізми захисту, необхідно формалізувати саму природу деструктивних впливів. Це визначає першочергову задачу дослідження: розробити модель загроз та вразливостей ІБ, специфічну для транспортно-логістичної галузі. Саме ця модель дозволить систематизувати вектори атак на всіх рівнях взаємодії та стане базисом для подальшої розробки методу кількісного оцінювання рівня ІБ ТЛЦ.

Аналіз останніх галузевих досліджень та звітів (зокрема, GatePoint Research) показує, що транспортно-логістичні організації вважають упередження загроз кібербезпеки своєю щоденною проблемою номер один (81%) [14].

Ключовими проблемами у сфері мережевої безпеки в галузі є:

- загрози програм-вимагачів (Ransomware) та шкідливого програмного забезпечення (77% респондентів);
- забезпечення дотримання політик безпеки (66%);

- контроль віддаленого доступу (64%) [15];
- нестача кваліфікованих ІТ-кадрів (60%) [14].

Окрім цього, галузь демонструє низьку готовність до викликів, пов'язаних із генеративним ШІ: лише 28% респондентів почали впроваджувати відповідні рішення, тоді як 56% ще оцінюють ризики або не готові до них.

Аналіз специфічних проблем ІБ у сфері транспортної логістики, з урахуванням підвищених ризиків воєнного часу, дозволив ідентифікувати та систематизувати основні категорії загроз і вразливостей для ТЛЦ у вигляді моделі, представленої в таблиці 1.3 [16].

Таблиця 1.3 – Модель загроз та вразливостей (категорії ризиків ІБ) для ТЛЦ

Категорії ризиків ІБ	Типи ризиків ІБ	Характеристика	Приклад реалізації ризику
1. Конфіденційність	Несанкціонований доступ до критичних операційних даних (запаси, локації, замовлення, терміни придатності)	Розголошення чутливих даних (маршрути, клієнти, комерційна таємниця, персонал). Ризик цілеспрямованих атак з боку ворожих сил або їхніх агентів для отримання стратегічної інформації.	Через фішинг викрадають детальні плани перевезення гуманітарної допомоги до прифронтових зон.
	Витік даних	Випадкова/навмисна передача даних назовні (помилки, соц. інженерія, інсайдери).	Email зі звітом клієнтів надіслано назовні, перехоплено.
	Прослуховування каналів	Перехоплення даних у каналах зв'язку (особливо радіо, супутник). Ризик перехоплення інформації про переміщення вантажів, особливо військових або гуманітарних.	Перехоплення координат/статусу вантажу з незашифрованого радіоканалу ворожою розвідкою.
2. Цілісність	Пошкодження/знищення даних	Втрата даних внаслідок кібератак (віруси-шифрувальники, DDoS), фізичних пошкоджень (ракетні удари, диверсії), збоїв в роботі обладнання, перебоїв з електропостачанням, бойових дій або стихійних	Програма вимагач блокує WMS/TMS. Серверна пошкоджена обстрілом, дані знищено.

Категорії ризиків ІБ	Типи ризиків ІБ	Характеристика	Приклад реалізації ризику
		лих.	
	Несанкціонована модифікація/фальсифікація	Навмисна зміна даних (маршрути, статус вантажу); внесення неправдивої інформації (фіктивні рейси). Ризик внесення неправдивої інформації в системи відстеження вантажів.	Хакери змінюють адресу доставки в TMS; Створення фіктивних перевезень для крадіжки коштів.
3. Доступність	Відмова в обслуговуванні (DoS/DDoS)	Перевантаження систем, недоступність сервісів для користувачів (в т.ч. координовані атаки). Ризик скоординованих атак на критично важливі системи для порушення постачання.	DDoS-атака на клієнтський портал унеможливорює розміщення замовлень.
	Збої обладнання / ПЗ	Зупинка систем (WMS, TMS, SCM) через техн. проблеми, вразливості ПЗ, невдалі оновлення.	Збій WMS після оновлення зупиняє роботу складу на цілий день, спричиняючи значні затримки.
	Порушення електропостачання або зв'язку	Втрата доступу через проблеми з енергопостачанням, пошкодження інфраструктури (обстріли, диверсії).	Відключення енергії зупиняє всі ІТ-системи; Втрата зв'язку з ТЗ на маршруті.
4. Автентичність та підзвітність	Підробка особистості (Spoofing)	Видача себе за іншого (користувач, система, орган влади) для доступу/обману.	Фішинг від імені «контролюючого органу» для отримання конфіденційних даних..
	Відмова від дій (Repudiation)	Заперечення виконаних дій через відсутність доказів (логів аудиту), включаючи випадки пошкодження або втрати вантажу.	Водій заперечує отримання інструкцій (без логування) – втрата вантажу.
	Відсутність належного обліку та аудиту	Неможливість відстежити дії користувачів та зміни в системах – ризик зловживань.	Неможливо встановити, хто змінив дані про кількість товару при виявленні розбіжності.
5. Людський фактор	Помилки персоналу	Ненавмисні дії співробітників – виток даних або збої у роботі систем.	Оператор помилково вводить не той код товару в WMS.

Категорії ризиків ІБ	Типи ризиків ІБ	Характеристика	Приклад реалізації ризику
	Інсайдерські загрози	Навмисні зловмисні дії (крадіжка даних, саботаж, зрада, робота на ворога).	Звільнений співробітник видаляє файли; завербований – передає дані про вразливості ворогу.
	Соціальна інженерія	Маніпуляція персоналом для отримання доступу/конфіденційної інформації.	Зловмисник дзвонить співробітнику підтримки, видаючи себе за керівника, і терміново просить пароль до системи, отримуючи таким чином доступ.
	Недостатня обізнаність	Недостатня підготовка персоналу до роботи в умовах воєнних дій або інших кризових ситуацій.	Дзвінок «керівника» з терміновим проханням надати пароль – компрометація доступу.
6. Ланцюги поставок (SCRM)	Атаки на ланцюг постачання	Компрометація систем третіх сторін (партнери, брокери, ІТ-постачальники) з доступом до даних ТЛЦ.	Злам системи митного брокера – витік даних про міжнародні перевезення ТЛЦ.
	Підробка, модифікація обладнання або ПЗ	Використання контрафактного / модифікованого обладнання / ПЗ з бекдорами / вразливостями.	Мережеве обладнання з «закладкою» від неперевіреного постачальника надає бекдор до мережі.
	Зрив/припинення поставок	Зрив поставок критичного обладнання/ПЗ/послуг (в т.ч. через війну, санкції, банкрутство).	Постачальник ПЗ на окупованій території припиняє підтримку – вразливі системи.
7. Фізична безпека	Несанкціонований фізичний доступ до об'єктів ТЛЦ	Проникнення на об'єкти ТЛЦ для крадіжки обладнання/даних, шпигунства.	Крадіжка ноутбуків з офісу на складі через «сліпі зони» відеоспостереження.
	Саботаж, диверсії, воєнні дії	Навмисне пошкодження/знищення інфраструктури ТЛЦ; захоплення/блокування об'єктів. Ризик захоплення або блокування об'єктів ТЛЦ.	Підриг підстанції/колій, що обслуговують ТЛЦ; пряме влучання в склад/офіс.
8. Кібертероризм та кібервійна	Цілеспрямовані кібератаки	Кібератаки з боку ворожих сил або терористичних угруповань з метою порушення транспортної	Координована атака ворожої держави на системи управління рухом ключових ТЛЦ – транспортний колапс.

Категорії ризиків ІБ	Типи ризиків ІБ	Характеристика	Приклад реалізації ризику
		інфраструктури. Поширення паніки та підлив економічної стабільності через кібератаки.	
	Деструктивні дії в кіберпросторі	Ведення розвідки, саботажу та дезінформаційних кампаній, спрямованих на ТЛЦ, з використанням кіберпростору.	Поширення фейків через соцмережі та зламані сайти про знищення ТЛЦ для паніки.

Представлена модель загроз (табл. 1.3) демонструє, що ризики для ТЛЦ мають комплексний характер і охоплюють як класичні ІТ-загрози (порушення конфіденційності, цілісності та доступності), так і інтегровані кіберфізичні ризики (атаки на ОТ-системи, фізичні диверсії) та загрози ланцюга поставок.

Багатоаспектність загроз ТЛЦ зумовлює потребу в комплексному оцінюванні ризиків ІБ. Згідно з концепцією Б. Шнайєра (B. Schneier) про «найслабшу ланку», ефективний захист вимагає системного аналізу технічних, організаційних і людських факторів на базі інтелектуальних ІТ ППР [17]. Розробка таких методів в умовах високої невизначеності визначає подальший напрям даного дослідження.

## 1.2. Сучасні підходи до оцінки рівня інформаційної безпеки

В умовах нестабільної світової економіки, обумовленої макроекономічною та геополітичною невизначеністю, питання забезпечення ІБ підприємств стає все більш актуальним.

Розвиток інформаційного суспільства створює нові можливості для економічного зростання поряд з новими загрозами ІБ. На сьогоднішній день ТЛЦ стають більш уразливими через зростаючу залежність від комп'ютерів, мереж, програм та додатків, соціальних мереж та даних.

Порушення ІБ можуть негативно позначитися на діяльності підприємств та

їх клієнтів як у фінансовому, так і у репутаційному плані. При цьому однією з найважливіших складових забезпечення ІБ підприємств є оцінка ризиків ІБ.

За результатами дослідження «Ризик у фокусі на 2025 рік», проведеного Європейською конфедерацією інститутів внутрішнього аудиту (European Confederation of Institutes of Internal Auditing (ECPIA)) [18], було визначено очікувані ризики, з якими можуть зіткнутися підприємства різних секторів економіки в найближчі 3 роки (рис. 1.4).

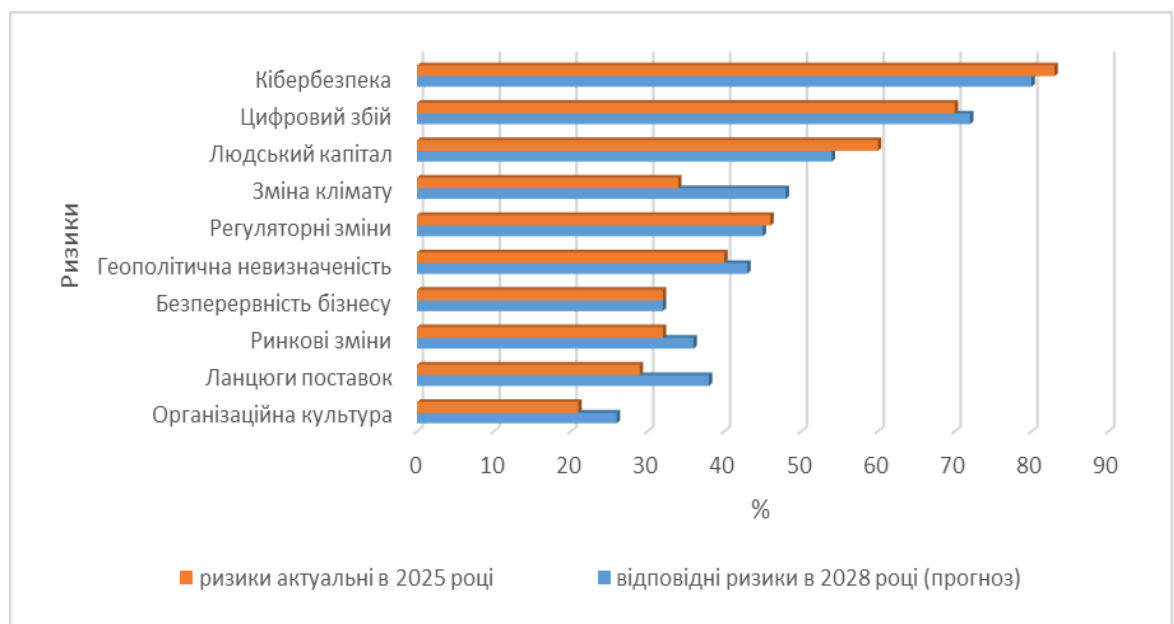


Рисунок 1.4 – Топ-10 ризиків, з якими можуть зіткнутися підприємства в найближчі 3 роки

Респонденти дев'ятий рік поспіль першочерговою загрозою вважають кібербезпеку (83%), а швидкозростаючі цифрові збої, за прогнозами, до 2028 року будуть посідати друге місце серед ризиків (72%). Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Адміністрації Державної служби спеціального зв'язку та захисту інформації України, повідомила, що в Україні у 2024 році було опрацьовано 4315 кіберінцидентів. Це на 69,8% більше, ніж у 2023 році. Тобто, спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України, зокрема на

транспортно-логістичні системи, що забезпечують під час війни постачання військової техніки, гуманітарної допомоги, а також підтримують економічну стабільність [19].

Питання оцінки ризику ІБ з кожним роком набуває все більшої актуальності. Зокрема, І. Обертинюк, О. Кареліна в статті [20] презентують технологію оцінки ризиків ІБ для підприємства «Укртелеком» відповідно до вітчизняних нормативних документів та міжнародних стандартів, використовуючи методологію CRAMM. Окремим питанням є економічна оцінка захисту інформації. І. Карпович та ін. в роботах [21] та [22] детально досліджують методику оцінки рівня ризиків ІБ та обґрунтування оптимальних витрат на захист інформації. Автори пропонують нові підходи до моделювання заходів безпеки та розробляють методику оцінки ризиків, що поєднує теорію графів з експертними оцінками. О. Потій та ін. [23] провели докладний аналіз методів оцінки і управління ризиками кібер- та ІБ, визначили необхідність адаптації та удосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів. Є. Кузьмініх та ін. [24] розглянули оцінку ризиків ІБ з використанням нечіткої логіки та здійснили класифікацію ризиків.

Питанням застосування різних програмних продуктів для оцінки ризиків ІБ присвячені роботи: Х. Разікін (K. Razikin), Б. Соевіто (B. Soewito) [25] – OCTAVE Allegro для компаній роздрібної торгівлі; К. Шмітц (C. Schmitz), С. Папе (S. Pape) [26] – спрощена структура оцінки ризиків безпеки для підтримки прийняття рішень у сфері ІБ (LiSRA); П. Лофт (P. Loft) та ін. [27] – Continuous Agile Enterprise Security Architecture Review у 8 доменах (CAESAR8), що підтримує динамічні та цілісні огляди ризиків ІБ в ІТ-проектах; А. Іршейд (A. Irsheida) та ін. [28] провели порівняльний аналіз методологій управління ІБ ISO 27005, NIST SP 800-30, CRAMM, CORAS, OCTAVE Allegro та COBIT 5 зосередившись на їхній придатності, гнучкості та здатності залучати різні групи користувачів у контексті хмарних обчислень. Але запропоновані оцінки не

враховують специфіки транспортно-логістичної галузі і ТЛЦ, зокрема.

Оцінка ризиків ІБ у транспортній галузі представлена в роботі К. Бернсмед (K. Bernsmed) та ін. [29], де розглядаються удосконалення методології оцінки ризиків безпеки SESAR (SecRAM) в області управління повітряним рухом. У статті Б. Гюнеш (B. Gunes) та ін. [30] для чотирьох розроблених сценаріїв кібератаки була застосована методологія оцінки ризику з використанням інтегрованого підходу до управління кібербезпекою з урахуванням фізичних кіберактивів контейнерного порту. У роботі Л. Лян (L. Liang) та ін. [31] проаналізовані ризики ІБ компонентів з відкритим вихідним кодом у транспортній галузі та запропоновані заходи щодо управління ними. У дослідженні С. Алфарісі (S. Alfarisi) та Н. Суранта (N. Surantha) [32] застосування OCTAVE Allegro допомогло виявити критичні активи та ризики автопарку. О. Мельниченко та ін. [33] описують процес аналізу, оцінки та управління ризиками ІБ в системах надання транспортних послуг. У роботі систематизовано процес оцінювання ризиків ІБ на транспорті, визначені шляхи попередження та протидії інформаційним загрозам, як при проектуванні, так і при експлуатації систем надання транспортних послуг.

Однак, наголошуючи на істотних здобутках провідних вчених в обраному напрямку дослідження, необхідно зауважити, що отримані ними результати вимагають певної систематизації та адаптації до специфіки ТЛЦ у питаннях оцінки ризиків ІБ.

Оцінка ризиків ІБ є найбільш складним і відповідальним етапом процесу управління безпекою. Методика оцінки ризиків – це систематичний процес ідентифікації, аналізу та оцінювання потенційних ризиків.

Відомі методики оцінки та аналізу ризиків класифікують за типом оцінки: якісні (використовують описові шкали); кількісні (ризик оцінюється числовим значенням); гібридні (поєднують обидва підходи).

Результати аналізу, що включають класифікацію методик за типом оцінки, властиві їм переваги та недоліки, а також оцінку їхньої релевантності та



доцільності застосування в специфічних умовах українських ТЛЦ, представлено у таблиці 1.4.

Таблиця 1.4 – Класифікація інструментів оцінки ризиків ІБ за типом оцінки, перевагами, недоліками та придатністю для ТЛЦ [17]

Інструменти оцінки ризиків ІБ	Тип оцінки	Переваги	Недоліки	Придатність для ТЛЦ
1. FAIR [34]	Кількісна	Фінансова оцінка ризику.	Складний збір даних, вимагає експертної оцінки.	<i>Середня.</i> Розглядають для обґрунтування інвестицій в ІБ, якщо потрібна грошова оцінка.
2. CORAS [35]	Гібридна	Моделювання складних систем (ІТ/ОТ), візуалізація.	Може вимагати спеціальних знань UML.	<i>Висока.</i> Аналіз ризиків взаємопов'язаних ІТ/ОТ систем, комунікація з стейкхолдерами.
3. EBIOS [36]	Якісна	Прагматичний, ітеративний, враховує екосистему.	Не розглядає випадкові ризики, суб'єктивність.	<i>Середня.</i> Фокусується на аналізі сценаріїв навмисних загроз (актуально в умовах війни) та аналізі ризиків в рамках своєї екосистеми (партнери, постачальники).
4. FMEA [37]	Якісна	Швидкий та простий процес; залучає бізнес-підрозділи до ідентифікації ризиків.	Залежить від досвіду фасилітатора та експертів.	<i>Середня.</i> Корисний для малих/середніх ТЛЦ. Для швидкої початкової ідентифікації ключових ризиків при обмежених ресурсах або як перший крок.
5. FRAP [38]	Якісна	Виявлення потенційних проблем на ранніх стадіях. Пріоритезація RPN (Risk Priority Number).	Трудомісткий, суб'єктивний RPN, потрібні глибокі знання про систему або процес.	<i>Середня.</i> Аналіз відмов критичних фізичних/автоматизованих систем (WMS, контроль доступу) ІБ. Допомогає зрозуміти наслідки відмови ключових компонентів.
6. HAZOP [39]	Якісна	Спеціалізація на ОТ, аналіз безпеки і операційності.	Ресурсномісткий, вимагає участі експертів з різних галузей.	<i>Висока.</i> Особливо рекомендований для ТЛЦ зі значною часткою систем ОТ для аналізу безпеки та безперебійності систем ОТ (АСУТП, SCADA) якщо є ресурси на залучення експертів.
7. PASTA [40]	Якісна	Детальний каталог базових заходів захисту, особливо корисний для роботи з німецькими партнерами.	Специфічний для Німеччини, може бути надлишковим.	<i>Середня.</i> Якщо ТЛЦ співпрацює з німецькими партнерами або потребує дуже детального каталогу базових заходів захисту.
8. Threat Modeling (включаючи STRIDE, PASTA) [41]	Якісна	Фокус на атакуючому, 7 етапів, бізнес-контекст.	Складний, ресурсномісткий.	<i>Висока.</i> Глибоке моделювання атак на критичні додатки/API, виявлення складних загроз.
9. IT-Grundschutz [42]	Якісна	Проактивне виявлення загроз (в SDLC) на ранніх етапах розробки.	Ефективність залежить від знань та досвіду команди.	<i>Висока.</i> Проактивний аналіз загроз ІТ/ОТ систем при розробці/модифікації. Вимагає відповідної експертизи в команді.
10. CRAMM	Гібридна	Структурований,	Потрібне	<i>Середня.</i> Структурований підхід для

Інструменти оцінки ризиків ІБ	Тип оцінки	Переваги	Недоліки	Придатність для ТЛЦ
[43]		поєднує якісні та кількісні елементи.	спеціалізоване ПЗ для повної функціональності.	оцінки переважно ІТ-інфраструктури (при готовності до використання ПЗ). Менш орієнтований на ОТ та ланцюги поставок.
11. MAGERIT [44]	Гібридна	Орієнтований на активи, надає каталог елементів та керівництво з технік аналізу ризиків.	Може бути складним для дуже великих структур.	<i>Середня.</i> Детальний аналіз ризиків активів, взаємодія з іспанськими партнерами/регуляторами.
12. NIST [45]	Гібридна	Забезпечує загальну рамку та принципи управління ризиками (де-факто стандарт).	Вимагає конкретизації через інші стандарти NIST.	<i>Дуже висока.</i> Ідеально підходить для ТЛЦ як критичної інфраструктури з чутливими даними. Надає надійну основу для побудови та оцінки ІБ.
13. NIST CSFP [46]	Гібридна з акцентом на якісну	Гнучкий фреймворк (Identify-Recover), вкл. SCRM (версія 2.0).	Не є дуже детальним у конкретних технічних контролях.	<i>Висока.</i> Основа для побудови або вдосконалення комплексної програми ІБ ТЛЦ, включаючи SCRM. Дозволяє адаптацію до розміру, ресурсів та специфіки.
14. NIST RMF [47]	Гібридна з акцентом на якісну	Комплексний процес для ЖЦ систем (IT/OT/SCRM), інтеграція з SP 800-53.	Складний у повному впровадженні, ресурсномісткий.	<i>Висока.</i> Для (середніх/великих) ТЛЦ які потребують комплексного підходу до ризиків ІТ, ОТ та ланцюгів поставок, особливо при взаємодії з американськими партнерами.
15. NIST SP 800-161 [48]	Гібридна з акцентом на якісну	Спеціалізація на SCRM (ризики ланцюга поставок).	Орієнтований на федеральні агентства США (але принципи універсальні).	<i>Висока.</i> Управління SCRM. Детальні настанови з ризиків ланцюга поставок. Критично для ТЛЦ.
16. OWASP [49]	Гібридна	Спеціалізація на Web/API, практичні інструменти, активна спільнота та безкоштовні ресурси. Допомагає впроваджувати безпечну розробку (Secure SDLC).	Вузький фокус (Web/API), Top 10 - не вичерпний стандарт.	<i>Висока.</i> Безпека Web/API. Оцінка вебзастосунків/API (як доповнення до основи).
17. НБУ [50]	Гібридна	Обов'язковий для фінсектору України.	Обмежена сфера, жорсткість, можливе відставання.	<i>Низька.</i> Вимоги специфічні для банків/фінсектору і зазвичай не застосовуються до ТЛЦ (окрім винятків).
18. ISO/IEC 27001:2022 [51]	Дозволяє всі типи	Міжнародний стандарт на СУІБ (ISMS), демонструє зрілість.	Ресурсоємне впровадження саме СУІБ.	<i>Висока.</i> Є основою для СУІБ. Впровадження доцільне для ТЛЦ, які прагнуть продемонструвати високий рівень ІБ партнерам/клієнтам або мають такі вимоги за контрактом/регуляціями.
19. ISO/IEC 27005:2022 [52]	Дозволяє всі типи	Міжнар. стандарт-настанова з управління ризиками ІБ,	Не дає конкретного методу оцінки, лише процес.	<i>Висока.</i> Для будь-якого ТЛЦ, що впроваджує управління ризиками ІБ відповідно до міжнародних практик, особливо в рамках підготовки до

Інструменти оцінки ризиків ІБ	Тип оцінки	Переваги	Недоліки	Придатність для ТЛЦ
		підтримує ISO 27001.		сертифікації ISO 27001.

Проведена систематизація та порівняльний аналіз можуть слугувати основою для прийняття обґрунтованих рішень щодо вибору найбільш адекватної методології управління ризиками ІБ для ТЛЦ. Для ТЛЦ, що характеризуються складними ІС, інтегрованими ланцюгами поставок та активною взаємодією через вебінтерфейси та API, вибір методики має бути стратегічним рішенням.

Ключовим є розуміння того, як результати оцінки ризиків впливають на вибір методів виявлення атак та, відповідно, на формування ефективних контрзаходів. Наприклад, для ТЛЦ з розгалуженою автоматизованою інфраструктурою оцінка ризиків за допомогою методик, що аналізують стани систем (на кшталт FMEA або HAZOP), допомагає обґрунтувати впровадження моніторингу аномалій стану. Для захисту клієнтських порталів та API застосування методик моделювання загроз (OWASP, PASTA) вказує на пріоритетність сигнатурних чи евристичних методів для виявлення вебатак.

Для дослідження цих взаємозв'язків було проведено систематизацію, яка демонструє зв'язок між методиками оцінки ризиків, їхньою вартістю/доступністю та відповідними методами/підходами до виявлення атак. Результати цієї систематизації наведено у таблиці 1.5.

Таблиця 1.5 – Інструменти оцінки ризиків ІБ: вартість/доступність та зв'язок з виявленням атак [17]

Інструменти оцінки ризиків ІБ	Платний/Безкоштовний (б/к)	Методи виявлення атак	Підходи до виявлення атак
1. FAIR	Документація (Open FAIR) – б/к; Інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Статистичний, аналіз систем станів.	Статистичний, імовірнісний.
2. CORAS	Документація, академічні інструменти (ПЗ), – б/к; Комерційне ПЗ, експертиза, консультанти, навчання – платні.	Аналіз систем станів, графі сценаріїв атак.	Імовірнісний, евристичний, інформаційний.
3. EBIOS	Документація – б/к; Інструменти (ПЗ), експертиза, консультації, навчання – можуть бути платні.	Аналіз систем станів, графі сценаріїв атак.	Імовірнісний, евристичний.

Інструменти оцінки ризиків ІБ	Платний/Безкоштовний (б/к)	Методи виявлення атак	Підходи до виявлення атак
4. FMEA	Метод – б/к; Глибока експертиза, консультанти, навчання – платні.	Аналіз систем станів.	Евристичний, інформаційний.
5. FRAP	Процес – б/к; Внутрішні витрати часу фасилітаторів, експертиза, консультанти, навчання – платні.	Експертні системи.	Евристичний.
6. HAZOP	Процес – б/к; Внутрішні витрати часу різнопрофільних експертів – платні.	Аналіз систем станів, експертні системи.	Евристичний, інформаційний.
7. PASTA	Документація доступна, інструменти (ПЗ) – часто б/к; Експертиза, консультанти, навчання, внутрішні витрати часу – платні.	Графи сценаріїв атак.	Евристичний, інформаційний.
8. Threat Modeling (включаючи STRIDE, PASTA)	Методики (STRIDE etc.) – (б/к); Експертиза, консультанти, навчання, внутрішні витрати часу, інструменти (ПЗ) є як б/к так і платні.	Графи сценаріїв атак, аналіз систем станів.	Евристичний, інформаційний.
9. IT-Grundschutz	Документація, каталоги – б/к; Інструменти (ПЗ), сертифікація, аудит – платні.	Засновані на специфікаціях, сигнатурний.	Інформаційний, статистичний.
10. CRAMM	ПЗ, експертиза, консультанти, навчання – платні.	Статистичний, експертні системи.	Статистичний, евристичний.
11. MAGERIT	Документація, базове ПЗ (PILAR) – б/к; Інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Експертні системи, статистичний.	Евристичний, статистичний.
12. NIST	Стандартизація, настанови – б/к; Впровадження, інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Підтримує вибір усіх типів.	Підтримує вибір усіх типів.
13. NIST CSF	Фреймворк – б/к; Впровадження, інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Підтримує вибір усіх типів (в рамках Detect).	Підтримує вибір усіх типів.
14. NIST RMF	Фреймворк – б/к; Впровадження, інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Підтримує вибір усіх типів (при виборі контролів).	Підтримує вибір усіх типів.
15. NIST SP 800-161	Стандарт – б/к; Впровадження, інструменти (ПЗ), експертиза, консультанти, навчання – платні.	Підтримує вибір усіх типів (для SCRM).	Підтримує вибір усіх типів.
16. OWASP	Документи, інструменти (ПЗ) – переважно б/к; Експертиза, консультанти, навчання, внутрішні витрати часу – платні.	Засновані на специфікаціях, сигнатурний, статистичний (для вебатак).	Інформаційний, статистичний.
17. НБУ	Документи – б/к; Впровадження, аудит (для піднаглядних) – платні.	Експертні системи, сигнатурний, статистичний (відповідно до вимог).	Евристичний, інформаційний, статистичний.
18. ISO/IEC 27005:2022	Документи – б/к; Впровадження, аудит – платні.	Підтримує вибір усіх типів.	Підтримує вибір усіх типів.

Різноманіття характеристик представлених у таблицях 1.4 та 1.5 методик унеможлиблює визначення єдиного, універсального, «найкращого» підходу для всіх ТЛЦ.

Аналіз наукових публікацій свідчить про зростаючий інтерес до систем підтримки прийняття рішень (СППР) у сфері ІБ. Це особливо актуально для таких складних і критично важливих кіберфізичних систем, як ТЛЦ. Важливо підкреслити, що інформаційна безпека в цьому контексті є комплексним поняттям, яке охоплює не лише кібербезпеку, а й захист від фізичних загроз, ризиків, пов'язаних із людським фактором, та операційних процесів, що вимагає інтегрованого підходу та інструментів для стратегічного планування.

Серед фундаментальних досліджень, які закладають методологічні основи для побудови СППР, праці В. Л. Бурячка, С. В. Толюпи та ін. [53], [54], а також С. Б. Ома (S. Eom) [55] формують підходи до системного аналізу та прийняття рішень в управлінні, зокрема з урахуванням обробки евристичних даних. На державному рівні стратегічне значення підтримки рішень у сфері ІБ підкреслює у своїй роботі Є. Л. Добровольський [56]. Сучасні СППР, як зазначено у праці С. Зибіна [57], базуються на комплексних алгоритмах, що охоплюють аналіз проблем, ризиків та загроз, а також формування цілей, рішень та альтернатив. Таким чином, створено міцний теоретичний базис для проектування інтелектуальних систем управління.

Існуючі СППР можна класифікувати за їхніми архітектурними підходами, кожен з яких має свої переваги та обмеження.

*Експертно-орієнтовані архітектури.* Наприклад, робота О. Мілова пропонує модулі для експертної оцінки та рекомендацій [58]. Однак ключовим недоліком таких систем є статичність: вони не здатні до самонавчання та адаптації, а їхні висновки повністю залежать від суб'єктивності введених експертних оцінок.

*Процесно-орієнтовані архітектури.* Дослідження В. Biswas (Б. Бісвас) та ін. пропонує архітектуру на базі методології OCTAVE Allegro [59]. Такі системи

забезпечують структурованість, але успадковують обмеження методологій: недостатню гнучкість для роботи з нечіткими даними та невизначеністю, що є критичним для динамічного середовища ТЛЦ.

*Контекстно-орієнтовані (когнітивні) архітектури.* Система C3-SEC (Г. Рольдан-Моліна (G. Roldán-Molina) та ін.) моделює когнітивний процес аналізу загроз для створення ситуаційної обізнаності [60]. Проте її архітектура меншою мірою сфокусована на стратегічному плануванні, зокрема на оптимізації інвестицій у заходи захисту та аналізі «витрати-вигода».

Існуючі міжнародні стандарти (ISO/IEC 27001[51], ISO/IEC 27005 [52], NIST Cybersecurity Framework [45]) визначають ключові компоненти та процеси управління ІБ, але не пропонують готових архітектурних рішень для інтелектуалізації процесу прийняття рішень. Застосування цих стандартів у динамічному середовищі ТЛЦ виявляє прогалини в комплексних інструментах для стратегічного управління ризиками та оптимізації інвестицій в ІБ, особливо з урахуванням браку реальних даних (А. Азарова та ін. [61], О. Мельниченко та ін. [62]). Роботи С. Карновале (S. Carnovale), С. Єніюрт (S. Yeniyurt) [63] та Р. Садегі (R. Sadeghi) та ін. [64] додатково акцентують увагу на необхідності врахування «людського фактора» та управління кіберризиками в закупівлях і логістиці, що підтверджує актуальність стратегічних СППР.

Отже, проведений аналіз демонструє, що наявні архітектурні рішення є або занадто статичними, або орієнтованими переважно на оперативний рівень. Стандарти ІБ надають методологічну рамку, але не вирішують проблему інтелектуалізації стратегічного управління. Цей огляд підводить до ключової проблеми, яка буде розглядатися далі.

### **1.3. Проблема невизначеності в задачах оцінки стану інформаційної безпеки ТЛЦ**

Специфічними особливостями при вирішенні завдань створення системи

забезпечення ІБ ТЛЦ є:

- неузгодженість та застарілість стандартів, як в галузях інформаційних технологій та кібербезпеки, так і в галузях транспорту і логістики;
- неповнота та невизначеність вихідної інформації про характерні загрози ІБ;
- широке використання операційних технологій;
- багатокритеріальність завдання створення та оцінки стану системи забезпечення ІБ, пов'язана з необхідністю обліку великої кількості показників (вимог) системи забезпечення ІБ;
- наявність як кількісних, так і якісних показників, які необхідно враховувати при вирішенні завдань розробки та впровадження системи забезпечення ІБ;
- неможливість застосування класичних методів оптимізації;
- нестача кваліфікованих кадрів, здатних забезпечити захист ТЛЦ.

Як впливає з наведених особливостей, джерела невизначеності в задачах оцінки ІБ ТЛЦ є багатограними. Їх можна конкретизувати наступним чином.

*Неповнота та відсутність статистичних даних.* Існує об'єктивна неповнота вихідної інформації. Для новітніх цілеспрямованих атак та специфічних загроз воєнного часу репрезентативна вибірка для побудови точних імовірнісних моделей, як правило, відсутня.

*Нечіткість та суб'єктивізм експертних оцінок.* Через брак кількісних даних система змушена покладатися на якісні показники. Експерти оперують лінгвістичними поняттями («високий ризик», «ймовірна загроза»), які є нечіткими за своєю природою.

*Стохастичність та динамічність загроз.* Середовище загроз не є статичним. Воно характеризується постійним зростанням кількості атак та появою нових, непередбачуваних векторів (наприклад, пов'язаних з GenAI). Це робить будь-яку статичну оцінку ризику актуальною лише на дуже короткий термін часу.

Виявлені джерела невизначеності безпосередньо призводять до

неадекватності управлінських рішень. Як показав аналіз у 1.2, існуючі СППР та методології мають фундаментальні недоліки:

- експертно-орієнтовані архітектури є статичними, нездатними до адаптації та повністю залежать від суб'єктивності введених оцінок;
- процесно-орієнтовані архітектури (на кшталт на базі OCTAVE Allegro) успадковують недостатню гнучкість для роботи з нечіткими даними та невизначеністю, що є критичним для ТЛЦ;
- когнітивні архітектури меншою мірою сфокусовані на стратегічному плануванні та аналізі «витрати-вигода».

Проведений аналіз підтверджує, що стандартні методи фокусуються на окремих компонентах і недостатньо враховують кумулятивні та системні взаємозв'язки у кіберфізичному ландшафті ТЛЦ. Також вони не враховують унікальну специфіку логістичних операцій (критичність, своєчасність, конвергенцію ІТ/ОТ). Все це вимагає значних ресурсів та експертизи для підтримки актуальності, що важко реалізувати в умовах браку кадрів та коштів.

Ці недоліки вказують на те, що існуючі підходи є недостатніми для адекватного управління ризиками ІБ, та обґрунтовують необхідність розробки нової технології, здатної ефективно працювати в умовах глибокої невизначеності.

#### **1.4 Аналіз існуючих моделей оцінки ризиків ІБ**

Розробка інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ вимагає врахування двох ключових аспектів:

- 1) обов'язкового національного регуляторного контексту;
- 2) унікальної технологічної природи об'єкта.

Регуляторний контекст визначається тим, що ТЛЦ віднесено до об'єктів критичної інфраструктури. Як наслідок, будь-яка модель оцінки ризиків для них повинна узгоджуватися з вимогами національного законодавства. Ключовим нормативним актом у цій сфері є Наказ Адміністрації Державної служби



спеціального зв'язку та захисту інформації України від 14.01.2025 № 17 «Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури» [65]. Він встановлює обов'язковий процес оцінки та зобов'язує секторальні органи проводити її відповідно до затвердженої методики. Таким чином, фундаментальною вимогою до математичної моделі визначення рівня ризику ТЛЦ є її здатність надавати кількісні показники, які можна зіставити з критеріями, визначеними цим національним стандартом.

Технологічна специфіка ТЛЦ характеризується глибокою інтеграцією кіберфізичних систем, де поряд з корпоративними ІТ-системами (ERP, CRM) функціонують критичні операційні технології та промислові системи автоматизації (WMS, SCADA, автоматизовані лінії сортування).

Оцінка ризиків для ІТ та ОТ кардинально відрізняється через різні пріоритети:

- пріоритетами при визначенні ІТ-ризиків є: конфіденційність, цілісність, доступність. При цьому розглядають фінансові та репутаційні наслідки;
- пріоритетами ОТ-ризиків є: безпека, доступність, цілісність. Наслідки – фізичні (зупинка ланцюгів постачання, пошкодження обладнання, загроза життю).

Через цю подвійну природу (ІТ/ОТ) єдиної простої формули ризику недостатньо. Необхідний комбінований підхід. Глобальним стандартом для безпеки промислової системи автоматизації є ІЕС 62443 [66]. Цей стандарт пропонує архітектурний підхід до управління ризиками, що ідеально підходить для ТЛЦ, та передбачає наступний двоетапний процес оцінки.

Етап 1. Початкова оцінка ризиків. Це швидке сортування для ідентифікації зон високого ризику. Метод полягає в тому, що оцінка припускає ймовірність загрози рівною одиниці ( $L = 1$ ). Аналіз фокусується виключно на найгіршому сценарії наслідків. Це дозволяє миттєво визначити найкритичніші зони (на кшталт «системи управління сортуванням»).

Етап 2. Детальна оцінка ризиків. Для зон високого ризику, що

ідентифіковані на етапі 1, проводиться повний, детальний аналіз. Припущення  $L = 1$  знімається. Аналітики розглядають реалістичні вектори загроз, ймовірності та ефективності контрзаходів.

Для проведення детальної оцінки необхідна деталізована математична модель. Незважаючи на те, що існують різні кількісні підходи, вони мають суттєві обмеження в контексті ТЛЦ.

Детерміністична модель (ALE). Класичні кількісні формули, як Annualized Loss Expectancy (ALE), що базуються на  $ALE = (AV \cdot EF) \cdot ARO$ , вимагають точних одиничних вхідних значень. В умовах кібербезпеки ТЛЦ, де дані про частоту нових атак (ARO) відсутні, а вартість активів (AV), наприклад «репутація», є нечіткою, цей підхід створює ілюзію точності і є непридатним.

Стохастичні моделі (FAIR, VaR). Більш просунуті моделі, наприклад FAIR, розглядають ризик як розподіл ймовірностей та використовують симуляції Монте-Карло. Ці моделі достатньо точні, при цьому вони вимагають великих обсягів статистичних даних для побудови достовірних розподілів. Нажаль в умовах війни для ТЛЦ такі дані відсутні.

Проведений аналіз, узагальнений у табл. 1.5, демонструє методологічну прогалину. Якісні моделі (ISO) – суб’єктивні; детерміністичні (ALE) – неточні; стохастичні (FAIR) – вимагають даних, яких немає.

Таблиця 1.6 – Порівняльний аналіз ключових інструментів оцінки ризиків

Інструмент	Тип	Основна формула / концепція	Придатність для агрегації	Недоліки
ISO 27005 [52]/ NIST 800-30 [67] (загальний процес)	Якісний (матричний)	$R = (P, I)_{mxn}$ , де $P$ – ймовірність; $I$ – вплив; $R$ – рівень ризиків (Low, Med, High).	Дуже низька. Математично некоректно додавати ранги.	Суб’єктивність оцінок, відсутність точного числового виразу для розрахунків.
Класичний ALE (фінансова оцінка)	Кількісний (детерміністичний)	$ALE = (AV \cdot EF) \cdot ARO$ , де $AV$ – вартість активу (ум. од.);	Низька. Статистично некоректна (додавання середніх).	Вимагає точних історичних даних про інциденти, яких зазвичай немає для нових загроз.

Інструмент	Тип	Основна формула / концепція	Придатність для агрегації	Недоліки
		$EF$ – % втрат; $ARO$ – частота на рік.		
Алгоритм Обертинюк-Кареліної [20]	Кількісний (імовірнісний)	$CTh = 1 - \prod_{t=1}^n (1 - Th_t)$ , $R = CTh \cdot D$ , де $CTh$ – загальний рівень загрози; $Th_t$ – рівень окремої загрози; $D$ – критичність доступу.	Використовує формулу об'єднання ймовірностей.	Не дозволяє налаштовувати вагу різних активів; складно оцінити точну ймовірність $Th$ для всіх векторів.
FAIR [34] (фінансова квантифікація)	Кількісний (стохастичний)	$R = LEF \times LM$ , де $LEF$ – розподіл частоти подій втрат, $LM$ – розподіл величини втрат (симуляція тисячі сценаріїв метод Монте-Карло)	Висока. Моделює розподіли, а не окремі числа.	«Чорна скринька» для користувача; вимагає складного ПЗ та великої статистики.
ІЕС 62443-3-2 [66] (критична інфраструктура)	Якісний (архітектурний)	$R = f(Impact)$ , при $L = 1$ . Концепції: Zones, Conduits, SL-T.	Низька. Мета – сегментація мережі та визначення вимог.	Орієнтований на проєктування захисту (SL), а не на динамічний розрахунок поточного рівня ризику.
WSM (Weighted Sum) [68]	Кількісний (бальний)	$R = \sum_{i=1}^n w_i \cdot v_i$ , де $w_i$ – вага фактора; $v_i$ – нормоване значення фактора; $n$ – кількість факторів.	Висока. Дозволяє ранжувати активи за важливістю.	Лінійна залежність, не враховує невизначеність та нечіткість думок експертів.

Це обґрунтовує необхідність розробки комплексної моделі, яка б поєднувала:

– структурованість багатокритеріальних підходів;

- здатність працювати з нечіткими експертними даними, які є основним джерелом даних;
- адаптивність та здатність моделювати нелінійні взаємодії.

### **1.5 Постановка задачі дослідження**

Проведений вище аналіз доводить, що система забезпечення ІБ ТЛЦ є носієм властивостей складної кіберфізичної системи. Як було показано в 1.1, ефективність ТЛЦ базується на глибокій інтеграції інформаційних (TMS, WMS) та операційних (AGV, AS/RS) технологій, що створює унікальні вектори атак. Модель загроз (табл. 1.3) підтвердила, що ці системи є пріоритетною ціллю, а ризики посилюються в умовах війни, загрожуючи не лише економіці, а й обороноздатності.

Водночас аналіз існуючих підходів та програмних засобів (п. 1.2) виявив суттєву прогалину у стандартних методиках (NIST, ISO) та СППР. Вони є або занадто статичними, або негнучкими, або орієнтованими на операційний, а не стратегічний рівень. Вони не адаптовані до специфіки ІТ/ОТ-конвергенції та погано враховують ключову проблему, деталізовану в п. 1.3, – глибоку невизначеність.

Ця невизначеність (неповнота даних про нові атаки, нечіткість експертних оцінок) робить класичні методи оцінки ризиків неадекватними. Існуючі технології не надають керівництву ТЛЦ інструментів для обґрунтованого прийняття рішень щодо оптимізації захисту.

Це обґрунтовує нагальну наукову та практичну необхідність у розробці нової ІТ ППР. Така технологія має долати зазначені обмеження шляхом застосування інтелектуальних підходів (зокрема, теорії нечітких множин та нейронечітких систем), які здатні адекватно моделювати та обробляти нечітку вхідну інформацію для підтримки прийняття стратегічних рішень щодо захисту ТЛЦ.

Проведений аналіз, що виявив специфіку ТЛЦ як об'єкта захисту, комплексність загроз та неадекватність існуючих методів в умовах невизначеності, дозволяє чітко сформулювати мету та завдання дисертаційного дослідження.

*Метою* дисертаційного дослідження є підвищення ефективності підтримки прийняття рішень при забезпеченні інформаційної безпеки ТЛЦ шляхом поєднання методів експертної аналітики та використання гнучких адаптивних нейронечітких систем.

Логіку та взаємозв'язок поставлених задач для досягнення мети дисертаційної роботи відображено у логічно-структурній моделі дослідження (рис. 1.5).

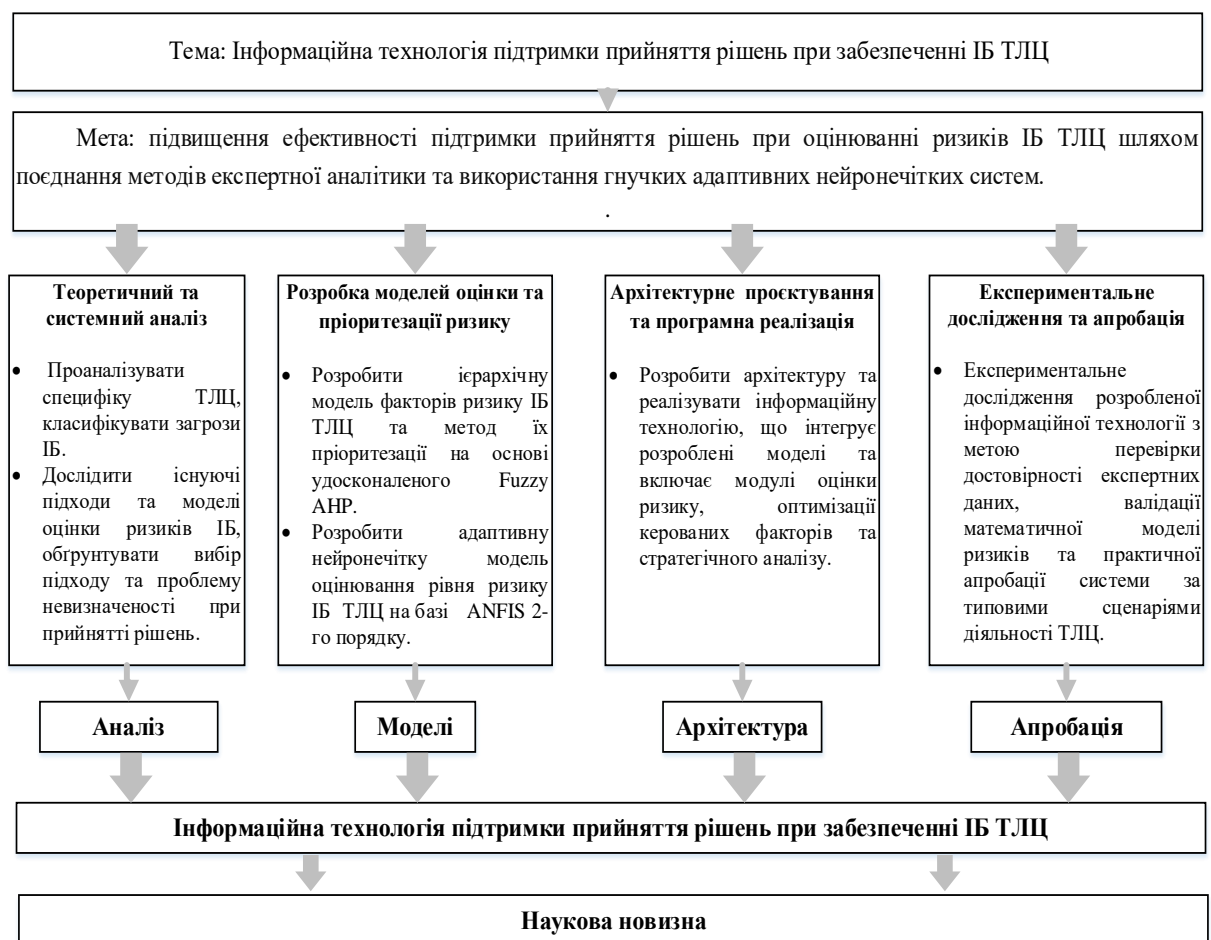


Рисунок 1.5 – Логічно-структурна модель дослідження

*Етап 1. Теоретичний та системний аналіз.* На першому етапі виконано

системний аналіз ТЛЦ як складного об'єкта захисту. Ідентифіковано специфіку інформаційних потоків ТЛЦ та визначено критичні точки вразливостей динамічних логістичних процесів. Проведено ґрунтовне дослідження проблеми невизначеності. Виконано порівняльний аналіз існуючих підходів до оцінювання ризиків ІБ. Це дозволило обґрунтувати вибір методів та сформулювати концептуальні положення щодо захисту ТЛЦ в умовах воєнних ризиків та обмеженості вихідних даних.

*Етап 2. Розробка моделей оцінки та пріоритезації ризику.* Математичне забезпечення інформаційної технології базуватиметься на побудові ієрархічної системи показників, яка інтегрує технічні, програмні та кадрові аспекти безпеки у єдину структуру оцінювання. Пріоритезацію факторів ризику передбачається здійснювати із застосуванням удосконаленого методу Fuzzy АНР, що стане підґрунтям для синтезу адаптивної моделі на базі ANFIS другого ступеня. Заплановано розробку алгоритмів нечіткого виводу для ефективного агрегування різномірних даних, що дозволить створити математичну базу для стратегічного управління витратами на систему захисту.

*Етап 3. Архітектурне проектування та програмна реалізація.* Технічне втілення розроблених рішень передбачає об'єктно-орієнтоване моделювання процесів підтримки прийняття рішень із використанням методологій IDEF0 та UML. Архітектуру системи планується проектувати на принципах сервіс-орієнтованого підходу для забезпечення масштабованості. Програмна реалізація охоплюватиме створення модулів обробки даних, інтелектуального обчислювального ядра та інтерфейсу користувача з детальною специфікацією форматів вхідних і вихідних потоків.

*Етап 4. Експериментальне дослідження та апробація.* Завершальна стадія роботи буде присвячена експериментальному дослідженню, де шляхом імітаційного моделювання планується провести верифікацію адекватності та обчислювальної стійкості моделі ANFIS. Увага буде приділена аналізу адаптивних властивостей системи при зміні стратегічних пріоритетів безпеки.

Кінцевим кроком дослідження передбачено практичну апробацію технології у діяльності діючого ТЛЦ для підтвердження її практичної цінності та оцінки організаційної ефективності впровадження.

## **Висновки до розділу 1**

У даному розділі проведено комплексний аналіз проблеми підтримки прийняття рішень в управлінні ІБ ТЛЦ, що дозволяє сформулювати наступні висновки.

Проаналізовано специфіку ІБ для ТЛЦ. Встановлено, що ТЛЦ є стратегічними об'єктами критичної інфраструктури, життєво важливими для економіки та обороноздатності України. Їхня унікальна вразливість зумовлена глибокою конвергенцією інформаційних та операційних технологій (WMS, TMS, AS/RS), а також розмитим периметром безпеки через високий ступінь інтеграції з зовнішніми системами (митниця, постачальники). Розроблена модель загроз класифікувала 8 категорій специфічних ризиків, що підтверджує кіберфізичну природу загроз.

Досліджено основні методи оцінки ІБ. Огляд світових стандартів (NIST, ISO), спеціалізованих методологій (CORAS, HAZOP, EBIOS) та архітектур існуючих СППР (експертних, процесних, когнітивних) показав, що, хоча існує багато інструментів, оптимальним для ТЛЦ є диференційований підхід.

Виявлено головний недолік існуючих підходів – це їхня нездатність адекватно працювати в умовах глибокої невизначеності. Існуючі системи є статичними та суб'єктивними (експертні системи), негнучкими. Вони не надають інструментів для здійснення стратегічного аналізу та механізмів для обробки нечітких лінгвістичних оцінок експертів при обмеженості статистичних даних про новітні загрози.

Сформульовано мету та задачі дослідження. Виявлена науково-практична проблема – розрив між потребами ТЛЦ у гнучкому стратегічному інструменті та

обмеженістю існуючих методів, що не враховують невизначеність, обґрунтовує мету дослідження: розробку інформаційної технології на основі гібридних інтелектуальних моделей (Fuzzy AHP, ANFIS), здатної комплексно оцінювати ризики ІБ ТЛЦ та підтримувати прийняття рішень щодо оптимізації захисту. Сформульовані етапи дослідження є послідовними кроками для досягнення поставленої мети.

Результати досліджень, наведених в розділі, опубліковані в роботах [11], [12], [16], [17].



## **РОЗДІЛ 2. МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТРАНСПОРТНО-ЛОГІСТИЧНОГО ЦЕНТРУ**

### **2.1 Концептуальна модель інтегрального оцінювання рівня ризику ІБ ТЛЦ**

Аналіз, проведений у першому розділі, продемонстрував, що ТЛЦ є складним кіберфізичним об'єктом, який функціонує в умовах глибокої невизначеності [69], [70]. Специфіка захисту ТЛЦ характеризується неповнотою вхідних даних, нечіткістю експертних оцінок та стохастичною природою кібератак. Існуючі методи оцінки ризиків є переважно статичними, що зумовлює необхідність розробки адаптивної ІТ ППР [17], [20], здатної реагувати на зміни ландшафту загроз у реальному часі [71].

Для реалізації такої технології розроблено концептуальну модель інтегрального оцінювання рівня ризику ІБ ТЛЦ, яка базується на гібридному підході [72]. Цей підхід системно поєднує експертні знання з адаптивністю машинного навчання, інтегруючи різноманітні математичні методи для вирішення специфічних задач на кожному етапі [73]. Зокрема:

- для формалізації лінгвістичних оцінок – нечітка логіка (Fuzzy Logic) [74], [75];
- для ієрархічної пріоритезації факторів ризику за допомогою нечітких чисел – метод Fuzzy AHP [76], [77];
- для самонавчання моделі на основі історичних даних – адаптивні нейронечіткі системи (ANFIS) [78], [79].

Графічна інтерпретація запропонованої концептуальної моделі наведена на рисунку 2.1.

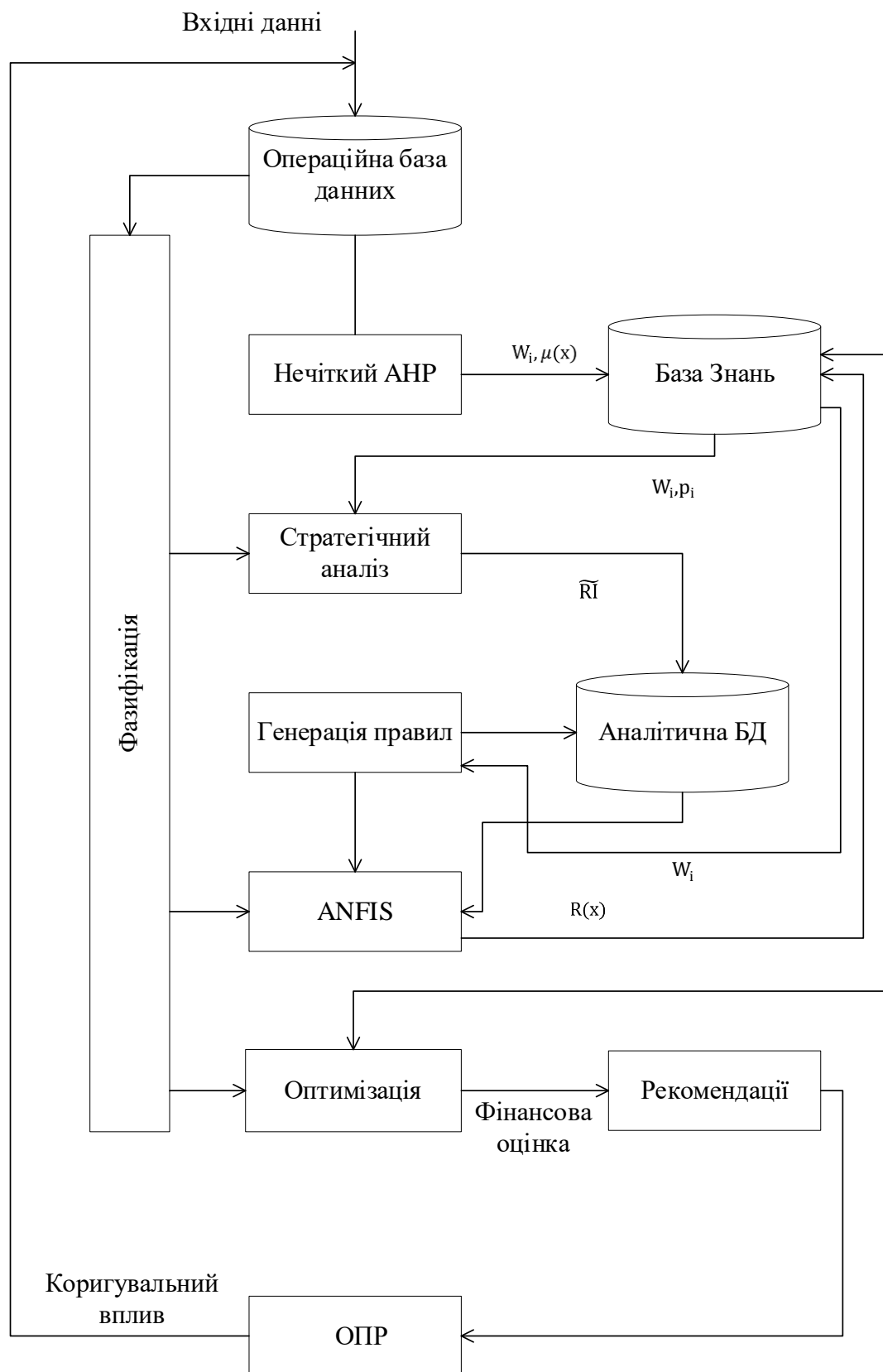


Рисунок 2.1 – Концептуальна модель інтегрального оцінювання рівня ризику ІБ  
ТЛЦ

Модель побудована за модульним принципом і складається з 6 взаємопов'язаних блоків, що забезпечують повний цикл обробки інформації від отримання необроблених даних до формування керуючих впливів. Функціональне призначення модулів наведено у таблиці 2.1.

Таблиця 2.1 – Функціональна структура моделі інтегрального оцінювання рівня ризику ІБ ТЛЦ

№	Модуль моделі	Призначення та функції у моделі
1	Фазифікація	Формалізація вхідних даних. Перетворення чітких значень або якісних лінгвістичних оцінок у нечіткі змінні [80], [81].
2	Fuzzy АНР	Пріоритезація факторів. Розрахунок вагових коефіцієнтів ( $w_i$ ) на основі матриць парних порівнянь для встановлення ієрархії загроз [77], [82].
3	Стратегічний аналіз	Аналіз стратегічного стану ІБ ТЛЦ на основі удосконаленої матриці Дж. Х. Вілсона [83], [84] та експертної інтегральної оцінки $\widetilde{RI}$ методом Fuzzy SAW [85] з урахуванням рівня впевненості експерта.
4	Генерація бази правил	Формування простору знань відбувається шляхом логічної побудови повного набору продукційних правил («ЯКЩО-ТО») на основі структури факторів. Це фундамент для вирішення проблеми дефіциту вхідних даних. Система автоматично генерує синтетичну навчальну вибірку (використовуючи рушій Мамдані), що забезпечує коректне первинне налаштування параметрів ще до появи реальної статистики інцидентів [86].
5	ANFIS	Адаптивне нейромережеве ядро. На першому етапі здійснюється апроксимація (первинне навчання) на основі згенерованої вибірки, а на другому етапі – адаптація параметрів під реальні інциденти для розрахунку $R(X)$ [87].
6	Оптимізація	Інтелектуальна підтримка прийняття рішень. Пошук оптимального вектора керуючих впливів для мінімізації функціоналу інтегрального ризику при заданих ресурсних обмеженнях [88].

Критично важливою особливістю є чітке розмежування потоків даних та логічних структур через взаємодію двох сховищ.

1. *Операційна база даних (ОБД)* – вхідний інформаційний вузол системи, призначений для інтеграції та первинної обробки різномірних даних у реальному часі. Вона виступає інтелектуальним шлюзом, що забезпечує збір та верифікацію необробленої інформації від сенсорів, SIEM-систем та експертів для потреб модулів попередньої обробки (Фазифікації та Fuzzy АНР).

ОБД зберігає дані ключових інформаційних потоків, що забезпечують

безперервний цикл аналізу ризиків. Основний масив складають дані поточного моніторингу, представлені часовими рядами індикаторів безпеки (кількість спроб доступу, обсяг трафіку, стан портів), які надходять від мережевих сенсорів. Для їх первинної обробки в архітектурі передбачено використання алгоритму агрегованої динамічної оцінки [89], що дозволяє згорнути множину параметрів у єдиний вектор стану безпеки в режимі реального часу.

З метою виявлення прихованих закономірностей у потоках даних може бути використаний фрактальний детектор трафіка [90]. Цей інструмент дозволяє ідентифікувати аномальну активність на ранніх стадіях її виникнення через аналіз самоподібності трафіку, що суттєво підвищує чутливість моделі до складних загроз. Додатково проводиться моніторинг поведінкових факторів [91], що забезпечує комплексний захист від цільових атак, які не завжди мають виражені технічні аномалії.

Окрему складову ОБД становлять вхідні експертні дані, зокрема необроблені матриці парних порівнянь та анкети фахівців, що слугують основою для розрахунку вагових коефіцієнтів ієрархії загроз. Також до бази надходять дані зворотного зв'язку щодо зміни стану системи після впровадження рекомендованих захисних заходів. Це дозволяє в динаміці оцінювати їхню ефективність та коригувати параметри моделі відповідно до реального стану захищеності ТЛЦ.

*Аналітична база даних (АБД)* – репозитарій аналітичної статистики та навчальних вибірок. Він виконує функцію довгострокового сховища верифікованих інцидентів та є джерелом даних – «вчителем» для навчання та адаптації нейромережі ANFIS. Її призначення полягає у забезпеченні можливості переходу від статичного експертного оцінювання до динамічного адаптивного навчання на основі накопичених даних. Основу АБД становить історія оцінок, яка об'єднує результати стратегічних  $\widetilde{RI}$  та уточнених адаптивних показників ризику  $R(X)$ , створюючи базу для аналізу динаміки стану безпеки ТЛЦ. Паралельно з цим у базі накопичується верифікована статистика реальних інцидентів у вигляді

навчальних пар «вхід  $\rightarrow$  вихід», які є емпіричною базою для періодичного автоматизованого перенавчання моделі та уточнення її параметрів під впливом нових загроз.

Синтетична навчальна вибірка розв'язує проблему початкової невизначеності шляхом трансформації якісного експертного досвіду в кількісний масив для навчання нейромережі. Процес її формування передбачає генерацію репрезентативної множини входних векторів  $(x_1, \dots, x_n)$ , що охоплюють весь фазовий простір станів системи. Ці вектори обробляються рушієм нечіткого виведення Мамдані (модуль 4), який, спираючись на базу правил, генерує відповідні еталонні значення. Сформований набір пар «вхід–вихід» ( $X \rightarrow Y$ ) стає основою для навчання з учителем архітектури ANFIS. Це дозволяє системі засвоїти логіку експертних рішень ще до накопичення реальної статистики інцидентів, що забезпечує високу точність оцінювання ризиків з першого дня експлуатації технології.

*База знань (БЗ)* – інтелектуальне ядро та репозиторій моделі. В ній акумулюється повна математична структура системи. Вона містить структурні метадані, що визначають ієрархію та логічні зв'язки між факторами ризику, а також систему продукційних правил, які пов'язують умови та відповідні їм висновки. Математичний базис БЗ розподілено на параметри антецедентів (умова «ЯКЩО») та консеквентів (висновок «ТО»). У частині антецедентів зберігаються типи та параметри функцій належності, зокрема їх центри ( $c$ ) та ширина ( $\sigma$ ), які підлягають динамічній адаптації. Оскільки модель реалізована на архітектурі ANFIS, висновки правил формуються за алгоритмом Такагі-Сугено, де замість статичних лінгвістичних оцінок використовується структура поліномів  $f(x)$  та матриця налаштовуваних коефіцієнтів, що визначають внесок кожного входного фактора в загальний результат правила.

Динамічний характер БЗ забезпечується через реалізацію циклічного зв'язку між інформаційними сховищами. Модуль ANFIS зчитує входні факти з ОБД (синтетичні або реальні інциденти) та здійснює розрахунок похибки

прогнозування. Шляхом мінімізації цієї похибки нейромережа генерує оновлені набори параметрів, які автоматично перезаписуються у БЗ, замінюючи застарілі оцінки. Такий механізм самоорганізації дозволяє БЗ еволюціонувати синхронно зі зміною ландшафту загроз, підтримуючи актуальність логічного виведення в умовах мінливого середовища ТЛЦ.

Математичний апарат моделі передбачає розрахунок інтегрального показника рівня ризику  $R$  на двох рівнях, що дозволяє досягти балансу між швидкістю прийняття рішень та точністю отриманих оцінок.

На першому рівні здійснюється експертна інтегральна оцінка ( $\widetilde{RI}$ ), що формується за результатами роботи модуля 3 методом лінійної згортки (Fuzzy SAW) з урахуванням впевненості експерта, що дозволяє нівелювати вплив суб'єктивності на ранніх етапах аналізу та оперативно виявляти критичні вразливості ІБ ТЛЦ.

На другому рівні виконується уточнена адаптивна оцінка ( $R(X)$ ), що розраховується нейронечіткою мережею (модуль 5), яка враховує нелінійні ефекти та синергію факторів. Це забезпечує високу точність результатів на основі реальної статистики інцидентів.

Практична реалізація запропонованої концептуальної моделі вимагає формування єдиного методологічного простору. Функціонування архітектури забезпечується синергією наступних методів та підходів.

Математичний апарат нечіткої логіки (Fuzzy Logic) є базовим засобом формалізації якісних експертних суджень. Використовується в модулях 1 та 4 для перетворення лінгвістичних змінних у кількісні значення через функції належності в безперервному діапазоні  $[0, 1]$ , що дозволяє математично оперувати категоріями типу «високий ризик» або «низька впевненість».

Метод нечіткого аналізу ієрархій (Fuzzy АНР) у модулі 2 виступає інструментом пріоритезації чинників ризику. Використання нечітких трикутних чисел у межах модифікованого класичного методу Т. Сааті [92] забезпечує високу достовірність визначення пріоритетності загроз шляхом математичної

формалізації неоднозначності експертних суджень під час парного порівняння факторів.

Метод Fuzzy SAW, реалізований у модулі 3, базується на використанні нечіткої арифметики для агрегування лінгвістичних терм-оцінок факторів ризику. Специфіка методу полягає у впровадженні вагового коефіцієнта впевненості експерта, який масштабує результат згортки залежно від надійності джерела інформації. Такий підхід дозволяє формалізувати ступінь достовірності експертного висновку та забезпечує верифікацію даних ще на етапі стратегічного аналізу, запобігаючи врахуванню сумнівних оцінок у подальших обчисленнях.

Гібридний метод навчання ANFIS становить інтелектуальну основу модуля 5. П'ятишарова нейронна мережа реалізує нечітке виведення типу Такагі-Сугено, поєднуючи алгоритм зворотного поширення похибки та метод найменших квадратів. Це забезпечує структурно-параметричну ідентифікацію моделі ризику  $R(X)$  шляхом трансформації якісних експертних правил у точні нелінійні залежності, що адаптуються під впливом реальної статистики інцидентів.

Методи математичного програмування та умовної оптимізації застосовуються у модулі 6 для інтелектуальної підтримки прийняття рішень. Процес ґрунтується на розв'язанні задачі мінімізації цільової функції інтегрального ризику  $R(X)$  при заданих ресурсних, часових та бюджетних обмеженнях. Це дозволяє трансформувати результати адаптивного моделювання у конкретний вектор оптимальних захисних заходів для ТЛЦ.

Комплексний підхід забезпечує фундамент побудови системи, що інтегрує інструментарій експертного аналізу (Fuzzy AHP, SAW) для нівелювання апріорної невизначеності та методи обчислювального інтелекту (ANFIS) для динамічної адаптації моделі до нових емпіричних даних.

Таким чином, застосування запропонованої концептуальної моделі спрямоване на забезпечення підвищення ефективності управління ризиками ІБ ТЛЦ. Це досягається завдяки поєднанню експертного досвіду з адаптивними алгоритмами самонавчання. Це надає можливість оперативної ідентифікації

загроз та оптимізації витрат на захисні заходи. Така архітектура спрямована на досягнення цільового рівня безпеки об'єкта в умовах високої невизначеності та обмеженості ресурсів.

Математичний апарат та алгоритмічна реалізація кожного модуля моделі розглядаються у наступних підрозділах.

## **2.2 Експертна нечітка модель стратегічного аналізу факторів ризику ІБ ТЛЦ**

Для реалізації експертної нечіткої моделі стратегічного аналізу факторів ризику ІБ ТЛЦ пропонується комплексний метод, що поєднує експертні знання та теорію нечітких множин.

Методологічну основу моделі складають стандарти ISO/IEC 27005, NIST RMF. Для ідентифікації технічних загроз адаптовано STRIDE та OWASP. Оцінка експлуатаційної надійності об'єктів ТЛЦ базується на методах FMEA та HAZOP. Інтеграція кількісних та якісних показників реалізована із залученням CORAS та FAIR.

Узагальнена графічна інтерпретація ієрархічної структури експертної нечіткої моделі стратегічного аналізу факторів ризику наведена на рисунку 2.2.

Нижче наведено детальну реалізацію кожного етапу ієрархії.

*Етап 1. Ідентифікація факторів і підфакторів.* Цей етап ґрунтується на структурній декомпозиції процесу оцінювання ризиків, що дозволяє представити складну систему безпеки ТЛЦ у вигляді впорядкованої ієрархії. Враховуючи високий ступінь невизначеності вхідних даних, параметри моделі доцільно розглядати не як чіткі числа, а як лінгвістичні змінні. Це дозволяє формалізувати експертні знання та врахувати різномірну природу факторів впливу.



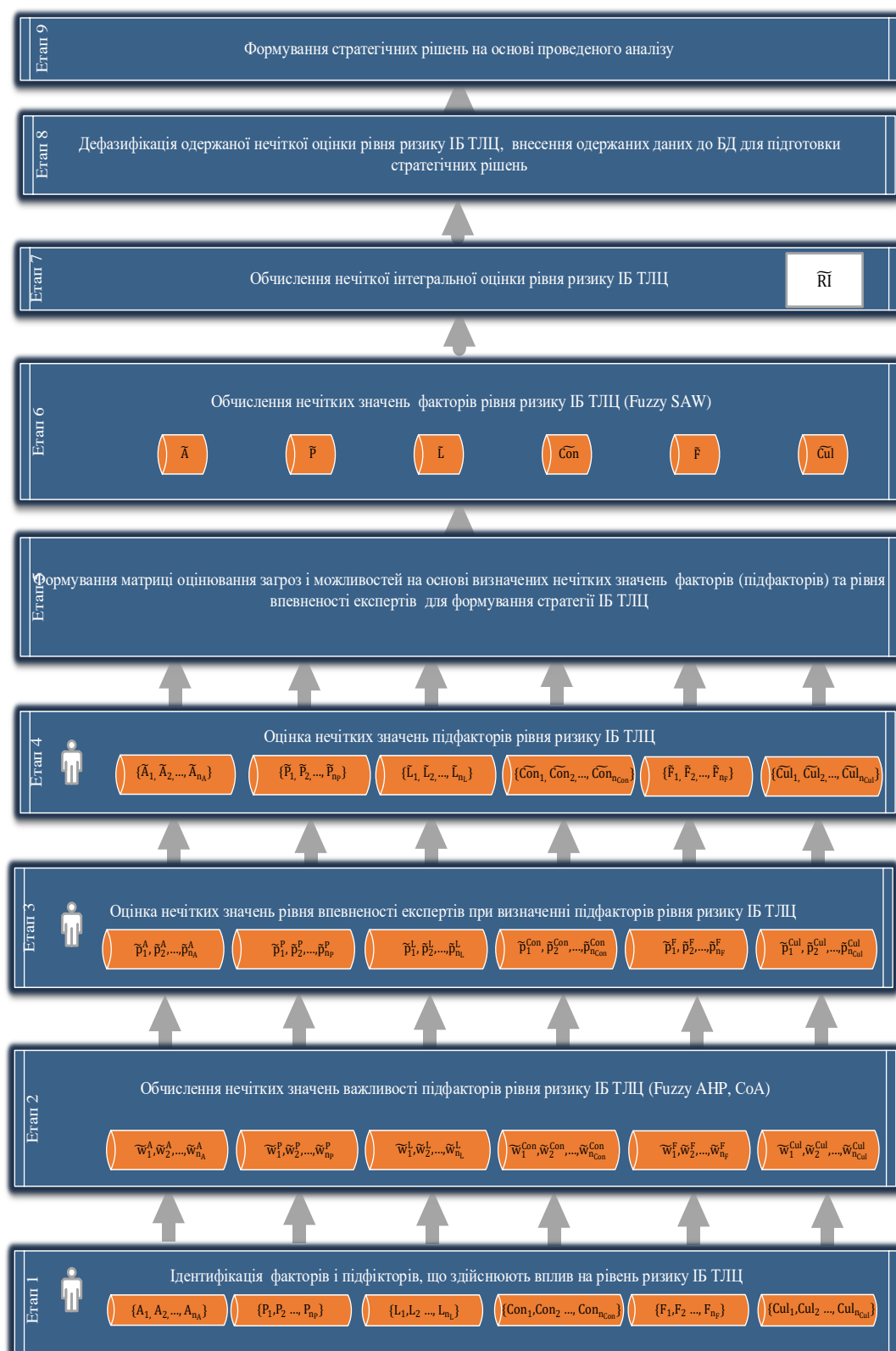


Рисунок 2.2 – Ієрархічна структура експертної нечіткої моделі стратегічного аналізу факторів ризику ІБ ТЛЦ

До множини факторів оцінювання віднесено: цінність активів, ймовірність реалізації загрози через наявні вразливості, збитки від загроз, рівень управління інформаційними ресурсами, витрати на створення та експлуатацію системи захисту, а також культуру інформаційної безпеки.

Формалізація та змістовна характеристика цих факторів наведена у таблиці 2.2.

Таблиця 2.2 – Формалізація та змістовна характеристика факторів ризику ІБ ТЛЦ

Умовне позначення	Найменування фактору ризику	Змістовна інтерпретація показника
<i>A</i>	Рівень цінності активів	Кількісна міра критичності інформаційних та матеріальних ресурсів (апаратного забезпечення, ПЗ, баз даних) для забезпечення безперервності бізнес-процесів. Визначається через потенціал порушення конфіденційності, цілісності або доступності [89], [90], [91].
<i>P</i>	Ймовірність реалізації загрози через наявні вразливості	Ймовірнісна оцінка можливості успішної експлуатації вразливостей системи певним джерелом загрози. Розраховується як функція від частоти виникнення інцидентів та наявності передумов для атаки [63], [90].
<i>Los</i>	Рівень збитків від загроз	Оцінка масштабу негативних наслідків (фінансових, репутаційних, операційних) для ТЛЦ у випадку реалізації загрози. Враховує стратегічні цілі підприємства та вартість відновлення штатного режиму функціонування [63], [90], [92].
<i>Con</i>	Рівень контролю інформаційних ресурсів	Характеристика ефективності механізмів моніторингу інформаційних потоків, прогнозування логістичних навантажень, аналізу зовнішнього середовища та управління зв'язками з громадськістю [92].
<i>F</i>	Рівень витрат на створення та функціонування СУБ	Показник ресурсних затрат – співвідношення витрат на розробку, впровадження та супровід комплексної системи захисту інформації до величини відвернених збитків. Відображає економічну доцільність захисних заходів (вартість менше пошкодження) [90], [93].
<i>Cul</i>	Рівень культури інформаційної безпеки	Інтегральний показник, що характеризує рівень компетентності персоналу, ступінь усвідомлення ризиків та дисципліну дотримання політик ІБ, виступаючи фактором мінімізації ризиків соціальної інженерії [99], [100], [101].

Математичне представлення моделі оцінки рівня ризику:

$$R = f(A, P, Los, Con, F, Cul), \quad (2.1)$$

де  $R$  – рівень ризику ІБ ТЛЦ;

$A = \{A_1, A_2, \dots, A_j\}$  – рівень цінності активів;

$P = \{P_1, P_2, \dots, P_i\}$  – імовірність реалізації загрози через наявні вразливості;

$Los = \{Los_1, Los_2, \dots, Los_k\}$  – рівень збитків від загроз;

$Con = \{Con_1, Con_2, \dots, Con_n\}$  – рівень контролю інформаційних ресурсів;

$F = \{F_1, F_2, \dots, F_m\}$  – рівень витрат на створення та експлуатацію ІБ системи;

$Cul = \{Cul_1, Cul_2, \dots, Cul_s\}$  – рівень культури інформаційної безпеки.

На основі визначених факторів побудовано повну ієрархічну модель класифікації, яка декомпозує глобальну мету оцінювання на підфактори другого та третього рівнів [102]. Графічна інтерпретація моделі наведена на рис. 2.3.

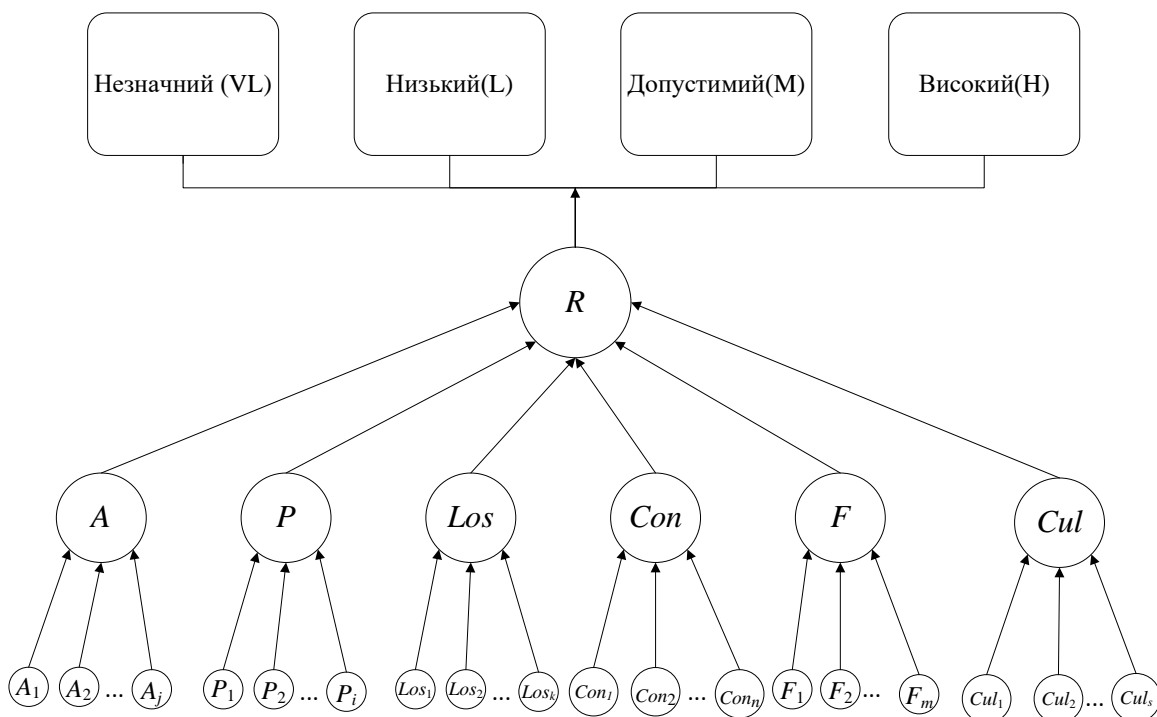


Рисунок 2.3 – Ієрархічна модель класифікації факторів для оцінки рівня ризику ІБ ТЛЦ

Детальний склад ієрархічної моделі з описом елементів декомпозиції наведено у таблиці 2.3.

Таблиця 2.3 – Трирівнева ієрархічна модель факторів ризику ІБ ТЛЦ

Рівень 1 Фактор	Рівень 2 Підфактор	Рівень 3 Елемент декомпозиції
Рівень цінності активів $A = \{A_1, A_2, \dots, A_{n_A}\}$	A1. Дані	A1.1. Дані про вантажі
		A1.2. Дані про маршрути
		A1.3. Дані клієнтів
		A1.4. Фінансові дані
		A1.5. Інформація про запаси
		A1.6. Дані про дотримання норм
	A2. Системи	A2.1. TMS (система управління транспортом)
		A2.2. WMS (система управління складом)
		A2.3. GPS/GLONASS
		A2.4. ERP (система планування ресурсів)
		A2.5. Системи зв'язку (диспетчери)
		A2.6 Системи EDI/API
	A3. Репутація компанії	A3.1. Довіра клієнтів/партнерів
		A3.2. Здатність виконувати зобов'язання
		A3.3. Фінансова стабільність
		A3.4. Надійність для державних/гуманітарних контрактів
		A3.5 Прозорість для міжнародних партнерів
Ймовірність реалізації загроз $P = \{P_1, P_2, \dots, P_{n_P}\}$	P1. Кібератаки	P1.1. Технічна реалізація (фішинг)
		P1.2. Атаки на ланцюг поставок
		P1.3. Атаки на вебзастосунки та БД
		P1.4. Атаки на хмарні інфраструктури
		P1.5. АРТ-атаки (державні актори)
		P1.6. Атаки на ОТ-системи (кіберфізичні)
	P2. Людський фактор	P2.1. Психологічна вразливість персоналу
		P2.2. Недбалість та помилки
		P2.3. Внутрішні зловмисники
		P2.4. Фізична та психологічна втома
		P2.5. Брак кваліфікації для нових загроз
Рівень збитків від загроз $Los = \{Los_1, Los_2, \dots, Los_{n_P}\}$	Los1. Операційні збитки	Los1.1. Повна зупинка логістики (WMS/TMS)
		Los1.2. Параліч операцій (втрата зв'язку)
		Los1.3. Втрата/пошкодження вантажів
		Los1.4. Втрата цілісності даних
		Los1.5. Втрата ключових маршрутів/вузлів
	Los2. Фінансові збитки	Los2.1. Втрата доходів (через простої)
		Los2.2. Пряме фізичне знищення активів
		Los2.3. Витрати на відновлення (включаючи викуп)
		Los2.4. Штрафи та компенсації (контракти)
		Los2.5. Підвищення витрат на страхування
	Los3. Репутаційні збитки	Los3.1. Втрата довіри клієнтів/партнерів
		Los3.2. Зниження конкурентоспроможності
		Los3.3. Втрата державних/оборонних

Рівень 1 Фактор	Рівень 2 Підфактор	Рівень 3 Елемент декомпозиції
		контрактів
		Los3.4. Потрапляння до «чорних списків» партнерів
		Los3.5. Звинувачення у сприянні ворогу
	Los4. Безпека та правові наслідки	Los4.1. Загроза життю і здоров'ю
		Los4.2. Кримінальна відповідальність (недбалість, держзрада)
		Los4.3. Судові позови / розслідування
		Los4.4. Втрата ліцензій (митного брокера)
		Los4.5. Екологічні збитки
Рівень контролю $Con$ $= \{Con_1, Con_2, \dots, Con_{n_{con}}\}$	Con1. Технічні засоби	Con1.1. Системи моніторингу та управління доступом (SIEM, IAM, MFA, сегментація)
		Con1.2. Засоби захисту периметру та кінцевих точок (NGFW, IDS/IPS, EDR)
		Con1.3. Засоби безперервності та конфіденційності (резервне копіювання, шифрування, VPN)
		Con1.4. Захист OT-сегменту
		Con1.5. Резервні/захищені канали зв'язку
		Con1.6. Системи фізичної ІБ
	Con2. Організаційні заходи	Con2.1. Політики та Регламенти надзвичайних ситуацій
		Con2.2. Управління ризиками ланцюга поставок (SCRM)
		Con2.3. Фізична безпека
		Con2.4. Аудит та управління вразливостями
		Con2.5. Перевірка персоналу (Background checks)
		Con2.6. Процедури взаємодії з державними органами
Рівень витрат $F = \{F_1, F_2, \dots, F_{n_F}\}$	F1. Інвестиції в персонал та процеси (OpEx)	F1.1. Технічне обслуговування та супровід (включаючи ЗП фахівців)
		F1.2. Навчання та підвищення кваліфікації
		F1.3. Проведення аудитів та тестування
		F1.4. Закупівля даних Threat Intelligence
		F1.5. Витрати на страхування
	F2. Інвестиції в технології (CapEx)	F2.1. Закупівля ПЗ/АЗ безпеки (SIEM, EDR, Backups)
		F2.2. Інфраструктура відновлення
		F2.3. Створення резервного (гео-розподіленого) центра обробки даних (ЦОД)
		F2.4. Автономне/резервне живлення
		F2.5. Фізичне укріплення ЦОД
Рівень культури ІБ	Cul1. Позиція адміністрації	Cul1.1. Включення ІБ в бізнес-стратегію
		Cul1.2. Виділення адекватних ресурсів
		Cul1.3. Особиста участь

Рівень 1 Фактор	Рівень 2 Підфактор	Рівень 3 Елемент декомпозиції
$Cul$ $= \{Cul_1, Cul_2, \dots, Cul_{nCul}\}$	$Cul2.$ компетенції з ІБ працівників	Cul1.4. Політика нульової толерантності
		Cul2.1. Навчання диспетчерів (соціальна інженерія)
		Cul2.2. Регулярні тренінги (фішинг, паролі)
		Cul2.3. Тестування (фішинг-симуляції)
		Cul2.4. Програми підвищення обізнаності
		Cul2.5. Навчання з реагування на надзвичайні ситуації (воєнні)
	$Cul3.$ Контроль над діями	Cul3.1. Дотримання політик
		Cul3.3. Моніторинг дій користувачів
		Cul3.2. Політики чистого столу/блокування

Запропонована ієрархічна модель охоплює всі критичні аспекти функціонування ТЛЦ, що дозволяє перейти до етапу оцінювання вагових коефіцієнтів.

*Етап 2. Обчислення нечітких значень важливості факторів (підфакторів).* Метою другого етапу стратегічного аналізу є визначення вектора вагових коефіцієнтів  $W = \{w_A, w_P, w_{Los}, w_{Con}, w_F, w_{Cul}\}$ , який відображає ступінь впливу кожного факторів на інтегральний рівень ризику ІБ ТЛЦ. Процедура базується на експертному оцінюванні та включає наступні кроки.

*Крок 1. Побудова нечіткої матриці парних порівнянь.* Експерти (або група експертів) здійснюють попарне порівняння факторів, використовуючи лінгвістичні терми Т1, наведені в таблиці 2.4. Для математичної формалізації цих оцінок використовуються трикутні нечіткі числа (TFN).

Результати порівняння подаються у вигляді нечіткої квадратної матриці  $\tilde{Q}$ :

$$\tilde{Q} = (\tilde{q}_{ij})_{n \times n} = \begin{bmatrix} (1,1,1) & \tilde{q}_{12} & \dots & \tilde{q}_{1n} \\ \tilde{q}_{21} & (1,1,1) & \dots & \tilde{q}_{2n} \\ \dots & \dots & \dots & \dots \\ \tilde{q}_{n1} & \tilde{q}_{n2} & \dots & (1,1,1) \end{bmatrix}, \quad (2.2)$$

де  $\tilde{q}_{ij} = (\alpha_{ij}, \beta_{ij}, \gamma_{ij})$  – нечітка оцінка переваги  $i$ -го фактора над  $j$ -м;

$\tilde{q}_{ji} = \tilde{q}_{ij}^{-1} = (\frac{1}{\gamma_{ij}}, \frac{1}{\beta_{ij}}, \frac{1}{\alpha_{ij}})$ ,  $i, j = 1, \dots, n$ ,  $i \neq j$  – обернена оцінка.

Для перетворення лінгвістичних суджень експертів у нечіткі числа використано стандартну шкалу Сааті, адаптовану для нечіткої логіки (табл. 2.4) [77].

Таблиця 2.4 – Шкала АНР та відповідні трикутні нечіткі числа

	Лінгвістична змінна	Позначення	Шкала TFN $\alpha_{ij}(\alpha_{ij}, \beta_{ij}, \gamma_{ij})$	Обернене значення $\alpha_{ji}(1/\gamma_{ij}, 1/\beta_{ij}, 1/\alpha_{ij})$
1	Рівнозначність	E	(1,1,1)	(1,1,1)
2	Дуже слабка перевага	E&M	(1,2,3)	(1/3, 1/2, 1)
3	Помірна перевага	M	(2,3,4)	(1/4, 1/3, 1/2)
4	Помірно-сильна перевага	M&S	(3,4,5)	(1/5, 1/4, 1/3)
5	Перевага	S	(4,5,6)	(1/6, 1/5, 1/4)
6	Сильна перевага	S&VS	(5,6,7)	(1/7, 1/6, 1/5)
7	Більш ніж сильна перевага	VS	(6,7,8)	(1/8, 1/7, 1/6)
8	Дуже сильна перевага	VS&ES	(7,8,9)	(1/9, 1/8, 1/7)
9	Екстремальна перевага	ES	(8,9,9)	(1/9, 1/9, 1/8)

Графічна інтерпретація функцій належності для використаної шкали оцінювання наведена на рисунку 2.5.

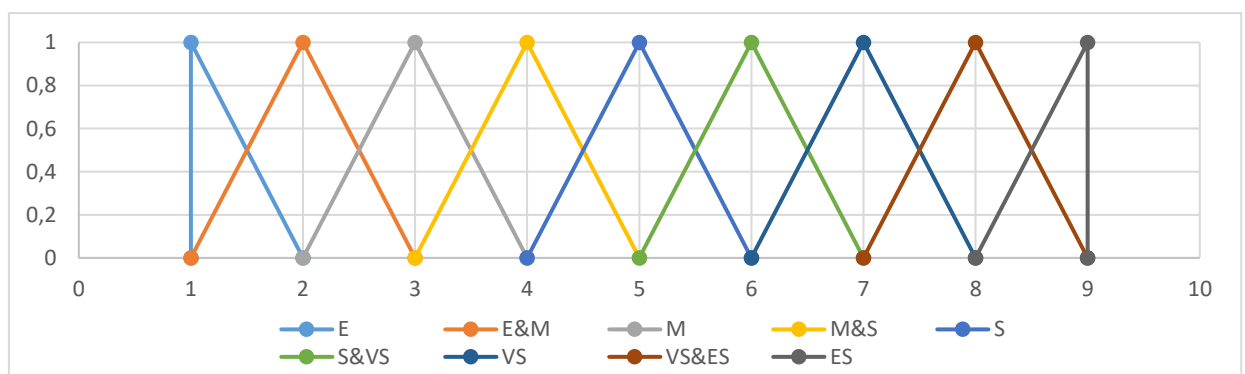


Рисунок 2.4 – Функції належності термів при застосуванні методу Fuzzy АНР

У випадку групового оцінювання ( $K$  експертів), індивідуальні оцінки агрегуються за допомогою геометричного середнього перед проведенням подальших розрахунків. Нехай  $\tilde{q}_{ijk}$  – оцінка  $k$ -го експерта при порівнянні  $i$ -го фактора з  $j$ -м. Тоді агреговане значення  $\tilde{q}_{ij}$  розраховується за формулою:

$$\tilde{q}_{ij} = (\tilde{q}_{ij}^1 \otimes \tilde{q}_{ij}^2 \otimes \dots \otimes \tilde{q}_{ij}^K)^{\frac{1}{K}} = \left( \prod_{k=1}^K l_{ijk}^{\frac{1}{K}}, \prod_{k=1}^K m_{ijk}^{\frac{1}{K}}, \prod_{k=1}^K u_{ijk}^{\frac{1}{K}} \right), \quad (2.3)$$

де  $\tilde{q}_{ij} = (l_{ij}, m_{ij}, u_{ij})$  – елементи агрегованої матриці парних порівнянь  $\tilde{Q}$ .

*Крок 2.* Розрахунок нечітких синтетичних значень методом Чанга (Chang D. Y.) [103], [104]. На рисунку 2.5 представлена блок-схема алгоритму розрахунку ваг методом Чанга.

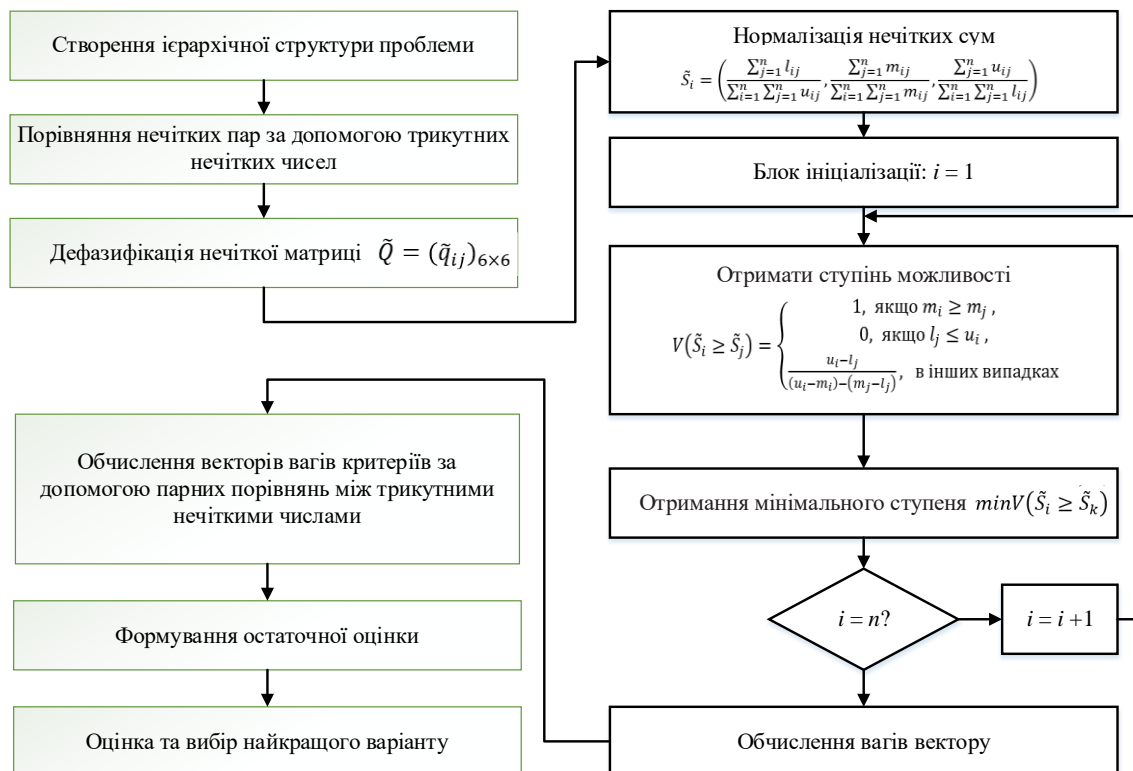


Рисунок 2.5 – Блок-схема алгоритму розрахунку ваг методом розширеного аналізу Чанга

Згідно з наведеною схемою, для кожного фактора обчислюється значення нечіткої агрегованої оцінки  $\tilde{S}_i$ , яке характеризує відносний вклад цього фактора до загальної структури ризику. Розрахунок виконується за формулою:

$$\tilde{S}_i = \sum_{j=1}^n \tilde{q}_{ij} \otimes \left[ \sum_{i=1}^n \sum_{j=1}^n \tilde{q}_{ij} \right]^{-1} = \left( \frac{\sum_{j=1}^n l_{ij}}{\sum_{i=1}^n \sum_{j=1}^n u_{ij}}, \frac{\sum_{j=1}^n m_{ij}}{\sum_{i=1}^n \sum_{j=1}^n m_{ij}}, \frac{\sum_{j=1}^n u_{ij}}{\sum_{i=1}^n \sum_{j=1}^n l_{ij}} \right), \quad (2.4)$$

де  $n$  – кількість факторів (розмірність матриці парних порівнянь);

$l_{ij}, m_{ij}, u_{ij}$  – нижня, середня та верхня межі нечіткого числа  $\tilde{a}_{ij}$ , що відповідає оцінці  $i$ -го фактора відносно  $j$ -го;

$\sum_{j=1}^n l_{ij}$  – сума нижніх меж оцінок для конкретного  $i$ -го рядка (локальна вага);

$\sum_{i=1}^n \sum_{j=1}^n u_{ij}$  – загальна сума верхніх меж усіх елементів матриці.



Сума  $n$  трикутних чисел знаходиться як:

$$\sum_{j=1}^n \tilde{q}_{ij} = (\sum_{j=1}^n l_{ij}, \sum_{j=1}^n m_{ij}, \sum_{j=1}^n u_{ij}). \quad (2.5)$$

*Крок 3.* Обчислення ступеня можливості. На цьому етапі у методі Чанга виникає ризик «нульових ваг». Ступінь можливості того, що  $\tilde{S}_i \geq \tilde{S}_j$ , визначається як:

$$V(\tilde{S}_i \geq \tilde{S}_j) = \sup_{x \geq y} [\min(\mu_{S_i}(x), \mu_{S_j}(y))]. \quad (2.6)$$

Для трикутних чисел це значення розраховується аналітично:

$$V(\tilde{S}_i \geq \tilde{S}_j) = \begin{cases} 1, & \text{якщо } m_i \geq m_j, \\ 0, & \text{якщо } l_j \leq u_i, \\ \frac{u_i - l_j}{(u_i - m_i) - (m_j - l_j)}, & \text{в інших випадках} \end{cases}, \quad (2.7)$$

де  $\tilde{S}_i = (l_i, m_i, u_i)$ ,  $\tilde{S}_j = (l_j, m_j, u_j)$ .

Первинна (ненормалізована) вага фактора визначається як мінімальний ступінь можливості того, що він переважає всі інші фактори:

$$d_i = \min V(\tilde{S}_i \geq \tilde{S}_k), k = 1, \dots, n; k \neq i. \quad (2.8)$$

Вектор ваг нормалізується для отримання фінальних значень за методом Чанга:

$$w_i^{ch} = \frac{d_i}{\sum_{k=1}^n d_k}. \quad (2.9)$$

Аналіз практичного застосування методу Чанга виявив суттєвий недолік: коли функції належності нечітких чисел мають малу площу перетину, метод може привласнювати факторам нульові ваги ( $w_i = 0$ ), навіть якщо експерти надали їм значущість. Це є неприпустимим для критичних систем безпеки де ігнорування навіть малого ризику може мати фатальні наслідки.

З метою усунення цього недоліку, пропонуємо удосконалений підхід, що полягає у інтеграції методу Чанга з алгоритмом Баклі (Buckley's geometric mean method). Такий підхід дозволяє отримати стійку оцінку.

*Крок 4.* Розрахунок ваг за методом Баклі [105]. Логіка цього процесу наведена на рисунку 2.6.

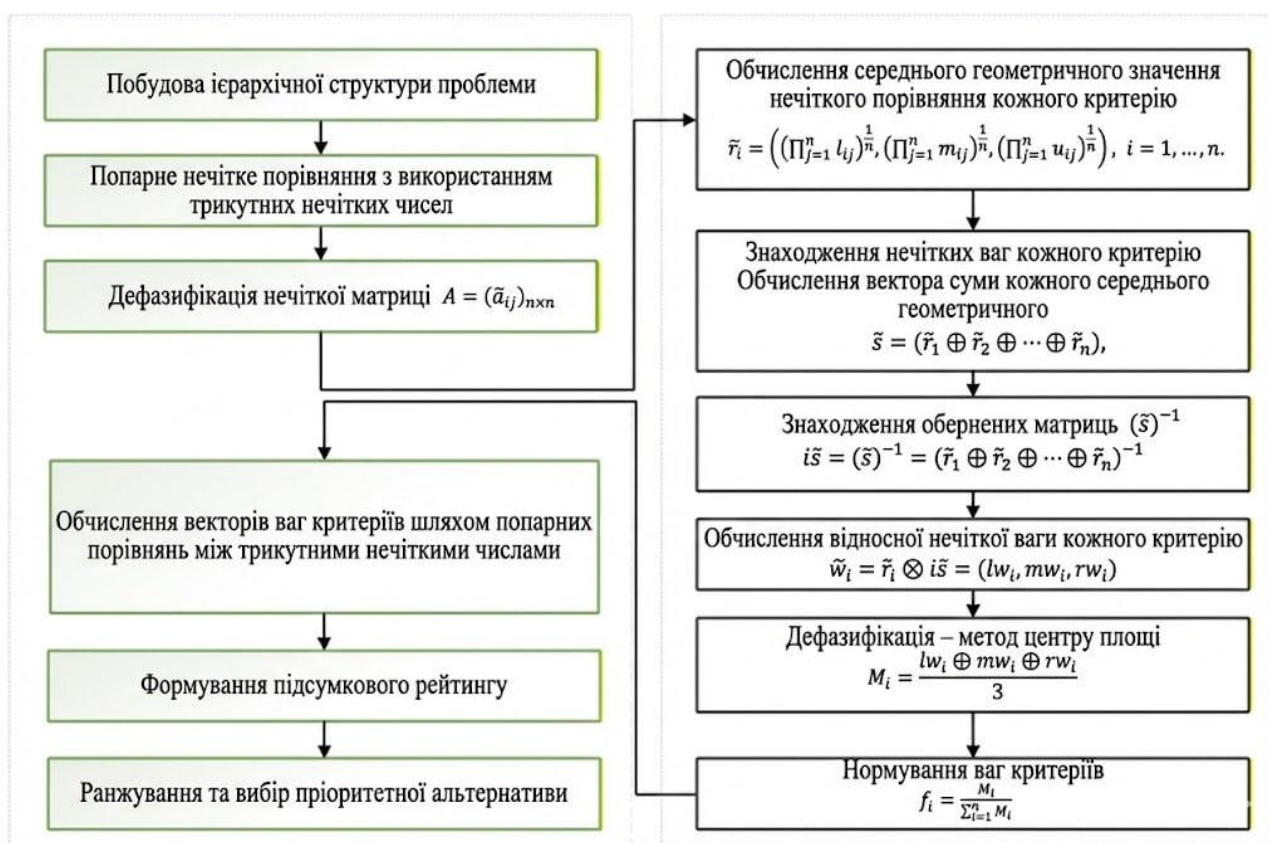


Рисунок 2.6 – Блок-схема алгоритму розрахунку ваг методом Баклі

Спочатку обчислюється нечітке геометричне середнє  $\tilde{r}_i$  для кожного рядка:

$$\tilde{r}_i = (\tilde{q}_{i1} \otimes \tilde{q}_{i2} \otimes \dots \otimes \tilde{q}_{in})^{\frac{1}{n}}, \quad (2.10)$$

де  $n$  – кількість факторів.

Далі визначається нечітка вага фактора  $\tilde{w}_i$ :

$$\tilde{w}_i = \tilde{r}_i \otimes (\tilde{r}_1 \oplus \tilde{r}_2 \oplus \dots \oplus \tilde{r}_n)^{-1}. \quad (2.11)$$

*Крок 5. Дефазифікація та визначення ваги.* Отримані нечіткі ваги методу Баклі  $\tilde{w}_i = (l_i, m_i, u_i)$  підлягають дефазифікації методом центру площі (Center of Area – CoA) [84, 85]. Для трикутного числа  $\tilde{w} = (l, m, u)$  чітке значення  $w^{def}$  дорівнює:

$$x_i^{def} = \frac{(u-l)+(m-l)}{3} + l = \frac{l+m+u}{3}. \quad (2.12)$$

Отримані значення необхідно нормалізувати для отримання ваг за методом Баклі  $w_i^B$ :

$$w_i^B = \frac{x_i^{def}}{\sum_{j=1}^n x_j^{def}}. \quad (2.13)$$

Фінальний інтегрований ваговий коефіцієнт розраховується як середнє арифметичне нормалізованих значень, отриманих двома методами:

$$W_i = \frac{w_i^{Ch} + w_i^B}{2}. \quad (2.14)$$

Такий підхід дозволяє врахувати перетин нечітких множин (Чанг) і зберегти повну інформацію про структуру переваг (Баклі).

На основі експертного опитування сформовано агреговану нечітку матрицю парних порівнянь факторів ризику (Додаток Г, табл. Г. 1).

Для верифікації запропонованої модифікації розрахунки проведено паралельно різними методами. Результати зведено у таблицю 2.5.

Таблиця 2.5 – Компаративний аналіз вагових коефіцієнтів

Фактор	Метод Чанга, $w_i^{Ch}$	Метод Баклі, $w_i^B$	Інтегрована оцінка, $W_i$	Ранг
<i>A</i>	0,156	0,153	0,155	<b>3</b>
<i>P</i>	0,225	0,228	0,227	<b>2</b>
<i>Los</i>	0,341	0,361	0,351	<b>1</b>
<i>Con</i>	0,044	0,039	0,042	<b>6</b>
<i>F</i>	0,128	0,122	0,125	<b>4</b>
<i>Cul</i>	0,105	0,109	0,107	<b>5</b>

Для перевірки достовірності експертних оцінок розраховано індекс узгодженості (*CR*). Його розрахункове значення  $CR = 0.027$  значно менше граничного значення 0.1. Це свідчить про високу узгодженість думок експертів, а отже, отримані результати є математично коректними та можуть бути використані для подальшого моделювання.

Отриманий розподіл ваг дозволяє зробити наступні висновки щодо пріоритетів захисту ТЛЦ:

- найвагомішим фактором є рівень збитків ( $w_{Los} = 0.35$ ). Це пояснюється специфікою ТЛЦ як об'єкта критичної інфраструктури, де наслідки інциденту можуть призвести не лише до фінансових втрат, а й до зупинки логістичних ланцюгів державного значення;

- фактор імовірності реалізації загрози ( $w_P = 0.22$ ) має вищий пріоритет, ніж номінальна цінність активів ( $w_A = 0.155$ ). Це свідчить про зміну парадигми захисту від пасивного «збереження вартості» до проактивного «запобігання інциденту»;
- фактор рівень культури ІБ ( $w_{Cul} = 0.10.7$ ) має вагу в 2,5 рази більшу, ніж фактор технічного контролю ( $w_{Con} = 0.042$ ), що підтверджує критичну роль людського фактору в сучасних системах кібербезпеки.

Результати розрахунків вагових коефіцієнтів факторів ризику ІБ ТЛЦ, отримані за допомогою методу Fuzzy АНР, представлені в таблиці Г.2 Додатку Г.

*Етап 3. Оцінка нечітких значень рівня впевненості експерта при оцінці підфакторів рівня ризику ІБ ТЛЦ.* Для лінгвістичного оцінювання рівня впевненості експерта скористаємося терм-множиною  $T2 = \{\text{дуже низька} - VL; \text{низька} - L; \text{середня} - M; \text{висока} - H; \text{дуже висока} - VH\}$ . Семантика термів задається нечіткими числами на інтервалі  $[0; 1]$  (рис. 2.7) з відповідними функціями належності та нечіткими числами – VL: (0,0; 0,0; 0,25); L: (0,15; 0,3; 0,45); M: (0,35; 0,5; 0,65); H: (0,55; 0,7; 0,85); VH: (0,75; 1,0; 1,0).

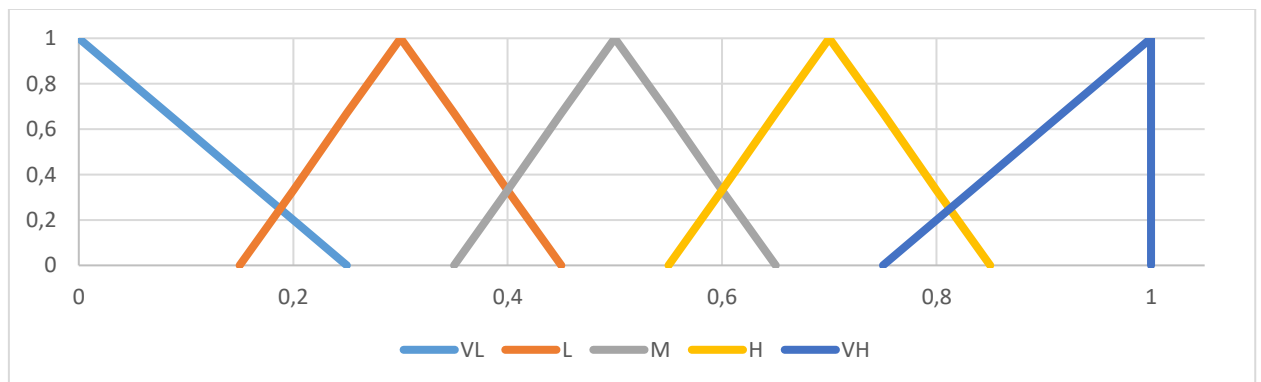


Рисунок 2.7 – Функції належності термів оцінювання рівня впевненості експертів

Таким чином для кожного підфактора одержимо нечіткі оцінки рівня впевненості експертів, агрегуючи які, матимемо: для  $A$ -факторів:  $\tilde{p}_1^A, \tilde{p}_2^A, \dots, \tilde{p}_{n_A}^A$ ; для  $P$ -факторів:  $\tilde{p}_1^P, \tilde{p}_2^P, \dots, \tilde{p}_{n_P}^P$ ; для  $Los$ -факторів:  $\tilde{p}_1^L, \tilde{p}_2^L, \dots, \tilde{p}_{n_L}^L$ ; для  $Con$ -

факторів:  $\tilde{p}_1^{Con}, \tilde{p}_2^{Con}, \dots, \tilde{p}_{n_{Con}}^{Con}$ ; для  $F$ -факторів:  $\tilde{p}_1^F, \tilde{p}_2^F, \dots, \tilde{p}_{n_F}^F$ ; для  $Cul$ -факторів:  $\tilde{p}_1^{Cul}, \tilde{p}_2^{Cul}, \dots, \tilde{p}_{n_{Cul}}^{Cul}$ .

*Етап 4. Оцінка нечітких значень підфакторів ризику ІБ ТЛЦ.* Оскільки фахівцям важко дати точну числову оцінку наведеним факторам, вони розглядаються як лінгвістичні змінні. При цьому кожен фактор має специфічний вектор впливу на загальний. Характер взаємозв'язку та напрямок впливу визначених факторів на інтегральний показник ризику узагальнено в таблиці 2.6.

Таблиця 2.6 – Характер взаємозв'язку та напрямок впливу факторів на інтегральний показник рівня ризику ІБ ТЛЦ

Фактор	Характеристика	Вплив на ризик ІБ	Пояснення
$x_A$	Рівень цінності активів	Збільшує	Збільшує потенційний масштаб збитків ( $x_L$ ).
$x_P$	Імовірність реалізації загрози через наявні вразливості	Збільшує	Прямо збільшує компонент ймовірності ризику.
$x_L$	Рівень збитків від загроз	Збільшує	Прямо збільшує компонент впливу ризику.
$x_{Con}$	Рівень контролю інформаційних ресурсів	Зменшує	Знижує ймовірність ( $x_P$ ) реалізації загроз.
$x_{Cul}$	Рівень витрат на створення та функціонування СУІБ	Зменшує	Знижує ймовірність ( $x_P$ ) успішних атак через людський фактор.
$x_F$	Рівень культури інформаційної безпеки	Зменшує (непрямий)	Інвестиція, спрямована на зниження інших факторів ризику ( $x_P, x_L$ через $x_C, x_{Cul}$ ).

Оскільки, експертні оцінки факторів можуть сприяти як підвищенню ризику так і його зниженню, пропонуємо задавати семантику термів нечіткими числами на інтервалі  $[-1; 1]$  (рис. 2.8). Для цього використовуються наступні терм-множини:

- для факторів, що збільшують ризик ( $x_A, x_P, x_L$ ) застосовується терм-множина  $T_3 = \{\text{незначний} - NSt; \text{дуже низький} - VLt; \text{низький} - Lt; \text{середній} - Mt; \text{високий} - Ht; \text{дуже високий} - VHt; \text{екстремальний} - EHt\}$ , де вищі значення термів відповідають зростанню загрози;
- для факторів, що зменшують ризик ( $x_{Con}, x_{Cul}$ ) застосовується терм-множина  $T_4$

= {незначний – NSo; дуже низький – VLo; низький – Lo; середній – Mo; високий – Ho; дуже високий – VHo; екстремальний – EHo}, де вищі значення термів вказують на ефективність заходів протидії та зниження загального рівня ризику.

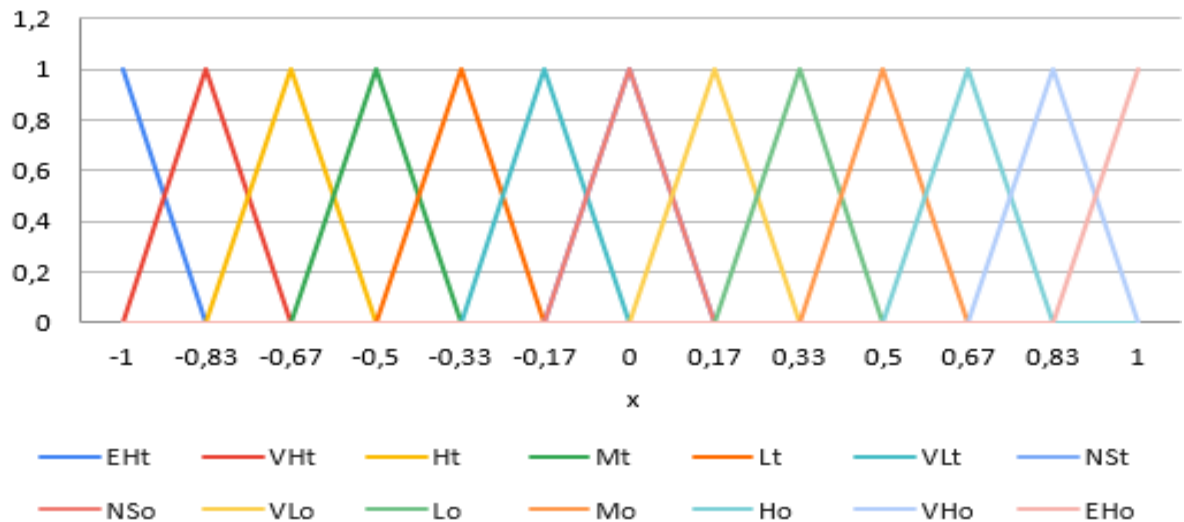


Рисунок 2.8 – Функції належності термів оцінювання підфакторів рівня ризику  
ІБ ТЛЦ

Семантика кожного терму описується відповідними функціями належності у вигляді нечітких чисел у триангулярному представленні.

Шкала оцінювання поділяється на дві групи.

Для факторів, що сприяють підвищенню рівня ризику, діапазон  $[-1; 0]$ : NSt:  $(-0.17; 0.00; 0.00)$ ; VLt:  $(-0.33; -0.17; 0.00)$ ; Lt:  $(-0.50; -0.33; -0.17)$ ; Mt:  $(-0.67; -0.50; -0.33)$ ; Ht:  $(-0.83; -0.67; -0.50)$ ; VHt:  $(-1.00; -0.83; -0.67)$ ; EHt:  $(-1.00; -1.00; -0.83)$ .

Для факторів, що сприяють зниженню рівня ризику, діапазон  $[0; 1]$ : NSo:  $(0.00; 0.00; 0.17)$ ; VLo:  $(0.00; 0.17; 0.33)$ ; Lo:  $(0.17; 0.33; 0.50)$ ; Mo:  $(0.33; 0.50; 0.67)$ ; Ho:  $(0.50; 0.67; 0.83)$ ; VHo:  $(0.67; 0.83; 1.00)$ ; EHo:  $(0.83; 1.00; 1.00)$ .

В результаті отримаємо нечіткі оцінки всіх факторів від кожного експерта для ІБ ТЛЦ, агрегуючи які, матимемо:

– для А-факторів:  $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_{n_A}$ ;

- для  $P$ -факторів:  $\tilde{P}_1, \tilde{P}_2, \dots, \tilde{P}_{n_P}$ ;
- для  $Los$ -факторів:  $\tilde{L}_1, \tilde{L}_2, \dots, \tilde{L}_{n_L}$ ;
- для  $Con$ -факторів:  $\tilde{Con}_1, \tilde{Con}_2, \dots, \tilde{Con}_{n_{Con}}$ ;
- для  $F$ -факторів:  $\tilde{F}_1, \tilde{F}_2, \dots, \tilde{F}_{n_F}$ ;
- для  $Cul$ -факторів:  $\tilde{Cul}_1, \tilde{Cul}_2, \dots, \tilde{Cul}_{n_{Cul}}$ .

*Етап 5. Формування матриці оцінювання загроз і можливостей на основі визначених нечітких значень факторів (підфакторів) та рівня впевненості експертів для формування стратегії ІБ ТЛЦ. Застосування нечітких лінгвістичних оцінок факторів, що впливають на рівень ризику ІБ ТЛЦ, та нечітких значень оцінки рівня впевненості експертів дозволяє створити детальнішу та більш інформативну матрицю оцінювання факторів – модифіковану матрицю Дж. Х. Вілсона (рис. 2.9) [106].*

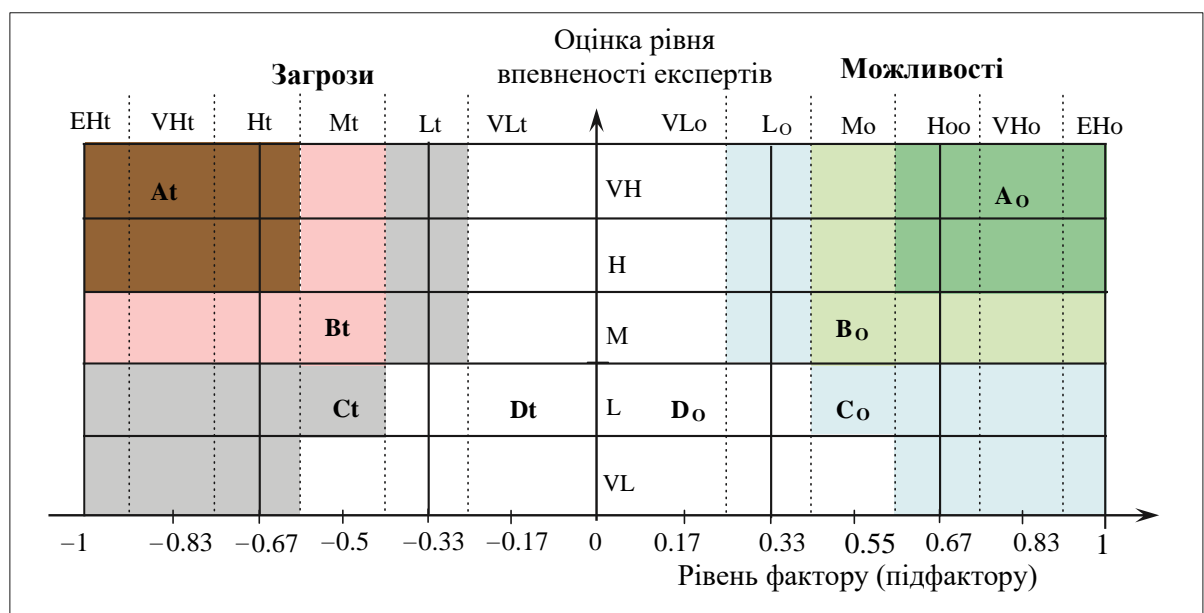


Рисунок 2.9 – Матриця нечіткого оцінювання загроз і можливостей факторів рівня ризику ІБ ТЛЦ (о – можливості, t – загрози)

Кожний фактор, який розглядається, позиціонують у даній матриці відповідно до лінгвістичних оцінок, одержаних на етапах 3 і 4. Це надає змогу

наочно представити критично важливі для транспортно-логістичного центру аспекти ризику ІБ.

Оцінки, що потрапили до зони  $A_0$ , потребують уваги та впровадження відповідних заходів захисту. Ці аспекти є фундаментальними для безперебійної роботи компанії та забезпечення прийняттого рівня ІБ ТЛЦ.

Зона  $B_0$ , також потребує ретельного вивчення та потенційного використання для підвищення рівня ІБ.

Впровадження  $C_0$  можливе за умови наявності достатніх ресурсів та проведення детального аналізу ризиків та вигод.

Існуючі вразливості, віднесені до зони  $A_t$ , становлять найбільшу загрозу для компанії та можуть призвести до серйозних наслідків, таких як збої в роботі транспортних систем, втрата конфіденційних даних, фінансові втрати та руйнування репутації. Усунення цих вразливостей є пріоритетним завданням.

Фактори, що потрапили до зони  $B_t$ , також потребують уваги керівництва, оскільки вони можуть призвести до значних проблем в роботі компанії та вимагають своєчасного реагування.

Зона  $C_t$ , хоча і менш критична, також повинна перебувати під постійним моніторингом, оскільки ігнорування може призвести до накопичення проблем в майбутньому.

*Етап 6. Обчислення нечітких значень підфакторів рівня ризику ІБ ТЛЦ методом Fuzzy SAW.* Зазначимо, що в формулах нечіткого адитивного зважування (2.15-2.20) включений і рівень впевненості експертів по кожному фактору [107]:

$$\tilde{A} = \bigoplus_{i=1}^{n_A} \tilde{w}_i^A \otimes \tilde{p}_i^A \otimes \tilde{A}_i = (w_{1i}^A p_{1i}^A A_{1i}; w_{2i}^A p_{2i}^A A_{2i}; w_{3i}^A p_{3i}^A A_{3i}); \quad (2.15)$$

$$\tilde{P} = \bigoplus_{i=1}^{n_P} \tilde{w}_i^P \otimes \tilde{p}_i^P \otimes \tilde{P}_i = (w_{1i}^P p_{1i}^P P_{1i}; w_{2i}^P p_{2i}^P P_{2i}; w_{3i}^P p_{3i}^P P_{3i}); \quad (2.16)$$

$$\tilde{Los} = \bigoplus_{i=1}^{n_L} \tilde{w}_i^L \otimes \tilde{p}_i^L \otimes \tilde{Los}_i = (w_{1i}^L p_{1i}^L Los_{1i}; w_{2i}^L p_{2i}^L Los_{2i}; w_{3i}^L p_{3i}^L Los_{3i}); \quad (2.17)$$

$$\begin{aligned} \tilde{Con} = \bigoplus_{i=1}^{n_{Con}} \tilde{w}_i^{Con} \otimes \tilde{p}_i^{Con} \otimes \tilde{Con}_i = \\ (w_{1i}^{Con} p_{1i}^{Con} Con_{1i}; w_{2i}^{Con} p_{2i}^{Con} Con_{2i}; w_{3i}^{Con} p_{3i}^{Con} Con_{3i}); \end{aligned} \quad (2.18)$$

$$\tilde{F} = \bigoplus_{i=1}^{n_F} \tilde{w}_i^F \otimes \tilde{p}_i^F \otimes \tilde{F}_i = (w_{1i}^F p_{1i}^F F_{1i}; w_{2i}^F p_{2i}^F F_{2i}; w_{3i}^F p_{3i}^F F_{3i}); \quad (2.19)$$



$$\begin{aligned} \widetilde{Cul} = & \bigoplus_{i=1}^{n_{Cul}} \widetilde{w}_i^{Cul} \otimes \widetilde{p}_i^{Cul} \otimes \widetilde{Cul}_i = \\ & (w_{1i}^{Cul} p_{1i}^{Cul} Cul_{1i}; w_{2i}^{Cul} p_{2i}^{Cul} Cul_{2i}; w_{3i}^{Cul} p_{3i}^{Cul} Cul_{3i}) \end{aligned} \quad (2.20)$$

*Етап 7. Обчислення експертної нечіткої оцінки рівня ризику ІБ ТЛЦ.*  
Процедура обчислення нечіткої оцінки рівня ризику ІБ ТЛЦ представлена на рисунку 2.10.

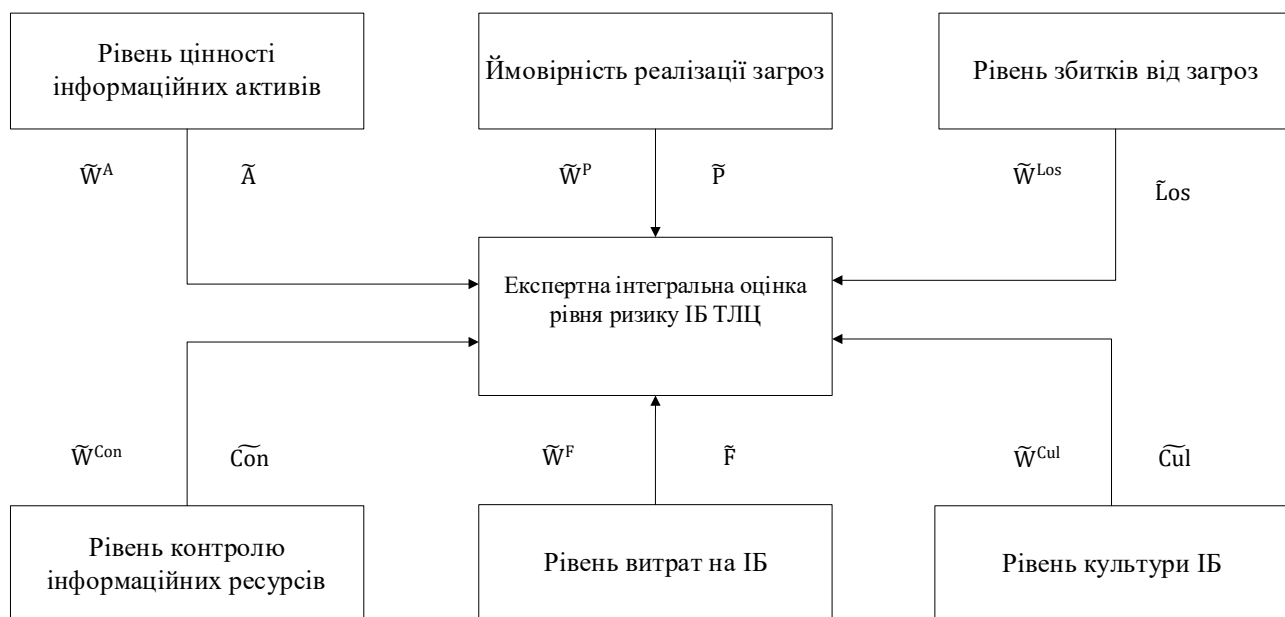


Рисунок 2.10 – Структура експертної інтегральної оцінки рівня ризику ІБ ТЛЦ

Для проведення розрахунків скористаємося формулою:

$$\begin{aligned} \widetilde{RI} = & \widetilde{W}^A \otimes p_i^A \otimes \widetilde{A} \oplus \widetilde{W}^P \otimes p_i^P \otimes \widetilde{P} \oplus \widetilde{W}^{Los} \otimes p_i^{Los} \otimes \widetilde{Los} \oplus \widetilde{W}^{Con} \otimes p_i^{Con} \otimes \widetilde{Con} \oplus \\ & \widetilde{W}^F \otimes p_i^F \otimes \widetilde{F} \oplus \widetilde{W}^{Cul} \otimes p_i^{Cul} \otimes \widetilde{Cul}, \end{aligned} \quad (2.21)$$

де  $\widetilde{W}^A, \widetilde{W}^P, \widetilde{W}^{Los}, \widetilde{W}^{Con}, \widetilde{W}^F, \widetilde{W}^{Cul}$  – нечіткі вагові коефіцієнти факторів, що знаходяться методом Fuzzy АНР (крок 1-4 етапу 2). Для ранжирування факторів рівня ризику ІБ ТЛЦ можна скористатися нечітким добутком ваги конкретного фактору й значенням впевненості експерта, наприклад, для факторів рівень цінності інформаційних активів ІБ:  $p_i^A \otimes \widetilde{A}_i$  з наступною його дефазифікацією та нормуванням.

*Етап 8. Дефазифікація одержаної нечіткої оцінки рівня ризику ІБ ТЛЦ, внесення одержаних даних до БД для підготовки стратегічних рішень.* Дефазифіковані оцінки рівня ризиків ІБ ТЛЦ (вихідні дані моделі) представлені в таблиці 2.7.

Таблиця 2.7 – Вихідні дані моделі оцінки рівня ризиків ІБ ТЛЦ

	Якісні значення $\widetilde{RI}$	Інтервали терма «Ризик»	Усереднені значення	Характеристика
1.	Незначний (VL)	(0,0; 0,0; 0,25)	0,125	Ризиком можна знехтувати. Перенесення ризику (перенесення відповідальності за ризик на треті особи).
2.	Низький (L)	(0,15; 0,3; 0,45);	0,3	Рівень ризику дозволяє працювати. Ухилення від ризику (відмова від залучення до ризикової ситуації або дії, що запобігають її виникненню). Провести розподіл відповідальності.
3.	Допустимий (M)	(0,35; 0,5; 0,65);	0,5	Рівень ризику не дозволяє стабільно працювати. Прийняття ризику (готовність організації зазнати шкоди від конкретного ризику у разі, якщо його рівень вважається прийнятним). Потрібна термінова реакція на ризик.
4.	Високий (H)	(0,55; 0,7; 0,85)	0,7	Рівень ризику дуже високий і є неприпустимим для ТЛЦ. Мінімізація ризику (виконання дій для зменшення ймовірності та/або негативних наслідків, пов'язаних із ризиком). Вимагає глибоких досліджень системи забезпечення ІБ.

*Етап 9. Трансформація отриманих результатів у конкретні управлінські дії.* Базуючись на дефазифікованій інтегральній оцінці рівня ризику та його лінгвістичній інтерпретації (етап 8), а також на аналізі позиціювання факторів у матриці загроз і можливостей (етап 6), для кожного ідентифікованого ризику обирається адекватна стратегія реагування: зниження, ухилення, перенесення або прийняття.

На основі обраних стратегій формується комплексний план заходів із забезпечення ІБ ТЛЦ. Пріоритетними є дії, спрямовані на нівелювання критичних

загроз (зони  $A_t$ ,  $B_t$  матриці) та факторів з найвищими ваговими коефіцієнтами (визначеними на етапі 2). План включає перелік конкретних технічних та організаційних рішень, оцінку необхідних ресурсів (фінансових, кадрових, часових) та призначення відповідальних осіб.

Окрему увагу приділено використанню можливостей для підвищення загального рівня безпеки шляхом посилення факторів, що знижують ризик (зони  $A_o$ ,  $B_o$ ,  $C_o$ ): підвищення ефективності контролю, оптимізація витрат та розвиток культури ІБ. Сформовані стратегічні рішення та план заходів документуються і подаються на затвердження керівництву ТЛЦ. Крім того, ці результати слугують вхідними даними для подальшого детального моделювання та оптимізації системи захисту в рамках запропонованої ІТ ППР.

Апробація запропонованої методики експертного інтегрального оцінювання рівня ризику ІБ ТЛЦ здійснювалася шляхом проведення експериментального моделювання із залученням групи профільних експертів.

Процес моделювання складався з кількох послідовних етапів.

1. На першому етапі експертами було здійснено лінгвістичне оцінювання вхідних параметрів моделі. Для кожної групи підфакторів другого рівня були сформовані нечіткі матриці попарних порівнянь, на основі яких обчислено нечіткі значення їх локальних ваг ( $w_{ij}$ ).

Для проведення експериментального дослідження було розроблено деталізовані метричні шкали, які встановлюють чітку відповідність між фізичними показниками функціонування ТЛЦ (вартість активів, частота інцидентів, результати тестування персоналу тощо) та лінгвістичними термами. Вхідні метрики та їх інтерпретація наведені в таблиці 2.8

Таблиця 2.8 – Вхідні дані моделі

<i>Рівень цінності активів</i>				
№ п/п	Оцінка рівня цінності активів	Вартість активу (в ум. одиницях)	Інтервали терма «Цінність активу»	Усереднене значення
1	Дуже мала	0 – 5000	0-0,25	0,1
2	Низька	5001 – 50000	0,15-0,45	0,3

3	Середня	50001 – 300000	0,35-0,65	0,5
4	Висока	300001 – 1000000	0,55-0,85	0,7
5	Критично дуже висока	більше 1000001	0,75-1,00	0,9
<i>Ймовірність реалізації загроз через наявні вразливості</i>				
№ п/п	Оцінка ймовірності реалізації загроз через наявні вразливості	Частота реалізації загрози через наявні вразливості	Інтервали терма «Реалізація загрози через наявні вразливості»	Усереднене значення
1	Низька	Для нових активів ймовірність виконання загрози низька	0-0,3	0,15
2	Середня	Один – два на рік. Для нових активів ймовірність виконання загрози середня	0,21-0,75	0,48
3	Висока	Більше 2-х разів на рік. Для нових активів ймовірність виконання загрози висока	0,6-1,00	0,8
<i>Рівень збитків від загроз</i>				
№ п/п	Оцінка рівня збитків від загроз	Вартість збитків (в ум. одиницях)	Інтервали терма «Рівень збитків від загроз»	Усереднене значення
1	Незначний	0 – 5000	0-0,2	0,1
2	Допустимий	5001 – 50000	0,20-0,50	0,35
3	Високий	50001 – 300000	0,5-0,8	0,65
4	Критичний	більше 300001	0,8-1,0	0,9
<i>Рівень контролю інформаційних ресурсів</i>				
№ п/п	Оцінка рівня контролю інформаційних ресурсів	Характеристика оцінки рівня контролю ІР	Інтервали терма «Рівень контролю ІР»	Усереднене значення
1	Повний	Використовується приватний ІР	0,95-1,00	0,97
2	Високий	Провайдер надає послуги з використання інфраструктури	0,60-0,90	0,7
3	Середній	Конкретний провайдер надає послуги зі зберігання, обробки інформації та адміністрування системи	0,40-0,75	0,58
4	Низький	Ресурси з низьким рівнем контролю	0,10-0,50	0,25
<i>Рівень витрат на створення та експлуатацію системи ІБ</i>				

№ п/п	Оцінка рівня витрат на створення та експлуатацію системи ІБ	Вартість створення та експлуатації системи ІБ (в ум. одиницях)	Інтервали терма «Рівень витрат на створення та експлуатацію системи ІБ»	Усереднене значення
1	Низькі	50 – 1000	0-0,30	0,15
2	Середні	900 – 100000	0,25-0,60	0,42
3	Високі	90000 – 550000	0,55-0,80	0,55
4	Значні	більше 500000	0,75-1,00	0,875
<i>Рівень культури ІБ</i>				
№ п/п	Оцінка рівня культури ІБ	Кількість балів отриманих за тестування	Інтервали терма	Усереднене значення
1	Низький	0-30	0-0,3	0,15
2	Середній	21-75	0,21-0,75	0,48
3	Високий	60-100	0,6-1,0	0,8

Для подальшої математичної обробки та нормалізації даних використано уніфіковану шкалу переведення лінгвістичних термів у чіткі числа (усереднені значення), що наведена в таблиці 2.9.

Таблиця 2.9 – Відповідність якісних значень усередненим кількісним значенням змінних

Змінна	Якісні значення	Назва терма	Межі терма	Усереднені значення
Рівень цінності активів, $x_1$	дуже мала	VL	0-0,25	0,1
	низька	L	0,15-0,45	0,3
	середня	M	0,35-0,65	0,5
	висока	H	0,55-0,85	0,7
	дуже висока	VH	0,75-1,00	0,9
Імовірність реалізації загрози через наявні вразливості, $x_2$	мала	L	0-0,3	0,15
	середня	M	0,21-0,75	0,48
	висока	H	0,6-1,0	0,8
Рівень збитків від загрози, $x_3$	незначний	L	0-0,2	0,1
	допустимий	M	0,20-0,50	0,35
	високий	H	0,5-0,8	0,65
	критичний	L	0,8-1,0	0,9
Рівень контролю інформаційних ресурсів, $x_4$	низький	L	0,10-0,50	0,25
	середній	M	0,40-0,75	0,5
	високий	H	0,60-0,9	0,7
	повний	VH	0,95-1,00	0,97
Рівень витрат на створення та експлуатацію системи	низький	L	0-0,30	0,15
	середній	M	0,25-0,60	0,42
	високий	H	0,55-0,80	0,65

Змінна	Якісні значення	Назва терма	Межі терма	Усереднені значення
ІБ, $x_5$	значний	VH	0,75-1,00	0,75
Рівень культури інформаційної безпеки ТЛЦ, $x_6$	низький	L	0-0,3	0,15
	середній	M	0,21-0,75	0,48
	високий	H	0,6-1,0	0,8

Додатково експерти надали лінгвістичну оцінку рівню впевненості в оцінці. У рамках даного експерименту для більшості факторів цей показник було визначено як «високий» (H – High). Також було отримано прямі експертні оцінки стану самих підфакторів ( $x_{ij}$ ).

Вхідні дані експертного опитування для другого рівня ієрархії наведено в табл. Г. 3 Додатку Г.

2. На другому етапі було проведено фазифікацію отриманих лінгвістичних змінних – їх перетворення у відповідні нечіткі числа згідно з визначеними раніше функціями належності. Результати фазифікації представлені в таблиці Г.4 Додатку Г.

3. На третьому етапі, для забезпечення співставності даних було проведено процедуру нормалізації нечітких ваг та нечітких значень підфакторів. Нормалізовані значення, готові для подальших обчислень, зведено в таблицю Г.5 Додатку Г.

4. Четвертим етапом стало дослідження чутливості моделі та впливу невизначеності на кінцевий результат. Моделювання було проведено для трьох різних сценаріїв, що відрізняються рівнем упевненості експерта в оцінках:

- сценарій L – низька ймовірність (L – Low);
- сценарій M – середня ймовірність (M – Medium);
- сценарій H – висока ймовірність (H – High).

Вхідні агреговані дані для факторів першого рівня, що використовувалися у цих сценаріях, наведені в таблиці Г.6 Додатку Г.

5. На п'ятому етапі, використовуючи модифікований метод Fuzzy SAW, було розраховано проміжні нечіткі оцінки впливу кожного з шести головних

факторів ризику для кожного з трьох сценаріїв. Результати розрахунків представлені в таблиці Г.7 та узагальнені в таблиці Г.8 Додатку Г.

6. На завершальному етапі, використовуючи формулу адитивної згортки, було обчислено фінальну нечітку інтегральну оцінку рівня ризику ІБ ТЛЦ ( $\widetilde{RI}$ ) для трьох досліджуваних сценаріїв. Результати наведено в таблиці 2.10.

Таблиця 2.10 – Інтегральний рівень ризику ІБ ТЛЦ за різними сценаріями

Рівень ризику ІБ ТЛЦ, $\widetilde{RI}$								
низький рівень впевненості експерта, $L$			середній рівень впевненості експерта, $M$			високий рівень впевненості експерта, $H$		
$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$
0,0200	0,1811	0,299	0,0229	0,1833	0,2938	0,0241	0,1842	0,2917

Аналіз отриманих даних (табл. 2.10) дозволяє зробити важливий висновок щодо поведінки моделі в умовах невизначеності. Зі зростанням упевненості експертів в імовірності реалізації факторів (перехід від сценарію  $L$  до  $H$ ), спостерігається звуження носія нечіткої множини результуючого ризику:

- сценарій  $L$  – інтервал  $[0,0200; 0,299]$ , ширина = 0,279;
- сценарій  $M$  – інтервал  $[0,0229; 0,2938]$ , ширина = 0,2709;
- сценарій  $H$  – інтервал  $[0,0241; 0,2917]$ , ширина = 0,2676.

Така динаміка свідчить про коректність роботи алгоритму. Підвищення якості та вірогідності вхідної інформації безпосередньо знижує рівень невизначеності фінального результату.

Для прийняття управлінських рішень було проведено дефазифікацію експертної інтегральної оцінки для найбільш релевантного сценарію (висока ймовірність,  $H$ ). Усереднене чітке експертне значення рівня ризику ІБ ТЛЦ становить  $RI = 0,167$ , що згідно з розробленою лінгвістичною шкалою класифікації (табл. 2.7) відповідає терму «Низький ризик».

Отриманий результат вказує на стійкий стан системи захисту, який забезпечує стабільне функціонування ключових бізнес-процесів ТЛЦ. Зафіксований рівень загроз не створює передумов для паралізації логістичних ланцюгів або критичного порушення конфіденційності клієнтських даних. У

даному випадку рекомендована стратегія управління полягає у безперервному моніторингу ситуації та трансфері залишкових ризиків на треті сторони (наприклад, через механізми страхування), що дозволяє уникнути впровадження високовартісних додаткових засобів захисту.

Експериментальне дослідження, реалізоване мовою Python (бібліотека FuzzyPy), підтвердило працездатність запропонованої інформаційної технології. Поєднання ієрархічної декомпозиції факторів, методу Fuzzy АНР для визначення ваг та модифікованого алгоритму Fuzzy SAW забезпечує ефективну обробку суб'єктивних неформалізованих даних, гарантуючи точність стратегічного оцінювання в умовах динамічного середовища ТЛЦ.

### **2.3 Адаптивна нейронечітка модель оцінювання інтегрального рівня ризику ІБ ТЛЦ**

Застосування методу Fuzzy SAW для експертного інтегрального оцінювання ризику ІБ ТЛЦ виявило обмеження щодо динамічності та відображення нелінійних зв'язків. Експериментальна спроба апроксимації результатів за допомогою методу найменших квадратів підтвердила неадекватність лінійних підходів в умовах невизначеності: отримане критично високе середньоквадратичне відхилення довело неспроможність лінійної структури адаптуватися до нечітких переходів [108].

З огляду на це, визначено доцільність використання архітектури ANFIS другого ступеня. Такий вибір забезпечує врахування синергетичного ефекту взаємодії факторів та динамічність оцінювання.

Поряд із цим існує проблема дефіциту статистичних даних («холодний старт»), яку необхідно вирішити для запуску та навчання моделі ANFIS.

Для подолання проблеми дефіциту статистичних даних («холодний старт») запропоновано механізм автоматизованої генерації повної нечіткої бази правил (БЗ) типу Мамдані. Така база виступає формалізованою експертною моделлю



(«синтетичним вчителем»), що описує повний простір можливих станів системи [111].

Генерація відбувається шляхом перебору всіх можливих комбінацій лінгвістичних термів вхідних факторів  $(x_1, \dots, x_6)$  за допомогою декартового добутку:

$$RB_{total} = T_1 \times T_2 \times \dots \times T_6, \quad (2.22)$$

де  $T_i = \{t_{i,1}, t_{i,2}, \dots, t_{i,N_i}\}$  – множина лінгвістичних термів для  $i$ -го фактора,  $N_i$  – кількість термів.

Загальна кількість правил:

$$N_{rules} = \prod_{i=1}^6 N_i. \quad (2.23)$$

Для кожного згенерованого  $k$ -го правила автоматично обчислюється еталонний ризиковий індекс  $R_{index}^{(k)}$  – цільове значення для навчання:

$$R_{index}^{(k)} = \frac{\sum_{i=1}^6 w_i \cdot S_i \cdot \text{Norm}\left(\text{Ind}(t_i^{(k)})\right)}{\sum_{i=1}^6 |w_i|}, \quad (2.24)$$

де  $k$  – індекс поточного правила в згенерованій базі ( $k = 1, \dots, N_{rules}$ );

$w_i$  – ваговий коефіцієнт  $i$ -го фактора, отриманий з модуля Fuzzy АНР;

$S_i \in \{-1, +1\}$  – знаковий індикатор напрямку впливу  $i$ -го фактора на ризик (табл. 2.7);

$t_i^{(k)}$  – лінгвістичний терм  $i$ -го фактора в антецеденті  $k$ -го правила;

$\text{Ind}(t)$  – функція, що повертає порядковий номер терма  $t$  у терм-множині  $i$ -го фактора;

$\text{Norm}(\cdot)$  – функція нормалізації, що перетворює індекс терма в діапазон  $[0, 1]$  або  $[-1, 1]$ , відповідно до обраної шкали моделювання [112].

Фрагмент сформованої повної бази знань, структурованої у вигляді мережі нечітких продукцій, наведено в табл. 2.11.

Таблиця 2.11 – Фрагмент нечіткої бази знань (продукційні правила)

№ правила	Цінність активу, $x_1$	Імовірність реалізації загрози через наявну вразливість, $x_2$	Рівень збитків від загрози, $x_3$	Рівень контролю інформаційних ресурсів, $x_4$	Рівень витрат на створення та експлуатацію системи ІБ, $x_5$	Рівень культури ІБ ТЛЦ, $x_6$	Ризик, $R$
1	VL	VL	VL	L	H	H	L
2	VL	VL	VL	L	H	M	L
...	...	...	...	...	...	...	...
2880	VH	H	VH	H	VH	L	VH

Оскільки формування повної бази правил (2880 комбінацій для обраної конфігурації) призводить до комбінаторного вибуху, лінійний перебір стає неефективним. Для структурування цих знань застосовано архітектуру Rete [113]. Вона трансформує лінійний список правил в оптимізований граф, що мінімізує повторні обчислення та забезпечує миттєвий доступ до еталонних значень під час навчання нейромережі.

Модуль 5 реалізує нейронечітку модель (ANFIS) – «учень», що функціонує як універсальний апроксиматор для відтворення та узагальнення знань, імплементованих в експертній системі (модуль 4) [114]. Архітектура моделі відповідає мережі Такагі-Сугено-Канга (TSK) другого ступеня [115], що дозволяє моделювати складні нелінійні залежності між вхідними факторами та кінцевим рівнем ризику (рис. 2.11).

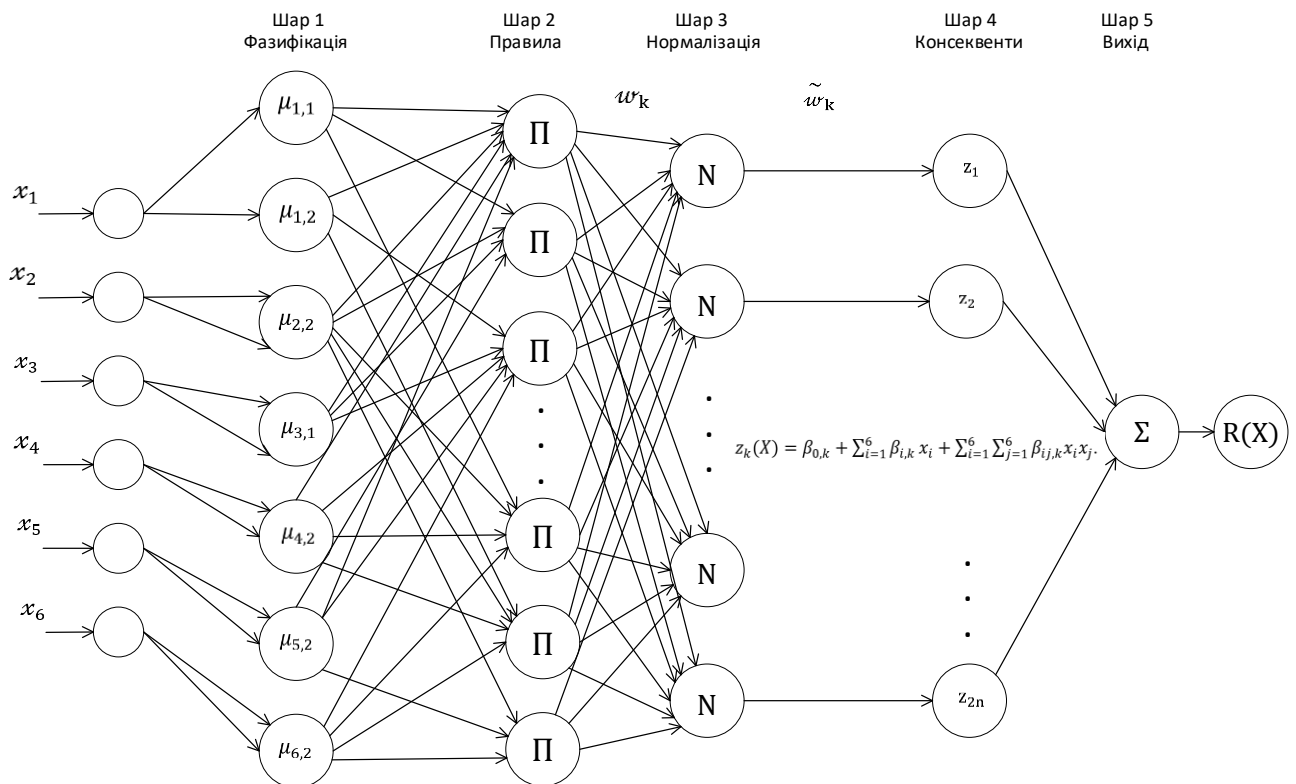


Рисунок 2.11 – Топологія мережі ANFIS (6 входів) для апроксимації функції ризику

Ключовою перевагою підходу є локально-адаптивна структура: система нечітких правил виконує декомпозицію простору входних факторів на окремі контексти. Для кожного контексту застосовується власний поліном першого або другого ступеня, що дозволяє враховувати як прямий вплив факторів, так і ефекти взаємодії між ними.

Алгоритм реалізації моделі.

*Крок 1.* Формалізація структури правил. База знань системи представляється як сукупність параметричних сутностей. Кожне нечітке правило  $k$  визначається двома компонентами:

- **антецедент** (набір лінгвістичних умов для входних факторів, що визначає область простору ознак, в якій діє дане правило):  
 $IF (x_1 \text{ is } A_1^{(k)}) \text{ AND } (x_2 \text{ is } A_2^{(k)}) \text{ AND } \dots \text{ AND } (x_6 \text{ is } A_6^{(k)})$ . Параметри функцій

належності  $\mu_{A_i^k(x_i)}$  є адаптивними і підлягають налаштуванню в процесі навчання мережі;

- **консеквент** (вектор коефіцієнтів локального полінома, що апроксимує характер залежності вихідної змінної (ризик) від вхідних факторів у межах активації даного правила):  $THEN z_k(X) = \beta_{0,k} + \sum_{i=1}^6 \beta_{i,k} x_i + \sum_{i=1}^6 \sum_{j=1}^6 \beta_{ij,k} x_i x_j$ .

*Крок 2.* Локальний поліноміальний висновок. Для кожного правила  $k$  обчислюється вихідний сигнал  $z_k$  за поліномом другого (обраного) порядку:

$$z_k(X) = \beta_{0,k} + \sum_{i=1}^6 \beta_{i,k} x_i + \sum_{i=1}^6 \sum_{j=1}^6 \beta_{ij,k} x_i x_j. \quad (2.25)$$

Це дозволяє моделювати як лінійний, так і нелінійний вплив факторів та їх взаємодії.

*Крок 3.* Ініціалізація коефіцієнтів. Для прискорення збіжності алгоритму навчання та уникнення локальних мінімумів здійснюється інтелектуальна ініціалізація параметрів поліноміальних консеквентів. Початкові значення лінійних коефіцієнтів  $\beta_{i,k}^{(0)}$  для кожного  $i$ -го фактора визначаються на основі відповідних нормалізованих ваг  $w_i$ , отриманих з модуля Fuzzy АНР, з прямим урахуванням характеру впливу фактора на інтегральний ризик:

$$\beta_{i,k}^{(0)} = w_i \cdot S_i, \quad (2.26)$$

де  $w_i$  – нормалізований ваговий коефіцієнт  $i$ -го фактора ( $w_i > 0$ );

$S_i$  – знаковий індикатор впливу  $i$ -го фактора:

$$S_i = \begin{cases} -1, & \text{для факторів, що зменшують ризик } (x_4, x_5, x_6); \\ +1, & \text{для факторів, що збільшують ризик } (x_1, x_2, x_3). \end{cases} \quad (2.27)$$

Інші коефіцієнти моделі (вільний член  $\beta_{0,k}^{(0)}$  та коефіцієнти при квадратичних і перехресних членах  $\beta_{ij,k}^{(0)}$ ) ініціалізуються малими випадковими значеннями з рівномірного розподілу:  $\beta_{0,k}^{(0)}, \beta_{ij,k}^{(0)} \sim U(-\varepsilon, +\varepsilon)$ , де  $\varepsilon$  – мале додатне число.

*Крок 4.* Генерація еталону та навчання. На цьому етапі Rete-мережа

функціонує як «синтетичний вчитель», що генерує цільовий сигнал для налаштування нейромережі. Процес конвертації знань у дані здійснюється шляхом ітеративного обходу графа. Логічні умови предикатних вузлів, що відповідають вхідним лінгвістичним термам трансформуються у вхідний вектор ознак  $X$ , а вихідні значення вузлів нечіткої продукції – у цільовий вектор еталонного ризику  $R_r$ . Пряме звернення ANFIS до структури Rete-мережі забезпечує цілісність передачі знань від експертної системи до нейромережевого апроксиматора без використання проміжних зовнішніх файлів.

Для забезпечення валідності регресійного аналізу та навчання ANFIS на основі повної бази знань було сформовано репрезентативну навчальну вибірку, що складається з рівномірно розподілених контрольних точок. Це дозволяє моделі коректно узагальнити правила для всього простору можливих станів системи. Фрагмент сформованої навчальної вибірки представлено в таблиці 2.12.

Таблиця 2.12 – Фрагмент репрезентативної навчальної вибірки для налаштування параметрів моделі ANFIS

№ правила	Цінність активу, $\bar{x}_1$	Імовірність реалізації загрози через наявну вразливість, $\bar{x}_2$	Рівень збитків від загрози, $\bar{x}_3$	Рівень контролю інформаційних ресурсів, $\bar{x}_4$	Рівень витрат на створення та експлуатацію системи ІБ, $\bar{x}_5$	Рівень культури ІБ ТЛЦ, $\bar{x}_6$	Ризик, $R_r$
1	0,10	0,15	0,10	0,25	0,75	0,87	0,18
15	0,10	0,15	0,10	0,50	0,42	0,42	0,32
120	0,30	0,48	0,35	0,25	0,65	0,55	0,41
540	0,50	0,48	0,35	0,70	0,42	0,42	0,54
1024	0,70	0,48	0,65	0,50	0,15	0,15	0,68
1500	0,70	0,80	0,65	0,97	0,15	0,15	0,75
2100	0,90	0,80	0,90	0,70	0,15	0,42	0,84
2880	0,90	0,80	0,90	0,97	0,15	0,15	0,92

Представлені у таблиці 2.19 дані є результатом нормалізації та квантування нечітких правил, де вхідні вектори  $x$  відповідають ядрам відповідних нечітких множин, а цільові значення ризику обчислені за допомогою експертного алгоритму нечіткого виведення (модуль 4).

Оптимізація параметрів усіх локальних поліномів здійснюється шляхом градієнтного спуску із мінімізацією середньоквадратичної помилки (MSE) між виходом ANFIS та еталонними значеннями з модуля 4:

$$MSE = \frac{1}{N} \sum_{p=1}^N (R_p - R_{r,p})^2 \rightarrow \min, \quad (2.28)$$

де  $N$  – кількість навчальних прикладів,  $R_p$  – вихід ANFIS для  $p$ -го прикладу,  $R_{r,p}$  – еталонний ризик для  $p$ -го прикладу. Оптимізація відбувається не тільки для коефіцієнтів поліномів, але й для параметрів функцій належності, що є стандартом для ANFIS.

*Крок 5. Редукція моделі.* Після первинного навчання проводиться ітеративне спрощення:

- обчислюються глобальні середні значення коефіцієнтів локальних поліномів по всіх правилах;
- здійснюється ідентифікація та відсів статистично незначущих коефіцієнтів, абсолютне значення яких менше за критичний поріг  $\delta$ :  $|\beta_{ij,k}| < \delta$ . Значення критичного порогу  $\delta$  визначають на основі статистичних критеріїв значущості, зокрема з використанням  $t$ -статистики Стюдента [116] для перевірки нульової гіпотези про рівність відповідного коефіцієнта нулю при заданому рівні надійності. Поріг може встановлюватися емпіричним шляхом на основі аналізу чутливості моделі до зміни її параметрів;
- визначаються незначущі коефіцієнти та виключаються з вектора параметрів, що оптимізуються для подальших ітерацій навчання;
- процес навчання та редукції повторюється ітеративно, доки всі активні коефіцієнти моделі не набудуть статистичної значущості.

*Крок 6. Агрегація та фінальний результат.* Ступінь виконання правила  $w_k(X)$  обчислюється як  $T$ -норма (добуток) ступенів належності:

$$w_k(X) = \prod_{i=1}^6 \mu_{A_i^{(k)}}(x_i). \quad (2.29)$$

Нормалізована вага правила:

$$\bar{w}_k(X) = \frac{w_k(X)}{\sum_{j=1}^{N_{rules}} w_j(X)}. \quad (2.30)$$

Фінальний рівень ризику  $R \in [0,1]$  обчислюється як зважена сума виходів правил з наступною нормалізацією через сигмоїдну функцію:

$$R(X) = \sigma\left(\sum_{k=1}^{N_{rules}} \bar{w}_k(X) \cdot z_k(X)\right), \quad (2.31)$$

де  $\sigma(y) = \frac{1}{1+e^{-\lambda y}}$  – сигмоїдна функція активації, що відображає результат у діапазон  $[0,1]$ ;  $\lambda$  – коефіцієнт нахилу сигмоїди;  $\bar{w}_k(X)$  – нормалізована активація правила  $k$ ;  $z_k(X)$  – локальний висновок  $k$ -го правила.

Модуль підтримує оцінку адекватності на тестових даних (MAE, RMSE, кореляція між передбачуваним і фактичним ризиком) [117].

Модель можна зберігати та відновлювати, включаючи всі правила, коефіцієнти, параметри та конфігурацію факторів і термів.

Важливою архітектурною особливістю розробленої інформаційної технології є підтримка повного життєвого циклу (ЖЦ) нейронечіткої моделі. Згідно з методологією, запропонованою у [118], життєвий цикл розробки нейронечіткої моделі охоплює етапи структурної та параметричної ідентифікації. При цьому, як зазначається у [87], ключовим аспектом є забезпечення збіжності алгоритму навчання на етапі тестування моделі.

Це забезпечує збереження її структурного стану й можливість безперервного еволюційного розвитку в умовах динамічного середовища ТЛЦ.

ЖЦ моделі базується на трьох ключових механізмах:

1. Серіалізація та збереження топології. Система забезпечує серіалізацію навченої моделі, зберігаючи вагові коефіцієнти поліномів і матрицю активних правил. Це дозволяє зафіксувати виявлену на етапі редукції топологію значущих зв'язків. При перезапуску або масштабуванні системи не потрібно повторно проводити ресурсомісткий процес відсіву незначущих правил – модель миттєво відновлюється в оптимізованому стані, готовому до експлуатації;

2. Безперервне донавчання на емпіричних даних. На початковому етапі модель функціонує на базі «синтетичного вчителя» (Rete-генератора). Перевагою

використання Rete-структури, є можливість миттєвого порівняння прогнозів нейромережі з еталонними експертними правилами на будь-якому етапі навчання, що дозволяє контролювати відхилення (MSE) не лише на статистичних даних, а й щодо експертної логіки. У процесі експлуатації ТЛЦ відбувається накопичення реальної статистики інцидентів та результатів аудиту безпеки. Методологія передбачає режим поступового донавчання. Збережені коефіцієнти моделі використовуються як стартова точка, а градієнтна оптимізація продовжується вже на реальних, а не синтетичних даних. Це дозволяє плавно трансформувати систему з експертної в гібридну, підвищуючи точність прогнозів по мірі накопичення статистики.

3. Адаптивна реконфігурація в умовах змін. Критичною вимогою до систем захисту в умовах війни є здатність реагувати на зміну зовнішніх умов (адаптивна реконфігурація). При зміні стратегічних пріоритетів (наприклад, введення воєнного стану) оператор оновлює лише вхідні матриці парних порівнянь у модулі Fuzzy АНР. Це слугує тригером для автоматичної перебудови моделі:

- система генерує нові еталонні сигнали з урахуванням нових ваг;
- запускається процес перенавчання поліноміальних ядер для існуючої бази правил;
- модель адаптує свою «чутливість» до ризиків без необхідності переписування коду чи ручної зміни правил.

## **2.4 Оптимізація та стратегічне управління ризиками ІБ ТЛЦ**

Логічним завершенням процесу моделювання є перехід від оцінювання рівня ризику, описаного в п. 2.3 до формування науково обґрунтованих рекомендацій щодо мінімізації ризику ІБ ТЛЦ. Вихідним результатом розробленої адаптивної нейронечіткої моделі є явна диференційована аналітична функція  $R(X)$  (поліном другого ступеня) [119], [120]. Це дозволяє застосувати методи математичного аналізу для пошуку оптимальних стратегій захисту.



Розглянемо математичний апарат розв'язання оберненої задачі моделювання – знаходження вектора керованих параметрів захисту, який забезпечує мінімально можливий рівень ризику при заданих ресурсних обмеженнях та фіксованому зовнішньому контексті.

Завдання управління ризиком ІБ ТЛЦ формалізується як задача нелінійного програмування. Це вважається одним з ефективних підходів підтримки прийняття рішень в транспортно-логістичних системах [121].

Вектор вхідних змінних  $X = \{x_1, \dots, x_6\}$  визначається двома підмножинами:

1. Некеровані змінні ( $X_{fix}$ ). Це фактори зовнішнього середовища:  $x_1$  – рівень цінності активів,  $x_2$  – ймовірність реалізації загроз через наявні вразливості,  $x_3$  – рівень збитків від загроз. Їх значення фіксовані на момент прийняття рішення ( $x_i = c_i = const$ ).

2. Керовані змінні ( $X_{ctrl}$ ). Важелі впливу:  $x_4$  – рівень контролю інформаційних ресурсів,  $x_5$  – рівень витрат на створення та експлуатацію ІБ,  $x_6$  – рівень культури ІБ. Їх значення необхідно оптимізувати.

Цільова функція ризику  $R(X)$ , отримана з ANFIS-моделі це квадратичний поліном вигляду:

$$R(X) = \beta_0 + \sum_{i=1}^n \beta_i x_i + \sum_{i=1}^n \beta_{ii} x_i^2 + \sum_{i=1}^{n-1} \sum_{j=i+1}^n \beta_{ij} x_i x_j, \quad (2.32)$$

де  $n = 6$  – загальна кількість факторів;

$\beta_0$  – вільний член (константа зміщення);

$\beta_i$  – коефіцієнти лінійних членів, що відображають прямий вплив факторів  $x_i$ ;

$\beta_{ii}$  – коефіцієнти квадратичних членів, що відображають нелінійні ефекти насичення;

$\beta_{ij}$  – коефіцієнти членів парної взаємодії, що відображають синергетичні ефекти між факторами  $x_i$  та  $x_j$ .

Задача оптимізації полягає у мінімізації функції шляхом варіювання керованих змінних при заданих обмеженнях:

$$\begin{cases} \min_{X_{ctrl}} R(X_{fin}, X_{ctrl}) \\ 0 \leq x_j \leq 1, \forall x_j \in X_{ctrl} \end{cases} \quad (2.33)$$

Обмеження у вигляді одиничного гіперкуба обумовлені використанням нормованих лінгвістичних змінних і гарантують фізичну реалістичність знайдених рішень.

Для розв'язання поставленої задачі застосовано підхід, що ґрунтується на символічному аналізі похідних, що дозволяє отримати точний аналітичний розв'язок.

*Етап 1.* Редукція розмірності моделі. На першому кроці виконується спрощення цільової функції шляхом підстановки фіксованих значень некерованих факторів  $x_i \in X_{fix}$  у загальне рівняння полінома.

Це дозволяє перейти від глобальної функції  $R(X)$  до локальної функції  $R_{loc}(X_{ctrl})$ , яка залежить виключно від керованих змінних. Математично це виглядає як згортання всіх членів, що не містять змінних з  $X_{ctrl}$ , у модифікований вільний член  $\beta'_0$ :

$$R_{loc}(X_{ctrl}) = \beta'_0 + \sum_{x_j \in X_{ctrl}} \beta'_j x_j + \sum_{x_j \in X_{ctrl}} \beta_{jj} x_j^2 + \sum_{x_j, x_k \in X_{ctrl}, j < k} \beta_{jk} x_j x_k, \quad (2.34)$$

де  $\beta'_0$  та  $\beta'_j$  – перераховані коефіцієнти, що включають вплив фіксованих факторів.

*Етап 2.* Обчислення символічних градієнтів. Для аналізу чутливості ризику до зміни керованих факторів аналітично обчислюється вектор градієнта – набір частинних похідних локальної функції:

$$\nabla R_{loc} = \left\{ \frac{\partial R_{loc}}{\partial x_j} \mid x_j \in X_{ctrl} \right\}. \quad (2.35)$$

Символьний вираз для часткової похідної по конкретному керованому фактору  $x_k$  має вигляд лінійної функції відносно інших змінних:

$$\frac{\partial R_{loc}}{\partial x_k} = \beta'_k + 2\beta_{kk}x_k + \sum_{x_j \in X_{ctrl}, j \neq k} \beta_{kj} x_j. \quad (2.36)$$

*Етап 3.* Визначення точок екстремуму та стратегій. Аналіз поведінки отриманих символічних похідних дозволяє визначити оптимальну стратегію для кожного фактора. Дослідження знаку виразу  $\frac{\partial R_{loc}}{\partial x_k}$  на відрізку  $x_k \in [0, 1]$  надає можливість розглянути наступні два випадки:

1. Граничний оптимум. Якщо похідна  $\frac{\partial R_{loc}}{\partial x_k}$  не змінює знак на всьому діапазоні (функція монотонна), оптимум досягається на межі:

- якщо  $\frac{\partial R_{loc}}{\partial x_k} > 0$  (ризик зростає при збільшенні фактора), то  $x_k^* = 0$ ;
- якщо  $\frac{\partial R_{loc}}{\partial x_k} < 0$  (ризик спадає при збільшенні фактора), то  $x_k^* = 1$ .

2. Внутрішній оптимум. Якщо похідна змінює знак, це свідчить про наявність локального екстремуму (точки насичення). У цьому випадку система символічно розв'язує рівняння стаціонарності для знаходження точної точки оптимуму  $x_k^* \in (0, 1)$ :

$$\beta'_k + 2\beta_{kk}x_k + \sum_{x_j \in X_{ctrl}, j \neq k} \beta_{kj} x_j = 0. \quad (2.37)$$

Результатом функціонування модуля 6 є визначений набір оптимальних значень керованих факторів  $X_{ctrl}^* = \{x_j^*\}$ , а також деталізований аналітичний звіт. Цей звіт містить розраховані числові значення, символічні математичні вирази частинних похідних, які обґрунтовують вибір стратегії управління (на кшталт, стратегії максимізації фактора у випадку монотонного спадання функції ризику).

Отримані математичні результати проходять етап інтерпретації та трансформуються у вербальні управлінські рекомендації для керівництва ТЛЦ. Залежно від комбінації зовнішніх умов та розрахованих оптимумів, система може запропонувати стратегію тотальної мобілізації («максимізувати всі заходи контролю») або гнучкий диференційований підхід.

Проведений аналіз поліноміальної моделі ризику дозволяє виявити фундаментальні нелінійні закономірності функціонування системи ІБ ТЛЦ. Глибока інтерпретація значень коефіцієнтів полінома (вільного члена, лінійних та квадратичних ефектів) та особливо їх парних взаємодій розкриває приховану внутрішню механіку формування інтегрального ризику.

Узагальнені результати теоретичного аналізу ключових елементів розробленої поліноміальної моделі, що демонструють їх фізичний та економічний зміст у контексті ІБ ТЛЦ, систематизовано та наведено в таблиці 2.13.

Таблиця 2.13 – Теоретична інтерпретація елементів поліноміальної моделі ризику ІБ ТЛЦ

Рівень аналізу	Математичний елемент моделі	Ключові коефіцієнти	Теоретична інтерпретація в контексті ІБ ТЛЦ
1. Базова топологія	Вільний член $\beta_0$ – калібрувальне зміщення	$\beta_0 < 0$	Оскільки ризик завжди в діапазоні $[0, 1]$ , це вказує на наявність «запасу стійкості» або «порогу активації» системи. За відсутності активних заходів захисту ( $x_4 = x_5 = x_6 = 0$ ), незначні загрози не призводять до миттєвого виникнення ризику. Система має певну інерцію.
		$\beta_0 > 0$	У стані абсолютного спокою (немає активів, немає загроз, немає захисту), модель показує наявність базового ризику
		$\beta_0 = 0$	Ризик з'являється тоді і тільки тоді, коли з'являється принаймні один фактор загрози.
2. Лінійна чутливість	Знаки лінійних коефіцієнтів $\beta_i$ – функціональна дихотомія	$\text{sing}(\beta_i) > 0$	Фактори, збільшення яких призводить до зростання інтегрального ризику $R$ (цінність активів, ймовірність загроз).
		$\text{sing}(\beta_i) < 0$	Фактори, збільшення яких призводить до зменшення інтегрального ризику $R$ (рівень контролю, бюджет ІБ).
3. Нелінійна динаміка	Квадратичні члени $\beta_{ii}x_i^2$ – кривизна чутливості	$\beta_{ii} > 0$	Опуклість загроз – прискорення. Ризик зростає нелінійно коли перехід до критичних рівнів загрози генерує непропорційно великий приріст інтегрального ризику.
		$\beta_{ii} < 0$	Увігнутість захисту – насичення. Математичне підтвердження закону спадної граничної віддачі. Ефективність нарощування заходів захисту знижується за мірою наближення до їх максимального рівня ( $x_i \rightarrow 1$ ).
		$\beta_{ii} = 0$	Точка, де функція ризику припиняє зменшуватися при подальшому збільшенні значення фактора $x_k$ .
4. Теорія взаємодій	Члени парної взаємодії	$\beta_{ij} > 0$	Мультиплікація загроз. Взаємне посилення факторів ризику. Демонструє мультиплікативний

Рівень аналізу	Математичний елемент моделі	Ключові коефіцієнти	Теоретична інтерпретація в контексті ІБ ТЛЦ
	$\beta_{ij}x_ix_j$ – коефіцієнт синергії		ефект при комбінації факторів загрози (на кшталт, висока ймовірність $\times$ великі збитки).
		$\beta_{ij} < 0$	Протективна синергія. Конструктивна інтерференція захисних заходів. Комплексна ефективність системи захисту перевищує просту суму ефективностей її індивідуальних компонентів.
		$\beta_{ij} = 0$	Відсутність прямої парної взаємодії (синергії або антагонізму) між двома факторами $x_i$ та $x_j$ у формуванні підсумкового рівня ризику $R$ . Фактори $x_i$ та $x_j$ впливають на ризик незалежно (адитивно).
5. Диференціальний аналіз	Частинні похідні $\frac{\partial R}{\partial x_j}$ – динамічна гранична ефективність	$\frac{\partial R}{\partial x_j} > 0$ (на всьому діапазоні)	Контрпродуктивний захід. Збільшення фактора $x_k$ монотонно підвищує ризик. На кшталт, надмірний контроль може сповільнити логістику настільки, що ризики збоїв перевищать вигоду від безпеки. Рекомендація: мінімізація заходу.
		$\frac{\partial R}{\partial x_j} < 0$ (на всьому діапазоні)	Безумовно корисний захід. Збільшення фактора $x_k$ монотонно знижує ризик. На кшталт, інвестиції в культуру ІБ при її низькому рівні дають значний позитивний ефект. Рекомендація: максимізація заходу.
		$\exists x_k^* \in (0,1)$ $\frac{\partial R}{\partial x_j} = 0$	Внутрішній оптимум (точка насичення). Існує оптимальний рівень $x_k^*$ , перевищення якого неефективне (закон спадної віддачі). На кшталт, надмірний бюджет ( $x_5$ ) веде до неефективних витрат, а надмірний контроль ( $x_4$ ) – до «тіньового ІТ». Рекомендація: підтримка на оптимальному рівні.

Отримані висновки підтверджують необхідність застосування комплексного, диференційованого підходу до управління ІБ ТЛЦ, який враховує

не лише індивідуальні характеристики факторів, а й їх складну нелінійну взаємодію.

## **Висновки до розділу 2**

У другому розділі дисертаційної роботи розроблено математичне забезпечення інтегрального оцінювання ризиків ІБ ТЛЦ. Проведене дослідження дозволило отримати наступні результати:

Розроблено концептуальну модель ІТ, яка базується на гібридному підході, що поєднує експертні знання з адаптивними алгоритмами машинного навчання (ANFIS). Модульна архітектура системи, яка включає шість функціональних блоків та дворівневу структуру баз даних (операційну та аналітичну), забезпечує повний цикл управління ризиками: від первинної фазифікації вхідних потоків у реальному часі до формування оптимальних керуючих впливів.

Запропоновано метод стратегічного аналізу на основі трирівневої ієрархічної декомпозиції факторів ризику. Використання такої структури у поєднанні з модифікованим методом Fuzzy АНР (синтез алгоритмів Чанга та Баклі) дозволило системно пріоритезувати чинники та нівелювати проблему «нульових ваг». Для наочної інтерпретації результатів та вибору стратегій захисту в умовах суб'єктивної невизначеності впроваджено показник впевненості експерта та удосконалено матрицю Дж. Х. Вілсона шляхом введення нечітких координат. Розрахунок експертної інтегральної оцінки стратегічного ризику реалізовано за допомогою методу Fuzzy SAW, що забезпечує верифікацію даних ще до етапу неймережевого моделювання. Експериментальне тестування підтвердило, що підвищення впевненості експертів призводить до звуження носія нечіткої множини результату, що доводить збіжність розроблених алгоритмів та їх здатність до коректної обробки неформалізованих даних у динамічному середовищі ТЛЦ.

Обґрунтовано використання архітектури ANFIS із поліноміальною структурою консеквентів другого ступеня для уточнення інтегральної оцінки ризику. Розроблено механізм подолання проблеми відсутності даних шляхом автоматизованої генерації синтетичної навчальної вибірки за допомогою нечіткого висновку Мамдані. Це забезпечує працездатність моделі за умов відсутності ретроспективних даних, трансформуючи лінгвістичну базу правил у точний нелінійний апроксиматор. Для оптимізації процесу вилучення еталонних значень із бази правил, яка набуває комбінаторної складності через значну кількість факторів, застосовано алгоритм Rete. Він трансформує лінійний перебір правил у мережеву структуру графа. Така архітектура дозволяє мінімізувати обчислювальні витрати при формуванні еталонних значень для навчання та забезпечує високу продуктивність інформаційної технології в умовах складної конфігурації вхідних факторів.

Формалізовано задачу управління ризиками як задачу нелінійне програмування. Застосування символьного градієнта до диференційовної функції  $R(X)$  дозволило визначити оптимальні параметри захисту та ідентифікувати «точки насичення» витрат. Інтерпретація коефіцієнтів моделі виявила ефекти «протективної синергії» та «мультиплікації загроз», що обґрунтовує перевагу системного підходу над адитивним у безпеці ТЛЦ.

Основні наукові результати, отримані у розділі 2, опубліковані у статтях [77], [89], [93], [106] і тезах [90], [91], [102], [108].

## **РОЗДІЛ 3. ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІБ ТЛЦ**

### **3.1 Функціональне моделювання процесів підтримки прийняття рішень**

Розглянуті у попередньому розділі математичні моделі та методи експертного та адаптивного оцінювання рівня ризику ІБ ТЛЦ створюють теоретичне підґрунтя для розробки інформаційної технології ППР для забезпеченні ІБ ТЛЦ. З метою практичної імплементації запропонованого підходу в архітектурі СППР необхідно декомпонувати загальний процес функціонування на три логічно взаємопов'язані етапи:

1. Агрегація даних та аналіз контексту безпеки;
2. Адаптивне моделювання та оцінювання ризиків (стратегічне і адаптивне моделювання);
3. Синтез управлінських рішень.

Для всебічного аналізу потоків даних та формалізації цих етапів в інформаційній системі ТЛЦ використано методи функціонального моделювання, зокрема методологію IDEF0 [122], [123].

Контекстна діаграма IDEF0 (рівень А-0) представлена на рисунку 3.1, відображає функціональну структуру інформаційної технології як єдину цілісну систему.



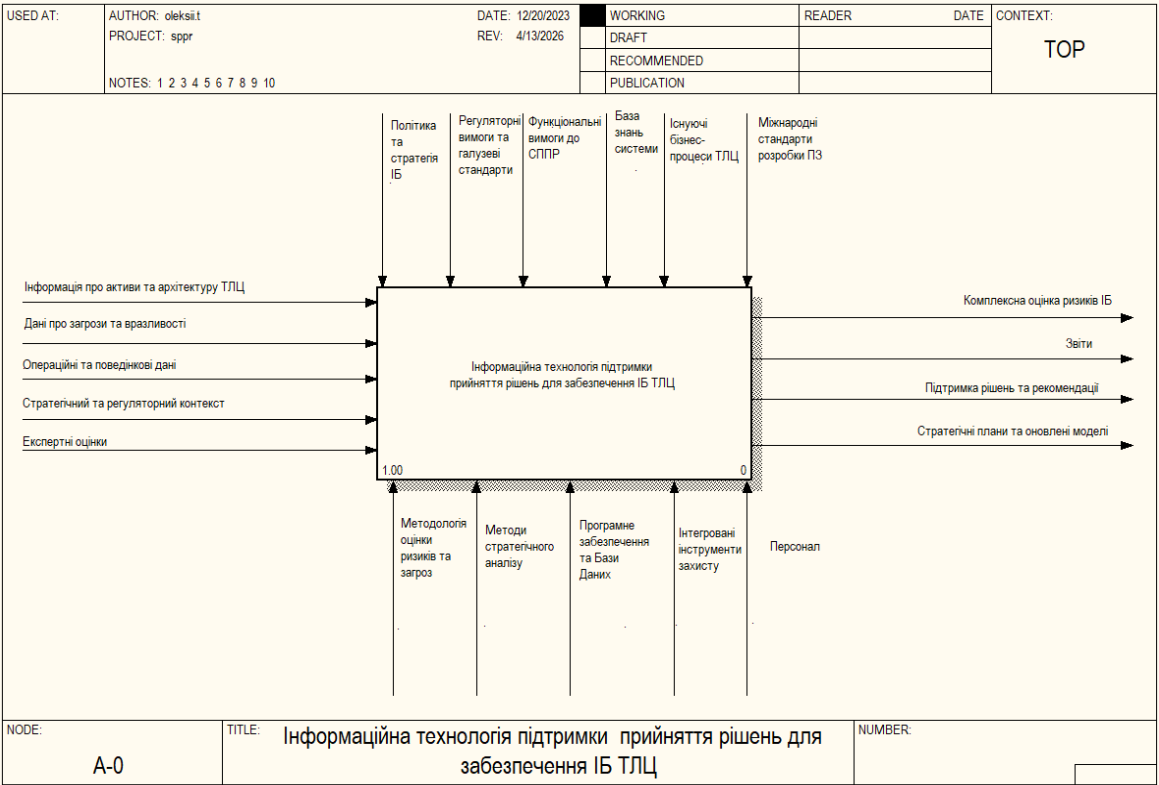


Рисунок 3.1 – Контекстна діаграма інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ

- Входи* – вхідні дані та ресурси, що підлягають трансформації в системі:
- інформація про активи та архітектуру (дані з CMDB про конвергентну інфраструктуру ТЛЦ, WMS, TMS, промислові контролери, IoT-датчики);
  - дані про загрози та вразливості (потік зовнішніх даних Threat Intelligence, CVE, MITRE ATT&CK та результати внутрішніх сканувань);
  - операційні та поведінкові дані (телеметрія реального часу, системні логи, мережевий трафік);
  - стратегічний та регуляторний контекст (бізнес-цілі, SLA);
  - експертні оцінки (структуровані знання експертів, отримані через анкетування).

*Керуючі елементи* – правила, стандарти та обмеження функціонування технології:

- політика та стратегія ІБ (визначення допустимого рівня ризику);

- регуляторні вимоги та галузеві стандарти (ISO/IEC 27001, NIST CSF, GDPR);
- функціональні вимоги до СППР (бюджетні ліміти, часові рамки);
- БЗ системи (продукційні правила, лінгвістичні шкали, функції належності);
- існуючі бізнес-процеси та процедури безпеки.

*Механізми* – ресурси та інструменти реалізації:

- методологія оцінки ризиків ІБ (адаптивна методика);
- методи стратегічного аналізу (Fuzzy AHP, ANFIS, матриця Дж. Х. Вілсона);
- ПЗ та БЗ (серверна частина, СУБД, модулі обробки знань);
- інтегровані інструменти захисту (SIEM, IDS/IPS);
- персонал (інженери з безпеки, аналітики, ОПР).

*Виходи* – результати функціонування системи:

- комплексна оцінка ризиків ІБ (кількісні та якісні показники);
- звіти (аналітичні зведення, індикатори компрометації);
- підтримка рішень та рекомендації (ранжований список контрзаходів з обґрунтуванням «витрати-вигода»);
- стратегічні плани та оновлені моделі (результат самонавчання системи).

Для наочного відображення функціональних процесів системи була побудована діаграма декомпозиції функціонального блоку А0 (рис. 3.2).

Декомпозиція системи (рівень А1) виділяє чотири ключові функціональні блоки:

1. Блок «Агрегація даних та аналіз контексту безпеки» забезпечує збір та консолідацію різномірної інформації з широкого спектру джерел, включаючи дані про технічний стан обладнання, зовнішні вектори загроз, телеметрію мережевого функціонування та результати експертного оцінювання. Основне завдання – здійснення первинної обробки вхідних потоків, що передбачає їхню верифікацію, фільтрацію від інформаційного «шуму» та нормалізацію для приведення даних до уніфікованого стандарту, необхідного для коректного подальшого аналізу та моделювання.

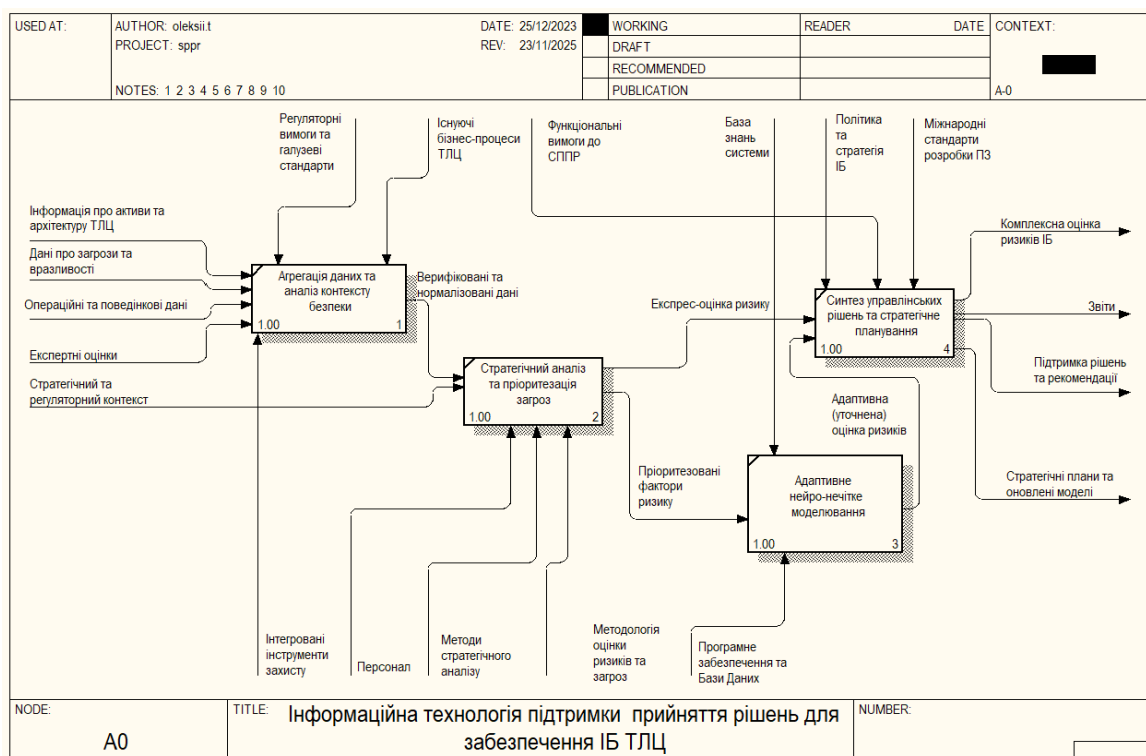


Рисунок 3.2 – Діаграма декомпозиції інформаційної технології підтримки прийняття рішень для забезпеченні ІБ ТЛЦ (A1)

2. Блок «Стратегічний аналіз та пріоритезація загроз» виконує попередню селекцію виявлених факторів. Здійснюється диференціація ризиків: критичні фактори передаються для глибокого інтелектуального аналізу, тоді як стандартні оцінки – спрямовуються безпосередньо до модулів формування оперативної звітності, що дозволяє оптимізувати обчислювальні ресурси системи.

3. Блок «Адаптивне нейро-нечітке моделювання» – це інтелектуальне ядро системи. Воно детально обробляє найскладніші загрози. Система працює гібридно: для нових, невідомих загроз використовує закладені правила (експертний підхід), а для знайомих ситуацій – нейромережу, яка постійно навчається на історії інцидентів, покращуючи об'єктивність та точність отриманих результатів оцінювання.

4. Блок «Синтез управлінських рішень та стратегічне планування» забезпечує фінальний етап, де об'єднуються результати експертної оцінки та глибокого аналізу. Враховуючи бюджетні обмеження та політику безпеки, модуль

формує для керівника (ОПР) готові рекомендації, план дій та підсумкові звіти.

Для деталізації інформаційного обміну між виділеними процесами та зовнішніми сутностями розроблено діаграму потоків даних (Data Flow Diagram – DFD) представлену на рисунку 3.3.

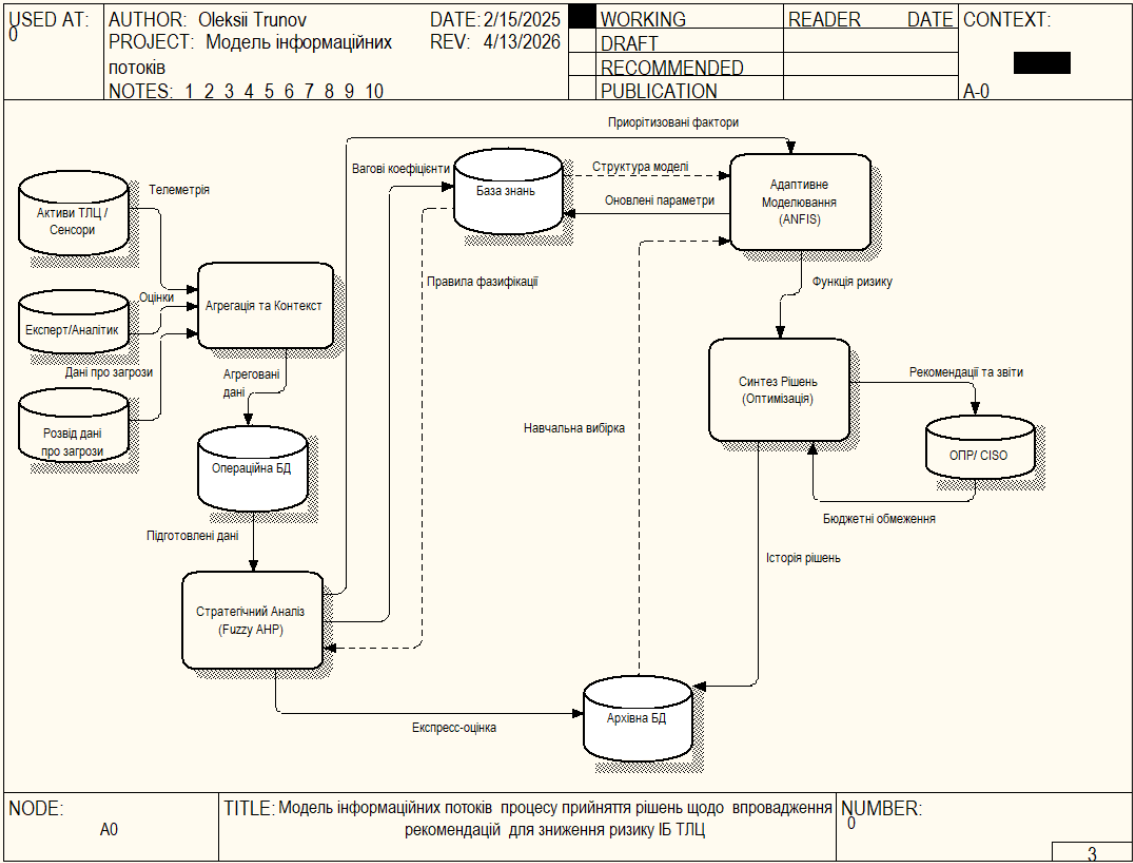


Рисунок 3.3 – Діаграма інформаційних потоків процесу прийняття рішень щодо впровадження рекомендацій для зниження ризику ІБ ТЛЦ (DFD)

Побудована модель DFD дозволяє відстежити повний цикл трансформації даних від моменту їх надходження у систему до формування керуючого впливу. Ключовими потоками даних є потоки:

- вхідної телеметрії від активів ТЛЦ, що накопичуються у сховищі часових рядів;
- нормалізованих векторів загроз, що передаються від модуля агрегації до модуля нечіткого виведення;

– керуючих сигналів (рекомендацій), що спрямовуються до ОПР для затвердження.

Такий рівень деталізації потоків даних дозволяє забезпечити необхідний базис для визначення вимог до пропускної здатності каналів зв'язку, структури БД та регламентів обміну інформацією між модулями системи.

Застосування методології IDEF3 дозволяє суттєво доповнити функціональну модель IDEF0 шляхом деталізованого опису сценарної послідовності процесів та часової динаміки їхньої взаємодії. На рисунку 3.4 представлена діаграма процесу експертного нечіткого оцінювання рівня ризику ІБ ТЛЦ у стандарті IDEF3.

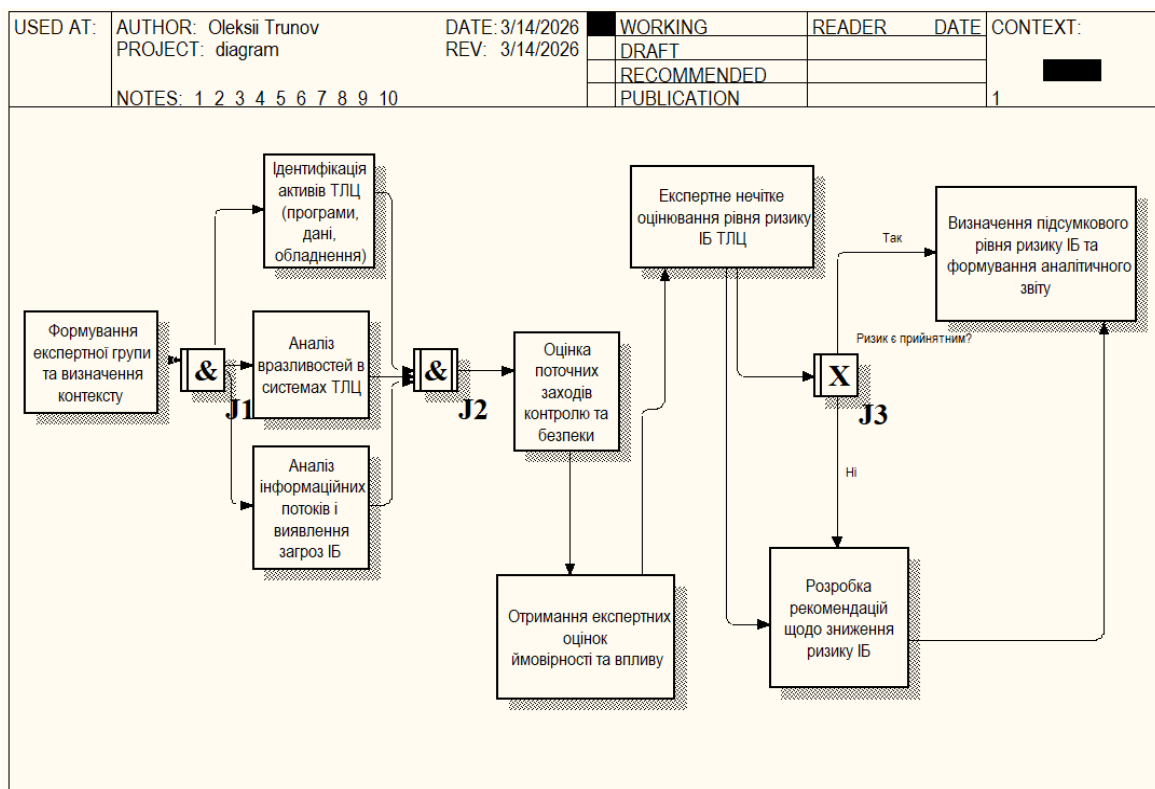


Рисунок 3.4 – Діаграма процесу експертного нечіткого оцінювання ІБ ТЛЦ (IDEF3)

Діаграма описує весь шлях від опитування експертів до створення готового звіту. Застосування Fuzzy SAW перетворює розрізнені експертні оцінки на структуровану систему пріоритетів, дозволяючи ідентифікувати критичні ризики

в умовах нечіткості. Це забезпечує відбір найбільш критичних векторів загроз для їх подальшого адаптивного моделювання шляхом трансформації математичних розрахунків у стратегічно обґрунтовані висновки для ОПР. Такий підхід дозволяє не лише структурувати процес прийняття рішень, мінімізувати часові витрати на документування результатів, а й знизити вплив суб'єктивного фактора.

Побудовані функціональні моделі (рис. 3.1–3.5) дозволяють визначити межі системи та структуру інформаційних потоків. Проте для розуміння практичної взаємодії суб'єктів управління (експертів, інженерів та ОПР) із алгоритмічними компонентами СППР необхідно представити узагальнену інформаційно-логічну схему функціонування технології (рис. 3.5).

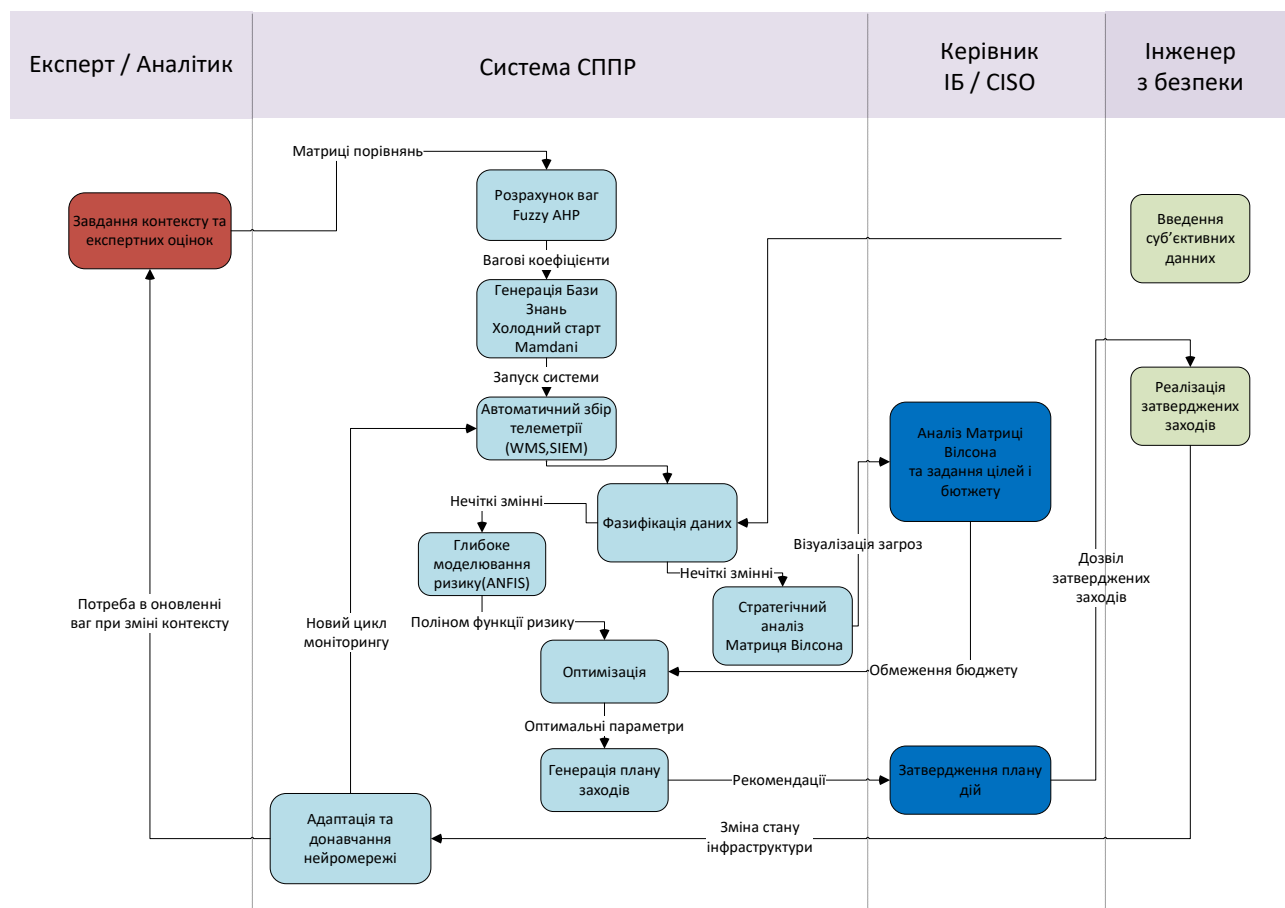


Рисунок 3.5 – Загальна інформаційно-логічна схема функціонування та взаємодії суб'єктів ІТ ППР

Представлена схема інтегрує математичний апарат та функціональні процеси у єдиний технологічний цикл.

Експерт/Аналітик забезпечує початкове налаштування контексту та формування матриць попарних порівнянь для методу Fuzzy АНР, що дозволяє системі розрахувати ваги факторів та здійснити «холодний старт» моделі Mamdani.

Інженер з безпеки відповідає за введення суб'єктивних даних та контроль автоматичного збору телеметрії, яка після фазифікації стає основою для глибокого моделювання ризику в ANFIS.

Керівник (ОПР) на основі аналізу матриці Дж. Х. Вілсона та заданих бюджетних обмежень ініціює прескриптивну оптимізацію, результатом якої є затверджений план заходів.

Цикл адаптації забезпечує донавчання нейромережі на основі змін стану інфраструктури, що гарантує актуальність прогностичних оцінок у динамічному середовищі ТЛЦ. Це дозволяє перейти від функціонального опису до проєктування технічної архітектури та програмної реалізації відповідних модулів.

Сформований комплекс моделей IDEF0 та IDEF3 визначає межі системи та логіку інформаційних потоків. Подальша програмна реалізація для деталізації динамічної взаємодії користувачів із компонентами СППР та формування вимог до архітектури системи потребує переходу до об'єктно-орієнтованого моделювання засобами мови UML.

### **3.2 Моделювання сценаріїв взаємодії користувачів мовою UML**

Якщо моделі IDEF0 та DFD описують внутрішню логіку, то для формалізації взаємодії персоналу ТЛЦ із системою використано діаграми прецедентів (Use Case Diagram) мови UML [124], [125]. Це дозволяє деталізувати вимоги до інтерфейсу системи.

У системі ідентифіковано три ключові ролі (актори), характеристики яких

наведено у таблиці 3.1.

Таблиця 3.1 – Характеристика суб'єктів взаємодії в ІТ ППР

Актор (Роль)	Рівень управління	Ключова функціональна відповідальність
Інженер з безпеки (Адміністратор)	Технічний / Операційний	Моніторинг активів, збір телеметрії, управління доступом.
Інженер зі знань (Експерт/Аналітик)	Аналітичний / Методологічний	Налаштування БЗ, верифікація нейромережових моделей, формалізація правил.
Особа, що приймає рішення (ОПР)	Стратегічний	Вибір стратегії захисту, затвердження планів на основі моделювання.

1. Інженер з безпеки (Адміністратор) здійснює технічний супровід та операційний моніторинг. Виконує первинний збір даних про стан об'єктів ТЛЦ: ідентифікація та інвентаризація активів системи, здійснення безперервного контролю поточної телеметрії, що надходить із датчиків та інтегрованих систем спостереження; адміністрування прав користувачів та керування рівнями доступу до ресурсів системи.

2. Інженер зі знань (Експерт/Аналітик) здійснює налаштування та супровід інтелектуального ядра системи. Реалізує задання формалізації суб'єктивних експертних оцінок у формі чітких продукційних правил, визначення та налаштування параметрів лінгвістичних змінних для нечіткого логічного виводу, верифікацію результатів роботи та контроль процесу навчання ANFIS-моделі, забезпечення адекватності бази знань поточним загрозам.

3. Особа, що приймає рішення (ОПР/Керівник) виконує функції стратегічного управління безпекою та ризиками. Проводить глобальний моніторинг ландшафту ризиків ТЛЦ за допомогою інтерактивних аналітичних панелей, здійснює інтерпретацію та оцінювання результатів, отриманих у ході моделювання сценаріїв оптимізації, остаточно приймає вибір та затверджує фінальну стратегію захисту на основі аналітичних висновків системи.

Візуалізацію сценаріїв використання системи представлено на рис. 3.6.



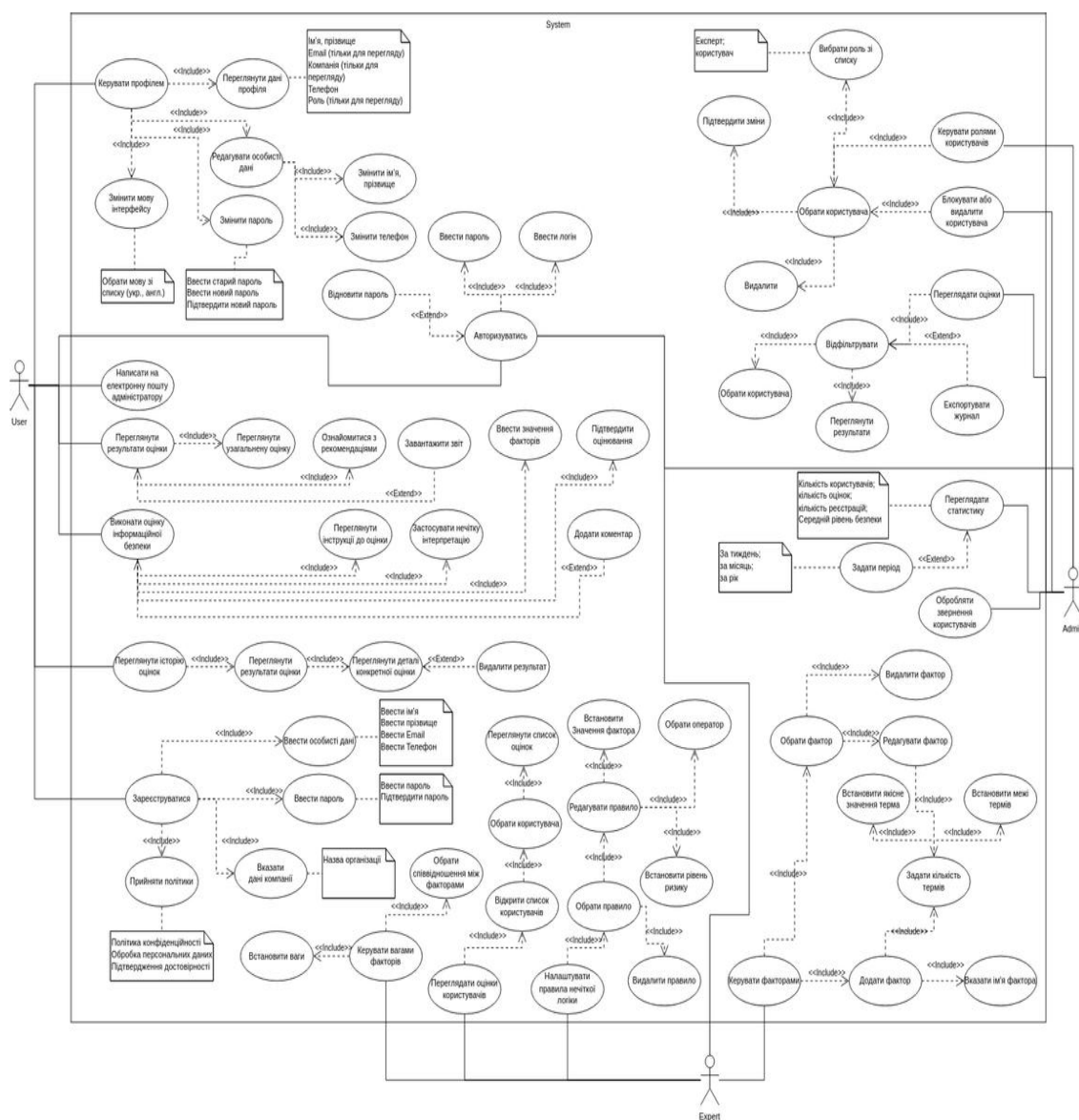


Рисунок 3.6 – Загальна діаграма варіантів використання (Use Case)

*Сценарії взаємодії для користувача.* Основною функцією є ініціація оцінювання, введення даних та отримання звіту. Це реалізує сценарій «швидкої перевірки» безпеки ТЛЦ (рис. 3.7).







можливість незалежного оновлення інтелектуальних компонентів.

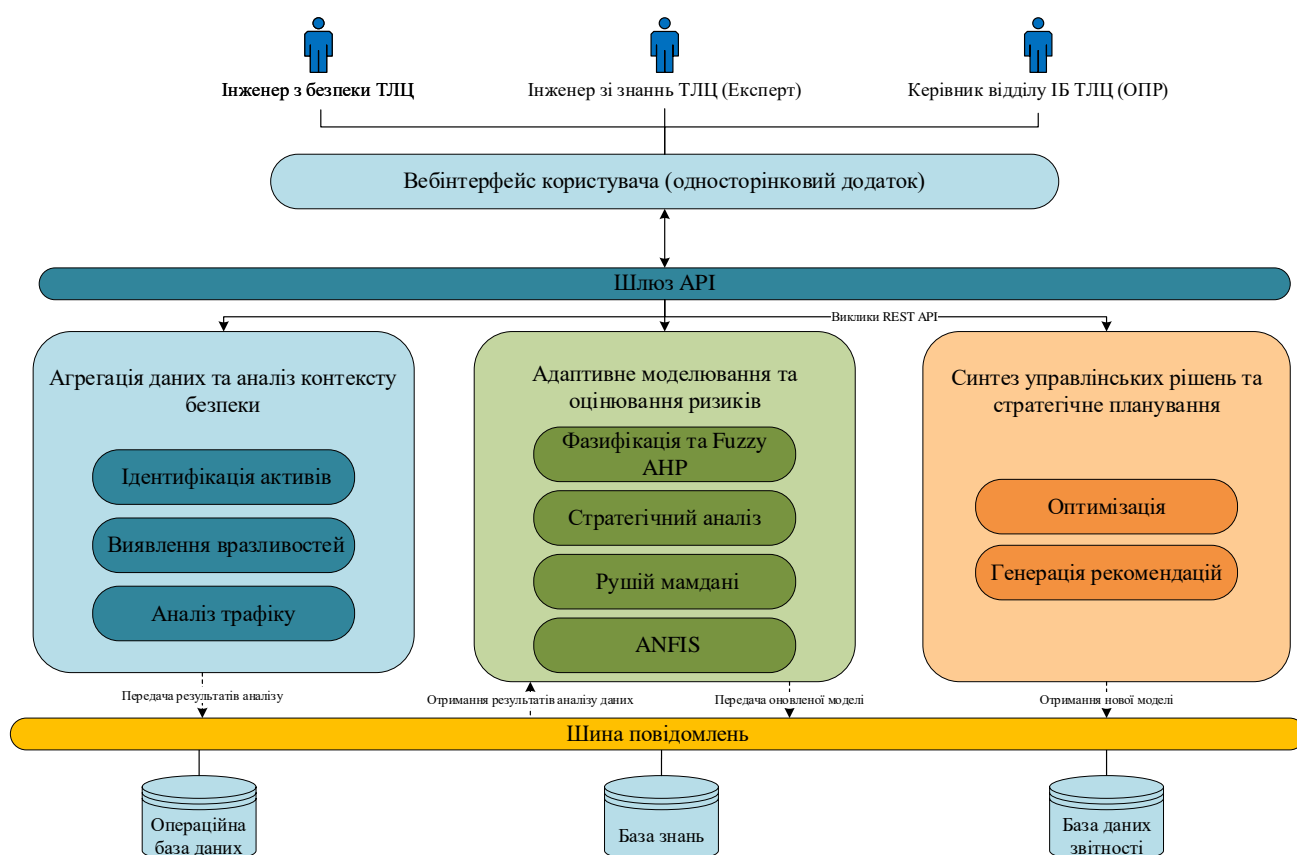


Рисунок 3.10 – Чотирирівнева багатокomпонентна сервіс-орієнтована архітектура ІТ ППР

Функціональний розподіл системи реалізовано за наступною ієрархією рівнів:

*Рівень 1.* Інтерфейси користувача. Реалізований у вигляді односторінкового вебзастосунка (SPA – Single Page Application). Взаємодія користувачів із системою регламентується моделлю керування доступом на основі ролей (RBAC), що визначає доступний набір інструментів для кожного актора:

- інженер з безпеки здійснює первинний збір даних, ідентифікацію активів та моніторинг поточної телеметрії;

- інженер зі знань (експерт) забезпечує формалізацію експертних оцінок, налаштування лінгвістичних змінних, верифікацію продукційних правил та контроль навчання ANFIS-моделі;
- ОПР (керівник) виконує аналіз ландшафту ризиків, оцінювання результатів оптимізації та вибір стратегій захисту через аналітичні панелі.

*Рівень 2.* Інтеграційний рівень. Центральний компонент рівня API Gateway, який виконує роль єдиної точки входу (Single Point of Entry). Він забезпечує маршрутизацію запитів до відповідних сервісів, автентифікацію та авторизацію сесій, балансування навантаження між екземплярами сервісів бізнес-логіки.

*Рівень 3.* Рівень бізнес-логіки. На цьому рівні зосереджена алгоритмічна складова ІТ, розділена на три функціональні сервіси:

1. Сервіс «Агрегація даних та аналіз контексту безпеки» забезпечує автоматизований збір даних із CMDB, кореляцію вразливостей (CVE) та первинну статистичну обробку телеметрії.

2. Сервіс «Адаптивне моделювання та оцінювання ризиків». Це інтелектуальне ядро системи, що реалізує дворівневу схему аналізу для мінімізації обчислювальних витрат і вирішення проблеми «холодного старту». Функціональний цикл оцінювання складається з двох послідовних етапів:

1). Етап стратегічного аналізу (експертна оцінка) – забезпечує попередню обробку даних для зниження обчислювального навантаження на систему шляхом відсіювання несуттєвих подій. Включає наступні компоненти:

- фазифікація та Fuzzy АНР. Забезпечує перетворення вхідних чітких метрик у лінгвістичні змінні та розрахунок нормалізованих ваг загроз на основі матриць парних порівнянь;
- стратегічний аналіз (фільтрація). Виконує селекцію факторів ризику за матрицею Дж. Х. Вілсона (вплив; впевненість) для виділення пріоритетних загроз перед початком ресурсомісткого моделювання.

2). Етап моделювання забезпечує поглиблену оцінку відібраних критичних загроз. Реалізує двофазний алгоритм для вирішення проблеми «холодного

старту» (відсутності історичних даних на етапі впровадження):

- рушій Мамдані (експертна фаза) генерує синтетичні еталони на основі продукційних правил та механізму логічного виведення (алгоритм Rete). Це дозволяє системі функціонувати як експертній та надавати валідні оцінки ризиків з моменту запуску, ще до накопичення статистики;
- ANFIS при накопиченні достатнього обсягу даних автоматично активується неймережеве донавчання моделі. Цей компонент коригує параметри функцій належності на основі реальної статистики інцидентів, забезпечуючи мінімізацію похибки прогнозування в процесі експлуатації.

3. Сервіс «Синтез управлінських рішень та стратегічне планування» містить наступні складові:

- оптимізація (пошук вектора захисних заходів, що мінімізує функціонал ризику при заданих бюджетних обмеженнях);
- генерація рекомендацій (формування автоматизованих звітів та планів реагування).

*Рівень 4. Рівень даних.* Ефективне управління різномірною інформацією забезпечується впровадженням концепції поліглотної персистентності. Відповідно до цього, збереження даних розділено на три цільові сегменти:

1. Operational DB (Time-series). Відповідає за зберігання високочастотних часових рядів подій безпеки та телеметрії активів. Як технологічне рішення обрано TimescaleDB, що дозволяє ефективно обробляти потоки даних від IoT-сенсорів та систем моніторингу в реальному часі (рис. 3.11).

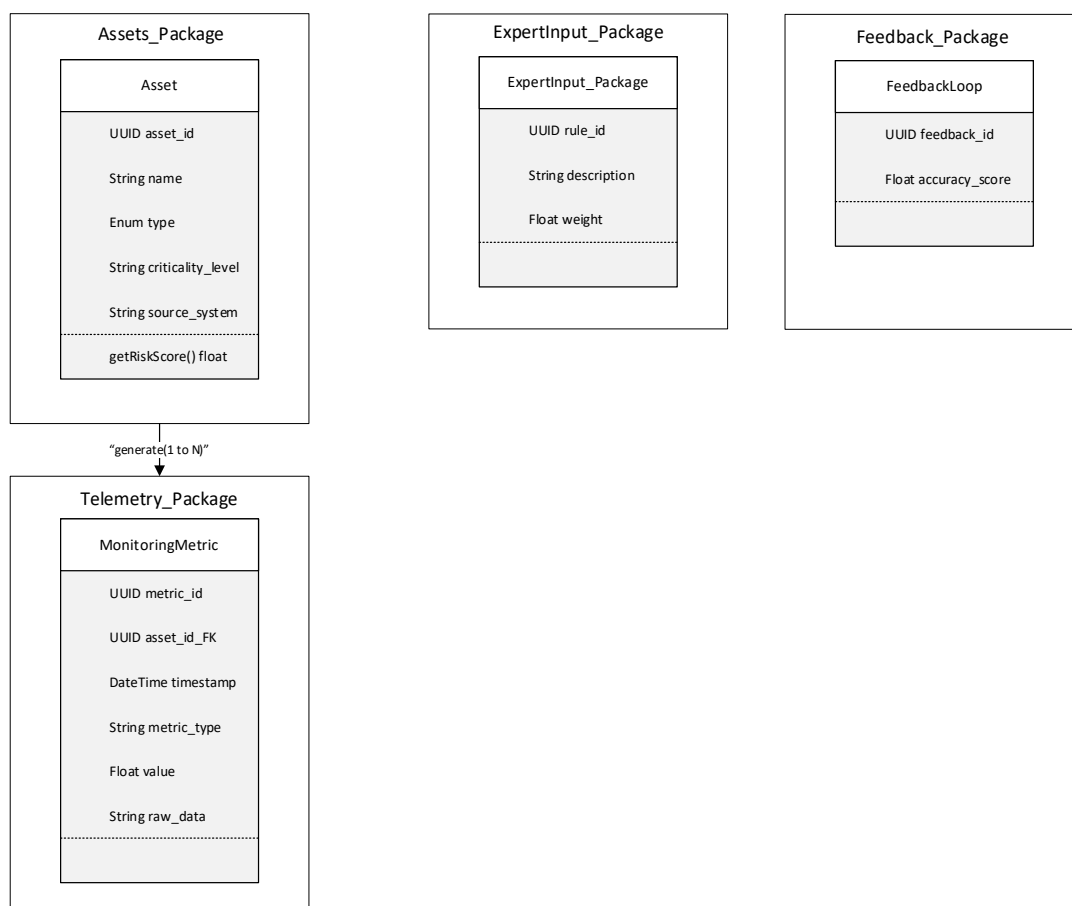


Рисунок 3.11 – Логічна модель операційної бази даних

2. Knowledge Base (Graph + Relational). Це комбіноване сховище для моделювання складної топології активів та зберігання правил нечіткої логіки.

Neo4j (Graph DB) використовується для моделювання зв'язків між активами ТЛЦ, загрозами та вразливостями, що критично для аналізу ланцюгових реакцій при кібератаках.

PostgreSQL (Relational) зберігає структуровані правила нечіткої логіки, лінгвістичні змінні та параметри функцій належності (рис. 3.12).



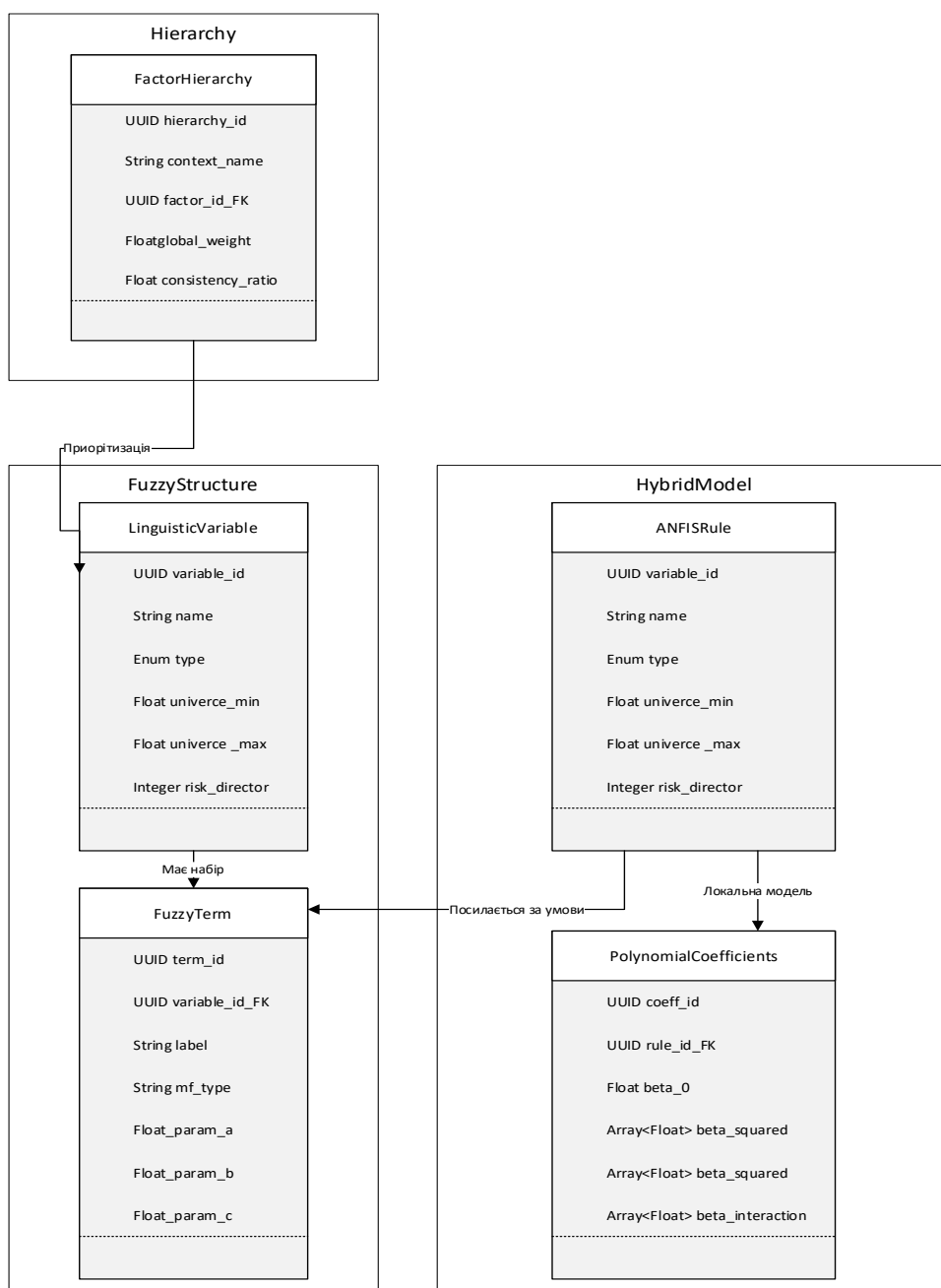


Рисунок 3.12 – Логічна структура бази знань

3. Reporting DB (Document-oriented). Призначена для архівування неструктурованих звітів, історії рішень та навчальних вибірок. Використання MongoDB дозволяє гнучко зберігати JSON-документи стратегічних звітів та історію оцінювання ризиків без жорсткої схеми даних (рис. 3.13).

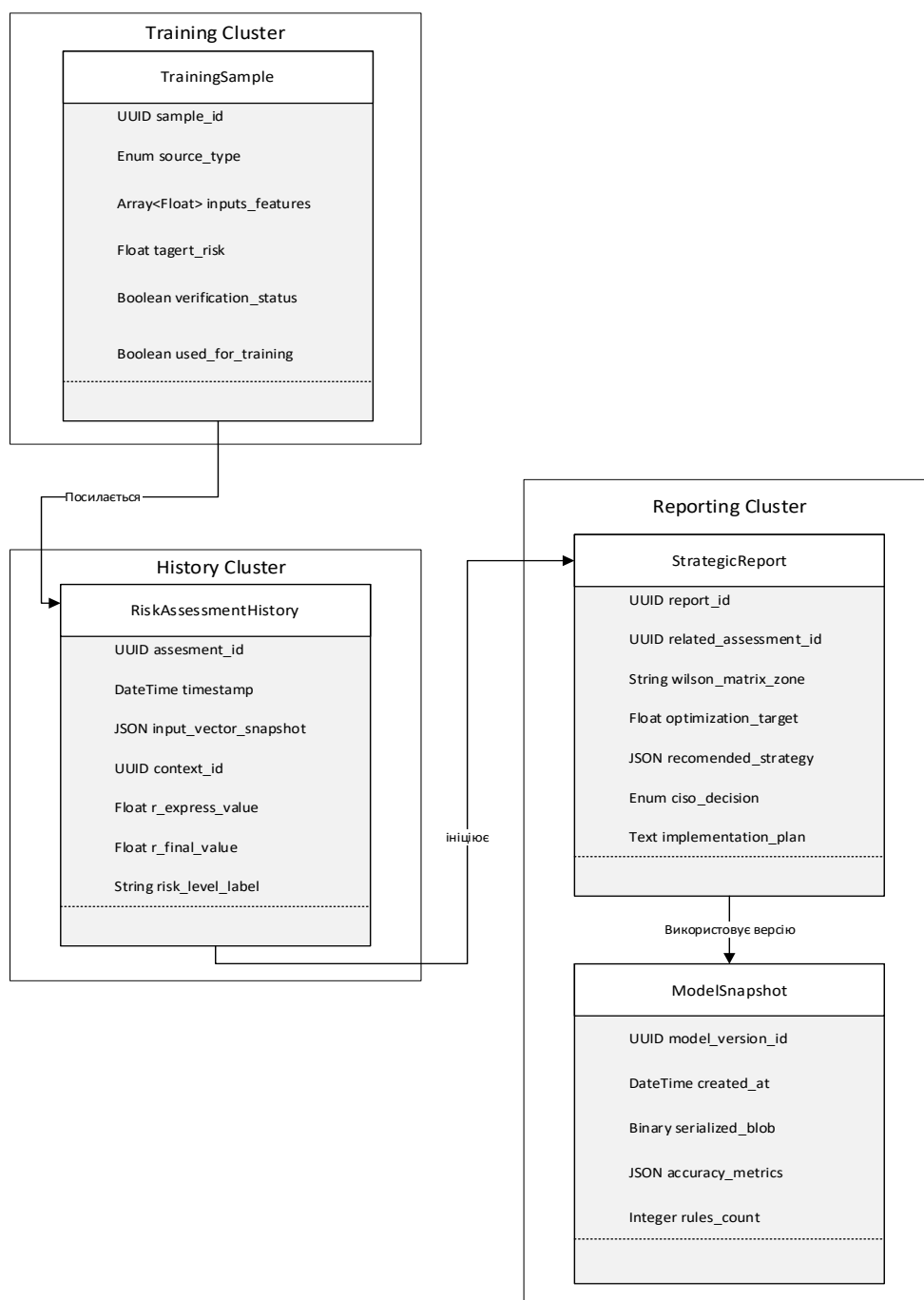


Рисунок 3.13 – Логічна структура аналітичної бази даних

Для забезпечення цілісного розуміння взаємодії між описаними рівнями логіки (рівень 3) та даними (рівень 4), загальна схема інформаційних потоків у системі наведена на рисунку 3.14.

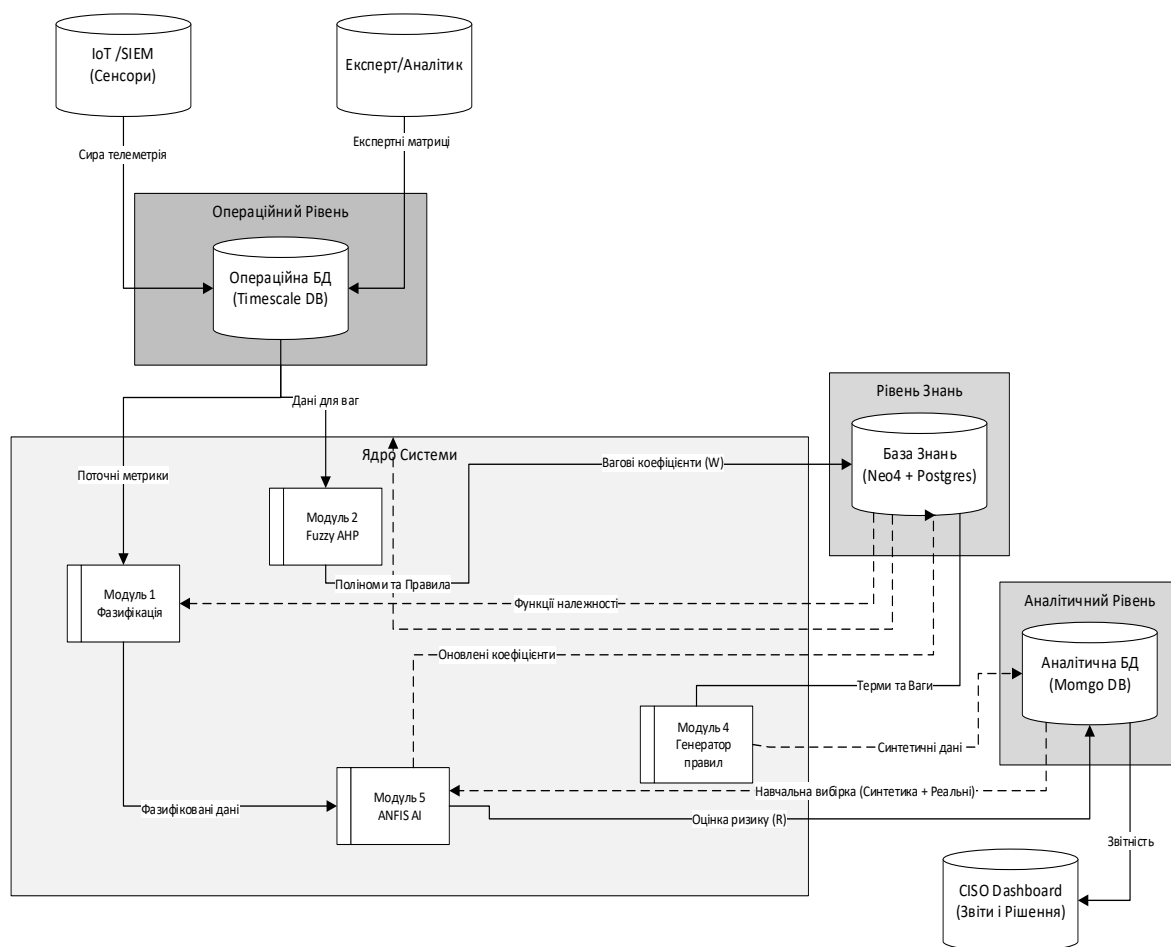


Рисунок 3.14 – Схема взаємодії компонентів системи та потоків даних

Для забезпечення технологічної незалежності та оперативного розгортання в умовах різномірної інфраструктури ТЛЦ, архітектурне рішення передбачає контейнеризацію всіх програмних компонентів на базі Docker. Використання даної технології гарантує розгортання СППР як на локальних серверах ТЛЦ, так і у хмарному середовищі з мінімальними витратами на конфігурацію.

### 3.4 Програмна реалізація компонентів інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ

Реалізація бізнес-логіки системи (рівень 3 архітектури) виконана мовою програмування Python з використанням бібліотек для наукових обчислень (NumPy, Pandas, SymPy) та машинного навчання (PyTorch). Статична структура

програмного комплексу, що відображає ієрархію класів, їхні атрибути та методи, наведена на діаграмі класів (Додаток Д).

Програмна реалізація декомпонована на три ключові функціональні блоки.

1. Блок *«Агрегація даних та аналіз контексту безпеки»*. Програмна реалізація даного блоку спрямована на формування вхідного вектора ознак для інтелектуального ядра СППР. Оскільки методи детекції аномалій базуються на раніше розробленому математичному апараті, у межах даної ІТ цей блок функціонує як сервіс збору та первинної обробки гетерогенних даних.

Логіка його роботи базується на інтеграції декількох спеціалізованих інструментів аналізу. Зокрема, для ідентифікації прихованих закономірностей у мережеских потоках ТЛЦ використовується фрактальний детектор трафіка, алгоритмічна база якого детально описана в [90]. Це дозволяє ідентифікувати аномальну активність на ранніх стадіях через аналіз локальної самоподібності трафіку, що суттєво підвищує чутливість загальної моделі до складних кіберзагроз.

Додатково в сервісі реалізовано моніторинг поведінкових факторів [91]. Даний інструмент забезпечує комплексний захист від цільових атак, які не мають виражених технічних аномалій, але проявляються через нетипові патерни дій суб'єктів системи.

Для оцінювання статистичної стабільності інфраструктури програмно реалізовано обчислення показника Херста [16]. Розрахунок виконується в режимі реального часу за методом R/S-аналізу, що дозволяє виявляти стан довготривалої залежності в трафіку як ознаку потенційного інциденту.

У результаті функціонування даного блоку, сирі дані від систем моніторингу та IoT-сенсорів трансформуються у нормалізований JSON-об'єкт. Він містить значення ключових факторів  $(x_1, \dots, x_n)$ , які через шину повідомлень передаються до інтелектуального ядра (ANFIS) для прийняття управлінських рішень. Таким чином, блок агрегації забезпечує високу якість вхідних знань при мінімальному обчислювальному навантаженні на основні модулі системи.

2. Блок «Адаптивне моделювання та оцінювання ризиків» є інтелектуальним центром системи, що забезпечує перетворення експертних знань у математичну модель та її подальшу адаптацію. Програмна реалізація блоку розділена на дві підсистеми.

2.1. Підсистема стратегічного аналізу (експертна оцінка). Дана підсистема відповідає за первинну формалізацію знань та пріоритезацію факторів. Вона включає: модуль фазифікації, модуль Fuzzy АНР, модуль стратегічного аналізу та модуль обчислення оцінки ризику.

2.1.1. Модуль фазифікації вхідних та вихідних факторів призначений для визначення вхідних та вихідних лінгвістичних змінних, їх універсумів та відповідних функцій належності. Це базовий підмодуль, який може бути використаний для генерації правил, фазифікації даних та обчислення інтегрального показника ризику.

Метою модуля є формалізація експертних знань шляхом визначення наборів лінгвістичних термів для кожного фактора та параметричного опису відповідних функцій належності. Модуль забезпечує автоматичне формування структури антецедентів (вхідних факторів) та консеквента (вихідного фактора) для подальшої генерації бази правил Мамдані. Параметри функцій належності та межі універсальних множин завантажуються як зовнішні конфігураційні дані, що забезпечує гнучкість моделі та можливість її динамічної адаптації під мінливі умови функціонування ТЛЦ. Вихідні параметри:

1. `Antecedents (x1-x6)` – шість об'єктів типу `ctrl.Antecedent`, кожен із яких містить універсум (0...1), набір лінгвістичних змінних та відповідні трикутні функції належності;
2. `Consequent (R_risk)` – об'єкт типу `ctrl.Consequent`, що містить універсум та набір термів ризику (L, M, H, VH);
3. `Confidence antecedent` – об'єкт типу `ctrl.Antecedent` із визначеними термами рівня впевненості.

Нижче подано детальний опис складових модуля Fuzzification, який

забезпечує визначення семантики кожного фактору, побудову трикутних функцій належності для всіх термів, задання стандартної нечіткої структури відповідно до методології Мамдані. Таблиця 3.2 узагальнює ключові елементи коду, їх тип та функціональне призначення.

Таблиця 3.2 – Опис елементів модуля фазифікації: класів, методів та атрибутів вхідних та вихідних факторів.

Елемент коду	Тип	Детальне призначення та опис реалізації
<code>skfuzzy.control</code>	Бібліотека класів	Частина бібліотеки SciKit-Fuzzy, що забезпечує реалізацію компонентів системи нечіткого логічного виведення: антецедентів, консеквентів, контролерів та правил.
<code>Universe</code>	Масив NumPy	Універсум значень від 0 до 1 з кроком 0.01. Використовується для всіх лінгвістичних змінних системи.
<code>x1_asset, x2_threat, x3_damage, x4_control, x5_costs, x6_culture</code>	Клас <code>ctrl.Antecedent</code>	Визначає вхідний фактор системи. Є контейнером для лінгвістичних термів.
<code>R_risk</code>	Клас <code>ctrl.Consequent</code>	Визначає вихідний фактор системи. Є контейнером для його термів.
<code>fuzz.trimf</code>	Функція	Побудова трикутних функцій належності для кожного терму. Кожна функція задає форму нечіткої множини у межах універсуму. Визначає ступінь з яким конкретні значення фактора належать термам.
<code>setup_fuzzy_system</code>	Метод	Створює всі вхідні антецеденти та вихідний консеквент ризику. Викликає метод побудови функцій належності факторів.
<code>setup_membership_functions</code>	Метод	Формує трикутні функції належності
<code>setup_factor_parameters</code>	Метод	Задає список факторів і

Елемент коду	Тип	Детальне призначення та опис реалізації
		визначає які з них збільшують ризик, а які зменшують
get_antecedent	Метод	Повертає об'єкт <code>ctrl.Antecedent</code> за назвою фактора.
get_confidence_antecedent	Метод	Повертає нечітку змінну впевненості експертів.
linguistic_to_fuzzy	Метод	Конвертує лінгвістичний терм фактора у параметри відповідної функції належності.
confidence_to_fuzzy	Метод	Конвертує лінгвістичний терм рівня впевненості у параметри відповідної функції належності.
_get_fuzzy_triangle	Метод	Обчислює трикутне нечітке число, визначаючи ліву межу, ядро та праву межу на основі параметрів трикутної функції належності.
crisp_to_fuzzy	Метод	Автоматично знаходить лінгвістичний терм для чіткого вхідного значення фактора та повертає параметри його функції належності.
crisp_confidence_to_fuzzy	Метод	Автоматично знаходить лінгвістичний терм для чіткого значення впевненості та повертає параметри його функції належності.
Defuzzify	Метод	Виконує дефазифікацію через метод центроїда та повертає чітке значення ризику.
interpret_risk_level	Метод	Перетворює чітке значення ризику на лінгвістичний рівень.

Код модуля наведений в Додатку Е лістинг Е.1.

2.1.2. Модуль визначення нечітких вагових коефіцієнтів реалізує процедуру визначення вагових коефіцієнтів факторів ІБ на основі методу Fuzzy АНР. На

відміну від класичного АНР, нечітка модифікація дозволяє враховувати лінгвістичну невизначеність та нечіткість експертних оцінок, подаючи їх у вигляді трикутних нечітких чисел.

Метою модуля є формування нечіткої матриці парних порівнянь, перевірка її узгодженості та обчислення фінальних ваг факторів.

Вхідні параметри:

1. `factors` – список ідентифікаторів факторів;
2. `fuzzy_scale` (опціонально) – словник, що визначає відповідність лінгвістичних оцінок експертів трикутним нечітким числам.

Вихідні параметри:

1. `fuzzy_matrix` – тривимірна матриця із трикутними нечіткими числами;
2. `CR` – числове значення індексу узгодженості;
3. `is_consistent` – булевий показник прийнятності матриці;
4. `weights` – словник із фінальними вагами факторів після дефазифікації та нормалізації.

Модуль забезпечує:

- формування нечіткої матриці парних порівнянь за експертними оцінками;
- побудову обернених трикутних чисел для зворотних порівнянь;
- перевірку узгодженості матриці;
- обчислення нечітких сум для кожного фактору;
- визначення ступеня домінування за допомогою функції можливості;
- отримання фінальних ваг.

Таблиця 3.3 узагальнює ключові елементи коду, їх тип та функціональне призначення.

Таблиця 3.3 – Опис елементів модуля визначення нечітких вагових коефіцієнтів: класів, методів та атрибутів.

Елемент коду	Тип	Детальне призначення та опис реалізації
--------------	-----	---



FuzzyAHP	Клас	Основний клас, що реалізує всі етапи нечіткого аналізу ієрархій. Зберігає фактори, нечітку шкалу, RI-коефіцієнти та методи обчислення ваг.
factors	Атрибут екземпляра	Список назв факторів, що розглядаються в моделі.
FUZZY_SCALE	Атрибут екземпляра	Словник лінгвістичних оцінок та їх трикутних чисел.
RI	Атрибут екземпляра	Таблиця випадкової узгодженості Сааті (Random Index) для розрахунку CR.
N	Атрибут екземпляра	Кількість факторів.
build_fuzzy_matrix	Метод	Створює нечітку матрицю парних порівнянь на основі експертних оцінок. Автоматично генерує обернені трикутні числа для зворотних елементів матриці.
check_consistency	Метод	Обчислює відношення узгодженості (CR) на основі чіткої матриці (медіан нечітких чисел). Повертає CR та булеву оцінку ( $CR < 0.1$ ).
calculate_weights	Метод	Обчислює ваги факторів. Знаходить суму нечітких чисел, нормалізація, обчислення ступеня можливості домінування, регуляризація та нормалізація до 1.
degree_of_possibility	Функція	Обчислює ступінь, з яким одне нечітке число є більшим за інше.

Код модуля наведений в Додатку Е лістинг Е.2.

2.1.3. Модуль стратегічного аналізу (удосконалена матриця Дж. Х. Вілсона) призначений для графічного представлення експертних оцінок факторів ризику у вигляді матриці Вілсона. Він дозволяє одночасно враховувати вплив фактору та впевненість експерта. Така візуалізація використовується для розмежування факторів на загрози та можливості, визначення їхньої пріоритетності та інтенсивності впливу.

Модуль використовується як допоміжний інструмент для експертного аналізу, документування оцінок та презентації результатів у складі загальної методики оцінювання ризику ІБ ТЛЦ.

Вхідні параметри:

1. `factors_data` – словник зі значеннями факторів та оцінками впевненості експертів.

Вихідні результати:

1. графік матриці Вільсона;
2. точки факторів – автоматично нанесені на графік відповідно до їхнього типу (загроза/можливість), інтенсивності та впевненості.

Модуль `WilsonMatrix` виконує роль візуального аналітичного інструменту, що дозволяє:

- виявляти фактори, які становлять найбільшу загрозу (зони At–Bt);
- ідентифікувати потенційні можливості (зони Ao–Bo);
- аналізувати рівень впевненості експертів, що супроводжує кожную оцінку;
- проводити порівняльний аналіз впливу різних факторів моделі ризику;
- графічно представляти результати.

Таблиця 3.4 узагальнює ключові елементи коду, їх тип та функціональне призначення.

Таблиця 3.4 – Опис елементів модуля стратегічного аналізу: класів, методів та атрибутів.

Елемент коду	Тип	Детальне призначення та опис реалізації
<code>WilsonMatrix</code>	Клас	Основний клас, що відповідає за створення Матриці Вільсона, побудову зон, сітки, підписів та нанесення факторів.
<code>setup_axes</code>	Метод	Встановлює межі осей (X: [-1, 1], Y: [0, 1]), базові лінії координат, підписи осей.
<code>setup_grid_lines</code>	Метод	Генерує вертикальні та горизонтальні

Елемент коду	Тип	Детальне призначення та опис реалізації
		допоміжні лінії.
setup_zones	Метод	Створює прямокутні зони Матриці Вільсона: загрози (Dt, Ct, Bt, At) та можливості (Do, Co, Bo, Ao). Кожна зона має власний колір і назву, яка додається на графік.
setup_labels	Метод	Додає текстові підписи. Забезпечує логічну структуру навігації по матриці.
add_factor_point	Метод	Додає точку фактору на матрицю.
add_all_factors	Метод	Автоматично додає всі шість стандартних факторів моделі.

Код модуля наведений в Додатку Е лістинг Е.3.

2.1.4. Модуль обчислення оцінки ризику реалізує процедуру обчислення експертної нечіткої інтегральної оцінки рівня ризику ІБ ТЛЦ. Підхід ґрунтується на використанні нечітких чисел факторів та коефіцієнтів впевненості, вагових коефіцієнтів, операцій нечіткої арифметики, дефазифікації та інтерпретації ризику.

Метою модуля є формування повної нечіткої оцінки ризику, а також перетворення її на чітку оцінку та відповідний терм.

Вхідні параметри:

1. `factor_values` – словник значень факторів (у вигляді лінгвістичних термів або чисел);
2. `confidence_levels` – словник рівнів впевненості експертів;
3. `weights` – словник вагових коефіцієнтів факторів.

Вихідні параметри:

1. `fuzzy_integral` – інтегральна оцінка ризику, як нечітке число;
2. `crisp_risk` – дефазифікована оцінка ризику;
3. `risk_level` – лінгвістична оцінка ризику.

Таблиця 3.5 узагальнює ключові елементи коду, їх тип та функціональне

призначення.

Таблиця 3.5 – Опис елементів модуля обчислення оцінки ризику: класів, методів та атрибутів.

Елемент коду	Тип	Детальне призначення та опис реалізації
<code>fuzzy_multiply</code>	Метод	Множення двох трикутних нечітких чисел.
<code>fuzzy_add</code>	Метод	Додавання нечітких трикутних чисел.
<code>fuzzy_negate</code>	Метод	Інверсія нечіткого числа ( $1 - x$ ), використовується для негативних факторів.
<code>fuzzy_product</code>	Метод	Реалізує множення рівня впевненості експерта на значення фактора.
<code>parse_input_value</code>	Метод	Перетворює значення факторів (число або лінгвістичний терм) у нечітке число.
<code>parse_confidence_value</code>	Метод	Перетворює значення впевненості у нечітке трикутне число.
<code>multiply_confidence_factor</code>	Метод	Обчислення множення рівня впевненості експерта на значення всіх факторів.
<code>calculate_risk</code>	Метод	Фінальне обчислення ризику.

Повний програмний код реалізації даного модуля наведено у Додатку Е лістинг Е.4.

2.2. Підсистема моделювання забезпечує поглиблену оцінку та самонавчання системи, вирішуючи проблему «холодного старту». Утримує модуль генерації еталонної бази знань та Rete-оптимізація; модуль трансформації бази правил до Rete-мережі; модуль ANFIS.

2.2.1. Модуль автоматизованої генерації бази правил (Mamdani Generator). Першим етапом роботи системи є вирішення проблеми «холодного старту» шляхом автоматичного формування експертної БЗ. Модуль розроблений для автоматизації процесу створення повної бази нечітких правил типу Мамдані, яка

виконує роль стартової моделі. За відсутності реальних статистичних даних на початковому етапі експлуатації в ТЛЦ така база описує всі можливі взаємозв'язки між вхідними факторами ( $x_1, \dots, x_6$ ) на основі їх термів, вагових коефіцієнтів і напрямку впливу на ризик.

Вхідні дані:

1. `terms (dict)` – набір лінгвістичних термів для кожного фактора (наприклад: VL, L, M, H, VH) та їх числових центроїдів;
2. `weights (dict)` – вектор вагових коефіцієнтів факторів, що відображає їх важливість для активу;
3. `risk_reducing (set)` – множина факторів з оберненим впливом (збільшення значення яких зменшує ризик);
4. `expert_rules (csv, опціонально)` – набір правил від експертів для верифікації точності генерації.

Вихідні дані:

1. `rules (list[dict])` – сформована база знань у вигляді списку об'єктів, де кожен містить антецедент (умови) та консеквент (розрахований ризик  $R$  і його клас);
2. `rules_full.csv` – фізичний файл експорту бази знань для збереження на диску.

На рисунку 3.15 представлена схема роботи методів класу MamdaniRuleBaseGenerator, яка ілюструє логіку взаємодії його складових [127].

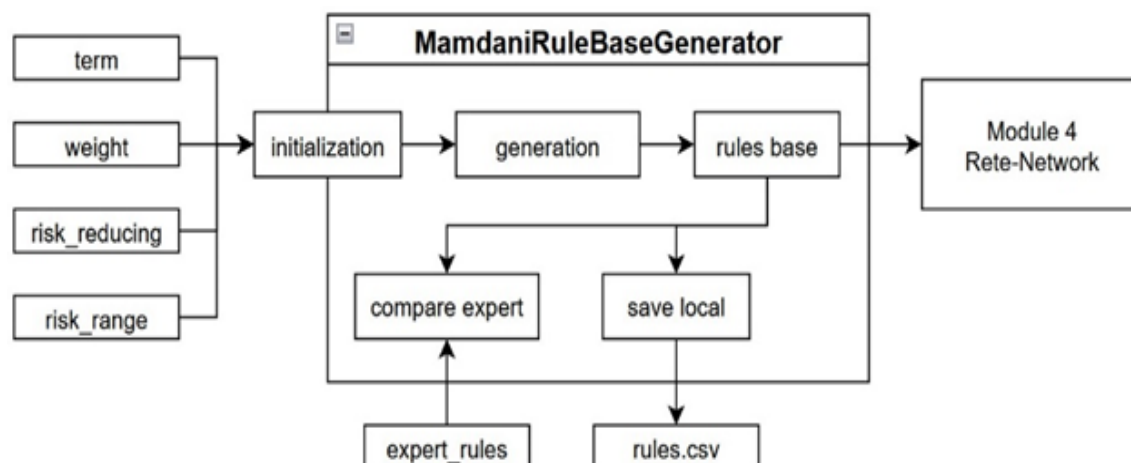


Рисунок 3.15 – Схема роботи модуля генерації бази правил

Основні елементи програмної реалізації модуля та їх призначення наведені в таблиці 3.6.

Таблиця 3.6 – Опис елементів модуля генерації правил: класів, методів та атрибутів

Елемент коду	Тип	Детальне призначення та опис реалізації
MamdaniRuleBaseGenerator	Клас	Генерує повну базу нечітких правил типу Мамдані на основі вхідних параметрів. Містить повний цикл методів для генерації, збереження, перевірки.
DEFAULT_TERMS	Атрибут класу	Стандартний набір термів для шести вхідних факторів (x1–x6). Кожен фактор має словник лінгвістичних значень (“VL”, “L”, “M”, “H”, “VH”) та їх числових представлень.
DEFAULT_WEIGHTS	Атрибут класу	Словник базових ваг факторів ризику, які використовуються при обчисленні інтегрального ризикового індексу.
DEFAULT_RISK_REDUCEING	Атрибут класу	Множина факторів, для яких високі значення зменшують загальний ризик (обернений вплив).
__init__	Метод	Ініціалізує терми, ваги та множину «risk reducing» факторів. Формує список назв факторів і порожній список правил. Викорисовує значення за замовчуванням, якщо вони не визначені при виклику.
classify_risk	Статичний метод	Класифікує ризиковий індекс r_index у лінгвістичний рівень (“L”, “M”, “H”, “VH”). Пороги визначаються фіксованими межами.
generate_rules	Метод	Метод генерації бази правил. Перебирає всі комбінації термів за допомогою itertools.product. Для кожної комбінації обчислює ризиковий індекс з урахуванням ваг і напрямку впливу факторів, класифікує результат, і формує список правил.
save_local	Метод	Зберігає згенеровані правила у CSV-файл і записує дані з полями факторів, R_index та R.

Елемент коду	Тип	Детальне призначення та опис реалізації
<code>compare_with_expert</code>	Метод	Порівнює автоматично згенеровану базу правил з експертною таблицею (CSV). Об'єднує обидві таблиці для аналізу збігів та обрахунку точності генерації.
<code>terms,</code> <code>risk_reducing</code> <code>weights,</code>	Атрибут екземпляра	Конфігураційні параметри генератора: терми для кожного фактору, вагові коефіцієнти та множина факторів з оберненим впливом.
<code>rules</code>	Атрибут екземпляра	Зберігає поточну згенеровану базу правил у вигляді списку словників.
<code>factor_names</code>	Атрибут екземпляра	Список ідентифікаторів усіх факторів, упорядкований згідно з визначеними термами.

Повний програмний код реалізації даного модуля наведено у Додатку Е, лістинг Е.5.

2.2.2. Модуль трансформації бази правил до Rete-мережі та оптимізації логічного виведення. На відміну від класичного підходу, який виконує послідовну перевірку кожного правила, Rete-архітектура дозволяє багаторазово використовувати спільні умови, мінімізуючи повторні обчислення.

У межах загальної системи модуль виступає еталонною моделлю («вчителем»), що формує навчальну вибірку для нейромережевого компонента.

Вхідні дані:

1. `rules_data` (`DataFrame` | `list`) – повна база нечітких правил, отримана від модуля генерації;
2. `fact` (`dict`) – вхідний вектор поточного стану активу (набір значень термів) для пошуку відповідних правил.

Вихідні дані:

1. `ReteNetwork` (`object structure`) – граф об'єктів у пам'яті (`AlphaNode` → `BetaNode` → `OutputNode`), підготовлений для логічного виведення;

2. `activated_rules (list)` – список правил, умови яких задовольняють вхідному факту.

Логіка роботи Rete-мережі відображена на рисунку 3.16.

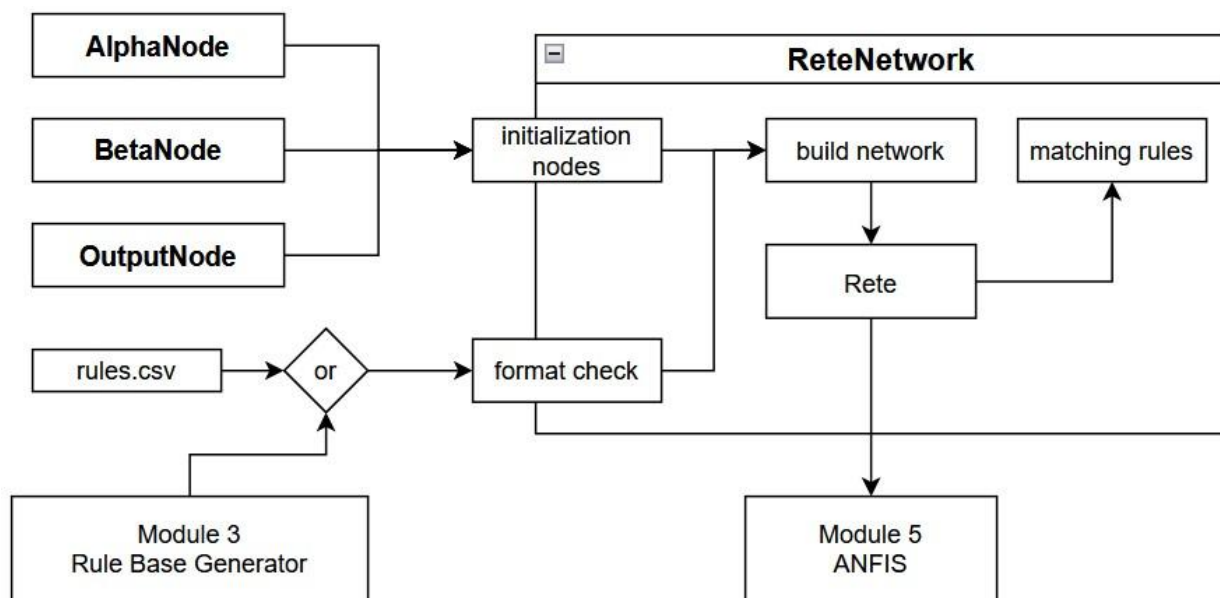


Рисунок 3.16 – Схема функціонування модуля трансформації та логічного виведення на базі Rete-мережі

Програмна реалізація базується на об'єктно-орієнтованому підході, де кожен вузол мережі є окремим об'єктом. Опис основних класів наведено в таблиці 3.7.

Таблиця 3.7 – Опис класів реалізації Rete-мережі: класів, методів та атрибутів

Елемент коду	Тип	Призначення та опис реалізації
<code>FuzzyReteNode</code>	Клас	Батьківський клас для всіх типів вузлів. Містить список вихідних вузлів <code>output_nodes</code> і метод для з'єднання з ними.
<code>connect</code>	Метод	Створює з'єднання між поточним вузлом і переданим об'єктом типу <code>FuzzyReteNode</code> , додаючи його до списку <code>output_nodes</code> .
<code>AlphaNode</code>	Клас	Вузол верхнього рівня мережі Rete, який відповідає за перевірку умов по окремих факторах (наприклад, $x_1 = H$ ). При активації перевіряє факт і передає сигнал далі у відповідні $\beta$ -вузли.
<code>activate (AlphaNode)</code>	Метод	Отримує факт і активує зв'язані вузли,



Елемент коду	Тип	Призначення та опис реалізації
		якщо значення фактора збігається з термом, закріпленим за вузлом.
BetaNode	Клас	Вузол, що реалізує логіку об'єднання кількох умов (AND) і формування наслідку. Зберігає набір умов (conditions), результат правила (R) та індекс ризику (R_index). Після активації всіх умов передає результат до вихідного вузла.
activate (BetaNode)	Метод	Позначає виконання окремої умови правила. Коли всі умови задовольняються, активує вихідний вузол.
reset (BetaNode)	Метод	Скидає стан виконаних умов (matched_conditions), готуючи вузол до обробки нового факту.
OutputNode	Клас	Вихідний вузол мережі. Збирає активовані правила після проходження факту через мережу.
activate (OutputNode)	Метод	Додає результат (R) активованого правила до списку activated_rules.
reset (OutputNode)	Метод	Очищує список активованих правил перед новим запуском.
ReteNetwork	Клас	Центральний клас, який формує повну мережу Rete з набору правил. Створює та з'єднує $\alpha$ - та $\beta$ -вузли, а також реалізує механізм запуску фактів.
init (ReteNetwork)	Метод	Ініціалізує структуру мережі: створює вузли $\alpha$ та $\beta$ на основі переданих правил (DataFrame або список словників). Забезпечує з'єднання між вузлами і підключення вихідного вузла.
run_fact	Метод	Запускає обробку факту та повертає список активованих правил.
alpha_nodes, beta_nodes, output_node	Атрибути екземпляра	Зберігають структуру мережі: $\alpha$ -вузли (умови), $\beta$ -вузли (правила) та вихідний вузол, що збирає результати.

Повний програмний код реалізації Rete-мережі наведено у Додатку Е лістинг Е.6.

2.2.3. Модуль ANFIS («Учень») є ключовим елементом інтелектуальності системи, що функціонує як універсальний апроксиматор. Архітектура моделі відповідає мережі Такагі-Сугено-Канга (TSK) другого ступеня. Це дозволяє системі не лише оцінювати ризики, а й навчатися на нових даних, коригуючи вагові коефіцієнти правил.

Для кожного нечіткого правила  $k$  обчислюється локальний поліноміальний висновок:  $z_k = f_k(x) = c_{k0} + \sum_{i=1}^6 c_{ki} \cdot x_i + \sum_{i=1}^6 c_{kii} \cdot x_i^2 + \sum_{1 \leq i < j \leq 6} c_{ij} \cdot x_i \cdot x_j$ .

Процес навчання включає етап редукції моделі – автоматичного відключення («заморожування») статистично незначущих коефіцієнтів для запобігання перенавчанню. Схема функціонування модуля наведена на рисунку 3.17.

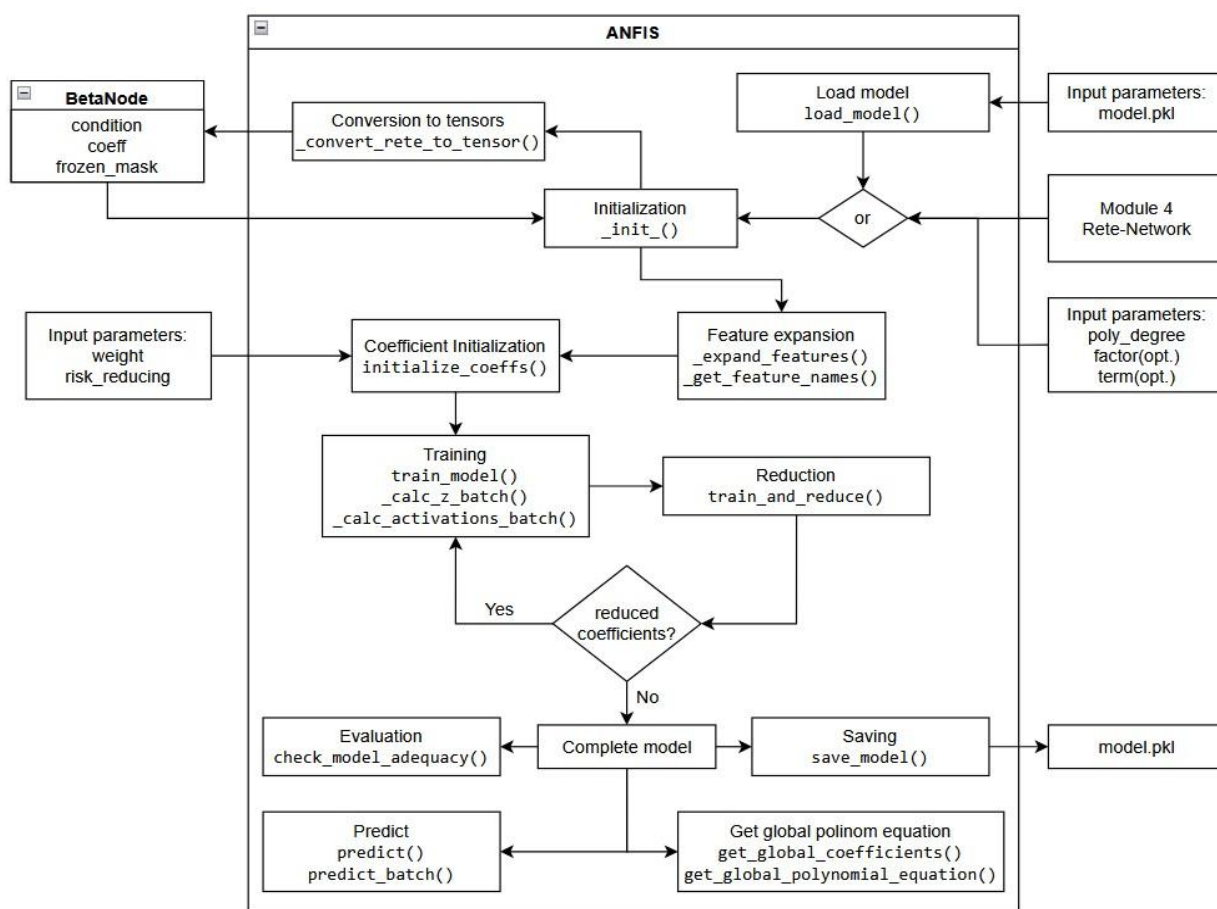


Рисунок 3.17 – Архітектура та схема роботи ANFIS модуля

Реалізація виконана з використанням фреймворку PyTorch, що забезпечує використання GPU для прискорення навчання. Ключові методи описані в таблиці 3.8.

Таблиця 3.8 – Опис класів реалізації роботи ANFIS модуля: класів, методів та атрибутів

Елемент коду	Тип	Детальне призначення та опис реалізації
BetaNode	Клас	Представляє окреме нечітке правило у вигляді параметричної моделі. Містить коефіцієнти полінома, маску «заморожених» ваг (для редукції) та умови активації.
conditions	Атрибут екземпляра	Словник числових значень термів для поточного правила.
poly_degree	Атрибут екземпляра	Ступінь полінома у лінійній частині моделі (1 – лінійна, 2 – з квадратами та перехресними членами)
frozen_mask	Тензор (Атрибут)	Маска, яка визначає активні/заморожені коефіцієнти при скороченні моделі.
activation	Атрибут	Поточне значення активації правила.
ANFIS	Клас	Основний клас адаптивної нечіткої нейромережі типу ANFIS, що навчається на базі правил Rete-мережі. Забезпечує ініціалізацію, навчання, редукцію та оцінку адекватності моделі.
DEFAULT_FACTORS	Атрибут класу	Базовий перелік входних факторів ( $x_1$ – $x_6$ ).
DEFAULT_TERMS	Атрибут класу	Базовий набір числових представлень лінгвістичних термів для кожного фактора.
__init__	Метод	Ініціалізує структуру мережі, створює набір правил BetaNode, формує навчальні вибірки з Rete-мережі.
_expand_features	Метод	Формує розширене представлення векторів ознак, додаючи квадрати та перехресні добутки при поліномі другого ступеня.
_get_feature_names	Метод	Генерує список імен усіх ознак (у т.ч. поліноміальних).
update_config	Метод	Оновлює набір факторів або термів без повного створення мережі.
initialize_coeffs	Метод	Ініціалізує коефіцієнти правил за вагами факторів ризику з урахуванням їх напрямку впливу (позитивний або обернений).
_convert_rete_to_tensor	Метод	Перетворює правила Rete-мережі у тензорні представлення $X$ (вхід) і $y$ (вихід).
_calc_activations_batch	Метод	Обчислює ступінь активації кожного правила для пакета прикладів, нормалізує результати.
_calc_z_batch	Метод	Формує поліноміальні оцінки $z\_rules$ для кожного правила і виконує агрегацію з урахуванням активацій.
train_model	Метод	Виконує повноцінне навчання мережі

Елемент коду	Тип	Детальне призначення та опис реалізації
		методом зворотного поширення похибки (MSE). Маска <code>frozen_mask</code> гарантує збереження неактивних коефіцієнтів.
<code>train_and_reduce</code>	Метод	Поєднує навчання та редукцію моделі: після кожного циклу видаляє статистично незначущі коефіцієнти й перенавчає модель.
<code>predict_batch</code>	Метод	Повертає прогнознi значення для пакета даних (застосовується сигмоїдна функція).
<code>Predict</code>	Метод	Прогноз для одного набору факторів.
<code>get_global_coefficients</code>	Метод	Обчислює усереднені глобальні коефіцієнти всієї системи правил.
<code>get_global_polynomial_equation</code>	Метод	Формує текстове представлення глобального поліноміального рівняння у вигляді $R = \text{sigmoid}(\dots)$ .
<code>check_model_adequacy</code>	Метод	Оцінює адекватність моделі за тестовою Rete-мережею, обчислюючи MAE, RMSE та коефіцієнт кореляції.
<code>save_model</code>	Метод	Зберігає параметри навченої моделі у файл <code>.pkl</code> (через <code>pickle</code> ).
<code>load_model</code>	Метод	Завантажує раніше збережену модель із файлу <code>.pkl</code> та відновлює структуру правил.
<code>rules, X, Y, factor_names, terms_num, feature_names</code>	Атрибути екземпляра	Робочі структури моделі: набір правил, навчальні дані, імена факторів і розгорнутих ознак.

Повний програмний код реалізації даного модуля наведено у Додатку Е лістинг Е.7.

3. Блок «Синтез управлінських рішень та стратегічне планування» завершує цикл ППР, трансформуючи результати нейронечіткого моделювання у конкретні управлінські рекомендації. Програмна реалізація базується на модулі оптимізації керованих факторів, який реалізує процедуру визначення оптимальних значень керованих факторів ІБ ТЛЦ на основі глобального поліноміального рівняння ANFIS-моделі.

Підхід, реалізований у модулі, ґрунтується на символічному аналізі похідних, що дозволяє:

- визначати аналітичний вплив кожного керованого фактора;

- знаходити точки екстремуму у межах  $[0; 1]$ ;
- встановлювати оптимальні значення при різних комбінаціях зовнішніх умов;
- формувати рекомендації у вигляді управлінських стратегій.

Метою модуля є побудова символічної функції ризику на основі ANFIS-моделі, аналіз її часткових похідних та визначення оптимальної інтенсивності керованих заходів безпеки.

Вхідні параметри:

1. `fixed_vars` – словник сталих (зовнішніх) факторів, значення яких відомі та не підлягають оптимізації;
2. `controlled_vars` – список керованих змінних, для яких виконується оптимізація у межах  $[0;1]$ ;
3. `anfis_model` – модель типу ANFIS, що містить глобальне поліноміальне рівняння.

Вихідні параметри:

1. `optimal_values` – словник оптимальних значень керованих факторів;
2. `analysis` – структурований звіт, що включає похідні, їх знаки, висновки та обґрунтування.

Модуль забезпечує:

- парсинг поліноміального рівняння ANFIS-моделі (константа, лінійні та квадратичні члени);
- побудову повного символічного виразу функції ризику  $R(x)$ ;
- підстановку значень сталих факторів та спрощення функції;
- обчислення символічних часткових похідних за керованими змінними;
- аналіз знаків похідних у контрольних точках  $(0; 0.5; 1)$  для визначення монотонності та характеру впливу факторів на інтегральний ризик;
- пошук точок екстремуму розв’язанням рівняння  $\frac{\partial f}{\partial x}$ ;
- визначення стратегії: мінімум на межі, максимум на межі або внутрішній оптимум;

- генерацію практичних рекомендацій щодо рівня застосування заходів безпеки.

Таблиця 3.9 узагальнює ключові елементи коду, їх тип та функціональне призначення.

Таблиця 3.9 – Опис елементів модуля оптимізації керованих факторів: класів, методів та атрибутів.

Елемент коду	Тип	Детальне призначення та опис реалізації
Sympy	Бібліотека	Забезпечує символічні обчислення, похідні, розв'язування рівнянь, підстановки.
Re	Бібліотека	Використовується для парсингу текстового представлення поліноміального рівняння ANFIS.
fixed_vars	Атрибут екземпляра	Задання сталих зовнішніх факторів ризику.
controlled_vars	Атрибут екземпляра	Набір змінних, які модуль оптимізує.
symbolic_vars	Атрибут екземпляра	Символьні змінні $x_1 \dots x_n$ , створені через SymPy.
parse_anfis_equation	Метод	Отримує з ANFIS поліном ризику, виконує первинне очищення та передає рядок до парсера.
parse_equation_string	Метод	Витягує коефіцієнти лінійних, квадратичних та парних інтеракційних членів.
build_symbolic_expression	Метод	Формує символічний вираз функції ризику $R(x)$ .
get_simplified_function	Метод	Підставляє сталі змінні у формулу та спрощує вираз.
get_gradient	Метод	Обчислює частинні похідні $df/dx_i$ для керованих факторів.
analyze_derivative_behavior	Метод	Аналізує знак похідної у тестових точках та визначає стратегію оптимізації.
find_zero_gradient	Метод	Шукає точку $df/dx = 0$ у межах $[0;1]$ .
comprehensive_analysis	Метод	Повний цикл аналізу та формування рекомендацій.
analyze_strategy_implications	Метод	Інтерпретує результат оптимізації

Елемент коду	Тип	Детальне призначення та опис реалізації
		як стратегічні рекомендації.

Повний програмний код реалізації даного модуля наведено у Додатку Е, лістинг Е.8.

Програмна реалізація розглянутих модулів формує цілісне алгоритмічне ядро системи «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів» (свідоцтво про реєстрацію авторського права на твір № 143390 від 23.02.2026 р., Додаток А), яке завдяки використанню нечіткої логіки, Rete-алгоритма та нейромережі здатне ефективно функціонувати в умовах невизначеності та динамічних змін ландшафту кіберзагроз.

Для функціонування розроблених модулів та навчання моделі ANFIS встановлено певні вимоги до програмно-апаратного середовища.

Серед програмних засобів основою є операційні системи на базі Linux (Ubuntu 22.04 LTS і вище) або Windows 11 із підсистемою WSL2, де основним середовищем виконання виступає Python 3.9+. До складу ключових бібліотек входять PyTorch не нижче версії 2.0 для реалізації алгоритмів нейромережевого навчання, SciKit-Fuzzy для нечіткого логічного виведення, SymPy для виконання символьних математичних операцій та FastAPI для організації REST-інтерфейсу і шлюзу API.

Апаратні вимоги передбачають використання процесорів Intel Core i5/i7 одинадцятого покоління або аналогів AMD Ryzen, а також наявність від 16 ГБ оперативної пам'яті для коректної обробки Rete-мережі та тензорів ANFIS. Додаткове застосування графічного прискорювача NVIDIA з підтримкою CUDA (від 4 ГБ VRAM) дозволяє скоротити час ітерацій градієнтного спуску при навчанні моделі. Контейнеризація всіх компонентів на базі Docker забезпечує ізоляцію програмних залежностей модулів та спрощує розгортання системи в

інфраструктурі ТЛЦ.

### **Висновки до розділу 3**

У розділі 3 вирішено завдання проєктування та програмної реалізації інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ. Отримано наступні результати:

За допомогою методологій IDEF0, IDEF1, DFD та IDEF3 формалізовано функціональну структуру системи. Побудовані моделі дозволили декомпонувати процес управління ризиками на послідовні етапи: від агрегації сирих даних телеметрії до селекції критичних загроз та синтезу управлінських рішень. Це забезпечило чітке визначення меж системи та логіки інформаційних потоків.

Розроблено сценарії взаємодії користувачів засобами мови UML. Рольова модель (інженер з безпеки, експерт-аналітик, ОПР) дозволила розмежувати зони відповідальності та сформулювати вимоги до інтерфейсів системи. Розробка діаграм варіантів використання забезпечила відповідність розробленого ПЗ вимогам стандарту RBAC.

Обґрунтовано чотирирівневу багатокомпонентну сервіс-орієнтовану архітектуру інформаційної технології. Застосування принципу поліглотної персистентності на рівні даних (використання TimescaleDB, Neo4j, MongoDB) дозволило оптимізувати зберігання різномірної інформації від високочастотних часових рядів телеметрії до складних графових зв'язків топології активів.

Реалізовано програмне ядро системи, що поєднує експертну модель Мамдані та адаптивну нейромережу ANFIS. Такий підхід вирішує проблему «холодного старту» системи та забезпечує її подальше самонавчання на основі накопиченої статистики інцидентів. Впровадження Rete-алгоритму дозволило оптимізувати процес логічного виведення, мінімізуючи обчислювальні витрати.

Програмно реалізовано модуль прескриптивної оптимізації на основі символьних обчислень. Використання аналітичного аналізу похідних



поліноміального рівняння ризику дозволило автоматизувати пошук оптимальних значень керованих факторів безпеки, що забезпечує мінімізацію інтегрального ризику при заданих бюджетних обмеженнях.

Визначено технічні вимоги та стек технологій (Python, PyTorch, Docker), що гарантують масштабованість та кросплатформність системи. Контейнеризація модулів забезпечує швидке розгортання ІТ ППР у динамічній інфраструктурі сучасних транспортно-логістичних центрів.

Отримані проектні рішення та програмні засоби створюють необхідну базу для проведення експериментальних досліджень та перевірки ефективності запропонованої технології.

Основні наукові результати, отримані у розділі 3, опубліковані у статтях [89], [126] і тезах [90], [127].

## РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ВЕРИФІКАЦІЯ АДАПТИВНОЇ НЕЙРОНЕЧІТКОЇ МОДЕЛІ

### 4.1 Експериментальна верифікація та структурний аналіз моделі

Експериментальні дослідження та практична апробація розроблених у роботі моделей здійснювалися в межах виконання державного проекту прикладного дослідження «Розробка інформаційно-аналітичної системи управління логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки» (№ 0124U000696) [128] та відповідно до плану науково-дослідної роботи Національного університету «Чернігівська політехніка» – «Системний аналіз інформаційних процесів управління логістичною діяльністю» (№0124U003344).

Концептуальні засади побудови подібних інтелектуальних СППР для ТЛЦ та волонтерської діяльності були попередньо опрацьовані автором у працях [129], [130].

Першим етапом експериментальних досліджень стала перевірка адекватності розробленої нейронечіткої моделі (ANFIS). Метою є підтвердження того, що математичне ядро системи коректно інтерпретує вхідні дані та логічно реагує на типові сценарії функціонування ТЛЦ [131]. Це дозволяє виявити нелінійні залежності, які неможливо зафіксувати класичними методами лінійної згортки.

Для проведення верифікації моделі спочатку було зафіксовано базовий вектор вагових коефіцієнтів. Для цього використано дефазифіковані значення (центроїди), отримані за результатами Fuzzy АНР у п. 2.2 (стан «мирного часу»). Саме ці ваги визначають вклад кожного фактора у формування ризику:

$$W = \{\tilde{W}^A = 0.154; \tilde{W}^P = 0.225; \tilde{W}^{Los} = 0.354; \tilde{W}^{Con} = 0.043; \tilde{W}^F = 0.124; \tilde{W}^{Cul} = 0.100\}.$$

Враховуючи специфіку об'єкта дослідження – невеликого регіонального ТЛЦ з обмеженим ресурсним забезпеченням, було сформовано чотири типові

сценарії функціонування. Вхідні дані для них подано у вигляді лінгвістичних векторів  $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ , де використовуються терми: L (Low/Низький), M (Medium/Середній), H (High/Високий), VH (Very High/Дуже Високий).

Сценарій № 1 «Ідеальний захист» – теоретична модель ситуації, де регіональний ТЛЦ отримав повне фінансування на модернізацію. Характеризується мінімальним рівнем загроз (оновлені активи) при максимальному залученні всіх засобів захисту. Слугує еталоном («нульовою точкою») для калібрування системи. Визначається вектором: {L, L, L, VH, VH, VH}.

Сценарій № 2 «Середній стан» – типовий режим роботи ТЛЦ. Усі фактори збалансовані на середньому рівні: помірні загрози, стандартний бюджет на ІБ та базовий рівень підготовки диспетчерів. Вектор дозволяє перевірити стабільність моделі в умовах повсякденної рутини («сіра зона» невизначеності). Описується вектором: {M, M, M, M, M, M}.

Сценарій № 3 «Хибна економія» – характерна проблема для невеликих регіональних ТЛЦ. Керівництво інвестує в апаратне забезпечення та ПЗ, але економить на навчанні персоналу. В умовах високих зовнішніх загроз низька культура ІБ (на кшталт слабких паролів, фішингу) нівелює технічні витрати. Сценарій перевіряє здатність системи виявляти цю «слабку ланку». Визначається вектором: {H, H, H, M, M, L}.

Сценарій № 4 «Повна вразливість» – найгірший можливий випадок. Відповідає стану регіонального ТЛЦ із застарілою інфраструктурою, відсутністю бюджету на ІБ та критичною залежністю від даних. Максимальні загрози поєднуються з повною відсутністю захисту. Описується вектором: {VH, H, VH, L, L, L}.

На основі сценаріїв № 1-4 проведений порівняльний аналіз результатів, отриманих трьома методами:

1. Експертна оцінка. Оцінка ріння ІБ ТЛЦ за формулою (2.21) на основі експертних даних п. 2.2, що дає інтервальний результат  $(\widetilde{RI})$ .

2. Повна ANFIS-модель. Нейронечітка мережа з повною кількістю правил (2880) та складним поліномом.
3. Редукована ANFIS-модель. Оптимізована модель після редукції.

Результати експерименту наведено в таблиці 4.1.

Таблиця 4.1 – Порівняння результатів оцінювання ризику ІБ ТЛЦ (дані експерименту)

Сценарій	Характеристика вхідного вектора ( $x_1, \dots, x_6$ )	Рівень ризику ІБ ТЛЦ			
		Середня впевненість	Висока впевненість	ANFIS	ANFIS Reduced
1. Ідеальний захист	{L, L, L, VH, VH, VH}	0.1782	0.1392	0.1381	0.1352
2. Середній стан	{M, M, M, M, M, M}	0.3758	0.4347	0.4610	0.4642
3. Хибна економія	{H, H, H, M, M, L}	0.5543	0.6923	0.6978	0.7064
4. Повна вразливість	{VH, H, VH, L, L, L}	0.6806	0.8392	0.8530	0.8608

Аналіз отриманих результатів дозволяє зробити наступні висновки.

Порівняння стовпців «ANFIS» та «ANFIS Reduced» демонструє високу збіжність результатів. Максимальне абсолютне відхилення зафіксовано у сценарії № 3 і становить лише 0,0086 (<1,3%). Це підтверджує коректність процедури спрощення полінома. Вилучення статистично незначущих зв'язків не погіршує точність прогнозу, але знижує обчислювальне навантаження.

Незважаючи на середній рівень технічного захисту сценарія № 3 ( $x_4, x_5 = M$ ), модель оцінила ризик як «високий» (0,70). Це свідчить про те, що система коректно враховує нелінійну вагу фактора рівня культури ІБ. Отже, без належної підготовки персоналу технічні засоби втрачають ефективність.

Встановлено, що впевненість експерта безпосередньо визначає ступінь визначеності результату. При середній впевненості (за сценарієм № 4) спостерігається ефект згладжування оцінки (0,6806), що дозволяє уникати хибно-позитивних висновків при низькій надійності даних. За високої впевненості результат стає більш чітким та однозначним (0,8392), що дозволяє моделі точно

ідентифікувати граничний стан системи.

Візуалізацію отриманих результатів наведено на рис. 4.1.

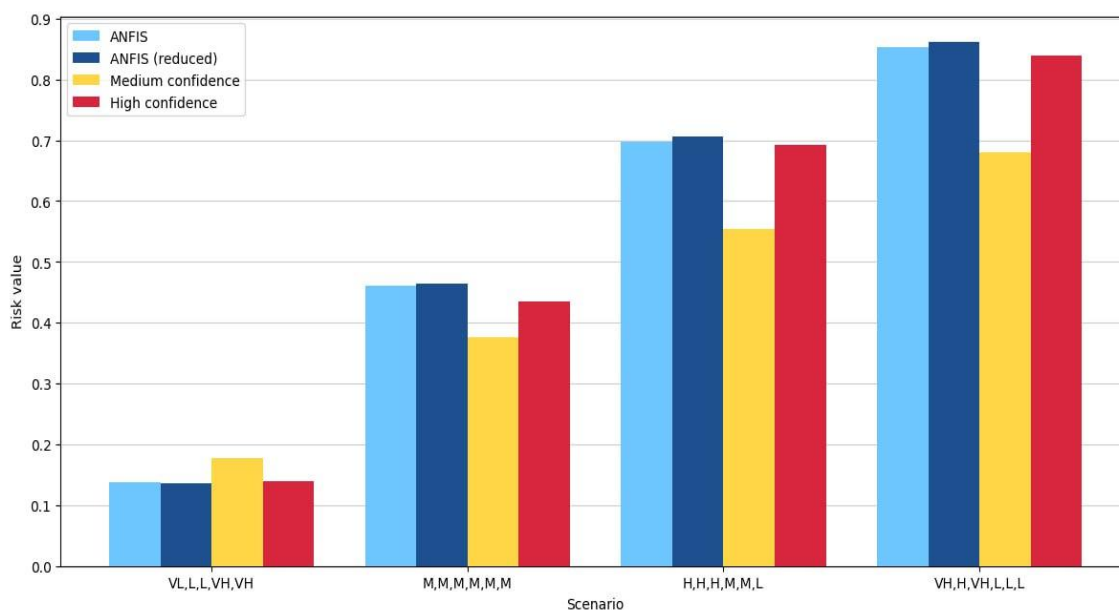


Рисунок 4.1 – Гістограма порівняння результатів оцінювання ризику ІБ ТЛЦ (ANFIS, ANFIS Reduced та експертна оцінка з урахуванням рівня впевненості)

Аналіз гістограми підтверджує, що редукована модель (темно-сині стовпці) майже ідентична повній моделі. Водночас висока впевненість у вхідних даних (червоні стовпці) дозволяє отримати більш визначені показники ризику, наближені до результатів нейромережевого навчання, тоді як середня впевненість (жовті стовпці) зміщує результат до нейтральної зони шкали як механізм захисту від неточності експертних суджень.

Для формування науково обґрунтованої стратегії захисту було проведено декомпозицію отриманого глобального поліноміального рівняння регресії. Тобто було здійснено перехід від нейромережевого моделювання до аналітичної інтерпретації, яка обґрунтовує внутрішні механізми прийняття рішень. Узагальнені результати теоретичного аналізу ключових елементів моделі систематизовано в таблиці 4.2.

Таблиця 4.2 – Інтерпретація елементів поліноміальної моделі ризику ІБ ТЛЦ

Рівень аналізу	Математичний елемент моделі	Значення	Теоретична інтерпретація в контексті ІБ ТЛЦ
1. Базова топологія	Вільний член $\beta_0$	$\beta_0 = 0,2368$	Калібрувальне зміщення вказує на наявність базового фонового ризику навіть за умов ідеального захисту.
2. Функціональна спрямованість	Знаки лінійних коефіцієнтів $\beta_i$	$\beta_{1,2,3} > 0$	Деструктивні чинники, позитивні значення яких підтверджують, що зростання загроз прямо збільшує інтегральний ризик.
		$\beta_{4,5,6} < 0$	Стримувальні чинники, від’ємні значення яких вказують на функцію пригнічення ризику за рахунок інвестицій та навчання.
3. Лінійна чутливість	Лінійні члени $\beta_i x_i$	$\beta_3 = 0.51$	Домінування рівня збитків. Тяжкість наслідків ( $x_3$ ) є найбільш значущим фактором ризику.
4. Теорія взаємодій	Взаємодія драйверів	$\beta_{23} = 0.12$	Мультиплікація загроз підтверджує парадигму «Ризик = Ймовірність × Наслідки».
	Взаємодія мітігаторів	$\beta_{56} = -0.13$	Синергія захисту визначається рівнем витрат на створення і експлуатацію системи та рівнем культури ІБ ТЛЦ, що підсилюють дію одне одного.

Аналіз вагових коефіцієнтів факторів загроз  $x_1$ ,  $x_2$ ,  $x_3$  виявив суттєву структурну асиметрію моделі, яка підпорядковується принципу Парето (20/80). Візуалізація цього розподілу наведена на рисунку 4.2.

Аналіз діаграми дозволяє виділити три групи факторів за ступенем їхнього впливу на інтегральний показник ризику.

Домінуючий фактор – рівень збитків від загроз ( $x_3$ ). Цей показник має найвищий коефіцієнт регресії та формує 60–65% загального потенціалу ризику. Це свідчить про те, що для ТЛЦ тяжкість наслідків одиничного інциденту є критичнішою за технічні аспекти вразливості.

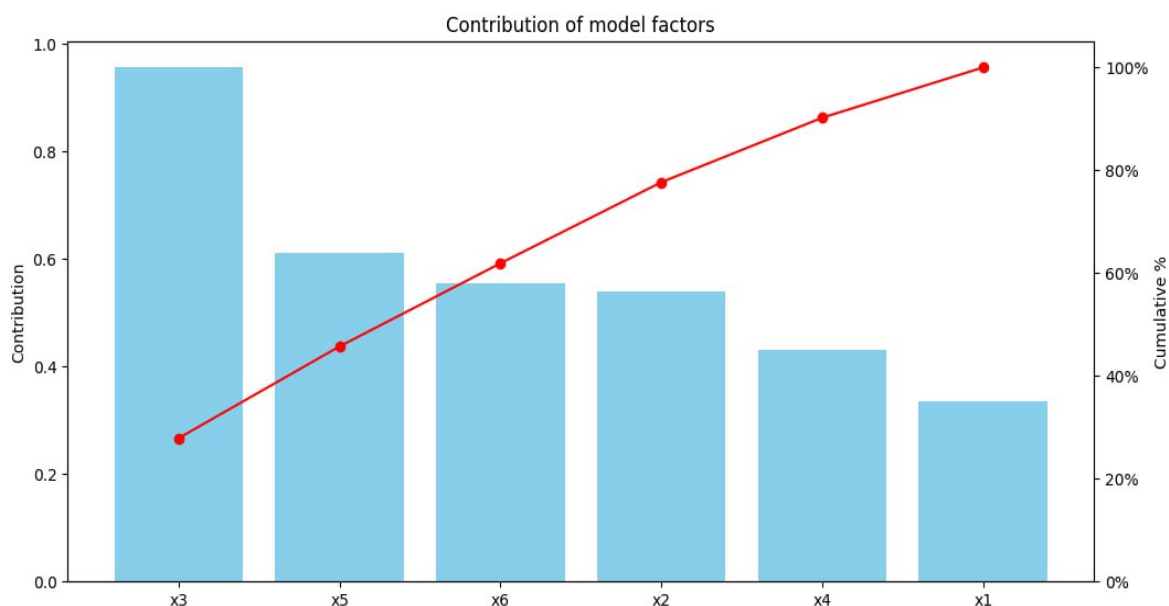


Рисунок 4.2 – Діаграма Парето значущості факторів у формування ризику

Значущий фактор – імовірність реалізації загрози через задані вразливості ( $x_2$ ) формує 20–25% впливу. Чинник поступається  $x_3$ , оскільки частота атак є зовнішнім параметром, тоді як рівень збитків визначається внутрішньою архітектурою ТЛЦ.

Мінорний фактор – рівень цінності активів ( $x_1$ ). Формує лише 10–15% варіативності ризику. У навченій моделі цей показник має найнижчу чутливість, що свідчить про стабільність активів порівняно з динамікою збитків та загроз.

Доведено, що стратегія архітектурної сегментації, зниження рівня збитків ( $x_3$ ) є у 1,8 рази ефективнішою за нарощування систем моніторингу інтенсивності атак ( $x_2$ ) та у 5 разів ефективнішою за спроби штучного заниження цінності активів ( $x_1$ ):

$$\frac{\partial R}{\partial x_3} = 1,8 \cdot \frac{\partial R}{\partial x_2} = 5 \cdot \frac{\partial R}{\partial x_1}.$$

Для підтвердження того, що нейронечітка мережа коректно імплементувала закладені експертні знання, було проведено співставлення початкових ваг (отриманих методом Fuzzy AHP у п. 2.2) та фінальних коефіцієнтів полінома, отриманих після навчання ANFIS. Результати ранжування факторів наведено в

таблиці 4.3, де для коректного порівняння використано модулі значень коефіцієнтів полінома.

Таблиця 4.3 – Кореляція між експертною оцінкою та параметрами навченої моделі

Фактор	Експертна вага (Fuzzy АНР)	Ранг (експерт)	Коефіцієнт полінома (ANFIS)	Ранг (модель)	Висновки
Рівень цінності активів ( $x_1$ )	0.154	3	0.161	6	Зниження пріоритету (поступається ресурсам)
Імовірність реалізації загрози через наявні вразливості ( $x_2$ )	0.225	2	0.275	3	Стабільний вплив
Рівень збитків від загроз ( $x_3$ )	0.354	1	0.494	1	Підтверджено (домінуючий)
Рівень контролю інформаційних ресурсів ( $x_4$ )	0.043	6	0.181	5	Посилення впливу (оперативний рівень)
Рівень витрат на створення та функціонування СУІБ ( $x_5$ )	0.124	4	0.303	2	Критичне зростання (недооцінено експертами)
Рівень культури ІБ ( $x_6$ )	0.100	5	0.266	4	Суттєве зростання (більший вплив, ніж контроль)

Спостерігається повна кореляція рангів між експертними очікуваннями та результатами моделювання. Фактор  $x_3$  (рівень збитків від загроз) залишається домінуючим в обох випадках, що підтверджує адекватність навчання нейромережі.

Модель ANFIS підвищила абсолютну вагу керуючих факторів ( $x_5$ ,  $x_6$ ) порівняно з експертною оцінкою. Це свідчить про те, що нейронечітка модель має підвищену чутливість ризику ІБ ТЛЦ до керуючих впливів, ніж це передбачалося експертами інтуїтивно. І це є перевагою використання методів обчислювального інтелекту для пошуку прихованих резервів оптимізації.



Проведений аналіз дозволяє побудувати чітку ієрархію ефективності керуючих факторів на основі абсолютних значень коефіцієнтів полінома.

1. Рівень витрат на створення і експлуатацію системи ІБ ( $x_5$ ) з коефіцієнтом 0,303 є найпотужнішим інструментом впливу, що визначає загальну ресурсну спроможність системи захисту.

2. Рівень культури ІБ ( $x_6$ ) з коефіцієнтом 0,266 підтверджує критичну роль людського фактора в забезпеченні ІБ ТЛЦ.

3. Рівень контролю ІБ ( $x_4$ ) з коефіцієнтом 0.181 має найменшу чутливість серед розглянутих факторів і вказує на допоміжну роль оперативного моніторингу порівняно з системними інвестиціями.

На основі цих даних проведено кількісний аналіз ефективності керуючих факторів.

1. Ефективність системного фінансування щодо забезпечення ІБ. Співвідношення впливу рівня витрат ( $x_5$ ) до рівня контролю ( $x_4$ ) становить:  $E = \frac{\beta_5}{\beta_4} = \frac{0.303}{0.181} \approx 1.67$ . Тобто системне забезпечення процесів у 1,67 рази ефективніше за точкові заходи контролю.

2. Ефективність людського фактору. Для оцінки ефективності інвестицій у персонал розраховано співвідношення впливу рівня культури ІБ ( $x_6$ ) до рівня контролю ( $x_4$ ):  $E = \frac{\beta_6}{\beta_4} = \frac{0.266}{0.181} \approx 1.5$ . Це означає, що вплив рівня культури ІБ (навчання персоналу) в 1.5 рази перевищує вплив рівня контролю, як суто адміністративного, так і технічного.

3. Стратегічний паритет. Важливо відзначити паритет між факторами рівня витрат ( $x_5$ ) та рівня культури ( $x_6$ ) –  $x_6 (0,266) \approx x_5 (0,300)$ . Такий результат вказує на те, що нарощування витрат на створення і експлуатацію системи ІБ ( $x_5$ ) без інвестування в культуру ІБ ТЛЦ ( $x_6$ ) є стратегічно помилковим. Пріоритетом для ТЛЦ має стати збалансований підхід, де навчання персоналу розглядається як актив, рівнозначний прямому фінансуванню системи захисту.

Отже, нейромережа трансформувала інтегральну модель ризику з

«техноцентричної» (орієнтація на активи та вразливості) на «ресурсоцентричну» (орієнтація на бюджет та культуру ІБ). Це дає керівництву ТЛЦ чіткий сигнал про те, що стійкість системи залежить не від вартості активів, а від стабільності фінансування та зрілості персоналу.

Розроблена модель враховує взаємний вплив факторів. Для ідентифікації прихованих нелінійних залежностей побудовано матрицю синергетичних ефектів (рис. 4.3).

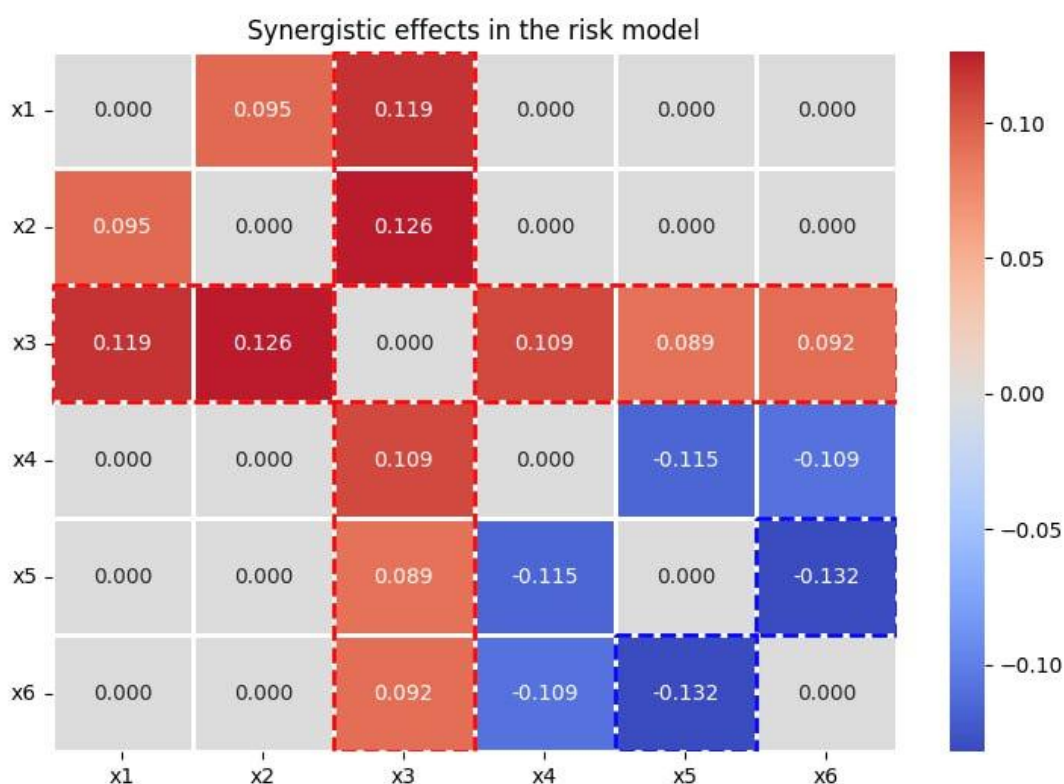


Рисунок 4.3 – Матриця синергетичних ефектів (Heatmap)

Аналіз ключових зон матриці дозволив виділити:

- *зона підсилення ризику* ( $x_3$  – рівень збитків), де стовпець та рядок фактора  $x_3$  забарвлені у насичений червоний колір. Це підтверджує роль критичності наслідків як головного мультиплікатора системи. Високий рівень збитків ( $x_3$ ) критично посилює негативний вплив від цінності активів ( $x_1$ ) та інтенсивності зовнішніх загроз ( $x_2$ ). Таким чином,  $x_3$  виступає «каталізатором», який перетворює помірні вразливості на стани з неприпустимим рівнем ризику;

- *зона стратегічної безпеки* ( $x_5$ ,  $x_6$ ), де перетин факторів «рівень витрат на ІБ» ( $x_5$ ) та «рівень культури ІБ» ( $x_6$ ) забарвлений в інтенсивний синій колір (від’ємний коефіцієнт взаємодії  $-0,132$ ). Це підтверджує наявність синергетичного ефекту мітигаторів, тобто стійкість системи захисту зростає нелінійно при одночасному забезпеченні стабільного фінансування та високої професійної зрілості персоналу.

Для верифікації топології простору рішень побудовано тривимірну діаграму розсіювання значень функції ризику (рис. 4.4).

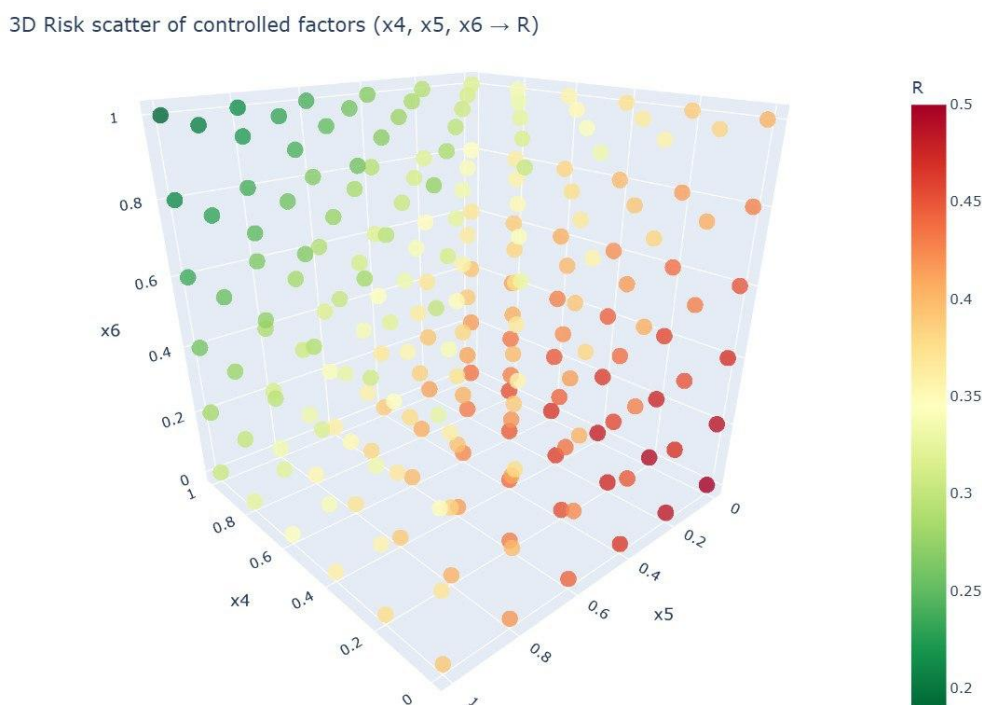


Рисунок 4.4 – 3D-діаграма розсіювання значень функції ризику (залежність від факторів  $x_4$ ,  $x_5$ ,  $x_6$ )

Візуалізація демонструє стійкий градієнтний перехід від зони критичного ризику (темно-червоні маркери) до зони безпеки (темно-зелені маркери). Впорядкована структура хмари розсіювання та наявність чітко вираженого глобального мінімуму (зелена зона) свідчать про відсутність локальних екстремумів та розривів у навченій нейронечіткій моделі. Тобто застосування

методів градієнтної оптимізації дозволить ефективно знайти найкращу стратегію захисту ТЛЦ.

## 4.2 Аналіз архітектурної масштабованості та обчислювальної ефективності

Другим етапом досліджень стала перевірка ефективності запропонованого методу редукції правил (Reducing) у порівнянні з класичним підходом (Basic) на базах знань різної розмірності.

Залежність похибок навчання (RMSE – корінь середньоквадратичної помилки, MAE – середня абсолютна помилка) від кількості правил у базі знань наведено на рисунках 4.5–4.6.

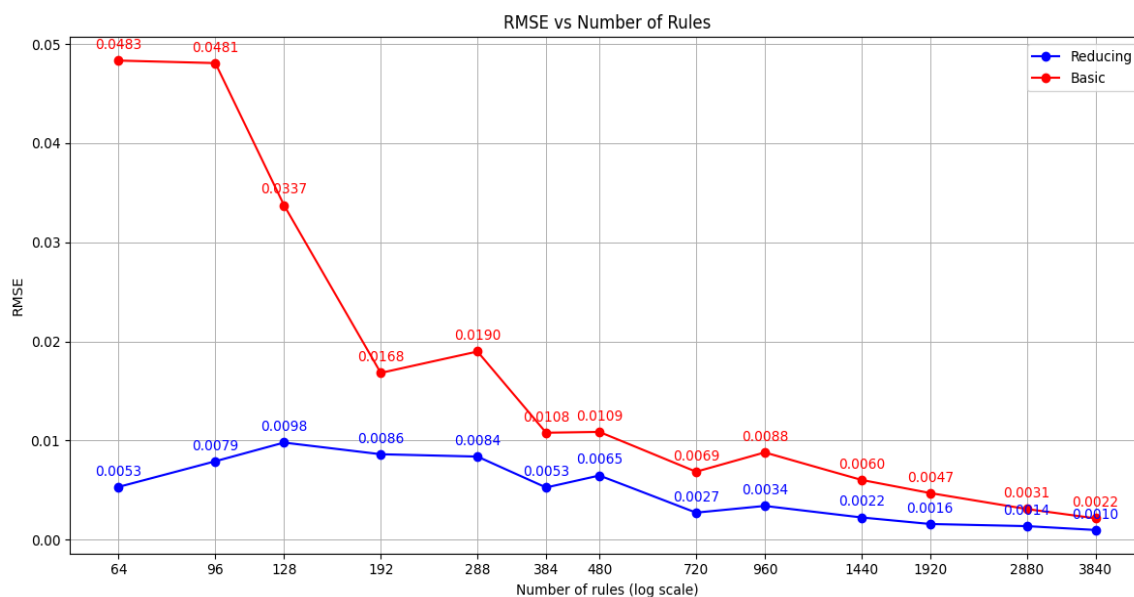


Рисунок 4.5 – Залежність похибок навчання (RMSE) від кількості правил

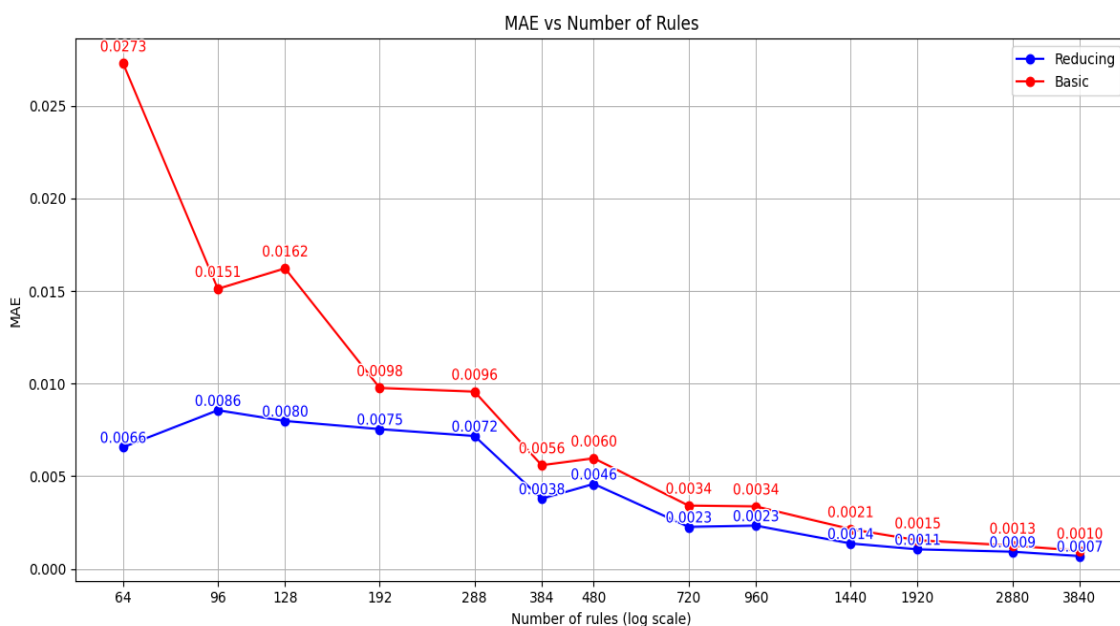


Рисунок 4.6 – Залежність похибок навчання (MAE) від кількості правил

Аналіз отриманих залежностей дозволяє зробити такі висновки. При мінімальній кількості правил (64–128) метод Reducing демонструє в 3–4 рази вищу точність. На кшталт, для 64 правил MAE методу Reducing становить 0.0066, тоді як для Basic – 0.0273. Це свідчить про ефективність алгоритму відбору найбільш значущих правил. Зі збільшенням бази знань (понад 1000 правил) точність обох методів асимптотично наближається до мінімуму ( $RMSE = 0.0015$ ), і різниця між ними стає статистично незначущою.

Залежність часу навчання від ступеня деталізації моделі (кількості правил) представлена на рисунку 4.7.

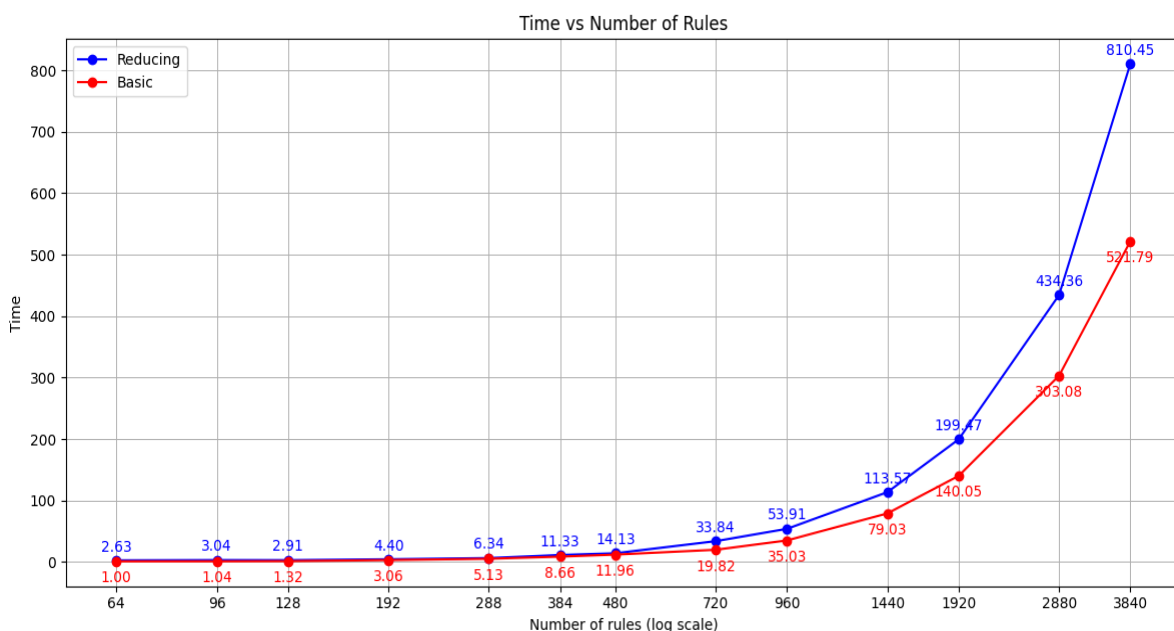


Рисунок 4.7 – Залежність часу навчання від деталізації бази знань

Експериментальні дані показують зростання для обох методів залежності часу  $T(N)$  від кількості правил  $N$ , що мають експоненційний характер, що підтверджує проблему «комбінаторного вибуху».

Метод Reducing вимагає додаткових обчислювальних ресурсів на ітеративну оптимізацію структури та розрахунок  $t$ -статистик. Однак, на великих масивах даних (понад 900 правил) відносна різниця в часі навчання нівелюється і стає несуттєвою для загальної продуктивності системи.

Результати експериментальних досліджень дозволяють сформулювати рекомендації щодо практичного застосування методології.

Для задач експертної оцінки та роботи в умовах обмежених обчислювальних ресурсів рекомендовано використовувати метод Reducing з базою правил, обсяг якої не перевищує 729. Це забезпечує високу точність (похибка  $< 1\%$ ) при мінімальних витратах часу.

Для задач глибокого аналізу та стратегічного планування, де критичною є деталізація, доцільно застосовувати «детальну» конфігурацію (понад 3000 правил), оскільки переваги методу редукції на таких масштабах нівелюються.

Підтверджена здатність системи до динамічної адаптації дозволяє рекомендувати її як основу для створення СППР захисту ТЛЦ, що функціонують у нестабільному середовищі.

#### **4.3 Дослідження адаптивних властивостей системи в умовах зміни стратегічних пріоритетів**

Третій етап обчислювального експерименту був присвячений дослідженню здатності адаптивної нейронечіткої моделі забезпечувати автоматичне коригування оцінок ризиків ІБ ТЛЦ при зміні зовнішнього контексту без потреби в структурній модифікації алгоритмічного забезпечення.

Враховуючи специфіку ТЛЦ як об'єкта критичної інфраструктури та дефіцит репрезентативних історичних даних про інциденти («проблема холодного старту»), експериментальні дослідження базувалися на використанні синтетичного набору даних. Формування вибірки здійснювалося за допомогою розробленого модуля генерації бази правил (рис. 3.14). Повний простір станів системи було автоматично синтезовано шляхом декартового добутку множин лінгвістичних термів вхідних факторів (повна база правил налічує 2880 унікальних правил). Для кожного вектора станів обчислювалося еталонне значення ризику ( $R_{\text{target}}$ ) на основі поточної експертної матриці ваг, що дозволило сформулювати навчальну вибірку для нейронечіткої мережі ANFIS.

Експеримент передбачав моделювання двох фаз функціонування системи.

1. Стан А (мирний час) – система налаштована на роботу в штатному режимі, де пріоритети збалансовані між економічною ефективністю та безпекою.
2. Стан В (воєнний час) – введення воєнного стану, що характеризується ескалацією кіберзагроз. На цьому етапі експертна група здійснила переоцінку пріоритетів у модулі Fuzzy АНР, що стало тригером для адаптації моделі.

Порівняльний аналіз вагових коефіцієнтів ( $W_i$ ), отриманих в результаті експертного оцінювання для обох фаз, наведено в таблиці 4.4.

Таблиця 4.4 – Динаміка зміни вагових коефіцієнтів факторів ризику при зміні стратегічного контексту

Назва фактора (позначення)	Вага, $W_A$ (стан А)	Вага, $W_B$ (стан В)	Динаміка змін
Рівень цінності активів ( $x_1$ )	0.154	0.150	Без суттєвих змін
Ймовірність реалізації загроз ( $x_2$ )	0.225	0.200	Незначне зниження
Рівень збитків ( $x_3$ )	0.354	0.450	Суттєве підвищення (+27%)
Рівень контролю ( $x_4$ )	0.043	0.040	Незначне зниження
Рівень витрат на ІБ ( $x_5$ )	0.124	0.124	Без змін
Рівень культури ІБ ( $x_6$ )	0.100	0.160	Підвищення (+60%)

Дані, представлені в таблиці 4.4, вказують на стратегічну адаптацію, що полягає у зміщенні фокусу з імовірності реалізації загроз ( $x_2$ ) на рівень збитків ( $x_3$ ) та рівень культури ІБ ( $x_6$ ). Зміна входних ваг ініціювала процес автоматичного перенавчання нейронечіткої мережі, яка відбувалася у два етапи.

1. Реконфігурація простору правил. Нові ваги ( $W_B$ ) були передані в модуль генерації синтетичної вибірки. Це призвело до перерозподілу вагових коефіцієнтів у базі знань. Правила, антецеденти яких містять високі значення рівня збитків (наприклад, «IF  $x_3$  is Н або VH»), отримали більший вплив на формування результуючого показника. Фактично відбувся перерозподіл «активаційної сили» правил. Сценарії, які в мирний час вважалися помірними, перейшли у категорію критичних.

2. Модифікація параметрів. На оновленій навчальній вибірці відбулося перенавчання нейромережі, що призвело до модифікації параметрів консеквентів (рис. 4.8).



```

results = anfis.check_model_adequacy(rete_test)
print(results)
anfis.get_global_polynomial_equation()

{'MAE': 0.0005699481116607785, 'RMSE': 0.0010042694630101323, 'Correlation': 0.9999748468399048}

'R = sigmoid(-0.2338 + 0.1718*x1 + 0.2801*x2 + 0.5038*x3 + -0.1809*x4 + -0.3056*x5 + -0.2657*x6 + 0.0711*x1^2 + 0.1598*x2^2 + 0.1896*x3^2 + -0.0

anfis = ANFIS(None, poly_degree=2)
anfis.load_model("anfis_f.p2.pkl")
test_samples = [
    {"x1": 0.1, "x2": 0.15, "x3": 0.1, "x4": 0.97, "x5": 0.15, "x6": 0.15},
    {"x1": 0.1, "x2": 0.15, "x3": 0.1, "x4": 0.97, "x5": 0.15, "x6": 0.42},
    {"x1": 0.1, "x2": 0.15, "x3": 0.1, "x4": 0.97, "x5": 0.15, "x6": 0.55},
    {"x1": 0.1, "x2": 0.15, "x3": 0.1, "x4": 0.97, "x5": 0.15, "x6": 0.87},
]

for i, sample in enumerate(test_samples, start=1):
    y_pred = anfis.predict(sample)
    print(f"Sample {i}: input={sample}, predict={y_pred:.4f}")

Model loaded from anfis_f.p2.pkl
Sample 1: input={'x1': 0.1, 'x2': 0.15, 'x3': 0.1, 'x4': 0.97, 'x5': 0.15, 'x6': 0.15}, predict=0.2770
Sample 2: input={'x1': 0.1, 'x2': 0.15, 'x3': 0.1, 'x4': 0.97, 'x5': 0.15, 'x6': 0.42}, predict=0.2487
Sample 3: input={'x1': 0.1, 'x2': 0.15, 'x3': 0.1, 'x4': 0.97, 'x5': 0.15, 'x6': 0.55}, predict=0.2354
Sample 4: input={'x1': 0.1, 'x2': 0.15, 'x3': 0.1, 'x4': 0.97, 'x5': 0.15, 'x6': 0.87}, predict=0.2031

```

Рисунок 4.8 – Схема структурної адаптації нейронечіткої мережі при зміні контексту

Це призвело до модифікації коефіцієнтів поліноміального рівняння, яке апроксимує залежність ризику від вхідних факторів.

Детальний аналіз змін коефіцієнтів (табл. 4.5) дозволяє інтерпретувати нову «логіку прийняття рішень» системи.

Таблиця 4.5 – Порівняльний аналіз коефіцієнтів полінома ризику

Тип коефіцієнта	Взаємодія факторів	Значення (стан А)	Значення (стан В)	Інтерпретація адаптації
Лінійні	Рівень збитків ( $x_3$ )	0.4944	0.6508	Система стала значно чутливішою до потенційних втрат (пріоритет воєнного стану)
	Рівень культури ІБ ( $x_6$ )	-0.2605	-0.4123	Посилено роль персоналу у зниженні ризику
Нелінійні (посилення)	Рівень цінності активів / Рівень збитків ( $x_1 x_3$ )	0.1170	0.1443	Критичні активи вимагають пріоритетного захисту від збитків
	Ймовірність реалізації загроз / Рівень збитків ( $x_2 x_3$ )	0.1228	0.1397	Зростання ваги класичної складової ризику
Нелінійні (мітігація)	Рівень контролю/	-0.1026	-0.1618	Синергетичний ефект – технічні засоби захисту

Тип коефіцієнта	Взаємодія факторів	Значення (стан А)	Значення (стан В)	Інтерпретація адаптації
пом'якшення, зменшення або послаблення)	Рівень культури ІБ ( $x_4x_6$ )			стають на 57% ефективнішими за умови високої культури персоналу

Аналіз нелінійних членів полінома підтвердив здатність моделі виявляти приховані залежності. Зокрема, суттєве зростання взаємодії  $x_4$  та  $x_6$  у фазі війни обґрунтовує тезу, що в екстремальних умовах самі лише технічні засоби (без компетентного персоналу) втрачають ефективність.

Для верифікації практичних наслідків адаптації було проведено тестування моделі на чотирьох контрольних сценаріях (п. 4.1).

Результати моделювання (табл. 4.6) демонструють різницю ( $\Delta$ ) в оцінці ризику між мирним та воєнним часом.

Таблиця 4.6 – Вплив адаптації на інтегральну оцінку ризику для типових сценаріїв

Сценарій	Вхідний вектор $X=\{x_1, x_2, x_3, x_4, x_5, x_6\}$	Ризик $R_A$ (стан А)	Ризик $R_B$ (стан В)	$\Delta$	Пояснення змін
1. Ідеальний захист	{L, L, L, VH, VH, VH}	0.1365	0.1183	-0.0182	Ризик знизився. Завдяки зростанню ваги рівня культури ІБ ( $x_6 = VH$ ), система «винагороджує» за якісну підготовку персоналу.
2. Середній стан	{M, M, M, M, M, M}	0.4607	0.4419	-0.0188	Незначне зниження. Система демонструє стабільність у «сірій зоні» збалансованих факторів.
3. Хибна економія	{H, H, H, M, M, L}	0.6968	0.7149	+0.0181	Ризик зріс. Система «карає» за критично низький рівень культури ІБ ( $x_6 = L$ ) при високих загрозах, попри середні витрати ( $x_5 = M$ ).
4. Повна вразливість	{VH, H, VH, L, L, L}	0.8526	0.8601	+0.0075	Ризик зріс. Домінуючий вплив критичних збитків ( $x_3 =$

Сценарій	Вхідний вектор $X=\{x_1, x_2, x_3, x_4, x_5, x_6\}$	Ризик $R_A$ (стан А)	Ризик $R_B$ (стан В)	$\Delta$	Пояснення змін
					VH) у поєднанні з відсутністю захисту наближає ризик до максимуму.

Експеримент підтвердив, що адаптована модель діє селективно. Вона не просто пропорційно підвищує рівень ризику для всіх об'єктів, а змінює профіль оцінювання, стаючи більш вимогливою до людського фактора та потенційних збитків, що повністю відповідає стратегії захисту критичної інфраструктури у воєнний час.

Для реалізації механізму еволюційного розвитку системи було застосовано методику адаптивного перенавчання. Відповідно до підходу, обґрунтованого в роботі І. Настак (I. Nastac) [132], процес адаптації базується на періодичному оновленні параметрів нейромережі при надходженні нових критичних даних, що дозволяє мінімізувати помилку прогнозування для нелінійних процесів.

Для проведення експериментальних досліджень та верифікації здатності розробленої системи до самонавчання було сформовано масив реальних даних, який відтворює процеси моніторингу інформаційної безпеки ТЛЦ. Зазначена вибірка моделює функціонування трьох подібних за структурою ТЛЦ упродовж операційного періоду тривалістю близько 22 місяців. Загальний обсяг сформованого масиву даних становить 3840 записів, що забезпечує достатню статистичну значущість для оцінки нейронечіткої моделі.

Для проведення навчання та подальшої валідації отриманий масив реальних даних було розподілено у класичному співвідношенні 80/20. Навчальна вибірка (3072 записи) використана для ітераційного донавчання параметрів функцій належності та консеквентних параметрів нечітких правил. Тестова вибірка (768 записів) застосована для незалежного оцінювання результатів, розрахунку метрик точності (Accuracy, Precision, Recall) та побудови матриці помилок.

Запобігання ефекту перенавчання моделі забезпечено використанням

зазначеної незалежної тестової вибірки, застосуванням методу ранньої зупинки (Early Stopping) та послідовною адаптацією на даних декількох об'єктів. Це дозволило досягти високої узагальнюючої здатності системи, за якої модель виявляє фундаментальні закономірності галузі, а не підлаштовується під випадкові шуми конкретної вибірки.

Оцінювання адаптивного потенціалу ANFIS проведено шляхом усунення розбіжностей між апіорними знаннями експертів (фаза «холодного старту») та об'єктивними показниками моніторингу. Для забезпечення високої адекватності моделі у програмному модулі формування БЗ було реалізовано наступні аналітичні механізми.

*Динамічна ідентифікація вагових коефіцієнтів.* На відміну від статичних експертних оцінок ( $W_{\text{expert}}$ ), опрацювання здійснювалося на основі вектора реальних ваг ( $W_{\text{reality}}$ ), визначених за фактичними даними. Зокрема, вплив чинника  $x_2$  було ідентифіковано як критичний (0,400), що зумовило адаптацію параметрів моделі під фактичні закономірності.

*Врахування системного зміщення.* В архітектурі моделі враховано постійне відхилення показників (на рівні 0,05), яке відображає наявність неврахованих зовнішніх загроз, притаманних специфічній інфраструктурі ТЛЦ. Таке зміщення зумовлене специфічним географічним розташуванням ТЛЦ та постійним впливом дестабілізуючих факторів.

*Розпізнавання ефектів синергії та нелінійності.* Модель успішно ідентифікувала нелінійні взаємодії чинників (наприклад, кумулятивний стрибок ризику при одночасному критичному стані  $x_1$  та  $x_3$ ), які зазвичай не враховуються експертами при лінійному формуванні правил.

*Опрацювання природної варіативності даних.* Наявність фонового шуму в реальних даних мережевих сенсорів дозволила підтвердити стабільність алгоритму при опрацюванні нечітких та зашумлених сигналів.

Даний підхід дозволяє більш об'єктивно оцінити швидкість збіжності алгоритму та стабільність моделі при масштабуванні на декількох ТЛЦ. Аналіз

кривої середньоквадратичної помилки (RMSE), наведений на рис. 4.9, дозволяє виділити три етапи адаптації нейронечіткої мережі до територіально розподілених ТЛЦ.

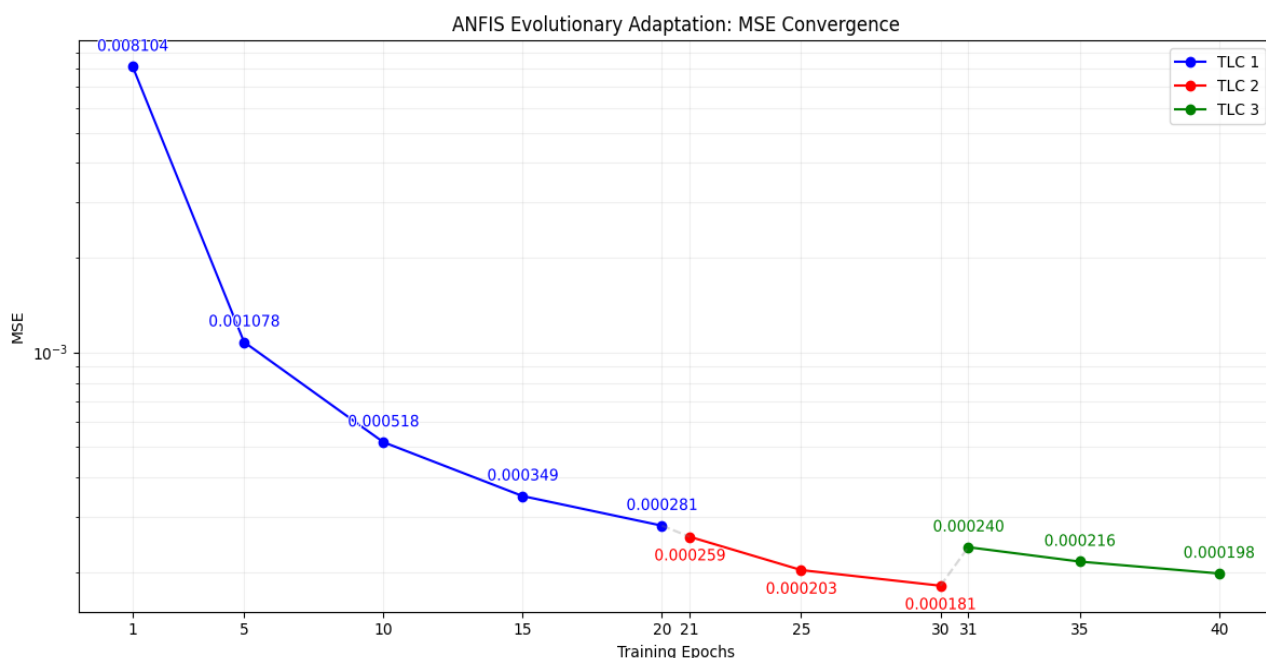


Рисунок 4.9 – Конвергенція помилки навчання нейронечіткої моделі в умовах адаптації

1. Інтенсивна адаптація (ТЛЦ 1, епохи 1–20). Спостерігається найбільш стрімке зниження MSE з 0,008104 до 0,000281. Основний стрибок точності (до 5-ї епохи) зумовлений швидким коригуванням апріорних експертних ваг алгоритмом навчання під реальні статистичні закономірності першого об'єкта.
2. Стабілізація знань (ТЛЦ 2, епохи 21–30). На цьому етапі модель демонструє монотонну конвергенцію до рівня 0,000181. Відсутність коливань підтверджує високу узагальнюючу здатність системи. Отримані раніше знання виявилися релевантними для другого ТЛЦ, що вимагало лише незначного уточнення параметрів.
3. Адаптивне донавчання (ТЛЦ 3, епохи 31–40). Введення даних третього об'єкта на 31-й епосі спричиняє локальний сплеск RMSE до 0,000240. Це пояснюється адаптацією до специфічних аномалій або нових граничних умов ТЛЦ 3, не

врахованих раніше. Проте вже до 40-ї епохи помилка знижується до 0,000198, що свідчить про успішну інтеграцію нових знань без ефекту «катастрофічного забування» попереднього досвіду.

Поетапне зниження RMSE до рівня  $< 0,0002$  підтверджує ефективність адаптації ANFIS у динамічному середовищі територіально розподілених об'єктів.

На кожному етапі адаптації проводилося комплексне тестування моделі на контрольній вибірці. Це дозволило оцінити зміну точності апроксимації після інтеграції даних кожного з трьох територіально розподілених ТЛЦ. Основні статистичні показники ефективності наведено у табл. 4.7.

Таблиця 4.7 – Статистичні показники точності моделі ANFIS на етапах адаптації.

Етап	MAE	RMSE	Correlation
Базова модель	0.089383	0.109579	0.702599
Після ТЛЦ 1	0.011888	0.016933	0.992841
Після ТЛЦ 2	0.010866	0.015738	0.993922
Після ТЛЦ 3	0.009879	0.014785	0.994522

Аналіз результатів підтверджує стрімке зростання точності вже після першого етапу адаптації (ТЛЦ 1), де середньоквадратична помилка (RMSE) знизилася майже у 7 разів порівняно з базовою моделлю. Подальше донавчання забезпечило стабілізацію коефіцієнта кореляції на рівні 0,994, що свідчить про високу адекватність налаштованих нечітких правил фактичним даним логістичної системи.

Оцінка диференційованих показників ефективності за категоріями ризику (табл. 4.8) підтверджує високу селективність моделі ANFIS після завершення циклу адаптації.

Таблиця 4.8 – Показники точності розпізнавання станів інформаційної безпеки ТЛЦ.

Клас	Точність (Precision)	Повнота (Recall)	Кількість (Support)	<i>F</i> -міра (середнє гармонійне між точністю та повнотою)
L	1.00	1.00	3	1.00
M	0.92	0.95	143	0.93
H	0.97	0.95	464	0.96
VH	0.93	0.96	158	0.94

Особливої уваги заслуговує здатність системи до ідентифікації критичних станів. Для класу VH (дуже високий ризик) показник повноти розпізнавання (Recall) досягає 0,96, що мінімізує ймовірність пропуску реальних загроз в умовах моніторингу ТЛЦ. Високі значення *F*-міра (від 0,93 до 1,00) свідчать про гармонійне поєднання точності та повноти охоплення даних, незважаючи на суттєву диспропорцію в обсягах вибірок між класами.

Візуалізація результатів у формі матриці помилок (рис. 4.10) підтверджує високу діагональну збіжність прогнозів, що свідчить про точність налаштованої бази знань.

Фактичний клас (Actual)	L	3	0	0	0
	M	0	136	7	0
	H	0	12	441	11
	VH	0	0	7	151
		L	M	H	VH
		Прогноз системи (Predicted)			

Рисунок 4.10 – Матриця помилок класифікації станів системи

Основний масив коректних рішень зосереджений у класі H (441 випадок). Поодинокі відхилення виникають лише між суміжними категоріями, що зумовлено нечіткою природою меж лінгвістичних термів, тоді як критичні стани (L та VH) ідентифікуються системою без помилок.

Проведене дослідження підтверджує ефективність адаптації нейронечіткої моделі ANFIS в умовах динамічного середовища територіально розподілених об'єктів. Завдяки ітераційному донавчанню на даних трьох ТЛЦ вдалося досягти стабілізації середньоквадратичної помилки на рівні  $RMSE = 0,0147$ . Це демонструє здатність системи самостійно компенсувати розбіжності між апріорними експертними знаннями та реальною статистикою, що відображається у зростанні коефіцієнта кореляції з 0,702 до 0,994.

Висока загальна точність класифікації (Accuracy = 95,2%) та стабільні показники повноти розпізнавання критичних загроз (Recall = 0,96 для класу VH)



доводять надійність запропонованого підходу. Отримані результати свідчать про те, що модель не лише успішно адаптується до специфічних аномалій окремих об'єктів, а й зберігає високу узагальнюючу здатність без ефекту втрати попереднього досвіду, що є критично важливим для інтелектуальних систем моніторингу інформаційної безпеки.

Проведені дослідження підтвердили, що розроблена система є адаптивною у двох аспектах.

1. Стратегічному, оскільки вона реагує на зміну контексту через механізм переналаштування ваг у Fuzzy АНР .

2. Еволюційному, оскільки вона здатна до самовдосконалення та підвищення точності шляхом послідовного навчання на історичних даних різних ТЛЦ, що робить її придатною для довготривалої експлуатації в динамічному кіберсередовищі.

#### **4.4 Прескриптивна аналітика та оптимізація стратегій захисту**

Вихідним результатом ANFIS-моделі є диференційована функція  $R(X)$ , що дозволяє застосувати методи градієнтного аналізу для пошуку оптимального вектора керування в залежності від зовнішнього контексту.

Отже, на четвертому етапі експериментального дослідження було проведено порівняння двох полярних станів функціонування ТЛЦ для визначення оптимальних стратегій.

Стан А (мирний час) характеризується низьким рівнем загроз та штатною роботою. Вектор некерованих факторів:  $X_{fix} = \{x_1 = 0,2; x_2 = 0,2; x_3 = 0,2\}$ .

При низьких значеннях загроз вагові коефіцієнти «драйверів ризику» у поліномі зменшуються, а квадратичні члени (ефекти насичення) стають більш вираженими.

У цьому сценарії спостерігається ефект спадної граничної корисності.

Похідні  $\frac{\partial f}{\partial x_i}$  прямують до нуля всередині діапазону  $[0, 1]$ . Математично це відповідає умові стаціонарності:  $\frac{\partial f}{\partial x_i} = 0$  при  $0 < x_i^* < 1$ .

Розрахунок показує, що подальше нарощування захисту понад певний рівень (наприклад,  $x_5 > 0.6$ ) дає мізерне зниження ризику, яке не виправдовує витрат.

Оптимальним вектором є:  $x_4^* \approx 0.5, x_5^* \approx 0.6, x_6^* \approx 0.5$ .

Це обґрунтовує стратегію раціональної достатності. У мирний час система рекомендує підтримувати збалансований рівень захисту, уникаючи надлишкових витрат.

Стан В (воєнний час) характеризується високим рівнем загроз та критичною цінністю активів.

Вектор некерованих факторів:  $X_{fix} = \{x_1 = 0.9; x_2 = 0.8; x_3 = 0.7\}$ .

Підстановка констант у глобальний поліном трансформує його у локальну функцію керування:  $f_{war}(x_4, x_5, x_6) = C - 0.099 x_4 - 0.244 x_5 - 0.199 x_6 - \dots$

Обчислення частинних похідних для цього стану показало, що вони зберігають від'ємний знак на всьому діапазоні допустимих значень  $[0, 1]$ :  $\frac{\partial f}{\partial x_4} < 0$ ,  $\frac{\partial f}{\partial x_5} < 0, \frac{\partial f}{\partial x_6} < 0$ .

Оскільки функція ризику монотонно спадає, глобальний мінімум знаходиться на правій межі гіперкуба:  $x_4^* \approx 1, x_5^* \approx 1, x_6^* \approx 1$ .

Це обґрунтовує стратегію тотальної оборони. В умовах критичних загроз «золотої середини» не існує. Будь-яка економія ресурсів призводить до неприпустимого зростання ризику, тому єдиним рішенням є максимізація всіх контрзаходів.

Узагальнення результатів прескриптивної аналітики наведено в таблиці 4.9.

Таблиця 4.9 – Матриця вибору оптимальної стратегії захисту

Характеристика	Стан А – Мир	Стан В – Війна
Цільова функція	<i>min</i> (Ризик+Витрати)	<i>min</i> (Ризик)
Тип оптимуму	Локальний баланс	Граничний (Абсолютний)

Характеристика	Стан А – Мир	Стан В – Війна максимум)
Рекомендація	Раціональна достатність Підтримка гігієни безпеки без надвитрат	Тотальна мобілізація. Залучення всіх наявних ресурсів (100%).
Економічне зростання	Оптимізація операційних витрат	Забезпечення виживання ТЛЦ

Запропонована адаптивна нейронечітка модель оцінювання інтегрального рівня ризику ТЛЦ не є статичним калькулятором. Вона діє як інтелектуальний радник, який в залежності від контексту змінює/перемикає парадигму керування (від економії ресурсів у стабільний період до безкомпромісного захисту в критичних умовах).

#### **4.5 Програмна реалізація інформаційної технології підтримки прийняття рішень**

Для практичного застосування розроблених моделей та методів було створено вебзастосунок «SecureFuzzy», що забезпечує кросплатформеність та доступність для користувачів без необхідності встановлення додаткового ПЗ. Додаток реалізує повний цикл оцінювання ризиків ІБ ТЛЦ від нечіткого налаштування експертами ваг факторів до автоматизованих рекомендацій щодо зниження рівня ризику.

Головне вікно системи (рис. 4.11) надає доступ до основних модулів вебзастосунку: модулів оцінювання, аналітичних інструментів та налаштування параметрів моделі.

Інтерфейс розроблено з урахуванням вимог до Usability [134], що дозволяє використовувати інформаційну технологію фахівцям без глибоких знань у галузі математичного моделювання та штучного інтелекту.

Модуль налаштування параметрів (Fuzzy AHP) надає доступ до математичного ядра розрахунку технічним фахівцям та аналітикам системи. Ключовою особливістю системи є її адаптивність.

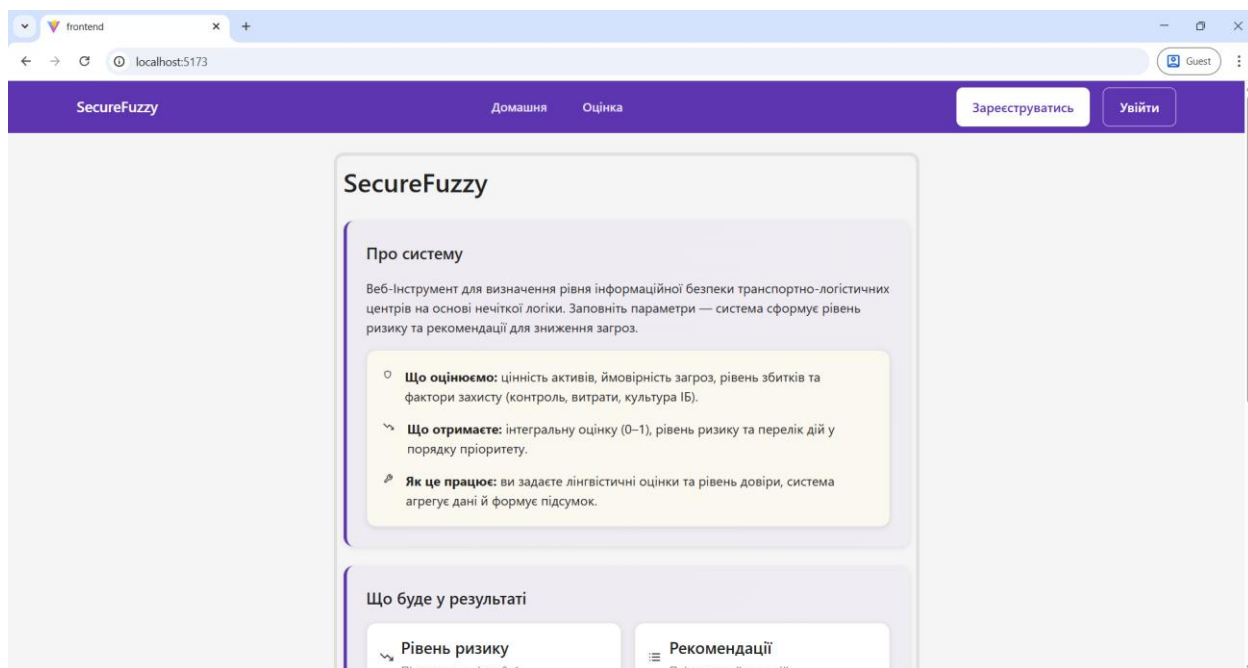


Рисунок 4.11 – Головне вікно системи «SecureFuzzy»

Модуль налаштування ваг (рисунок 4.12) дозволяє експертам встановлювати пріоритети для головних груп факторів ризику ( $x_1, \dots, x_6$ ) та автоматично розраховувати коефіцієнт узгодженості їхніх думок.

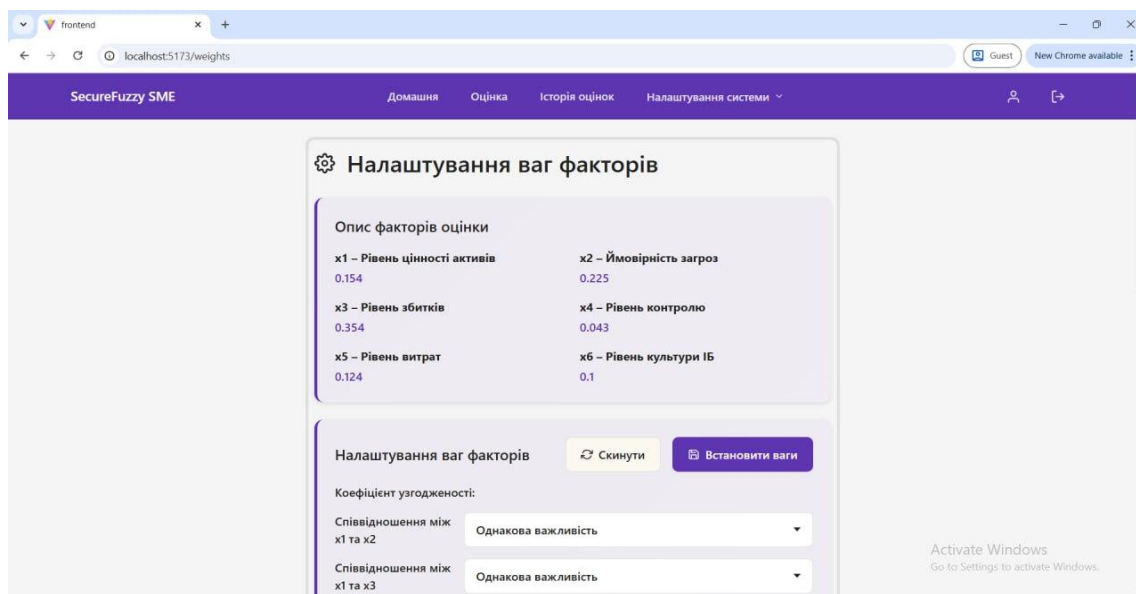


Рисунок 4.12 – Інтерфейс налаштування вагових коефіцієнтів факторів

Для деталізації оцінки ризику ІБ ТЛЦ реалізовано модуль управління підфакторами (рис. 4.13), де користувач може коригувати ваги локальних

параметрів (на кшталт, типи збитків або категорії загроз), використовуючи лінгвістичні змінні.

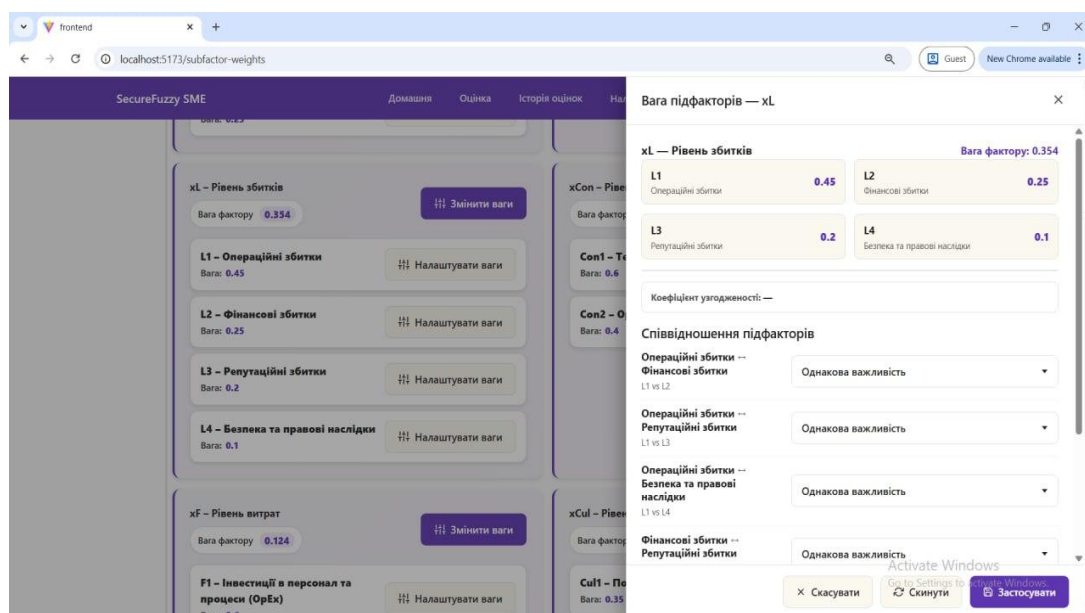


Рисунок 4.13 – Налаштування параметрів підфакторів оцінювання

Для наочного представлення стану ІБ ТЛЦ в систему імплементовано матрицю Дж. Х. Вільсона (рис. 4.14).

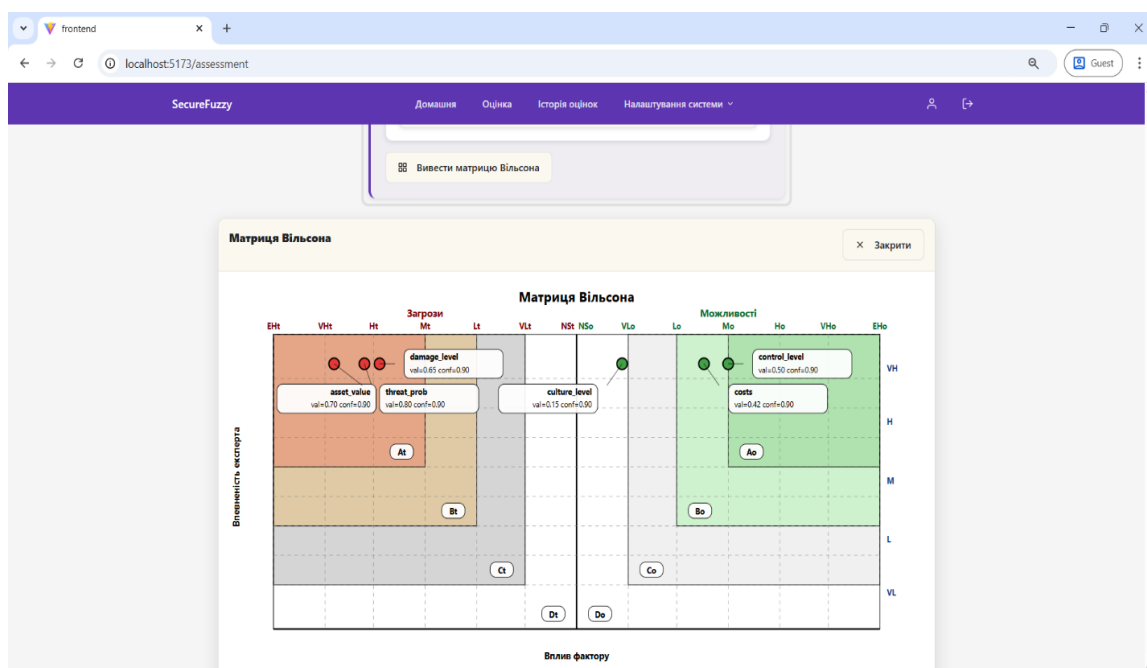


Рисунок 4.14 – Візуалізація пріоритетів ІБ (матриця Вільсона)

Цей інструмент розподіляє загрози у координатах (вплив; впевненість) і дозволяє ідентифікувати пріоритетні напрями роботи та стратегічно розподіляти ресурси для забезпечення ІБ ТЛЦ:

- зона критичних загроз (червона зона) – потребують негайної реакції та прямих інвестицій у засоби захисту для запобігання критичним збиткам;
- зона стабільності (зелена зона) – поточні заходи захисту ефективні, на них слід спиратися при побудові стратегії;
- зона невизначеності (жовта зона) – вимагає додаткового аудиту та поглибленого збору інформації для уточнення моделі.

Завдяки такій візуалізації, система «SecureFuzzy» перетворює складні результати стратегічного аналізу у наочну карту ризиків, зрозумілу для прийняття управлінських рішень без додаткової спеціальної підготовки персоналу.

Процес оцінювання ризику ІБ ТЛЦ відбувається у кілька етапів. Спочатку система виконує експертну-оцінку (рис. 4.15).

Рисунок 4.15 – Інтерфейс експертної оцінки поточного рівня ризику

Для технічних фахівців доступна вкладка математичної інтерпретації (рис. 4.16), де відображаються глобальне поліноміальне рівняння, згенероване модулем ANFIS, та метрики точності моделі (MAE, RMSE). Система демонструє високу точність апроксимації ( $RMSE \approx 0,0017$ ).

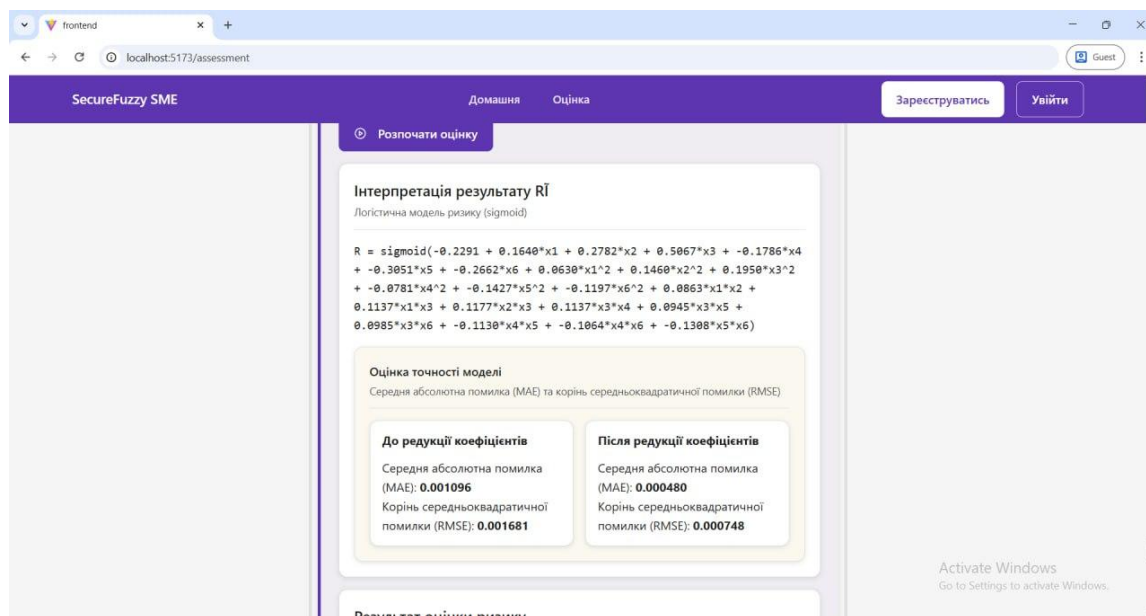


Рисунок 4.16 – Математична інтерпретація моделі та метрики точності

Підсумкова панель (рис. 4.17) трансформує числовий результат нейромережі у лінгвістичну мітку (на кшталт, «Високий рівень ризику») та формує пріоритезований план дій.

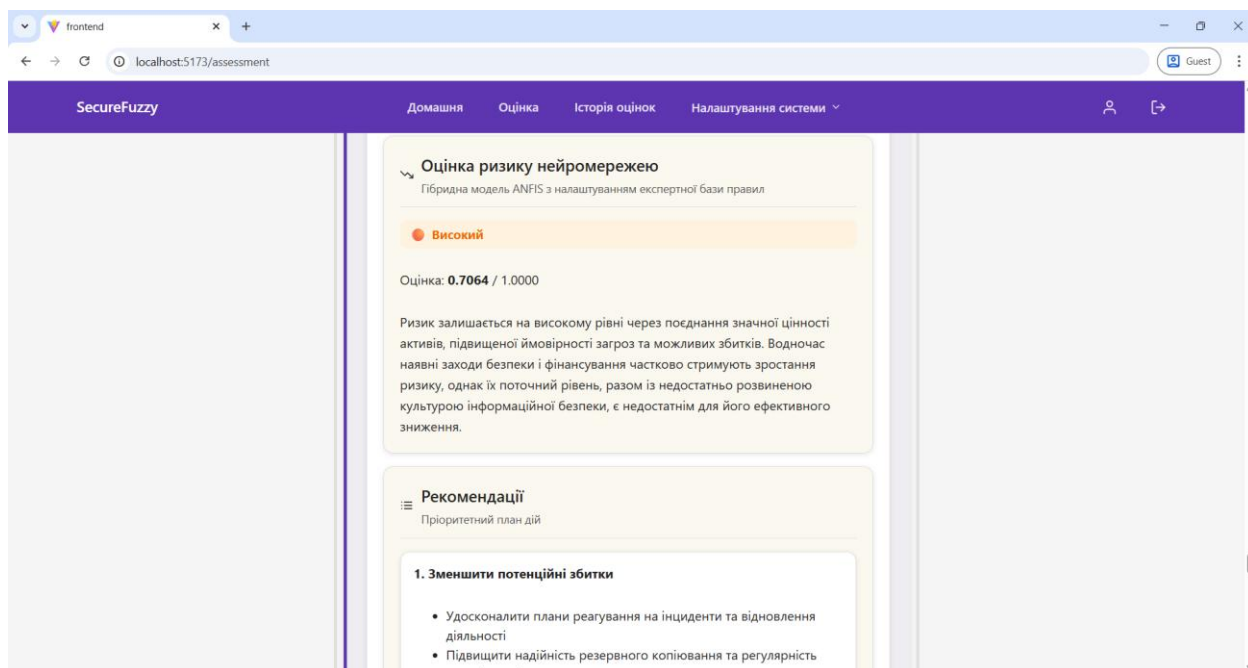


Рисунок 4.17 – Відображення нечіткого значення інтегрального рівня ризику та його інтерпретація

На основі виявлених вразливостей система формує пріоритезований план дій (рис. 4.18). Всі визначені заходи з забезпечення ІБ ТЛЦ представлені від найбільш критичних (зменшення потенційних збитків) до превентивних (підвищення культури ІБ).

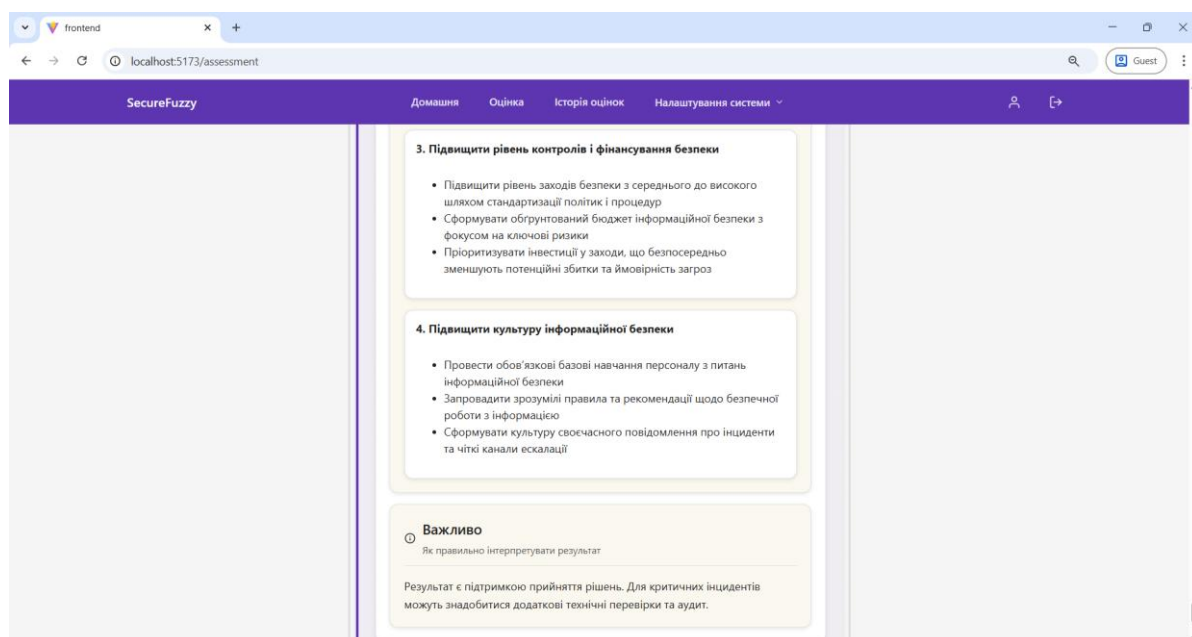


Рисунок 4.18 – Генерація автоматизованих рекомендацій щодо зниження рівня ризику



Це дозволяє керівництву ТЛЦ обирати пріоритетну стратегію забезпечуючи раціональне використання бюджету безпеки відповідно до наявного бюджету.

Розроблений вебзастосунок «SecureFuzzy» успішно пройшов апробацію і довів свою придатність для використання в реальних умовах діяльності транспортно-логістичних центрів, забезпечуючи автоматизацію процесів оцінювання ризиків та підтримки прийняття рішень для забезпечення ІБ ТЛЦ.

#### **Висновки до розділу 4**

У четвертому розділі проведено комплексну експериментальну перевірку розробленої інформаційної технології, верифікацію математичних моделей на реальних даних та апробацію програмного комплексу «SecureFuzzy». Отримані результати дозволяють сформулювати наступні висновки:

Експериментально підтверджено адекватність нейронечіткої моделі ANFIS через моделювання чотирьох типових сценаріїв захисту ТЛЦ. Порівняльний аналіз повної та редукованої моделей зафіксував високу збіжність результатів (відхилення  $<1,3\%$ ), що доводить коректність процедури спрощення полінома без втрати прогнозної точності. Виявлено домінуючий вплив рівня збитків (фактор  $x_3$ ), який формує понад 60% потенціалу ризику, що підтверджує пріоритетність архітектурної сегментації над нарощуванням засобів моніторингу.

Доведено високу адаптивність системи у двох аспектах – стратегічному та еволюційному. Стратегічна адаптивність реалізована через механізм переналаштування ваг у Fuzzy АНР, що дозволило моделі миттєво змінити профіль оцінювання при переході від стану «мирного часу» до умов критичних загроз.

Еволюційний – підтверджено результатами навчання на масиві з 3840 записів упродовж 22 місяців. Поетапне донавчання на даних трьох об'єктів забезпечило стабілізацію середньоквадратичної помилки на рівні  $RMSE = 0,0147$  та зростання коефіцієнта кореляції до 0,994 без ефекту «катастрофічного

забування» попереднього досвіду.

Обґрунтовано обчислювальну ефективність застосування алгоритму Rete та методу редукції правил. Встановлено, що при невеликій розмірності бази знань (до 128 правил) метод Reducing забезпечує у 3–4 рази вищу точність порівняно з класичним підходом. Використання алгоритму Rete дозволило мінімізувати час співставлення фактів, гарантуючи функціонування технології в режимі реального часу навіть за умов значного комбінаторного розширення простору станів.

Розроблено методологію прескриптивної аналітики, яка трансформує систему з аналітичного калькулятора в інтелектуального радника. Шляхом градієнтного аналізу поверхні відгуку функції ризику обґрунтовано вибір оптимальних стратегій: від «раціональної достатності» у стабільні періоди до «тотальної оборони» в умовах критичних загроз. Доведено, що системне інвестування в культуру ІБ (персонал) у 1,5 рази ефективніше за суто адміністративні заходи контролю.

Створено кросплатформний вебзастосунок «SecureFuzzy», архітектура якого базується на принципах сервіс-орієнтованої архітектури та використанні програмних модулів. Система реалізує повний цикл підтримки прийняття рішень від нечіткого налаштування ваг у Fuzzy АНР до генерації прескриптивних рекомендацій, що дозволяє менеджменту ТЛЦ обирати стратегію захисту відповідно до наявного бюджету.

Результати досліджень, наведених в розділі, опубліковані в роботах [128], [129], [130], [131], [133].

## ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-прикладне завдання створення інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ. На основі проведених теоретичних та експериментальних досліджень отримано такі результати:

1. Встановлено, що трансформація сучасних ТЛЦ у складні кіберфізичні системи зумовлює низьку дієвість наявних стандартів (NIST, ISO/IEC 27005) та класичних систем через статичність та нездатність опрацьовувати нечіткі дані. Задля реалізації гіпотези щодо поєднання експертної аналітики з обчислювальними методами сформовано трирівневу модель класифікації факторів, яка системно структурує взаємозалежність чинників ризику та є основою для розроблення моделі комплексного оцінювання.
2. Розроблено модель інтегрального оцінювання ризику інформаційної безпеки, побудовану на інтеграції експертних оцінок та системи ANFIS з поліноміальною функцією другого порядку. Об'єктивність розрахунків забезпечено методом Fuzzy АНР (інтеграція підходів Чанга та Баклі) з урахуванням впевненості фахівців, що дозволило подолати проблему «нульових ваг». Модель удосконалено впровадженням алгоритму Rete, для швидкодії у реальному часі, та символьним аналізом градієнтів, для оптимізації заходів. Дефіцит даних подолано через автоматизовану генерацію бази правил на основі виводу Mamdani з урахуванням експертної ваги та впливу факторів.
3. Експериментально підтверджено високу адаптивність та ефективність розробленої технології. Стратегічна адаптивність реалізована через механізм переналаштування ваг у Fuzzy АНР, що дозволило моделі миттєво змінити профіль оцінювання при переході від стану «мирного часу» до умов критичних загроз. Еволюційний розвиток підтверджено результатами навчання на масиві з 3840 записів, зібраних упродовж 22 місяців моніторингу трьох ТЛЦ. У

процесі адаптації (40 епох) досягнуто зниження середньоквадратичної помилки з  $RMSE = 0,109$  до  $0,0147$  та зростання кореляції з  $0,702$  до  $0,994$ . Показники точності (Accuracy = 95,2%) та повноти розпізнавання критичних станів (Recall = 0,96 для класу VH) засвідчують надійність виявлення критичних атак на логістичну інфраструктуру та високу узагальнюючу здатність моделі без ефекту втрати попереднього досвіду.

4. Обґрунтовано та реалізовано чотирирівневу багатокомпонентну сервіс-орієнтовану архітектуру, що базується на принципі поліглотної персистентності для обробки різнорідних даних безпеки. За допомогою методологій IDEF та UML розроблено комплекс моделей, що дозволило виділити функціональні модулі стратегічного аналізу, адаптивного моделювання ризиків та синтезу рекомендацій, об'єднані у вебзастосунок «SecureFuzzy». Практичне впровадження прескриптивної аналітики, яка трансформує систему з аналітичного калькулятора в інтелектуального радника шляхом градієнтного аналізу поверхні відгуку функції ризику обґрунтовує вибір оптимальних стратегій. Це дозволяє підвищити ефективність управління ризиками порівняно з наявними аналогами, забезпечуючи менеджмент ТЛЦ сучасним інструментарієм для зміцнення інформаційної безпеки стратегічних вузлів транспортної мережі України. Доведено, що системне інвестування в культуру ІБ (персонал) у 1,5 раза ефективніше за суто адміністративні заходи контролю.

Завдяки чотирирівневій багатокомпонентній сервісно-орієнтованій архітектурі та універсальності математичного ядра на базі ANFIS, запропонована інформаційна технологія може бути адаптована для інших секторів критичної інфраструктури, що характеризуються конвергенцією ІТ- та ОТ-технологій.

Подальший розвиток розробленої технології полягає у створенні модулів самостійної нейтралізації атак та безперервного спостереження за станом об'єктів. Це дозволить системі миттєво блокувати загрози без участі людини, що гарантує надійний захист логістичних центрів у реальному часі.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Bowersox D. J., Closs D. J., Cooper M. B. Supply Chain Logistics Management. New York : McGraw-Hill, 2002. 656 p. – URL: <https://www.mheducation.com/unitas/highered/sample-chapters/9780078096648.pdf>
- [2] Europlatforms EEIG. Logistics Centres: Directions for use. Brussels : Europlatforms, 2004. 64 p.
- [3] FV-2000. (1999). Quality of Freight Villages Structure and Operations. European Commission <https://cordis.europa.eu/project/id/IN97-SC.2115/pl>.
- [4] Григорак М. Ю. Інтелектуалізація ринку логістичних послуг : концепції, методологія, компетентність : монографія. Київ : Сік Груп Україна, 2017. 516 с.
- [5] Трунов, О. І., Дорош, М. С. (2023). Системи забезпечення інформаційної безпеки для транспортно-логістичних центрів. Математичне та імітаційне моделювання систем. МОДС 2022: тези доповідей Сімнадцятої міжнародної науково-практичної (С. 7-10). <http://ir.stu.cn.ua/handle/123456789/26927>.
- [6] Інформаційні системи і технології в транспортній логістиці: навч. посібник / О. Ф. Кір'янов, М. М. Мороз, В. Г. Загорянський, І. О. Кузев. Кременчук: Кременчуцький національний університет імені Михайла Остроградського, 2022. с.
- [7] Васильців Н. Трансформація та адаптація логістики до викликів в умовах воєнного стану. Економіка та суспільство. 2023. Вип. 55. DOI: <https://doi.org/10.32782/2524-0072/2023-55-78>.
- [8] Підсумки роботи транспорту України у 2024 році. Центр транспортних стратегій (ЦТС). URL: <https://cfts.org.ua> (дата звернення: 19.12.2025).
- [9] Аулін В. В., Митник М. М., Ляшук О. Л., Гевко І. Б., Цьонь О. П., Лисенко С. В., Гудь В. З., Гриньків А. В., Голуб Д. В., Бабій М. В. Формування та функціонування логістичних центрів в регіональних транспортно-логістичних системах України: монографія за заг. ред. д.т.н., проф. Ауліна В. В., д.т.н., проф. Ляшука О. Л. – Тернопіль : ФОП Паляниця В. А., 2024. – 393 с.

[10] Про мультимодальні перевезення : Закон України від 17.11.2021 № 1887-IX : за станом на 21.05.2024. URL: <https://zakon.rada.gov.ua/laws/show/1887-20#Text>.

[11] UNECE. Terminology on Combined Transport. New York ; Geneva : United Nations, 2001. 68 p.

[12] ENISA. Port Cybersecurity : Good practices for cyber security in the maritime sector. Athens : ENISA, 2019. 56 p.

[13] Дослідження потреб ключових стейкхолдерів для удосконалення логістичних операцій прикордонних регіонів в умовах воєнного часу : аналіт. звіт / В. Маргасова, М. Дорош, А. Дука, А. Приступа, О. Сакун, К. Гнедіна, О. Трунов. – Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2025. – 45 с. – DOI: [https://doi.org/10.54929/analytical\\_report-2025-01](https://doi.org/10.54929/analytical_report-2025-01).

[14] Trunov O., Dorosh M., Lytvyn S. Ensuring information security when working remotely // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 23) : зб. матеріалів VIII Міжнар. конф. (27–28 квіт. 2023, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 109–113. – URL: <http://ir.stu.cn.ua/handle/123456789/29075>.

[15] GatePoint Research. Pulse Report: Network Security Strategies. GatePoint Research. 2021. – URL: <https://www.gatepointresearch.com> (дата звернення: 19.12.2025).

[16] Трунов О., Дорош М. Систематизація підходів до оцінки ризиків інформаційної безпеки транспортно-логістичних центрів. Технічні науки та технології. 2025. № 2(40). С. 207–220. DOI: [https://doi.org/10.25140/2411-5363-2025-2\(40\)-207-220](https://doi.org/10.25140/2411-5363-2025-2(40)-207-220).

[17] Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 20th Anniversary ed. Hoboken : Wiley, 2015. 784 p.

[18] European Confederation of Institutes of Internal Auditing (ECIIA). (2024). Risk in Focus 2025: Hot topics for internal auditors. <https://www.eciia.eu/2024/09/risk->

in-focus-2025-hot-topics-for-internal-auditors/

[19] Державна служба спеціального зв'язку та захисту інформації України. (n.d.). CERT-UA минулого року опрацювала 4315 кіберінцидентів. <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv>

[20] Обертинюк, І. Л., Кареліна, О.В. (2018). Технології оцінки ризиків інформаційної безпеки відповідно до вітчизняних нормативних документів та міжнародних стандартів. Актуальні задачі сучасних технологій : зб. тез доповідей міжнар. наук.-техн. конф. Молодих учених та студентів, (С. 132-134). <https://m.tntu.edu.ua/storage/pages/00000742/Book-2-2018.pdf>

[21] Карпович, І. М., Гладка, О. М., Наконечна, Ю. А. (2020). Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки, 31(70), 5, 69–74. <https://doi.org/10.32838/2663-5941/2020.5/12>.

[22] Карпович, І., Гладка, О., Бухало, Ю. (2021). Технології моделювання і оцінки ризиків інформаційної безпеки. Технічні науки та технології, (1(23)), 62–68. [https://doi.org/10.25140/2411-5363-2021-1\(23\)-62-68](https://doi.org/10.25140/2411-5363-2021-1(23)-62-68)

[23] Потій, О., Горбенко, Ю., Замула, О. та Ісірова, К. (2021). Аналіз методів оцінки і управління ризиками кібер-і інформаційної безпеки. Радіотехніка, (206), 5-24. <https://doi.org/10.30837/rt.2021.3.206.01>

[24] Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. Encyclopedia, 1(3), 602–617. <https://doi.org/10.3390/encyclopedia1030050>

[25] Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23(3), 383–404. <https://doi.org/10.1016/j.eij.2022.03.001>

[26] Schmitz, C., Pape, S. (2020). LiSRA: Lightweight security risk assessment for decision support in information security. Computers & Security, Article 101656. <https://doi.org/10.1016/j.cose.2019.101656>

[27] Loft, P., He, Y., Yevseyeva, I., Wagner, I. (2022). CAESAR8: an agile enterprise architecture approach to managing information security risks. *Computers & Security*, 122, Article 102877. <https://doi.org/10.1016/j.cose.2022.102877>

[28] Irsheida, A., Murada, A., AlNajdawia, M., Qusefa A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, 204, 205–217. <https://doi.org/10.1016/j.procs.2022.08.025>

[29] Bernsmed, K., Bour, G., Lundgren, M., Bergström, E. (2022). An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. *Journal of Air Transport Management*, 102, Article 102223. <https://doi.org/10.1016/j.jairtraman.2022.102223>

[30] Gunes, B., Kayisoglu, G., Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, 103, Article 102196, <https://doi.org/10.1016/j.cose.2021.102196>.

[31] Liang, L., Wu, X., Deng J., Lv, X. (2022). Research on risk analysis and governance measures of open-source components of information system in transportation industry. *Procedia Computer Science*, 208:106-110. DOI: 10.1016/j.procs.2022.10.017

[32] Alfarisi, S., Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. *Bulletin of Electrical Engineering and Informatics*, 11(1), 530–540. <https://doi.org/10.11591/eei.v11i1.3241>

[33] Melnychenko, O., Ignatenko, O., Tsybulskyi, V., Degtiarova, A., Kashuba, M., & Derehuz, I. (2024). Development of a mechanism for information security risk management of transport service provision systems. *Eastern-European Journal of Enterprise Technologies*, 1(3 (127)), 27-36. DOI: <https://doi.org/10.15587/1729-4061.2024.298144>

[34] Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann.

[35] Lund, M. S., Stølen, K., & Vraalsen, F. (2011). *Model-Driven Risk Analysis: The CORAS Approach*. Springer. DOI: <https://doi.org/10.1007/978-3-642-12323-8>



[36] Agence nationale de la sécurité des systèmes d'information (ANSSI). EBIOS Risk Manager – The method. Paris : ANSSI, 2018. URL: <https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/>

[37] IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). Geneva : IEC, 2018.

[38] Memon, M.; Hameed, S. Information Security Risk Plans within Enterprise Architecture Framework//International Journal of Advanced Computer Science and Technology. 2019. T. 8, № 10. C. 82-88. URL: <https://doi.org/10.30534/ijacst/2019/018102019>

[39] IEC 61882:2016. Hazard and operability studies (HAZOP studies) – Application guide. Geneva : IEC, 2016.

[40] BSI Standard 200-2: IT-Grundschutz Methodology. Bonn : Federal Office for Information Security (BSI), 2017.

[41] UcedaVélez T., Morana M. M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken : Wiley, 2015.

[42] Shostack A. Threat Modeling: Designing for Security. Indianapolis : Wiley, 2014.

[43] Yazar Z. A Qualitative Risk Analysis and Management Tool – CRAMM. SANS Institute InfoSec Reading Room. 2002.

[44] Ministerio de Asuntos Económicos y Transformación Digital. MAGERIT – version 3.0: Methodology for Information Systems Risk Analysis and Management. Madrid, 2014.

[45] NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg : NIST, 2011.

[46] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg : NIST, 2024.

[47] NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Gaithersburg : National Institute of Standards and Technology, 2018. DOI:

<https://doi.org/10.6028/NIST.SP.800-37r2>

[48] NIST SP 800-161 Rev. 1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Gaithersburg : NIST, 2022.

[49] OWASP Foundation. Open Source Foundation for Application Security. URL: <https://owasp.org/> (дата звернення: 19.12.2025).

[50] Національний банк України. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : Лист від 03.03.2011 № 24-112/365. URL: <https://zakon.rada.gov.ua/laws/show/v0365500-11#Text>.

[51] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO/IEC, 2022.

[52] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva : ISO/IEC, 2022. URL: <https://www.iso.org/standard/80585.html>

[53] Бурячок В. Л. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник / В. Л. Бурячок, С. В. Толюпа, А. О. Аносов, В. А. Козачок, Н. В. Лукова-Чуйко. Київ : ДУТ, 2015. 345 с.

[54] Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Львів : Магнолія 2006, 2024. 320 с.

[55] Eom, S. B. (2020). Decision support systems. In Oxford Research Encyclopedia of Business and Management. Oxford University Press. <https://doi.org/10.1093/acrefore/9780190228637.013.1008>

[56] Добровольський, Є. Л. (2016). Методи і моделі інформаційно-аналітичної підтримки прийняття рішень у сфері забезпечення державної інформаційної безпеки (автореф. дис. ... канд. техн. наук: 05.13.06). Київ.

[57] Zybin, S. (2017). Subsystems and modules of decision support system. Function algorithms. Telecommunication and Information Technologies, 4(57), 58–70.

[58] Milov, O. (2019). Adaptive decision support systems for cyber security. *Advanced Information Systems*, 3(1), 131–135. <https://doi.org/10.20998/2522-9052.2019.1.22>

[59] Biswas, B., Sharmin, S., Hossain, M. A., & Alam, M. Z. (2024). Risk analysis-based decision support system for designing cybersecurity of information technology. *Journal of Business and Management Studies*, 6(5), 13–22. <https://doi.org/10.32996/jbms.2024.5.6.3>.

[60] Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A decision support system for corporations cybersecurity management. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). IEEE. <https://doi.org/10.23919/CISTI.2017.7975826>

[61] Azarova, A., Dohtieva, I., & Shyian, A. (2022). Decision support system for increasing the level of information security of the enterprise. *Information Technology and Computer Engineering*, 53(1), 12–18. <https://doi.org/10.31649/1999-9941-2022-53-1-12-18>

[62] Melnychenko, O., Ignatenko, O., Tsybulskyi, V., Degtiarova, A., Kashuba, M., & Derehuz, I. (2024). Development of a mechanism for information security risk management of transport service provision systems. *Eastern-European Journal of Enterprise Technologies*, 1(3(127)), 27–36. <https://doi.org/10.15587/1729-4061.2024.298144>

[63] Carnovale, S., & Yeniyurt, S. (2025). Balancing risk and resilience: How network structures and firm strategies mitigate supply chain disruptions. *International Journal of Physical Distribution & Logistics Management*. <https://doi.org/10.1108/IJPDLM-08-2024-0310>

[64] Sadeghi, R., Pournader, M., & Tabrizi, B. (2024). Explainable artificial intelligence and agile decision-making in supply chain cyber resilience. *Decision Support Systems*, 186, 114194. <https://doi.org/10.1016/j.dss.2024.114>

[65] Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури : Наказ Адміністрації Державної

служби спеціального зв'язку та захисту інформації України від 14.01.2025 № 17 : зареєстр. в М-ві юстиції України 07.03.2025 за № 375/43781, 376/43782. – URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-14-sichnya-2025-roku-17-pro-zatverdzhennya-metodiki-ta-kriteriyiv-i-pokaznikiv-ocinki-stanu-zakhishenosti-ob-yektiv-kritichnoyi-infrastrukturi>

[66] IEC 62443-3-2:2020. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design. Geneva : International Electrotechnical Commission, 2020. 106 p. URL: <https://webstore.iec.ch/publication/63695> (дата звернення: 11.11.2025)

[67] NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments / Joint Task Force Transformation Initiative. – Gaithersburg, MD : National Institute of Standards and Technology, 2012. – 95 p. – (Special Publication (NIST SP), 800-30 Rev. 1). – DOI: <https://doi.org/10.6028/NIST.SP.800-30r1>

[68] Taherdoost H. Analysis of simple additive weighting method (SAW) as a multi-attribute decision making technique: a step-by-step guide // Journal of Management Science and Engineering Research. – 2023. – Vol. 6, no. 1. – P. 21–24. – DOI: <https://doi.org/10.30564/jmser.v6i1.5400>

[69] Monostori L. Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP. 2014. Vol. 17. P. 9–13. – DOI: <https://doi.org/10.1016/j.procir.2014.03.115>

[70] Wang K. Logistics 4.0: Solution of Business Model and Technology. Advances in Manufacturing. 2016. Vol. 4, № 1. P. 2–17. DOI:10.2991/iwama-16.2016.13

[71] ENISA Threat Landscape 2025 : [report]. European Union Agency for Cybersecurity, 2025. 136 p. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (дата звернення: 04.02.2026).

[72] Haji S. A Hybrid Model for Information Security Risk Assessment / S. Haji, Q. Tan, R. S. Costa // International Journal of Advanced Trends in Computer Science and Engineering. – 2019. – Vol. 8, № 1.1. – P. 100–106. – DOI:

<https://doi.org/10.30534/ijatcse/2019/1981.12019> (дата звернення: 04.02.2026).

[73] Triantaphyllou E. Multi-criteria Decision Making Methods: A Comparative Study. Boston : Kluwer Academic Publishers, 2000. 278 p. (Applied Optimization ; vol. 44).

[74] Zadeh, 1965 Zadeh, L. A. (1965). Fuzzy sets. Information and Control, 8 (3), 338 – 353. [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X)

[75] Zadeh L. A. Computing with Words: Principal Concepts and Ideas. Berlin : Springer-Verlag, 2012. 312 p. DOI:10.1007/978-3-642-27473-2

[76] On Consistency in AHP and Fuzzy AHP / F. Liu [et al.] // Journal of Systems Science and Information. – 2017. – Vol. 5, no. 2. – P. 128–147.

[77] Modeling of the Information Security Risk of a Transport and Logistics Center Based on Fuzzy Analytic Hierarchy Process / O. Trunov, I. Skiter, M. Dorosh, E. Trunova, M. Voitsekhovska // Mathematical Modeling and Simulation of Systems. MODS 2023. – Cham : Springer, 2024. – Vol. 1091. – P. 306–322. – (Lecture Notes in Networks and Systems). – DOI: [https://doi.org/10.1007/978-3-031-67348-1\\_23](https://doi.org/10.1007/978-3-031-67348-1_23)

[78] Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control. IEEE Transactions on Systems, Man, and Cybernetics. 1985. Vol. 15, № 1. P. 116–132. DOI: 10.1109/TSMC.1985.6313399

[79] Wu, D., Lin, C.-T., Huang, J., Zeng, Z. (2019). On the Functional Equivalence of TSK Fuzzy Systems to Neural Networks, Mixture of Experts, CART, and Stacking Ensemble Regression. IEEE Transactions on Fuzzy Systems, 1. DOI: <http://doi.org/10.1109/tfuzz.2019.2941697>

[80] Кирик В. В. Математичний апарат штучного інтелекту в електроенергетичних системах : підручник / В. В. Кирик. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2019. – 224 с.

[81] Ross T. J. Fuzzy Logic with Engineering Applications. 4th ed. Chichester, UK : John Wiley & Sons, 2016. 614 p. URL: <https://pzs.dstu.dp.ua/logic/bibl/engineering.pdf>

[82] Vinogradova I., Podvezko V., Zavadskas E. K. Comparative Sensitivity

Analysis of Some Fuzzy AHP Methods. Mathematics. 2023. Vol. 11, no. 24. P. 4984.  
DOI: <https://doi.org/10.3390/math11244984>

[83] Ralston B., Wilson I. The Scenario Planning Handbook: Developing Strategies in Uncertain Times. Mason, Ohio : Thomson South-Western, 2006. 272 p.  
URL: <https://archive.org/details/scenarioplanning0000rals/page/n9/mode/2up>

[84] Балан В. Г. Стратегічний аналіз зовнішнього оточення підприємства з використанням нечітких даних // Економічний простір. – 2020. – № 156. – С. 109–115. – DOI: <https://doi.org/10.32782/2224-6282/156-19>

[85] CoA defuzzification method for evaluating Cpk under fuzzy environments / T.-C. Chu, K.-S. Huang, T.-M. Chang // Journal of Discrete Mathematical Sciences and Cryptography. – 2004. – Vol. 7, no. 3. – P. 271–280. – DOI: <https://doi.org/10.1080/09720529.2004.10698008>

[86] Mamdani E. H. Fuzzy Control. A Misconception of Theory and Application / E. H. Mamdani // IEEE Expert. – 1994. – Vol. 9, № 4. – P. 27–28.

[87] Jang J.-S. R. ANFIS: Adaptive-Network-Based Fuzzy Inference System / J.-S. R. Jang // IEEE Transactions on Systems, Man, and Cybernetics. – 1993. – Vol. 23, № 3. – P. 665–685. DOI:10.1109/21.256541.

[88] Atlam H. F. et al. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. Mobile Networks and Applications. 2021. Vol. 26. P. 2545–2557. DOI: <https://doi.org/10.1007/s11036-019-01214-w>

[89] Гребенник А. Алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту / А. Гребенник, О. Трунов // Технічні науки та технології. – 2025. – № 3(41). – С. 158–168. – DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-158-168](https://doi.org/10.25140/2411-5363-2025-3(41)-158-168)

[90] Трунов О. І. Загальна концепція фрактального детектора телекомунікаційного трафіка // Новітні технології у науковій діяльності і навчальному процесі : зб. тез доп. Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених (м. Чернігів, 19–20 квіт. 2023 р.). – Чернігів : НУ «Чернігівська



політехніка», 2023. – С. 114–116. URL: <http://ir.stu.cn.ua/handle/123456789/27778> (дата звернення: 05.02.2026).

[91] Trunov O., Dorosh M., Lytvyn S. Methods of detecting intrusions to computer networks transport and logistics industry // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 24) : зб. матеріалів VIII Міжнар. конф. (27–28 квіт. 2024, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 132–135. – URL: <http://ir.stu.cn.ua/handle/123456789/30881>

[92] Saaty T. L. Decision making with the analytic hierarchy process. International Journal of Services Sciences. 2008. Vol. 1, № 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590.

[93] Simulation of Strategies for Providing Information Security of the Transport and Logistics Center Based on Fuzzy Logic Methods / O. Trunov, M. Dorosh, I. Skiter, E. Trunova, M. Voitsekhovska // Mathematical Modeling and Simulation of Systems. MODS 2024. – Cham : Springer, 2025. – Vol. 1391. – P. 262–281. – (Lecture Notes in Networks and Systems). – DOI: [https://doi.org/10.1007/978-3-031-90735-7\\_21](https://doi.org/10.1007/978-3-031-90735-7_21)

[94] ДСТУ ISO/IEC 27000:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. Огляд і словник (ISO/IEC 27000:2023, IDT). – [Чинний від 2024–01–01]. – Київ : ДП «УкрНДНЦ», 2024.

[95]. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). – [Чинний від 2023–08–10]. – Київ : ДП «УкрНДНЦ», 2023.

[96] Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 31 бер. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>(дата звернення: 20.11.2025).

[97] Корченко О. Г., Романенко О. О. та ін. Основи кібербезпеки : монографія. – Київ : НАУ, 2021. – 400 с.

[98] Костюк Ю. В., Складанний П. М., Гулак Г. М. та ін. Системи захисту

інформації : підручник. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с. – URL: <https://elibrary.kubg.edu.ua/51359/>(дата звернення: 20.11.2025).

[99] Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing*. Springer, Cham. : Mathematical Modeling and Simulation of Systems. – 2020. – Vol. 1019. – P. 249-258. DOI [https://doi.org/10.1007/978-3-030-25741-5\\_25](https://doi.org/10.1007/978-3-030-25741-5_25)

[100] Геворкян А. Р. Формування основ культури інформаційної безпеки суспільства як фактор зміцнення національної безпеки // Вісник Національного університету цивільного захисту України. Серія: Державне управління. – 2021. – № 1 (14). – С. 168–177.

[101] Cyber Security Culture in organisations. – European Union Agency for Network and Information Security (ENISA), 2017. – 46 p. – URL: <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>

[102] Dorosh M., Trunov O., Sharovara O. Indirect impact factors in assessing information security risks of logistics operations in border regions // Управління проєктами у розвитку суспільства : зб. матеріалів XXII Міжнар. наук.-практ. конф. (м. Київ, 23 трав. 2025 р.). – Київ : КНУБА, 2025. – С. 20–23. – URL: <http://pmkiev.com.ua/home>

[103] Chang D. Y. Applications of the extent analysis method on fuzzy AHP / D. Y. Chang // *European Journal of Operational Research*. – 1996. – Vol. 95, № 3. – P. 649–655. – DOI: [https://doi.org/10.1016/0377-2217\(95\)00300-2](https://doi.org/10.1016/0377-2217(95)00300-2)

[104] Liu Y., Eckert C. M., Earl C. A review of fuzzy AHP methods for decision-making with subjective judgements. *Expert Systems with Applications*. 2020. Vol. 161. Article 113738.

[105] Buckley J. J. Fuzzy hierarchical analysis / J. J. Buckley // *Fuzzy Sets and Systems*. – 1985. – Vol. 17, № 3. – P. 233–247. – DOI: [https://doi.org/10.1016/0165-0114\(85\)90090-9](https://doi.org/10.1016/0165-0114(85)90090-9)



[106] Strategic analysis in the selection of sites for NPP construction based on fuzzy logic methods / I. Skiter, V. V. Derenhovskiy, O. V. Mykhailov, Ye. A. Menshenin, O. B. Savchuk, O. I. Trunov // Nuclear Power and the Environment. – 2024. – Vol. 31, no. 3. – P. 12–22. – DOI: <https://doi.org/10.31717/2311-8253.24.3.2>

[107] Taherdoost H. Analysis of simple additive weighting method (SAW) as a multi-attribute decision making technique: a step-by-step guide. Journal of Management Science and Engineering Research. – 2023. – Vol. 6, no. 1. – P. 21–24. – DOI: <https://doi.org/10.30564/jmser.v6i1.5400>

[108] Трунов О. І., Дорош М. С. Прогнозування рівня ризику інформаційної безпеки транспортно-логістичного центру // Математичне та імітаційне моделювання систем. МОДС 2023 : тези доповідей Вісімнадцятої міжнар. конф. (13–15 листоп. 2023 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2023. – С. 60–65. – URL: <http://ir.stu.cn.ua/handle/123456789/29144>

[109] Automated Expert System Knowledge Base Development Method for Information Security Risk Analysis / D. Vitkus, Z. Steckevicius, N. Goranin et al. International Journal of Computers Communications & Control. 2019. Vol. 14, issue 6. P. 743–758. DOI: 10.15837/ijccc.2019.6.3668.

[110] Nikolenko S. I. Synthetic Data for Deep Learning. Cham : Springer, 2021. 363 p. DOI: 10.1007/978-3-030-75178-4.

[111] Neuro-Symbolic Artificial Intelligence: The State of the Art / ed. by P. Hitzler, M. K. Sarker. IOS Press, 2021. DOI: 10.3233/FAIA342.

[112] Li Y., Wang S., Li X. Research on Rete algorithm improvement strategy based on Spark in big data environment. The Journal of Supercomputing. 2022. Vol. 78. P. 14225–14243. DOI: 10.1007/s11227-022-04423-z

[113] Development of a complex method for finding a solution for neuro-fuzzy expert systems / O. Sova, A. Shyshatskyi, D. Malitskyi, O. Zhuk. Eastern-European Journal of Enterprise Technologies. 2020. Vol. 6, issue 4 (108). P. 22–31. DOI: 10.15587/1729-4061.2020.216662.

[114] Development of a fuzzy risk assessment model for information security

management / Y. Zdorenko, A. Yanko, M. Myziura, N. Fesokha. Technology Audit and Production Reserves. 2025. Vol. 4, issue 2 (84). P. 71–79. DOI: 10.15587/2706-5448.2025.334954.

[115] On the Functional Equivalence of TSK Fuzzy Systems to Neural Networks, Mixture of Experts, CART, and Stacking Ensemble Regression / D. Wu, C.-T. Lin, J. Huang et al. IEEE Transactions on Fuzzy Systems. 2019. Vol. 28, issue 10. DOI: 10.1109/TFUZZ.2019.2941697.

[116] An Introduction to Statistical Learning: with Applications in R / G. James, D. Witten, T. Hastie, R. Tibshirani. 2nd ed. New York: Springer, 2021. DOI: 10.1080/24754269.2021.1980261.

[117] Лавров, В., Дудатьєв, А., & Гарнага, В. (2025). Нейро-нечітка система ANFIS для оцінювання ризику дезінформації в умовах інформаційної війни. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(28), 321–333. <https://doi.org/10.28925/2663-4023.2025.28.805>

[118] Abraham A. Neuro-fuzzy systems: state-of-the-art modeling techniques // Bio-Inspired Applications of Connectionism : International Work-Conference on Artificial Neural Networks (IWANN 2001). Berlin : Springer, 2001. P. 269–276. DOI: 10.1007/3-540-45720-8\_30.

[119] Bodyanskiy Ye., Vynokurova O., Pliss I., Peleshko D. Hybrid adaptive systems of computational intelligence and their on-line learning in IT energy management tasks // Green IT Engineering: Concepts, Models, Complex Systems Architectures, Eds. by Vyacheslav Kharchenko, Yuriy P Kondratenko, Janusz Kacprzyk, Series: Studies in Systems, Decision and Control, Book 74, Publisher: Springer. – 2017. – P. 229–244. URL: [https://link.springer.com/chapter/10.1007/978-3-319-44162-7\\_12](https://link.springer.com/chapter/10.1007/978-3-319-44162-7_12)

[120] Згуровський М. З., Зайченко Ю. П. Системи і методи штучного інтелекту. Київ : Академперіодика, 2025. 744 с. DOI: <https://doi.org/10.15407/akademperiodyka.551.744>

[121] Development of a decision support system based on expert evaluation for

the situation center of transport cybersecurity / V. Lakhno, B. Akhmetov, A. Korchenko et al. Journal of Theoretical and Applied Information Technology. 2018. Vol. 96, No. 14. P. 4530–4540. URL: <https://www.jatit.org/volumes/Vol96No14/18Vol96No14.pdf> (дата звернення: 02.03.2026).

[122] Авраменко В. С. Проектування інформаційних систем : навч. посіб. / В. С. Авраменко, А. С. Авраменко. – Черкаси : Черкаський національний університет ім. Б. Хмельницького, 2017. – 434 с.

[123] Крижановський Є. М., Ящолт А. Р., Жуков С. О. Моделювання бізнес-процесів та управління ІТ-проектами : електрон. навч. посіб. комбінованого (локального та мережного) використання. Вид. 2-ге, змін. та доповн. Вінниця : ВНТУ, 2022. 129 с.

[124] Seidl M., Scholz M., Huemer C., Kappel G. UML @ Classroom: An Introduction to Object-Oriented Modeling. Cham : Springer, 2015. 215 p. (Undergraduate Topics in Computer Science). DOI: <https://doi.org/10.1007/978-3-319-12742-2>.

[125] Шаховська Н. Б., Литвин В. В. Проектування інформаційних систем : навч. посіб. Львів : Магнолія 2006, 2023. 380 с.

[126] Трунов О. І. Архітектура інтелектуальної системи підтримки прийняття рішень для управління інформаційною безпекою транспортно-логістичних центрів / О. І. Трунов, М. С. Дорош // Наука і техніка сьогодні. Серія «Техніка». – 2025. – № 11(52). – С. 2804–2817. – DOI: [https://doi.org/10.52058/2786-6025-2025-11\(52\)-2804-2817](https://doi.org/10.52058/2786-6025-2025-11(52)-2804-2817)

[127] Туревський Д., Трунов О. Автоматизація генерації повної бази нечітких правил для моделі оцінки ризиків ІБ // Математичне та імітаційне моделювання систем. МОДС 2025 : тези доповідей Двадцятої міжнар. конф. (10–12 листоп. 2025 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 64–67. – URL: <https://ir.stu.cn.ua/handle/123456789/33857>

[128] Trunov O. I. Information and analytical system for management of logistics operations for restoration of border regions // Юність науки – 2024: соціально-

економічні та гуманітарні аспекти розвитку суспільства : зб. тез доп. XIV Міжнар. наук.-практ. конф. студентів, аспірантів і молодих вчених (м. Чернігів, 24–26 квіт. 2024 р.). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 1162–1163. – URL: <http://ir.stu.cn.ua/handle/123456789/30262>

[129] Трунов О. І., Суботін І. Л. Розробка сучасної інформаційної системи забезпечення волонтерської діяльності // Математичне та імітаційне моделювання систем. МОДС 2024 : тези доповідей Дев'ятнадцятої міжнар. наук.-практ. конф. (11–13 листоп. 2024 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 57–60. – URL: <https://ir.stu.cn.ua/handle/123456789/31373>

[130] Trunov O. I. Decision support system for ensuring information security of a transport and logistics center // Юність науки – 2025 : зб. тез доп. XIV Міжнар. наук.-практ. конф. студентів, аспірантів і молодих вчених (м. Чернігів, 23–25 квіт. 2025 р.). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 1162–1163. – URL: <http://ir.stu.cn.ua/handle/123456789/32545>

[131] Trunov O., Dorosh M. Ensuring information security in the transportation of nuclear // Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 25) : зб. матеріалів X Міжнар. конф. (25–26; 29–30 квіт. 2025, м. Славутич). – Чернігів : НУ «Чернігівська політехніка», 2025. – С. 109–113. – URL: <https://ir.stu.cn.ua/handle/123456789/33540>

[132] Nastac I. An Adaptive Retraining Technique to Predict the Critical Process Variables. Turku : Turku Centre for Computer Science, 2004. 23 p. (TUCS Technical Report; no. 616). – URL: [https://www.researchgate.net/publication/31595661\\_An\\_Adaptive\\_Retraining\\_Technique\\_to\\_Predict\\_the\\_Critical\\_Process\\_Variables](https://www.researchgate.net/publication/31595661_An_Adaptive_Retraining_Technique_to_Predict_the_Critical_Process_Variables)

[133] Трунов О. І., Дорош М. С. Генетичний алгоритм в логістиці: оптимізація маршрутів // Математичне та імітаційне моделювання систем. МОДС 2024 : тези доповідей Дев'ятнадцятої міжнар. наук.-практ. конф. (11–13 листоп. 2024 р., м. Чернігів). – Чернігів : НУ «Чернігівська політехніка», 2024. – С. 64–67.

– URL: <https://ir.stu.cn.ua/handle/123456789/31373>

[134] Nielsen Norman Group. Usability 101: Introduction to Usability. 2024.  
URL: <https://www.nngroup.com/articles/usability-101-introduction-to-usability/> (дата  
звернення: 07.03.2026).

## ДОДАТКИ

## Додаток А

## Свідоцтво про реєстрацію авторського права

**УКРАЇНА**



**СВІДОЦТВО**

**про реєстрацію авторського права на твір**

**№ 143390**

**Комп'ютерна програма «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів»**  
(вид, назва твору)

**Автор (співавтори) Трунов Олексій Ігорович, Дорош Марія Сергіївна**  
(прізвище, ім'я, по батькові (за наявності), посядлом (за наявності))

**Авторські майнові права належать повністю Національний університет «Чернігівська політехніка», вул. Шевченка, 95, м. Чернігів, 14030**  
(прізвище, ім'я, по батькові (за наявності) фізичної особи / найменування юридичної особи, адреса)

Дата реєстрації 23 лютого 2026 р.

Директор Державної організації  
«Український національний  
офіс інтелектуальної власності  
та інновацій»

  
**Олена ОРЛЮК**

  
М.П.



НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ  
ДЕРЖАВНА ОРГАНІЗАЦІЯ  
«УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ ТА ІННОВАЦІЙ»  
(УКРНОІВІ)

Оригіналом цього документа є електронний документ з ідентифікатором:

**CR4056230226**

Для отримання оригіналу документа необхідно:

1. Перейти за посиланням: <https://sis.nipo.gov.ua>
2. Обрати пункт меню «СЕРВІСИ» «Отримати оригінал документу».
3. Вказати ідентифікатор документу та натиснути на кнопку «Завантажити».

Цей ідентифікатор є конфіденційною інформацією,  
не повідомляйте його нікому



## Додаток Б

## Акти та довідки про впровадження результатів дисертаційного дослідження

№ 26/03 від 26.03.2026 р.

ЗАТВЕРДЖУЮ  
Директор ТОВ «СІВЕРТРАНС»Юрій ЛИТВИНЕНКО  
«26» березня 2026 року

## АКТ

про впровадження наукових результатів, що отримані аспірантом  
Національного університету «Чернігівська політехніка»  
ТРУНОВИМ Олексієм Ігоровичем  
при виконанні дисертаційної роботи на здобуття ступеня доктора філософії

Комісія у складі:

Голова комісії – директор ТОВ «СІВЕРТРАНС» – Юрій ЛИТВИНЕНКО

Члени комісії:

- юристконсульт – Віктор ВІКТОРОВСЬКИЙ;
- логіст – Юлія ОМЕЛЬЯНЕНКО.

розглянула реалізацію наукових результатів, отриманих ТРУНОВИМ Олексієм Ігоровичем у ході проведення дослідження на тему «Інформаційна технологія підтримки прийняття рішень при забезпеченні інформаційної безпеки транспортно-логістичного центру».

Комісія встановила:

1. Під час розроблення інформаційної технології підтримки прийняття рішень при забезпеченні інформаційної безпеки транспортно-логістичного центру особисто ТРУНОВИМ О. І.:

- сформовано трирівневу ієрархічну модель класифікації факторів, що впливають на рівень ризику інформаційної безпеки (ІБ) транспортно-логістичного центру (ТЛЦ), яка дозволяє системно структурувати та враховувати взаємозалежність різномірних чинників, специфічних для кіберфізичних систем транспортно-логістичних центрів;
- запропоновано модель та її програмну реалізацію інтегрального оцінювання ризику інформаційної безпеки, яка базується на інтеграції експертної нечіткої оцінки та адаптивної нейронечіткої системи висновків (ANFIS) з поліноміальною функцією другого порядку, що

забезпечує підвищення точності оцінки у динамічному середовищі, та підтримку прийняття рішень з ІБ ТЛЦ.

2. Отримані наукові результати дозволяють

- забезпечити високу точність розпізнавання загроз. Експериментально підтверджено показники точності на масиві з 3840 реальних прецедентів (RMSE = 0,0147, Accuracy = 95,2%, Recall = 0,96);
- проводити прескриптивну оптимізацію стратегій захисту. Шляхом градієнтного аналізу поверхні відгуку функції ризику система дозволяє обирати найкращий вектор контрзаходів при наявних ресурсних обмеженнях.

Економічний ефект від впровадження не розраховувався через наукове призначення результатів.

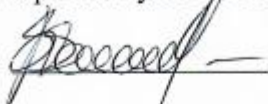
Акт складено для подання у спеціалізовану вчену раду.

Голова комісії  
директор ТОВ «СІВЕРТРАНС» – Юрій ЛИТВИНЕНКО.



Члени комісії:

юрисконсульт – Віктор ВІКТОРОВСЬКИЙ;



логіст – Юлія ОМЕЛЬЯНЕНКО.



МІНІСТЕРСТВО ОСВІТИ І  
НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

вул. Шевченка, 95, Чернігів, 14030,  
Україна



тел. +38(0462) 665-103;  
факс +38(0462) 665-105  
E-mail: [estu@stu.cn.ua](mailto:estu@stu.cn.ua)  
[www.stu.cn.ua](http://www.stu.cn.ua)  
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND  
SCIENCE OF UKRAINE

CHERNIHIV POLYTECHNIC  
NATIONAL UNIVERSITY

95, Shevchenko str., Chernihiv, 14030,  
Ukraine

*24.03.2026 № 204/08 - 512*

На № \_\_\_\_\_ від \_\_\_\_\_

### ДОВІДКА ПРО ВПРОВАДЖЕННЯ

результатів дисертаційної роботи Трунова Олексія Ігоровича  
«Інформаційна технологія підтримки прийняття рішень при забезпеченні  
інформаційної безпеки транспортно-логістичного центру»,  
представленої на здобуття вченого ступеня доктора філософії  
зі спеціальності F3 (122) – Комп'ютерні науки

Результати наукових досліджень, викладені в дисертаційній роботі Трунова О.І., що включають методику експертного інтегрального оцінювання рівня ризику інформаційної безпеки з урахуванням нечіткої ваги факторів та рівня впевненості експертів, методику стратегічного аналізу та адаптивну нейро-нечітку модель для оперативного моніторингу станів транспортно-логістичних центрів в умовах відсутності початкових даних та високої невизначеності, були використані при виконанні проекту прикладного дослідження № 0124U000696 «Розробка інформаційно-аналітичної системи управління логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки». За результатами роботи отримано свідоцтво на реєстрацію авторського права на комп'ютерну програму №143390 «Гібридна інформаційно-аналітична система оцінки ризиків інформаційної безпеки транспортно-логістичних центрів».

Проректор з наукової роботи

к.т.н., доцент



Анатолій ПРИСТУПА

Войцеховська (0462) 655 115

Система управління якістю сертифікована  
за ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT)

The quality management system is certified according to the  
ISO 9001:2015



МІНІСТЕРСТВО ОСВІТИ І  
НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

вул. Шевченка, 95, Чернігів, 14030,  
Україна



тел. +38(0462) 665-103;  
факс +38(0462) 665-105  
E-mail: [estu@stu.cn.ua](mailto:estu@stu.cn.ua)  
[www.stu.cn.ua](http://www.stu.cn.ua)  
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND  
SCIENCE OF UKRAINE

CHERNIHIV POLYTECHNIC  
NATIONAL UNIVERSITY

95, Shevchenko str., Chernihiv, 14030,  
Ukraine

23.03.2016 № 102/02-54  
На № \_\_\_\_\_ від \_\_\_\_\_

### ДОВІДКА ПРО ВПРОВАДЖЕННЯ

результатів дисертаційної роботи Трунова Олексія Ігоровича  
«Інформаційна технологія підтримки прийняття рішень при забезпеченні  
інформаційної безпеки транспортно-логістичного центру»,  
представленої на здобуття вченого ступеня доктора філософії зі  
спеціальності F3 (122) – Комп'ютерні науки.

Результати наукових досліджень, викладені в дисертаційній роботі  
Трунова О. І., використовуються на кафедрі інформаційних технологій та  
програмної інженерії при проведенні лекцій та лабораторних робіт з освітніх  
компонент «Операційні системи. Частина 1», «Системи штучного інтелекту»,  
«Кодування та захист інформації», «Системи захисту обчислювальних мереж»,  
«Моделювання, аналіз та інструментальні засоби інформаційної безпеки» в  
процесі навчання бакалаврів та магістрів спеціальності F2 (121) – Інженерія  
програмного забезпечення та з дисципліни «Моделі та методи інформаційної  
безпеки інженерії програмного забезпечення» в процесі навчання аспірантів  
спеціальності F2 (121) – Інженерія програмного забезпечення.

Перший проректор  
д.е.н., професор



Сергій ШКАРЛЕТ

Білоус 093 2 570 570

Система управління якістю сертифікована  
за ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT)

The quality management system is certified according to the  
ISO 9001:2015

## Додаток В

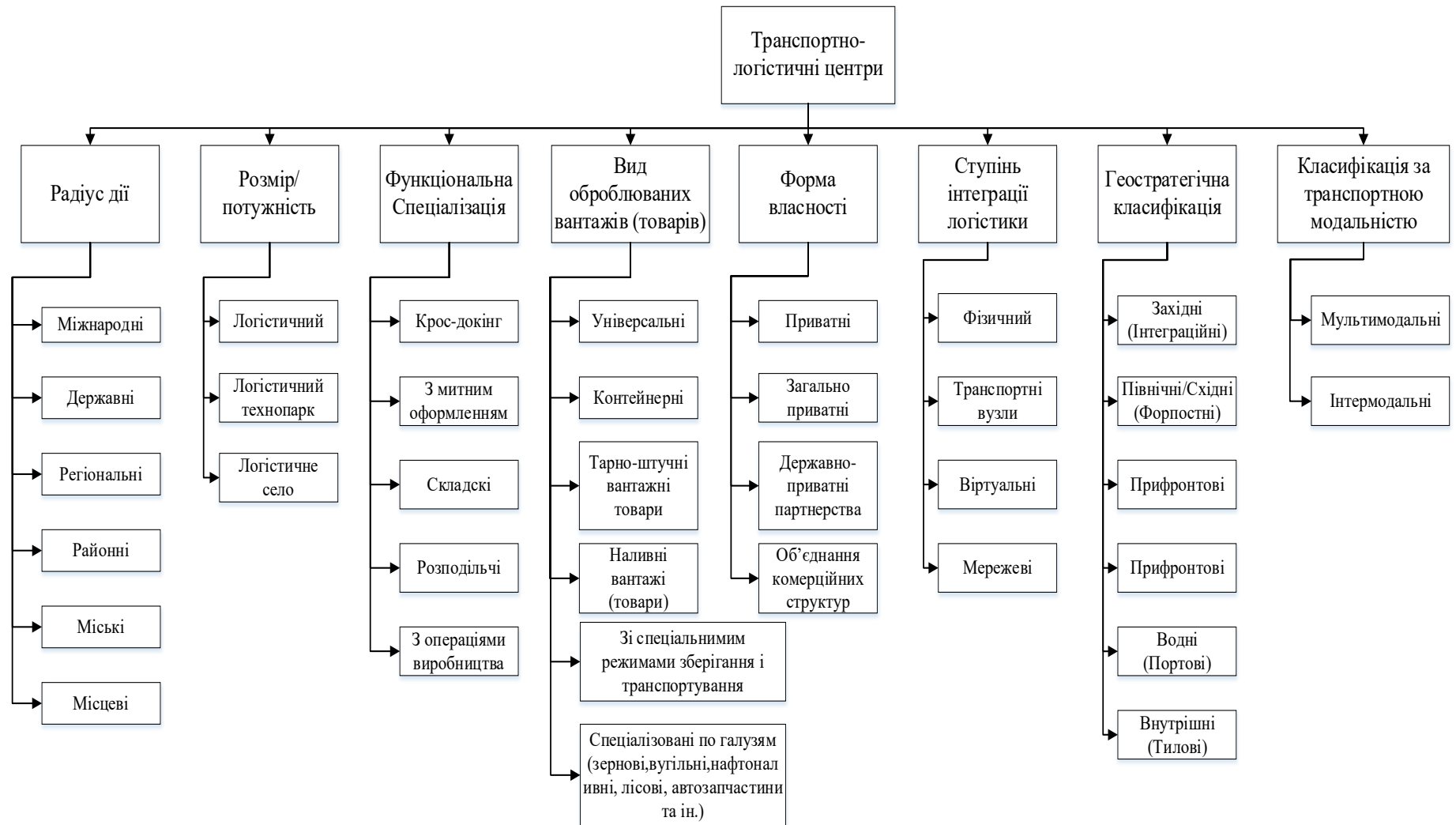


Рисунок 1 – Багатовимірна класифікація ТЛЦ для аналізу ризиків інформаційної безпеки

## Додаток Г

Таблиця Г.1 – Агрегована нечітка матриця парних порівнянь факторів ризику *A, P, Los, Con, F, Cul*

Factor	<i>A</i>			<i>P</i>			<i>Los</i>			<i>Con</i>			<i>F</i>			<i>Cul</i>		
	<i>l</i>	<i>m</i>	<i>u</i>	<i>l</i>	<i>m</i>	<i>u</i>	<i>l</i>	<i>m</i>	<i>u</i>	<i>l</i>	<i>m</i>	<i>u</i>	<i>l</i>	<i>m</i>	<i>u</i>	<i>l</i>	<i>m</i>	<i>u</i>
<i>A</i>	1	1	1	1/3	1/2	1	1/4	1/3	1/2	2	3	4	1	2	3	1	2	3
<i>P</i>	1	2	3	1	1	1	1/3	1/2	1	4	5	6	1	2	3	1	2	3
<i>Los</i>	2	3	4	1	2	3	1	1	1	5	6	7	2	3	4	2	3	4
<i>Con</i>	1/4	1/3	1/2	1/6	1/5	1/4	1/7	1/6	1/5	1	1	1	1/4	1/3	1/2	1/4	1/3	1/2
<i>F</i>	1/3	1/2	1	1/3	1/2	1	1/4	1/3	1/2	2	3	4	1	1	1	1	2	3
<i>Cul</i>	1/3	1/2	1	1/3	1/2	1	1/4	1/3	1/2	2	3	4	1/3	1/2	1	1	1	1

Таблиця Г.2 – Ієрархічна модель факторів ризику ІБ ТЛЦ та їх вагові коефіцієнти

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
хА Рівень цінності активів (0.155)	А1. Дані (0.40)	А1.1. Дані про вантажі (0.18)	Найцінніший актив. Витік цих даних – це пряма передача ворогу розвідданих про переміщення військової техніки та гуманітарної допомоги, що призводить до зриву операцій та фізичного знищення вантажів.
		А1.2. Дані про маршрути (0.15)	
		А1.3. Дані клієнтів (0.18)	Компрометація підриває економічну стійкість та довіру міжнародних партнерів (гуманітарних фондів), що критично для відновлення.
		А1.4. Фінансові дані (0.19)	
		А1.5 Інформація про запаси (0.15)	Дані про запаси (на кшталт, пального, продовольства) є стратегічною цінністю для ворога.
		А1.6 Дані про дотримання норм (0.15)	Необхідні для міжнародних перевезень та митниці.
	А2. Системи (0.35)	А2.1. TMS (система управління транспортом) (0.18)	Це кіберфізичні (ІТ/ОТ) системи. Їх злам (на кшталт., Ransomware або АРТ) – це не просто втрата даних, а фізичний саботаж: зупинка складів, блокування відвантажень,
		А2.2. WMS (система управління складом) (0.18)	

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
		A2.3. GPS/GLONASS (0.15)	перенаправлення транспорту у небезпечні зони.
		A2.4. ERP (Система планування ресурсів) (0.20)	"Мозок" та "нервова система" ТЛЦ. Злам ERP паралізує бізнес. Злам систем зв'язку (АТС) або API (на кшталт, з митницею) зупиняє координацію та міжнародні перевезення.
		A2.5. Системи зв'язку (диспетчери) (0.15)	
		A2.6 Системи EDI/API (0.14)	
	A3. Репутація компанії (0.25)	A3.1. Довіра клієнтів/партнерів (0.30)	В умовах війни репутація ТЛЦ як надійного партнера, здатного доставити вантаж безпечно та вчасно попри ризики, є ключовим фактором виживання бізнесу та отримання оборонних та гуманітарних контрактів
		A3.2. Здатність виконувати зобов'язання (0.25)	
		A3.3. Фінансова стабільність (0.15)	
		A3.4. Надійність для державних/гуманітарних контрактів (0.20)	
		A3.5 Прозорість для міжнародних партнерів (0.10)	
хР Ймовірність загроз (0.222)	P1 Кібератаки (0.70)	P1.1. Соціальна інженерія (0.20)	Ймовірність атак державних акторів є максимальна. Їхня мета – не викуп, а параліч логістики. Атаки на ланцюг поставок (злам постачальника TMS/WMS) є вкрай імовірним вектором.
		P1.2. Атаки на ланцюг поставок (0.20)	
		P1.3. Атаки на вебзастосунки та БД (0.15)	
		P1.4. Атаки на хмарні інфраструктури (0.10)	
		P1.5. АРТ-атаки (державні актори) (0.25)	Ймовірність є максимальною. Ворожі спецслужби цілеспрямовано атакують ТЛЦ як критичну інфраструктуру. Їхня мета – не викуп, а параліч логістики та фізичний саботаж.
		P1.6. Атаки на ОТ-системи (кіберфізичні) (0.10)	
	P2. Людський фактор (0.30)	P2.1. Соціальна інженерія (0.40)	Підвищений стрес персоналу збільшує недбалість. Соціальна інженерія стає більш витонченою (на кшталт, фейкові запити "від військових"). Ризик завербованих інсайдерів (зрадників) зростає
		P2.2. Недбалість та помилки (0.25)	
		P2.3. Внутрішні зловмисники (0.15)	

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
			експоненційно.
		P2.4. Фізична та психологічна втома (0.15)	В умовах війни (повітряні тривоги, стрес, робота 24/7) втома персоналу є окремою загрозою, що призводить до недбалості та помилок, які не пов'язані з некомпетентністю.
		P2.5. Брак кваліфікації для нових загроз (0.05)	Не просто недбалість, а відсутність у персоналу знань, як реагувати на специфічні воєнні загрози (наприклад, виявлення GPS-маячків, робота в умовах РЕБ)
xL Рівень збитків (0.354)	L1. Операційні збитки (0.45)	L1.1. Повна зупинка логістики (WMS/TMS) (0.40)	Найкритичніший збиток для ТЛЦ під час війни. Це не просто втрата грошей, а зрив постачання для Сил Оборони, гуманітарних місій та зупинка відновлення територій.
		L1.2. Параліч операцій (0.20) (втрата зв'язку)	
		L1.3. Втрата/пошкодження вантажів (0.15)	
		L1.4. Втрата цілісності даних (0.15)	Катастрофічний збиток. Це ситуація, коли ТЛЦ не може довіряти своїм системам (WMS/TMS) – невідомо, де який вантаж, куди його везти. Це гірше, ніж просто зупинка – система бреше.
		L1.5. Втрата ключових маршрутів/вузлів (0.10)	Збиток, коли внаслідок кібератаки (наприклад, злам GPS) транспорт потрапляє в зону ураження, і компанія втрачає не лише вантаж, а й безпечний маршрут, який тепер скомпрометований.
	L2. Фінансові збитки (0.25)	L2.1. Втрата доходів (0.30) (через простої)	Прямі фінансові втрати, які є особливо болючими під час економічної кризи, спричиненої війною. Особливий ризик (L22). кібератака (витік даних про місцезнаходження) призводить до фізичного удару (ракета, дрон) та знищення складів, транспорту, пального
		L2.2. Пряме фізичне знищення активів (0.30)	
		L2.3. Витрати на відновлення (включаючи	



Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
		викуп) (0.20)	
		L2.4. Штрафи та компенсації (контракти) (0.10)	
		L2.5. Підвищення витрат на страхування (0.10)	Після інциденту ІБ страхові тарифи (кібер- та воєнні ризики) для ТЛЦ зростають до космічних рівнів, роблячи бізнес нерентабельним.
	L3. Репутаційні збитки (0.20)	L3.1. Втрата довіри клієнтів/партнерів (0.30)	Втрата репутації "надійного" партнера в умовах війни може призвести до втрати ключових міжнародних та державних контрактів L33.
		L3.2. Зниження конкурентоспроможності (0.20)	
		L3.3. Втрата державних/оборонних контрактів (0.25)	Інцидент ІБ призведе до негайного розриву контрактів з Міністерством оборони та іншими силовими відомствами.
		L3.4. Потрапляння до "чорних списків" партнерів (0.15)	Міжнародні партнери (наприклад, гуманітарні місії ООН) внесуть ТЛЦ до списку "ненадійних" (скомпрометованих) компаній.
		L3.5. Звинувачення у сприянні ворогу (0.10)	Інцидент (витік даних) може трактуватися як сприяння ворогу (L35), що є катастрофою.
	L4. Безпека та правові наслідки (0.10)	Los4.1. Загроза життю і здоров'ю (0.40)	Найкатастрофічніший наслідок. Атака на ОТ/GPS може відправити водія в зону ураження (L41). В умовах воєнного стану недбалість, що призвела до витіку даних про військові вантажі, може бути кваліфікована СБУ як кримінальний злочин (L42).
		Los4.2. Кримінальна відповідальність (недбалість, держзрада) (0.25) Судові позови / Розслідування (0.15)	
		L4.3. Судові позови / Розслідування (0.15)	
		L4.4. Втрата ліцензій (митного брокера) (0.15)	Втрата спеціальних ліцензій (наприклад, митного брокера, перевезення небезпечних вантажів) через доведену невідповідність вимогам

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
			безпеки.
		L4.5. Екологічні збитки (0.05)	Наслідок кіберфізичної атаки, що призвела до аварії (наприклад, витік пального, хімікатів), з відповідними штрафами.
xCon Рівень контролю (0.045)	Con1. Технічні засоби ( 0.60)	Con1.1. Системи моніторингу та управління доступом (0.25) (SIEM, IAM, MFA, Сегментація)	Пріоритет на виявленні (SIEM) та стійкості (Backups). В умовах війни неможливо запобігти 100% атак (особливо APT), тому критично важливо їх вчасно виявити та швидко відновитися.
		Con1.2. Засоби захисту периметру та кінцевих точок (0.20) (NGFW, IDS/IPS, EDR)	
		Con1.3. Засоби безперервності та конфіденційності (0.20) (Резервне копіювання, Шифрування, VPN)	
		Con1.4. Захист ОТ- сегменту (0.15)	Наявність окремих засобів моніторингу та захисту для кіберфізичних систем (AS/RS, SCADA, промислові контролери), які не бачить класичний EDR.
		Con1.5. Резервні/захищені канали зв'язку (0.10)	Наявність та готовність резервних каналів (наприклад, Starlink, супутниковий зв'язок) на випадок руйнування наземної інфраструктури або роботи РЕБ.
		Con1.6. Системи фізичної ІБ (0.10)	Технічні засоби фізичної безпеки (СКУД, "розумний" відеонагляд, датчики руху), інтегровані з SIEM.
	Con2. Організаційні заходи (0.40)	Con2.1. Політики та Регламенти надзвичайних ситуацій (НС) (0.30)	Регламенти дій у (НС) (на кшталт, процедури при обстрілах, втраті зв'язку, евакуації ЦОД) та фізична безпека.
		Con2.2. Управління ризиками ланцюга поставок (SCRM) (0.20)	Наявність формалізованих процедур аудиту та контролю ІТ-постачальників (ПЗ для WMS/TMS) та логістичних

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
		Con2.3. Фізична безпека (0.10)	партнерів.
		Con2.4. Аудит та Управління вразливостями (0.15)	Регулярні аудити, сканування вразливостей та своєчасне управління патчами (оновленнями), особливо для критичних систем (WMS, TMS) та мережевого обладнання, включаючи ПЗ АТС.
		Con2.5. Перевірка персоналу (Background checks) (0.15)	Наявність процедур перевірки персоналу (особливо нових та тих, хто має високі привілеї) на зв'язки з ворогом або криміналом.
		Con2.6. Процедури взаємодії з державними органами (0.10)	Чіткий регламент, хто і як має право надавати інформацію на запити військових/СБУ, щоб запобігти соціальній інженерії.
xF Рівень витрат (0.125)	F1 Інвестиції в персонал та процеси (OpEx) (0.60)	F1.1. Технічне обслуговування та супровід (включаючи ЗП фахівців) (0.40)	В умовах браку кадрів та постійного стресу, інвестиції у кваліфікованих фахівців (ЗП) та регулярне навчання (адаптація до нових загроз) є важливішими за одноразову закупівлю "заліза".
		F1.2. Навчання та підвищення кваліфікації (0.25)	
		F1.3. Проведення аудитів та тестування (0.15)	
		F1.4. Закупівля даних Threat Intelligence (0.10)	Постійні витрати на підписку на сервіси, що надають актуальні індикатори компрометації (IoC) та дані про тактики АРТ-груп, що атакують Україну.
		F1.5. Витрати на страхування (0.10)	Постійні операційні витрати на покриття полісів кібер- та воєнних ризиків, які є надзвичайно високими.
	F2. Інвестиції в технології (CapEx) (0.40)	F2.1. Закупівля ПЗ/АЗ безпеки (SIEM, EDR, Backups) (0.30)	Пріоритет надається технологіям виявлення/реагування (SIEM, EDR) та забезпечення стійкості (резервне копіювання), що є критичним в умовах війни.
		F2.2. Інфраструктура відновлення (0.20)	
		F2.3. Створення	Капітальні витрати на

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
		резервного (гео- розподіленого) ЦОД (0.20)	створення "дзеркала" інфраструктури у безпечному регіоні (наприклад, на заході України або в хмарі ЄС).
		F2.4. Автономне/резервне живлення (0.15)	Закупівля та встановлення потужних генераторів, ДБЖ, сонячних панелей для забезпечення роботи ІТ-систем під час блекаутів.
		F2.5. Фізичне укріплення ЦОД (0.15)	Капітальні інвестиції у фізичний захист серверних приміщень (наприклад, перенесення у підвал, захист від уламків).
xCul Рівень культури ІБ ( 0.099)	Cul1. Позиція адміністрації (0.35)	Cul1.1. Включення ІБ в бізнес-стратегію (0.40)	«Tone at the top» – найважливіший аспект. Якщо керівництво ТЛЦ в умовах війни не вважає ІБ пріоритетом (економить на безпеці заради операцій), жодні заходи не будуть ефективними.
		Cul1.2. Виділення адекватних ресурсів (0.30)	
		Cul1.3. Особиста участь (tone at the top) (0.20)	
		Cul1.4 Політика нульової толерантності (0.10)	
	Cul2. ІБ- компетенції працівників (0.30)	Cul2.1. Навчання диспетчерів (соціальна інженерія) (0.30)	"Людський фаєрвол". В умовах війни посилюється соціальна інженерія (напр., фейкові накази "від військових"). Диспетчери є найбільш вразливою ланкою.. Практична перевірка знань персоналу.
		Cul2.2. Регулярні тренінги (фішинг, паролі) (0.25)	
		Cul2.3 Тестування (фішинг-симуляції) (0.20)	
		Cul2.4. Програми підвищення обізнаності (0.15)	
		Cul2.5. Навчання з реагування на НС (воєнні) (0.10)	
	Cul3. Контроль над діями ( 0.15)	Cul3.1. Дотримання політик (0.30)	Культура – це не лише знання, а й виконання правил. Оцінює, наскільки політики ІБ є частиною щоденної рутини, а не "папірцем", особливо в стресових умовах.
		Cul3.3. Моніторинг дій користувачів (0.25)	

Рівень 1 Фактор (вага)	Рівень 2 Підфактор (вага)	Рівень 3 Елемент/Під- підфактор( вага)	Деталізація та обґрунтування (контекст ТЛЦ)
			Контроль за привілейованими акаунтами, виявлення аномалій.
		Cul3.2. Політики чистого столу/блокування (0.20)	Оцінює, наскільки суворо та постійно співробітники (особливо диспетчери, оператори WMS, офісний персонал) дотримуються базових правил фізичної та цифрової гігієни: блокування робочих станцій під час відсутності ( <i>Win+L</i> ) та прибирання робочого місця від конфіденційних документів (накладних, маршрутних листів, стікерів з паролями).
		Cul3.4. Система мотивації (бонуси/штрафи) (0.15)	Впровадження KPI з ІБ для ключового персоналу.
		Cul3.5. Автоматизований контроль (0.10)	Використання DLP-систем для контролю виконання політик.
	Cul4. Комунікації ( 0.10)	Cul4.1. Механізм повідомлення про інциденти (0.40)	Забезпечує зворотний зв'язок. Позитивна культура заохочує співробітників негайно повідомляти про підозрілі події, не боячись покарання.
		Cul4.2. Анонімні канали "гарячої лінії" (0.20)	Можливість анонімно повідомити про інсайдера чи зловживання.
		Cul4.3. Зворотний зв'язок (що зроблено) (0.20)	Персонал має бачити, що на його повідомлення реагують.
		Cul4.4. Інформування про нові загрози (0.20)	Регулярні дайджести про актуальні фішингові кампанії.
	Cul5. Емоційний клімат ( 0.10)	Cul5.1. Загальний рівень задоволеності (1)	Високий стрес через війну підвищує недбалість. Токсичний емоційний клімат (невиплати ЗП, погані умови) підвищує ризик завербованих інсайдерів.

Таблиця Г.3 – Вхідні дані експертного опитування (лінгвістична оцінка, другий рівень)

Фактори	нечітке значення ваги підфактору, $\tilde{w}_i^X$			лінгвістична оцінка рівня впевненості експерта, $\tilde{p}_i^X$	лінгвістичне значення підфактору, $\tilde{x}_i$
	$v_{1i}^X$	$v_{2i}^X$	$v_{3i}^X$		
Рівень цінності активів, $A$					
$A_1$	0,2832	0,4915	0,8004	$H$	$Lt$
$A_2$	0,1809	0,3060	0,5496	$H$	$Lt$
$A_3$	0,0719	0,1249	0,2185	$H$	$Lt$
$A_4$	0,0494	0,0777	0,1396	$H$	$Lt$
Ймовірність реалізації загрози через наявні вразливості, $P$					
$P_1$	0,25	0,38	0,27	$H$	$Lt$
$P_2$	0,2127	0,2400	0,2300	$H$	$Lt$
$P_3$	0,1504	0,1824	0,2300	$H$	$Lt$
$P_4$	0,1616	0,2019	0,2735	$H$	$Lt$
Рівень збитків від загрози, $Los$					
$Los_1$	0,1789	0,3675	0,7555	$H$	$Lt$
$Los_2$	0,0627	0,1135	0,1905	$H$	$Lt$
$Los_3$	0,0920	0,2164	0,4630	$H$	$Lt$
$Los_4$	0,0627	0,1135	0,2039	$H$	$Lt$
$Los_5$	0,0651	0,1191	0,2589	$H$	$Lt$
$Los_6$	0,0985	0,0701	0,1396	$H$	$Lt$
Рівень контролю інформаційних ресурсів, $Con$					
$Con_{1_1}$	0,2014	0,2600	0,3713	$H$	$Mo$
$Con_2$	0,2905	0,3275	0,3713	$H$	$Mo$
$Con_3$	0,2905	0,4126	0,5355	$H$	$Mo$
Рівень витрат на створення та експлуатацію системи ІБ, $F$					
$F_1$	0,3272	0,5127	0,7820	$H$	$Mo$
$F_2$	0,0696	0,0989	0,2023	$H$	$Mo$
$F_3$	0,0527	0,0989	0,1533	$H$	$Mo$
$F_4$	0,0940	0,1907	0,3404	$H$	$Mo$
$F_5$	0,0696	0,0989	0,1533	$H$	$Mo$
Рівень культури інформаційної безпеки, $Cul$					
$Cul_1$	0,2157	0,3940	0,6907	$H$	$Mo$
$Cul_2$	0,0866	0,1240	0,2101	$H$	$Mo$
$Cul_3$	0,0866	0,1240	0,2101	$H$	$Mo$
$Cul_4$	0,0866	0,1240	0,2101	$H$	$Mo$
$Cul_5$	0,1143	0,2341	0,3745	$H$	$Mo$

Таблиця Г.4 – Вхідні дані експертного опитування (нечітка оцінка, другий рівень)

Фактори	нечітке значення ваги підфактору, $\tilde{w}_i^X$			нечітка оцінка рівня впевненості експерта, $\tilde{p}_i^X$			нечіткі значення підфактору, $\tilde{x}_i$		
	$v_{1i}^X$	$v_{2i}^X$	$v_{3i}^X$	$p_{1i}^X$	$p_{2i}^X$	$p_{3i}^X$	$x_{1i}$	$x_{2i}$	$x_{3i}$
Рівень цінності активів, $A$									
$A_1$	0,2832	0,4915	0,8004	0,55	0,7	0,85	-0,5	-0,33	-0,17
$A_2$	0,1809	0,3060	0,5496	0,55	0,7	0,85	-0,5	-0,33	-0,17
$A_3$	0,0719	0,1249	0,2185	0,55	0,7	0,85	-0,5	-0,33	-0,17
$A_4$	0,0494	0,0777	0,1396	0,55	0,7	0,85	-0,5	-0,33	-0,17
Ймовірність реалізації загрози через наявні вразливості, $P$									
$P_1$	0,25	0,38	0,27	0,55	0,7	0,85	-0,5	-0,33	-0,17
$P_2$	0,2127	0,2400	0,2300	0,55	0,7	0,85	-0,5	-0,33	-0,17
$P_3$	0,1504	0,1824	0,2300	0,55	0,7	0,85	-0,5	-0,33	-0,17
$P_4$	0,1616	0,2019	0,2735	0,55	0,7	0,85	-0,5	-0,33	-0,17
Рівень збитків від загрози, $Los$									
$Los_1$	0,1789	0,3675	0,7555	0,55	0,7	0,85	-0,5	-0,33	-0,17
$Los_2$	0,0627	0,1135	0,1905	0,55	0,7	0,85	-0,5	-0,33	-0,17
$Los_3$	0,0920	0,2164	0,4630	0,55	0,7	0,85	-0,5	-0,33	-0,17
$Los_4$	0,0627	0,1135	0,2039	0,55	0,7	0,85	-0,5	-0,33	-0,17
$Los_5$	0,0651	0,1191	0,2589	0,55	0,7	0,85	-0,5	-0,33	-0,17
$Los_6$	0,0985	0,0701	0,1396	0,55	0,7	0,85	-0,5	-0,33	-0,17
Рівень контролю інформаційних ресурсів, $Con$									
$Con_{11}$	0,2014	0,2600	0,3713	0,55	0,7	0,85	0,33	0,50	0,6
$Con_2$	0,2905	0,3275	0,3713	0,55	0,7	0,85	0,33	0,50	0,6
$Con_3$	0,2905	0,4126	0,5355	0,55	0,7	0,85	0,33	0,50	0,6
Рівень витрат на створення та експлуатацію системи ІБ, $F$									
$F_1$	0,3272	0,5127	0,7820	0,55	0,7	0,85	0,33	0,50	0,6
$F_2$	0,0696	0,0989	0,2023	0,55	0,7	0,85	0,33	0,50	0,6
$F_3$	0,0527	0,0989	0,1533	0,55	0,7	0,85	0,33	0,50	0,6
$F_4$	0,0940	0,1907	0,3404	0,55	0,7	0,85	0,33	0,50	0,6
$F_5$	0,0696	0,0989	0,1533	0,55	0,7	0,85	0,33	0,50	0,6
Рівень культури інформаційної безпеки, $Cul$									
$Cul_1$	0,2157	0,3940	0,6907	0,55	0,7	0,85	0,33	0,50	0,6
$Cul_2$	0,0866	0,1240	0,2101	0,55	0,7	0,85	0,33	0,50	0,6
$Cul_3$	0,0866	0,1240	0,2101	0,55	0,7	0,85	0,33	0,50	0,6
$Cul_4$	0,0866	0,1240	0,2101	0,55	0,7	0,85	0,33	0,50	0,6
$Cul_5$	0,1143	0,2341	0,3745	0,55	0,7	0,85	0,33	0,50	0,6

Таблиця Г.5 – Нормалізовані дані експертного опитування (нечітка оцінка, другий рівень)

Фактори	нормалізоване нечітке значення ваги підфактору, $w_i^X$			нечітка оцінка рівня впевненості експерта, $p_i^X$			нормалізоване нечітке значення підфактору, $\bar{x}_i$		
	$w_{1i}^X$	$w_{2i}^X$	$w_{3i}^X$	$p_{1i}^X$	$p_{2i}^X$	$p_{3i}^X$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$
$A_1$	0,2579	0,4477	0,7291	0,55	0,7	0,85	0,1667	0,3333	0,50
$A_2$	0,1648	0,2786	0,5006	0,55	0,7	0,85	0,1667	0,3333	0,50
$A_3$	0,0655	0,1137	0,1996	0,55	0,7	0,85	0,1667	0,3333	0,50
$A_4$	0,0450	0,0708	0,1272	0,55	0,7	0,85	0,1667	0,3333	0,50
Ймовірність реалізації загрози через наявні вразливості, $P$									
$P_1$	0,091	0,1349	0,0982	0,55	0,7	0,85	0,1667	0,3333	0,50
$P_2$	0,0764	0,0862	0,0826	0,55	0,7	0,85	0,1667	0,3333	0,50
$P_3$	0,0540	0,0655	0,0826	0,55	0,7	0,85	0,1667	0,3333	0,50
$P_4$	0,0580	0,0725	0,0982	0,55	0,7	0,85	0,1667	0,3333	0,50
Рівень збитків від загрози, $Los$									
$Los_1$	0,0501	0,1029	0,2116	0,55	0,7	0,85	0,1667	0,3333	0,50
$Los_2$	0,0176	0,0318	0,0534	0,55	0,7	0,85	0,1667	0,3333	0,50
$Los_3$	0,0258	0,0606	0,1297	0,55	0,7	0,85	0,1667	0,3333	0,50
$Los_4$	0,0176	0,0318	0,0571	0,55	0,7	0,85	0,1667	0,3333	0,50
$Los$	0,0182	0,0333	0,0725	0,55	0,7	0,85	0,1667	0,3333	0,50
$Los_6$	0,0276	0,0196	0,0391	0,55	0,7	0,85	0,1667	0,3333	0,50
Рівень контролю інформаційних ресурсів, $Con$									
$Con_{11}$	0,1974	0,2548	0,3639	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Con_2$	0,2848	0,3210	0,3639	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Con_3$	0,2848	0,4044	0,5249	0,55	0,7	0,85	0,2222	0,3333	0,4444
Рівень витрат на створення та експлуатацію системи ІБ, $F$									
$F_1$	0,3026	0,4741	0,7231	0,55	0,7	0,85	0,2222	0,3333	0,4444
$F_2$	0,0643	0,0914	0,1870	0,55	0,7	0,85	0,2222	0,3333	0,4444
$F_3$	0,0488	0,0914	0,1417	0,55	0,7	0,85	0,2222	0,3333	0,4444
$F_4$	0,0868	0,1763	0,3148	0,55	0,7	0,85	0,2222	0,3333	0,4444
$F_5$	0,0643	0,0914	0,1417	0,55	0,7	0,85	0,2222	0,3333	0,4444
Рівень культури інформаційної безпеки, $Cul$									
$Cul_1$	0,1970	0,3598	0,6307	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Cul_2$	0,0791	0,1132	0,1919	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Cul_3$	0,0791	0,1132	0,1919	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Cul_4$	0,0791	0,1132	0,1919	0,55	0,7	0,85	0,2222	0,3333	0,4444
$Cul_5$	0,1043	0,2138	0,3420	0,55	0,7	0,85	0,2222	0,3333	0,4444



Таблиця Г.6 – Вхідні дані для моделювання сценаріїв (перший рівень)

Фактори	нечітке значення ваги фактору, $V_i^X$			лінгвістична оцінка рівня впевненості експерта, $\tilde{p}_i^X$	нечітке значення фактору, $\tilde{x}_i$		
	$V_{i1}^X$	$V_{i2}^X$	$V_{i3}^X$	$\tilde{p}_i^X$	$x_{1i}$	$x_{2i}$	$x_{3i}$
Низький рівень впевненості експерта, $L$							
$A$	0,0685	0,1534	0,3274	$L$	0,0480	0,2740	0,4280
$P$	0,0969	0,2252	0,5034	$L$	0,0552	0,2919	0,4029
$Los$	0,1708	0,3582	0,7739	$L$	0,0404	0,1799	0,2798
$Con$	0,0248	0,0448	0,0707	$L$	0,0806	0,3850	0,5345
$F$	0,0571	0,1218	0,2623	$L$	0,0435	0,2232	0,3333
$Cul$	0,0475	0,0966	0,2102	$L$	0,0426	0,2216	0,3358
Середній рівень впевненості експерта, $M$							
$A$	0,0685	0,1534	0,3274	$M$	0,0480	0,2740	0,4280
$P$	0,0969	0,2252	0,5034	$M$	0,0632	0,2980	0,3888
$Los$	0,1708	0,3582	0,7739	$M$	0,0469	0,1820	0,2711
$Con$	0,0248	0,0448	0,0707	$M$	0,0935	0,3932	0,5133
$F$	0,0571	0,1218	0,2623	$M$	0,0497	0,2265	0,3238
$Cul$	0,0475	0,0966	0,2102	$M$	0,0486	0,2245	0,3269
Високий рівень впевненості експерта, $H$							
$A$	0,0685	0,1534	0,3274	$H$	0,0558	0,2779	0,4163
$P$	0,0969	0,2252	0,5034	$H$	0,0658	0,3000	0,38423
$Los$	0,1708	0,3582	0,7739	$H$	0,0490	0,1827	0,2681
$Con$	0,0248	0,0448	0,0707	$H$	0,0978	0,3960	0,5063
$F$	0,0571	0,1218	0,2623	$H$	0,0517	0,2276	0,3207
$Cul$	0,0475	0,0966	0,2102	$H$	0,0505	0,2255	0,3240

Таблиця Г.7 – Нормалізовані проміжні дані розрахунку факторів

Фактори	нормалізоване нечітке значення важливості фактору, $W_i^X$			нечітка оцінка рівня впевненості експерта, $p_i^X$			нормалізоване нечітке значення фактору, $\bar{x}_i$		
	$W_{i1}^X$	$W_{i2}^X$	$W_{i3}^X$	$p_{1i}^X$	$p_{2i}^X$	$p_{3i}^X$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$
Низький рівень впевненості експерта, $L$									
$A$	0,0569	0,1274	0,2718	0,15	0,3	0,45	0,0640	0,3653	0,5707
$P$	0,0805	0,187	0,4179	0,15	0,3	0,45	0,0736	0,3892	0,5371
$Los$	0,1418	0,2974	0,6425	0,15	0,3	0,45	0,0808	0,3597	0,5595
$Con$	0,0206	0,0372	0,0587	0,15	0,3	0,45	0,0806	0,3850	0,5345
$F$	0,0474	0,1011	0,2178	0,15	0,3	0,45	0,0725	0,3720	0,5555
$Cul$	0,0394	0,0802	0,1745	0,15	0,3	0,45	0,0711	0,3693	0,5597
Середній рівень впевненості експерта, $M$									
$A$	0,0569	0,1274	0,2718	0,35	0,5	0,65	0,0640	0,3653	0,5707
$P$	0,0805	0,187	0,4179	0,35	0,5	0,65	0,0843	0,3973	0,5184
$Los$	0,1418	0,2974	0,6425	0,35	0,5	0,65	0,0938	0,3640	0,5423
$Con$	0,0206	0,0372	0,0587	0,35	0,5	0,65	0,0935	0,3932	0,5133
$F$	0,0474	0,1011	0,2178	0,35	0,5	0,65	0,0828	0,3775	0,5397
$Cul$	0,0394	0,0802	0,1745	0,35	0,5	0,65	0,0809	0,3742	0,5448
Високий рівень впевненості експерта, $H$									
$A$	0,0569	0,1274	0,2718	0,55	0,7	0,85	0,0744	0,3705	0,5551
$P$	0,0805	0,187	0,4179	0,55	0,7	0,85	0,0877	0,3999	0,5124
$Los$	0,1418	0,2974	0,6425	0,55	0,7	0,85	0,0981	0,3654	0,5366
$Con$	0,0206	0,0372	0,0587	0,55	0,7	0,85	0,0978	0,3960	0,5063
$F$	0,0474	0,1011	0,2178	0,55	0,7	0,85	0,0861	0,3793	0,5346
$Cul$	0,0394	0,0802	0,1745	0,55	0,7	0,85	0,0841	0,3758	0,5400

Таблиця Г.8 – Нечіткі значення впливу факторів на рівень ризику ІБ ТЛЦ з урахуванням сценаріїв імовірності

Фактори	нечітке значення при низькому рівні впевненості експерта, $L$			нечітке значення при середньому рівні впевненості експерта, $M$			нечітке значення при високому рівні впевненості експерта, $H$		
	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$	$\bar{x}_{1i}$	$\bar{x}_{2i}$	$\bar{x}_{3i}$
$A$	0,0150	0,1496	0,2511	0,0153	0,1433	0,2376	0,0177	0,1503	0,2440
$P$	0,0245	0,2352	0,3791	0,0285	0,2409	0,3757	0,0295	0,2407	0,3714
$Los$	0,0473	0,4047	0,6843	0,0558	0,4134	0,6793	0,0582	0,4127	0,6717
$Con$	0,0068	0,0588	0,0855	0,0081	0,0601	0,0823	0,0084	0,0600	0,0805
$F$	0,0142	0,1315	0,2165	0,0165	0,1337	0,2135	0,0171	0,1333	0,2107
$Cul$	0,0116	0,1069	0,1772	0,0134	0,1084	0,1744	0,0139	0,1079	0,1719



Рисунок В – Діаграма класів ядра системи «SecureFuzzy»

## Додаток Е

## Лістинг Е.1 – Код реалізації модуля 1. Фазифікація вхідних та вихідних факторів.

```

import numpy as np
import skfuzzy as fuzz
from skfuzzy import control as ctrl
from typing import Dict, Tuple

class FuzzySystem:
    def __init__(self):
        self.universe = np.arange(0, 1.01, 0.01)
        self.antecedents = {}
        self.confidence_antecedent = None
        self.risk = None
        self.confidence_terms = {}
        self.factors = []
        self.factor_types = {}

        self.setup_fuzzy_system()
        self.setup_factor_parameters()

    def setup_fuzzy_system(self):
        # Антецеденти (вхідні фактори)
        self.antecedents = {
            'A': ctrl.Antecedent(self.universe, 'asset_value'),
            'P': ctrl.Antecedent(self.universe, 'threat_prob'),
            'Los': ctrl.Antecedent(self.universe, 'damage_level'),
            'Con': ctrl.Antecedent(self.universe, 'control_level'),
            'F': ctrl.Antecedent(self.universe, 'costs'),
            'Cul': ctrl.Antecedent(self.universe, 'culture_level')
        }

        # Консеквент (вихід - ризик)
        self.risk = ctrl.Consequent(self.universe, 'risk_ib')
        self.confidence_antecedent = ctrl.Antecedent(self.universe,
'expert_confidence')

        self.setup_membership_functions()

    def setup_membership_functions(self):
        #Налаштування функцій належності для факторів ризику
        self.antecedents['A']['VL'] =
fuzz.trimf(self.antecedents['A'].universe, [0.0, 0.1, 0.21])
        self.antecedents['A']['L'] =
fuzz.trimf(self.antecedents['A'].universe, [0.21, 0.3, 0.40])
        self.antecedents['A']['M'] =
fuzz.trimf(self.antecedents['A'].universe, [0.41, 0.5, 0.60])
        self.antecedents['A']['H'] =
fuzz.trimf(self.antecedents['A'].universe, [0.61, 0.7, 0.80])

```

```

        self.antecedents['A']['VH']
fuzz.trimf(self.antecedents['A'].universe, [0.81, 0.9, 1.0])

        self.antecedents['P']['L']
fuzz.trimf(self.antecedents['P'].universe, [0.0, 0.15, 0.3])
        self.antecedents['P']['M']
fuzz.trimf(self.antecedents['P'].universe, [0.21, 0.48, 0.75])
        self.antecedents['P']['H']
fuzz.trimf(self.antecedents['P'].universe, [0.6, 0.8, 1.0])

        self.antecedents['Los']['L']
fuzz.trimf(self.antecedents['Los'].universe, [0.0, 0.1, 0.2])
        self.antecedents['Los']['M']
fuzz.trimf(self.antecedents['Los'].universe, [0.2, 0.35, 0.5])
        self.antecedents['Los']['H']
fuzz.trimf(self.antecedents['Los'].universe, [0.5, 0.65, 0.8])
        self.antecedents['Los']['VH']
fuzz.trimf(self.antecedents['Los'].universe, [0.8, 0.9, 1.0])

        self.antecedents['Con']['L']
fuzz.trimf(self.antecedents['Con'].universe, [0.1, 0.25, 0.5])
        self.antecedents['Con']['M']
fuzz.trimf(self.antecedents['Con'].universe, [0.4, 0.5, 0.75])
        self.antecedents['Con']['H']
fuzz.trimf(self.antecedents['Con'].universe, [0.6, 0.7, 0.9])
        self.antecedents['Con']['VH']
fuzz.trimf(self.antecedents['Con'].universe, [0.95, 0.97, 1.0])

        self.antecedents['F']['L']
fuzz.trimf(self.antecedents['F'].universe, [0.0, 0.15, 0.3])
        self.antecedents['F']['M']
fuzz.trimf(self.antecedents['F'].universe, [0.25, 0.42, 0.6])
        self.antecedents['F']['H']
fuzz.trimf(self.antecedents['F'].universe, [0.55, 0.65, 0.8])
        self.antecedents['F']['VH']
fuzz.trimf(self.antecedents['F'].universe, [0.75, 0.75, 1.0])

        self.antecedents['Cul']['L']
fuzz.trimf(self.antecedents['Cul'].universe, [0.0, 0.15, 0.3])
        self.antecedents['Cul']['M']
fuzz.trimf(self.antecedents['Cul'].universe, [0.25, 0.42, 0.6])
        self.antecedents['Cul']['H']
fuzz.trimf(self.antecedents['Cul'].universe, [0.55, 0.55, 0.8])
        self.antecedents['Cul']['VH']
fuzz.trimf(self.antecedents['Cul'].universe, [0.75, 0.87, 1.0])

        self.risk['VL'] = fuzz.trimf(self.risk.universe, [0.0, 0.0, 0.25])
        self.risk['L'] = fuzz.trimf(self.risk.universe, [0.15, 0.3, 0.45])
        self.risk['M'] = fuzz.trimf(self.risk.universe, [0.35, 0.5, 0.65])
        self.risk['H'] = fuzz.trimf(self.risk.universe, [0.55, 0.7, 0.85])
        self.risk['VH'] = fuzz.trimf(self.risk.universe, [0.75, 1.0, 1.0])

        #Налаштування функцій належності для впевненості експертів
        self.confidence_antecedent['VL'] = fuzz.trimf(
            self.confidence_antecedent.universe, [0.0, 0.0, 0.25])

```

```

    )
    self.confidence_antecedent['L'] = fuzz.trimf(
        self.confidence_antecedent.universe, [0.15, 0.3, 0.45]
    )
    self.confidence_antecedent['M'] = fuzz.trimf(
        self.confidence_antecedent.universe, [0.35, 0.5, 0.65]
    )
    self.confidence_antecedent['H'] = fuzz.trimf(
        self.confidence_antecedent.universe, [0.55, 0.7, 0.85]
    )
    self.confidence_antecedent['VH'] = fuzz.trimf(
        self.confidence_antecedent.universe, [0.75, 1.0, 1.0]
    )

def setup_factor_parameters(self):
    self.factors = ['A', 'P', 'Los', 'Con', 'F', 'Cul']

    self.factor_types = {
        'A': 'positive',
        'P': 'positive',
        'Los': 'positive',
        'Con': 'negative',
        'F': 'negative',
        'Cul': 'negative'
    }

def get_antecedent(self, factor: str) -> ctrl.Antecedent:
    return self.antecedents.get(factor)

def get_confidence_antecedent(self) -> ctrl.Antecedent:
    return self.confidence_antecedent

def linguistic_to_fuzzy(self, linguistic_value: str, factor: str) ->
Tuple[float, float, float]:
    #Конвертація лінгвістичного значення у нечітке число для факторів
    try:
        antecedent = self.antecedents[factor]
        return self._get_fuzzy_triangle(antecedent, linguistic_value)
    except Exception as e:
        print(f"Помилка в linguistic_to_fuzzy для
{factor}={linguistic_value}: {e}")

def confidence_to_fuzzy(self, confidence_level: str) -> Tuple[float,
float, float]:
    #Конвертація рівня впевненості у нечітке число
    try:
        return self._get_fuzzy_triangle(self.confidence_antecedent,
confidence_level)
    except Exception as e:
        print(f"Помилка в confidence_to_fuzzy для {confidence_level}:
{e}")

def _get_fuzzy_triangle(self, antecedent: ctrl.Antecedent,
linguistic_value: str) -> Tuple[float, float, float]:

```

```

linguistic_value = linguistic_value.upper()

if linguistic_value in antecedent.terms:
    mf = antecedent[linguistic_value].mf
    universe = antecedent.universe

    # Знаходимо ядро (значення з належністю 1)
    core_indices = np.where(mf == 1.0)[0]
    if len(core_indices) > 0:
        core = float(universe[core_indices[0]])
    else:
        core_index = np.argmax(mf)
        core = float(universe[core_index])

    # Знаходимо ліву та праву межі
    left_indices = np.where(mf > 0)[0]
    right_indices = np.where(mf > 0)[0]

    if len(left_indices) > 0 and len(right_indices) > 0:
        left = float(universe[left_indices[0]])
        right = float(universe[right_indices[-1]])
        return (left, core, right)

def crisp_to_fuzzy(self, crisp_value: float, factor: str) ->
Tuple[float, float, float]:
    #Конвертація чіткого значення у нечітке число для факторів
    try:
        antecedent = self.antecedents[factor]
        crisp_value = float(crisp_value)

        max_membership = 0
        best_term = None

        for term in antecedent.terms:
            membership = fuzz.interp_membership(antecedent.universe,
antecedent[term].mf, crisp_value)
            if membership > max_membership:
                max_membership = membership
                best_term = term

        if best_term:
            return self.linguistic_to_fuzzy(best_term, factor)

    except Exception as e:
        print(f"Помилка в crisp_to_fuzzy для {factor}={crisp_value}:
{e}")

def crisp_confidence_to_fuzzy(self, crisp_confidence: float) ->
Tuple[float, float, float]:
    #Конвертація чіткого значення впевненості у нечітке число
    try:
        crisp_confidence = float(crisp_confidence)

        max_membership = 0

```

```

        best_term = None

        for term in self.confidence_antecedent.terms:
            membership = fuzz.interp_membership(
                self.confidence_antecedent.universe,
                self.confidence_antecedent[term].mf,
                crisp_confidence
            )
            if membership > max_membership:
                max_membership = membership
                best_term = term

        if best_term:
            return self.confidence_to_fuzzy(best_term)

    except Exception as e:
        print(f"Помилка в {crisp_confidence_to_fuzzy} для {crisp_confidence}: {e}")

def defuzzify(self, fuzzy_number: Tuple[float, float, float]) -> float:
    #Дефазифікація нечіткого числа
    try:
        x = np.arange(0, 1.01, 0.01)
        a, b, c = fuzzy_number
        mf = fuzz.trimf(x, [a, b, c])
        result = fuzz.defuzz(x, mf, 'centroid')
        return float(result)
    except Exception as e:
        print(f"Помилка в defuzzify: {e}")

def interpret_risk_level(self, risk_score: float) -> str:
    try:
        risk_score = float(risk_score)
        memberships = {}

        for term_name, term_set in self.risk.terms.items():
            membership = fuzz.interp_membership(
                self.risk.universe,
                term_set.mf,
                risk_score
            )
            memberships[term_name] = membership

        best_term = max(memberships.items(), key=lambda x: x[1])[0]

        term_translations = {
            'VL': 'Дуже низький',
            'L': 'Низький',
            'M': 'Допустимий',
            'H': 'Високий',
            'VH': 'Критичний'
        }

        return term_translations.get(best_term, best_term)

```



```

        except Exception as e:
            print(f"Помилка в risk_score_to_linguistic для {risk_score}: {e}")
            return None

```

Лістинг E2 – Код реалізації модуля 2. Обчислення ваг факторів методом нечіткого ієрархічного аналізу.

```

from typing import List, Tuple, Dict

import numpy as np

class FuzzyAHP:

    def __init__(self, factors: List[str], fuzzy_scale: Dict[str,
        Tuple[float, float, float]] = None):

        self.factors = factors

        self.n = len(factors)

        self.RI = {1: 0, 2: 0, 3: 0.58, 4: 0.90, 5: 1.12, 6: 1.24, 7: 1.32,
            8: 1.41, 9: 1.45, 10: 1.49}

        self.FUZZY_SCALE = fuzzy_scale or {

            'однаково важливі': (1, 1, 1), 'трохи важливіше': (2, 3, 4),
            'важливіше': (4, 5, 6),

            'дуже важливіше': (6, 7, 8), 'абсолютно важливіше': (8, 9, 9)

        }

    def build_fuzzy_matrix(self, pairwise_comparisons: List[Dict[str, str]])
-> np.ndarray:

        matrix = np.ones((self.n, self.n, 3))

        factor_indices = {name: i for i, name in enumerate(self.factors)}

        for comp in pairwise_comparisons:

            i, j = factor_indices[comp['factor_i']], factor_indices[comp['factor_j']]

            value = comp['value']

```

```

        if value in self.FUZZY_SCALE:

            matrix[i, j] = self.FUZZY_SCALE[value]

            matrix[j, i] = (1/matrix[i, j, 2], 1/matrix[i, j, 1],
1/matrix[i, j, 0])

        else: raise ValueError(f"Невідоме значення: {value}")

    return matrix

def check_consistency(self, fuzzy_matrix: np.ndarray) -> Tuple[float,
bool]:

    if self.n > len(self.RI) or self.n <= 2: return 0.0, True

    crisp_matrix = fuzzy_matrix[:, :, 1]

    eigenvalues, _ = np.linalg.eig(crisp_matrix)

    lambda_max = np.max(eigenvalues).real

    CI = (lambda_max - self.n) / (self.n - 1)

    CR = CI / self.RI[self.n]

    return CR, CR < 0.10

def calculate_weights(self, fuzzy_matrix: np.ndarray) -> Dict[str,
float]:

    fuzzy_sums = np.sum(fuzzy_matrix, axis=1)

    total_sum = np.sum(fuzzy_sums, axis=0)

    inv_total_sum = (1 / total_sum[2], 1 / total_sum[1], 1 /
total_sum[0])

    s = [(fs[0]*inv_total_sum[0], fs[1]*inv_total_sum[1],
fs[2]*inv_total_sum[2]) for fs in fuzzy_sums]

def degree_of_possibility(s_i, s_j):

    _, m_i, u_i = s_i; l_j, m_j, _ = s_j

    if m_i >= m_j: return 1.0

```

```

        if l_j >= u_i: return 0.0

        return (u_i - l_j) / ((m_j - l_j) + (u_i - m_i))

    raw_weights = [min(degree_of_possibility(s[i], s[j]) for j in
range(self.n) if i != j) for i in range(self.n)]

    epsilon = 0.001 * max(raw_weights) if max(raw_weights) > 0 else 1e-
9

    regularized_weights = [w + epsilon for w in raw_weights]

    total_weight = sum(regularized_weights)

    final_weights = [w / total_weight for w in regularized_weights]

    return {factor: weight for factor, weight in zip(self.factors,
final_weights)}

```

### Лістинг Е3 – Код реалізації модуля 6. Матриця Дж. Х. Вілсона.

```

import matplotlib.pyplot as plt
import numpy as np
import matplotlib.patches as patches

class WilsonMatrix:
    def __init__(self, figsize=(12, 8)):
        self.fig, self.ax = plt.subplots(figsize=figsize)
        self.setup_axes()
        self.setup_grid_lines()
        self.setup_zones()
        self.setup_labels()

    def setup_axes(self):
        # Встановлюємо межі
        self.ax.set_xlim(-1, 1)
        self.ax.set_ylim(0, 1)

        # Основні лінії осей
        self.ax.axhline(y=0, color='black', linewidth=1.5)
        self.ax.axvline(x=0, color='black', linewidth=1.5)

        # Прибираємо стандартну сітку
        self.ax.grid(False)

        # Підписи осей
        self.ax.set_xlabel('Вплив фактору', fontsize=10, fontweight='bold')
        self.ax.set_ylabel('Впевненість експерта', fontsize=10,
fontweight='bold')

    def setup_grid_lines(self):

```

```

# Визначення всіх меж для рівнів по X
x_levels = {
    'NS': (0, -0.17),
    'VL': (0, -0.33),
    'L': (-0.17, -0.5),
    'M': (-0.33, -0.67),
    'H': (-0.50, -0.83),
    'VH': (-0.67, -1),
    'EH': (-0.83, -1),
    'NS_pos': (0, 0.17),
    'VL_pos': (0, 0.33),
    'L_pos': (0.17, 0.5),
    'M_pos': (0.33, 0.67),
    'H_pos': (0.50, 0.83),
    'VH_pos': (0.67, 1),
    'EH_pos': (0.83, 1),
}

# Визначення всіх унікальних X позицій для ліній
x_positions = set()
for start, end in x_levels.values():
    x_positions.add(start)
    x_positions.add(end)
x_positions = sorted(x_positions)

# Додаємо вертикальні лінії для всіх X позицій
for x_pos in x_positions:
    if x_pos != 0:
        self.ax.axvline(x=x_pos, color='gray', linewidth=0.8,
linestyle='--', alpha=0.7)

# Визначення меж для рівнів по Y
y_levels = {
    'VL': (0.0, 0.25),
    'L': (0.15, 0.45),
    'M': (0.35, 0.65),
    'H': (0.55, 0.85),
    'VH': (0.75, 1.0)
}

# Визначення всіх унікальних Y позицій для ліній
y_positions = set()
for start, end in y_levels.values():
    y_positions.add(start)
    y_positions.add(end)
y_positions = sorted(y_positions)

# Додаємо горизонтальні лінії для всіх Y позицій
for y_pos in y_positions:
    self.ax.axhline(y=y_pos, color='gray', linewidth=0.8,
linestyle='--', alpha=0.7)

def setup_zones(self):
    zones = [
        # Загрози (ліва частина)

```

```

        {'name': 'Dt', 'x_range': (-1.0, 0), 'y_range': (0.0, 1.0),
        'color': 'white'},
        {'name': 'Ct', 'x_range': (-1.0, -0.17), 'y_range': (0.15,
1.0), 'color': 'gray'},
        {'name': 'Bt', 'x_range': (-1.0, -0.33), 'y_range': (0.35,
1.0), 'color': 'orange'},
        {'name': 'At', 'x_range': (-1.0, -0.5), 'y_range': (0.55, 1.0),
        'color': 'red'},

        # Можливості (права частина)
        {'name': 'Do', 'x_range': (0, 1.0), 'y_range': (0.0, 1.0),
        'color': 'white'},
        {'name': 'Co', 'x_range': (0.17, 1.0), 'y_range': (0.15, 1.0),
        'color': 'lightgray'},
        {'name': 'Bo', 'x_range': (0.33, 1.0), 'y_range': (0.35, 1.0),
        'color': 'lime'},
        {'name': 'Ao', 'x_range': (0.5, 1.0), 'y_range': (0.55, 1.0),
        'color': 'green'},
    ]

    for zone in zones:
        rect = patches.Rectangle(
            (zone['x_range'][0], zone['y_range'][0]),
            zone['x_range'][1] - zone['x_range'][0],
            zone['y_range'][1] - zone['y_range'][0],
            linewidth=1, edgecolor='black', facecolor=zone['color'],
            alpha=0.6
        )
        self.ax.add_patch(rect)

        # Додавання назв зон
        if zone['name'] in ['At', 'Bt', 'Ct', 'Dt']:
            # Для загроз - лівий верхній кут
            text_x = zone['x_range'][1] - 0.1
            text_y = zone['y_range'][0] + 0.1
            ha = 'left'
        else:
            text_x = zone['x_range'][0] + 0.1
            text_y = zone['y_range'][0] + 0.1
            ha = 'right'

        self.ax.text(text_x, text_y, zone['name'], ha=ha, va='top',
                     fontsize=9, fontweight='bold',
                     bbox=dict(boxstyle="round,pad=0.2",
facecolor='white',
                                     alpha=0.8, edgecolor='black'))

    def setup_labels(self):
        # Підписи рівнів по осі X (для загроз)
        x_labels_threats = {
            -0.03: 'NSt', -0.17: 'VLt', -0.33: 'Lt', -0.5: 'Mt', -0.67:
            'Ht', -0.83: 'VHt', -1: 'EHt'
        }

        for pos, label in x_labels_threats.items():

```

```

        self.ax.text(pos, 1.02, label, ha='center', va='bottom',
                     fontsize=8, fontweight='bold', color='darkred')

# Підписи рівнів по осі X (для можливостей)
x_labels_opportunities = {
    0.03: 'NSo', 0.17: 'VLo', 0.33: 'Lo', 0.5: 'Mo', 0.67: 'Ho',
0.83: 'VHo', 1: 'EHo'
}

for pos, label in x_labels_opportunities.items():
    self.ax.text(pos, 1.02, label, ha='center', va='bottom',
                 fontsize=8, fontweight='bold', color='darkgreen')

# Підписи рівнів по осі Y (праворуч)
y_labels = {
    0.12: 'VL', 0.3: 'L', 0.5: 'M', 0.7: 'H', 0.88: 'VH'
}

for pos, label in y_labels.items():
    self.ax.text(1.02, pos, label, ha='left', va='center',
                 fontsize=8, fontweight='bold', color='darkblue')

# Заголовки зон
self.ax.text(-0.5, 1.05, 'Загрози', ha='center', fontsize=11,
             fontweight='bold', color='darkred')
self.ax.text(0.5, 1.05, 'Можливості', ha='center', fontsize=11,
             fontweight='bold', color='darkgreen')

x_ticks = np.arange(-1.0, 1.1, 0.1)
self.ax.set_xticks(x_ticks)

def add_factor_point(self, factor_type, value, confidence, label,
                    color, size=80):
    if not (0 <= value <= 1):
        raise ValueError(f"Значення фактора {label} повинно бути в
діапазоні [0, 1]")
    if not (0 <= confidence <= 1):
        raise ValueError(f"Впевненість для {label} повинна бути в
діапазоні [0, 1]")

    # Визначаємо позицію по X в залежності від типу фактора
    if factor_type == 'threat':
        influence = -value
    elif factor_type == 'opportunity':
        influence = value
    else:
        raise ValueError("Тип фактора повинен бути 'threat' або
'opportunity'")

    # Додавання точки
    scatter = self.ax.scatter(influence, confidence, c=color, s=size,
                             edgecolors='black', linewidth=1.5,
zorder=5)
    # Визначаємо зміщення для тексту
    offset_x = -0.03 if factor_type == 'threat' else 0.03

```

```

        self.ax.annotate(f'{label}\nval={value:.2f} conf={confidence:.2f}',
                        (influence, confidence),
                        xytext=(influence + offset_x, confidence + 0.02),
                        fontsize=7, fontweight='bold',
                        ha='right' if factor_type == 'threat' else 'left',
                        bbox=dict(boxstyle="round,pad=0.2",
                                facecolor='white',
                                alpha=0.9, edgecolor='black'))

    return scatter

def add_all_factors(self, factors_data):
    threat_factors = ['asset_value', 'threat_prob', 'damage_level']
    opportunity_factors = ['control_level', 'costs', 'culture_level']

    for i, factor in enumerate(threat_factors):
        if factor in factors_data:
            data = factors_data[factor]
            self.add_factor_point(
                factor_type='threat',
                value=data['value'],
                confidence=data['confidence'],
                label=factor,
                color='red',
                size=80
            )

    for i, factor in enumerate(opportunity_factors):
        if factor in factors_data:
            data = factors_data[factor]
            self.add_factor_point(
                factor_type='opportunity',
                value=data['value'],
                confidence=data['confidence'],
                label=factor,
                color='limegreen',
                size=80
            )

def show(self, title="Матриця Вільсона"):
    self.ax.set_title(title, fontsize=12, fontweight='bold', pad=35)
    self.ax.set_aspect('equal')
    plt.tight_layout()
    plt.show()

```

#### Лістинг Е4 – Код реалізації модуля 8. Обчислення оцінки ризику.

```

from typing import Dict, Tuple, Union, List
from Fuzzification import FuzzySystem

class FuzzyRiskCalculator:
    def __init__(self):

```

```

        self.fuzzy_system = FuzzySystem()

    def fuzzy_multiply(self, a: Tuple[float, float, float],
                       b: Tuple[float, float, float]) -> Tuple[float,
float, float]:
        #Множення двох нечітких трикутних чисел
        return (a[0] * b[0], a[1] * b[1], a[2] * b[2])

    def fuzzy_add(self, a: Tuple[float, float, float],
                  b: Tuple[float, float, float]) -> Tuple[float, float,
float]:
        #Додавання двох нечітких трикутних чисел
        return (a[0] + b[0], a[1] + b[1], a[2] + b[2])

    def fuzzy_negate(self, a: Tuple[float, float, float]) -> Tuple[float,
float, float]:
        #Зміна знаку нечіткого числа
        return (1.0 - a[2], 1.0 - a[1], 1.0 - a[0])

    def fuzzy_product(self, confidence: Tuple[float, float, float],
                      value: Tuple[float, float, float]) ->
Tuple[float, float, float]:
        try:
            p1, p2, p3 = confidence
            x1, x2, x3 = value

            Y1 = p1 * x1
            Y2 = p2 * x1 + p1 * x2
            Y3 = p1 * x3 + p3 * x1

            return (float(Y1), float(Y2), float(Y3))
        except Exception as e:
            print(f"Помилка в fuzzy_product: {e}")
            return (0.0, 0.0, 0.0)

    def parse_input_value(self, value: Union[float, str, int], factor: str)
-> Tuple[float, float, float]:
        #Парсинг вхідних значень факторів у нечіткі числа

        try:
            if isinstance(value, (int, float)):
                return self.fuzzy_system.crisp_to_fuzzy(float(value),
factor)
            elif isinstance(value, str):
                return self.fuzzy_system.linguistic_to_fuzzy(value, factor)

        except Exception as e:
            print(f"Помилка в parse_input_value для {factor}={value}: {e}")

    def parse_confidence_value(self, confidence_value: Union[float, str]) -
> Tuple[float, float, float]:
        #Парсинг значень впевненості у нечіткі числа
        try:

```



```

        if isinstance(confidence_value, (int, float)):
            return
self.fuzzy_system.crisp_confidence_to_fuzzy(float(confidence_value))
        elif isinstance(confidence_value, str):
            return
self.fuzzy_system.confidence_to_fuzzy(confidence_value)

    except Exception as e:
        print(f"Помилка в parse_confidence_value для
{confidence_value}: {e}")

    def multiply_confidence_factor(self, factor_values: Dict[str,
Union[float, str]],
                                confidence_levels: Dict[str, Union[float,
str]]) -> Dict[str, Tuple[float, float, float]]:

        confidence_by_factor = {}

        for factor in self.fuzzy_system.factors:
            if factor in factor_values and factor in confidence_levels:
                try:
                    raw_value = factor_values[factor]
                    confidence_value = confidence_levels[factor]

                    fuzzy_value = self.parse_input_value(raw_value, factor)
                    fuzzy_confidence =
self.parse_confidence_value(confidence_value)

                    Xij = self.fuzzy_product(fuzzy_confidence, fuzzy_value)
                    confidence_by_factor[factor] = Xij

                except Exception as e:
                    print(f"Помилка при обробці фактора {factor}: {e}")
                    confidence_by_factor[factor] = (0.0, 0.0, 0.0)

        return confidence_by_factor

    def calculate_risk(self,
                                factor_values: Dict[str, Union[float,
str]],
                                confidence_levels: Dict[str, Union[float,
str]],
                                weights: Dict[str, float]) -> Dict:

        confidence_by_factor =
self.multiply_confidence_factor(factor_values, confidence_levels)
        integral_result = (0.0, 0.0, 0.0)

        for factor in self.fuzzy_system.factors:
            if factor in confidence_by_factor and factor in weights:
                try:
                    Xij = confidence_by_factor[factor] # piX * X
                    weight = weights[factor]
                    fuzzy_weight = (weight, weight, weight)

```

```

        W_Xij = self.fuzzy_multiply(fuzzy_weight, Xij)

        factor_type = self.fuzzy_system.factor_types[factor]

        if factor_type == 'positive':
            contribution = W_Xij
            integral_result = self.fuzzy_add(integral_result,
contribution)

        else:
            inverted_Xij = self.fuzzy_negate(Xij)
            contribution = self.fuzzy_multiply(fuzzy_weight,
inverted_Xij)
            integral_result = self.fuzzy_add(integral_result,
contribution)

    except Exception as e:
        print(f"Помилка при обчисленні впливу фактора {factor}:
{e}")

    # Дефазифікація
    crisp_risk = self.fuzzy_system.defuzzify(integral_result)
    risk_level = self.fuzzy_system.interpret_risk_level(crisp_risk)

    print(f"Інтегральна оцінка ризику: {integral_result}")
    print(f"Чітке значення ризику: {crisp_risk:.4f}")
    print(f"Рівень ризику: {risk_level}")

    return {
        'fuzzy_integral': integral_result,
        'crisp_risk': crisp_risk,
        'risk_level': risk_level
    }

```

### Лістинг E5 – Код реалізації модуля 3. Генерація повної бази правил.

```

import itertools
import csv
import pandas as pd
from pathlib import Path

class MamdaniRuleBaseGenerator:
    # Default generator parameters
    DEFAULT_TERMS = {
        "x1": {"VL": 0.1, "L": 0.3, "M": 0.5, "H": 0.7, "VH": 0.9},
        "x2": {"L": 0.15, "M": 0.48, "H": 0.8},
        "x3": {"L": 0.1, "M": 0.35, "H": 0.65, "VH": 0.9},
        "x4": {"VH": 0.97, "H": 0.7, "M": 0.5, "L": 0.25},
        "x5": {"L": 0.15, "M": 0.42, "H": 0.65, "VH": 0.75},
        "x6": {"L": 0.15, "M": 0.42, "H": 0.55, "VH": 0.87},
    }

    DEFAULT_WEIGHTS = {

```

```

        "x1": 0.154,
        "x2": 0.225,
        "x3": 0.354,
        "x4": 0.043,
        "x5": 0.124,
        "x6": 0.1,
    }

    DEFAULT_RISK_REDUCING = {"x4", "x5", "x6"}

    def __init__(self, terms=None, weights=None, risk_reducing=None):
        self.terms = terms if terms is not None else self.DEFAULT_TERMS
        self.weights = weights if weights is not None else
self.DEFAULT_WEIGHTS
        self.risk_reducing = risk_reducing if risk_reducing is not None else
self.DEFAULT_RISK_REDUCING
        self.factor_names = list(self.terms.keys())
        self.rules = []

    @staticmethod
    def classify_risk(r_index):
        if r_index <= 0.21:
            return "L"
        elif r_index <= 0.41:
            return "M"
        elif r_index <= 0.65:
            return "H"
        else:
            return "VH"

    def generate_rules(self):
        term_lists = [list(self.terms[f].keys()) for f in self.factor_names]
        self.rules = []

        for combo in itertools.product(*term_lists):
            r_index = 0.0
            for f_name, term_name in zip(self.factor_names, combo):
                v = self.terms[f_name][term_name]
                if f_name in self.risk_reducing:
                    v = 1.0 - v
                r_index += self.weights[f_name] * v

            consequence = self.classify_risk(r_index)
            self.rules.append({
                **dict(zip(self.factor_names, combo)),
                "R_index": round(r_index, 6),
                "R": consequence
            })
        return self.rules

    def save_local(self, path="rules_full.csv"):
        if not self.rules:
            raise ValueError("Rules not generated yet use
generate_rules().")

```

```

        out_path = Path(path)
        with out_path.open("w", newline="", encoding="utf-8") as csvfile:
            writer = csv.DictWriter(csvfile, fieldnames=self.factor_names +
["R_index", "R"])
            writer.writeheader()
            for r in self.rules:
                writer.writerow(r)

    def compare_with_expert(self, expert_path):
        if not self.rules:
            raise ValueError("Rules not generated yet. Call generate_rules()
first.")

        expert = pd.read_csv(expert_path)

        # conversion of an expert number into a term
        def num_to_term(factor, value):
            term_values = self.terms[factor]
            closest_term = min(term_values.items(), key=lambda x: abs(x[1]-
value))[0]
            return closest_term

        for f in self.factor_names:
            first_value = expert[f].iloc[0]
            if not isinstance(first_value, str):
                expert[f+"_term"] = expert[f].apply(lambda v: num_to_term(f,
v))
            else:
                expert[f+"_term"] = expert[f]

        # index recalculation
        def calc_r_index(row):
            r_index = 0
            for f in self.factor_names:
                v = self.terms[f][row[f+"_term"]]
                if f in self.risk_reducing:
                    v = 1 - v
                r_index += self.weights[f] * v
            return r_index

        expert["R_index_calc"] = expert.apply(calc_r_index, axis=1)
        expert["R_calc"] = expert["R_index_calc"].apply(self.classify_risk)

        auto_rules = pd.DataFrame(self.rules)
        auto_rules["key"] = auto_rules[self.factor_names].agg("-".join,
axis=1)
        expert["key"] = expert[[f+"_term" for f in
self.factor_names]].agg("-".join, axis=1)

        merged = pd.merge(auto_rules, expert, on="key", suffixes=("_auto",
"_expert"))
        merged["match"] = merged["R_auto"] == merged["R_calc"]

        return merged

```

**Лістинг Е6 – Код реалізації модуля 4. Створення Rete-мережі на основі повної бази правил з модуля 3.**

```

import pandas as pd
import numpy as np
from typing import Dict, List, Tuple

class FuzzyReteNode:
    def __init__(self):
        self.output_nodes: List['FuzzyReteNode'] = []

    def connect(self, node: 'FuzzyReteNode'):
        self.output_nodes.append(node)

class AlphaNode(FuzzyReteNode):
    def __init__(self, factor: str, term: str):
        super().__init__()
        self.factor = factor
        self.term = term

    def activate(self, fact: Dict[str, str]):
        if fact.get(self.factor) == self.term:
            for node in self.output_nodes:
                node.activate(self.factor, True)

class BetaNode(FuzzyReteNode):
    def __init__(self, conditions: Dict[str, str], R: str, R_index: float):
        super().__init__()
        self.conditions = conditions
        self.R = R
        self.R_index = R_index
        self.matched_conditions = {k: False for k in conditions}

    def activate(self, fact_name: str, matched: bool):
        self.matched_conditions[fact_name] = matched
        if all(self.matched_conditions.values()):
            for node in self.output_nodes:
                node.activate(self.R)

    def reset(self):
        self.matched_conditions = {k: False for k in self.conditions}

class OutputNode:
    def __init__(self):
        self.activated_rules: List[str] = []

    def activate(self, R: str):
        self.activated_rules.append(R)

    def reset(self):
        self.activated_rules = []

class ReteNetwork:
    def __init__(self, rules_data):

```

```

self.alpha_nodes: Dict[Tuple[str, str], AlphaNode] = {}
self.beta_nodes: List[BetaNode] = []
self.output_node = OutputNode()

if isinstance(rules_data, pd.DataFrame):
    rules_df = rules_data
elif isinstance(rules_data, list):
    rules_df = pd.DataFrame(rules_data)
else:
    raise ValueError("rules_data must be DataFrame or list[dict]")

for idx, row in rules_df.iterrows():
    conditions = {f"x{i+1}": row[f"x{i+1}"] for i in range(6)}
    beta_node = BetaNode(conditions, R=row["R"],
R_index=row["R_index"])
    beta_node.connect(self.output_node)
    self.beta_nodes.append(beta_node)

    for factor, term in conditions.items():
        key = (factor, term)
        if key not in self.alpha_nodes:
            self.alpha_nodes[key] = AlphaNode(factor, term)
            self.alpha_nodes[key].connect(beta_node)

def run_fact(self, fact: Dict[str, str]) -> List[str]:
    self.output_node.reset()
    for beta in self.beta_nodes:
        beta.reset()
    for (factor, term), alpha in self.alpha_nodes.items():
        alpha.activate(fact)
    return self.output_node.activated_rules

```

### Лістинг Е7 – Код реалізації модуля 5. Гібридне адаптивне виведення.

```

import torch
import torch.nn as nn
import torch.optim as optim
from typing import List, Dict
import itertools
import pickle

device = torch.device("cuda" if torch.cuda.is_available() else "cpu")

class BetaNode(nn.Module):
    def __init__(self, conditions: Dict[str, float], poly_degree: int = 1,
feature_dim: int = 0):
        super().__init__()
        self.conditions = conditions
        self.poly_degree = poly_degree
        expanded_dim = feature_dim + 1
        coeff_init = torch.randn(expanded_dim) * 0.1
        self.coeffs = nn.Parameter(coeff_init.to(device))
        self.frozen_mask = torch.ones_like(self.coeffs, device=device)

```

```

        self.activation = 0.0

class ANFIS(nn.Module):

    DEFAULT_FACTORS = ["x1", "x2", "x3", "x4", "x5", "x6"]

    DEFAULT_TERMS = {
        "x1": {"VL":0.1, "L":0.3, "M":0.5, "H":0.7, "VH":0.9},
        "x2": {"L":0.15, "M":0.48, "H":0.8},
        "x3": {"L":0.1, "M":0.35, "H":0.65, "VH":0.9},
        "x4": {"L":0.25, "M":0.5, "H":0.7, "VH":0.97},
        "x5": {"L":0.15, "M":0.42, "H":0.65, "VH":0.75},
        "x6": {"L":0.15, "M":0.42, "H":0.55, "VH":0.87}
    }

    def __init__(self, rete=None, poly_degree: int = 1,
                  factor_names: List[str] = None, terms_num: Dict[str,
Dict[str, float]] = None):
        super().__init__()
        self.rules: List[BetaNode] = nn.ModuleList()
        self.X, self.y = None, None
        self.poly_degree = poly_degree
        self.factor_names = factor_names or self.DEFAULT_FACTORS
        self.terms_num = terms_num or self.DEFAULT_TERMS
        self.feature_names = self._get_feature_names(poly_degree)

        if rete is not None:
            self.X, self.y = self._convert_rete_to_tensor(rete)
            for row in self.X:
                cond_dict = dict(zip(self.factor_names, row.tolist()))
                self.rules.append(BetaNode(cond_dict, poly_degree,
len(self.feature_names)))

    def _expand_features(self, x_vec: torch.Tensor, degree: int = 1):
        if x_vec.dim() == 1:
            x_vec = x_vec.unsqueeze(0)
        B, n = x_vec.shape
        features = [x_vec]

        if degree == 2:
            squares = x_vec ** 2
            features.append(squares)
            cross_terms = []
            for i, j in itertools.combinations(range(n), 2):
                cross_terms.append((x_vec[:, i] * x_vec[:,
j])).unsqueeze(1))
            if cross_terms:
                features.append(torch.cat(cross_terms, dim=1))

        return torch.cat(features, dim=1)

    def _get_feature_names(self, degree: int = 1):
        names = self.factor_names.copy()
        if degree == 2:
            names += [f"{f}^2" for f in self.factor_names]

```

```

        for i, j in itertools.combinations(self.factor_names, 2):
            names.append(f"{i}*{j}")
    return names

    def update_config(self, factor_names: List[str] = None, terms_num:
Dict[str, Dict[str, float]] = None):
        if factor_names is not None:
            self.factor_names = factor_names
        if terms_num is not None:
            self.terms_num = terms_num
        self.feature_names = self._get_feature_names(self.poly_degree)
        print("Configuration updated")

    def initialize_coeffs(self, weights: Dict[str, float], risk_reducing:
set):
        with torch.no_grad():
            for r in self.rules:
                for i, f in enumerate(self.factor_names):
                    val = weights.get(f, 0.0)
                    if f in risk_reducing:
                        val = -val
                    r.coeffs[i+1].copy_(torch.tensor(val, device=device))

    def _convert_rete_to_tensor(self, rete):
        X_list, y_list = [], []
        for beta in rete.beta_nodes:
            numeric_conditions = [self.terms_num[f][term] for f, term in
beta.conditions.items()]
            X_list.append(numeric_conditions)
            y_list.append(float(getattr(beta, "R_index", beta.R)))
        X_tensor = torch.tensor(X_list, dtype=torch.float32, device=device)
        y_tensor = torch.tensor(y_list, dtype=torch.float32, device=device)
        return X_tensor, y_tensor

    def _calc_activations_batch(self, X_batch):
        batch_size = X_batch.size(0)
        n_rules = len(self.rules)
        X_exp = X_batch.unsqueeze(1).expand(batch_size, n_rules,
len(self.factor_names))
        rule_terms = torch.tensor([[rule.conditions[f] for f in
self.factor_names]
                                   for rule in self.rules], device=device)
        rule_terms_exp = rule_terms.unsqueeze(0).expand(batch_size,
n_rules, len(self.factor_names))
        activations = 1 - torch.abs(X_exp - rule_terms_exp)
        activations = torch.clamp(activations, min=0.0)
        activations = torch.prod(activations, dim=2)
        activations = activations / activations.sum(dim=1, keepdim=True)
        return activations

    def _calc_z_batch(self, X_batch):
        X_poly = self._expand_features(X_batch, self.poly_degree)
        coeffs_matrix = torch.stack([r.coeffs * r.frozen_mask for r in
self.rules], dim=0)
        c0 = coeffs_matrix[:, 0]

```



```

        cf = coeffs_matrix[:, 1:]
        activations = self._calc_activations_batch(X_batch)
        z_rules = torch.matmul(X_poly, cf.t()) + c0.unsqueeze(0)
        z_total = (activations * z_rules).sum(dim=1)
        return z_total

    def predict_batch(self, X_batch):
        z_total = self._calc_z_batch(X_batch)
        return torch.sigmoid(z_total)

    def predict(self, x: Dict[str, float]):
        X_tensor = torch.tensor([x[f] for f in self.factor_names],
                                dtype=torch.float32, device=device).unsqueeze(0)
        return self.predict_batch(X_tensor)[0]

    def train_model(self, lr=0.01, epochs=50, batch_size=32):
        if self.X is None or self.y is None:
            raise ValueError("No data")
        optimizer = optim.Adam(self.parameters(), lr=lr)
        n = self.X.size(0)

        for ep in range(epochs):
            perm = torch.randperm(n)
            mse_epoch = 0.0
            for i in range(0, n, batch_size):
                idx = perm[i:i+batch_size]
                X_batch, y_batch = self.X[idx], self.y[idx]
                optimizer.zero_grad()
                y_pred = self.predict_batch(X_batch)
                loss = ((y_batch - y_pred) ** 2).mean()
                loss.backward()
                for r in self.rules:
                    if hasattr(r, 'frozen_mask'):
                        r.coeffs.grad *= r.frozen_mask
                optimizer.step()
                mse_epoch += loss.item() * X_batch.size(0)
            mse_epoch /= n
            print(f"Epoch {ep+1}/{epochs}, MSE={mse_epoch:.6f}")

    def train_and_reduce(self, initial_epochs=50, batch_size=32,
                        reduction_epochs=20, significance_threshold=0.05, load_filepath=None):
        if load_filepath is not None:
            self.load_model(load_filepath)
        else:
            self.train_model(lr=0.01, epochs=initial_epochs,
                            batch_size=batch_size)

        max_rounds = 5
        round_idx = 0

        while round_idx < max_rounds:
            print(f"\nModel reduction, round {round_idx+1}")
            print("Global equation:")
            print(self.get_global_polynomial_equation())

```

```

        global_coeffs = self.get_global_coefficients()
        insignificant = [i for i, c in enumerate(global_coeffs) if
abs(c) < significance_threshold]

        new_insignificant = []
        for i in insignificant:
            if any(r.frozen_mask[i].item() == 1 for r in self.rules):
                new_insignificant.append(i)

        if not new_insignificant:
            print("Reduction complete.")
            break

        print(f"Removing coefficients with indices: {insignificant}
(|value| < {significance_threshold})")

        for r in self.rules:
            with torch.no_grad():
                for i in insignificant:
                    r.frozen_mask[i] = 0

        self.train_model(lr=0.01, epochs=reduction_epochs,
batch_size=batch_size)
        round_idx += 1

def get_global_coefficients(self):
    coeff_len = len(self.rules[0].coeffs)
    global_coeffs = torch.zeros(coeff_len,
device=self.rules[0].coeffs.device)
    for r in self.rules:
        global_coeffs += (r.coeffs * r.frozen_mask).detach()
    global_coeffs /= len(self.rules)
    return global_coeffs

def get_global_polynomial_equation(self):
    n_rules = len(self.rules)
    coeffs_sum = torch.zeros(len(self.feature_names)+1, device=device)
    for r in self.rules:
        coeffs_sum += (r.coeffs * r.frozen_mask).detach()
    coeffs_avg = coeffs_sum / n_rules
    terms = []
    if coeffs_avg[0].item() != 0:
        terms.append(f"{coeffs_avg[0].item():.4f}")
    for i, f in enumerate(self.feature_names):
        if coeffs_avg[i+1].item() != 0:
            terms.append(f"{coeffs_avg[i+1].item():.4f}*{f}")
    return f"R = sigmoid({' + '.join(terms)})"

def check_model_adequacy(self, rete_test):
    X_test, y_true = self._convert_rete_to_tensor(rete_test)
    y_pred = self.predict_batch(X_test)
    mae = torch.mean(torch.abs(y_true - y_pred)).item()
    rmse = torch.sqrt(torch.mean((y_true - y_pred)**2)).item()
    corr = torch.corrcoef(torch.stack([y_true, y_pred]))[0,1].item() if

```

```

len(y_true) > 1 else 0.0
    return {'MAE': mae, 'RMSE': rmse, 'Correlation': corr}

def save_model(self, filepath: str):
    data = {
        'rules': [
            {'conditions': r.conditions, 'coeffs':
r.coeffs.detach().cpu()}
            for r in self.rules
        ],
        'factor_names': self.factor_names,
        'terms_num': self.terms_num,
        'poly_degree': self.poly_degree
    }
    with open(filepath, 'wb') as f:
        pickle.dump(data, f)
    print(f"Model saved in {filepath}")

def load_model(self, filepath: str):
    with open(filepath, 'rb') as f:
        data = pickle.load(f)

    self.rules = nn.ModuleList()
    self.poly_degree = data.get('poly_degree', 1)
    self.factor_names = data.get('factor_names', self.DEFAULT_FACTORS)
    self.terms_num = data.get('terms_num', self.DEFAULT_TERMS)
    self.feature_names = self._get_feature_names(self.poly_degree)

    for r_data in data['rules']:
        r = BetaNode(r_data['conditions'],
poly_degree=self.poly_degree)
        r.coeffs = nn.Parameter(r_data['coeffs'].to(device))
        r.frozen_mask = torch.ones_like(r.coeffs, device=device)
        self.rules.append(r)

    print(f"Model loaded from {filepath}")

```

### Лістинг Е.8 – Код реалізації модуля 7. Оптимізація керованих факторів.

```

import sympy as sp
import re

class OptimizeFactors:
    def __init__(self, fixed_vars=None, controlled_vars=None,
anfis_model=None):
        self.fixed_vars = fixed_vars or {}
        self.controlled_vars = controlled_vars or []
        self.all_vars = list(self.fixed_vars.keys()) + self.controlled_vars
        self.n_controlled = len(self.controlled_vars)
        self.symbolic_vars = {i: sp.Symbol(f'x{i}')} for i in self.all_vars}
        self.coefficients = self.parse_anfis_equation(anfis_model)

    def parse_anfis_equation(self, anfis_model):

```

```

        try:
            equation = anfis_model.get_global_polynomial_equation() #'R =
sigmoid(-0.2368 + 0.1729*x1 + 0.2806*x2 + 0.5089*x3 + -0.1797*x4 + -
0.3102*x5 + -0.2650*x6 + 0.0692*x1^2 + 0.1531*x2^2 + 0.1989*x3^2 + -
0.0785*x4^2 + -0.1460*x5^2 + -0.1147*x6^2 + 0.0911*x1*x2 + 0.1152*x1*x3 +
0.1166*x2*x3 + 0.1142*x3*x4 + 0.0943*x3*x5 + 0.0935*x3*x6 + -0.1170*x4*x5 +
-0.1024*x4*x6 + -0.1338*x5*x6)' #
            print(f"Отримане рівняння з ANFIS: {equation}")
            return self._parse_equation_string(equation)
        except Exception as e:
            return print(f"Помилка отримання рівняння з ANFIS: {e}")

def _parse_equation_string(self, equation_str):

    coefficients = {
        'const': 0.0,
        'linear': {},
        'quadratic': {},
        'interaction': {}
    }

    equation_clean = equation_str.replace('\R = sigmoid(',
'').replace(')', '').strip()
    pattern = r'([+-]?\s*\d+\.? \d*)\s*\*?\s*([a-zA-Z0-9^]*)'
    matches = re.findall(pattern, equation_clean)

    for coef_str, var_part in matches:
        coef_str = coef_str.replace(' ', '')
        if coef_str == '+' or coef_str == '':
            coefficient = 1.0
        elif coef_str == '-':
            coefficient = -1.0
        else:
            coefficient = float(coef_str)

        if var_part == '':
            coefficients['const'] += coefficient
        else:
            if '^2' in var_part:
                var_idx = int(var_part.replace('x', '').replace('^2',
''))
                coefficients['quadratic'][var_idx] = coefficient
            elif '*' in var_part:
                vars = var_part.split('*')
                var1 = int(vars[0].replace('x', ''))
                var2 = int(vars[1].replace('x', ''))
                if var1 > var2:
                    var1, var2 = var2, var1
                coefficients['interaction'][(var1, var2)] = coefficient
            else:
                var_idx = int(var_part.replace('x', ''))
                coefficients['linear'][var_idx] = coefficient

    return coefficients

```

```

def build_symbolic_expression(self):
    expr = self.coefficients['const']

    for i, coef in self.coefficients['linear'].items():
        if i in self.symbolic_vars:
            expr += coef * self.symbolic_vars[i]

    for i, coef in self.coefficients['quadratic'].items():
        if i in self.symbolic_vars:
            expr += coef * self.symbolic_vars[i] ** 2

    for (i, j), coef in self.coefficients['interaction'].items():
        if i in self.symbolic_vars and j in self.symbolic_vars:
            expr += coef * self.symbolic_vars[i] *
self.symbolic_vars[j]

    return expr

def get_simplified_function(self):
    full_expr = self.build_symbolic_expression()
    substitutions = [(self.symbolic_vars[i], value)
                      for i, value in self.fixed_vars.items()]
    simplified_expr = full_expr.subs(substitutions)

    return simplified_expr

def get_gradient(self):
    simplified_expr = self.get_simplified_function()

    gradient = {}
    for var_idx in self.controlled_vars:
        var_symbol = self.symbolic_vars[var_idx]
        derivative = sp.diff(simplified_expr, var_symbol)
        gradient[var_idx] = derivative

    return gradient

def _safe_float_conversion(self, expr, default=0.0):
    try:
        simplified = sp.simplify(expr)
        if simplified.is_number:
            return float(simplified)
        else:
            return float(simplified.evalf())
    except (TypeError, ValueError):
        return default

def analyze_derivative_behavior(self):
    print("\nПоведінка похідних:")

    gradient = self.get_gradient()
    optimal_strategy = {}
    analysis = {}

    for var_idx in self.controlled_vars:

```

```

deriv_expr = gradient[var_idx]
print(f"Похідна для x{var_idx}: {deriv_expr}")

test_cases = [
    {self.symbolic_vars[v]: 0 for v in self.controlled_vars},
    {self.symbolic_vars[v]: 1 for v in self.controlled_vars},
    {self.symbolic_vars[v]: 0.5 for v in self.controlled_vars}
]

deriv_signs = []
for i, test_case in enumerate(test_cases):
    deriv_value = deriv_expr.subs(test_case)
    deriv_float = self._safe_float_conversion(deriv_value)
    deriv_signs.append(deriv_float)

    case_names = ["всі дорівнюють 0", "всі дорівнюють 1", "всі
дорівнюють 0,5"]
    print(f"    При {case_names[i]}: df/dx{var_idx} =
{deriv_float:.6f}")

    if all(d > 0 for d in deriv_signs):
        optimal_value = 0.0
        strategy = "Функція завжди зростає"
        reasoning = "Похідна завжди > 0"

    elif all(d < 0 for d in deriv_signs):
        optimal_value = 1.0
        strategy = "Функція завжди спадає"
        reasoning = "Похідна завжди < 0"

    else:
        optimal_value = self.find_zero_gradient(var_idx)
        strategy = f"Оптимум при {optimal_value:.4f}"
        reasoning = "Знак похідної змінюється, оптимум всередині
діапазону"

    optimal_strategy[var_idx] = optimal_value
    analysis[var_idx] = {
        'derivative': deriv_expr,
        'strategy': strategy,
        'reasoning': reasoning,
        'optimal_value': optimal_value,
        'derivative_signs': deriv_signs
    }

    print(f"{strategy}. {reasoning}")

return optimal_strategy, analysis

def find_zero_gradient(self, var_idx):
    try:
        gradient = self.get_gradient()
        deriv_expr = gradient[var_idx]
        other_vars = [v for v in self.controlled_vars if v != var_idx]
        substitutions = [(self.symbolic_vars[i], 0.5) for i in

```

```

other_vars]
    simplified_deriv = deriv_expr.subs(substitutions)
    simplified_deriv = sp.simplify(simplified_deriv)
    solutions = sp.solve(simplified_deriv,
self.symbolic_vars[var_idx])
    real_solutions = []
    for s in solutions:
        try:
            s_eval = self._safe_float_conversion(s)
            if 0 <= s_eval <= 1:
                real_solutions.append(s_eval)
        except:
            continue

    if real_solutions:
        return float(real_solutions[0])
    else:
        test_min =
simplified_deriv.subs([(self.symbolic_vars[var_idx], 0)])
        test_max =
simplified_deriv.subs([(self.symbolic_vars[var_idx], 1)])

        test_min_float = self._safe_float_conversion(test_min)
        test_max_float = self._safe_float_conversion(test_max)

        if test_min_float < 0 and test_max_float > 0:
            return 0.5
        elif test_min_float < 0:
            return 1.0
        else:
            return 0.0

    except Exception as e:
        print(f"Помилка при пошуку нуля градієнта: {e}")
        return 0.5

def comprehensive_analysis(self):

    print("Сталі фактори (зовнішні ризики):")
    for var_idx, value in self.fixed_vars.items():
        print(f"  x{var_idx} = {value}")
    print("Керовані змінні (важелі впливу):")
    for var_idx in self.controlled_vars:
        print(f"  x{var_idx} = [0, 1]")

    optimal_values, analysis = self.analyze_derivative_behavior()
    self._analyze_strategy_implications(optimal_values, analysis)

    return optimal_values, analysis

def _analyze_strategy_implications(self, optimal_values, analysis):
    print(f"\nПРАКТИЧНІ РЕКОМЕНДАЦІЇ:")
    all_max = all(v == 1.0 for v in optimal_values.values())
    all_min = all(v == 0.0 for v in optimal_values.values())

```

```

        if all_max:
            print("• Рекомендація: Максимізувати всі заходи контролю")
            print("• Обґрунтування: В умовах високих зовнішніх ризиків
необхідно")
            print("  застосовувати максимально доступний захист")
            print("• Пріоритет: Комплексний підхід до управління ризиками")

        elif all_min:
            print("• Рекомендація: Мінімізувати втручання")
            print("• Обґрунтування: Зовнішні ризики низькі, надмірний
контроль")
            print("  може бути неефективним використанням ресурсів")
            print("• Пріоритет: Моніторинг та готовність до реагування")

        else:
            print("• Рекомендація: Диференційований підхід")
            print("• Обґрунтування: Різні фактори потребують різного рівня
контролю")
            print("• Пріоритет: Балансування між ефективністю та
ресурсами")

    print(f"\nДЕТАЛЬНІ РЕКОМЕНДАЦІЇ:")
    for var_idx in self.controlled_vars:
        opt_val = optimal_values[var_idx]

        if opt_val == 1.0:
            action = "Максимально активувати"
        elif opt_val == 0.0:
            action = "Мінімально втручатися"
        else:
            action = "Підтримувати на оптимальному рівні"

        print(f"  x{var_idx}: {action} ({opt_val:.3f})")

```