ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

САЛІЄВА ОЛЬГА ВОЛОДИМИРІВНА

УДК 004.056.5:004.81(043.5)

ДИСЕРТАЦІЯ

МОДЕЛІ ТА ЗАСОБИ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ КОГНІТИВНОГО МОДЕЛЮВАННЯ

125 «Кібербезпека»
12 «Інформаційні технології»

Подається на здобуття ступеня доктора філософії

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

Науковий керівник: Яремчук Юрій Євгенович,
доктор технічних наук, професор

Вінниця – 2021

АНОТАЦІЯ

Салієва О. В. Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (12 «Інформаційні технології»). – Вінницький національний технічний університет, Вінниця, МОН України. – Національний університет «Львівська політехніка», МОН України, Львів, 2021.

Дисертаційна робота присвячена актуальним питанням розробки функціональних когнітивних моделей для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, для підвищення їхньої захищеності та розробки програмних засобів для реалізації оцінювання за запропонованими моделями.

У роботі отримано такі наукові результати:

1. Вперше запропоновано модель оцінювання рівня захищеності об’єкта критичної інфраструктури на основі когнітивного підходу, який надає можливість спростити розрахунки та зменшити час обробки вхідної інформації; покращити наочність представлення даних; при побудові когнітивної карти врахувати як кількісні, так і якісні фактори; за потреби легко розширити їх кількість, за рахунок введення додаткових вершин і дуг графа когнітивної карти; визначити найвагоміші фактори, зокрема, визначено такі фактори як захищеність системи захисту інформації, інсайдерський вплив, захищеність комп’ютерної мережі; проводити сценарне моделювання, у результаті якого визначено, що рівень захищеності об’єкта критичної інфраструктури підвищиться на 2 % при максимально позитивному впливі найвагоміших факторів.

2. Вперше запропоновано модель оцінювання рівня захищеності системи захисту інформації на основі когнітивного підходу з використанням нечітких когнітивних карт, який дозволяє збільшити швидкість обробки вхідної інформації та зменшити час на її опрацювання; покращити наочність представлення даних;

використовувати неповну, нечітку інформацію та суб'єктивні судження експертів предметної області; врахувати як кількісні, так і якісні фактори, що впливають на захищеність системи захисту інформації; виявити найвагоміші фактори, зокрема, як такі, визначено фізичний захист, організаційне забезпечення захисту інформації, несанкціонований доступ до інформації зловмисником; проводити сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності системи захисту інформації підвищиться на 19 % при максимально позитивному впливі найвагоміших факторів.

3. Вдосконалено модель для оцінювання рівня захищеності комп'ютерної мережі на основі когнітивного підходу з використанням нечітких когнітивних карт, яка більш точно відображає предметну область та надає можливість краще враховувати мінливість характеру процесів, що відбуваються у досліджуваній системі, у часі; визначити найвагоміші загрози комп'ютерної мережі, зокрема, як такі, визначено шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі; проводити сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності комп'ютерної мережі підвищиться на 63 % при максимальному послабленні впливу найвагоміших загроз.

4. Отримав подальшого розвитку підхід до визначення допустимих витрат на забезпечення захищеності об'єкта критичної інфраструктури й системи захисту інформації та допустимої інтенсивності зниження рівня їхньої захищеності на основі ранжування загроз із використанням теорії нечітких відношень, який надає можливість зменшити час обробки вхідної інформації та спростити проміжні розрахунки, оперуючи нечіткими вхідними даними і здійснюючи нечітку формалізацію критеріїв оцінювання; проводити не тільки кількісне, а й якісне оцінювання як вхідних даних, так і вихідних результатів.

Практичне значення отриманих результатів роботи полягає у:

1. Розробці структури програми для реалізації оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, у вигляді семи взаємозалежних програмних модулів: модуля створення концептів,

модуля створення і присвоєння сили зв’язку між концептами, модуля побудови матриці суміжності, модуля візуалізації та редагування моделі, модуля обчислення системних показників нечіткої когнітивної карти, модуля динамічного часового аналізу та модуля дослідження імпульсних процесів на когнітивній карті. Здійснено програмну реалізацію запропонованих модулів.

2. Розробці програмних засобів для реалізації оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, за запропонованими когнітивними моделями дослідження захищеності комп’ютерної мережі, системи захисту інформації та об’єкта критичної інфраструктури.

3. Доведенні достовірності впливу загроз на рівень захищеності комп’ютерної мережі, системи захисту інформації та об’єкта критичної інфраструктури, визначеного за результатами когнітивного моделювання. Отримані результати надають можливість спрогнозувати розвиток ситуації для прийняття вчасних та ефективних управлінських рішень, спрямованих на підвищення захищеності досліджуваних систем захисту інформації, що циркулює в інформаційних системах.

4. Проведені динамічного часового аналізу впливу факторів загроз на рівень захищеності об’єкта критичної інфраструктури, у результаті якого було визначено та здійснено порівняння рівнів впливу досліджуваних загроз на захищеність даного об’єкту у різні моменти часу.

5. Проведені симпліціального аналізу структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури, у результаті якого було сформовано множину управляючих для всієї системи концептів та встановлено взаємозв’язні концепти, вплив на які всередині кожного блоку дозволить за найменших зусиль підвищити рівень захищеності досліджуваного об’єкта.

6. Дослідженні розвитку у часі когнітивної моделі для визначення зміни рівня захищеності системи захисту інформації, шляхом введення імпульсних впливів у концепти когнітивної карти, що надало змогу прослідкувати

еволюційний розвиток системи та сприятиме підвищенню ефективності прогнозування розвитку ситуацій при впливі ймовірних загроз.

На основі аналізу сучасних методів та моделей оцінювання впливу загроз на рівень інформаційної безпеки, встановлено, що більшість з них потребують складних розрахунків й тривалого часу для опрацювання вхідних даних. Зазначені проблеми дозволяють вирішити методи когнітивного моделювання. Проте переважна більшість проаналізованих когнітивних моделей орієнтована на проведення аналізу стану інформаційної безпеки, оцінювання ризиків її порушення, але не забезпечує безпосереднього визначення зміни рівня захищеності системи при впливі на неї потенційних загроз. Проведений аналіз дозволили окреслити завдання, що потребують подальших наукових досліджень для їх практичного використання.

Розроблено когнітивні моделі для оцінювання рівня захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури. На основі структурно-топологічного аналізу визначено основні показники нечітких когнітивних карт та найвагоміші загрози захищеності досліджуваних систем. Для отримання прогнозів розвитку ситуації на основі сценарного моделювання визначено відносну зміну рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, при максимальному впливі найвагоміших загроз. Достовірність отриманих результатів доведено за допомогою множинного регресійного аналізу.

Використовуючи теорію нечітких відношень, здійснено ранжування загроз, що стало основою для пропорційного розподілу допустимих витрат на забезпечення захищеності системи захисту інформації та об'єкта критичної інфраструктури. Отримані результати є корисними для встановлення балансу між рівнем інформаційного ризику та допустимими витратами на проведення заходів інформаційної безпеки. Крім того, на основі визначених рангів загроз встановлено допустиму інтенсивність зниження рівня захищеності досліджуваних систем, що сприятиме вчасному впровадженню ефективних механізмів протидії загрозам, раціональному перерозподілу сил і засобів для їхньої нейтралізації.

Проведено симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури, на основі якого визначено управляючі та зв’язні концепти системи. Вплив на взаємозв’язані всередині кожного блоку концепти симпліціального комплексу дозволить при найменших зусиллях підвищити рівень захищеності об’єкта критичної інфраструктури.

Здійснено динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта критичної інфраструктури, який надає можливість визначити зміну рівня захищеності даного об’єкта у часі при впливі конкретних загроз та порівняти силу даних впливів.

Проведено дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту інформації. У результаті чого, розглянуто еволюційний розвиток системи при введенні збурень у досліджувані концепти та встановлено найвпливовіші з них.

Для реалізації запропонованих моделей розроблено програмні засоби, які дозволяють зменшити час на опрацювання вхідних даних, збільшити швидкість їх обробки та покращити наочність досліджуваної системи.

Одержані наукові результати впроваджено у Головному управлінні Пенсійного фонду України у Вінницькій області (акт про впровадження від 01.10.2020 р.), Хмельницькому зональному відділі Військової служби правопорядку (акт про впровадження від 16.11.2020 р.), відокремленому підрозділі «Південно-Західна електроенергетична система» ПАТ «Національна енергетична компанія «Укренерго» (акт про впровадження від 20.11.2020 р.) та у навчальному процесі Вінницького національного технічного університету на кафедрі менеджменту та безпеки інформаційних систем для підготовки фахівців за спеціальністю 125 «Кібербезпека» (акт про впровадження від 16.11.2020 р.).

Ключові слова: інформаційна безпека, загрози безпеці, система захисту інформації, рівень захищеності, когнітивне моделювання, нечітка когнітивна карта, нечітке відношення, транзитивне замикання, регресійний аналіз, симпліціальний аналіз, імпульсне моделювання.

ABSTRACT

Saliieva O. V. Models and means of assessing the level of security of information security systems based on cognitive modeling. – Qualifying scientific work on the rights of the manuscript.

Thesis for the degree of PhD in the specialty 125 "Cybersecurity" (12 "Information Technology"). - Vinnytsia National Technical University, Vinnytsia, Ministry of Education and Science of Ukraine. - Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2021.

The dissertation is devoted to actual issues of development of functional cognitive models for assessing the level of security of information security systems circulating in information systems, to increase their security and development of software for the implementation of assessment of the proposed models.

The following scientific results were obtained in the work:

1. For the first time, a model for estimating the level of protection of a critical infrastructure object on the basis of a cognitive approach has been proposed, which provides an opportunity to simplify calculations and reduce the processing time of input information; improve the clarity of the input data; when constructing a cognitive map to take into account both quantitative and qualitative factors; if necessary, it is easy to expand their number by introducing additional vertices and arcs of the graph of the cognitive map; identify the most important factors, in particular, identified such factors as security of the information security system, insider influence, security of the computer network; to conduct scenario modeling, as a result of which it is determined that the level of protection of the critical infrastructure will increase by 2% with the maximum positive impact of the most important factors.

2. For the first time, a model for assessing the level of security of the information security system based on a cognitive approach using fuzzy cognitive maps, which allows to increase the processing speed of input information and reduce the time for its processing; improve the clarity of data presentation; use incomplete, fuzzy information and subjective judgments of subject matter experts; take into account both quantitative

and qualitative factors that affect the security of the information security system; identify the most important factors, in particular, as defined physical protection, organizational support for information protection, unauthorized access to information by an attacker; to conduct scenario modeling of the situation development, as a result of which it is determined that the level of security of the information protection system will increase by 19% with the most positive influence of the most important factors.

3. Improved model for assessing the level of security of a computer network based on a cognitive approach using fuzzy cognitive maps, which more accurately reflects the subject area and allows better consideration of the variability of the processes occurring in the system over time; identify the most important threats to the computer network, in particular, as identified malware, physical impact on the network by an attacker and unintentional actions, errors of network users; to conduct scenario modeling of the development of the situation, as a result of which it is determined that the level of security of the computer network will increase by 63% with the maximum mitigation of the impact of the most important threats.

4. The approach to determining the allowable costs for ensuring the security of critical infrastructure and information security system and the allowable intensity of reducing their security based on threat ranking using fuzzy relationship theory, which allows to reduce the processing time of input information and simplify intermediate calculations, operating with fuzzy input data and carrying out fuzzy formalization of evaluation criteria; to conduct not only quantitative but also qualitative evaluation of both input data and output results.

The practical significance of the obtained results of work is:

1. Development of a program structure for implementing the assessment of the level of security of information security systems circulating in information systems, in the form of seven interdependent software modules: module for creating concepts, module for creating and assigning communication between concepts, module for constructing adjacency matrix, visualization module and editing of the model, the module of calculation of system indicators of fuzzy cognitive map, the module of dynamic time analysis and the module of research of pulse processes on the cognitive

map. The software implementation of the offered modules is carried out.

2. Development of a software to implement the assessment of the level of security of information security systems circulating in information systems, according to the proposed cognitive models of the study of computer network security, information security system and critical infrastructure.

3. Proving the reliability of the impact of threats on the level of security of the computer network, information security system and critical infrastructure, determined by the results of cognitive modeling. The obtained results provide an opportunity to predict the development of the situation for timely and effective management decisions aimed at improving the security of the studied information security systems circulating in information systems.

4. Conducted a dynamic time analysis of the impact of threat factors on the level of protection of critical infrastructure, which identified and compared the levels of impact of the studied threats on the security of this object at different times.

5. Simplified analysis of the structure of the cognitive model to study the level of protection of critical infrastructure, which resulted in the formation of a set of control concepts for the whole system and established interconnected concepts, the impact of which within each block will allow to increase the level of protection. object.

6. Study of the development of the cognitive model over time to determine the change in the level of security of the information security system, by introducing impulse influences into the concepts of the cognitive map, which allowed to trace the evolutionary development of the system and help improve forecasting.

Based on the analysis of modern methods and models for assessing the impact of threats on the level of information security, it was found that most of them require complex calculations and long time to process the input data. These problems can be solved by methods of cognitive modeling. However, the vast majority of analyzed cognitive models are focused on analyzing the state of information security, assessing the risks of its violation, but does not provide a direct determination of changes in the level of security of the system under the influence of potential threats. The analysis allowed to outline the tasks that require further research for their practical use.

Cognitive models have been developed to assess the level of security of a computer network, information security system and critical infrastructure. Based on the structural and topological analysis, the main indicators of fuzzy cognitive maps and the most significant threats to the security of the studied systems are determined. To obtain forecasts of the situation on the basis of scenario modeling, a relative change in the level of security of information security systems circulating in information systems, with the maximum impact of the most important threats. The reliability of the obtained results was proved by multiple regression analysis.

Using fuzzy relationship theory, threat ranking was performed, which became the basis for the proportional distribution of allowable costs to ensure the security of the information security system and the critical infrastructure. The obtained results are useful for establishing a balance between the level of information risk and eligible costs for information security measures. In addition, on the basis of certain ranks of threats, the allowable intensity of reducing the level of protection of the studied systems has been established, which will facilitate the timely implementation of effective mechanisms to counter threats, rational redistribution of forces and means to neutralize them.

A simplicial analysis of the structure of the cognitive model was conducted to study the level of protection of the critical infrastructure object, on the basis of which the control and coherent concepts of the system were determined. Influencing the interconnected concepts of the simplicial complex within each block will allow to increase the level of protection of the critical infrastructure object with the least effort.

A dynamic temporal analysis of the impact of threat factors on the level of protection of critical infrastructure is performed, which provides an opportunity to determine the change in the level of protection of this object over time under the influence of specific threats and compare the strength of these impacts.

The study of impulse processes on the cognitive map to determine the change in the level of security of the information security system. As a result, the evolutionary development of the system during the introduction of changes into the studied concepts is considered and the most influential of them are established.

To implement the proposed models, software tools have been developed that allow to reduce the time for processing input data, increase the speed of their processing and improve the visibility of the studied system.

The obtained scientific results were implemented in the Main Department of the Pension Fund of Ukraine in Vinnytsia region (certificate of implementation of 01.10.2020), Khmelnytsky zonal department of the Military Law Enforcement Service (certificate of implementation of 16.11.2020), a separate subdivision of "South-Western Electric Power system" of PJSC "National Energy Company "Ukrenergo" (certificate of implementation of 20.11.2020) and in the educational process of Vinnytsia National Technical University at the Department of Management and Security of Information Systems for training specialists in the specialty 125 "Cybersecurity" (certificate of implementation of 16.11.2020).

Keywords: information security, security threats, information security system, level of security, cognitive modeling, fuzzy cognitive map, fuzzy relationship, transient closure, regression analysis, simplicial analysis, pulse modeling.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

[1] О. В. Салієва, та Ю. Є. Яремчук, «Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі», *Реєстрація, зберігання і обробка даних*, т. 21, № 4, с. 28–39, 2019.

[2] N. Mumtaz, A. Begum, B. Gul, S. Noor, R. Odarchenko, I. Machalin and O. Saliieva «Semantic, Digitization, Design and Implementation of Ontology in Social Internet-Services», *Conflict Management in Glodal Information Networks*, vol. 2588, pp. 228-249, 2019.

[3] О. В. Салієва, та Ю. Є. Яремчук, «Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання», *Безпека інформації*, т. 26, № 1, с. 42-49, 2020.

[4] О. В. Салієва, та Ю. Є. Яремчук, «Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень», *Захист інформації*, т. 22, № 1, с. 51–59, 2020.

[5] О. В. Салієва, та Ю. Є. Яремчук, «Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури», *Безпека інформації*, т. 26, № 2, с. 64-73, 2020.

[6] О. В. Салієва, та Ю. Є. Яремчук, «Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз», *Реєстрація, зберігання і обробка даних,* т. 22, № 2, с. 63-76, 2020.

[7] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу», *Вісник Вінницького політехнічного інституту,* № 4, с. 98-104, 2020.

[8] О. В. Салієва, та Ю. Є. Яремчук, «Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури», *Захист інформації,* т. 22, №3, с. 148–157, 2020.

[9] О. В. Салієва, та Ю. Є. Яремчук, «Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об'єкта критичної

інфраструктури», *Реєстрація, зберігання і обробка даних,* т. 22, №3, с. 68-75, 2020.

[10] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури за результатами когнітивного моделювання», *Вісник Черкаського державного технологічного університету,* №3, с. 85-93, 2020.

[11] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності систем захисту інформації», *Вісник Вінницького політехнічного інституту,* №5, с. 56-62, 2020.

[12] О. В. Салієва, «Системологічне дослідження суб'єктів захисту інформації», у *Матеріалах XLV науково-технічної конференції підрозділів ВНТУ*, м. Вінниця, 2016, с. 2190-2191.

[13] О. В. Салієва, Я. Ю. Яремчук, «Порівняння моделей інформаційної безпеки за характеристиками суб'єктів», у *Матеріалах конференції «Управління знаннями та конкурентна розвідка»,* м. Харків, 2019, с. 67-68.

[14] О. В. Салієва, «Аналіз впливу загроз безпеці комп'ютерної мережі з використанням когнітивного моделювання», у *Матеріалах XLVII науково-технічної конференції підрозділів ВНТУ*, м. Вінниця, 2020, с. 2725-2726.

[15] О. В. Салієва, «Оцінювання рівня захищеності системи безпеки на основі когнітивного моделювання», у *Матеріалах всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи»*, м. Вінниця, 2020, с. 1215-1216.

[16] О. В. Салієва, «Визначення витрат на забезпечення захищеності системи захисту інформації ранжуванням загроз», у *Матеріалах VI Міжнародної науково-практичної конференції «Перспективні напрями захисту інформації»*, м. Одеса, 2020, с. 83-84.

[17] Ю. Є. Яремчук, О. В. Салієва, «Оцінювання рівня захищеності об'єкта критичної інфраструктури», у *Матеріалах науково-практичної конференції*

«Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання», м. Київ, 2020, с. 280-281.

[18] О. В. Салієва, «Визначення впливу загроз на рівень захищеності комп’ютерної мережі за когнітивною моделлю на основі регресійного аналізу», *у Матеріалах науково-технічної конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології»,* м. Київ, 2020, с. 105-106.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизована система;

ЗІ – захист інформації;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційна технологія;

КІ – критична інфраструктура;

КМ – комп’ютерна мережа;

КСЗІ – комплексна система захисту інформації;

НКК – нечітка когнітивна карта;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення.

ВСТУП

Обґрунтування вибору теми дослідження. Активна інформатизація сучасного суспільства та збільшення потоків конфіденційної інформації спричинили необхідність забезпечення інформаційної безпеки (ІБ) у різних сферах суспільної діяльності. Адже, будь-які процеси у фінансовій, промисловій, політичній або соціальній галузях безпосередньо пов’язані з інформаційними ресурсами та використанням інформаційних технологій (ІТ).

У той же час, у зв’язку із зростаючою складністю інформаційних систем (ІС) та технологій, збільшується й кількість потенційних загроз цим системам. Тому для забезпечення ІБ та прогнозування розвитку конкретних ситуацій важливе місце займає оцінювання рівня захищеності систем захисту інформації (ЗІ), що циркулює в ІС.

Вирішення даного питання можливе за допомогою методів статистичного аналізу, зокрема кореляційно-регресійного. Проте дані методи потребують складних розрахунків, значної кількості експериментальних даних, тривалого часу для їх опрацювання і не забезпечують можливості роботи з якісними факторами, які визначаються експертним шляхом. У зв’язку з цим варто звернути увагу на когнітивний підхід, що базується на побудові нечітких когнітивних карт (НКК), вперше запропонованих Бартом Коско.

Пріоритетом вибору НКК є їхня простота, конструктивність та наочність, виявлення структури причинно-наслідкових зв’язків між елементами складної системи, які важко піддаються кількісному аналізу традиційних методів, використання знань та досвіду експертів предметної області, адаптація до невизначеності вихідних даних та умов досліджуваної задачі. Крім того, варто зауважити простоту розширення факторів за рахунок введення додаткових вершин та дуг графа когнітивної карти.

Значний внесок у розвиток когнітивного моделювання внесли такі вчені: Авдєєва З. К., Борисов В. В., Горелова Г. В., Кузнєцов О. П., Кулініч А. А., Максимов В. І., Ротштейн О. П., Сальмерон Дж., Силов В. Б., Толмен Дж., Федулов А. С. та ін.

Водночас, вирішення питань ІБ на основі когнітивного підходу висвітлюється у роботах Ажмухамедова І. М., Васільєва В. І., Вульфіна М. Б., Камаєва В. А., Машкіної І. В., Натрова В. В., Скжинського П., Степанової К. С., Шведа Р. та ін. Переважна більшість даних досліджень орієнтована на проведення аналізу стану ІБ, оцінювання ризиків її порушення, проте не забезпечують безпосереднього визначення зміни рівня захищеності системи при впливі на неї потенційних загроз. Тому *актуальною є наукова задача* спрямована на оцінювання рівня захищеності систем ЗІ, що циркулює в ІС при впливі потенційних загроз на основі когнітивного моделювання. З огляду на це, доцільною є розробка та аналіз відповідних когнітивних моделей, які дозволять спрогнозувати поведінку досліджуваних систем у конкретних ситуаціях і, відповідно, вчасно розробити чіткий план для підвищення рівня їхньої захищеності.

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана в плані наукових досліджень, проваджених кафедрою менеджменту та безпеки інформаційних систем Вінницького національного технічного університету (ВНТУ). Дослідження виконувалися у Центрі інформаційних технологій та захисту інформації ВНТУ і науково-дослідній лабораторії технічного захисту інформації ВНТУ.

Науково-дослідна робота проводилась відповідно до тематики науково-дослідної роботи ВНТУ. Зокрема, робота над дисертацією проводилася в рамках науково-дослідних та науково-технічних робіт:

– створення комплексної системи захисту інформації (КСЗІ) в автоматизованій системі (АС) відокремленого підрозділу «Південно-Західна електроенергетична система» Приватного акціонерного товариства «Національна енергетична компанія «Укренерго» №5261 від 27.05.2019 р.;

– створення КСЗІ в АС Хмельницького зонального відділу Військової служби правопорядку №5267 від 11.07.2019 р.;

– створення КСЗІ в АС Головного управління Пенсійного фонду України у Вінницькій області №5284 від 27.02.2020 р.

Мета і завдання дослідження. Метою роботи є підвищення рівня захищеності систем ЗІ, що циркулює в ІС, створенням функціональних когнітивних моделей для оцінювання рівня їхньої захищеності та програмних засобів реалізації цих моделей.

Відповідно до вказаної у роботі мети **потрібно вирішити такі основні завдання:**

– провести аналіз загроз системі ЗІ та існуючих моделей і засобів для оцінювання впливу загроз на рівень ІБ;

– розробити когнітивні моделі для визначення ступеню впливу загроз на рівень захищеності систем ЗІ, що циркулює в ІС;

– дослідити структурні властивості розроблених когнітивних моделей;

– провести сценарне моделювання для визначення відносної зміни рівня захищеності систем ЗІ, що циркулює в ІС;

– дослідити достовірність впливу загроз на рівень захищеності систем ЗІ, що циркулює в ІС, визначеного за сценарним моделюванням на основі когнітивного підходу;

– провести симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури (КІ);

– здійснити ранжування загроз системі ЗІ та об’єкту КІ для визначення допустимої інтенсивності зниження рівня їхньої захищеності й витрат на забезпечення захищеності даних систем;

– провести динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта КІ;

– дослідити імпульсні процеси на когнітивній карті для визначення зміни рівня захищеності системи ЗІ;

– розробити інструментальні програмні засоби для реалізації оцінювання рівня захищеності за запропонованими моделями.

Об’єктом дослідження дисертаційної роботи є оцінювання рівня захищеності систем ЗІ, що циркулює в ІС.

Предметом дослідження є моделі та засоби оцінювання рівня захищеності систем ЗІ на основі когнітивного підходу.

Методи дослідження. Для вирішення поставлених задач використовувалися: теорія забезпечення ІБ та ЗІ, методи системного аналізу, теорії когнітивного моделювання, теорії графів, нечіткої логіки, теорії множин, регресійного аналізу, динамічної каузальної алгебри, а також методи програмування.

Наукова новизна отриманих результатів.

1. Вперше запропоновано модель оцінювання рівня захищеності об’єкта КІ на основі когнітивного підходу з використанням НКК, який надає можливість спростити розрахунки та зменшити час обробки вхідної інформації; покращити наочність представлення вхідних даних; при побудові НКК врахувати як кількісні так і якісні фактори, що впливають на захищеність об’єкту; за потреби легко розширити кількість факторів, за рахунок введення додаткових вершин і дуг графа когнітивної карти; визначити найвагоміші фактори, зокрема, визначено такі фактори як захищеність системи ЗІ, інсайдерський вплив, захищеність комп’ютерної мережі (КМ); проводити сценарне моделювання, у результаті якого визначено, що рівень захищеності об’єкта КІ підвищиться на 2 % при максимально позитивному впливі найвагоміших факторів.

2. Вперше запропоновано модель оцінювання рівня захищеності системи ЗІ на основі когнітивного підходу з використанням НКК, який дозволяє збільшити швидкість обробки вхідної інформації та зменшити час на її опрацювання; покращити наочність представлення даних; використовувати неповну, нечітку інформацію та суб’єктивні судження експертів предметної області; врахувати як кількісні так і якісні фактори, що впливають на захищеність системи ЗІ; виявити найвагоміші фактори, зокрема, як такі, визначено фізичний захист, організаційне забезпечення ЗІ, НСД до інформації зловмисником; проводити сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності системи ЗІ підвищиться на 19 % при максимально позитивному впливі найвагоміших факторів.

3. Вдосконалено модель для оцінювання рівня захищеності КМ на основі когнітивного підходу з використанням НКК, яка більш точно відображає предметну область та надає можливість краще враховувати мінливість характеру процесів, які відбуваються у досліджуваній системі, в часі; визначити найвагоміші загрози КМ, зокрема, визначено такі як шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі; проводити сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності КМ підвищиться на 63 % при максимальному послабленні впливу найвагоміших загроз.

4. Отримав подальшого розвитку підхід до визначення допустимих витрат на забезпечення захищеності об’єкта КІ й системи ЗІ та допустимої інтенсивності зниження рівня їхньої захищеності на основі ранжування загроз із використанням теорії нечітких відношень, який надає можливість зменшити час обробки вхідної інформації та спростити проміжні розрахунки, оперуючи нечіткими вхідними даними і здійснюючи нечітку формалізацію критеріїв оцінювання; проводити не тільки кількісне, а й якісне оцінювання як вхідних даних, так і вихідних результатів.

Практичне значення отриманих результатів.

1. Розроблено структуру програми для реалізації оцінювання рівня захищеності систем ЗІ, що циркулює в ІС, у вигляді семи взаємозалежних програмних модулів: модуля створення концептів, модуля створення і присвоєння сили зв’язку між концептами, модуля побудови матриці суміжності, модуля візуалізації та редагування моделі, модуля обчислення системних показників НКК, модуля динамічного часового аналізу та модуля дослідження імпульсних процесів на когнітивній карті. Здійснено програмну реалізацію запропонованих модулів.

2. Розроблено програмні засоби для реалізації оцінювання рівня захищеності систем ЗІ, що циркулює в ІС, за запропонованими когнітивними моделями дослідження захищеності КМ, системи ЗІ та об’єкта КІ.

3. На основі множинного регресійного аналізу доведено достовірність впливу загроз на рівень захищеності КМ, системи ЗІ та об’єкта КІ, визначеного за результатами когнітивного моделювання. Отримані результати надають можливість спрогнозувати розвиток ситуації для прийняття вчасних та ефективних управлінських рішень, спрямованих на підвищення захищеності досліджуваних систем ЗІ, що циркулює в ІС.

4. Проведено динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта КІ, результати якого дозволяють визначити та порівняти рівні впливу досліджуваних загроз на захищеність даного об’єкта у різні моменти часу.

5. Здійснено симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об’єкта КІ, у результаті якого було сформовано множину управляючих для всієї системи концептів та встановлено взаємозв’язні вершини, вплив на які всередині кожного блоку дозволить за найменших зусиль підвищити рівень захищеності досліджуваного об’єкта.

6. Досліджено розвиток у часі когнітивної моделі для визначення зміни рівня захищеності системи ЗІ, шляхом введення імпульсних впливів у концепти когнітивної карти. Це дослідження надало змогу прослідкувати еволюційний розвиток системи, що сприятиме підвищенню ефективності прогнозування розвитку ситуацій при впливі ймовірних загроз.

Особистий внесок здобувача. Усі наукові положення, які є основним змістом дисертаційної роботи, розроблено та обґрунтовано здобувачем особисто.

У друкованих працях, опублікованих у співавторстві, автору дисертації належать: розробка та аналіз когнітивної моделі для визначення рівня захищеності КМ при впливі на неї потенційних загроз [1]; створення концепцій та опис взаємозв’язків між їхніми елементами, необхідними для розробки онтології домену, що підлягає семантичному оцифровуванню [2], це посприяло зародженню ідеї щодо опису системи за допомогою множини факторів, найвагоміших з точки зору вирішення досліджуваної проблеми, та взаємозв’язків між ними; розробка та аналіз когнітивної моделі на основі НКК, яка дозволяє

визначати рівень захищеності системи ЗІ [3]; ранжування загроз для визначення витрат на забезпечення захищеності системи ЗІ [4]; розробка та аналіз когнітивної моделі для дослідження рівня захищеності об'єкта КІ [5], [17]; порівняльний аналіз моделей ІБ за характеристиками суб'єктів [13]; визначення допустимої інтенсивності зниження рівня захищеності об'єкта КІ ранжуванням загроз [6]; дослідження достовірності впливу загроз на рівень захищеності КМ, визначеного за сценарним моделюванням на основі когнітивного підходу [7]; проведення динамічного часового аналіз впливу факторів загроз на рівень захищеності об'єкта КІ [8]; встановлення достовірності впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ за результатами когнітивного моделювання [10]; проведення симпліціального аналізу структури когнітивної моделі для дослідження рівня захищеності об'єкта КІ [9]; визначення зміни рівня захищеності системи ЗІ на основі імпульсного моделювання [11]. З робіт, що опубліковані в співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація матеріалів дисертації. Основні положення роботи та її результати доповідались, обговорювались та були схвалені на таких науково-технічних конференціях та семінарах: XLV науково-технічній конференції підрозділів ВНТУ (м. Вінниця, 2016 р.); 23-му Міжнародному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті», конференція «Управління знаннями та конкурентна розвідка» (м. Харків, 2019 р.); щорічному міжвідомчому міжрегіональному семінарі Наукової Ради НАН України «Технічні засоби захисту інформації» (м. Київ, 2020 р.); XLVII науково-технічній конференції підрозділів ВНТУ (м. Вінниця, 2020 р.); Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи», (м. Вінниця, 2020 р.); VI Міжнародній науково-практичній конференції «Перспективні напрями захисту інформації» (м. Одеса, 2020); науково-практичній конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання» (м. Київ, 2020); науково-технічній конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології» (м. Київ, 2020).

Публікації. За матеріалами дисертаційної роботи опубліковано 18 наукових праць, з яких 10 статей у наукових фахових виданнях України [1], [3] – [11], 1 стаття в науковому періодичному виданні іншої держави, яке включено до міжнародної наукометричної бази (Scopus) [2], 7 – у матеріалах і тезах конференцій [12] – [18].

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел (125 найменувань) і 5 додатків. Основний зміст викладено на 124 сторінках друкованого тексту, містить 30 рисунків, 21 таблицю. Загальний обсяг роботи – 208 сторінок.

РОЗДІЛ 1
АНАЛІЗ МЕТОДИК ТА МОДЕЛЕЙ ДЛЯ ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загальні положення інформаційної безпеки

Стрімкий розвиток процесу інформатизації сучасного суспільства зумовив необхідність забезпечення ІБ в усіх сферах людської діяльності. Адже реалізація цілеспрямованих або ненавмисних впливів на інформаційну сферу з боку як зовнішніх так і внутрішніх джерел може завдати шкоди безпеці та призвести до моральних, матеріальних, фінансових, репутаційних та інших збитків. Актуальність забезпечення ІБ пояснюється цінністю накопичених інформаційних ресурсів та критичною залежністю від ІТ.

Питання, що стосуються ІБ та визначають її правові аспекти, висвітлені у Конституції України [19], у Законах України: «Про національну безпеку України» [20], «Про концепцію національної програми інформатизації» [21], «Про захист інформації в інформаційно-телекомунікаційних системах» [22], «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [23], у «Доктрині інформаційної безпеки» [24], у «Стратегії кібербезпеки України» [25] та в інших нормативно-правових документах.

В статті 17 Конституції України зазначається, що найважливішими функціями держави, справою всього Українського народу є захист суверенітету і територіальної цілісності України, забезпечення її економічної та ІБ [19].

У [23] було дано визначення змісту поняття «інформаційної безпеки» як стану захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування ІТ; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Дещо в іншому ракурсі розглядається дане поняття у [21], а саме, ІБ визначається як невід’ємна частина політичної, економічної, оборонної та інших

складових національної безпеки. У [20] поняття «інформаційна безпека» не розкривається, увага фокусується на інформаційній сфері національної безпеки, перераховуються загрози та напрями державної політики. Не подається значення цього терміну і у [24], а лише визначаються мета та принципи ІБ, національні інтереси та актуальні їм загрози, пріоритети державної політики в інформаційній сфері.

Незважаючи на те, що ІБ протягом двох останніх десятиліть є об'єктом актуальних наукових досліджень, проте у науковій літературі немає єдиного цілісного погляду на зміст даного поняття. Вивченням загальнотеоретичних та окремих аспектів забезпечення ІБ займаються вітчизняні та зарубіжні дослідники, зокрема, В. А. Авраменко, В. М. Брижко, В. К. Гасеський, Р. А. Калюжний, В. А. Ліпкан, А. А. Тер-Акопов , В. О. Хорошко, М. П. Хрипков, В. І . Ярочкін та ін.

Так, наприклад, український дослідник В. А. Ліпкан характеризує ІБ як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування ІТ або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [26]. У той час як у роботі [27], під ІБ розуміється стан захищеності інформації, яка забезпечує життєво важливі інтереси людини. На думку авторів роботи [28], ІБ – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні ІТ, інфраструктури та інформаційних ресурсів, ЗІ й прав суб'єктів, що беруть участь в інформаційній діяльності. Р. А. Калюжний вважає, що ІБ – вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації [29].

Таким чином, ІБ являє собою комплексне та системне поняття, яке визначається динамічним характером сучасного інформаційного суспільства, тому її слід досліджувати через призму єдності усіх її елементів.

Діяльність із забезпечення ІБ повинна здійснюватися на основі певних принципів таких як законність, баланс інтересів особи, суспільства і держави, комплексність, системність, інтеграція з міжнародними системами безпеки, економічна ефективність [30]. При цьому використовують різні способи, засоби і прийоми, які у сукупності складають методи.

Важливими методами аналізу стану забезпечення ІБ є методи опису і класифікації. Для здійснення ефективного інформаційного захисту слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і, відповідно, сформулювати систему заходів для управління ними. У якості розповсюджених методів аналізу рівня забезпечення ІБ використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи щодо їхньої нейтралізації. Вибір методів аналізу стану забезпечення ІБ залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. У сфері ІБ, зазвичай, виділяють такі рівні захисту [31]:

– фізичний: здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних та управлінських технологій;

– програмно-технічний: здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності;

– управлінський: здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів;

– технологічний: здійснюється реалізація політики ІБ за рахунок застосування комплексу сучасних автоматизованих ІТ;

– рівень користувача: реалізація політики ІБ спрямована на зменшення рефлексивного впливу на об'єкти ІБ, унеможливлення інформаційного впливу з боку соціального середовища;

– рівень інформаційно-телекомунікаційних мереж: дана політика реалізується у форматі координації дій суб'єктів системи ІБ, які пов'язані між собою однією метою;

– процедурний: вживаються заходи, що реалізуються суб'єктами (управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування відновлювальних робіт та ін.).

Також серед методів забезпечення ІБ можна виділити декілька типів [32]:

– однорівневі методи будуються на підставі одного принципу управління ІБ;

– багаторівневі методи будуються на основі декількох принципів управління ІБ, кожен з яких слугує вирішенню окремого завдання;

– комплексні методи – багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення ІБ, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

– інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Зауважимо, що ЗІ не обмежується тільки технічними методами. Для ефективного забезпечення ІБ важливе місце посідають різноманітні моделі та методи оцінювання загроз та небезпек. При цьому необхідною є ідентифікація можливих джерел загроз, факторів, що сприяють їхньому прояву (вразливостей) і, як наслідок, визначення актуальних загроз безпеці інформації. Притримуючись цього принципу, моделювання і класифікацію джерел загроз та їх проявів, можна проводити на основі аналізу взаємодії логічного ланцюга [33]:

Джерело загрози → Загроза → Вразливість → Реалізація загрози → Наслідки.

Причому загрози інформації виражаються у порушенні її цілісності, конфіденційності, повноти і доступності, а джерелами загроз можуть виступати

конкуренти, злочинці, корупціонери, адміністративно-управлінські органи тощо [34].

Для протидії загрозам ІБ вживаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку зниження вразливостей об’єкта безпеки. Відповідно виділяють дві предметні області протидії: одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів із забезпечення ІБ [32].

Отже, можна зробити висновок, що ІБ охоплює технічні, правові, організаційні, психологічні аспекти та зумовлює надзвичайну складність і багаторівневість системних зв’язків між елементами, що входять до її складу. В свою чергу, забезпечення ІБ є безперервним процесом, який має системний характер та досягається реалізацією найбільш раціональних методів та комплексним використанням необхідних засобів (фізичних, апаратних, програмних, криптографічних). При чому найкращий результат отримується тоді, коли всі використовувані засоби та методи об’єднані в цілісний механізм, функціонування якого має контролюватися, обновлюватися та доповнюватися в залежності від змін як внутрішнього так і зовнішнього середовища. Крім того, необхідно зауважити, що весь цей процес має супроводжуватися належною підготовкою спеціалістів даної галузі, адміністрації, співробітників, користувачів та дотриманням ними усіх встановлених правил.

1.2 Аналіз потенційних загроз інформаційній безпеці

Важливим фактором розвитку сучасного суспільства є забезпечення ІБ, яка є ключовим елементом будь-яких процесів незалежно від сфери суспільної діяльності. При цьому особлива увага приділяється аналізу потенційних загроз ІБ, реалізація яких призводить до матеріальних, фінансових, репутаційних та інших збитків.

Загрози характеризують можливі дії, які можуть бути здійсненні по відношенню до системи і, які можуть призвести до порушення основних сервісів, наприклад: цілісності, конфіденційності, доступності, достовірності інформації. Вони мають прояви у різноманітних формах. Згідно із [35] фактори, що

впливають на ІБ, можна класифікувати за такими ознаками:

– природою їх виникнення: об’єктивні та суб’єктивні;

– за місцем виникнення: внутрішні та зовнішні. Джерелом внутрішніх загроз є інсайдер: довірена особа, співробітник, підрядник або постачальник, який володіє інформацією, що, як правило, не відома на загал. Інсайдер може представляти собою загрозу навіть без злих намірів. А джерелом зовнішніх загроз є аутсайдер: особа або група осіб, які не мають права внутрішнього доступу (кримінальні структури, потенційні злочинці і хакери, терористи, не доброчесні партнери, представники силових структур, аварійних служб і т. п.) [36];

– за мотивацією: зловмисні та ненавмисні. Ненавмисні загрози виникають незалежно від волі і бажання людей: ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують ІС. Іноді такі помилки є загрозами (невірно введені дані, помилка в програмі, котра викликає колапс системи), іноді вони створюють ситуації, якими не лише можуть скористатися зловмисники, а які самі по собі становлять безпосередню небезпеку об’єкта [37]. Навмисні загрози, на відміну від ненавмисних, можуть бути створені тільки людьми, що діють цілеспрямовано з метою дезорганізувати роботу ІС.

За видом порушення виділяють такі класи загроз [38]:

– загрози порушення конфіденційності інформації. Дані загрози направлені на розголошування конфіденційної або секретної інформації. У разі їх реалізації інформація стає відомою особам, які не повинні мати доступу до неї;

– загрози порушення цілісності інформації. Цей клас загроз направлений на зміну або спотворення інформації, що призводить до порушення якості або повного її знищення. Цілісність інформації може бути порушена умисно, а також у результаті об’єктивних дій з боку середовища, що оточує систему;

– загрози порушення доступності інформації (відмова в обслуговуванні). Ці загрози направлені на створення таких ситуацій, коли певні умисні дії або знижують працездатність ІС, або блокують доступ до деяких її ресурсів;

– загрози відмови від вчинених дій з інформацією (загрози неспростовності);

– загрози, пов’язані з неможливістю встановлення авторства електронних документів (загрози автентичності);

– загрози порушення вимог законодавства (порушення прав інтелектуальної власності, патентного права, нелегальне використання програмного забезпечення (ПЗ) і т. п.).

За джерелами походження загрози бувають:

– природного походження – включають в себе небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградацію ґрунтів чи надр, природні пожежі тощо;

– техногенного походження – транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв’язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів державного управління тощо;

– антропогенного походження – вчинення людиною різноманітних дій з руйнування ІС, ресурсів, ПЗ об’єкта тощо [37].

Якщо детальніше розглянути технічний ЗІ, то у [39] відзначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– НСД шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Витік інформації по технічним каналам зв’язку – це специфічний клас загроз, що потребує для своєї реалізації спеціальних навиків та обладнання для проведення технічної розвідки. Такі методи використовуються у випадку, коли інформація, яку хочуть перехопити має значну цінність. До даного класу загроз

відноситься [40]:

– побічне електромагнітне випромінення інформативного сигналу від технічних засобів і ліній передачі інформації;

– наведення інформативного сигналу на лінії зв’язку, заземлення, електроживлення;

– радіовипромінення, модульовані інформативним сигналом, паразитне випромінення;

– радіовипромінення, зумовлені впливом на технічні засоби високочастотних сигналів, створених за допомогою розвідувальної апаратури;

– апаратні закладки;

– акустичне випромінення мовного каналу;

– віброакустичне випромінення мовного каналу;

– перегляд інформації з екранів дисплеїв за допомогою оптичних засобів;

– телевізійна і фотографічна розвідка.;

– зміни струму споживання, обумовленні інформативними сигналами, які обробляються технічними засобами;

– електричні сигнали, що виникають за допомогою перетворення інформативного сигналу із акустичного в електричний за рахунок мікрофонного ефекту і , які поширюються по лініям передачі інформації.

Крім того, у [35] вищезазначений перелік поповнює такий вид загроз як дефекти, збої та відмови ПЗ чи технічних засобів та систем об’єктів інформаційної діяльності. У свою чергу, О. Астахов відмічає, що ПЗ може виступати в таких якостях:

– засіб обробки інформації, який може бути використаний для порушення безпеки інформаційних активів;

– вихідні тексти і файли програм самі по собі являються інформаційними активами, що наражаються на ті ж загрози безпеці, як і будь-які інші активи;

– об’єкт інтелектуальної власності, що потребує юридичного захисту.

По відношенню до програмних засобів можуть бути реалізовані такі види загроз [40]:

– псування ПЗ та резервних копій;

– внесення несанкціонованих змін у вихідні тексти ПЗ;

– використання неліцензійного ПЗ;

– порушення ліцензійних угод;

– порушення конфіденційності програмних кодів.

В окремий клас можна віднести загрози, які реалізуються за допомогою програмних засобів:

– використання помилок проектування, кодування або конфігурації для отримання НСД;

– використання закладок в ПЗ;

– збій роботи засобів ЗІ;

– маскарад, перехват паролів або злам паролей користувачів;

– нецільове використання ПЗ;

– аналіз мережевого трафіка з метою перехоплення інформації;

– заміна, вставлення, видалення або зміна даних користувачів в інформаційному потоці;

– помилки користувачів та технічного персоналу;

– впровадження шкідливого ПЗ;

– витік конфіденційної інформації через електронні канали зв’язку (електронна пошта, системи миттєвих повідомлень і т. п.) або на зовнішніх пристроях та носіях інформації;

– і т. п [40].

Більшість загроз, що відносяться до цього класу реалізуються шляхом здійснення локальних або віддалених атак на інформаційні активи системи внутрішніми і зовнішніми зловмисниками. Результатом вдалого проведення цих загроз є отримання НСД до інформації електронного архіву, що зберігається на робочих місцях адміністраторів, конфігураційної інформації активного мережевого обладнання, а також до даних, які передаються через канали зв’язку.

Існують також загрози технічним засобам, до них відносяться загрози доступності, цілісності і, в деяких випадках, конфіденційності інформації, що

зберігається, обробляється та передається через канали зв’язку, пов’язані з пошкодженнями та відмовами технічних засобів системи та пошкодженням лінії зв’язку. У цьому класі доцільно розглянути такі основні види загроз [40]:

– навмисне або ненавмисне фізичне пошкодження технічних засобів внутрішніми зловмисниками;

– фізичне пошкодження мережевого та каналоутворюючого обладнання внутрішніми зловмисниками;

– фізичне пошкодження ліній зв’язку зовнішніми або внутрішніми зловмисниками;

– перебої в системі електроживлення;

– відмови технічних засобів;

– встановлення неперевірених технічних засобів або заміна апаратних компонентів, які вийшли з ладу, на неідентичні компоненти;

– крадіжка носіїв конфіденційної інформації внутрішніми зловмисниками в наслідок відсутності контролю за їхнім належним використанням та зберіганням.

За даними дослідження, проведеного Executive Information Network, в 80% випадків носієм загрози є людина. Вона може порушити ІБ через розголошення інформації; НСД до неї; спотворення, знищення або блокування інформації із застосуванням технічних засобів; помилки при експлуатації технічних чи програмних засобів, систем ЗІ та ін.

У свою чергу, розголошення інформації, що підлягає захисту, може здійснюватися через [35]:

– передачу інформації по відкритим лініям зв’язку;

– обробку інформації на незахищених технічних засобах;

– опублікування інформації у пресі та інших засобах масової інформації;

– копіювання інформації на незареєстрований носій;

– передачу носія інформації особам, які не мають права доступу до неї;

– втрату носія інформації;

– і т. п.

НСД до інформації може здійснюватися шляхом [35]:

– підключення до технічних засобів та систем об’єктів інформаційної діяльності;

– використання закладних засобів/пристроїв;

– використання ПЗ технічних засобів об’єктів інформаційної діяльності через: маскування під зареєстрованого користувача, дефекти та уразливості ПЗ об’єктів інформаційної діяльності, внесення програмних закладок, застосування вірусів або іншого шкідливого програмного коду);

– розкрадання носія інформації;

– порушення функціонування технічних засобів обробки інформації.

Якщо розглянути матеріально-речовинний канал витоку інформації, то можна виділити фізичні загрози, які здійснюються через фізичний НСД у приміщення організації, в кабінети і серверні кімнати, до обладнання, паперових документів, носіїв інформації і т. п. У наслідок цих дій може відбутися крадіжка або пошкодження комп’ютерного обладнання, носіїв інформації, паперових документів; переконфігурування або створення можливості обійти засоби ЗІ.

У свою чергу О. Литвиненко [41] відзначає, що основні загрози ІБ можна представити у такому вигляді:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Типові загрози ІБ описано у [42] :

– фізичне пошкодження (пожежа, забруднення, знищення обладнання або носіїв, корозія, пил, волога тощо);

– природні явища (кліматичні, сейсмічні, вулканічні, метеорологічні, повені тощо);

– втрата необхідних сервісів (кондиціювання, системи водопостачання, електроживлення, телекомунікації тощо);

– несправності в наслідок випромінення (електромагнітного, теплового, електромагнітного імпульсу тощо);

– компрометація інформації (дистанційне шпигунство, підслуховування, викрадення носіїв або документів, обладнання, злочинне використання апаратних чи програмних засобів тощо);

– технічні несправності (пошкодження обладнання, насиченість ІС, неправильна робота обладнання або ПЗ, порушення ремонтопридатності ІС тощо);

– несанкціоновані дії (несанкціоноване використання обладнання, шахрайське копіювання ПЗ, використання підробленого або скопійованого ПЗ, перекручування даних, незаконне їх опрацювання тощо);

– компрометація функцій (помилка під час використання, зловживання правами, фальсифікація прав, порушення працездатності персоналу, заперечення дій тощо).

Таким чином, існує безліч загроз ІБ, які за певними ознаками відносяться до того чи іншого класу. Для запобігання, усунення чи зменшення сили впливу даних загроз необхідно проаналізувати їх та створити модель загроз. Дослідження даної моделі дозволить визначити найвагоміші загрози, спрогнозувати стан ІБ, що в свою чергу, сприятиме вчасному впровадженню необхідних механізмів для забезпечення інформаційного захисту.

1.3 Аналіз існуючих методів оцінювання впливу загроз на рівень інформаційної безпеки

Для дослідження рівня захищеності системи ЗІ, що циркулює в ІС існують різні підходи:

– оцінювання ризиків;

– визначення актуальних загроз [43].

Відомі різні методи оцінювання ризиків, зокрема:

– методи пов’язані з якісним оцінюванням рівня ризиків (FRAP, OCTAVE, EBIOS та ін.) дозволяють визначити загрози, що впливають на рівень ІБ, можливі збитки від прояву ризиків, заходи для зменшення або запобігання ризику [44];

– кількісні методи (RiskWatch, ГРИФ, ISAMM, Mehari та ін.) передбачають чисельне визначення величин окремих ризиків та інтегральної оцінки ризику в цілому. Кількісний аналіз базується на теорії ймовірностей, математичній статистиці, теорії дослідження операцій. Якість аналізу залежить від точності і повноти числових значень і від обґрунтованості використовуваних моделей [45];

– методи, які використовують змішане оцінювання (як якісне, так і кількісне (CRAMM, MSAT, MAGERIT та ін.)).

Для прийняття рішення щодо вибору того чи іншого методу оцінювання ризиків ІБ потрібно переконатися, що він досить повно враховує потреби досліджуваної системи, а також детально описує процеси і необхідні дії.

Розглянемо найбільш поширені інформаційні методи визначення інформаційних ризиків: CRAMM, OCTAVE, MSAT, RiskWatch.

CRAMM – один з перших методів аналізу ризиків у сфері ІБ, розроблений центральним Агентством з комп’ютерів і телекомунікацій Великобританії і використовується в якості державного стандарту [46].

Дослідження ІБ системи за допомогою CRAMM складається з трьох стадій.

На першій стадії аналізується все, що стосується ідентифікації та визначення цінності фізичних, програмних та інформаційних ресурсів системи.

Потім будується модель ІС з позиції безпеки, яка дозволяє виділити критичні елементи.

На другій стадії розглядається все, що відноситься до ідентифікації та оцінювання рівнів загроз для груп ресурсів та їх вразливостей. Для оцінювання цінності активів використовується шкала від 1 до 10. Рівень загроз оцінюється за шкалою: дуже низький, низький, середній, високий, дуже високий; а рівень

вразливостей: низький, середній, високий. На основі цієї інформації складається матриця ризику і визначається підсумковий рівень ризику, який може приймати значення від 1 до 7.

Третя стадія дослідження полягає у пошуку адекватних контрзаходів.

Таким чином, CRAMM – приклад методу розрахунку, при якому первинні оцінки даються на якісному рівні, а потім проводиться перехід до кількісної оцінки (в балах).

Розглянемо переваги та недоліки даного методу.

Переваги CRAMM [46]:

– є універсальним і підходить для організацій як державного, так і комерційного сектору;

– метод добре апробований;

– вдала система моделювання ІТ;

– ємна база даних для оцінювання ризиків і вибору контрзаходів;

– можливість використання як засобу аудиту.

Недоліки методу CRAMM [47]:

– вимагає спеціальної підготовки і високої кваліфікації аудитора;

– більше підходить для аудиту вже існуючих ІС, а не для тих, які знаходяться на стадії розробки;

– порівняно висока трудомісткість;

– велика кількість звітів;

– не дає змоги створювати власні шаблони звітів або модифікувати наявні;

– припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як “уникнення” або “прийняття”, не розглядаються.

– ПЗ CRAMM існує тільки на англійській мові;

– висока вартість ліцензії.

Далі розглянемо методику OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), яка розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей [48]. Методика

має ряд модифікацій, зокрема OCTAVE-S і OCTAVE Allegro, які розраховані на організації різного розміру та галузі діяльності.

OCTAVE передбачає три фази аналізу ризиків:

– розробка профілю загроз, пов’язаних з активом;

– ідентифікація інфраструктурних уразливостей;

– розробка стратегії та планів безпеки.

Ця методика пропонує скласти профіль загроз та дерево варіантів. Профіль загрози включає в себе вказівки на актив, тип доступу до активу, джерело загрози, тип порушення або мотив, результат і посилання на описи загрози в загальнодоступних каталогах [49].

Перевагами даної методики є:

– швидке впровадження;

– можливе застосування для організацій різного розміру та галузей зайнятості;

– комерційні програмні продукти, що реалізовують положення методики;

– високий рівень гнучкості;

– не потребує спеціальної підготовки для роботи із засобами.

Недоліки OCTAVE:

– не дає кількісної оцінки ризиків;

– припускає використання як способів зниження ризику лише його зниження і прийняття;

– не спрямований на специфіку банківської сфери.

Проаналізуємо методику оцінювання ризиків MSAT (Microsoft Security Assessment Tools). Дана методика розроблена, щоб допомогти організаціям оцінити уразливості в IT-середовищах, надати список проблем розміщених за пріоритетам і список рекомендацій щодо мінімізації цих загроз [50].

MSAT містить більше 200 питань, що охоплюють інфраструктуру, додатки, операції і персонал. Питання, пов’язані з ними відповіді і рекомендації виводяться із загальноприйнятих практичних рекомендацій, стандартів, таких як ISO 17799 та

NIST-800.x, а також рекомендацій та приписів від групи надійних обчислень Microsoft та інших зовнішніх джерел з безпеки [51].

Оцінювання ризику за даною методикою складається з двох частин:

– визначення профілю ризику для бізнесу – загальні небезпеки, з якими стикається компанія;

– оцінки індексу ешелонованого захисту, який відноситься до реалізації багаторівневого захисту, що включає технічний, організаційний і робітничий контроль.

Для вимірювання розподілу ризику в усіх областях аналізу, профіль ризику для бізнесу та індекс ешелонованого захисту порівнюються.

Зазначимо переваги MSAT:

– простота використання;

– можливість оцінювання рівня безпеки для підприємств різних масштабів;

– повнота результуючих звітів, на основі яких програма здатна давати рекомендації щодо підвищення або зниження ступеня безпеки;

– безкоштовний програмний продукт.

Однак останнє оновлення MSAT було в 2009 році, за цей час IT змінилися і рівень загроз помітно зріс. Тобто дана методологія не розрахована на вимір ефективності сучасних заходів безпеки.

Розглянемо методику RiskWatch розроблену американською компанією RiskWatch, Inc. за участю NIST, Міністерства оборони США і Міністерства оборони Канади [52].

У RiskWatch в якості показників для оцінювання і управління ризиками використовуються прогнозовані середньорічні втрати та оцінку повернення від інвестицій. Методика RiskWatch включає в себе чотири фази [53].

Перша фаза – визначення предмета дослідження. На даному етапі здійснюється опис об’єкта дослідження і його параметрів, таких як інфраструктура досліджуваної системи, вимоги щодо забезпечення ІБ, клас організації.

Друга фаза – введення даних, що описують конкретні характеристики досліджуваної системи.

Класи інцидентів отримують шляхом зіставлення категорії втрат і категорії ресурсів. Для виявлення можливих вразливостей використовується опитувальний лист, що складається з широкого спектру питань, пов’язаних з категоріями ресурсів. Встановлюється частота виникнення кожної з актуальних загроз, вразливість і цінність активів.

Очікувана частота реалізації загроз визначається в термінах середньорічної оціночної частоти загрози. База знань RiskWatch визначає для кожної загрози стандартну оціночну частоту. Для обчислення величини ризику використовується локальна оціночна частота загрози.

Третя фаза – оцінювання ризиків. На даному етапі здійснюється визначення зв’язків між активами, втратами, частотою реалізації загроз і вразливостями, виявленими на попередніх етапах.

Четверта фаза – формування звітів.

Як недоліки RiskWatch можна визначити те, що даний метод можна використовувати в тому випадку якщо потрібно провести аналіз ризиків на програмно-технічному рівні без урахування організаційних і адміністративних чинників. Розглянутий метод не враховує комплексний підхід до ІБ, ПЗ RiskWatch існує тільки англійською мовою і характеризується високою вартістю ліцензії . Суттєвими перевагами RiskWatch є інтуїтивно зрозумілий інтерфейс, гнучкість методу, що забезпечується можливістю введення нових категорій, описів, питань і т. п. [54].

У науковій літературі значна увага приділяється вирішенню проблем оцінювання впливу загроз на рівень ІБ. Так, О. М. Астахов у роботі [40] використовує системний підхід до управління інформаційними ризиками, що ґрунтується на міжнародних стандартах BS 7799-3 та ISO/IEC 27005. Застосування ймовірнісного підходу висвітлено в роботі С. Ф. Гончара [55], Г. А. Черней [56] поєднує експертний та ймовірнісний підходи щодо аналізу інформаційних ризиків, В. М. Бєлов [57] використовує експертний підхід з

урахуванням міжнародних стандартів тощо.

У роботі [58] для оцінювання інформаційних ризиків використано ймовірнісний підхід, запропоновано методику оцінювання сукупного впливу загроз на рівень інформаційного ризику, виокремлені етапи управління інформаційними ризиками.

Автори роботи [59] представили процес оцінювання ризиків ІБ у вигляді послідовності елементарних перевірок, кожна з яких характеризується матрицею умовної ймовірності. Значення елементів визначаються законами розподілу контрольованих параметрів. У результаті запропоновано алгоритм, що дозволяє з множини доступних елементарних перевірок вибрати таку послідовність перевірок, яка забезпечує найбільшу інформаційну продуктивність процесу оцінювання ризиків ІБ.

Вирішення даного питання методом експертних оцінок висвітлено у роботі [60]. Зокрема, схематично представлено послідовність дій: формулювання мети дослідження, відбір експертів та формування експертної групи, складання анкет, анкетування, обробка та аналіз експертних оцінок. Запропоновано статистичний інструментарій для обробки та аналізу отриманих результатів анкетування експертів.

Автори роботи [61] запропонували підхід, який дозволяє кількісно уточнити оцінку ризиків, що може бути отримана за допомогою якісної методики FAIR. Розробка методики проводилася з використанням математичного апарату теорії ймовірностей, а сааме Байєсовських мереж.

У роботі [62] автори запропонували метод оцінювання ризиків на основі відкритих баз даних вразливостей за рахунок модифікації процедур визначення параметрів оцінювання ризику і оцінки поточних значень параметрів з можливістю інтеграції (як альтернатива оцінок експертів) значень показників. Даний метод, дозволяє автоматизувати процес оцінювання ризиків без залучення експертів відповідної предметної області.

Аналіз існуючих методів показав, що вони потребують складних розрахунків, наявності достатньо повної статистичної інформації, тривалого часу

для опрацювання необхідних даних. Крім того, в більшості з них оцінювання ризиків ведеться тільки до рівня активів, і не враховується їх вплив на функціонування досліджуваної системи. Причому вирішення даної задачі безпосередньо пов'язане з людським фактором та характеризується високим ступенем невизначеності, складністю формалізації впливу загроз. Тому для вирішення даного питання доцільно звернути увагу на методи когнітивного підходу, який надає можливість вирішувати вищезазначені проблеми, наглядно представляючи досліджувану систему за допомогою гнучких конструктивних моделей, які здатні адекватно реагувати на зміни.

1.4 Аналіз моделей забезпечення інформаційної безпеки на основі нечіткої логіки та когнітивного моделювання

Для вирішення завдань пов'язаних із аналізом загроз та ризиків ІБ зручно використовувати методи нечіткої логіки. Так у роботі [63] побудована нечітка ієрархічна модель, яка містить лінгвістичні змінні і нечіткі бази знань; запропонована лінгвістична оцінка ризиків інформаційних активів, що базується на методології Coras [64].

У [65] показано, що при розрахунку ризику загрози ІБ за допомогою моделі нечітких множин з різними можливими варіантами складу експертних даних для одних і тих же загроз рівні ризику ІБ можуть істотно відрізнятися. В якості таких даних розглядалися: функції приналежності, терм-множини, продукційні правила.

Автор праць [66] – [67] розробив методи та моделі для нечіткого кількісного оцінювання ризиків ІБ, які базуються на теорії нечітких множин. Однак в запропонованих автором методиках не враховується вплив активів на кінцевий результат функціонування організації.

У [68] було розроблено нечітку продукційну модель, яка дозволяє істотно розширити можливості існуючих методик, зняти обмеження на кількість врахованих вхідних змінних та інтегрувати як якісні, так і кількісні підходи до оцінювання ризиків. Використані в методиці механізми оцінювання ризику на основі нечіткої логіки дозволяють отримати лінгвістичний опис ступеня ризику,

що надає змогу ІТ-менеджерам виявити пріоритети ризиків і вибрати план заходів щодо зниження рівня найбільш небезпечних загроз ІБ організації.

І. В. Сібікіна [69] представила етапи побудови та аналіз адекватності нечіткої моделі для аналізу ризиків ІБ. Описала процедури збору і обробки експертної інформації, необхідної для побудови системи нечіткого виведення. Запропонувала методику побудови лінгвістичних шкал, в основу якої покладено метод статистичного експерименту. На основі експертних даних було побудовано функції належності нечітких змінних, сформовано продукційні правила. Отримана модель дозволяє встановити залежність значень вихідний змінної «ступінь ризику» від значень вхідних змінних «рівень загрози», «ступінь збитків» і «ступінь вразливості».

У роботі [70] автори описують загальні положення оцінювання ризиків ІБ з використанням теорії нечітких множин. Лінгвістичні змінні характеризують загальні параметри, які найчастіше використовуються при оцінюванні ризиків: ймовірність загрози, активи і співвідношення уразливості в активах до загроз.

Автор праці [71] описує нечітку модель оцінювання ризику для всієї організації і бере в якості вихідних характеристик нечіткі змінні, що описують фактори ризику (організаційні, технічні рівні ЗІ, цінність і обсяг інформаційних ресурсів). Причому не беруться до уваги конкретні вразливості та їх вплив на цільову систему.

У роботі [72] розглядається процес створення нечіткої продукційної моделі оцінювання ризику ІБ. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збитки організації. Взаємозв’язок між факторами (антецедентом) і показниками ризику (консеквентом) являє собою бінарне нечітке відношення на декартовому добутку відповідних нечітких множин. Нечітке причинно-наслідкове відношення між антецеденом і консеквентом задається у вигляді нечіткої продукції. Механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризику.

Автори праці [73] побудували модель оцінювання загального рівня інформаційних ризиків у CRM-системі із застосуванням лінгвістичного підходу, що забезпечує кількісний опис окремих елементів моделі за умов нечіткої інформації щодо значення критеріїв оцінювання чинників (факторів) ризику. Це дає можливість виділити значущі чинники ризику, їх наслідки в умовах дії агента загрози і, тим самим, визначити альтернативні шляхи для уникнення негативного впливу ризику.

У роботі [74] запропоновано підхід для оцінювання ризиків ІБ, заснований на концепції логіко-лінгвістичної нечіткої моделі, що базується на наборі правил Мамдані.

Слід зазначити, що для забезпечення ІБ важливим є питання оцінювання сукупної дії загроз на систему та можливість визначення ризиків при різноманітних сценаріях реалізації множини загроз. Дані питання можливо вирішити за допомогою методів когнітивного моделювання. Когнітивні моделі будуються експертом або ж групою експертів досліджуваної предметної області на підставі теоретичної, статистичної та експертної інформації про об’єкт дослідження [75]. Адекватність моделі визначається повнотою комплексу вихідних знань; модель може уточнюватися в процесі дослідження та застосування, будучи сама по собі джерелом структурованих знань.

Методи когнітивного моделювання базуються на використанні НКК, яким властива відносна простота інтерпретації, інтегрованість з методами оцінок результатів аналізу, наочність, гнучкість, конструктивність, адаптація до невизначеності вхідних даних, використання знань і досвіду експертів предметної області, відсутність необхідності передчасної специфікації даних та відносин впливу [76].

НКК складної системи (проблеми) являє собою орієнтований граф, вершини якого (концепти) представляють системні змінні, а дуги – причинно-наслідкові зв’язки між концептами, причому ваги цих зв’язків визначають силу впливу концептів один на одного [77].

Когнітивна карта є моделлю представлення знань експертів про закони розвитку та властивості досліджуваної ситуації, а їх різноманітність визначається різними способами експертного визначення сили причинно-наслідкових відносин і значень факторів у когнітивній карті [78].

Різні інтерпретації вершин, ребр, ваг, а також різні функції, що визначають вплив зв'язків на фактори, призвели до виникнення різних моделей (модифікацій когнітивних карт) та засобів їх аналізу [79]. На сьогодні існує багато різновидів НКК: знакові когнітивні карти [80], НКК Коско [81], НКК Силова [82], нечіткі узагальнені когнітивні карти [83], реляційні НКК [84], продукційні НКК [85], інтервальні («сірі») НКК [86], нейтрософські НКК [87], динамічні когнітивні карти [88] та інші [89]. Вони відрізняються способом представлення відношень між концептами, значень концептів та алгоритмів, що забезпечують передачу впливу за когнітивною картою.

Питанням застосування НКК для вирішення задач ІБ приділяється достатня увага, зокрема, у роботах [90] – [99].

Так К. С. Степанова у своїй роботі [93] запропонувала модель загроз ІБ на основі побудови НКК Коско. На відміну від простих когнітивних карт, НКК Коско являє собою нечіткий орієнтований граф зі зворотним зв'язком, вузли якого є нечіткими множинами. Спрямовані ребра графа не тільки відображають причинно-наслідкові зв'язки між концептами, а й визначають ступінь впливу (вагу) взаємопов'язаних концептів. Концепти у НКК Коско можуть набувати значення з діапазону дійсних чисел [0; 1]. Термін «нечіткі» означає те, що причинні зв'язки можуть набувати не тільки значення, що дорівнює 0 або 1, а лежать у діапазоні дійсних чисел, що відображають «силу» впливу одного концепту на інший [81]. Таким чином, НКК об'єднує у собі властивості нечітких систем і нейронних мереж. Проте даний тип НКК має деякі обмеження, які пов'язані з тим, що значення концептів являють собою чіткі числа.

У роботах [94], [95], [97] для аналізу інформаційних загроз та визначення ризиків безпеці автори запропонували когнітивні моделі, використовуючи НКК Силова, які описують вплив потенційних загроз на досліджувану систему. Дані

НКК базуються на доволі легкому моделюванні та швидкому обчисленні. Зв'язки між концептами в НКК Силова можуть бути як додатними – такими, що підсилюють вплив одного концепту на інший, так і від'ємними – такими, які послаблюють даний вплив. Тобто В. Б. Силов запропонував підхід, який розширює діапазон зміни значень причинних зв'язків до [-1; 1]. Проблема опрацювання від'ємних впливів вирішується шляхом подвоєння потужності множини концептів і роздільного опрацювання додатних і від'ємних впливів. А відношення між концептами НКК розглядаються як елементи нечіткої матриці суміжності для графа НКК. Крім того, нечіткі значення вихідних концептів отримуються із використанням характерних для нечіткої логіки операцій Т-норм над нечіткими значеннями вхідних концептів і ваг впливу [82]. Хоча варто зауважити, що для комплексного оцінювання впливу декількох факторів на один концепт використовується операція пошуку максимуму серед ваг впливу, що не завжди відображає ймовірність реалізації атаки на даний концепт.

Автор праці [91] для оцінювання стану захищеності даних в умовах можливої реалізації інформаційних загроз пропонує нечітку когнітивну модель, яка складається з шести ієрархічних рівнів. Вхідними даними моделі є лінгвістичні оцінки стану засобів ЗІ. На основі цих оцінок розраховуються значення концептів на вищих рівнях. Недоліком даної моделі є те, що для визначення ступеня впливу концептів один на одного використовується метод експертних оцінок «Дельфі», який є трудомістким і потребує значних часових затрат.

У роботі [92] для оцінювання ризиків ІБ використовують нечіткі продукційні когнітивні карти. Особливістю даних карт є те, що значення концептів виражають через нечіткі лінгвістичні змінні, для опису впливів між концептами використовують базу нечітких продукційних правил, при передаванні впливу когнітивною картою використовується алгоритм нечіткого виведення типу Мамдані, а для операції агрегування застосовується операція нечіткого додавання з перенесенням. Дана операція використовується для агрегування двох впливів від вхідних концептів, поданих у вигляді нечітких множин (функцій належності)

вихідного концепту. Цей вид акумулювання дає змогу обробляти нечіткі числа за двома “координатами” (приналежності й базової множини) і враховувати адитивний характер впливів окремих концептів. Проте його механізм виглядає досить довільним. Зазначимо, що нечіткі продукційні когнітивні карти мають додаткові переваги порівняно з НКК Коско, хоча одночасно характеризуються трудомісткістю та складністю реалізації, адже потребують використання великої кількості правил.

Для вирішення задачі оцінювання інформаційних ризиків у [96] автори скористалися апаратом нечітких сірих когнітивних карт, які відрізняються від звичайних НКК тим, що для встановлення впливів між концептами використовують «сірі» (інтервальні) числа. Перевагами застосування НКК даного типу є те, що вони дозволяють перейти від точкових оцінок експертів до інтервальних і, як наслідок, до отримання інтервальних оцінок кінцевих результатів, які є більш логічними, достовірними. Крім того, інтервальні оцінки можуть відображати діапазон думок групи експертів, що дозволяє більш повно врахувати наявні для аналізу ризику дані. Проте нечіткі «сірі» когнітивні карти характеризуються високою складністю обчислювальної реалізації.

У роботі [98] для оцінки ризиків ІБ застосовано когнітивне моделювання за допомогою мережі Байєса [99] на основі графа атак, яке є зручним для формування суджень в умовах невизначеності відповідно до оцінок ймовірностей подій і зв’язку між подіями. Проте недоліком такого підходу є складність масштабування, так як для великих корпоративних ІС необхідний перехід до наближених імовірнісних висновків.

Таким чином, існує безліч моделей та засобів забезпечення ІБ, які базуються на методах нечіткої логіки та когнітивного моделювання. Проте переважна більшість з них орієнтована на проведення аналізу стану ІБ та оцінювання ризиків та не вирішують питання безпосереднього визначення рівня захищеності системи при впливі на неї потенційних загроз. Тому актуальною є науково-технічна задача спрямована на оцінювання рівня захищеності систем ЗІ, що циркулює в ІС при впливі на них потенційних загроз на основі когнітивного підходу.

1.5 Постановка задачі

Метою дисертаційної роботи є розробка:

– функціональних моделей для оцінювання рівня захищеності систем ЗІ, що циркулює в ІС;

– програмних засобів для реалізації запропонованих моделей.

Відповідно до вказаної мети потрібно вирішити такі основні задачі:

– провести аналіз загроз системі ЗІ та існуючих моделей й засобів для оцінювання впливу загроз на рівень ІБ;

– розробити комплекс когнітивних моделей, які визначають ступінь впливу найвагоміших загроз на рівень захищеності досліджуваних систем;

– провести структурно-топологічний аналіз розроблених когнітивних моделей;

– на основі сценарного моделювання визначити відносну зміну рівня захищеності систем ЗІ, що циркулює в ІС;

– дослідити достовірність впливу загроз на рівень захищеності систем ЗІ, що циркулює в ІС, визначеного за сценарним моделюванням на основі когнітивного підходу;

– провести симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта КІ;

– здійснити ранжування загроз для визначення допустимої інтенсивності зниження рівня захищеності системи ЗІ і об’єкта КІ та знаходження витрат на забезпечення їхньої захищеності;

– провести динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта КІ;

– провести дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи ЗІ;

– розробити інструментальні програмні засоби для реалізації запропонованих моделей.

1.6 Висновки до розділу 1

У даному розділі було розглянуто основні положення ІБ. Обґрунтовано надзвичайну складність і багаторівневість системних зв’язків між складовими ІБ. У результаті підсумовано, що забезпечення ІБ досягається тоді, коли всі використовувані засоби та методи об’єднані в цілісний механізм, функціонування якого контролюється, обновлюється та доповнюється в залежності від змін як внутрішнього, так і зовнішнього середовища. Також проаналізовано можливі загрози ІБ. Розглянуто джерела й характер їхнього походження та шляхи ймовірної реалізації. Проведений аналіз надає змогу дослідити потенційні загрози, що, в свою чергу, дозволить вчасно провести комплекс відповідних заходів для запобігання, усунення чи зменшення сили впливу даних загроз.

Крім того, було проаналізовано методи оцінювання впливу загроз на рівень ІБ, які пов’язані із якісним, кількісним та змішаним оцінюванням інформаційних ризиків. Виділено їх переваги та недоліки. Розглянуто ряд моделей для оцінювання ризиків ІБ на основі нечіткої логіки. У результаті чого, встановлено, що більшість з наведених методів та моделей потребують складних розрахунків й тривалого часу для опрацювання необхідних даних, при чому оцінювання ризиків найчастіше ведеться тільки до рівня активів, і не враховується їх вплив на функціонування досліджуваної системи. У свою чергу, аналіз моделей розроблених на основі НКК показав, що застосування когнітивного підходу дозволяє вирішити вищезазначені питання, покращити наочність представлення проблеми, визначати стан ІБ при різноманітних сценаріях реалізації множини загроз та спростити процедуру розширення кількості факторів за рахунок введення додаткових вершин і дуг графа НКК. Проте варто зазначити, що переважна більшість розглянутих когнітивних моделей орієнтована на проведення аналізу стану ІБ, оцінювання ризиків її порушення, але не забезпечує безпосереднього визначення зміни рівня захищеності системи при впливі на неї потенційних загроз. Тому актуальною є наукова задача спрямована на розробку когнітивних моделей оцінювання рівня захищеності систем ЗІ, що циркулює в ІС.

РОЗДІЛ 2
РОЗРОБКА ТА АНАЛІЗ КОГНІТИВНИХ МОДЕЛЕЙ ДЛЯ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Розробка та аналіз когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі

Сучасне життя неможливо уявити без використання КМ, які надають своїм користувачам безліч можливостей, зокрема: інтерактивність, спільний доступ до даних, швидкий обмін текстовою, звуковою та відеоінформацією у реальному часі, оперативний зворотній зв'язок, сумісне використання технічних ресурсів та ін. [100].

Для належного функціонування мережі та надійного забезпечення усіх вищеперерахованих послуг особлива увага приділяється організації мережевої безпеки. Адже КМ та їхні ресурси постійно перебувають під загрозою зараження шкідливим ПЗ чи здійсненням різних типів мережевих атак. У наслідок цих атак зловмисники можуть отримати НСД до інформаційних ресурсів, здійснити крадіжку, знищення або псування даних, порушити функціонування та доступність сервісу, отримати контроль над роботою усієї системи. Щоб попередити вищезазначені дії, необхідно проаналізувати вплив можливих загроз на систему, оцінити силу їхньої дії, виділивши найвагоміші із них.

Вирішення даного питання можливе за допомогою методів статистичного аналізу, зокрема, дисперсійного та кореляційно-регресійного аналізу. Проте дані методи потребують складних розрахунків, наявності достатньо повної статистичної інформації, тривалого часу для опрацювання необхідних даних. У зв'язку з цим, варто звернути увагу на когнітивний підхід, який надає можливість вирішувати задачі, що не піддаються строгій формалізації, наглядно представляти досліджувану систему або проблему, використовувати неповну, нечітку інформацію та суб'єктивні судження експертів предметної області, будувати гнучкі, конструктивні моделі, які адекватно реагують на зміни.

Враховуючи вищезазначені переваги когнітивного моделювання, проведемо на його основі дослідження впливу загроз на рівень захищеності КМ.

Для досягнення поставленої мети, насамперед, проаналізуємо ймовірні загрози мережевій безпеці, що характеризують можливі дії, які можуть бути здійсненні по відношенню до системи. Вони мають прояви у різноманітних формах, але найпоширенішими є такі [36]:

– випадкові: особа, яка не ознайомлена з відповідним регламентом і політикою, або через неналежний догляд, створює випадковий ризик;

– несанкціоновані зміни: оновлення, виправлення та інші зміни в операційних системах, програмних додатках, конфігураціях, можливостях взаємодії та обладнанні можуть створити несподівану загрозу безпеці систем промислової автоматики та контролю або відповідного промислового процесу.

З метою виявлення загальних тенденцій зміни мережевої безпеки дослідимо корпоративну мережу із загальними характеристиками.

Розглянемо перелік можливих загроз, реалізація яких призведе до негативних наслідків функціонування мережі [101] – [104]:

1. Scan Attacks – пошук можливих вразливостей системи:

– Packet sniffers – перехоплення та аналіз трафіка;

– Ping sweeps – знаходження IP-адрес працюючих комп’ютерів;

– Port scanner – сканування відкритих TCP- та UDP-портів;

– Phishing – спосіб отримання необхідної інформації безпосередньо у користувачів КМ.

2. Web Attacks:

– Cross-Site Scripting (XSS) – зловмисний збір інформації користувача, через сторінки веб-додатку;

– SQL Injection – один із поширених способів зламу сайтів і програм, що працюють з базами даних, заснований на впровадженні у запит довільного SQL-коду;

– Path Traversal – обробка зловмисником HTTP-запитів, для того, щоби обійти контролі доступу та перейти до інших каталогів і файлів у системі.

3. Spoofing – підміна довіреного суб’єкта:

– IP-spoofing – використання чужої IP-адреси відправника з метою обману системи безпеки;

– DNS-spoofing – зміна даних кешу доменних імен з метою присвоєння помилкової IP-адреси;

– DHCP-spoofing – підміна шлюзу за замовчуванням (default gateway).

4. Атаки, спрямовані на отримання доступу до системи:

– Password Attacks – злам паролю;

– Trust Exploitation – компрометація довіреного хоста, використовуючи його для атак на інші хости у мережі;

– атака man-in-the-middle – компрометація каналу зв’язку, при якому зловмисник здійснює втручання у протокол передавання даних, видаляючи або змінюючи інформацію.

5. Перехоплення сеансу (session hijacking) – використання поточного комп’ютерного сеансу для отримання НСД до інформації або послуг у КМ.

6. Compromised-Key Attack – перехоплення секретного ключа.

7. Спамінг – зловживання можливостями електронної пошти.

8. Атака відмови в обслуговуванні (Denial of Service, DoS) – лавинна маршрутизація пакетів, що призводить до перевантаження мережі і, як наслідок, робить її недоступною.

9. Шкідливе ПЗ (trojan, worms, virus, botnet та ін.) – спрямоване на перешкоджання роботи мережі, збір конфіденційної інформації або отримання доступу до приватних комп’ютерних систем.

10. Фізичний вплив на мережу з боку зловмисника – призводить до руйнування або виведення з ладу фізичних компонентів, таких як апаратне забезпечення, пристрої, призначені для зберігання ПЗ, з’єднувальні елементи, датчики, контролери.

11. Розголошення інформації – умисні або необережні дії користувача, в наслідок яких особа, що не має доступу до даної інформації, ознайомлюється з нею.

12. Ненавмисні дії, помилки користувачів мережі – включають у себе дії, що здійснюються випадково, через незнання, неуважність або недбалість, з цікавості, але без злого умислу.

13. Природні явища та явища техногенного характеру (аварії, урагани, землетруси, пожежі і т. п.).

Для побудови НКК, яка визначає стан безпеки КМ, насамперед, необхідно сформувати з вищезазначеного переліку множину найбільш вагомих з точки зору вивчення даної проблеми концептів. У результаті опитування та узгодження думок групи експертів даної предметної області було визначено такі концепти:

K_1 – мережеві атаки зловмисника (Scan Attacks, Web Attacks, Spoofing, атаки, спрямовані на отримання доступу до системи, перехоплення сеансу та Compromised-Key Attack);

K_2 – спамінг зловмисника;

K_3 – шкідливі програми;

K_4 – фізичний вплив на мережу з боку зловмисника;

K_5 – DoS-атаки зловмисника;

K_6 – розголошення інформації користувачем;

K_7 – ненавмисні дії, помилки користувачів мережі;

K_8 – надійність, відмовостійкість технічних і програмних засобів;

K_9 – захищеність КМ;

K_{10} – відмовостійкість обслуговування роботи мережі;

K_{11} – природні явища та явища техногенного характеру.

Сформувавши перелік концептів, визначимо значення сили впливу між кожною парою концептів шляхом обробки даних, отриманих у результаті експертного опитування.

Для цього задамо нечітку лінгвістичну шкалу, що являє собою впорядковану множину лінгвістичних значень (термів) оцінок настання ймовірних наслідків, отриманих у результаті дії одного концепту на інший:

$$СИЛА\ ЗВ'ЯЗКУ = \begin{Bmatrix} Не\ впливає;\ Дуже\ слабка;\ Слабка; \\ Середня;\ Сильна;\ Дуже\ сильна \end{Bmatrix} \quad (2.1)$$

Кожному із цих значень поставимо у відповідність деякий числовий діапазон, що належить відрізку [0, 1] для додатних зв'язків і відрізку [–1, 0] для від'ємних зв'язків:

$$w_{ij} = \begin{Bmatrix} (0{,}85;\ 1],\ позитивна\ дуже\ сильна; \\ (0{,}6;\ 0{,}85],\ позитивна\ сильна; \\ (0{,}35;\ 0{,}6],\ позитивна\ середня; \\ (0{,}15;\ 0{,}35],\ позитивна\ слабка; \\ (0;\ 0{,}15],\ позитивна\ дуже\ слабка; \\ 0,\ не\ впливає; \\ (0;\ -0{,}15],\ негативна\ дуже\ слабка; \\ (-0{,}15;\ -0{,}35],\ негативна\ слабка; \\ (-0{,}35;\ -0{,}6],\ негативна\ середня; \\ (-0{,}6;\ -0{,}85],\ негативна\ сильна; \\ (-0{,}85;\ -1],\ негативна\ дуже\ сильна \end{Bmatrix} \quad (2.2)$$

НКК, яка ілюструє множинні причинно-наслідкові зв'язки та характер взаємодії визначених факторів, зображена на рис. 2.1.

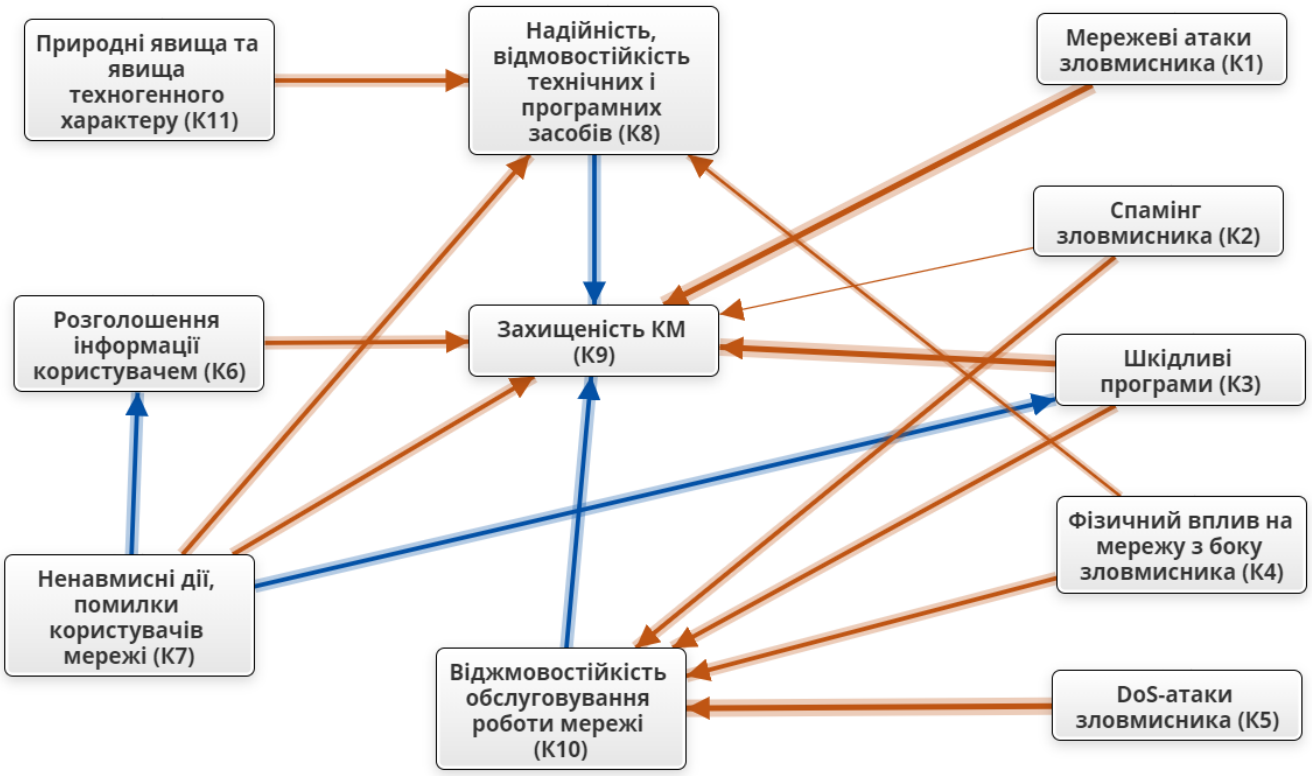


Рисунок 2.1 – НКК дослідження стану мережевої безпеки

Моделювання виконано з використанням засобів ПЗ Mental Modeler [105].

Побудована НКК складається з одинадцяти концептів:

1) шість концептів типу «Driver» – впливають на інші концепти, а на них не впливає жодний з концептів системи;

2) один концепт типу «Receiver» – на нього впливають концепти системи, а він не впливає ні на жоден з них;

3) чотири концепти типу «Ordinary» – звичайні, проміжні концепти, які впливають, і на яких впливають деякі концепти системи.

Для визначення складності розробленої НКК, обчислимо щільність зв'язків, використавши формулу

$$d = \frac{m}{n(n-1)}, \tag{2.3}$$

де m — кількість зв'язків, а n — кількість концептів.

У нашому випадку $n = 11, m = 16$, тому $d = 0{,}15$. Це вказує на достатню складність розробленої когнітивної моделі.

Для виконання аналізу НКК необхідно врахувати весь опосередкований взаємовплив концептів один на одного. Для цього на підставі побудованої когнітивної карти сформуємо матрицю суміжності $W = \left\lfloor w(K_i, K_j) \right\rfloor_{n \times n}$ (табл. 2.1).

Таблиця 2.1

Матриця суміжності НКК предметної області

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	0	0	0	0	0	0	0	0	–0,85	0	0
K_2	0	0	0	0	0	0	0	0	–0,15	–0,5	0
K_3	0	0	0	0	0	0	0	0	–0,9	–0,61	0
K_4	0	0	0	0	0	0	0	-0,38	0	–0,75	0
K_5	0	0	0	0	0	0	0	0	0	–0,98	0
K_6	0	0	0	0	0	0	0	0	–0,75	0	0
K_7	0	0	0,5	0	0	0,58	0	–0,55	–0,65	0	0
K_8	0	0	0	0	0	0	0	0	0,55	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0,55	0	0
K_{11}	0	0	0	0	0	0	0	–0,82	0	0	0

На основі матриці суміжності розраховуються основні системні показники НКК (рис. 2.2).

Component	Indegree	Outdegree	Centrality
Природні явища та явища техногенного характеру (К11)	0	0.82	0.82
Розголошення інформації користувачем (К6)	0.58	0.75	1.33
Ненавмисні дії, помилки користувачів мережі (К7)	0	2.2800000000000002	2.2800000000000002
Віджмовостійкість обслуговування роботи мережі (К10)	2.84	0.55	3.3899999999999997
Захищеність КМ (К9)	4.3999999999999995	0	4.3999999999999995
Надійність, відмовостійкість технічних і програмних засобів (К8)	1.75	0.55	2.3
DoS-атаки зловмисника (К5)	0	0.98	0.98
Шкідливі програми (К3)	0.5	1.51	2.01
Спамінг зловмисника (К2)	0	0.65	0.65
Фізичний вплив на мережу з боку зловмисника (К4)	0	1.13	1.13
Мережеві атаки зловмисника (К1)	0	0.85	0.85

Рисунок 2.2 – Основні показники НКК предметної області

Проаналізувавши значення даних показників можна визначити найвагоміші концепти досліджуваної системи: K_3 – шкідливі програми; K_4 – фізичний вплив на мережу з боку зловмисника; K_7 – ненавмисні дії, помилки користувачів мережі. Також доцільно зазначити, що найменший вплив на роботу мережі має такий концепт як K_2 – спамінг зловмисника.

Для отримання прогнозів розвитку ситуації визначимо відносну зміну концептів системи при максимальному значенні впливу на них найвагоміших факторів. Тобто змоделюємо відповідні сценарії.

Сценарій 1. Розглянемо, як зміниться стан системи при максимальному збільшенні значення концепту K_3 – шкідливі програми.

До шкідливих програм належать: троянські та шпіонські програми, черв'яки, віруси, логічні бомби та деякі інші види програм, спрямовані на порушення ІБ. Ці програми можуть проникати на атаковані комп'ютери різними шляхами. Найчастіше це відбувається, коли користувач завантажує файли із

неперевірених джерел (змінних носіїв чи веб-сайтів) або безпечно відкриває підозрілий файл, який надходить йому на електронну пошту. Існують і більш небезпечні представники шкідливих програм, що мають власні механізми «розмноження», копії таких програм розповсюджуються на комп'ютери у мережі без участі користувачів [101].

У досліджуваній системі концепт K_3 – шкідливі програми безпосередньо впливає на K_{10} – відмовостійкість обслуговування роботи мережі та K_9 – захищеність КМ.

У результаті максимального збільшення значення впливу шкідливих програм відмовостійкість обслуговування роботи мережі знизиться на 0,04, а захищеність КМ – на 0,05 (рис. 2.3).

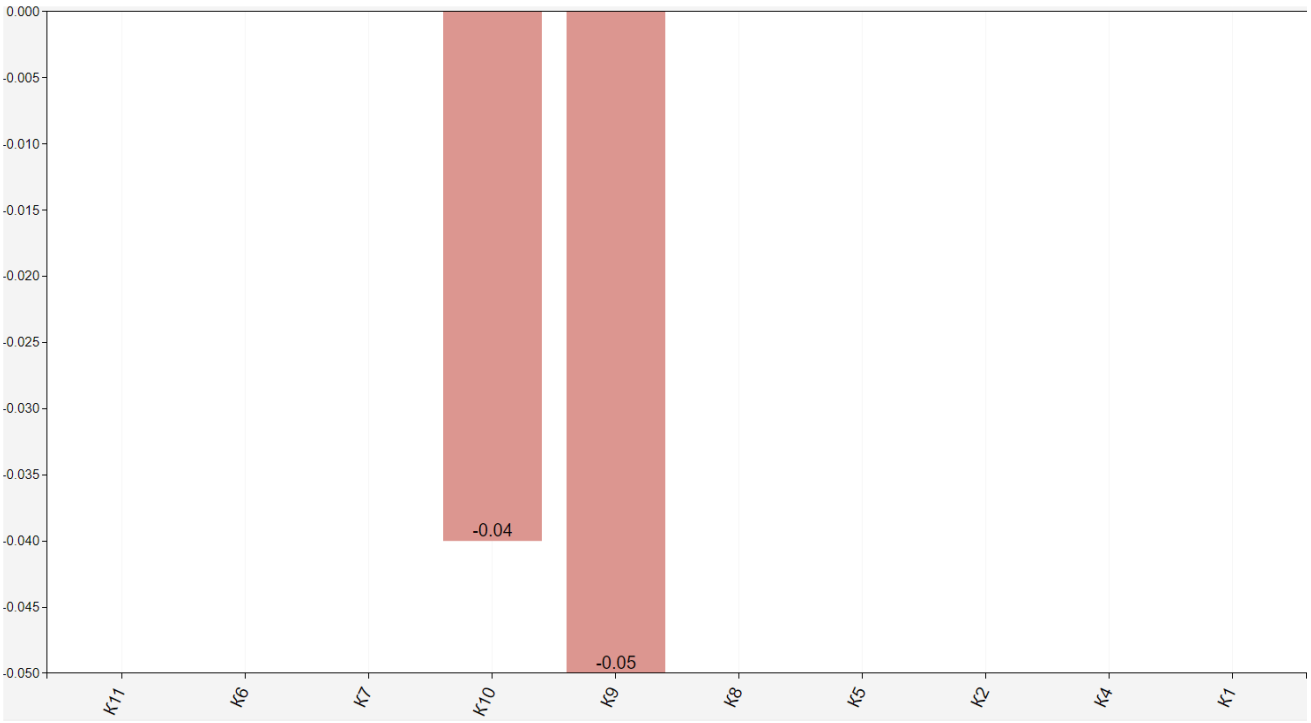


Рисунок 2.3 – Сценарій, що відображає реакцію системи на максимально негативні зміни концепту K_3 – шкідливі програми

Для запобігання або попередження негативної дії шкідливих програм доцільно регулярно оновлювати ПЗ, включаючи операційну систему та усі додатки, використовувати надійні антивірусні програми, створювати резервні копії, які зберігаються на жорсткому диску в автономному режимі тощо.

Сценарій 2. Змоделюємо ситуацію, яка відображатиме зміни у системі при максимальному підвищенні значення концепту K_4 – фізичний вплив на мережу з боку зловмисника.

У даному випадку важливе місце посідають фізичні засоби захисту мережі, які призначені для створення перешкод на шляху потенційного зловмисника, який може несанкціоновано проникнути в приміщення, вчинити акт вандалізму, здійснити крадіжку та інші дії, які негативно вплинуть на роботу мережі.

Концепт K_4 – фізичний вплив на мережу з боку зловмисника має безпосередній вплив на такі концепти системи як: K_8 – надійність, відмовостійкість технічних і програмних засобів, K_{10} – відмовостійкість обслуговування роботи мережі, та опосередковано впливає на K_9 – захищеність КМ. Дослідимо відносні зміни значень цих концептів (рис. 2.4).

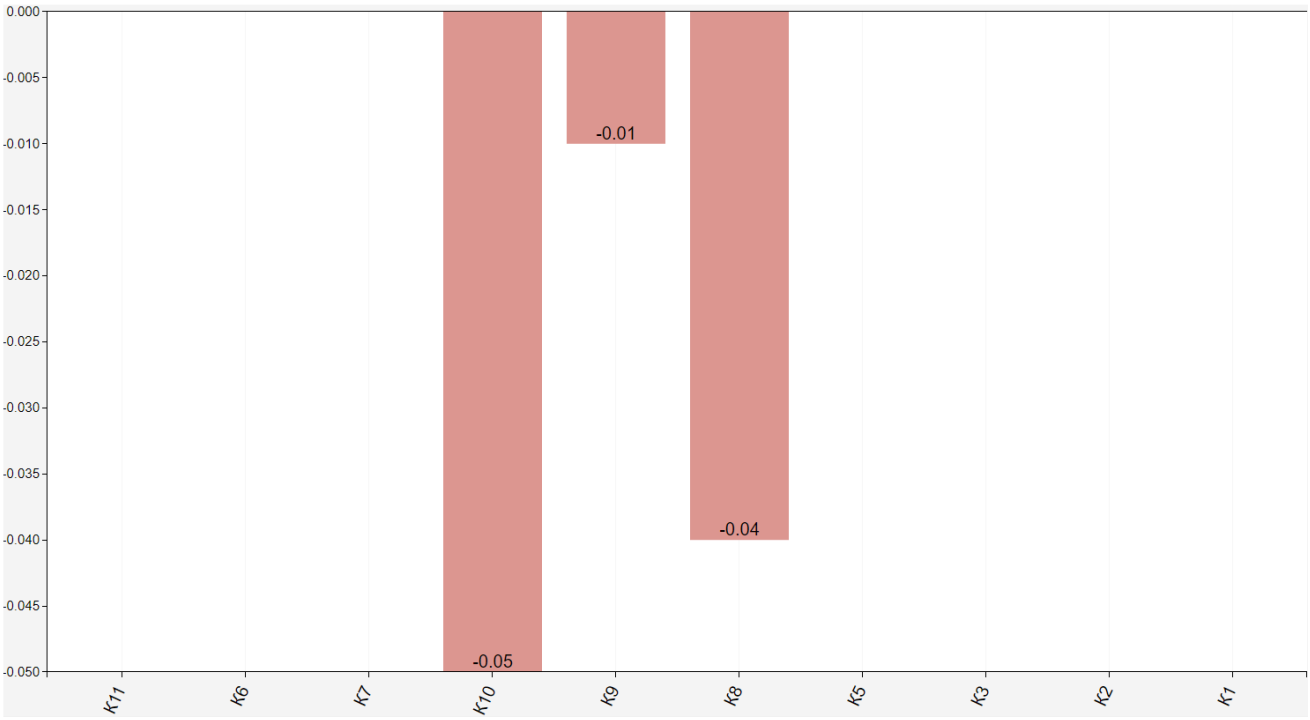


Рисунок 2.4 – Сценарій, що відображає реакцію системи на максимально негативні зміни концепту K_4 – фізичний вплив на мережу з боку зловмисника

На основі даної стовпчастої діаграми можна зробити висновок, що при збільшенні значення даного концепту захищеність КМ зменшиться на 0,01, надійність, відмовостійкість технічних і програмних засобів – на 0,04, а відмовостійкість обслуговування роботи мережі – на 0,05. Тому особливу увагу

потрібно звернути на підсилення фізичних засобів, що дозволять вирішити задачі, пов'язані із захистом території, приміщень, обладнання та здійснення контрольованого доступу до них.

Сценарій 3. Дослідимо можливі зміни концептів при максимальному збільшенні негативного впливу на мережу концепту K_7 – ненавмисні дії, помилки користувачів мережі.

Ненавмисні дії, помилки користувачів, операторів і системних адміністраторів, які обслуговують мережу можуть призвести як до несправностей чи повної непрацездатності системи, так і до створення слабких місць, якими можуть скористатися зловмисники.

Концепт K_7 – ненавмисні дії, помилки користувачів мережі має безпосередній вплив на K_3 – шкідливі програми, K_6 – розголошення інформації користувачем, K_8 – надійність, відмовостійкість технічних і програмних засобів, K_9 – захищеність КМ та опосередковано впливає на K_{10} – відмовостійкість обслуговування роботи мережі. Розглянемо відносні зміни значень цих концептів (рис. 2.5).

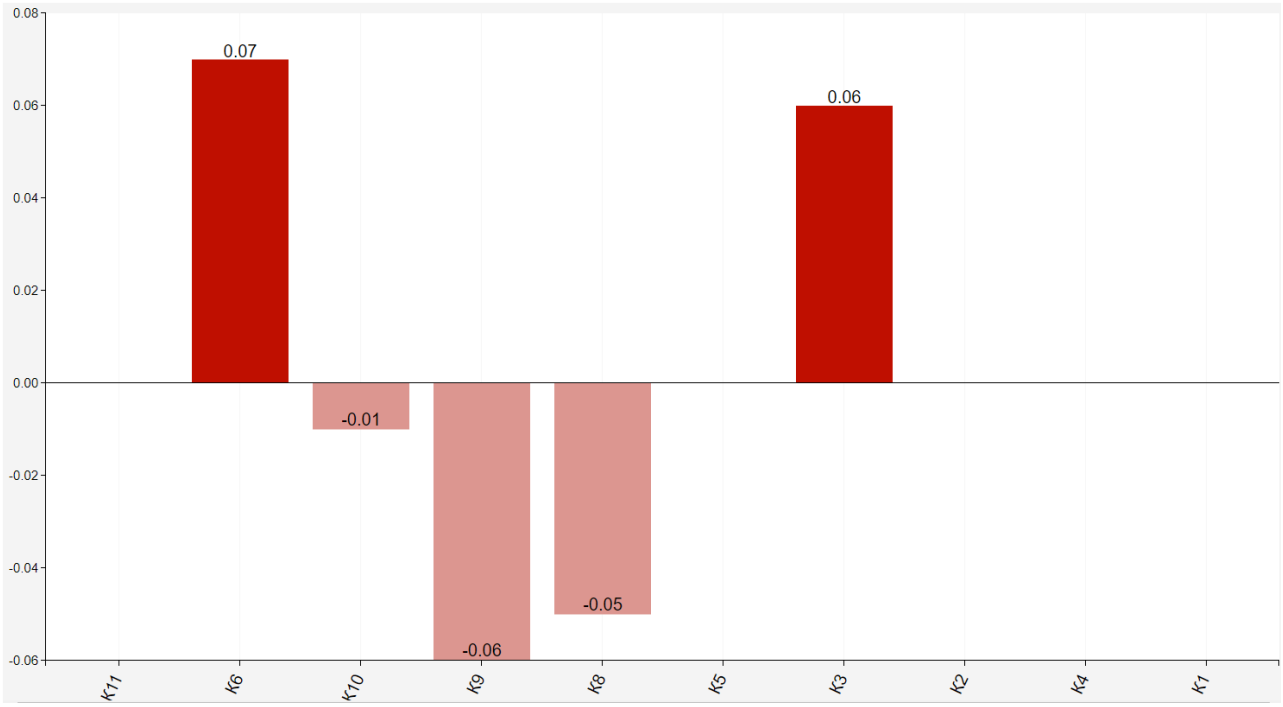


Рисунок 2.5 – Сценарій, що відображає реакцію системи на максимальні негативні зміни концепту K_7 – ненавмисні дії, помилки користувачів мережі

Отримана гістограма показує, що в результаті вищезазначених дій збільшиться значення таких концептів як K_3 – шкідливі програми (на 0,06) та K_6 – розголошення інформації користувачем (на 0,07), що призведе до погіршення відмовостійкості обслуговування роботи мережі на 0,01, надійності, відмовостійкості технічних і програмних засобів – на 0,05, у свою чергу, захищеність КМ зменшиться на 0,06. Таким чином, необхідно правильно організовувати роботу зі співробітниками, яка передбачає якісний підбір і розстановку персоналу, включаючи навчання правил роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил ЗІ, проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв, періодичне проходження навчання та ін.

На рис. 2.6 відображено відносну зміну рівня захищеності КМ при комплексному максимальному послаблені впливу найвагоміших загроз.

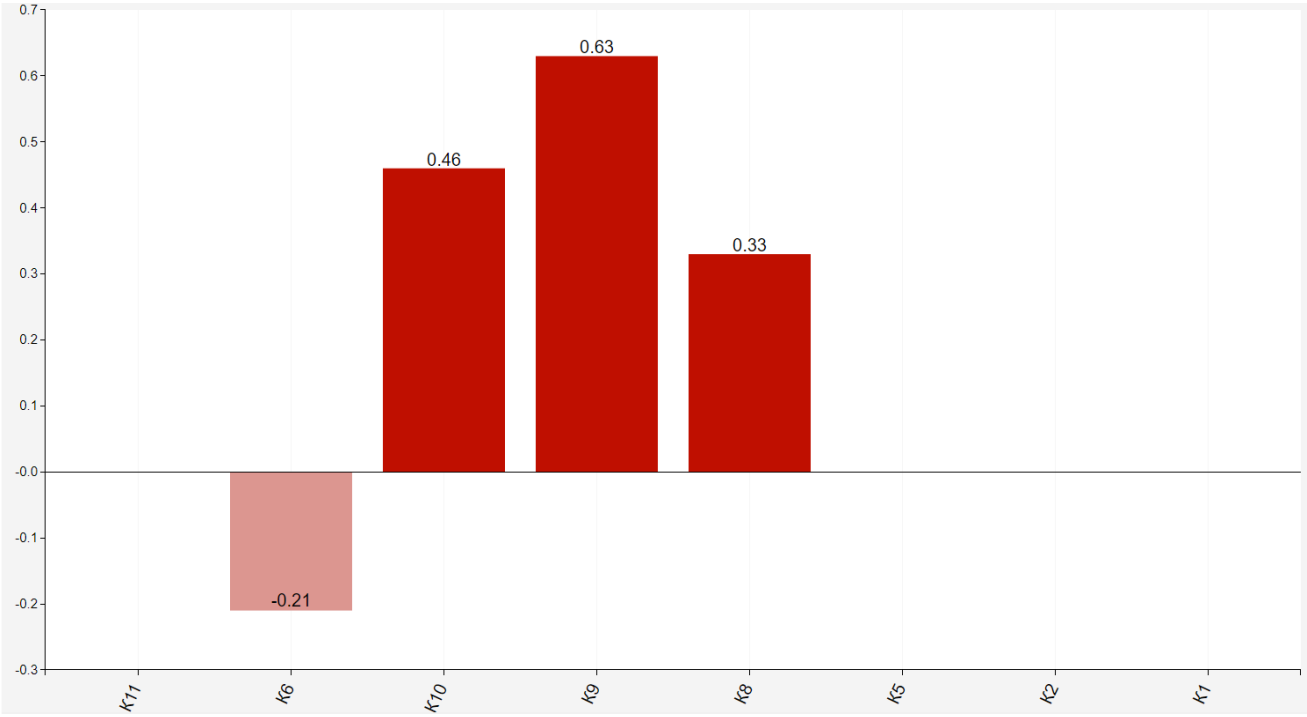


Рисунок 2.6 – Сценарій, що відображає реакцію системи при комплексному максимальному послаблені впливу найвагоміших загроз

У результаті аналізу даної гістограми можна зробити висновок, що при

заданих умовах захищеність КМ підвищиться на 0,63 умовні одиниці, тобто на 63%.

Отже, розроблена НКК аналізу впливу загроз на рівень захищеності мережі відображає, головним чином, якісні тенденції розвитку ситуації та являється одним із засобів оптимізації робіт при налаштуванні захисту КМ.

Результати даного дослідження надають можливість прогнозувати стан мережевої безпеки, що, у свою чергу, сприяє впровадженню необхідних механізмів попередження, захисту та контролю доступу на відповідних рівнях мережевої інфраструктури.

2.2 Розробка та аналіз когнітивної моделі для визначення рівня захищеності системи захисту інформації

У попередньому пункті було запропоновано когнітивну модель, яка дозволяє аналізувати вплив загроз на рівень захищеності КМ, але не розглядає задачу оцінювання стану захищеності системи ЗІ в цілому. Тому актуальним є дослідження пов’язане з визначенням рівня захищеності системи ЗІ на основі когнітивного підходу.

В якості об’єкта дослідження оберемо систему ЗІ із загальними характеристиками, щоб виявляти загальні тенденції зміни рівня захищеності при впливі потенційних загроз.

При комплексному підході до захищеності досліджуваної системи на основі когнітивної моделі, насамперед, необхідно сформувати множину концептів – найвагоміших факторів з точки зору вивчення даної проблеми. Аналізуючи дані отримані в результаті експертного опитування, для побудови НКК аналізу стану захищеності системи ЗІ було сформовано такі концепти:

– K_1 – захист від витоку технічними каналами. Зауважимо, що технічні канали включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали [39];

– K_2 – захист каналу передавання інформації. До таких каналів можна віднести лінії технічних засобів передавання інформації й систем їх життєзабезпечення (мережа електроживлення, заземлення, пожежна й охоронна сигналізація, системи опалення, водопостачання, вентиляції тощо), що проходять через периметр контрольованої зони і виходять за її межі;

– K_3 – розголошення інформації персоналом. Розголошення виражається у повідомленні, передаванні, наданні, пересиланні, опублікуванні, втраті й у інших формах обміну і дій з діловою та науковою інформацією [34];

– K_4 – фізичний захист. Фізичний НСД до приміщення організації, у кабінети і серверні кімнати, до обладнання, паперових документів, запам'ятовуючих пристроїв, носіїв інформації і т. п. може призвести до їх крадіжки або ж пошкодження [40];

– K_5 – НСД до інформації зловмисником. НСД може здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування неправдивої інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів [39];

– K_6 – організаційне забезпечення ЗІ. Даний концепт забезпечує організацію охорони, режиму, роботу з кадрами, з документами; використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності тощо [34];

– K_7 – ненавмисні дії, помилки обслуговуючого персоналу. Дана загроза включає у себе дії, що здійснюються випадково, через відсутність необхідних знань, неуважність або недбалість, з цікавості, але без злого умислу;

– K_8 – надійність, відмовостійкість технічних та програмних засобів. Досліджувана система має бути захищена від фізичних відмов обладнання, забезпечуючи працездатність компонентів програмно-технічної платформи та оперативне відновлення резервних копій;

– K_9 – нормативно-правове забезпечення захисту. Нормативно-правове

забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови КСЗІ; права, обов'язки й відповідальність персоналу роботи яких пов'язані з ІБ; етапи створення КСЗІ [106];

– K_{10} – природні явища та явища техногенного характеру. До цієї загрози можуть відноситись вибух, аварія, пожежа, затоплення, ураган, землетрус і т. п.;

– K_{11} – захищеність системи ЗІ.

Наступним кроком є визначення сили зв'язку між кожною парою концептів. Для цього використаємо нечітку лінгвістичну шкалу (2.1) та її відповідність (2.2) деякому числовому діапазону.

Розробка експертами в галузі ІБ структури знань про систему захисту, списку концептів та сили зв'язку між ними дозволяє побудувати НКК ідентифікації стану захищеності системи ЗІ (рис. 2.7).

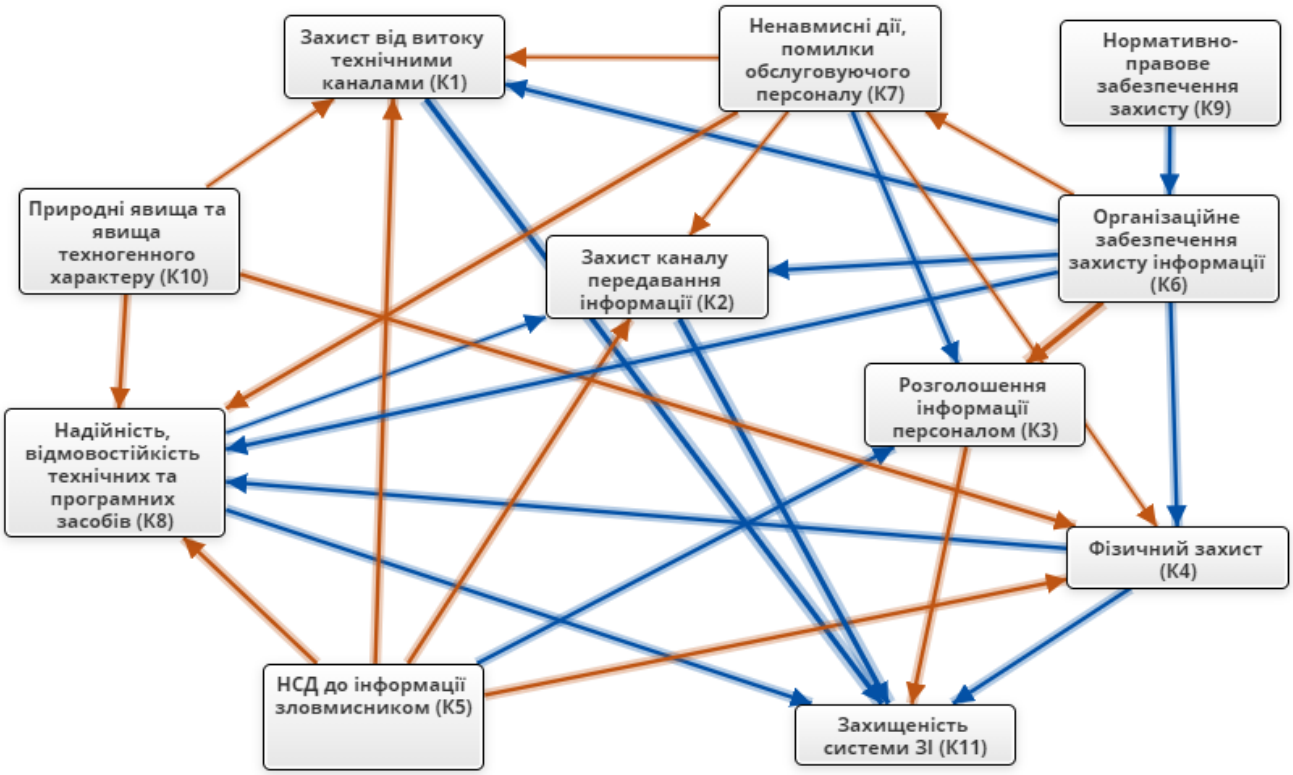


Рисунок 2.7 – НКК дослідження стану захищеності системи ЗІ

Проаналізувавши причинно-наслідкові зв'язки між концептами, зауважимо, що розроблена НКК містить:

1) три концепти типу «Driver» – впливають на інші концепти, а на них не впливає жодний з концептів системи;

2) один концепт типу «Receiver» – на нього впливають концепти системи, а він не впливає ні на жоден з них;

3) сім концептів типу «Ordinary» – звичайні, проміжні концепти, які впливають і на яких впливають деякі концепти системи.

Матриця суміжності $W = \left\lfloor w(K_i, K_j) \right\rfloor_{n \times n}$ даної НКК відображена у табл. 2.2

Таблиця 2.2

Матриця суміжності НКК предметної області

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	0	0	0	0	0	0	0	0	0	0	0,9
K_2	0	0	0	0	0	0	0	0	0	0	0,85
K_3	0	0	0	0	0	0	0	0	0	0	-0,75
K_4	0	0	0	0	0	0	0	0,5	0	0	0,7
K_5	-0,55	-0,7	0,82	-0,75	0	0	0	-0,55	0	0	0
K_6	0,7	0,65	-0,9	0,8	0	0	-0,3	0,7	0	0	0
K_7	-0,45	-0,3	0,58	-0,42	0	0	0	-0,55	0	0	0
K_8	0	0,25	0	0	0	0	0	0	0	0	0,55
K_9	0	0	0	0	0	0,55	0	0	0	0	0
K_{10}	-0,35	0	0	-0,5	0	0	0	-0,82	0	0	0
K_{11}	0	0	0	0	0	0	0	0	0	0	0

Для визначення структурно-топологічних властивостей отриманої НКК визначимо показники її структурної складності:

а) щільність НКК (d). Даний показник обчислюється за допомогою формули (2.3) та показує ступінь зв'язності графа, який відображає відповідну когнітивну карту. Для досліджуваної НКК $d = 0{,}25$, що вказує на достатньо велику кількість зв'язків між концептами, тобто на високу щільність розробленої НКК.

б) центральність концепта – характеризує ступінь взаємодії *i*-го концепту НКК з його сусідами:

– вихідна центральність – показує сукупну силу зв'язків (w_{ij}), що виходять з

аналізованого концепта K_i:

$$od_i = \sum_{j=1}^{n} w_{ij};$$

– вхідна центральність – показує сукупну силу зв'язків (w_{ij}), що входять до аналізованого концепта K_i:

$$id_i = \sum_{j=1}^{n} w_{ij};$$

– загальна центральність концепта обчислюється за формулою:

$$td_i = od_i + id_i. \quad (2.4)$$

Розрахунок показників центральності показав, що найбільш високу структурну значимість має концепт K_6 $(td_6 = 4{,}6)$, а також концепти K_8, K_{11}, K_4, K_5 (показники $td_8, td_{11}, td_4, td_5$ рівні відповідно 3,92; 3,75; 3,67; 3,36). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу в НКК для аналізу рівня захищеності системи ЗІ.

в) складність – представляє собою співвідношення кількості концептів типу «Receiver» до концептів типу «Driver». Чим більше значення даного коефіцієнта, тим складніші карти, оскільки припускається, що вони містять більше корисних результатів та менше контрольованих впливів на зовнішнє середовище.

Для розробленої НКК предметної області отримаємо співвідношення: $\frac{1}{3} \approx 0{,}33$, що вказує на недостатньо складні системи мислення.

г) індекс ієрархії (h):

$$h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}, \quad (2.5)$$

де $\sigma_{od}^2 = \frac{\sum_{i=1}^{n} (od_i - \mu_{od})^2}{n}$, $\mu_{od} = \frac{\sum_{i=1}^{n} od_i}{n}$.

При $h = 1$ система є повністю ієрархічною, при $h = 0$ – повністю демократичною. Демократичні системи більш адаптивні до змін зовнішнього середовища завдяки високому рівню їх інтеграції та зв'язності. У нашому випадку $h = 0{,}2$, що свідчить про високу демократичність досліджуваної системи.

На рис. 2.8 відображено кількісне значення основних системних показників розробленої НКК предметної області:

Component	Indegree	Outdegree	Centrality
Фізичний захист (К4)	2.4699999999999998	1.2	3.67
Захист від витоку технічними каналами (К1)	2.0500000000000003	0.9	2.95
Надійність, відмовостійкість технічних та програмних засобів (К8)	3.12	0.8	3.92
Нормативно-правове забезпечення захисту (К9)	0	0.55	0.55
НСД до інформації зловмисником (К5)	0	3.3699999999999997	3.3699999999999997
Захищеність системи ЗІ (К11)	3.7500000000000004	0	3.7500000000000004
Захист каналу передавання інформації (К2)	1.9000000000000001	0.85	2.75
Природні явища та явища техногенного характеру (К10)	0	1.67	1.67
Організаційне забезпечення захисту інформації (К6)	0.55	4.05	4.6
Ненавмисні дії, помилки обслуговуючого персоналу (К7)	0.3	2.3	2.5999999999999996
Розголошення інформації персоналом (К3)	2.3	0.75	3.05

Рисунок 2.8 – Основні показники НКК предметної області

Проаналізувавши вищезазначені показники, визначимо найвпливовіші концепти досліджуваної системи: K_6 – організаційне забезпечення ЗІ, K_4 – фізичний захист, K_5 – НСД до інформації зловмисником. Відмітимо, що найменший рівень впливу на систему ЗІ має концепт K_9 – нормативно-правове забезпечення захисту.

На етапі аналізу НКК предметної області проведемо сценарне моделювання для визначення відносної зміни рівня захищеності системи ЗІ при максимальному значенні впливу на неї найвагоміших концептів.

Сценарій 1. Стан концепта K_6 – організаційне забезпечення ЗІ активується, приймаючи максимально можливе негативне значення.

Зауважимо, що організаційна складова ЗІ відіграє значну роль при створенні надійного комплексного механізму безпеки. Адже більшість загроз обумовлюються не технічними аспектами, а діями зловмисників, необережністю

чи помилками персоналу. Тому важливо отримати прогноз розвитку даної ситуації.

Концепт K_6 у розробленій НКК має безпосередній вплив на концепти: K_1 – захист від витоку технічними каналами, K_2 – захист каналу передавання інформації, K_3 – розголошення інформації персоналом, K_4 – фізичний захист, K_7 – ненавмисні дії, помилки обслуговуючого персоналу, K_8 – надійність, відмовостійкість технічних і програмних засобів та опосередкований вплив на K_{11} – захищеність системи ЗІ. Тому при зміні значення K_6 спостерігатиметься така реакція досліджуваної системи (рис. 2.9).

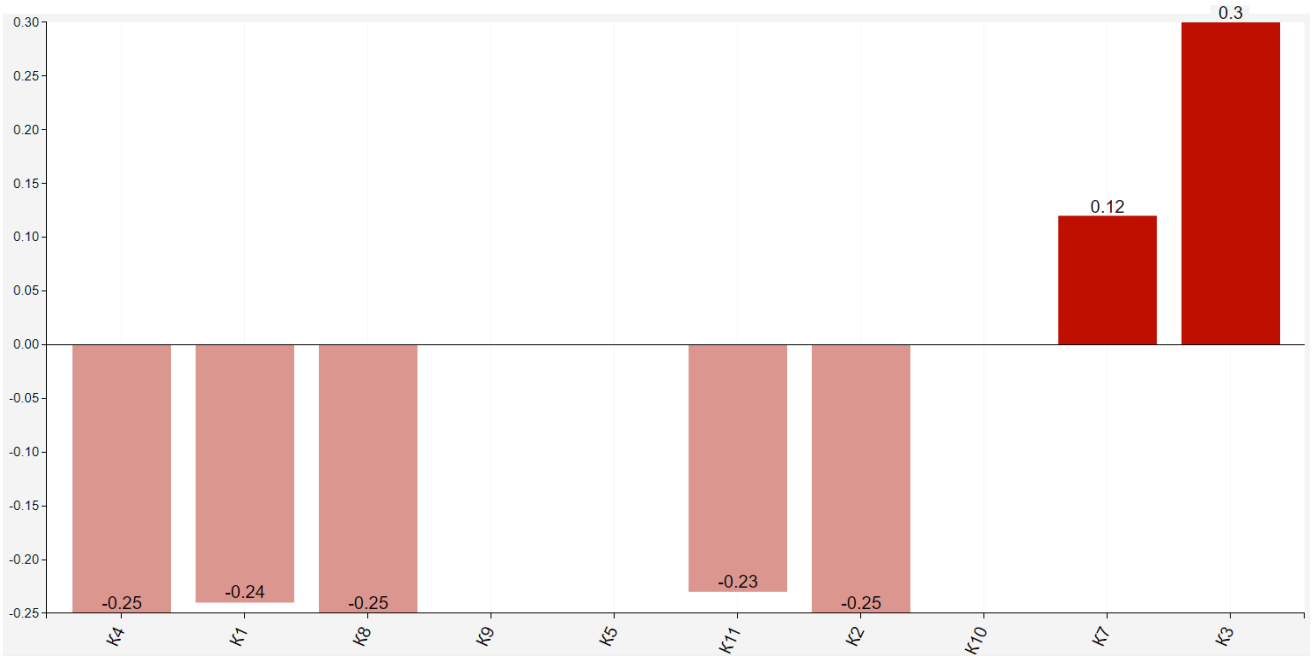


Рисунок 2.9 – Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_6

Отримана стовпчаста діаграма показує, що при неналежній організації забезпечення ЗІ спостерігатиметься збільшення значення концептів K_7 – ненавмисні дії, помилки обслуговуючого персоналу та K_3 – розголошення інформації персоналом, що, у свою чергу, призведе до зменшення захисту від витоку технічними каналами на 0,24, послаблення фізичного захисту, надійності, відмовостійкості технічних та програмних засобів, захисту каналу передавання

інформації – кожного на 0,25 і, у цілому, рівень захищеності системи ЗІ погіршиться на 0,23.

Для попередження негативних наслідків необхідно особливу увагу приділяти плануванню організаційних заходів, які мають здійснюватися спеціально створеною структурою, укомплектованою висококваліфікованими фахівцями з ІБ.

Сценарій 2. Максимальне зменшення значення концепту K_4 – фізичний захист.

Фізична безпека спрямована на захист від таємного проникнення на територію і у приміщення сторонніх осіб, часового контролю перебування персоналу на робочому місці, організації і дотримання надійного пропускного режиму і т. п.

У досліджуваній моделі концепт K_4 – фізичний захист має безпосередній вплив на концепти K_8 – надійність, відмовостійкість технічних та програмних засобів і K_{11} – захищеність системи ЗІ та опосередкований вплив на K_2 – захист каналу передавання інформації. Максимально негативна зміна значення K_4 призведе до такої ситуації (рис. 2.10).

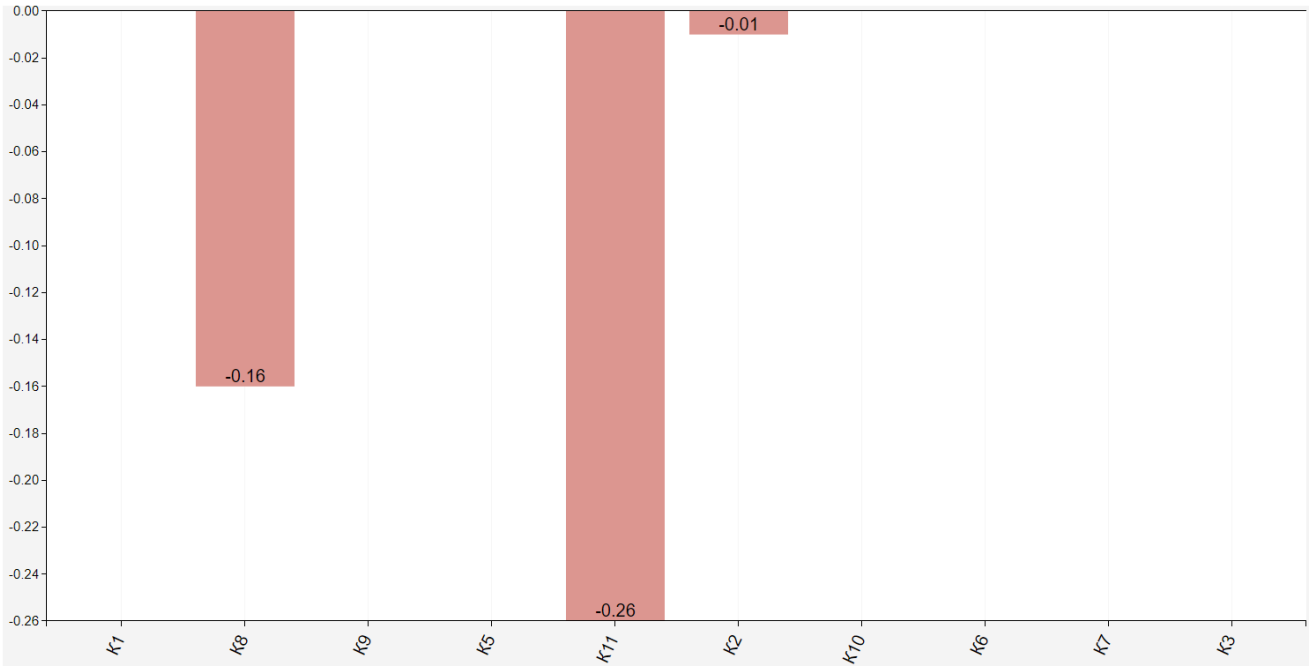


Рисунок 2.10 – Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_4

Проаналізувавши отриману гістограму, можна зробити висновки щодо відносної зміни концептів розробленої НКК, на які впливає K_4. Зокрема, прослідковується зменшення надійності, відмовостійкості технічних та програмних засобів на 0,16, послаблення захисту каналу передавання інформації на 0,01 та захищеності системи ЗІ – на 0,26.

Таким чином, щоб попередити вищезазначену ситуацію доцільно підсилити систему охорони периметра, відеоспостереження, охоронної сигналізації, контролю й управління доступом, систему збереження (сейфи, шафи тощо).

Сценарій 3. Максимальне посилення негативного значення концепта K_5 – НСД до інформації зловмисником.

Отримання НСД до інформації призводить до витоку даних, їх копіювання, модифікації, видалення, блокування доступу як до інформації так і до всієї системи, виведення її з ладу.

В побудованій НКК концепт K_5 – НСД до інформації зловмисником безпосередньо впливає на такі концепти: K_1 – захист від витоку технічними каналами, K_2 – захист каналу передавання інформації, K_3 – розголошення інформації персоналом, K_4 – фізичний захист, K_8 – надійність, відмовостійкість технічних та програмних засобів та має опосередкований вплив на K_{11} – захищеність системи ЗІ. Реакцію системи на збільшення значення даного концепта зображено на рис. 2.11.

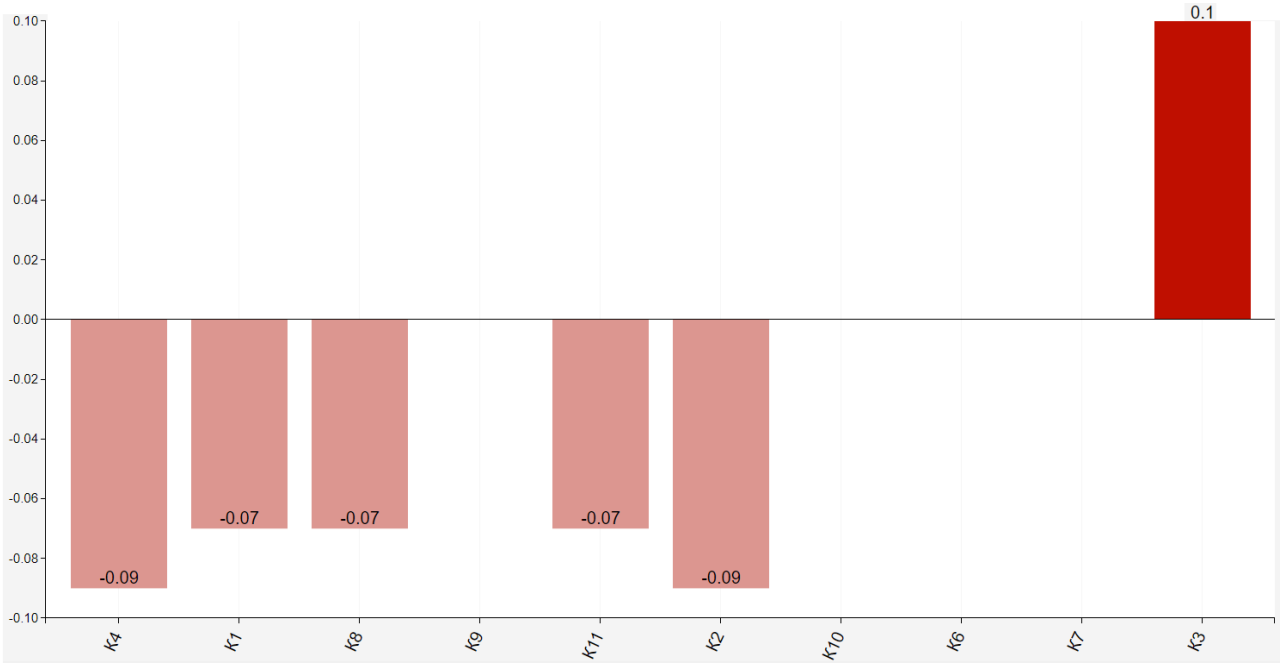


Рисунок 2.11 – Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_5

У результаті моделювання даного сценарію бачимо, що розголошення інформації персоналом збільшиться, при цьому захист від витоку технічними каналами, надійність, відмовостійкість технічних й програмних засобів та захищеність системи ЗІ послабляться на 0,07, а захист каналу передавання інформації та фізичний захист – на 0,09.

Щоб попередити наслідки вищезазначеного сценарію, варто підвищити заходи безпеки від НСД, використавши апаратні засоби захисту, систему контролю доступу до окремих документів, аутентифікацію, одноразові паролі тощо.

Розглянемо як зміниться захищеність системи ЗІ при максимально позитивному впливі найвагоміших концептів (рис. 2.12).

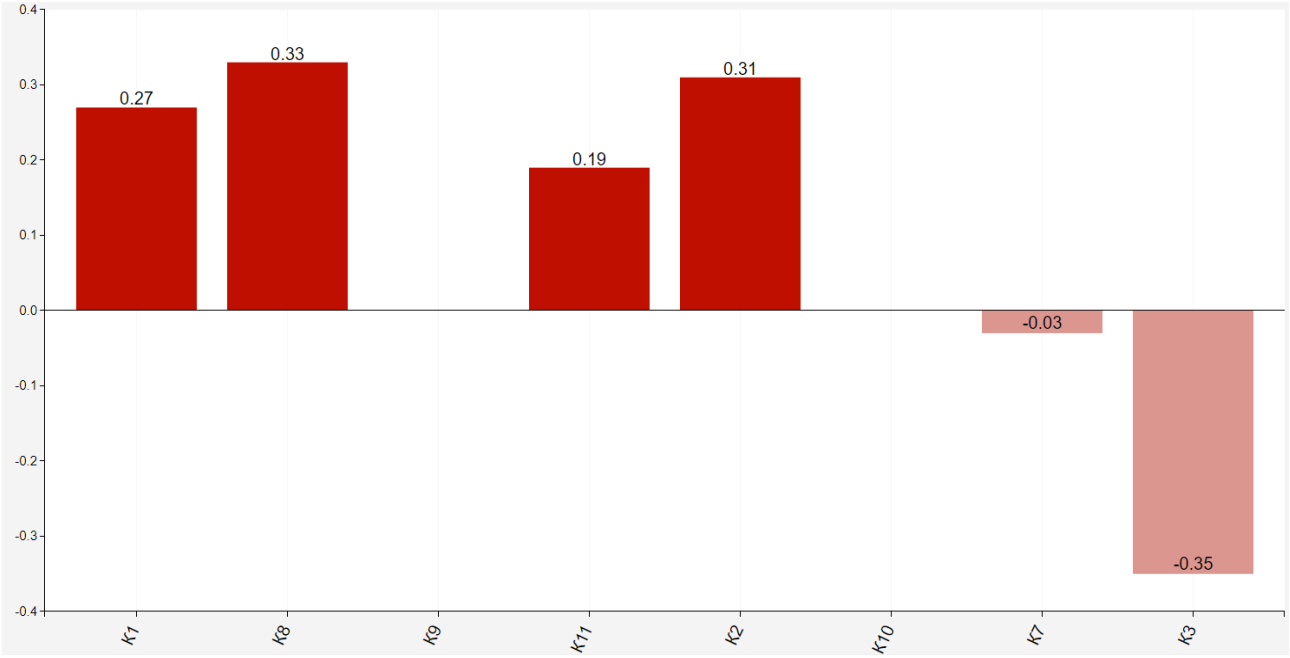


Рисунок 2.12 – Сценарій, що відображає реакцію системи при максимально позитивному впливі найвагоміших концептів

Отримана гістограма показує, що при максимально ефективному організаційному забезпеченню й фізичному захисті досліджуваної системи, за умови мінімального НСД до інформації зловмисником, захищеність системи ЗІ збільшиться на 0,19 умовних одиниць, тобто на 19 %.

Отже, розроблена когнітивна модель для визначення рівня захищеності системи ЗІ надає достатній ступінь деталізації, дозволяє враховувати наявність великої кількості альтернативних сценаріїв реалізації загроз. На основі даних отриманих у результаті запуску даних сценаріїв можна розробити чіткий план організації підвищення рівня захищеності системи ЗІ, вчасно провести необхідні заходи, що допоможуть запобігти, локалізувати, усунути або ж зменшити силу впливу ймовірних загроз ІБ.

2.3 Розробка та аналіз когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури

Стратегічно важливим для функціонування економіки і безпеки держави, суспільства та населення є захист об’єктів КІ – підприємств та установ (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість,

транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [107]. У свою чергу, інформатизація об'єктів КІ викликає безліч ризиків, пов'язаних із порушенням функціонування інформаційних систем КІ, що може призвести до розвитку надзвичайних ситуацій, пов'язаних з великомасштабним порушенням життєдіяльності як окремих міст, так і усієї держави в цілому. Тому варто звернути особливу увагу на забезпечення ІБ об'єктів КІ, враховуючи вплив потенційних загроз.

Дослідимо об'єкт КІ, який відноситься до класу об'єктів, що передбачає доступ до мережі Інтернет та відображає максимальне представлення структурних складових. Сформуємо множину загроз даному об'єкту, відмітивши, що основні напрями вектора атак направлені на ІТ-інфраструктуру та операційні технології [108]. Причому, велика кількість загроз спрямована на систему контролю та збору даних (SCADA) та на розподілені системи управління (DCS), які надають життєво важливі послуги КІ [109].

Доцільно виділити такі категорії загроз, на які має бути налаштовано захист КІ [110]:

– аварії й технічні збої, зокрема авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події, зумовлені недбалістю, організаційними помилками тощо;

– небезпечні природні явища, зокрема надзвичайні погодні умови, лісові, степові й торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені тощо;

– зловмисні дії, зокрема зловмисні дії груп або окремих осіб, таких як терористи, злочинці й диверсанти, а також бойові дії в умовах війни.

Особливо небезпечними є комбіновані загрози й загрози, реалізація яких

може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів КІ.

Загрози КІ можна розглядати не лише з огляду на характер їх походження, а й на елементи КІ, на які ці загрози спрямовані [110]:

– фізичні елементи, зокрема обладнання й ресурси об’єктів КІ;

– системи управління та комунікації, зокрема автоматизованих систем управління та систем зв’язку;

– персонал об’єктів, зокрема диспетчерський, оперативний, який безпосередньо забезпечує функціонування КІ у реальному часі.

У результаті проведення експертами аналізу можливих загроз безпеці КІ було сформовано множину найвагоміших концептів, з точки зору вивчення даної проблеми:

K_1 – природні явища;

K_2 – техногенний вплив;

K_3 – соціально-політичний вплив;

K_4 – економічний вплив;

K_5 – правовий вплив;

K_6 – військове вторгнення;

K_7 – терористичний вплив;

K_8 – промислове шпигунство;

K_9 – хакерський вплив;

K_{10} – вплив управлінських рішень та організаційних заходів;

K_{11} – інсайдерський вплив;

K_{12} – безпека каналів зв’язку КІ;

K_{13} – надійність, відмовостійкість складових КІ;

K_{14} – захищеність КІ;

K_{15} – захищеність системи ЗІ;

K_{16} – захищеність КМ;

K_{17} – безпека центру управління;

K_{18} – безпека обслуговуючих систем та обладнання;

K_{19} – безпека обслуговуючого персоналу;

K_{20} – захищеність сховищ даних;

K_{21} – захищеність хмарних серверів;

K_{22} – безпека інформаційної інфраструктури;

K_{23} – безпека Інтернет-додатків;

K_{24} – безпека Інтернет;

K_{25} – мережеві атаки;

K_{26} – шкідливі програми;

K_{27} – DoS-атаки.

Вплив загроз на K_{15} – захищеність системи ЗІ та K_{16} – захищеність КМ можна здійснювати на основі моделей, представлених у попередніх пунктах.

Наступним кроком є визначення сили впливу $w_{ij} \in [-1;1]$, що відображає зміни одного концепта K_i на зміну іншого K_j. Вирішення даної задачі здійснюється експертним шляхом за допомогою лінгвістичних термів (2.1) та відповідних їм числових діапазонів (2.2).

Визначивши склад концептів та силу впливу причинно-наслідкових зв’язків між ними, побудуємо НКК для дослідження рівня захищеності об’єкта КІ (рис. 2.13).

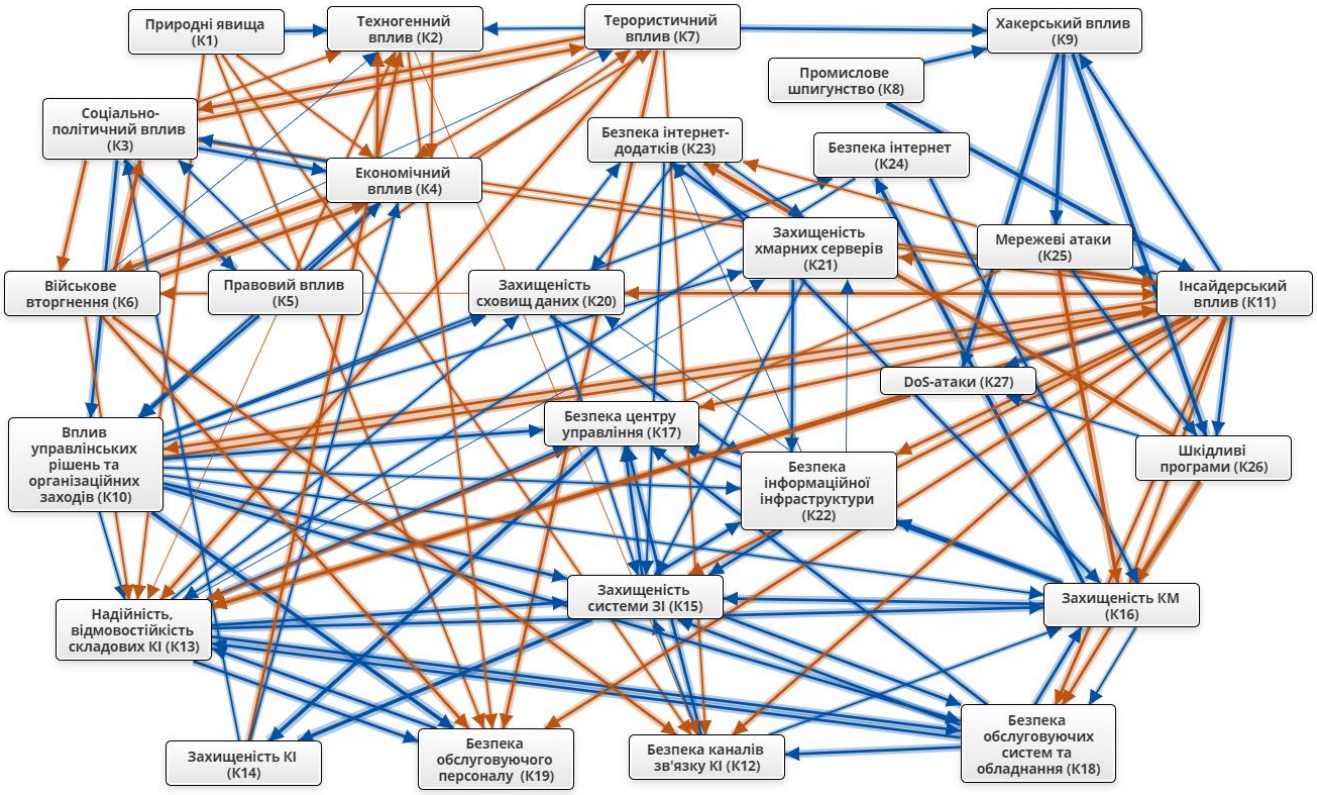


Рисунок 2.13 – НКК для дослідження рівня захищеності об’єкта КІ

Розглянемо матрицю $W = \left\| w(K_i, K_j) \right\|_{n \times n}$ взаємовпливів концептів даної НКК (табл. 2.3-2.4).

Таблиця 2.3

Матриця взаємовпливів концептів НКК предметної області на концепти $K_1 - K_{15}$

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
K_1	0	0,55	0	-0,4	0	0	0	0	0	0	0	-0,2	-0,3	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	-0,1	-0,15	0	0
K_3	0	-0,35	0	0,7	0,85	-0,7	-0,5	0	0	0,75	-0,2	0	0	0	0
K_4	0	-0,5	0,3	0	0	-0,87	-0,4	0	0	0,35	-0,35	0	0	0	0
K_5	0	-0,4	0,4	0,55	0	-0,4	-0,4	0	0	0,8	-0,1	0	0	0	0
K_6	0	0,1	-0,85	-0,85	0	0	0,1	0	0	0	0	-0,5	-0,4	0	0
K_7	0	0,2	-0,5	-0,2	0	0	0	0	0,8	0	0	-0,3	-0,55	0	0
K_8	0	0	0	0	0	0	0	0	0,7	0	0,9	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0	0	-0,7	0	0,2	0	0,7
K_{11}	0	0	0	0	0	0	0	0	0,8	-0,6	0	-0,6	-0,75	0	-0,8
K_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4

Продовження таблиці 2.3

K_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,55
K_{14}	0	-0,6	0,35	0,4	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{16}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,5
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{18}	0	0	0	0	0	0	0	0	0	0	0	0,7	0,5	0	0,8
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0	0,7	0	0
K_{20}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{21}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{22}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,6
K_{23}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4
K_{24}	0	0	0	0	0	0	0	0	0	0	0	0	0,35	0	0
K_{25}	0	0	0	0	0	0	0	0	0	0	0	0	-0,2	0	0
K_{26}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0	-0,6	0	0

Таблиця 2.4

Матриця взаємовпливів концептів НКК предметної області на концепти $K_{16} - K_{27}$

	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}
K_1	0	0	0	-0,2	0	0	0	0	0	0	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	0
K_3	0	0	0	0	0	0	0	0	0	0	0	0
K_4	0	0	0	0	0	0	0	0	0	0	0	0
K_5	0	0	0	0	0	0	0	0	0	0	0	0
K_6	0	0	0	-0,75	0	0	0	0	0	0	0	0
K_7	0	0	0	-0,55	0	0	0	0	0	0	0	0
K_8	0	0	0	0	0	0	0	0	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0,9	0,9	0,9
K_{10}	0,4	0,7	0,6	0,9	0,4	0,2	0,25	0	0,4	0	0	0
K_{11}	-0,8	-0,8	-0,8	-0,6	-0,6	-0,4	-0,8	0	0	0,3	0,5	0,2
K_{12}	0,3	0,65	0	0	0	0	0	0	0	0	0	0
K_{13}	0,55	0,55	0,8	0,55	0,2	0,1	0	0	0	0	0	0
K_{14}	0	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0,8	0,6	0	0	0	0,6	0	0	0	0	0
K_{16}	0	0,6	0,4	0	0	0	0,7	0	0,85	0	0	0

Продовження таблиці 2.4

K_{17}	0	0	0	0	0	0	0	0	0	0	0	0
K_{18}	0,8	0,8	0	0	0	0	0	0	0	0	0	0
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0
K_{20}	0	0	0	0	0	0	0,8	0,4	0	0	0	0
K_{21}	0	0	0	0	0	0	0,55	0,8	0	0	0	0
K_{22}	0	0	0	0	0,15	0,1	0	0,1	0	0	0	0
K_{23}	0,75	0	0	0	0,3	0,2	0	0	0	0	0	0
K_{24}	0,75	0	0	0	0	0	0	0	0	0	0	0
K_{25}	-0,9	0	0	0	0	0	0	-0,25	0	0	0,7	0
K_{26}	-0,9	0	-0,65	0	0	0	0	-0,85	0	0	0	0,2
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0

Визначимо структурно-топологічні властивості розробленої НКК, проаналізувавши такі показники структурної складності НКК як щільність, індекс ієрархії та центральність концептів:

а) щільність (d) розраховано за допомогою формули (2.3): $d = 0{,}18$. Дане значення вказує на достатню складність розробленої моделі. Чим вище значення щільності, тим більше потенційних політик управління;

б) центральність концепта – характеризує ступінь взаємодії і-го концепта НКК з його сусідами і обчислюється за формулою (2.4). Розрахунок показників центральності показав, що найбільш високу структурну значимість має концепт K_{11} $(td_i = 11{,}6)$, а також концепти $K_{16}, K_{15}, K_{13}, K_{10}$ (показники $td_{16,}\ td_{15}, td_{13}, td_{10}$ рівні відповідно 9,2; 8,39; 8,0; 7,95). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу у НКК для дослідження рівня захищеності об'єкта КІ. Зазначимо, що найменшу структурну значимість відіграє концепт K_8 $(td_i = 1{,}6)$;

в) індекс ієрархії визначається за формулою (2.5) і дорівнює $h = 0{,}16$, що свідчить про високу демократичність досліджуваної системи.

Виконаємо сценарне моделювання для оцінювання впливу найвагоміших загроз на рівень захищеності об'єкта КІ.

Сценарний аналіз дозволяє отримати прогноз розвитку досліджуваної

ситуації, визначити, оцінити і знизити рівень невизначеності впливу найвагоміших концептів, що впливають на захищеність об'єкта КІ. Це, у свою чергу, сприятиме формуванню стратегічних управлінських рішень щодо підсилення захисту об'єкта КІ. Метод побудови сценаріїв найбільш повно дозволяє проаналізувати вплив найвагоміших загроз на рівень захищеності об'єкта КІ в умовах невизначеності та мінливості оточуючого середовища.

Сценарій 1. Змоделюємо ситуацію, при якій спостерігатиметься максимальне збільшення інсайдерського впливу (K_{11}) на захищеність об'єкта КІ (рис. 2.14).

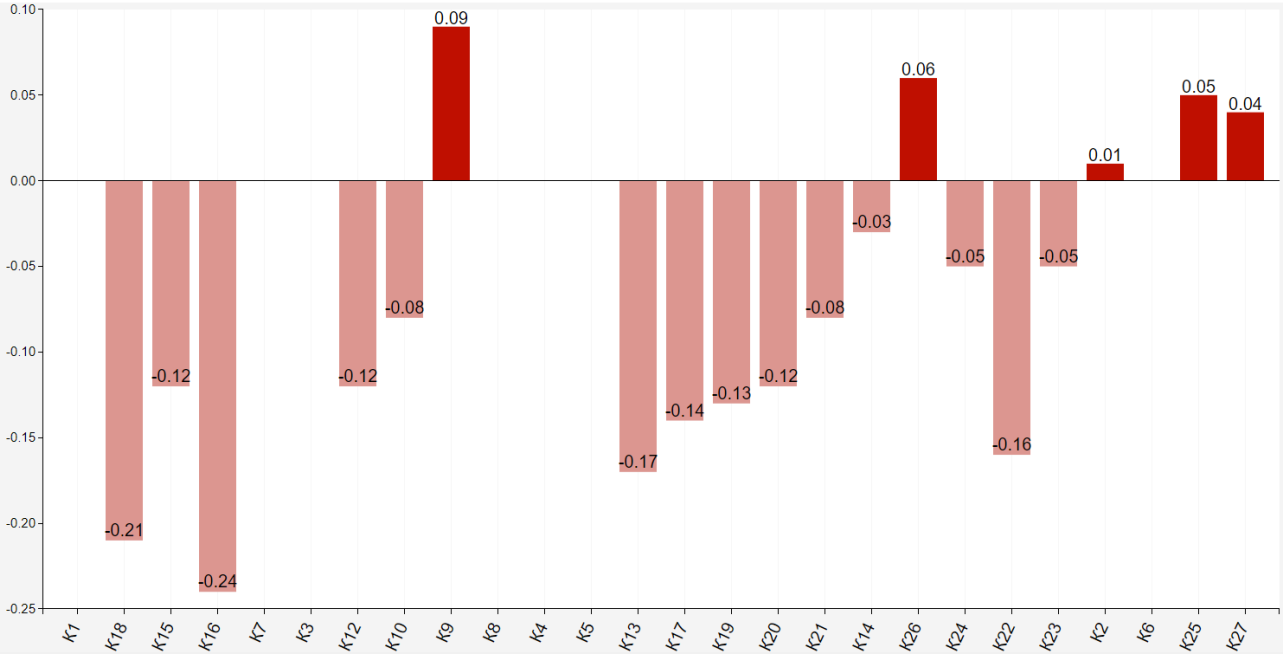


Рисунок 2.14 – Реакція досліджуваної системи на максимальний інсайдерський вплив

Зауважимо, що численні дослідження, проведені у останні роки, показують, що більше 80% усіх інцидентів, пов'язаних з порушенням ІБ, викликані внутрішніми загрозами. Джерелами таких загроз, що спричиняють порушення конфіденційності інформації, є, як правило, інсайдери, тобто особи, що мають через свій службовий стан доступ до інформації обмеженого доступу або ж співробітники, які намагаються його отримати [111].

Аналізуючи отриману стовпчасту діаграму можна зробити висновок, що

найбільше зменшиться значення концептів K_{16} – захищеність КМ (на 0,24) та K_{18} – безпека обслуговуючих систем та обладнання (на 0,21). Крім того, значно погіршиться K_{13} – надійність, відмовостійкість складових КІ (на 0,17), K_{22} – безпека інформаційної інфраструктури (на 0,16), K_{17} – безпека центру управління (на 0,14), K_{19} – безпека обслуговуючого персоналу (на 0,13), K_{12} – безпека каналів зв'язку КІ (на 0,12), K_{15} – захищеність системи ЗІ (на 0,12) та K_{20} – захищеність сховищ даних (на 0,12). Проте K_{14} – захищеність КІ послабиться лише на 0,03.

Для попередження негативних наслідків необхідно особливу увагу приділяти основним компонентам комплексної системи організованих заходів й технічних засобів захисту від інсайдерів, а саме [112]:

– нормативно-правовій базі;

– системі контролю та управління персоналізованим доступом до корпоративних ресурсів КІ;

– моніторингу дій користувачів інформації;

– використанню технічних засобів, що здійснюють контроль й очистку комп'ютерних систем;

– кадровому забезпеченню (обов'язкова наявність штатного спеціаліста, що забезпечує захист від внутрішніх загроз);

– забезпеченню відповідного рівня корпоративної культури, що впливає на підвищення рівня корпоративної безпеки КІ;

– ретельній підбір кадрів, що матимуть доступ до інсайдерської інформації;

– формування ефективного мотиваційного механізму для працівників.

Реалізація зазначених заходів допоможе зменшити інсайдерський вплив та підвищити рівень захищеності КІ.

Сценарій 2. Розглянемо як зміниться стан досліджуваної системи при максимальному послабленні концепта K_{16} – захищеність КМ.

Відмітимо, що КМ є базисом для функціонування ІС у різних сегментах діяльності об'єкта КІ. Адже вона забезпечує передавання даних і комунікацію між автоматизованими вузлами даного об'єкта, управління правами доступу до

інформаційних ресурсів і безпосередньо впливає на ефективне впровадження та застосування ІТ. Тому варто змоделювати даний сценарій для аналізу відносної зміни рівня захищеності досліджуваної системи (рис. 2.15).

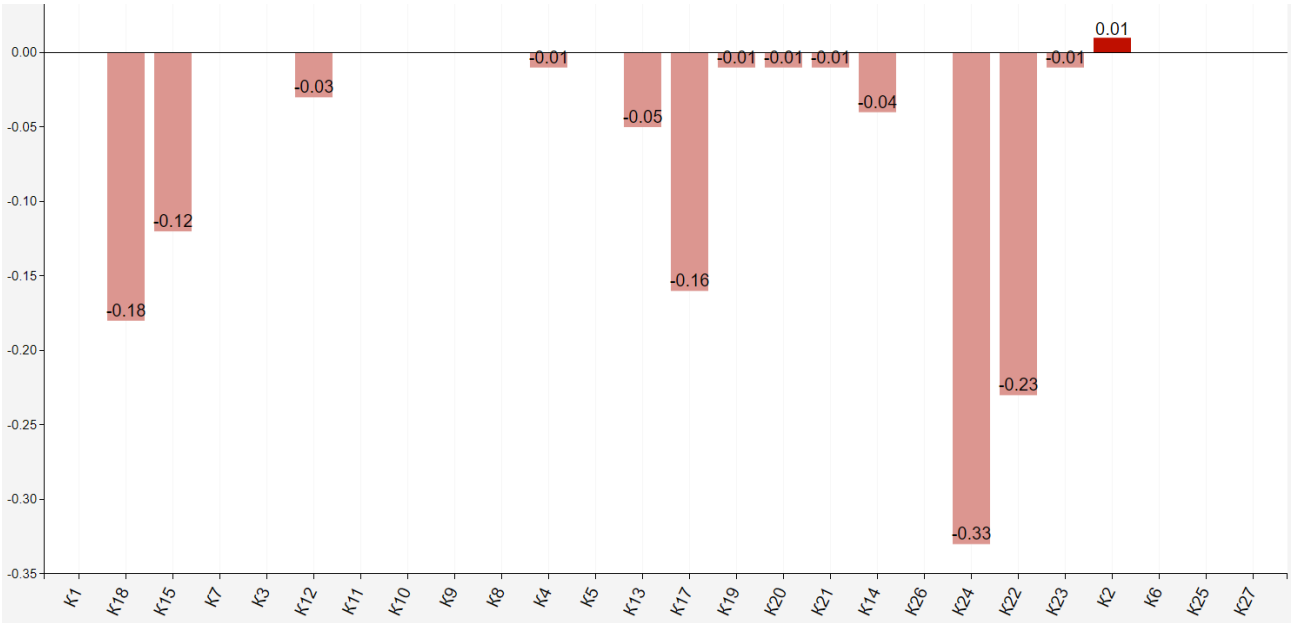


Рисунок 2.15 – Реакція досліджуваної системи при максимальному послабленні захисту КМ

Дослідивши отриману гістограму, можна зробити висновок, що при максимальному послабленні захисту КМ найбільше зменшиться значення концептів: K_{24} – безпека Інтернет (на 0,33), K_{18} – безпека обслуговуючих систем та обладнання (на 0,28), K_{22} – безпека інформаційної інфраструктури (на 0,25), K_{17} – безпека центру управління (на 0,24) та K_{15} – захищеність системи ЗІ (на 0,18). Значення інших концептів системи зміняться не суттєво. При цьому K_{14} – захищеність КІ послабиться на 0,06.

Щоб запобігти вищезазначеним негативним наслідкам необхідно впроваджувати та застосовувати ефективні механізми і засоби для забезпечення мережевої безпеки на об’єктах КІ, які захищатимуть мережу від НСД, випадкового або навмисного втручання у її роботу або спроб руйнування її компонентів.

Сценарій 3. Змоделюємо ситуацію, яка відображатиме зміни концептів

системи при максимально можливому послабленні захищеності системи ЗІ (рис. 2.16).

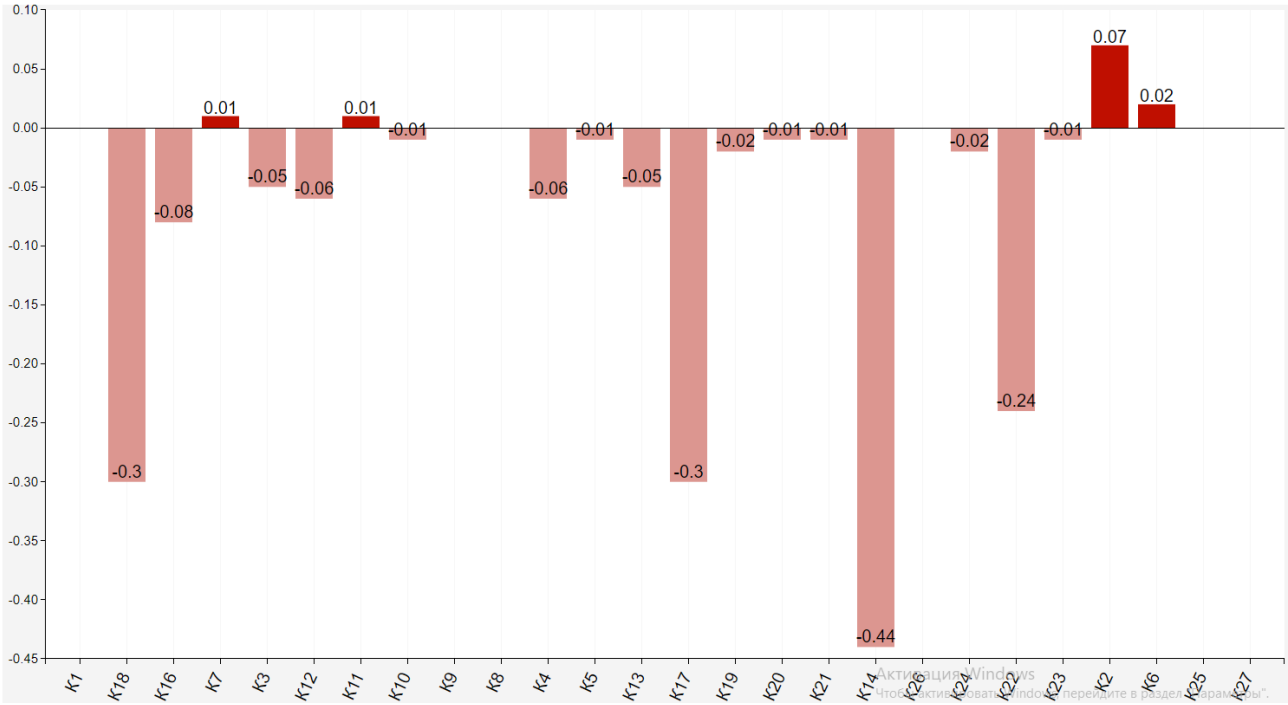


Рисунок 2.16 – Реакція досліджуваної системи при максимальному послабленні захищеності системи ЗІ

Основною метою створення системи ЗІ на об’єктах КІ є попередження та нейтралізація загроз, реалізація яких може призвести до порушення функціонування складових КІ, що, у свою чергу, може негативно вплинути на загальнодержавну, екологічну та суспільну безпеку. Дана система проводить комплексні адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські та інші заходи, спрямовані на забезпечення стійкого функціонування об’єктів КІ.

Проаналізувавши отриману стовпчасту діаграму, можна зробити висновок, що при максимальному послабленні захищеності системи ЗІ спостерігатиметься найбільша вразливість захищеності КІ, адже значення даного концепта знизиться на 0,44. При цьому безпека інформаційної інфраструктури (K_{22}) послабиться на 0,24, а безпека обслуговуючих систем та обладнання (K_{18}) і безпека центру управління (K_{17}) – на 0,3 кожна. Для попередження даної ситуації необхідно

особливу увагу приділити захищеності системи ЗІ, послаблення якої може призвести до вкрай негативних наслідків функціонування об’єктів КІ, що у результаті спровокує небезпечний вплив на навколишнє середовище та людство в цілому.

Розглянемо як зміниться захищеність КІ при максимально позитивному впливі найвагоміших концептів (рис. 2.17).

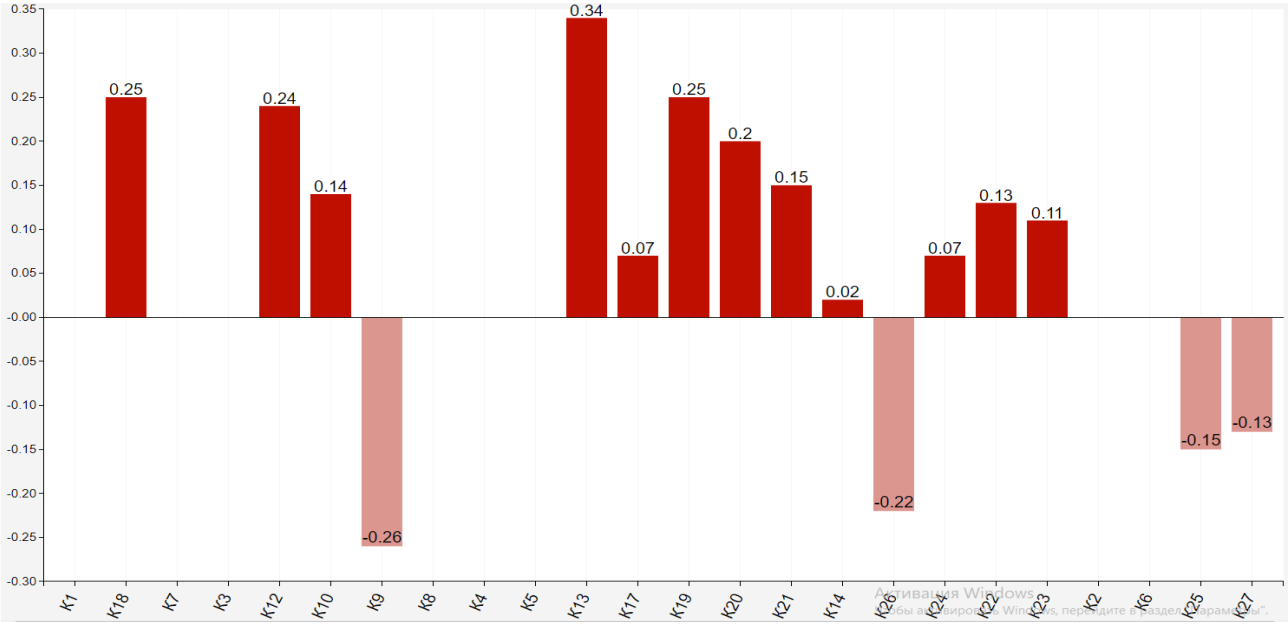


Рисунок 2.17 – Реакція досліджуваної системи при максимальному позитивному впливі найвагоміших концептів

Отримана стовбчаста діаграма показує, що при заданих умовах найбільше підвищиться надійність, відмовостійкість складових КІ (на 0,34), в однаковій мірі покращиться безпека обслуговуючого персоналу та безпека обслуговуючих систем та обладнання (на 0,25), а захищеність КІ зросте на 0,02 умовні одиниці, тобто на 2%.

Таким чином, розроблена когнітивна модель для дослідження рівня захищеності об’єкта КІ дозволяє прослідкувати відносну зміну досліджуваної системи на зміни тих чи інших концептів, визначивши найвагоміші з них. На основі результатів сценарного моделювання можна розробити чіткий план управління, спрямований на підвищення захищеності об’єктів КІ, які є стратегічно важливими для розвитку держави.

2.4 Висновки до розділу 2

У даному розділі для вирішення задачі визначення рівня захищеності систем ЗІ, що циркулює в ІС, використано когнітивний підхід, що базується на використанні НКК, яким властива простота, наочність, гнучкість, конструктивність, адаптація до невизначеності вхідних даних, використання знань і досвіду експертів предметної області.

Розроблено функціональні когнітивні моделі, які дозволяють визначити найвагоміші загрози, з точки зору вивчення даної проблеми, та проаналізувати відносну зміну рівня захищеності КМ, системи ЗІ та об’єкта КІ при впливі даних загроз.

Проведено структурно-топологічний аналіз побудованих НКК, результати якого свідчать про достатню їхню щільність, складність та демократичність, тобто запропоновані когнітивні карти є адаптивними до змін зовнішнього середовища завдяки високому рівню їх інтеграції та зв’язності.

Для кожної із запропонованих когнітивних моделей визначено концепти, які мають найвищу структурну значимість. Зокрема, для КМ такими концептами виявилися: шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі; для системи ЗІ – фізичний захист, організаційне забезпечення захисту інформації, НСД до інформації зловмисником; а для об’єкта КІ – захищеність системи ЗІ, інсайдерський вплив, захищеність КМ.

Проводено сценарне моделювання, у результаті якого при максимально позитивному впливі найвагоміших концептів визначено, що рівень захищеності КМ підвищиться на 63 %, системи ЗІ – на 19 %, а об’єкта КІ – на 2%.

Враховуючи отримані результати, можна розробити чіткий план організації підвищення рівня захищеності систем ЗІ, що циркулює в ІС, вчасно провести необхідні заходи, що допоможуть запобігти, локалізувати, усунути або ж зменшити силу впливу потенційних загроз ІБ.

РОЗДІЛ 3

ДОСЛІДЖЕННЯ ЗАПРОПОНОВАНИХ КОГНІТИВНИХ МОДЕЛЕЙ

3.1 Дослідження достовірності впливу загроз на рівень захищеності систем захисту інформації, що циркулює в інформаційних системах, визначеного на основі когнітивного підходу

У попередньому розділі дисертаційної роботи було розроблено когнітивні моделі, що дозволяють оцінити рівень захищеності КМ, системи ЗІ та об’єкта КІ. Здійснивши структурно-топологічний аналіз даних моделей, було визначено для кожної із них найвагоміші концепти. За допомогою сценарного моделювання досліджено відносну зміну рівня захищеності досліджуваних систем при впливі найвагоміших загроз. Доцільно перевірити достовірність отриманих результатів. Вирішення даної задачі можливе за допомогою методів статистичного аналізу, зокрема, за допомогою множинного регресійного аналізу, який дозволяє проаналізувати зв'язок між декількома незалежними змінними та цільовою (залежною) змінною [113].

Насамперед розглянемо модель для аналізу впливу загроз на рівень захищеності КМ. У результаті її дослідження було визначено найвагоміші концепти системи: шкідливі програми (K_3), фізичний вплив на мережу з боку зловмисника (K_4), ненавмисні дії, помилки користувачів мережі (K_7) та досліджено відносну зміну концепта захищеність КМ (K_9) за максимально негативного впливу кожної з загроз окремо. Внаслідок чого виявлено, що зі збільшенням значення концепта K_7 захищеність досліджуваної системи послабиться на 0,06; зі збільшенням концепта K_3 – на 0,05, а зі збільшенням концепта K_4 – на 0,01.

Для перевірки отриманих результатів використаємо дані, отримані в результаті моделювання десяти різних сценаріїв, що відображають відносну зміну захищеності КМ з заданими значеннями найвагоміших концептів (табл. 3.1).

Таблиця 3.1

Значення досліджуваних концептів під час моделювання $i-$го сценарію

i	K_{i3}	K_{i4}	K_{i7}	K_{i9}
1	1	1	1	-0,1
2	0,8	-0,4	1	-0,07
3	0,7	0,3	0,9	-0,06
4	0,6	0,2	0,8	-0,03
5	-0,5	0,1	0,5	0,21
6	1	0,5	-0,4	0,05
7	-0,3	0,7	0,5	0,15
8	0,4	-0,2	0,3	0,06
9	0,2	-0,8	0,9	0,03
10	-1	-1	-1	0,63

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_9 відносно K_3, K_4 та K_7) [114].

Позначимо $Y = \begin{pmatrix} -0,1 \\ -0,07 \\ -0,06 \\ -0,03 \\ 0,21 \\ 0,05 \\ 0,15 \\ 0,06 \\ 0,03 \\ 0,63 \end{pmatrix}$, $K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0.8 & -0.4 & 1 \\ 1 & 0.7 & 0.3 & 0.9 \\ 1 & 0.6 & 0.2 & 0.8 \\ 1 & -0.5 & 0.1 & 0.5 \\ 1 & 1 & 0.5 & -0.4 \\ 1 & -0.3 & 0.7 & 0.5 \\ 1 & 0.4 & -0.2 & 0.3 \\ 1 & 0.2 & -0.8 & 0.9 \\ 1 & -1 & -1 & -1 \end{pmatrix}$.

Рівняння множинної регресії матиме вигляд

$$\hat{y} = K_0' b, \tag{3.1}$$

де $\hat{y}$ – групова (умовна) середня змінної Y при заданому векторі значень $K_0' = (1 \quad K_{10} \quad K_{20} \ldots K_{p0})$; $b = (K'K)^{-1}K'Y$.

Для зручності обчислень складемо допоміжну таблицю 3.2.

Таблиця 3.2

Допоміжні проміжні дані

i	K_{i3}	K_{i4}	K_{i7}	y_i	K_{i3}^2	K_{i4}^2	K_{i7}^2	$K_{i3}K_{i4}$	$K_{i3}K_{i7}$	$K_{i4}K_{i7}$	y_iK_{i3}	y_iK_{i4}	y_iK_{i7}
1	1	1	1	-0,1	1	1	1	1	1	1	-0,1	-0,1	-0,1
2	0,8	-0,4	1	-0,07	0,64	0,16	1	-0,32	0,8	-0,4	-0,056	0,028	-0,07

Продовження таблиці 3.2

3	0,7	0,3	0,9	-0,06	0,49	0,09	0,81	0,21	0,63	0,27	-0,042	-0,018	-0,054
4	0,6	0,2	0,8	-0,03	0,36	0,04	0,64	0,12	0,48	0,16	-0,018	-0,006	-0,024
5	-0,5	0,1	0,5	0,21	0,25	0,01	0,25	-0,05	-0,25	0,05	-0,105	0,021	0,105
6	1	0,5	-0,4	0,05	1	0,25	0,16	0,5	-0,4	-0,1	0,05	0,025	-0,02
7	-0,3	0,7	0,5	0,15	0,09	0,49	0,25	-0,21	-0,15	0,35	-0,045	0,105	0,075
8	0,4	-0,2	0,3	0,06	0,16	0,04	0,09	-0,08	0,12	-0,06	0,024	-0,012	0,018
9	0,2	-0,8	0,9	0,03	0,04	0,64	0,81	-0,16	0,18	-0,72	0,006	-0,024	0,027
10	-1	-1	-1	0,63	1	1	1	1	1	1	-0,63	-0,63	-0,63
$\sum$	2,9	0,4	4,5	0,87	5,03	3,72	6,01	2,01	3,41	1,55	-0,916	-0,611	-0,673

У цьому випадку $K'K = \begin{pmatrix} i & \sum K_{i3} & \sum K_{i4} & \sum K_{i7} \\ \sum K_{i3} & \sum K_{i3}^2 & \sum K_{i3}K_{i4} & \sum K_{i3}K_{i7} \\ \sum K_{i4} & \sum K_{i3}K_{i4} & \sum K_{i4}^2 & \sum K_{i3}K_{i4} \\ \sum K_{i7} & \sum K_{i3}K_{i7} & \sum K_{i4}K_{i7} & \sum K_{i7}^2 \end{pmatrix}$, тоді

$$(K'K)^{-1} = \begin{pmatrix} 10 & 2.9 & 0.4 & 4.5 \\ 2.9 & 5.03 & 2.01 & 3.41 \\ 0.4 & 2.01 & 3.72 & 1.55 \\ 4.5 & 3.41 & 1.55 & 6.01 \end{pmatrix}^{-1} = \begin{pmatrix} 0.158 & -0.035 & 0.048 & -0.111 \\ -0.035 & 0.377 & -0.136 & -0.152 \\ 0.048 & -0.136 & 0.359 & -0.051 \\ -0.111 & -0.152 & -0.051 & 0.349 \end{pmatrix}.$$

Перемножаючи дану матрицю на вектор $K'Y = \begin{pmatrix} \sum y_i \\ \sum y_i K_{i3} \\ \sum y_i K_{i4} \\ \sum y_i K_{i7} \end{pmatrix} = \begin{pmatrix} 0.87 \\ -0.916 \\ -0.611 \\ -0.673 \end{pmatrix}$,

отримаємо:

$$b = \begin{pmatrix} 0.22 \\ -0.19 \\ -0.02 \\ -0.16 \end{pmatrix}. \qquad (3.2)$$

Враховуючи (3.1) та (3.2), складемо рівняння множинної регресії:

$$\hat{y} = 0.22 - 0.19K_3 - 0.02K_4 - 0.16K_7.$$

Оцінимо адекватність регресійної моделі за допомогою коефіцієнта детермінації (R^2), який є мірою якості рівняння регресії, характеристикою його прогностичної сили [107]: $R^2 = \dfrac{b' \cdot K'Y - n\overline{y^2}}{Y'Y - n\overline{y^2}}$.

Зазначимо, що коефіцієнт детермінації характеризує частку варіації залежної змінної, зумовленої регресією або мінливістю незалежних змінних; чим

ближче R^2 до одиниці, тим краще регресія описує залежність між незалежними змінними та залежною змінною.

Обчислимо добуток векторів:

$$b' \cdot K'Y = (0.22 \quad -0.19 \quad -0.02 \quad -0.16)\begin{pmatrix} 0.87 \\ -0.916 \\ -0.611 \\ -0.673 \end{pmatrix} = 0.485.$$

Крім того, $Y'Y = \sum_{i=1}^{10} y_i^2 = 0.4899$.

Визначимо множинний коефіцієнт детермінації:

$$R^2 = \frac{0{,}485 - 10 \cdot 0{,}087^2}{0{,}4899 - 10 \cdot 0{,}087^2} = 0{,}98.$$

Коефіцієнт детермінації $R^2 = 0{,}98$ свідчить про те, що варіація залежної змінної Y – захищеність КМ на 98% пояснюється мінливістю включених в модель незалежних змінних K_3 – шкідливі програми, K_4 – фізичний вплив на мережу з боку зловмисника та K_7 – ненавмисні дії, помилки користувачів мережі.

Для порівняння впливу кожного із найвагоміших концептів на захищеність КМ використаємо стандартизовані коефіцієнти регресії b'_j та коефіцієнти еластичності E_j $(j = 1, 2, ..., p)$ [114]:

$$b'_j = b_j \frac{s_{kj}}{s_y}, \tag{3.3}$$

де $s^2_{kj} = \frac{\sum (K_{ij} - \overline{K})^2}{i}$, $s^2_y = \frac{\sum (y_i - \overline{y})^2}{i}$.

$$E_j = b_j \frac{\overline{K}_j}{\overline{y}} \tag{3.4}$$

Стандартизований коефіцієнт регресії b'_j показує на скільки величин s_y зміниться в середньому залежна змінна Y зі збільшенням тільки $j - ї$ незалежної змінної на s_{kj}, а коефіцієнт еластичності E_j – на скільки відсотків (від середнього значення) зміниться в середньому Y зі збільшенням тільки K_j на 1%.

Використовуючи формули (3.3) та (3.4) обчислимо ці коефіцієнти:

$$b_1' = -0.19\frac{0.65}{0.04} = -3.09, \quad b_2' = -0.02\frac{0.62}{0.04} = -0.31, \quad b_3' = -0.16\frac{1.51}{0.04} = -6.08;$$

$$E_1 = -0.19\frac{0.29}{0.087} = -0.63, \quad E_2 = -0.02\frac{0.04}{0.087} = -0.008, \quad E_3 = -0.16\frac{0.45}{0.087} = -0.83.$$

Таким чином, збільшення значення концептів шкідливі програми (K_3), фізичний вплив на мережу з боку зловмисника (K_4) та ненавмисні дії, помилки користувачів мережі (K_7), на одне S_{K3} або S_{K4}, або S_{K7} послабить в середньому захищеність КМ відповідно на $3.09S_y$ або на $0.31S_y$, або на $6.08S_y$, а збільшення цих змінних на 1% (від своїх середніх значень) призведе в середньому до послаблення захищеності відповідно на 0,63%, 0,008% та 0,83%.

З аналізу значень обох показників обох випливає, що серед найвагоміших концептів досліджуваної системи ненавмисні дії, помилки користувачів мережі найбільше знижують рівень захищеності КМ, в той час як фізичний вплив на мережу з боку зловмисника послаблює захищеність мережі найменше. Це, у свою чергу, підтверджує достовірність результатів отриманих у другому розділі роботи, в наслідок проведеного сценарного моделювання.

Аналогічно проаналізуємо результати отримані в наслідок сценарного моделювання розробленої когнітивної моделі для визначення рівня захищеності системи ЗІ. Нагадаємо, що найвагомішими концептами досліджуваної системи визначено: фізичний захист (K_4), НСД до інформації зловмисником (K_5) та організаційне забезпечення ЗІ (K_6). За допомогою сценарного моделювання встановлено, що при максимально негативному впливі кожного з цих концептів захищеність системи ЗІ (K_{11}) відповідно погіршиться на 0,26; 0,23 та 0,07.

Порівняємо вплив найвагоміших концептів на захищеність досліджуваної системи за допомогою регресійного аналізу. Для досягнення поставленої мети змоделюємо десять різних сценаріїв, що відображають відносну зміну захищеності системи ЗІ при заданих значеннях обраних концептів (табл. 3.3).

Таблиця 3.3

Значення досліджуваних концептів під час моделювання $i-$го сценарію

i	K_{i4}	K_{i5}	K_{i6}	K_{i11}
1	1	1	1	0,08
2	0,9	-0,1	0,7	0,13
3	-0,1	-0,3	-0,1	-0,08
4	1	-0,2	1	0,16
5	-0,2	0,3	0,9	-0,04
6	0,8	0,2	-0,3	-0,01
7	1	-0,1	-0,2	0,06
8	-0,3	-0,5	0,8	0,01
9	0,7	0,8	0,9	0,05
10	0,5	-0,3	-0,1	0,02

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{11} відносно K_4, K_5 та K_6).

Позначимо $Y = \begin{pmatrix} 0.08 \\ 0.13 \\ -0.08 \\ 0.16 \\ -0.04 \\ -0.01 \\ 0.06 \\ 0.01 \\ 0.05 \\ 0.02 \end{pmatrix}$, $K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0.9 & -0.1 & 0.7 \\ 1 & -0.1 & -0.3 & -0.1 \\ 1 & 1 & -0.2 & 1 \\ 1 & -0.2 & 0.3 & 0.9 \\ 1 & 0.8 & 0.2 & -0.3 \\ 1 & 1 & -0.1 & -0.2 \\ 1 & -0.3 & -0.5 & 0.8 \\ 1 & 0.7 & 0.8 & 0.9 \\ 1 & 0.5 & -0.3 & -0.1 \end{pmatrix}$.

Для зручності обчислень складемо допоміжну таблицю 3.4.

Таблиця 3.4

Додаткові проміжні дані

i	K_{i4}	K_{i5}	K_{i6}	y_i	K_{i4}^2	K_{i5}^2	K_{i6}^2	$K_{i4}K_{i5}$	$K_{i4}K_{i6}$	$K_{i5}K_{i6}$	y_iK_{i4}	y_iK_{i5}	y_iK_{i6}
1	1	1	1	0,08	1	1	1	1	1	1	0,08	0,08	0,08
2	0,9	-0,1	0,7	0,13	0,81	0,01	0,49	-0,09	0,63	-0,07	0,117	-0,013	0,091
3	-0,1	-0,3	-0,1	-0,08	0,01	0,09	0,01	0,03	0,01	0,03	0,008	0,024	0,008
4	1	-0,2	1	0,16	1	0,04	1	-0,2	1	-0,2	0,16	-0,032	0,16
5	-0,2	0,3	0,9	-0,04	0,04	0,09	0,81	-0,06	-0,18	0,27	0,008	-0,012	-0,036
6	0,8	0,2	-0,3	-0,01	0,64	0,04	0,09	0,16	-0,24	-0,06	-0,008	-0,002	0,003
7	1	-0,1	-0,2	0,06	1	0,01	0,04	-0,1	-0,2	0,02	0,06	-0,006	-0,012
8	-0,3	-0,5	0,8	0,01	0,09	0,25	0,64	0,15	-0,24	-0,4	-0,003	-0,005	0,008
9	0,7	0,8	0,9	0,05	0,49	0,64	0,81	0,56	0,63	0,72	0,035	0,04	0,045
10	0,5	-0,3	-0,1	0,02	0,25	0,09	0,01	-0,15	-0,05	0,03	0,01	-0,006	-0,002
$\sum$	5,3	0,8	4,6	0,38	5,33	2,26	4,9	1,3	2,36	1,34	0,47	0,07	0,345

Враховуючи дані таблиці 3.4, знайдемо $(K'K)^{-1}$:

$$(K'K)^{-1} = \begin{pmatrix} 10 & 5.3 & 0.8 & 4.6 \\ 5.3 & 5.33 & 1.3 & 2.36 \\ 0.8 & 1.3 & 2.26 & 1.34 \\ 4.6 & 2.36 & 1.34 & 4.9 \end{pmatrix}^{-1} = \begin{pmatrix} 0.34 & -0.28 & 0.18 & -0.24 \\ -0.28 & 0.48 & -0.23 & 0.095 \\ 0.18 & -0.23 & 0.65 & -0.23 \\ -0.24 & 0{,}095 & -0.23 & 0.44 \end{pmatrix}.$$

Перемножаючи дану матрицю на вектор $K'Y = \begin{pmatrix} 0.38 \\ 0.47 \\ 0.07 \\ 0.345 \end{pmatrix}$, отримаємо $b = \begin{pmatrix} -0.07 \\ 0.14 \\ -0.08 \\ 0.092 \end{pmatrix}$.

Таким чином, рівняння множинної регресії матиме вигляд

$$\hat{y} = -0.07 + 0.14K_4 - 0.08K_5 + 0.092K_6.$$

Розрахуємо стандартизовані коефіцієнти регресії b'_j (3.3) та коефіцієнти еластичності E_j (3.4):

$$b'_1 = 0.14\frac{0.5}{0.07} = 1, \quad b'_2 = -0.08\frac{0.47}{0.07} = -0.54, \quad b'_3 = 0.092\frac{0.53}{0.07} = 0.7;$$

$$E_1 = 0.14\frac{0.53}{0.038} = 1.95, \quad E_2 = -0.08\frac{0.08}{0.038} = -0.17, \quad E_3 = 0.092\frac{0.46}{0.038} = 1.11.$$

Отже, збільшення значення концептів фізичний захист (K_4) та організаційне забезпечення ЗІ (K_6), на одне S_{K4}, або S_{K6} посилить в середньому захищеність системи ЗІ відповідно на S_y або на $0.7S_y$, а збільшення цих змінних на 1% (від своїх середніх значень) призведе в середньому до підвищення рівня захищеності відповідно на 1,95% та 1,11 %. Водночас збільшення значення концепта НСД до інформації зловмисником (K_5) на S_{K5} призведе до послаблення захищеності в середньому на $0.54S_y$, а збільшення даного концепта на 1% (від своїх середніх значень) призведе в середньому до зниження рівня захищеності системи ЗІ на 0,17%.

Таким чином, концепт фізичний захист (K_4) чинить більший вплив на захищеність системи ЗІ, ніж концепт організаційне забезпечення ЗІ (K_6), а концепт НСД до інформації зловмисником (K_5) має найменший вплив серед усіх найвагоміших концептів. Це, у свою чергу, підтверджує результати отримані у

другому розділі роботи, внаслідок проведеного сценарного моделювання.

Подібним чином проаналізуємо результати отримані внаслідок дослідження когнітивної моделі для визначення рівня захищеності об'єкта КІ. У цьому випадку найвагомішими концептами було визначено: інсайдерський вплив (K_{11}), захищеність системи ЗІ (K_{15}) та захищеність КМ (K_{16}). Відзначимо, що при максимально негативному впливі кожного з цих концептів захищеність об'єкта КІ (K_{14}) погіршиться на 0,03; 0,44 та 0,06 відповідно.

З метою проведення даного дослідження змоделюємо десять різних сценаріїв, що відображають відносну зміну захищеності об'єкта КІ при заданих значеннях найвагоміших концептів (табл. 3.5).

Таблиця 3.5

Значення досліджуваних концептів під час моделювання i – го сценарію

i	K_{i11}	K_{i15}	K_{i16}	K_{i14}
1	-1	1	1	0,02
2	-0,5	-0,7	0,8	-0,31
3	1	0,6	-0,9	-0,11
4	-0,2	-0,9	-0,7	-0,41
5	-0,1	-0,6	-0,2	-0,32
6	-0,9	-1	-1	-0,41
7	0,4	0,3	0,1	-0,11
8	0,6	-0,5	-0,1	-0,36
9	-0,8	-0,4	-0,9	-0,26
10	0,3	-0,8	-0,9	-0,44

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{14} відносно K_{11}, K_{15} та K_{16}).

Позначимо $Y = \begin{pmatrix} 0.02 \\ -0.31 \\ -0.11 \\ -0.41 \\ -0.32 \\ -0.41 \\ -0.11 \\ -0.36 \\ -0.26 \\ -0.44 \end{pmatrix}$, $K = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & -0.5 & -0.7 & 0.8 \\ 1 & 1 & 0.6 & -0.9 \\ 1 & -0,2 & -0.9 & -0,7 \\ 1 & -0.1 & -0.6 & -0.2 \\ 1 & -0.9 & -1 & -1 \\ 1 & 0.4 & 0.3 & 0.1 \\ 1 & 0.6 & -0.5 & -0.1 \\ 1 & -0.8 & -0.4 & -0.9 \\ 1 & 0.3 & -0.8 & -0.9 \end{pmatrix}$.

Для зручності обчислень складемо допоміжну таблицю 3.6.

Таблиця 3.6

Додаткові проміжні дані

i	K_{i11}	K_{i15}	K_{i16}	y_i	K_{i11}^2	K_{i15}^2	K_{i16}^2	$K_{i11}K_{i15}$	$K_{i11}K_{i16}$	$K_{i15}K_{i16}$	y_iK_{i11}	y_iK_{i15}	y_iK_{i16}
1	-1	1	1	0,02	1	1	1	-1	-1	1	-0,02	0,02	0,02
2	-0,5	-0,7	0,8	-0,31	0,25	0,49	0,64	0,35	-0,4	-0,56	0,155	0,217	-0,248
3	1	0,6	-0,9	-0,11	1	0,36	0,81	0,6	-0,9	-0,54	-0,09	-0,054	0,099
4	-0,2	-0,9	-0,7	-0,41	0,04	0,81	0,49	0,18	0,14	0,63	0,08	0,36	0,287
5	-0,1	-0,6	-0,2	-0,32	0,01	0,36	0,04	0,06	0,02	0,12	0,032	0,192	0,064
6	-0,9	-1	-1	-0,41	0,81	1	1	0,9	0,9	1	0,369	0,41	0,41
7	0,4	0,3	0,1	-0,11	0,16	0,09	0,01	0,12	0,04	0,03	-0,044	-0,033	-0,011
8	0,6	-0,5	-0,1	-0,36	0,36	0,25	0,01	-0,3	-0,06	0,05	-0,216	0,18	0,036
9	-0,8	-0,4	-0,9	-0,26	0,64	0,16	0,81	0,32	0,72	0,36	0,208	0,104	0,234
10	0,3	-0,8	-0,9	-0,44	0,09	0,64	0,81	-0,24	-0,27	0,72	-0,132	0,352	0,396
$\sum$	-1,2	-3	-2,8	-2,71	4,36	5,16	5,62	0,99	-0,81	2,81	0,342	1,748	1,287

Таким чином, отримаємо обернену матрицю:

$$(K'K)^{-1} = \begin{pmatrix} 10 & -1.2 & -3 & -2.8 \\ -1.2 & 4.36 & 0.99 & -0.81 \\ -3 & 0.99 & 5.16 & 2.81 \\ -2.8 & -0.81 & 2.81 & 5.62 \end{pmatrix}^{-1} = \begin{pmatrix} 0.13 & 0.035 & 0.043 & 0.049 \\ 0.035 & 0.28 & -0.088 & 0.1 \\ 0.043 & -0.088 & 0.32 & -0.15 \\ 0.049 & 0,1 & -0.15 & 0.29 \end{pmatrix}.$$

Перемножаючи дану матрицю на вектор $K'Y = \begin{pmatrix} -2.71 \\ 0.342 \\ 1.748 \\ 1.287 \end{pmatrix}$, матимемо $b = \begin{pmatrix} -0.2 \\ -0.024 \\ 0.22 \\ 0.016 \end{pmatrix}$

Отже, складемо рівняння множинної регресії:

$$\hat{y} = -0.2 - 0.024K_{11} + 0.22K_{15} + 0.016K_{16}.$$

Розрахуємо стандартизовані коефіцієнти регресії b'_j (3.3) та коефіцієнти

еластичності E_j (3.4):

$$b_1' = -0.024\frac{0.65}{0.14} = -0{,}11, \quad b_2' = 0.22\frac{0.65}{0.14} = 1.02, \quad b_3' = 0.016\frac{0.69}{0.14} = 0.08;$$

$$E_1 = -0.024\frac{-0.12}{-0.271} = -0.01, \quad E_2 = 0.22\frac{-0.3}{-0.271} = 0.24, \quad E_3 = 0.016\frac{-0.28}{-0.271} = 0.017.$$

Аналіз розрахованих коефіцієнтів показав, що збільшення значень концептів захищеність системи ЗІ (K_{15}) та захищеність КМ (K_{16}), на одне S_{K15}, або S_{K16} посилить в середньому захищеність об'єкта КІ відповідно на $1.02S_y$ або на $0.08S_y$, а збільшення цих змінних на 1% (від своїх середніх значень) призведе в середньому до підвищення рівня захищеності відповідно на 0,24% та 0,017 %. Водночас збільшення інсайдерського впливу (K_{11}) на S_{K11} призведе до послаблення захищеності в середньому на $0.11S_y$, а збільшення даного концепта на 1% (від своїх середніх значень) призведе в середньому до зниження рівня захищеності об'єкта КІ на 0,01%. Отримані дані підтверджують достовірність результатів одержаних за сценарним моделюванням у другому розділі роботи.

Таким чином, на основі множинного регресійного аналізу було доведено достовірність впливу загроз на рівень захищеності систем ЗІ, що циркулює в ІС, визначеного на основі когнітивного підходу.

3.2 Симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта критичної інфраструктури

У другому розділі роботи було запропоновано когнітивну модель для дослідження захищеності об'єкта КІ. Проведений структурний аналіз розробленої моделі дозволив визначити найвагоміші її концепти. Актуальними залишаються питання дослідження достовірності отриманих результатів, а також виявлення зв'язних концептів системи та суттєвих зв'язків між ними. Тому, слід звернути увагу на симпліціальний аналіз [115], який дозволяє вирішити вказані актуальні питання.

Здійснимо симпліціальний аналіз [115] структури розробленої нечіткої когнітивної моделі для дослідження захищеності об'єкта КІ.

У загальному випадку НКК можна представити у вигляді множини пар вершин, які пов'язані деяким відношенням λ, що породжує множину багатовимірних зв'язків між вершинами.

Під симплексом $\sigma_q^{v_i}$ розуміють множину елементів, яка співвідносить конкретному елементу v_i відношення λ розмірності q, а їх сукупність утворює симпліціальний комплекс $K_y(X;\lambda)$ за рядками (вершини кодуються як X) або $K_x(Y;\lambda^*)$ за стовпцями (вершини кодуються як Y). При цьому задача вивчення структури зв'язності комплексу K зводиться до побудови q-еквівалентності. Для кожного значення розмірності $q = 0, 1, 2, ..., \dim K$ ($\dim K$ – максимальна розмірність комплексу) можна визначити число різних класів еквівалентності Q_q. Дана операція називається q-аналізом симпліціального комплексу K, а вектор $Q = \{Q_{\dim K}, ..., Q_1, Q_0\}$ – першим структурним вектором комплексу, що дозволяє встановити зв'язність комплексів на усіх рівнях q [116].

Побудуємо і проаналізуємо симпліціальний комплекс, який відповідає НКК для дослідження захищеності об'єкта КІ.

Здійснимо перехід від нечітких значень матриці суміжності між концептами досліджуваної когнітивної моделі до значень «–1», «0», «1» таким чином:

– якщо значення сили зв'язку між концептами належить інтервалу [-1; 0), то присвоюємо значення «-1»;

– якщо значення сили зв'язку між концептами належить інтервалу [0; 0,5), то присвоюємо значення «0»;

– якщо значення сили зв'язку між концептами належить інтервалу [0,5; 1], то присвоюємо значення «1».

В отриманій матриці переходу підрахуємо одиниці у кожному i–тому рядку для обчислення розмірності симплексів комплексу $K_x(Y;\lambda)$:

$$q = q^{(v_i)} = \sum_{j=1}^{m} \lambda_{ij} - 1.$$

Впорядкувавши i–ті рядки зверху вниз за правилом: $q_1^{(v_i)} \succ q_2^{(v_i)} \succ q_3^{(v_i)} \succ ... \succ 0 \succ -1$ отримаємо матрицю (табл. 3.7-3.8).

Таблиця 3.7

Матриця переходу (зв'язок концептів K_i із концептами $K_1 - K_{15}$)

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
K_{11}	0	0	0	0	0	0	0	0	1	-1	0	-1	-1	0	-1
K_3	0	-1	0	1	1	-1	-1	0	0	1	-1	0	0	0	0
K_5	0	-1	0	1	0	-1	-1	0	0	1	-1	0	0	0	0
K_7	0	0	-1	-1	0	0	0	0	1	0	0	-1	-1	0	0
K_1	0	1	0	-1	0	0	0	0	0	0	0	-1	-1	0	0
K_6	0	0	-1	-1	0	0	0	0	0	0	0	-1	-1	0	0
K_{10}	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1
K_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
K_2	0	0	0	-1	0	0	0	0	0	0	0	-1	-1	0	0
K_4	0	-1	0	0	0	-1	-1	0	0	0	-1	0	0	0	0
K_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
K_{18}	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
K_{25}	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{16}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{26}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_8	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
K_{21}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{14}	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
K_{20}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{22}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
K_{23}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{24}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0

Таблиця 3.8

Матриця переходу (зв'язок концептів K_i із концептами $K_{16} - K_{27}$)

	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}	$q^{(v_i)}$
K_{11}	-1	-1	-1	-1	-1	-1	-1	0	0	0	0	0	**11**
K_3	0	0	0	0	0	0	0	0	0	0	0	0	**6**

Продовження таблиці 3.8

	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}	$q^{(\nu_i)}$
K_5	0	0	0	0	0	0	0	0	0	0	0	0	**5**
K_7	0	0	0	-1	0	0	0	0	0	0	0	0	**5**
K_1	0	0	0	-1	0	0	0	0	0	0	0	0	**4**
K_6	0	0	0	-1	0	0	0	0	0	0	0	0	**4**
K_{10}	0	1	1	1	0	0	0	0	0	0	0	0	**4**
K_{13}	1	1	1	1	0	0	0	0	0	0	0	0	**4**
K_2	0	0	0	-1	0	0	0	0	0	0	0	0	**3**
K_4	0	0	0	0	0	0	0	0	0	0	0	0	**3**
K_{15}	0	1	1	0	0	0	1	0	0	0	0	0	**3**
K_{18}	1	1	0	0	0	0	0	0	0	0	0	0	**3**
K_{25}	-1	0	0	0	0	0	0	-1	0	0	1	0	**3**
K_9	0	0	0	0	0	0	0	0	0	1	1	1	**2**
K_{16}	0	1	0	0	0	0	1	0	1	0	0	0	**2**
K_{26}	-1	0	-1	0	0	0	0	-1	0	0	0	0	**2**
K_8	0	0	0	0	0	0	0	0	0	0	0	0	**1**
K_{21}	0	0	0	0	0	0	1	1	0	0	0	0	**1**
K_{12}	0	1	0	0	0	0	0	0	0	0	0	0	**0**
K_{14}	0	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{20}	0	0	0	0	0	0	1	0	0	0	0	0	**0**
K_{22}	0	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{23}	1	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{24}	1	0	0	0	0	0	0	0	0	0	0	0	**0**
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0	**0**

Побудуємо симпліціальний комплекс $K_x(Y;\lambda)=\left\{\sigma_q^{(\nu_i)}\right\}$, що являє собою послідовність симплексів, які впорядковані за правилом спадання їх розмірності:

$$K_x(Y;\lambda)=\begin{Bmatrix}\sigma_{11}^{(11)};\sigma_6^{(3)};\sigma_5^{(5)};\sigma_5^{(7)};\sigma_4^{(1)};\sigma_4^{(6)};\sigma_4^{(10)};\sigma_4^{(13)};\sigma_3^{(2)};\sigma_3^{(4)};\sigma_3^{(15)};\sigma_3^{(18)};\sigma_3^{(25)};\sigma_2^{(9)};\\ \sigma_2^{(16)};\sigma_2^{(26)};\sigma_1^{(8)};\sigma_1^{(21)};\sigma_0^{(12)};\sigma_0^{(14)};\sigma_0^{(17)};\sigma_0^{(19)};\sigma_0^{(20)};\sigma_0^{(22)};\sigma_0^{(23)};\sigma_0^{(24)};\sigma_0^{(27)}\end{Bmatrix}.$$

З матриці переходу визначимо перший структурний вектор $Q_x=\left\{Q_{\dim K},...,Q_1,Q_0\right\}$ комплексу $K_x(Y;\lambda)$ наступним чином: для кожної розмірності $q^{(\nu_i)}$ кількість симплексів у кожному класі еквівалентності Q_q визначається

правилом: якщо хоча б одна вершина симплексу не входить в попередній симплекс більшої розмірності, то це окремий клас.

Значення зв'язності для $K_x(Y;\lambda)$:

$q=11,\quad Q_{11}=1,\quad \{K_{11}\};$

$q=6,\quad Q_6=2,\quad \{K_{11}\},\{K_3\};$

$q=5,\quad Q_5=3,\quad \{K_{11}\},\{K_3,K_5\},\{K_7\};$

$q=4,\quad Q_4=5,\quad \{K_{11},K_{13}\},\{K_3,K_5\},\{K_7,K_6\},\{K_1\},\{K_{10}\};$

$q=3,\quad Q_3=7,\quad \{K_{11},K_{13},K_{18}\},\{K_3,K_5,K_4\},\{K_7,K_6,K_2\},\{K_1\},\{K_{10}\},\{K_{15}\},\{K_{25}\};$

$q=2,\quad Q_2=10,\quad \{K_{11},K_{13},K_{18}\},\{K_3,K_5,K_4\},\{K_7,K_6,K_2\},\{K_1\},\{K_{10}\},\{K_{15}\},\{K_{25}\},\{K_9\},$
$\{K_{16}\},\{K_{26}\};$

$q=1,\quad Q_1=12,\quad \{K_{11},K_{13},K_{18}\},\{K_3,K_5,K_4\},\{K_7,K_6,K_2\},\{K_1\},\{K_{10}\},\{K_{15}\},\{K_{25}\},\{K_9\},\{K_{16}\},$
$\{K_{26}\},\{K_8\},\{K_{21}\};$

$q=0,\quad Q_0=1,\quad \{yci\ K_i\ (i=1,...27)\}.$

Структурний вектор комплексу $K_x(Y;\lambda)$ дорівнює: $Q_x=\{1\,2\,3\,5\,7\,10\,12\,1\}$.

Відмітимо, що на рівні $q=3$ з'явилися зв'язні концепти $\{K_{11},K_{13},K_{18}\},\{K_3,K_5,K_4\},\{K_7,K_6,K_2\}$ досліджуваної когнітивної карти. Це означає, що:

– вносячи управлінський вплив у концепт K_{11} (інсайдерський вплив), концепти K_{13} (надійність, відмовостійкість складових КІ) та K_{18} (безпека обслуговуючих систем та обладнання) відреагують на даний вплив;

– вносячи управлінський вплив у концепт K_3 (соціально-політичний вплив), спостерігатиметься реакція концептів K_5 (правовий вплив) та K_4 (економічний вплив);

– вносячи управлінський вплив у концепт K_7 (терористичний вплив), концепти K_6 (військове вторгнення) та K_2 (техногенний вплив) відреагують на нього.

Концепти K_1 (природні явища), K_9 (хакерський вплив), K_{10} (вплив управлінських рішень та організаційний заходів), K_{15} (захищеність системи ЗІ), K_{16} (захищеність КМ), K_{25} (мережеві атаки) та K_{26} (шкідливі програми), яким

відповідає симплекс найбільшої розмірності, можуть бути вибрані в якості управляючих концептів для всієї системи. Проте зазначимо, що концепт K_1 (природні явища) потрібно виключити з даного переліку, оскільки людина не має жодного впливу на силу його дії, тобто не може керувати ним.

Відмітимо, що у другому розділі роботи внаслідок структурно-топологічного аналізу серед найвпливовіших концептів були K_{15} (захищеність системи ЗІ) та K_{16} (захищеність КМ), які у результаті проведення симпліціального аналізу увійшли в множину управляючих. Це підтверджує достовірність отриманих результатів, які є корисними для прийняття управлінських рішень, що пов'язані зі зміцненням безпечного функціонування об'єкта КІ, швидкій адаптації до умов, що постійно змінюються, протистоянні впливу загроз, що враховуються в досліджуваній НКК.

3.3 Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації і об'єкта критичної інфраструктури та допустимої інтенсивності зниження рівня їхньої захищеності

Стрімким розвитком ІТ та впровадженням їх в усі сфери суспільного життя обумовлюється надзвичайна важливість створення надійних систем ЗІ. Проблема якісного функціонування даних систем, з огляду на появу нових та зростання рівня існуючих загроз в інформаційному просторі, набуває все більшої значущості. Причому важливою практичною проблемою є встановлення оптимального балансу між забезпеченням захищеності системи ЗІ та обсягом витрат на її підтримку, враховуючи раціональний розподіл між окремими напрямами захисту.

Окремо слід зазначити, що на початкових етапах створення дієвої системи захисту об'єктів КІ виникає необхідність визначення кількісної характеристики вагомості потенційних загроз, реалізація яких призведе до порушення функціонування досліджуваних об'єктів та проявлятиметься у вигляді припинення надання життєво необхідних послуг й товарів населенню як окремих міст, так і усієї держави в цілому. Це, в свою чергу, може спричинити соціально-політичну та економічну нестабільність, загострення конфліктів різного

характеру. При цьому основними джерелами загроз може бути високий рівень зношеності та аварійність основних фондів, вплив небезпечних природних явищ, напружена воєнно-політична та економічна ситуація у країні тощо.

У переважній більшості вищезазначені питання вирішуються за допомогою методів статистичного аналізу, які потребують розгляду значного обсягу інформації, складних розрахунків та займають тривалий час для опрацювання.

Одним з варіантів вирішення цієї проблеми може бути ранжування загроз, що дозволить визначити допустиму інтенсивність зниження досліджуваних систем та встановити пропорційне співвідношення допустимих витрат на забезпечення їхньої захищеності.

Багато вітчизняних та зарубіжних вчених у своїх працях приділили достатньо уваги вирішенню даного питання. Зокрема, у роботі [117] пропонується метод нестрогого ранжування. Відповідно до цього методу експерт виробляє нумерацію усіх критеріїв за спаданням ступеня прийнятності негативних наслідків, пов’язаних з даним критерієм безпеки. Потім проранжовані критерії послідовно нумеруються. Оцінка (ранг) критерію визначається його номером.

А. Г. Кащенко у своїй роботі [118] проводить ранжування інформаційних ризиків на основі нечіткої логіки, використовуючи алгоритм Мамдані, який одним з перших знайшов застосування у системах нечіткого виведення.

Крім того, існує безліч робіт, що стосуються ранжування елементів у інших сферах діяльності. Так, О. П. Ротштейн пропонує метод ранжування факторів, що впливають на надійність системи на основі теорії НКК [119]. За основу методу взято формалізацію причинно-наслідкових зв’язків у вигляді НКК, тобто орієнтованого графа, вершини якого відповідають надійності системи і факторам, що впливають на неї, а зважені дуги відображають сили впливів факторів один на одного і на надійність системи. Ранг фактора визначено як аналог індексу важливості елементу по Бірнбауму.

Звернемо увагу на ще одну роботу цього вченого [120], у якій він пропонує метод ранжування елементів багатофункціональної системи на основі нечіткої математики. Задача зводиться до автоматичної класифікації з використанням

транзитивного замикання нечіткого відношення схожості. Початкова інформація про систему задається у вигляді нечіткого відношення впливу відмов елементів на виконання функції. Ступені впливу елементів на функції системи обчислюються шляхом порівняння з найменшим впливом за шкалою Сааті.

Таким чином, для досягнення поставленої мети здійснимо ранжування загроз системи ЗІ та об’єкта КІ.

Насамперед, розглянемо систему ЗІ із загальними характеристиками.

Зазначимо, що загрози ІБ – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері [121].

Аналізуючи концепти когнітивної моделі для визначення рівня захищеності системи ЗІ (розробленої у другому розділі роботи), сформуємо множину найвагоміших загроз з точки зору вивчення даної проблеми:

– K_1 – захист від витоку технічними каналами;
– K_2 – захист каналу передавання інформації;
– K_3 – розголошення інформації персоналом;
– K_4 – фізичний захист;
– K_5 – НСД до інформації зловмисником;
– K_6 – організаційне забезпечення ЗІ;
– K_7 – ненавмисні дії, помилки обслуговуючого персоналу;
– K_8 – надійність, відмовостійкість технічних та програмних засобів;
– K_9 – нормативно-правове забезпечення захисту;
– K_{10} – природні явища та явища техногенного характеру.

Загрози ІБ призводять до не виконання таких критеріїв як [35]:

– C_1 – доступність – можливість за прийнятний час одержати необхідну інформаційну послугу;
– C_2 – цілісність – захищеність від руйнування та несанкціонованої зміни;
– C_3 – конфіденційність – властивість інформації бути недоступною і закритою для неавторизованого користувача, логічного об’єкта або процесу.

– C_4 – достовірність – захист від фальсифікації, підробки та шахрайства.

Далі здійснимо ранжування загроз системі ЗІ згідно методу ранжування представленого у [120].

Вплив загрози K_i, що призводить до не виконання критерію C_j задамо нечіткою множиною: $I_i = \left\{ \frac{\mu_{i1}}{C_1}, \frac{\mu_{i2}}{C_2}, ..., \frac{\mu_{im}}{C_m} \right\}$,

де μ_{ij} – число з інтервалу $[0,1]$, яке характеризує ступінь впливу загроз K_i на не виконання критерію C_j.

За допомогою методу найменшого впливу [122] визначимо число μ_{ij} , яке ставиться у відповідність кожній парі елементів (K_i, C_j) (табл. 3.9).

Таблиця 3.9

Початкові дані для методу найменшого впливу

K_i	C_l	f_{ij} / f_{il}			
		C_1	C_2	C_3	C_4
K_1	C_1	$\frac{11}{11}=1$	$\frac{12}{11}=7$	$\frac{13}{11}=9$	$\frac{14}{11}=5$
K_2	C_1	$\frac{21}{21}=1$	$\frac{22}{21}=7$	$\frac{23}{21}=5$	$\frac{24}{21}=5$
K_3	C_1	$\frac{31}{31}=1$	$\frac{32}{31}=6$	$\frac{33}{31}=9$	$\frac{34}{31}=7$
K_4	C_3	$\frac{41}{43}=9$	$\frac{42}{43}=4$	$\frac{43}{43}=1$	$\frac{44}{43}=5$
K_5	C_1	$\frac{51}{51}=1$	$\frac{52}{51}=7$	$\frac{53}{51}=9$	$\frac{54}{51}=7$
K_6	C_1	$\frac{61}{61}=1$	$\frac{62}{61}=6$	$\frac{63}{61}=7$	$\frac{64}{61}=6$
K_7	C_4	$\frac{71}{74}=7$	$\frac{72}{74}=5$	$\frac{73}{74}=3$	$\frac{74}{74}=1$
K_8	C_4	$\frac{81}{84}=9$	$\frac{82}{84}=5$	$\frac{83}{84}=6$	$\frac{84}{84}=1$
K_9	C_1	$\frac{91}{91}=1$	$\frac{92}{91}=5$	$\frac{93}{91}=6$	$\frac{94}{91}=5$
K_{10}	C_3	$\frac{101}{103}=9$	$\frac{102}{103}=3$	$\frac{103}{103}=1$	$\frac{104}{103}=1$

Зазначимо, що C_l містить усі критерії, на які загрози K_i мають найменший вплив, а f_{ij} / f_{il} – експертні порівняння сил впливу f_{ij} з найменшими силами впливу f_{il}.

Розрахуємо найменший ступінь впливу загрози K_i у системі ЗІ, використовуючи формулу:

$$\mu_{il} = \left(\frac{f_{i1}}{f_{il}} + \frac{f_{i2}}{f_{il}} + ... + \frac{f_{im}}{f_{il}} \right)^{-1}.$$

На основі даного значення обчислимо ступені впливу, що відповідають кожній парі (K_i, C_j):

$$\mu_{i1} = \mu_{il} \frac{f_{i1}}{f_{il}}, \quad \mu_{i2} = \mu_{il} \frac{f_{i2}}{f_{il}}, ..., \quad \mu_{im} = \mu_{il} \frac{f_{im}}{f_{il}}.$$

Отримані ступені впливу утворюють нечітке відношення впливу:

I=

1/22	7/22	9/22	5/22
1/18	7/18	5/18	5/18
1/23	6/23	9/23	7/23
9/19	4/19	1/19	5/19
1/24	7/24	9/24	7/24
1/20	6/20	7/20	6/20
7/16	5/16	3/16	1/16
9/21	5/21	6/21	1/21
1/17	5/17	6/17	5/17
9/14	3/14	1/14	1/14

(3.5)

Для нормалізації відношення (3.5) поділимо елементи кожного рядка на максимальне значення, яке є у відповідному рядку та отримаємо:

I=

0,11	0,78	1,0	0,56
0,14	1,0	0,71	0,71
0,11	0,67	1,0	0,77
1,0	0,44	0,11	0,56
0,11	0,78	1,0	0,78
0,14	0,86	1,0	0,86
1,0	0,71	0,43	0,14
1,0	0,56	0,67	0,11
0,17	0,83	1,0	0,83
1,0	0,33	0,11	0,11

(3.6)

Сформуємо нечітке відношення схожості, яке складається із сукупності

величин мір схожості (r_{ij}):

$$R = \left| r_{ij} /(K_i, K_j \right|,$$

Причому, $r_{ij} = 1 - d_{ij}$, де d_{ij} – відстань між нечіткими множинами впливу загроз K_i та K_j:

$$I_i = \left\{ \frac{\mu_{i1}}{K_1}, \frac{\mu_{i2}}{K_2}, ..., \frac{\mu_{im}}{K_m} \right\},$$

$$I_j = \left\{ \frac{\mu_{j1}}{K_1}, \frac{\mu_{j2}}{K_2}, ..., \frac{\mu_{jm}}{K_m} \right\}$$

Зазначимо, що для обчислення d_{ij} можна використовувати відносні відстані Хеммінга ($d_{ij}^{(h)}$) або Евкліда ($d_{ij}^{(e)}$):

$$d_{ij}^{(h)} = \frac{1}{n} \sum_{k=1}^{n} \left| \mu_{ik} - \mu_{jk} \right|,$$

$$d_{ij}^{(e)} = \frac{1}{n} \sqrt{\sum_{k=1}^{n} (\mu_{ik} - \mu_{jk})^2}.$$

Таким чином, провівши усі вищезазначені розрахунки, отримаємо нечітке відношення схожості для досліджуваної предметної області:

R=

1,0	0,83	0,92	0,47	0,94	0,9	0,51	0,53	0,9	0,33
0,83	1,0	0,8	0,46	0,39	0,86	0,5	0,5	0,86	0,32
0,92	0,8	1,0	0,44	0,96	0,92	0,46	0,5	0,93	0,3
0,47	0,46	0,44	1,0	0,41	0,38	0,75	0,72	0,4	0,86
0,94	0,39	0,96	0,41	1,0	0,95	0,46	0,47	0,96	0,28
0,9	0,86	0,92	0,38	0,95	1,0	0,42	0,44	0,98	0,24
0,51	0,5	0,46	0,75	0,46	0,42	1,0	0,89	0,45	0,8
0,53	0,5	0,5	0,72	0,47	0,44	0,89	1,0	0,46	0,8
0,9	0,86	0,93	0,4	0,96	0,98	0,45	0,46	1,0	0,26
0,33	0,32	0,3	0,86	0,28	0,24	0,8	0,8	0,26	1,0

(3.7)

Щоб розбити множину загроз на класи, що не перетинаються та містять елементи подібні за ступенем впливу, необхідно надати початковому не транзитивному відношенню схожості R властивість транзитивності. Таке перетворення забезпечує операція транзитивного замикання нечіткого відношення [123].

Для отримання транзитивного замикання відношення схожості скористаємося авторською програмою, лістинг якої наведено у додатку А.

У результаті із відношення (3.7), знайдемо:

$$R^2 = R \circ R =$$

1,0	0,86	0,94	0,53	0,94	0,94	0,53	0,53	0,94	0,53
0,86	1,0	0,86	0,5	0,86	0,86	0,51	0,53	0,86	0,5
0,94	0,86	1,0	0,5	0,96	0,95	0,51	0,53	0,96	0,5
0,53	0,5	0,5	1,0	0,47	0,47	0,8	0,8	0,47	0,86
0,94	0,86	0,96	0,47	1,0	0,96	0,51	0,53	0,96	0,47
0,94	0,86	0,95	0,47	0,96	1,0	0,51	0,53	0,98	0,44
0,53	0,51	0,51	0,8	0,51	0,51	1,0	0,89	0,51	0,8
0,53	0,53	0,53	0,8	0,53	0,53	0,89	1,0	0,53	0,8
0,94	0,86	0,96	0,47	0,96	0,98	0,51	0,53	1,0	0,46
0,53	0,5	0,5	0,86	0,47	0,44	0,8	0,8	0,46	1,0

(3.8)

$$R^3 = R^2 \circ R =$$

1,0	0,86	0,94	0,53	0,94	0,94	0,53	0,53	0,94	0,53
0,86	1,0	0,86	0,53	0,86	0,86	0,53	0,53	0,86	0,53
0,94	0,86	1,0	0,53	0,96	0,96	0,53	0,53	0,96	0,53
0,53	0,53	0,53	1,0	0,53	0,53	0,8	0,8	0,53	0,86
0,94	0,86	0,96	0,53	1,0	0,96	0,53	0,53	0,96	0,53
0,94	0,86	0,96	0,53	0,96	1,0	0,53	0,53	0,98	0,53
0,53	0,53	0,53	0,8	0,53	0,53	1,0	0,89	0,53	0,8
0,53	0,53	0,53	0,8	0,53	0,53	0,89	1,0	0,53	0,8
0,94	0,86	0,96	0,53	0,96	0,98	0,53	0,53	1,0	0,53
0,53	0,53	0,53	0,86	0,53	0,53	0,8	0,8	0,53	1,0

(3.9)

Подальші обчислення показують, що $R^3 = R^4$, тому транзитивне замикання матиме вигляд:

$$\overline{R} = R \cup R^2 \cup R^3 \cup ... \cup R^k \cup ... = R^3 \qquad (3.10)$$

Наступним кроком є знаходження рангів інформаційних загроз: $\rho_i = \sum_{i=1}^{m} \mu_{ij}$. Дані ранги відповідають загальному впливу $i-$тої загрози на виконання всіх критеріїв системою ЗІ.

Розкладемо нечітке відношення (3.10) за $\alpha-$рівнями:

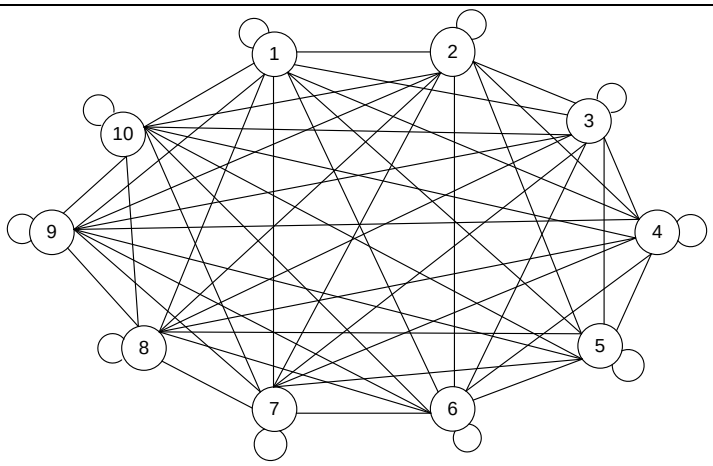
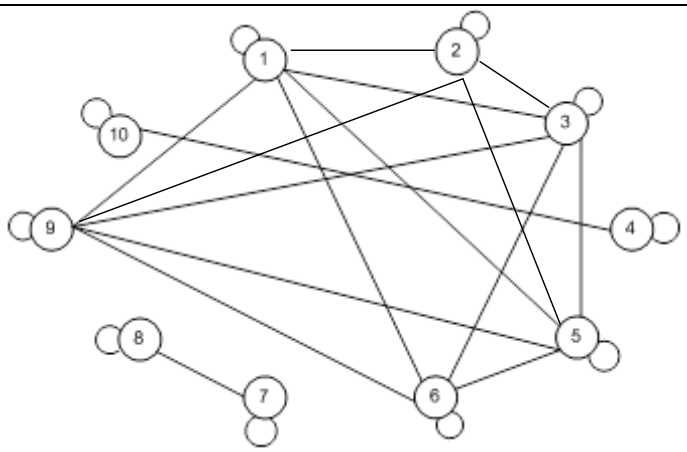
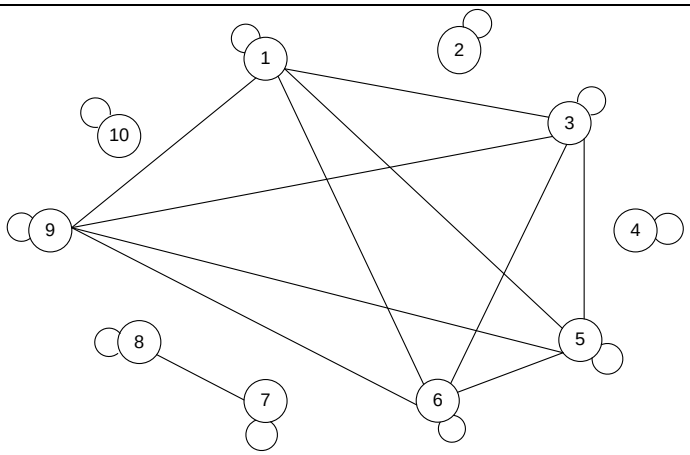
$$\overline{R} = \bigcup_{\alpha} \alpha R_{\alpha} = 0{,}53R_{0,53} \cup 0.86R_{0.86} \cup 0.89R_{0.89} \cup 0.94R_{0.94} \cup 0.96R_{0.96} \cup 0.98R_{0.98} \cup R_{1.0},$$

де $R_{\alpha}-$ чіткі відношення $\alpha-$рівня. Причому число α – рівень визначеності знань про систему.

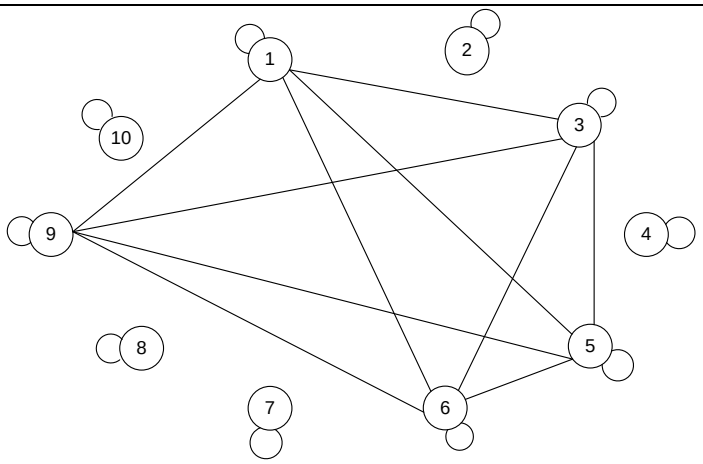
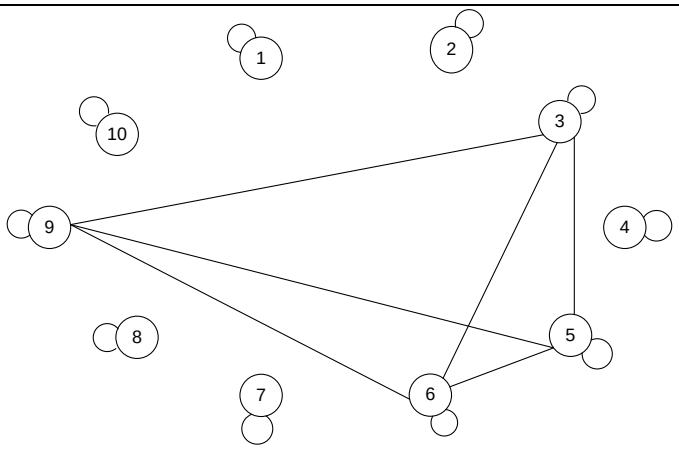
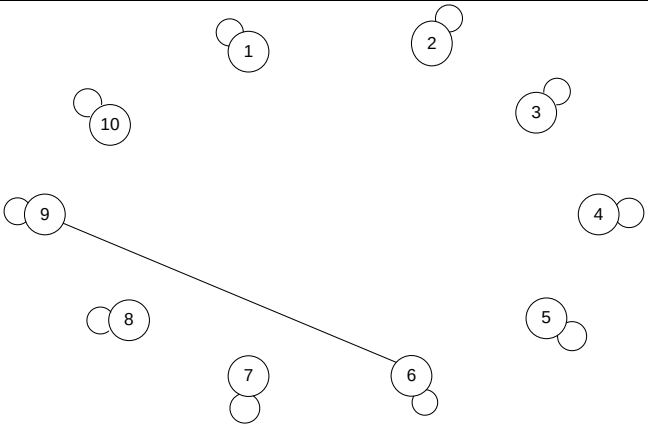
Вищезазначені відношення та їхні графи представимо у таблиці 3.10.

Таблиця 3.10

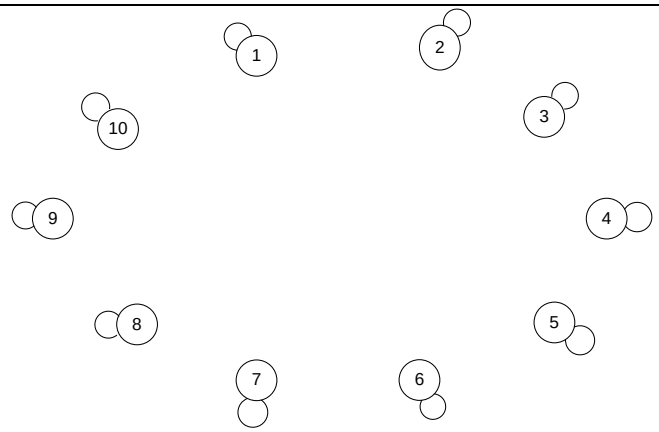
Відношення α – рівня та їхні графи

α	R_α	Граф
0,53	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
0,86	1 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 1 1 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 1 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 1	
0,89	1 0 1 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1	

Продовження таблиці 3.10

0,94	1 0 1 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1	
0,96	1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1	
0,98	1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1	

Продовження таблиці 3.10

1,0	1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1	

Розглянуті чіткі відношення $\alpha-$рівня утворюють класи загроз ІБ, які за вагомістю еквівалентні (табл. 3.11). Тобто загрози одного класу майже однакові за ступенем важливості й порівняльною динамікою їх наростання.

Таблиця 3.11

Класи загроз еквівалентних за вагомістю

Рівень	Число класів	Класи загроз
$\alpha = 0{,}53$	1	$\{K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_9, K_{10}\}$
$\alpha = 0{,}86$	2	$\{K_1, K_2, K_3, K_4, K_5, K_6, K_9, K_{10}\}$, $\{K_7, K_8\}$
$\alpha = 0{,}89$	5	$\{K_1, K_3, K_5, K_6, K_9\}$, $\{K_2\}$, $\{K_4\}$, $\{K_7, K_8\}$, $\{K_{10}\}$
$\alpha = 0{,}94$	6	$\{K_1, K_3, K_5, K_6, K_9\}$, $\{K_2\}$, $\{K_4\}$, $\{K_7\}$, $\{K_8\}$, $\{K_{10}\}$
$\alpha = 0{,}96$	7	$\{K_3, K_5, K_6, K_9\}$, $\{K_1\}$, $\{K_2\}$, $\{K_4\}$, $\{K_7\}$, $\{K_8\}$, $\{K_{10}\}$
$\alpha = 0{,}98$	9	$\{K_6, K_9\}$, $\{K_1\}$, $\{K_2\}$, $\{K_3\}$, $\{K_4\}$, $\{K_5\}$, $\{K_7\}$, $\{K_8\}$, $\{K_{10}\}$
$\alpha = 1$	10	$\{K_1\}$, $\{K_2\}$, $\{K_3\}$, $\{K_4\}$, $\{K_5\}$, $\{K_6\}$, $\{K_7\}$, $\{K_8\}$, $\{K_9\}$, $\{K_{10}\}$

Дерево загроз системи ЗІ на класи еквівалентності представлено на рисунку 3.1.

З рис. 3.1 видно, що при максимальній визначеності ($\alpha = 1$) кожна загроза представляє собою універсальний клас вагомості. Однак, якщо розглянути рівень $\alpha = 0{,}53$, то всі загрози системи ЗІ не розрізняються за рангами.

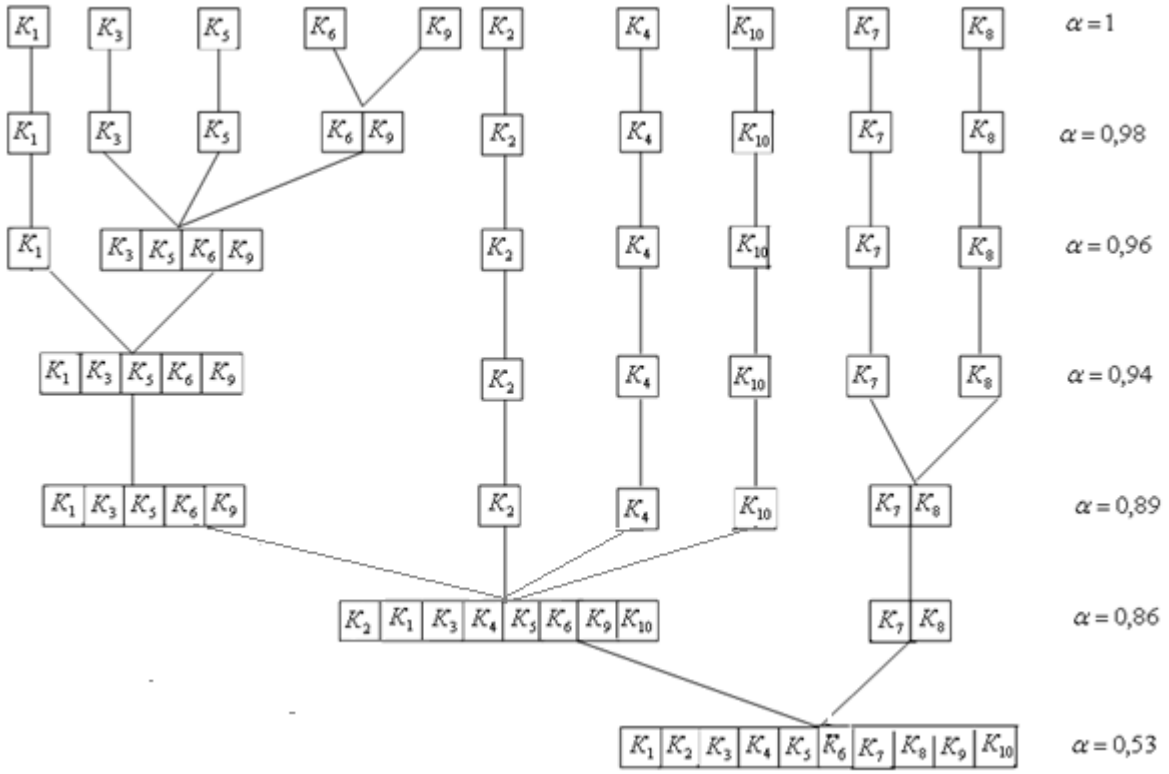


Рисунок 3.1 – Дерево декомпозиції на класи еквівалентності

Підсумовуючи значення рядків матриці (3.6), отримаємо кількісні значення рангів загроз:

$$\rho_1 = 2{,}45, \quad \rho_2 = 2{,}56, \quad \rho_3 = 2{,}55, \quad \rho_4 = 2{,}11, \quad \rho_5 = 2{,}67,$$
$$\rho_6 = 2{,}86, \quad \rho_7 = 2{,}28, \quad \rho_8 = 2{,}34, \quad \rho_9 = 2{,}83, \quad \rho_{10} = 1{,}55.$$

Врахувавши дані значення оберемо рівень визначеності $\alpha = 0{,}98$, на якому:

$$\rho_6 = \rho_9 = \frac{1}{2}(2{,}86 + 2{,}83) = 2{,}85, \quad \rho_1 = 2{,}45, \quad \rho_2 = 2{,}56, \quad \rho_3 = 2{,}55,$$
$$\rho_4 = 2{,}11, \quad \rho_5 = 2{,}67, \quad \rho_7 = 2{,}28, \quad \rho_8 = 2{,}34, \quad \rho_{10} = 1{,}55.$$

Якщо S_0 – допустимі витрати на забезпечення захищеності системи ЗІ, то ці витрати повинні розподіляться пропорційно рангам інформаційних загроз, тобто:

$$\sum_{i=1}^{10} S_i = S_0,\ S_6 = S_9 = 0{,}118S_0,\ S_1 = 0{,}101S_0,\ S_2 = 0{,}106S_0,\ S_3 = 0{,}105S_0,\ S_4 = 0{,}087S_0,$$
$$S_5 = 0{,}110S_0,\ S_7 = 0{,}094S_0,\ S_8 = 0{,}097S_0,\ S_{10} = 0{,}064S_0.$$

Аналогічно, якщо λ_0 – допустима інтенсивність зниження рівня захищеності системи ЗІ, то отримаємо необхідні λ-характеристики загроз:

$$\sum_{i=1}^{10}\lambda_i = \lambda_0,\ \lambda_6 = \lambda_9 = 0{,}118\lambda_0,\ \lambda_1 = 0{,}101\lambda_0,\ \lambda_2 = 0{,}106\lambda_0,\ \lambda_3 = 0{,}105\lambda_0,\ \lambda_4 = 0{,}087\lambda_0,$$
$$\lambda_5 = 0{,}110\lambda_0,\ \lambda_7 = 0{,}094\lambda_0,\ \lambda_8 = 0{,}097\lambda_0,\ \lambda_{10} = 0{,}064\lambda_0.$$

Отримані результати надають можливість застосувати комплексні заходи до кожного класу загроз безпеці системи ЗІ, які не відрізняються за вагомістю та доцільно вибудувати чіткий план організації захисту інформаційного простору, враховуючи ступінь впливу кожного класу загроз, забезпечити баланс між рівнем інформаційного ризику та допустимими витратами на проведення заходів ІБ.

Проведемо аналогічні дослідження по відношенню до об’єкта КІ. Для досягнення поставленої мети, оберемо з множини концептів когнітивної карти для визначення рівня захищеності об’єкта КІ (розробленої у другому розділі роботи), ті загрози, які є найважливішими з точки зору вивчення даного питання:

– K_1 – природні явища, техногенний вплив;

– K_2 – військове вторгнення;

– K_3 – терористичний вплив;

– K_4 – промислове шпигунство;

– K_5 – хакерський вплив;

– K_6 – інсайдерський вплив;

– K_7 – безпека каналів зв’язку КІ;

– K_8 – надійність, відмовостійкість складових КІ та безпека обслуговуючих систем і обладнання;

– K_9 – захищеність сховищ даних та хмарних серверів;

– K_{10} – безпека Інтернет та додатків;

– K_{11} – шкідливі програми;

– K_{12} – DoS-атаки.

Вищезазначені загрози виражаються в порушенні таких критеріїв як [34]:

– C_1 – доступність;

– C_2 – цілісність;

– C_3 – конфіденційність;

– C_4 – достовірність.

Здійснимо ранжування загроз ІБ об'єктів КІ на основі нечіткого транзитивного замикання та побудови нечітких відношень впливу та схожості [120].

Експертні порівняння сил впливу f_{ij} із найменшими силами впливу f_{il} представлено в таблиці 3.12.

Таблиця 3.12

Початкові дані для методу найменшого впливу

K_i	C_l	f_{ij} / f_{il}			
		C_1	C_2	C_3	C_4
K_1	C_3	$\frac{11}{13}=8$	$\frac{12}{13}=5$	$\frac{13}{13}=1$	$\frac{14}{13}=1$
K_2	C_4	$\frac{21}{24}=7$	$\frac{22}{24}=4$	$\frac{23}{24}=5$	$\frac{24}{24}=1$
K_3	C_4	$\frac{31}{34}=6$	$\frac{32}{34}=9$	$\frac{33}{34}=2$	$\frac{34}{34}=1$
K_4	C_1	$\frac{41}{41}=1$	$\frac{42}{41}=3$	$\frac{43}{41}=9$	$\frac{44}{41}=5$
K_5	C_4	$\frac{51}{54}=5$	$\frac{52}{54}=7$	$\frac{53}{54}=6$	$\frac{54}{54}=1$
K_6	C_1	$\frac{61}{61}=1$	$\frac{62}{61}=5$	$\frac{63}{61}=7$	$\frac{64}{61}=4$
K_7	C_2	$\frac{71}{72}=8$	$\frac{72}{72}=1$	$\frac{73}{72}=5$	$\frac{74}{72}=3$
K_8	C_3	$\frac{81}{83}=9$	$\frac{82}{83}=6$	$\frac{83}{83}=1$	$\frac{84}{83}=4$
K_9	C_1	$\frac{91}{91}=1$	$\frac{92}{91}=4$	$\frac{93}{91}=3$	$\frac{94}{91}=1$
K_{10}	C_4	$\frac{101}{104}=4$	$\frac{102}{104}=1$	$\frac{103}{104}=5$	$\frac{104}{104}=1$
K_{11}	C_4	$\frac{111}{114}=5$	$\frac{112}{114}=8$	$\frac{113}{114}=6$	$\frac{114}{114}=1$
K_{12}	C_3	$\frac{121}{123}=9$	$\frac{122}{123}=1$	$\frac{123}{123}=1$	$\frac{124}{123}=1$

Використовуючи дані таблиці 3.12, визначимо ступені впливу μ_{ij}, які утворюють нечітке відношення (3.11):

$$I=\begin{array}{|c|c|c|c|}\hline 8/15 & 5/15 & 1/15 & 1/15\\ \hline 7/17 & 4/17 & 5/17 & 1/17\\ \hline 6/18 & 9/18 & 2/18 & 1/18\\ \hline 1/18 & 3/18 & 9/18 & 5/18\\ \hline 5/19 & 7/19 & 6/19 & 1/19\\ \hline 1/17 & 5/17 & 7/17 & 4/17\\ \hline 8/17 & 1/17 & 5/17 & 3/17\\ \hline 9/20 & 6/20 & 1/20 & 4/20\\ \hline 1/9 & 4/9 & 3/9 & 1/9\\ \hline 4/11 & 1/11 & 5/11 & 1/11\\ \hline 5/20 & 8/20 & 6/20 & 1/20\\ \hline 9/12 & 1/12 & 1/12 & 1/12\\ \hline\end{array} \quad (3.11)$$

Нормалізуємо дане відношення, поділивши елементи кожного рядка на максимальне значення, яке міститься у відповідному рядку (3.11):

$$I=\begin{array}{|c|c|c|c|}\hline 1,0 & 0,63 & 0,13 & 0,13\\ \hline 1,0 & 0,57 & 0,71 & 0,14\\ \hline 0,67 & 1,0 & 0,22 & 0,11\\ \hline 0,11 & 0,33 & 1,0 & 0,56\\ \hline 0,71 & 1,0 & 0,86 & 0,14\\ \hline 0,14 & 0,71 & 1,0 & 0,57\\ \hline 1,0 & 0,13 & 0,63 & 0,38\\ \hline 1,0 & 0,67 & 0,11 & 0,44\\ \hline 0,25 & 1,0 & 0,75 & 0,25\\ \hline 0,8 & 0,2 & 1,0 & 0,2\\ \hline 0,63 & 1,0 & 0,75 & 0,13\\ \hline 1,0 & 0,11 & 0,11 & 0,11\\ \hline\end{array} \quad (3.12)$$

Сформуємо нечітке відношення схожості, яке має властивості рефлективності та симетричності:

$$R=\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 1,0 & 0,84 & 0,81 & 0,38 & 0,65 & 0,44 & 0,69 & 0,91 & 0,53 & 0,61 & 0,59 & 0,86\\ \hline 0,84 & 1,0 & 0,68 & 0,54 & 0,76 & 0,57 & 0,81 & 0,75 & 0,67 & 0,76 & 0,76 & 0,73\\ \hline 0,81 & 0,68 & 1,0 & 0,38 & 0,82 & 0,48 & 0,53 & 0,72 & 0,73 & 0,55 & 0,85 & 0,67\\ \hline 0,38 & 0,54 & 0,38 & 1,0 & 0,54 & 0,88 & 0,59 & 0,44 & 0,66 & 0,7 & 0,53 & 0,39\\ \hline 0,65 & 0,76 & 0,82 & 0,54 & 1,0 & 0,64 & 0,59 & 0,58 & 0,83 & 0,73 & 0,95 & 0,51\\ \hline 0,44 & 0,57 & 0,48 & 0,88 & 0,64 & 1,0 & 0,5 & 0,52 & 0,76 & 0,61 & 0,63 & 0,3\\ \hline 0,69 & 0,81 & 0,53 & 0,59 & 0,59 & 0,5 & 1,0 & 0,72 & 0,53 & 0,76 & 0,6 & 0,8\\ \hline 0,91 & 0,75 & 0,72 & 0,44 & 0,58 & 0,52 & 0,72 & 1,0 & 0,52 & 0,55 & 0,59 & 0,78\\ \hline 0,53 & 0,67 & 0,73 & 0,66 & 0,83 & 0,76 & 0,53 & 0,52 & 1,0 & 0,59 & 0,87 & 0,39\\ \hline 0,61 & 0,76 & 0,55 & 0,7 & 0,73 & 0,61 & 0,76 & 0,55 & 0,59 & 1,0 & 0,68 & 0,68\\ \hline 0,59 & 0,76 & 0,85 & 0,53 & 0,95 & 0,63 & 0,6 & 0,59 & 0,87 & 0,68 & 1,0 & 0,52\\ \hline 0,86 & 0,73 & 0,67 & 0,39 & 0,51 & 0,3 & 0,8 & 0,78 & 0,39 & 0,68 & 0,52 & 1,0\\ \hline\end{array} \quad (3.13)$$

Надамо початковому відношенню схожості R властивість транзитивності, визначаючи композицію відношень як максимінний добуток відповідних матриць за допомогою авторського програмного засобу (додаток А):

$$R^2 = \begin{pmatrix} 1,0 & 0,84 & 0,81 & 0,61 & 0,81 & 0,64 & 0,81 & 0,91 & 0,73 & 0,76 & 0,81 & 0,86 \\ 0,84 & 1,0 & 0,81 & 0,7 & 0,76 & 0,67 & 0,81 & 0,84 & 0,76 & 0,76 & 0,76 & 0,84 \\ 0,81 & 0,81 & 1,0 & 0,66 & 0,85 & 0,73 & 0,72 & 0,81 & 0,85 & 0,73 & 0,85 & 0,81 \\ 0,61 & 0,7 & 0,66 & 1,0 & 0,7 & 0,88 & 0,7 & 0,59 & 0,76 & 0,7 & 0,68 & 0,68 \\ 0,81 & 0,76 & 0,85 & 0,7 & 1,0 & 0,76 & 0,76 & 0,75 & 0,87 & 0,76 & 0,95 & 0,73 \\ 0,64 & 0,67 & 0,73 & 0,88 & 0,76 & 1,0 & 0,61 & 0,59 & 0,76 & 0,7 & 0,76 & 0,61 \\ 0,81 & 0,81 & 0,72 & 0,7 & 0,76 & 0,61 & 1,0 & 0,78 & 0,67 & 0,76 & 0,76 & 0,8 \\ 0,91 & 0,84 & 0,81 & 0,59 & 0,75 & 0,59 & 0,78 & 1,0 & 0,72 & 0,75 & 0,75 & 0,86 \\ 0,73 & 0,76 & 0,85 & 0,76 & 0,87 & 0,76 & 0,67 & 0,72 & 1,0 & 0,73 & 0,87 & 0,67 \\ 0,76 & 0,76 & 0,73 & 0,7 & 0,76 & 0,7 & 0,76 & 0,75 & 0,73 & 1,0 & 0,76 & 0,76 \\ 0,81 & 0,76 & 0,85 & 0,68 & 0,95 & 0,76 & 0,76 & 0,75 & 0,87 & 0,76 & 1,0 & 0,73 \\ 0,86 & 0,84 & 0,81 & 0,68 & 0,73 & 0,61 & 0,8 & 0,86 & 0,67 & 0,76 & 0,73 & 1,0 \end{pmatrix} \quad (3.14)$$

$$R^3 = \begin{pmatrix} 1,0 & 0,84 & 0,81 & 0,7 & 0,81 & 0,73 & 0,81 & 0,91 & 0,81 & 0,76 & 0,81 & 0,86 \\ 0,84 & 1,0 & 0,81 & 0,7 & 0,81 & 0,76 & 0,81 & 0,84 & 0,76 & 0,76 & 0,81 & 0,84 \\ 0,81 & 0,81 & 1,0 & 0,73 & 0,85 & 0,76 & 0,81 & 0,81 & 0,85 & 0,76 & 0,85 & 0,81 \\ 0,7 & 0,7 & 0,73 & 1,0 & 0,76 & 0,88 & 0,7 & 0,7 & 0,76 & 0,7 & 0,76 & 0,7 \\ 0,81 & 0,81 & 0,85 & 0,76 & 1,0 & 0,76 & 0,76 & 0,81 & 0,87 & 0,76 & 0,95 & 0,81 \\ 0,73 & 0,76 & 0,76 & 0,88 & 0,76 & 1,0 & 0,7 & 0,72 & 0,76 & 0,73 & 0,76 & 0,68 \\ 0,81 & 0,81 & 0,81 & 0,7 & 0,76 & 0,7 & 1,0 & 0,81 & 0,76 & 0,76 & 0,76 & 0,81 \\ 0,91 & 0,84 & 0,81 & 0,7 & 0,81 & 0,72 & 0,81 & 1,0 & 0,75 & 0,76 & 0,81 & 0,86 \\ 0,81 & 0,76 & 0,85 & 0,76 & 0,87 & 0,76 & 0,76 & 0,75 & 1,0 & 0,76 & 0,87 & 0,73 \\ 0,76 & 0,76 & 0,76 & 0,7 & 0,76 & 0,73 & 0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,76 \\ 0,81 & 0,81 & 0,85 & 0,76 & 0,95 & 0,76 & 0,76 & 0,81 & 0,87 & 0,76 & 1,0 & 0,81 \\ 0,86 & 0,84 & 0,81 & 0,7 & 0,81 & 0,68 & 0,81 & 0,86 & 0,73 & 0,76 & 0,81 & 1,0 \end{pmatrix} \quad (3.15)$$

$$R^4 = \begin{pmatrix} 1,0 & 0,84 & 0,81 & 0,73 & 0,81 & 0,76 & 0,81 & 0,91 & 0,81 & 0,76 & 0,81 & 0,86 \\ 0,84 & 1,0 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,84 & 0,81 & 0,76 & 0,81 & 0,84 \\ 0,81 & 0,81 & 1,0 & 0,76 & 0,85 & 0,76 & 0,81 & 0,81 & 0,85 & 0,76 & 0,85 & 0,81 \\ 0,73 & 0,76 & 0,76 & 1,0 & 0,76 & 0,88 & 0,7 & 0,72 & 0,76 & 0,73 & 0,76 & 0,7 \\ 0,81 & 0,81 & 0,85 & 0,76 & 1,0 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 0,95 & 0,81 \\ 0,76 & 0,76 & 0,76 & 0,88 & 0,76 & 1,0 & 0,76 & 0,75 & 0,76 & 0,76 & 0,76 & 0,73 \\ 0,81 & 0,81 & 0,81 & 0,7 & 0,81 & 0,76 & 1,0 & 0,81 & 0,76 & 0,76 & 0,81 & 0,81 \\ 0,91 & 0,84 & 0,81 & 0,72 & 0,81 & 0,75 & 0,81 & 1,0 & 0,81 & 0,76 & 0,81 & 0,86 \\ 0,81 & 0,81 & 0,85 & 0,76 & 0,87 & 0,76 & 0,76 & 0,81 & 1,0 & 0,76 & 0,87 & 0,81 \\ 0,76 & 0,76 & 0,76 & 0,73 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,76 \\ 0,81 & 0,81 & 0,85 & 0,76 & 0,95 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 1,0 & 0,81 \\ 0,86 & 0,84 & 0,81 & 0,7 & 0,81 & 0,73 & 0,81 & 0,86 & 0,81 & 0,76 & 0,81 & 1,0 \end{pmatrix} \quad (3.16)$$

$$R^5 = \begin{array}{|cccccccccccc|}
\hline
1,0 & 0,84 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,91 & 0,81 & 0,76 & 0,81 & 0,86 \\
0,84 & 1,0 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,84 & 0,81 & 0,76 & 0,81 & 0,84 \\
0,81 & 0,81 & 1,0 & 0,76 & 0,85 & 0,76 & 0,81 & 0,81 & 0,85 & 0,76 & 0,85 & 0,81 \\
0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,88 & 0,76 & 0,75 & 0,76 & 0,76 & 0,76 & 0,73 \\
0,81 & 0,81 & 0,85 & 0,76 & 1,0 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 0,95 & 0,81 \\
0,76 & 0,76 & 0,76 & 0,88 & 0,76 & 1,0 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 \\
0,81 & 0,81 & 0,81 & 0,76 & 0,81 & 0,76 & 1,0 & 0,81 & 0,81 & 0,76 & 0,81 & 0,81 \\
0,91 & 0,84 & 0,81 & 0,75 & 0,81 & 0,76 & 0,81 & 1,0 & 0,81 & 0,76 & 0,81 & 0,86 \\
0,81 & 0,81 & 0,85 & 0,76 & 0,87 & 0,76 & 0,81 & 0,81 & 1,0 & 0,76 & 0,87 & 0,81 \\
0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,76 \\
0,81 & 0,81 & 0,85 & 0,76 & 0,95 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 1,0 & 0,81 \\
0,86 & 0,84 & 0,81 & 0,73 & 0,81 & 0,76 & 0,81 & 0,86 & 0,81 & 0,76 & 0,81 & 1,0 \\
\hline
\end{array} \quad (3.17)$$

$$R^6 = \begin{array}{|cccccccccccc|}
\hline
1,0 & 0,84 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,91 & 0,81 & 0,76 & 0,81 & 0,86 \\
0,84 & 1,0 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,84 & 0,81 & 0,76 & 0,81 & 0,84 \\
0,81 & 0,81 & 1,0 & 0,76 & 0,85 & 0,76 & 0,81 & 0,81 & 0,85 & 0,76 & 0,85 & 0,81 \\
0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,88 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 \\
0,81 & 0,81 & 0,85 & 0,76 & 1,0 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 0,95 & 0,81 \\
0,76 & 0,76 & 0,76 & 0,88 & 0,76 & 1,0 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 \\
0,81 & 0,81 & 0,81 & 0,76 & 0,81 & 0,76 & 1,0 & 0,81 & 0,81 & 0,76 & 0,81 & 0,81 \\
0,91 & 0,84 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 1,0 & 0,81 & 0,76 & 0,81 & 0,86 \\
0,81 & 0,81 & 0,85 & 0,76 & 0,87 & 0,76 & 0,81 & 0,81 & 1,0 & 0,76 & 0,87 & 0,81 \\
0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 0,76 & 1,0 & 0,76 & 0,76 \\
0,81 & 0,81 & 0,85 & 0,76 & 0,95 & 0,76 & 0,81 & 0,81 & 0,87 & 0,76 & 1,0 & 0,81 \\
0,86 & 0,84 & 0,81 & 0,76 & 0,81 & 0,76 & 0,81 & 0,86 & 0,81 & 0,76 & 0,81 & 1,0 \\
\hline
\end{array} \quad (3.18)$$

Подальші обчислення показують, що $R^6 = R^7 = ... = R^\infty$, тому транзитивне замикання відношення R матиме вигляд:

$$\overline{R} = R \cup R^2 \cup R^3 \cup ... \cup R^k \cup ... = R^6.$$

Просумовуючи значення рядків матриці (3.12), знайдемо ранги загроз ІБ об'єктів КІ:

$$\rho_1 = 1{,}89, \quad \rho_2 = \rho_6 = 2{,}42, \quad \rho_3 = \rho_4 = 2, \quad \rho_5 = 2{,}71, \quad \rho_7 = 2{,}14,$$
$$\rho_8 = 2{,}22, \quad \rho_9 = 2{,}25, \quad \rho_{10} = 2{,}2, \quad \rho_{11} = 2{,}51, \quad \rho_{12} = 1{,}33.$$

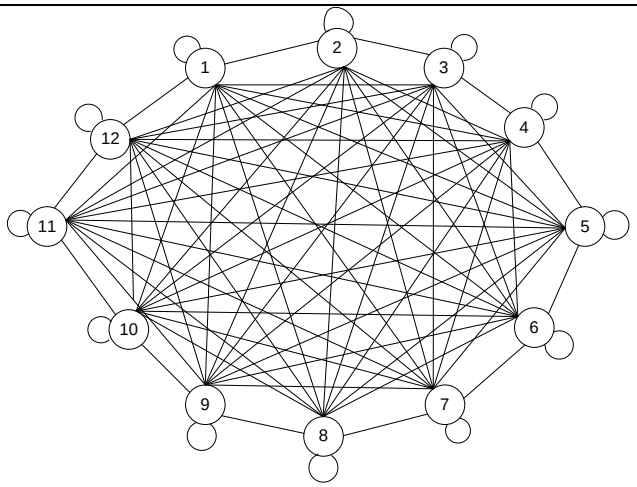
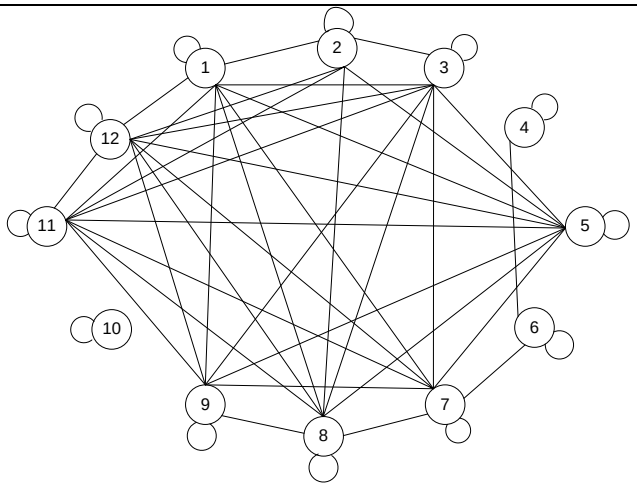
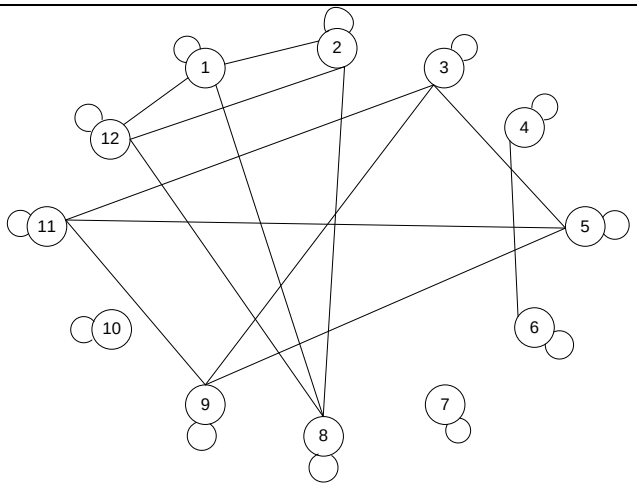
Нечітке відношення R розкладемо за α – рівнями наступним чином:

$$\overline{R} = \bigcup_\alpha \alpha R_\alpha = 0.76R_{0.76} \cup 0.81R_{0.81} \cup 0.84R_{0.84} \cup 0.85R_{0.85} \cup 0.86R_{0.86} \cup$$
$$\cup 0.87R_{0.87} \cup 0.88R_{0.88} \cup 0.91R_{0.91} \cup 0.95R_{0.95} \cup R_{1.0}.$$

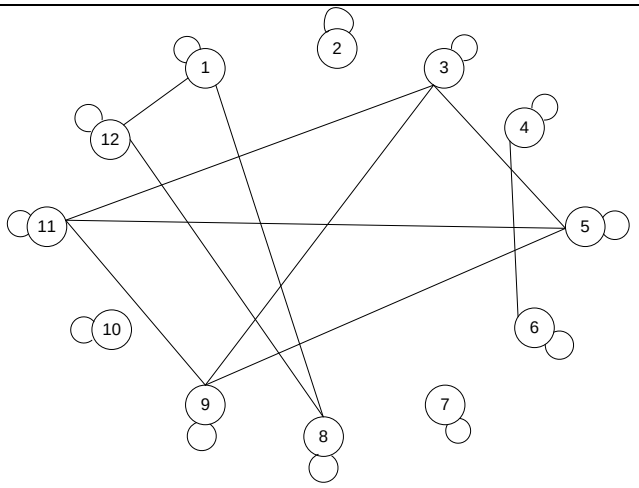
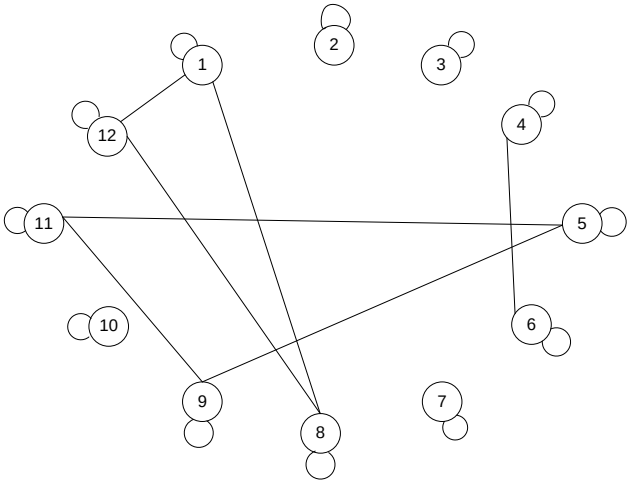
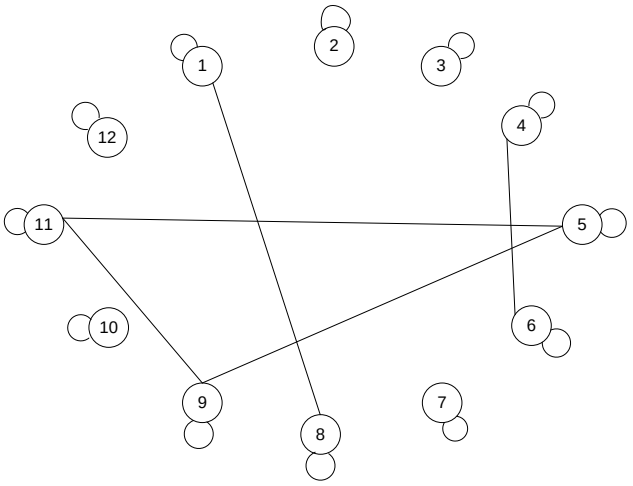
Дані відношення та відповідні їм графи відображено у таблиці 3.13.

Таблиця 3.13

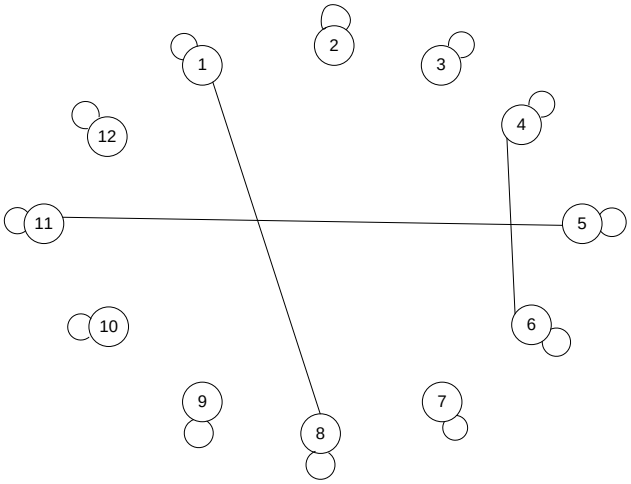
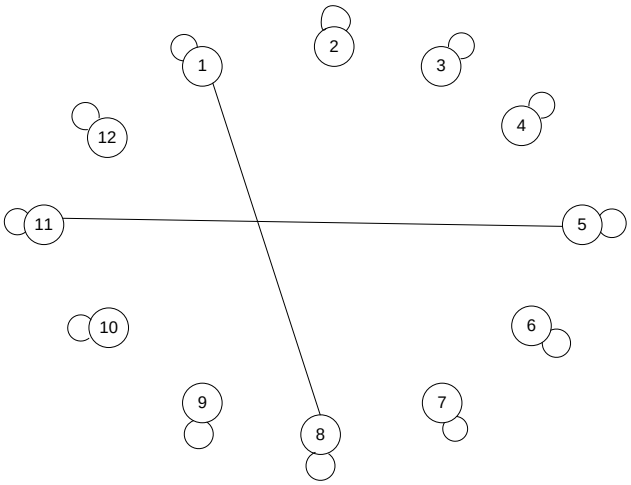
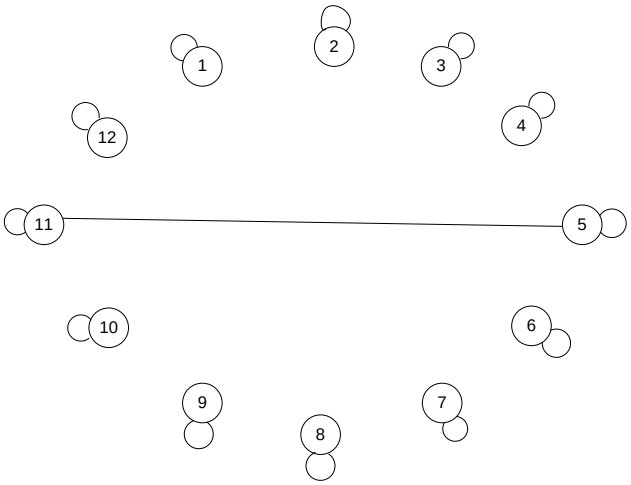
Відношення α – рівня та їхні графи

α	R_α	Граф
0,76	1 1	
0,81	1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1	
0,84	1 1 0 0 0 0 0 1 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 1	

Продовження таблиці 3.13

0,85	1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 1	
0,86	1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 1	
0,87	1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1	

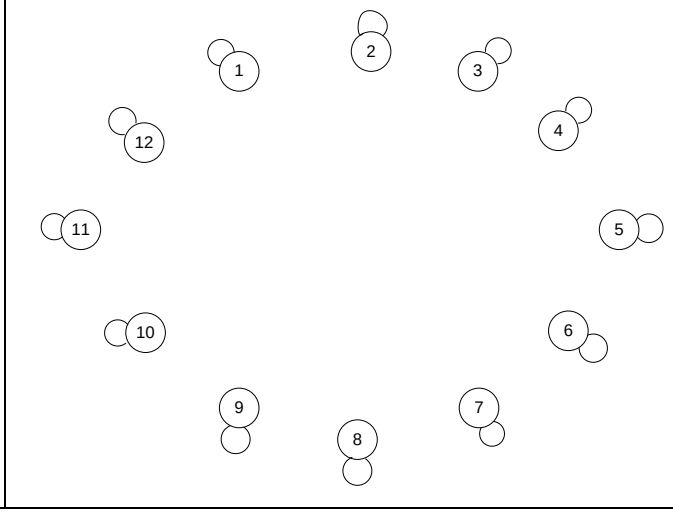
Продовження таблиці 3.13

0,88	1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1	
0,91	1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1	
0,95	1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1	

Продовження таблиці 3.13

1,0		

1	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	1



Таким чином, чіткі відношення $\alpha-$рівня утворюють класи елементів еквівалентних за вагомістю (табл. 3.14).

Таблиця 3.14

Класи загроз еквівалентних за вагомістю

Рівень	Число класів	Класи загроз
$\alpha = 0{,}76$	1	$\{K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_9, K_{10}, K_{11}, K_{12}\}$
$\alpha = 0{,}81$	2	$\{K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_9, K_{11}, K_{12}\}, \{K_{10}\}$
$\alpha = 0{,}84$	3	$\{K_1, K_2, K_3, K_4, K_5, K_6, K_8, K_9, K_{11}, K_{12}\}, \{K_7\}, \{K_{10}\}$
$\alpha = 0{,}85$	4	$\{K_1, K_3, K_4, K_5, K_6, K_8, K_9, K_{11}, K_{12}\}, \{K_2\}, \{K_7\}, \{K_{10}\}$
$\alpha = 0{,}86$	5	$\{K_1, K_4, K_5, K_6, K_8, K_9, K_{11}, K_{12}\}, \{K_2\}, \{K_3\}, \{K_7\}, \{K_{10}\}$
$\alpha = 0{,}87$	6	$\{K_1, K_4, K_5, K_6, K_8, K_9, K_{11}\}, \{K_2\}, \{K_3\}, \{K_7\}, \{K_{10}\}, \{K_{12}\}$
$\alpha = 0{,}88$	7	$\{K_1, K_4, K_5, K_6, K_8, K_{11}\}, \{K_2\}, \{K_3\}, \{K_7\}, \{K_9\}, \{K_{10}\}, \{K_{12}\}$
$\alpha = 0{,}91$	9	$\{K_1, K_5, K_8, K_{11}\}, \{K_2\}, \{K_3\}, \{K_4\}, \{K_6\}, \{K_7\}, \{K_9\}, \{K_{10}\}, \{K_{12}\}$
$\alpha = 0{,}95$	11	$\{K_5, K_{11}\}, \{K_1\}, \{K_2\}, \{K_3\}, \{K_4\}, \{K_6\}, \{K_7\}, \{K_8\}\{K_9\}, \{K_{10}\}, \{K_{12}\}$
$\alpha = 1$	12	$\{K_1\}, \{K_2\}, \{K_3\}, \{K_4\}, \{K_5\}, \{K_6\}, \{K_7\}, \{K_8\}, \{K_9\}, \{K_{10}\}, \{K_{11}\}, \{K_{12}\}$

На рис. 3.2 відобразимо дерево декомпозиції множини загроз на класи еквівалентності, які не перетинаються.

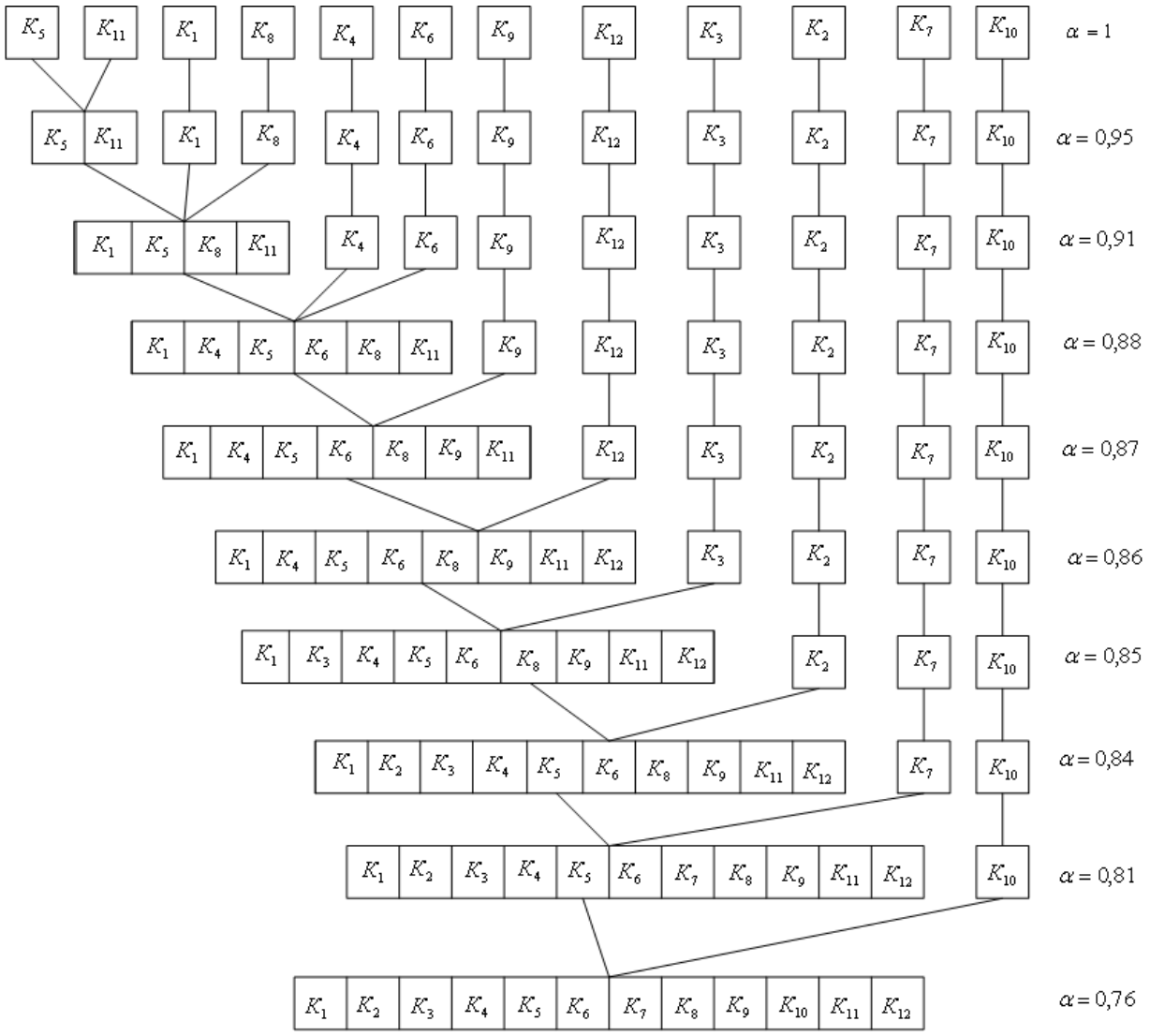


Рисунок 3.2 – Дерево декомпозиції множини загроз на класи еквівалентності

Враховуючи кількісні оцінки вагомості загроз, виберемо рівень невизначеності $\alpha = 0{,}95$. На даному рівні отримаємо:

$$\rho_1 = 1{,}89, \quad \rho_2 = \rho_6 = 2{,}42, \quad \rho_3 = \rho_4 = 2, \quad \rho_7 = 2{,}14,$$
$$\rho_8 = 2{,}22, \quad \rho_9 = 2{,}25, \quad \rho_{10} = 2{,}2, \quad \rho_{12} = 1{,}33, \quad \rho_5 = \rho_{11} = 2{,}61.$$

Якщо S_0 – допустимі витрати на забезпечення захищеності об’єкта КІ, то ці витрати повинні розподіляться пропорційно рангам інформаційних загроз, тобто:

$$\sum_{i=1}^{12} S_i = S_0, \quad S_1 = 0{,}072S_0, \quad S_2 = S_6 = 0{,}093S_0, \quad S_3 = S_4 = 0{,}077S_0, \quad S_5 = S_{11} = 0{,}1S_0,$$
$$S_7 = 0{,}082S_0, \quad S_8 = 0{,}085S_0, \quad S_9 = 0{,}086S_0, \quad S_{10} = 0{,}084S_0, \quad S_{12} = 0{,}051S_0.$$

Аналогічно, якщо λ_0 – допустима інтенсивність зниження рівня захищеності об’єкта КІ, то отримаємо необхідні λ – характеристики загроз:

$$\sum_{i=1}^{12}\lambda_i=\lambda_0,\quad \lambda_1=0{,}072\lambda_0,\quad \lambda_2=\lambda_6=0{,}093\lambda_0,\quad \lambda_3=\lambda_4=0{,}077\lambda_0,\quad \lambda_5=\lambda_{11}=0{,}1\lambda_0,$$
$$\lambda_7=0{,}082\lambda_0,\quad \lambda_8=0{,}085\lambda_0,\quad \lambda_9=0{,}086\lambda_0,\quad \lambda_{10}=0{,}084\lambda_0,\quad \lambda_{12}=0{,}051\lambda_0.$$

Таким чином, ранжування загроз об’єкта КІ дозволяє визначити допустиму інтенсивність зниження рівня захищеності даного об’єкта та витрати на забезпечення захищеності, що, в свою чергу, сприятиме вчасному впровадженню ефективних механізмів протидії загрозам, раціональному перерозподілу сил і засобів для їхньої нейтралізації.

Результати даного дослідження надають можливість сформувати вимоги до захищеності системи ЗІ та об’єкта КІ при ймовірній реалізації загроз з певними характеристиками, що сприятиме впровадженню необхідних механізмів захисту досліджуваних об’єктів із достатньою забезпеченістю інфраструктури резервними потужностями й ресурсами, які здатні в разі реалізації загроз швидко відновити втрачені функції.

3.4 Висновки до розділу 3

Даний розділ було присвячено дослідженню розроблених у другому розділі когнітивних моделей для аналізу рівня захищеності систем ЗІ, що циркулює в ІС. Зокрема, на основі множинного регресійного аналізу було доведено достовірність впливу загроз на рівень захищеності досліджуваних систем. При цьому було сформовано аналітичний вираз лінійної кореляційної залежності, що існує між цільовою змінною та досліджуваними загрозами. Визначено значення стандартизованого коефіцієнта регресії та коефіцієнта еластичності, які є необхідними для порівняння впливу кожної загрози окремо на рівень захищеності систем ЗІ, що циркулює в ІС. Отримані значення коефіцієнтів, проаналізовано та зроблено висновок про достовірність впливу визначених загроз на рівень захищеності досліджуваних систем, визначеного за сценарним моделюванням на основі когнітивного підходу.

Також проведено симпліціальний аналіз структури когнітивної моделі для визначення рівня захищеності об’єкта КІ. При цьому здійснено побудову комплексу, що являє собою послідовність симплексів, які впорядковані за

правилом спадання їх розмірності. Визначено перший структурний вектор даного комплексу, що дозволяє встановити зв'язність концептів на усіх рівнях q. Встановлено, що на рівні $q=3$ з'явилися зв'язні компоненти досліджуваної системи: $\{K_{11}, K_{13}, K_{18}\}, \{K_3, K_5, K_4\}, \{K_7, K_6, K_2\}$. Вивчення взаємозв'язків всередині кожного блоку концептів даного симпліціального комплексу сприятиме підвищенню захищеності об'єкта КІ. Крім того, запропоновано перелік концептів когнітивної моделі, які можна обрати в якості управляючих для всієї системи: K_9 (хакерський вплив), K_{10} (вплив управлінських рішень та організаційний заходів), K_{15} (захищеність системи ЗІ), K_{16} (захищеність КМ), K_{25} (мережеві атаки) та K_{26} (шкідливі програми). Оскільки до даної множини належать найвагоміші концепти, визначені у другому розділі роботи внаслідок проведення структурного аналізу досліджуваної моделі, то це підтверджує достовірність отриманих результатів.

З використанням теорії нечітких відношень здійснено ранжування загроз системи ЗІ та об'єкта КІ, на основі якого визначено допустиму інтенсивність зниження рівня захищеності досліджуваних систем та витрати на її забезпечення. Для досягнення мети сформовано множини загроз та критерії у порушенні яких вони виражаються. Експертним шляхом встановлено ступінь впливу даних загроз на визначені критерії. Вхідну інформацію формалізовано у вигляді нечіткого відношення впливу, яке перетворюється у нечітке відношення схожості та його транзитивне замикання. У результаті було здійснено розбиття множин загроз досліджуваних систем на класи, що не перетинаються та містять елементи подібні за ступенем впливу. Для кожної з множини загроз відображено дерево декомпозиції на класи еквівалентності. На основі визначених рангів запропоновано розподіл допустимих витрат на захищеність систем, що сприятиме раціональному використанню ресурсів та засобів для попередження, усунення або ж зменшення сили впливу вірогідних загроз ІБ. Крім того, визначено допустиму інтенсивність зниження рівня захищеності досліджуваних систем.

РОЗДІЛ 4
ДИНАМІЧНИЙ АНАЛІЗ ЗАПРОПОНОВАНИХ КОГНІТИВНИХ МОДЕЛЕЙ ТА РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ЇХ РЕАЛІЗАЦІЇ

4.1 Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта КІ

У другому розділі дисертаційної роботи було побудовано когнітивну модель для дослідження рівня захищеності об'єкта КІ, який відноситься до класу об'єктів, що передбачає доступ до мережі Інтернет та відображає максимальне представлення структурних складових. На основі запропонованої моделі визначено найвагоміші концепти та за допомогою сценарного моделювання знайдено відносну зміну рівня захищеності даного об'єкта. Однак, сценарний аналіз не надає можливість прослідкувати та порівняти вплив концептів на захищеність об'єкта КІ у часі. У зв'язку з цим, варто звернути увагу на апарат динамічної каузальної алгебри [124], який дозволяє отримати прогноз розвитку ситуації у конкретні моменти часу. Таким чином, проведемо динамічний часовий аналіз впливу встановлених найвагоміших концептів досліджуваної системи: K_{15} – захищеність системи ЗІ та K_{16} – захищеність КМ на K_{14} – захищеність КІ.

Обчислення впливу складається із двох паралельних «хвиль»: μ - хвилі, яка активізує шляхи (вважається, що шлях активізовано, якщо активні всі його вершини) та $I-T$ -хвилі, що визначає вплив за активізованими шляхами. Динаміка виражається у введенні умовного часу: припускається, що до $t-го$ моменту часу хвиля проходить шлях довжини t [125].

Крім матриці суміжності W, яка визначена в попередньому розділі та визначає розроблену когнітивну модель, розглянемо три векторні параметри:

– вектор стану вершин $\psi(t)=(\psi_1(t),\psi_2(t),...\psi_n(t))$, де $\psi_i(t)$ – стан вершини i в момент часу $t,\ \ i=1,...,n$;

– вектор вхідних впливів $(\mu_1(t),...,\mu_n(t))$;

– вектор порогів вершин $Q=(q_1,...,q_n)$, який не залежить від часу.

Стан вершини приймає одне із двох значень 0 або 1 і являється показником

її активності.

У даному випадку пороги задаються таким вектором:

$$Q = (0; 0; 0; 0; 0; 0; 0; 0; 2; 1; 0; 0; 0; 1; 0; 0; 3; 0; 0; 0; 0; 2; 0; 1; 1; 2; 1).$$

Насамперед, дослідимо вплив концепта K_{15} – захищеність системи ЗІ на K_{14} – захищеність КІ. Зауважимо, що вершина K_{15} активізується ззовні та залишається активною протягом усього процесу, тобто $\psi_{15}(t) = 1$ для будь-якого t. Задамо початковий вектор стану вершин:

$$\psi_{\Omega}(0) = (0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0).$$

Визначимо μ-хвилю, що породжує процес активізації вершин та відповідних шляхів за допомогою матричної операції [118]:

$$(\mu_1, ..., \mu_n) = \psi(t) \times W \tag{4.1}$$

та вектор станів в момент $t+1$:

$$\psi(t+1) = f_Q(\psi(t) \times W) = (f_{q1}(\mu_1), ..., f_{qn}(\mu_n)), \tag{4.2}$$

де $f_{qi}(\mu_i)$ – порогова функція у вершині i:

$$f_{qi}(\mu_i) = \begin{cases} 1, & якщо\ |\mu_i| \geq q_i, \\ 0, & якщо\ |\mu_i| \prec q_i. \end{cases} \tag{4.3}$$

Врахувавши вищезазначені формули, отримаємо:

$\psi_{\Omega}(0) \times W_{\Omega} = (0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0.95; 0; 0; 0.8; 0.6; 0; 0; 0; 0.6; 0; 0; 0; 0; 0)$,

$\psi_{\Omega}(1) = (1; 1; 1; 1; 1; 1; 1; 1; 0; 0; 1; 1; 1; 0; 1; 1; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 0)$,

$\psi_{\Omega}(1) \times W_{\Omega} = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; 0.25; -1; -0.35; 0.95; 2.6; 1.6; 2.6; 1; -2; -0.1; -0.1; 1.9; 1.2; 0.85; 0.3; 0.5; 0.2)$,

$\psi_{\Omega}(2) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 1; 1; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 0)$,

$\psi_{\Omega}(2) \times W_{\Omega} = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.15; 0.95; 3.3; 2; 3.3; 1.6; -1.1; 0.3; 0.1; 2.1; 1.2; 1.3; 1.2; 1.4; 1.1)$,

$\psi_{\Omega}(3) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 1)$,

$\psi_{\Omega}(3) \times W_{\Omega} = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.6; 1.9; 3.9; 1.9; 3.3; 1.6; -1.1; 0.45; 0.2; 2.1; 1.1; 1.3; 1.2; 2.1; 1.1)$,

$\psi_{\Omega}(4) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$,

$\psi_{\Omega}(4) \times W_{\Omega} = (0; -1; -0.3; -0.2; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.6; 1.9; 3.9; 0.95; 3.3; 0.95; -1.1; 0.45; 0.2; 2.1; 0.2; 1.3; 1.2; 2.1; 1.3)$,

$\psi_{\Omega}(5) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$.

Отже, в момент $t = 4$ процес стабілізується.

Оскільки особливістю даної когнітивної карти є наявність петель, то від K_{15} до K_{14} існують шляхи через K_{15} та K_{17} і множина вершин безпосередньо зв'язаних з вершиною K_{14} матиме вигляд: $N^{-}(K_{14}) = \{K_{15}, K_{17}\}$.

Визначимо вплив вздовж усіх активізованих шляхів, врахувавши, що непрямий вплив вершини i на вершину j на шляху P в момент часу t визначається із співвідношення [125]:

$$I_P(t) = \prod_{(k,l)\in E(P)} \psi_k(t) \cdot w_{kl}, \tag{4.4}$$

де $E(P)$ – множина ребер P,

$\psi_k(t)$ – стан вершини k в момент часу t,

w_{kl} – вага ребра (k,l) шляху P.

Розраховані значення I_P для конкретних шляхів у різні моменти часу занесено в таблиці 4.1-4.2.

Таблиця 4.1

Значення непрямих впливів вершини K_{15} на вершину K_{14}

$P(K_{15}, K_{14})$	$I_P(0)$	$I_P(1)$	$I_P(2)$	$I_P(3)$	$I_P(4)$
$(K_{15}, K_{22}, K_{15}, K_{14})$	0	0	0	0,342	0,342
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{14})$	0	0	0	0,05	0,05
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{14})$	0	0	0	0,004	0,004
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0,0004	0,0004
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,02	0,02
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,0003	0,0003
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,01	0,01

Продовження таблиці 4.1

$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{15}, K_{14})$	0	0	0	0,01	0,01
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0,023	0,023
$(K_{15}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0,004	0,004
$(K_{15}, K_{22}, K_{20}, K_{15}, K_{14})$	0	0	0	0,03	0,03
$(K_{15}, K_{18}, K_{16}, K_{22}, K_{15}, K_{14})$	0	0	0	0,192	0,192
$(K_{15}, K_{22}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,006	0,006
$(K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,008	0,008
$(K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,075	0,075
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,009	0,009
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{15}, K_{14})$	0	0	0	0,013	0,013
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,004	0,004
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0,0002	0,0002
$(K_{15}, K_{18}, K_{15}, K_{14})$	0	0,456	0,456	0,456	0,456
$(K_{15}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0,160	0,160	0,160	0,160
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{15}, K_{14})$	0	0,06	0,06	0,06	0,06
$(K_{15}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0,157	0,157	0,157	0,157
$(K_{15}, K_{18}, K_{13}, K_{16}, K_{15}, K_{14})$	0	0,078	0,078	0,078	0,078
$(K_{15}, K_{18}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0,01	0,01	0,01	0,01
$(K_{15}, K_{18}, K_{16}, K_{15}, K_{14})$	0	0,228	0,228	0,228	0,228

Таблиця 4.2

Значення непрямих впливів вершини K_{15} на вершину K_{14} через вершину K_{17}

$P(K_{15}, K_{14})$	$I_P(0)$	$I_P(1)$	$I_P(2)$	$I_P(3)$	$I_P(4)$
(K_{15}, K_{17}, K_{14})	0	0	0	0,76	0,76
$(K_{15}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0,274	0,274
$(K_{15}, K_{18}, K_{17}, K_{14})$	0	0	0	0,456	0,456
$(K_{15}, K_{18}, K_{12}, K_{17}, K_{14})$	0	0	0	0,259	0,259
$(K_{15}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0,128	0,128
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{17}, K_{14})$	0	0	0	0,072	0,072
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0,048	0,048

Продовження таблиці 4.2

$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0,04	0,04
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,004	0,004
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,0003	0,0003
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0,016	0,016
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{17}, K_{14})$	0	0	0	0,02	0,02
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,0002	0,0002
$(K_{15}, K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0,125	0,125
$(K_{15}, K_{18}, K_{13}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0,063	0,063
$(K_{15}, K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0,157	0,157
$(K_{15}, K_{18}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,008	0,008
$(K_{15}, K_{22}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,024	0,024
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,011	0,011
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0,01	0,01
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{17}, K_{14})$	0	0	0	0,015	0,015
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{17}, K_{14})$	0	0	0	0,005	0,005
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0,002	0,002
$(K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,018	0,018
$(K_{15}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0,182	0,182
$(K_{15}, K_{18}, K_{16}, K_{17}, K_{14})$	0	0	0	0,274	0,274
$(K_{15}, K_{18}, K_{16}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0,153	0,153
$(K_{15}, K_{22}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,005	0,005

Продовження таблиці 4.2

$(K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,006	0,006
$(K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0,06	0,06
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{17}, K_{14})$	0	0	0	0,075	0,075
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0,008	0,008
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0,01	0,01
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,003	0,003
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0,001	0,001
$(K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0,0001	0,0001

Знайдемо сумарний вплив $T_{(K_{15}, K_{14})}$ вершини K_{15} на вершину K_{14} з врахуванням впливу усіх шляхів, скориставшись рекурсивною формулою [125]:

$$T_{(i,\,j)}(t) = \sum_{k \in N^{-}(j)} \max_{P \in P(i,\,k,\,j)} I_P(t) \qquad (4.5)$$

Таким чином, отримаємо:

$$T_{(K_{15},\,K_{14})}(t) = \max_{P \in P(K_{15},\,K_{18},\,K_{15},\,K_{14})} I_P(t) + \max_{P \in P(K_{15},\,K_{17},\,K_{14})} I_P(t) = (0; 0.456; 0.456; 0.456; 0.456) + (0; 0; 0; 0.76; 0.76) =$$
$$= (0;\ 0.456;\ 0.456;\ 1.216;\ 1.216),$$

тобто в моменти часу $t = 0, 1, 2, 3, 4$ значення $T_{(K_{15},\,K_{14})}(t)$ дорівнюють, відповідно: 0, 0.456, 0.456, 1.216, 1.216.

Аналогічним чином визначимо вплив концепта K_{16} – захищеність КМ на K_{14} – захищеність КІ.

Задамо початковий вектор стану вершин:

$\psi_\Omega(0) = (0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0)$, тоді отримаємо такий процес:

$\psi_\Omega(0) \times W_\Omega = (0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0.5; 0; 0.6; 0.4; 0; 0; 0; 0.7; 0; 0.85; 0; 0; 0),$

$\psi_\Omega(1) = (1; 1; 1; 1; 1; 1; 1; 1; 0; 0; 1; 1; 1; 0; 0; 1; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 0),$

$\psi_\Omega(1) \times W_\Omega = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; 0.25; -1; -0.35; 0; 2.6; 1.6; 1.8; 0.4; -2;$
$-0.1; -0.1; 1.3; 1.2; 0.85; 0.3; 0.5; 0.2)$,

$\psi_\Omega(2) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 0; 1; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 0),$

$\psi_\Omega(2)\times W_\Omega = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.15; 0; 3.3; 2; 2.5; 1; -1.1; 0.3; 0.1; 1.5; 1.2; 1.3; 1.2; 1.4; 1.1)$,

$\psi_\Omega(3) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 1; 1; 0; 1; 1; 1; 1; 0; 1; 1; 1; 0; 1)$,

$\psi_\Omega(3)\times W_\Omega = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.6; 0.95; 3.3; 1.9; 3.3; 1.6; -1.1; 0.3; 0.1; 2.1; 0.95; 1.3; 1.2; 2.1; 1.1)$,

$\psi_\Omega(4) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$,

$\psi_\Omega(4)\times W_\Omega = (0; -0.4; -0.65; -0.6; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.6; 1.9; 3.9; 0.95; 3.3; 0.95; -1.1; 0.45; 0.2; 2.1; 0.2; 1.3; 1.2; 2.1; 1.3)$,

$\psi_\Omega(5) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$,

$\psi_\Omega(5)\times W_\Omega = (0; -1; -0.3; -0.2; 0.85; -2; -1.2; 0; 2.3; 1.3; -0.45; -1; -0.6; 1.9; 3.9; 0.95; 3.3; 0.95; -1.1; 0.45; 0.2; 2.1; 0.2; 1.3; 1.2; 2.1; 1.3)$,

$\psi_\Omega(6) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$.

У момент $t = 5$ процес стабілізується.

Визначивши непрямі впливів вершини K_{16} на вершину K_{14} (додаток Б), знайдемо сумарний вплив $T_{(K_{16}, K_{14})}$ концепта K_{16} на концепт K_{14}:

$$T_{(K_{16}, K_{14})}(t) = \max_{P\in P(K_{16}, K_{15}, K_{14})} I_P(t) + \max_{P\in P(K_{16}, K_{17}, K_{14})} I_P(t) = (0; 0; 0; 0.475; 0.475; 0.475) + (0; 0; 0; 0; 0.57; 0.57) =$$
$$= (0; 0; 0; 0.475; 1.045; 1.045),$$

тобто в моменти часу $t = 0, 1, 2, 3, 4, 5$ значення $T_{(K_{16}, K_{14})}(t)$ дорівнюють, відповідно: 0, 0, 0, 0.475, 1.045, 1.045.

На основі отриманих даних з використанням програмного засобу Microsoft Excel побудуємо графік, що демонструє динамічний вплив концепта K_{15} – захищеність системи ЗІ та K_{16} – захищеність КМ на K_{14} – захищеність КІ (рис. 4.1).

На графіку на осі абсцис відкладено час, а на осі ординат – рівень впливу досліджуваних концептів на захищеність КІ в умовних одиницях.

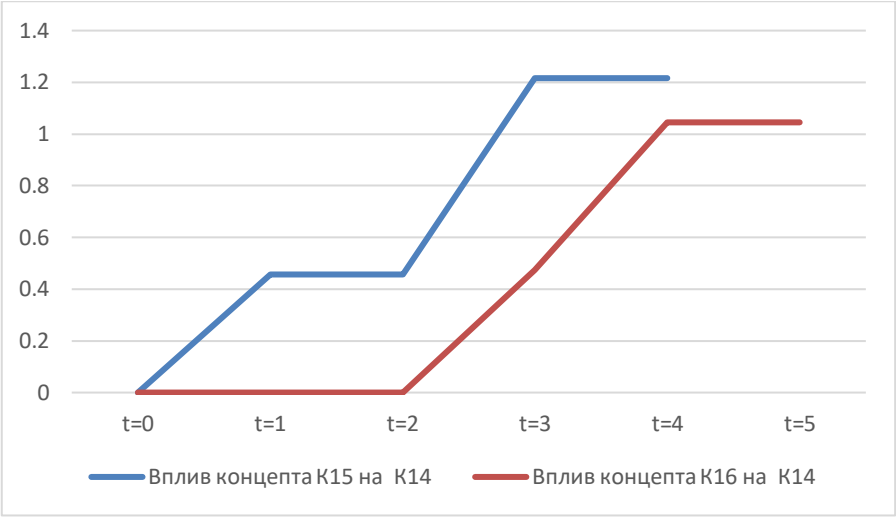


Рисунок 4.1 – Динамічний вплив концептів K_{15} та K_{16} на захищеність КІ

Для автоматизації динамічного моделювання аналізу впливу концептів розроблено програмний засіб, який надає змогу зменшити час на опрацювання даних та збільшити швидкість їхньої обробки.

З метою відображення динамічного впливу концептів K_{15} – захищеність системи ЗІ та K_{16} – захищеність КМ на K_{14} – захищеність КІ необхідно задати досліджувані концепти, матрицю взаємовпливів та визначити час стабілізації процесу (рис. 4.2).

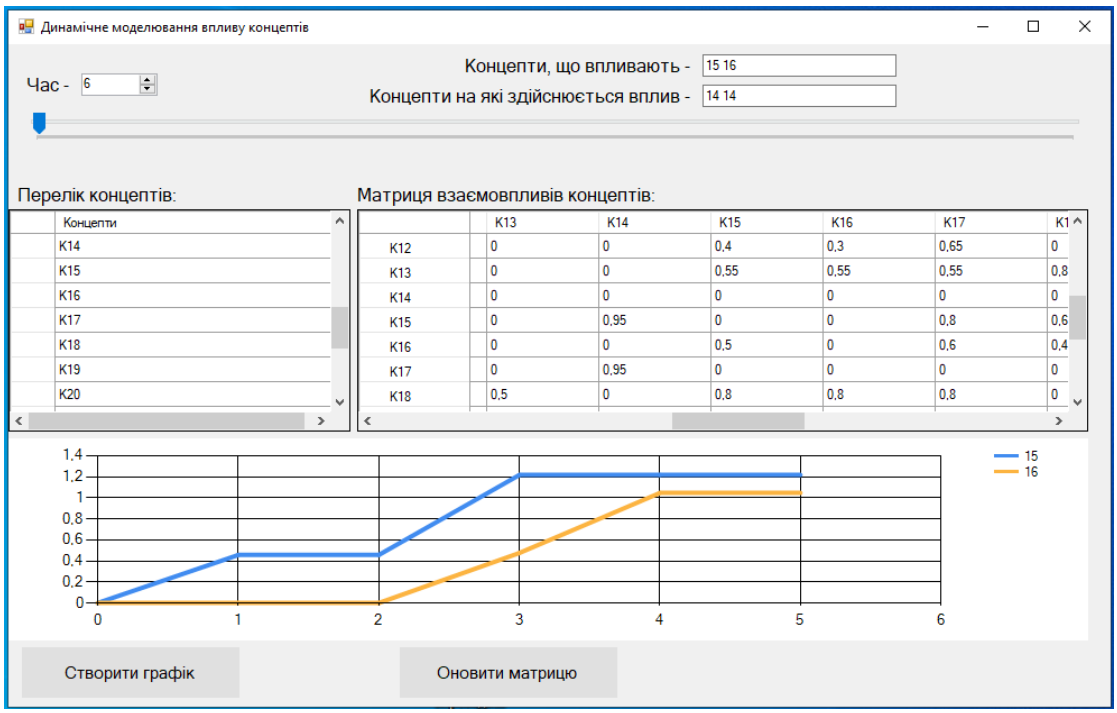


Рисунок 4.2 – Головне вікно розробленого програмного засобу

Проаналізувавши даний графік, можна зробити висновок, що концепт K_{15} має не нульовий вплив на захищеність КІ при $t=1$, а концепт K_{16} при $t=3$, при чому у даний момент часу рівень впливу K_{15} збільшиться на 0,76 умовних одиниць. Сумарний вплив концептів стабілізується при $t=5$, а починаючи з $t=4$ спостерігатиметься максимально можливий вплив даних концептів.

Крім того, даний графік наглядно демонструє більший рівень впливу концепта K_{15} на захищеність КІ, порівняно з концептом K_{16} у різні моменти часу. Даний результат збігається з тим, що був отриманий в наслідок проведеного сценарного моделювання у другому розділі роботи. Це, у свою чергу, підтверджує достовірність раніше отриманих результатів.

Отримані дані дозволяють спрогнозувати розвиток ситуації у конкретні моменти часу, що сприятиме забезпеченню стійкого, ефективного та безпечного функціонування об’єкта КІ.

4.2 Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності систем захисту інформації

Проведений динамічний часовий аналіз дозволяє розглянути та порівняти вплив одних концептів досліджуваної системи на інші, проте не надає змогу дослідити еволюційний розвиток системи в цілому. Дану задачу можна вирішити за допомогою імпульсного моделювання [80], при якому об’єкт дослідження розглядається як сукупність взаємодіючих між собою динамічних процесів, що протікають у реальному часі. При цьому для розгляду можливих тенденцій розвитку системи, у вершину (або сукупність вершин) когнітивної карти вносяться збурення – імпульси, які розповсюджуються по карті.

Змоделюємо імпульсні процеси розповсюдження збурень, введених почергово в усі вершини запропонованої у другому розділі НКК для визначення рівня захищеності системи ЗІ.

Вирішимо поставлене завдання за допомогою матриці транзитивного замикання *м* [80]:

$$M = E + W + W^2 + ... + W^n, \tag{4.6}$$

де W – матриця суміжності НКК;

n – порядок матриці W.

Для досліджуваної когнітивної моделі матриця транзитивного замикання M матиме вигляд (табл. 4.3).

Таблиця 4.3

Матриця транзитивного замикання НКК для визначення рівня захищеності системи ЗІ

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	1	0	0	0	0	0	0	0	0	0	0,9
K_2	0	1	0	0	0	0	0	0	0	0	0,85
K_3	0	0	1	0	0	0	0	0	0	0	-0,75
K_4	0	0,13	0	1	0	0	0	0,5	0	0	1,1
K_5	-0,55	-0,93	0,82	-0,75	1	0	0	-0,93	0	0	-2,9
K_6	0,84	1,1	-1,1	0,93	0	1	-0,3	1,3	0	0	3,8
K_7	-0,45	-0,49	0,58	-0,42	0	0	1	-0,76	0	0	-2
K_8	0	0,25	0	0	0	0	0	1	0	0	0,76
K_9	0,46	0,59	-0,59	0,51	0	0,55	-0,17	0,73	1	0	2,1
K_{10}	-0,35	-0,27	0	-0,5	0	0	0	-1,1	0	1	-1,5
K_{11}	0	0	0	0	0	0	0	0	0	0	1

Для простого імпульсного процесу з початковою вершиною K_i імпульс обчислюється таким чином [80]:

$$p_j(t) = \{\textit{елемент i, j матриці } W^n\}, \tag{4.7}$$

а значення вершини K_j в дискретні моменти часу $t = 0, 1, 2, ...m$ визначається за формулою:

$$V_j(t) = V_j(0) + \{\textit{елемент i, j в матриці } E + W + W^2 + ... + W^n\}. \tag{4.8}$$

Враховуючи формулу (4.8) та значення елементів матриці транзитивного замикання, для простого імпульсного процесу з початковою вершиною K_1 – захист від витоку технічними каналами (при нульових початкових умовах) отримаємо збільшення концепту K_{11} – захищеність системи ЗІ до 0,9. Якщо ж в якості початкової вершини розглядати K_2 – захист каналу передавання інформації, то спостерігатиметься збільшення захищеності до 0,85. Проте, взявши

за початкову вершину K_3 – розголошення інформації персоналом, отримаємо зменшення значення концепту K_{11} до 0,75.

Крім того, імпульсне моделювання надає можливість, вносячи збурення в усі вершини досліджуваної когнітивної карти почергово, переглянути еволюційний шлях системи, перехід її з одного стану в інший та визначити ті концепти, які найбільше послаблюватимуть або ж підсилюватимуть захищеність системи ЗІ. Виходячи з цього, проведено аналіз значень елементів матриці транзитивного замикання досліджуваної НКК, який показав, що при внесенні імпульсу в концепт K_6 – організаційне забезпечення ЗІ, концепт K_{11} – захищеність системи ЗІ збільшиться до максимального значення – 3,8. З метою наочного представлення реакції системи ЗІ на проходження цього імпульсного процесу, скористаємося розробленим програмним засобом. Для цього необхідно задати у відповідні комірки головного вікна матрицю суміжності, кількість ітерацій, ввести імпульс у відповідну вершину та натиснути кнопку «Створити графік» (рис. 4.3).

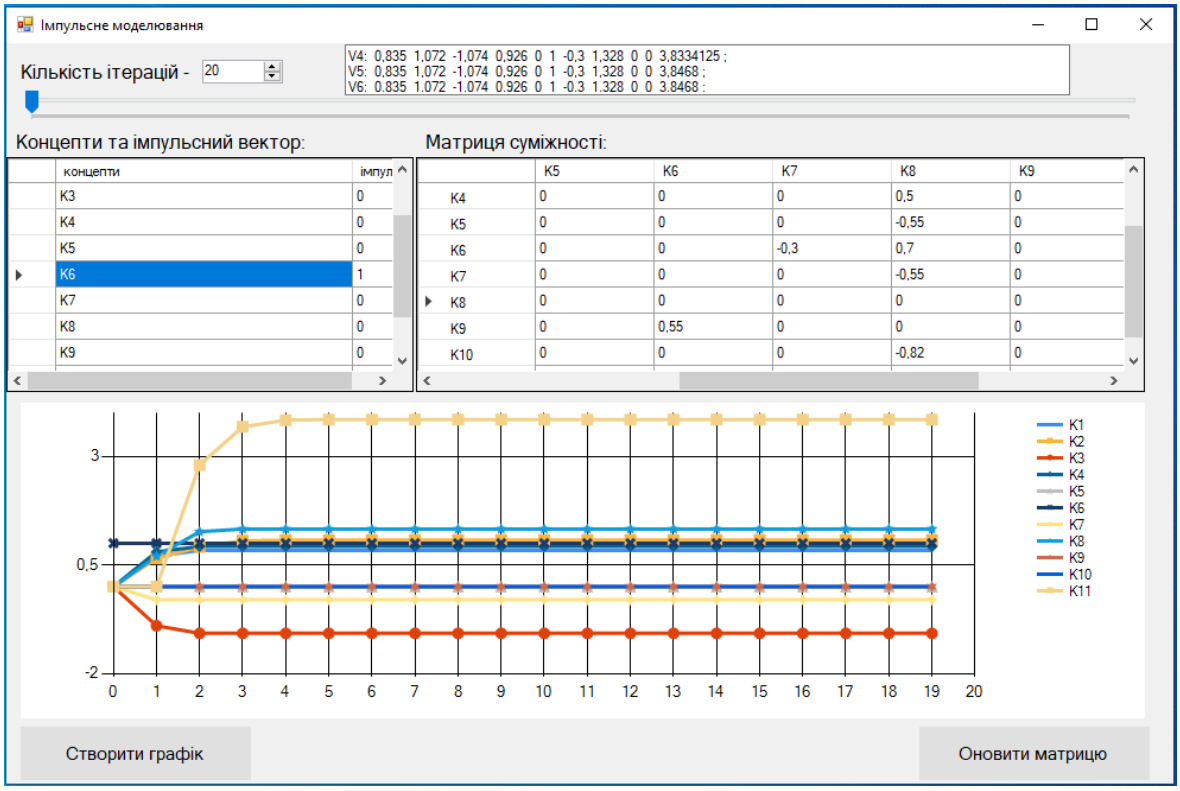


Рисунок 4.3 – Стан концептів досліджуваної системи при введенні імпульсу у K_6

Аналіз графіку представленого на рис. 4.3 показав, що K_{11} – захищеність системи ЗІ зростатиме до п’ятої ітерації, а далі процес стабілізується, при чому спостерігатиметься збільшення значень таких концептів як: K_1 – захист від витоку технічними каналами (до 0,84), K_2 – захист каналу передавання інформації (до 1,1), K_4 – фізичний захист (до 0,93), K_8 – надійність, відмовостійкість технічних та програмних засобів (до 1,3). Водночас, зменшиться значення двох концептів: K_3 – розголошення інформації персоналом (до 1,1) та K_7 – ненавмисні дії, помилки обслуговуючого персоналу (до 0,3).

Водночас, аналіз матриці транзитивного замикання показав, що концепт K_{11} – захищеність системи ЗІ максимально послабиться (до 2,9) при внесенні імпульсу у K_5 – НСД до інформації зловмисником. Водночас спостерігатиметься така зміна досліджуваної системи (рис. 4.4).

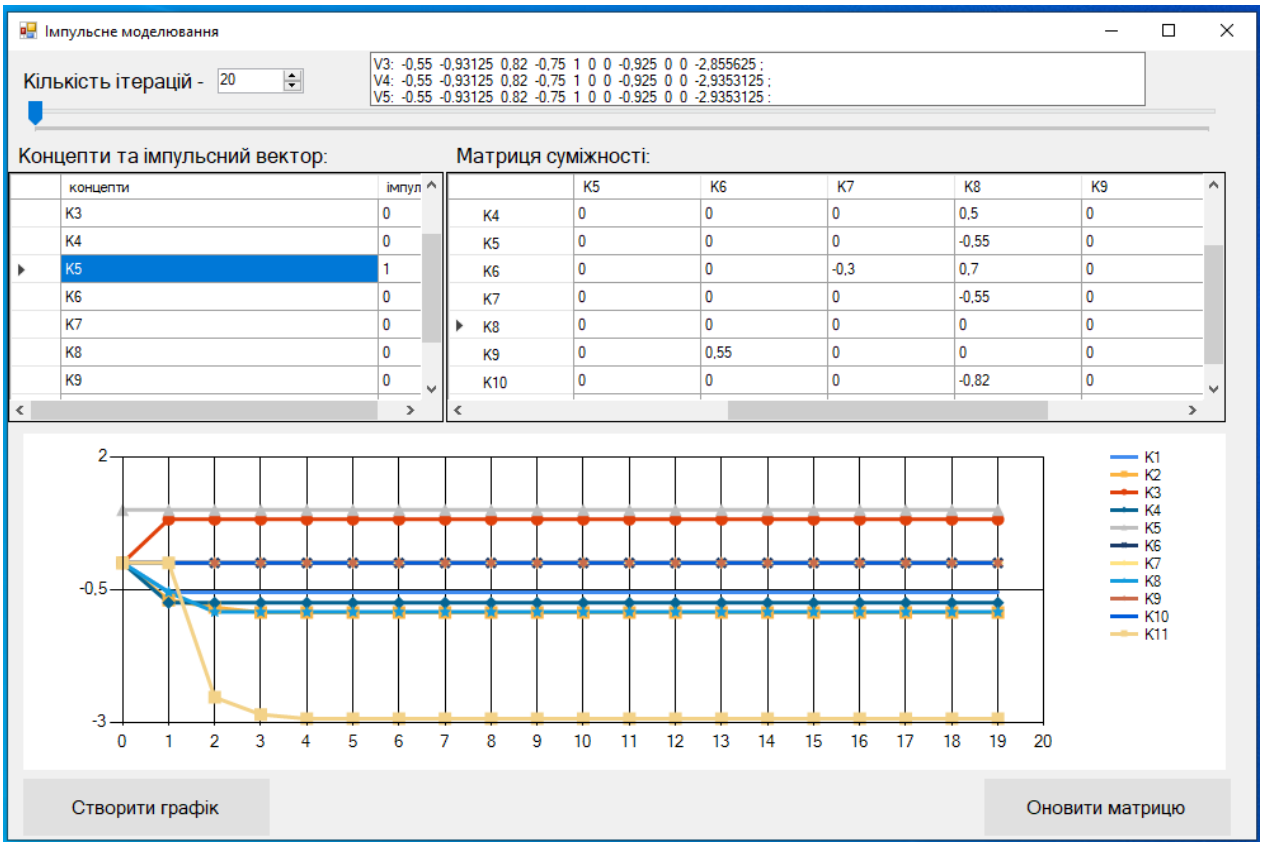


Рисунок 4.4 – Стан концептів досліджуваної системи при введенні імпульсу у K_5

Аналіз даного графіка свідчить про те, що K_{11} – захищеність системи ЗІ знижується до четвертої ітерації, а далі процес стабілізується, при чому

спостерігатиметься зменшення значень таких концептів як: K_1 – захист від витоку технічними каналами (до 0,55), K_2 – захист каналу передавання інформації (до 0,93), K_4 – фізичний захист (до 0,75) та K_8 – надійність, відмовостійкість технічних та програмних засобів (до 0,93). Разом з тим збільшиться значення концепту K_3 – розголошення інформації персоналом (до 0,82).

Таким чином, при введені імпульсів у концепти K_6 – організаційне забезпечення ЗІ та K_5 – НСД до інформації зловмисником, захищеність системи ЗІ набуває екстремальних значень. Отже, дані концепти є найвагомішими концептами досліджуваної системи, що також підтверджується результатами отриманими у другому розділі роботи внаслідок проведення структурно-топологічного аналізу когнітивної карти.

Одержані результати сприятимуть підвищенню якості прогнозування розвитку ситуації, що дозволить вчасно прийняти необхідні рішення та заходи для забезпечення захищеності систем ЗІ.

4.3 Розробка структури та модулів програми для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах

Для оцінювання впливу загроз на рівень захищеності досліджуваних систем за когнітивними моделями, доцільно реалізувати програмний засіб у вигляді таких взаємозалежних програмних модулів:

1. Модуль створення концептів.

2. Модуль створення і присвоєння сили зв’язку між концептами.

3. Модуль побудови матриці суміжності концептів (встановлення взаємних впливів концептів).

4. Модуль візуалізації та редагування моделі.

5. Модуль обчислення системних показників для дослідження поведінки і стійкості побудованої карти (щільність зв’язків НКК, ступінь впливу вхідних, вихідних зв’язків, центральність концептів, індекс ієрархії, оцінка складності, кількість концептів типу «Driver» – концепти, які впливають на інші, а на них не

впливає жоден із концептів системи, «Receiver» – концепти на які впливають, проте вони не мають жодного впливу на концепти НКК, «Ordinary» – концепти, які впливають і на яких впливають інші концепти системи).

6. Модуль динамічного часового аналізу, на основі створеної когнітивної моделі.

7. Модуль дослідження імпульсних процесів на когнітивній карті.

Враховуючи послідовність вищеописаних взаємозалежних програмних модулів пропонується розробка загальної структури програми, яка показана на рис. 4.5.

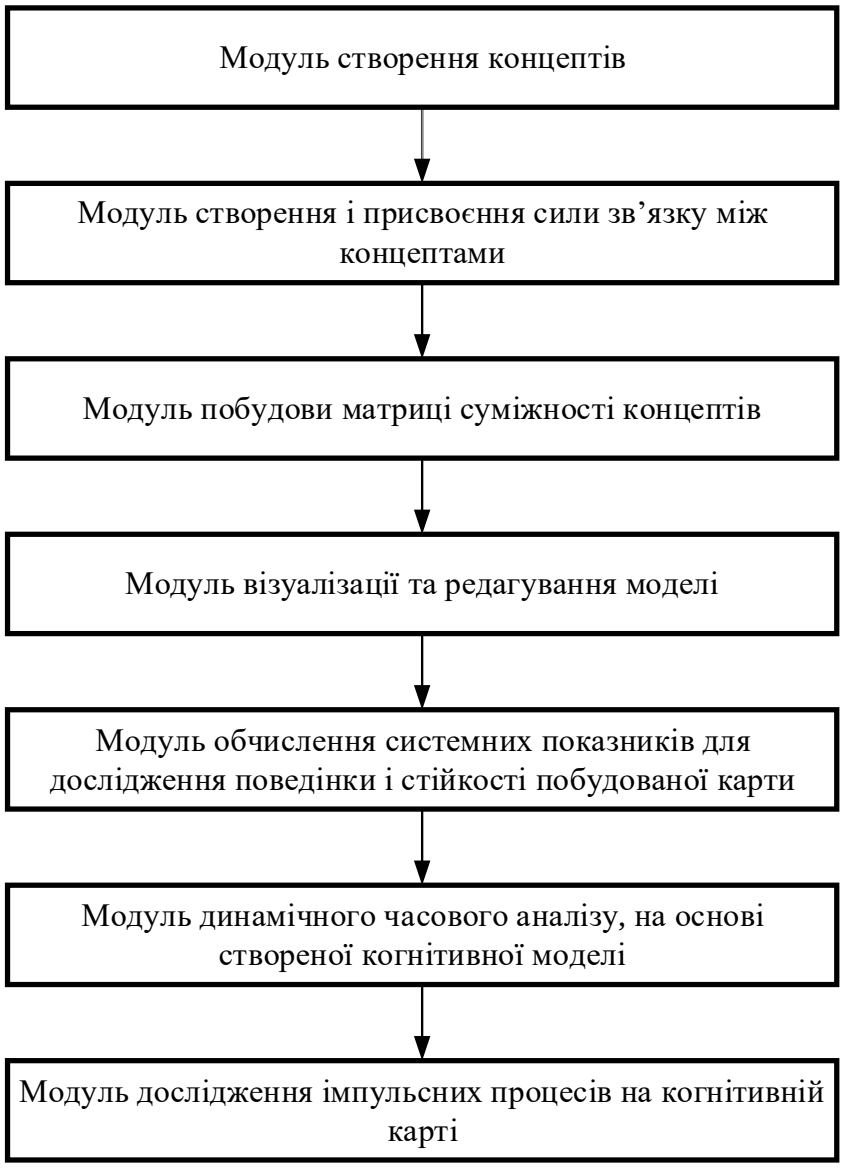


Рисунок 4.5 – Загальна структура програми

Усі модулі розроблюваної програми мають бути взаємозалежними, оскільки зміни будь-якого з її компонентів, повинні коректно відображатись на усіх інших.

Варто зазначити, що особливістю модулю створення концептів є те, що когнітивна карта може містити безліч концептів. Тому обов'язковою вимогою для забезпечення масштабування досліджуваних когнітивних карт має бути можливість додавання від двох і більше концептів.

Особливістю модулю побудови матриці взаємовпливів концептів має бути її гнучкість та легкість в редагуванні. Оскільки модулі програми є взаємозалежними, то матриця будується автоматично, базуючись на доданих концептах та створених на попередньому етапі роботи програми зв'язках. Тому необхідно забезпечити автоматичне оновлення матриці взаємозв'язків концептів, у разі змін когнітивної карти.

Модуль створення і присвоєння сили зв'язку між концептами, відповідає за встановлення значення сили впливу одного концепту на інший в діапазоні значень [-1, 1].

Модуль візуалізації та редагування моделі використовується для наочного представлення та внесення змін в досліджувану когнітивну карту.

Модуль обчислення системних показників для дослідження поведінки і стійкості побудованої карти відповідає за розрахунок таких параметрів як щільність, ступінь впливу вхідних, вихідних зв'язків, центральність, індекс ієрархії, оцінка складності, кількість концептів типу «Driver», «Receiver», «Ordinary». Іншим важливим показником для обчислення є складність, що представляє собою співвідношення кількості концептів типу «Receiver» до концептів типу «Driver». Усі підрахунки вищеперерахованих показників варто проводити за формулами описаними в другому розділі дисертаційної роботи.

Модуль динамічного аналізу відповідає за побудову графіку непрямого впливу досліджуваних концептів у часі, використовуючи апарат динамічної каузальної алгебри, що було описано у даному розділі.

Модуль дослідження імпульсних процесів на когнітивній карті дозволяє дослідити еволюційний розвиток системи та для наочності відображає отриманий

результат за допомогою графіка і текстового поля.

Згідно запропонованої структури програми, реалізацію доцільно проводити у вигляді додатку Windows Forms на мові програмування C# з використанням платформи .Net Framework.

Крок 1. Спочатку необхідно реалізувати модуль створення концептів. Створимо клас $Vertex$ який буде зберігати у собі усю інформацію про концепт:

```
class Vertex
   {
      public Vertex(string n, Rectangle r, int i, PictureBox pB)
      {
         name = n;
         rect = r;
         id = i;
         pictureBox = pB;
         …
      }
         private void MyTextBox_TextChanged(object sender, EventArgs e)
      {
         name = myTextBox.Text;
      }
}
```

При створенні концепту потрібно вказати його назву ($name$), координати та розмір ($rect$), ідентифікатор (id) та передати об’єкт $pictureBox$ на якому і буде зображений концепт. Останнє потрібно для того, щоб додати на екран користувача об’єкт $textBox$ який буде відображати назву концепту та за допомогою якого можна буде її редагувати. Метод $MyTextBox\_TextChanged$ виконується при зміні користувачем значення $textBox$ та записує нову назву до змінної $name$. Метод $renewal$ синхронізує координати $textBox$ з координатами концепту. І останній метод $remove$ видаляє $textBox$ концепту.

Далі напишемо метод $createVertex$, що буде створювати новий концепт та додавати до змінної $graph$ яка і буде зберігати усі концепти та зв'язки:

```
public void createVertex(string name)
      {
         Vertex V = new Vertex(name,
            new Rectangle(100 + vertexCounter * 10, 100 + vertexCounter * 10, 100, 30),
            vertexCounter,
            pictureBox);
         graph.Vertex.Add(V);
         pictureBox.Invalidate();
```

```
            graph.initializeMatrix();
            vertexCounter++;
        }
```

Крок 2. Наступним кроком потрібно реалізувати модуль створення зв'язків між концептами. Для цього створимо клас $Edge$ який буде містити інформацію про початковий та кінцевий концепт, а також силу зв'язку між ними:

```
class Edge {
    public void IniInitialize(PictureBox pB)
    {
        …
        pictureBox?.Controls.Add(myNumericUpDown);
    }
    private void MyNumericUpDown_ValueChanged(object sender, EventArgs e)
    {
        weight = (double)myNumericUpDown.Value;
    }
    public void renewalNumericLocation()
    {
        myNumericUpDown.Location = new Point(
            (startVertex.rect.X + endVertex.rect.X) / 2,
            (startVertex.rect.Y + endVertex.rect.Y) / 2
            );
    }
}
```

Як і в попередньому класі ми передаємо об'єкт $pictureBox$ для створення регулятора, але робимо це за допомогою окремого методу $IniInitialize$. Метод $MyNumericUpDown\_ValueChanged$ виконується при змінні показників регулятора, та записує нові данні у вагу зв'язку, а саме у змінну $weight$, в той час як метод $renewalWeight$ робить усе навпаки. Це потрібно для того, щоб при змінні ваги матриці взаємовпливів, змінювалися і показники лічильника. Метод $renewalNumericLocation$ оновлює координати регулятора, завжди розміщуючи його між початковим та кінцевим концептами. Останній метод у даному класі $remove$, він видаляє регулятор з $pictureBox$.

Крок 3. На цьому етапі необхідно реалізувати модуль побудови матриці взаємовпливів концептів. Створюємо клас $Graph$ який містить усю інформацію про додані зв'язки та концепти, а також будує матрицю суміжності:

```
class Graph
  {
    public Graph()
    {
```

```
        Vertex = new List<Vertex>();
        Edge = new List<Edge>();
    }
    public void initializeMatrix()
    {
        ...
    }
    public void Clear()
    {
        while (Vertex.Count != 0)
        {
            deleteVertex(0);
        }
        initializeMatrix();
    }
}
```

Метод $initializeMatrix$ заповнює матрицю взаємовпливів на основі концептів записаних у змінній $Vertex$ та доданих зв'язків у змінній $Edge$, також даний метод перевіряє вагу зв'язків та видаляє їх якщо вони рівні нулю. Метод $deleteVertex$ видаляє заданий концепт по id та усі зв'язки, що містили у собі цей концепт. Метод $clear$ видаляє усі зв'язки та концепти.

Крок 4. Реалізуємо модуль візуалізації та редагування моделі. Створимо клас $Drawing$, він буде відповідати за візуальне відображення усієї матриці та її редагування. Розглянемо деякі методи цього класу. Метод $panelDrawVertex\_Paint$ викликається при оновлені $pictureBox$ тим самим виводячи на дисплей користувача концепти та зв'язки між ними. Даний метод малює усі вершини та зв'язки, що знаходяться у об'єкті $graph$.

```
class Drawing
  {
    private void panelDrawVertex_Paint(object sender, PaintEventArgs e)
    {
        ...
    }

    private void PictureBox_CreateEdge(object sender, MouseEventArgs e)
    {
        ...
    }
   ...
  }
```

Метод $PictureBox\_CreateEdge$ у свою чергу створює зв'язок між вибраними концептами.

Крок 5. Даний програмний модуль відповідає за автоматичний обрахунок системних показників, щільність, ступінь впливу вхідних, вихідних зв'язків, центральність, індекс ієрархії, оцінка складності, кількість концептів типу «Driver», «Receiver», «Ordinary». Він реалізується класом $Statistics$ і має лише один метод $createStatistics$, що приймає змінну типу $Graph$, і на основі отриманих даних вираховує усі показники. Розглянемо частину коду:

```
class Statistics
  {
    public void createStatistics(Graph g)
    {
      driverComponents = 0;
      receiverComponents = 0;
      ordinaryComponents = 0;

      totalComponents = g.Vertex.Count;
      totalConnection = g.Edge.Count;
      density = (double)totalComponents / (double)(totalConnection * (totalConnection
- 1));

      ...

    }
  }
```

Метод даного класу нічого не повертає і має лише публічні змінні, у яких і зберігаються розраховані дані, які, в свою чергу, використовуються у головному класі $mainForm$ для виведення на екран користувача.

Крок 6. Модуль динамічного часового аналізу реалізується класом $DynamicModelingOfTheImpactOfConcepts$ і має дуже багато методів для обробки динамічного часового аналізу. Розглянемо основний метод $DynamicModelingOfTheImpactOfConcepts$ та метод обходу графа у глибину dfs:

```
class DynamicModelingOfTheImpactOfConcepts
{
  public ImpactSchedule calculationOfDynamicTimeAnalysis (Graph g, int time, Vertex
startV, Vertex endV)
  {
    ImpactSchedule result = new ImpactSchedule();
```

```
        ways = new List<int[]>();
        r = new List<int>();
        …
        dfs(startV.id, endV.id);
        …
        return result;
      }
      private void dfs(int v, int end)
      {
        …
      }
}
```

Метод dfs це рекурсивний метод обходу графа в глибину. Наш клас має такі глобальні змінні як $adjacencyMatrix$, що представляє собою матрицю взаємовпливів концептів, $used$ це масив який потрібен для роботи dfs і позначає пройдені концепти. Інші змінні зберігають масиви інформації для розрахунку сумарного впливу, який відображатиметься на графіку.

Крок 7. Модель імпульсного моделювання представлена класом $CognitiveModeling$. Даний клас має у собі три методи, основний з яких $Modeling$, інші розроблено для проведення розрахунків:

```
class CognitiveModeling
  {
    public List<double[]> Modeling(double[] P, Graph g, int iter)
    {
      …
      return masResult;
    }
    double[] PulseCunculation(double[,] matrix, double[] V, double[] P)
    {
      …
    }
    double[] PulseRewrite(double[] V, double[] V_1, double[,] matrix )
    {
      …
    }
}
```

Таким чином, розроблено програмні модулі запропонованого додатку для оцінювання впливу загроз на рівень захищеності досліджуваних систем за когнітивними моделями (Додаток В).

4.4 Застосування програмних модулів створеного додатку для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах

Для запуску та перегляду додатку, користувачеві достатньо лише відкрити програму, що представляє собою звичайний .exe файл, після чого відбудеться завантаження усіх необхідних модулів та відкриється головне вікно програми (рис. 4.6).

Рисунок 4.6 – Головне вікно додатку

Після завантаження додатку користувачеві буде доступно ряд функцій, а саме: «Додати концепт», «Відкрити» попередньо збережену когнітивну карту або «Зберегти» поточну, «Очистити усі дані».

Для того, щоб розпочати побудову нової когнітивної карти, достатньо натиснути на кнопку «Створити концепт» та ввести назву для новоствореного концепту, або залишити автоматично створену назву, що виглядає як «K(n)» де n-номер створеного концепту. Приклад створеної когнітивної карти зображено на рис. 4.7.

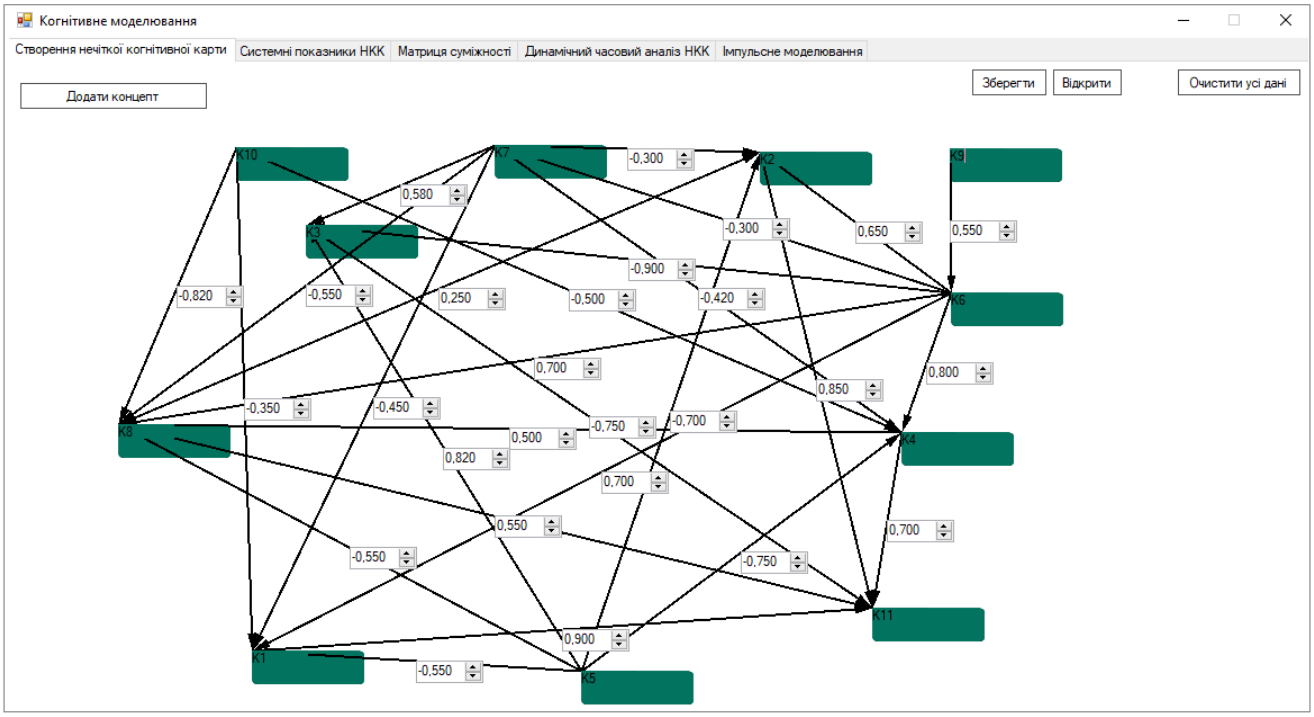
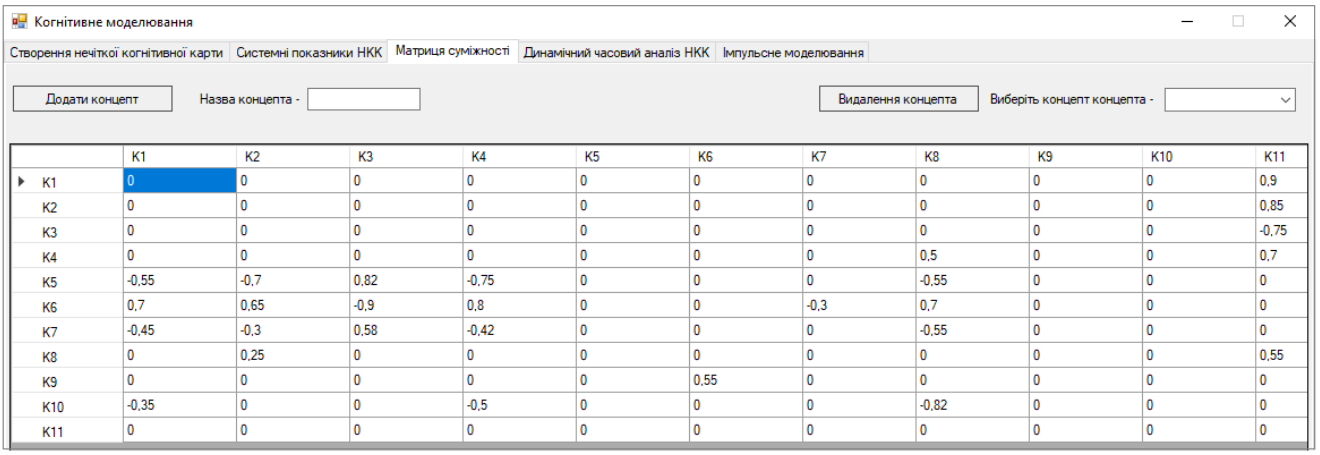


Рисунок 4.7 – Приклад створеної когнітивної карти

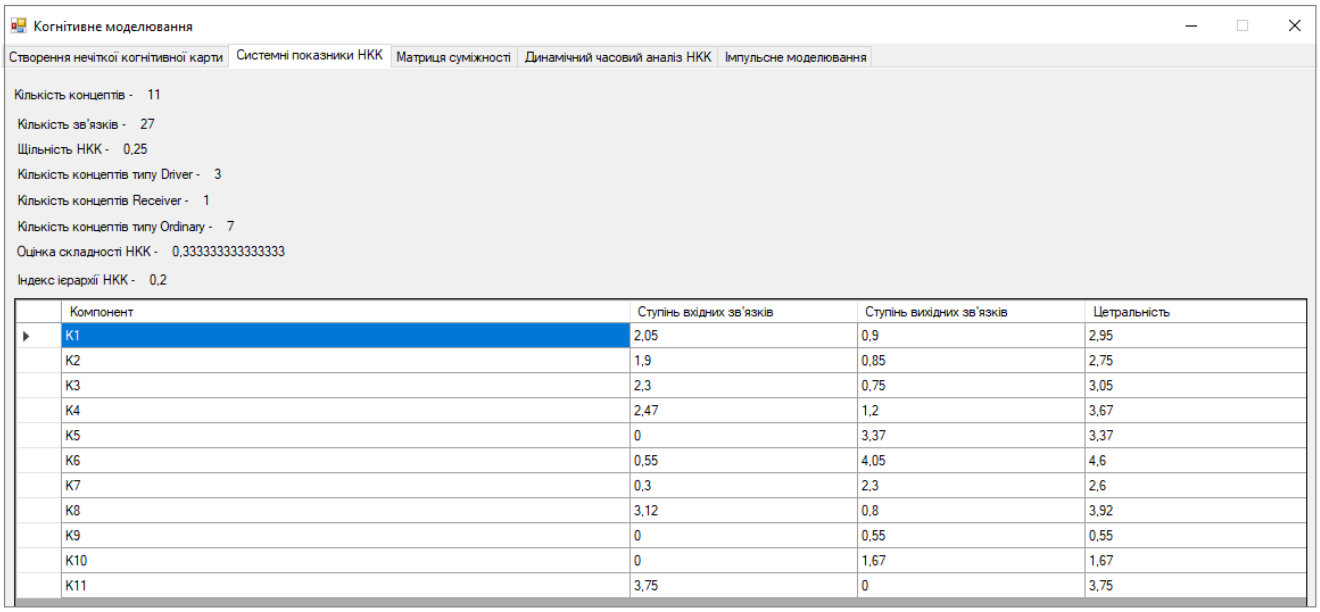
З’єднавши концепти між собою вказівними лініями, додаток автоматично будує матрицю взаємовпливів концептів (рис. 4.8), де користувач має змогу присвоїти сили зв’язку у діапазоні значень [-1, 1].



	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
K1	0	0	0	0	0	0	0	0	0	0	0,9
K2	0	0	0	0	0	0	0	0	0	0	0,85
K3	0	0	0	0	0	0	0	0	0	0	-0,75
K4	0	0	0	0	0	0	0	0,5	0	0	0,7
K5	-0,55	-0,7	0,82	-0,75	0	0	0	-0,55	0	0	0
K6	0,7	0,65	-0,9	0,8	0	0	-0,3	0,7	0	0	0
K7	-0,45	-0,3	0,58	-0,42	0	0	0	-0,55	0	0	0
K8	0	0,25	0	0	0	0	0	0	0	0	0,55
K9	0	0	0	0	0	0,55	0	0	0	0	0
K10	-0,35	0	0	-0,5	0	0	0	-0,82	0	0	0
K11	0	0	0	0	0	0	0	0	0	0	0

Рисунок 4.8 – Приклад матриці взаємовпливів концептів

На рис. 4.9 представлено приклад автоматичного обрахунку програмою системних показників (щільність, ступінь впливу вхідних, вихідних зв’язків, центральність, індекс ієрархії, оцінка складності, кількість концептів типу «Driver», «Receiver», «Ordinary»), після встановлення усіх необхідних взаємовпливів концептів.



Компонент	Ступінь вхідних зв'язків	Ступінь вихідних зв'язків	Цетральність
K1	2,05	0,9	2,95
K2	1,9	0,85	2,75
K3	2,3	0,75	3,05
K4	2,47	1,2	3,67
K5	0	3,37	3,37
K6	0,55	4,05	4,6
K7	0,3	2,3	2,6
K8	3,12	0,8	3,92
K9	0	0,55	0,55
K10	0	1,67	1,67
K11	3,75	0	3,75

Рисунок 4.9 – Приклад обрахунку системних показників

Для проведення динамічного часового аналізу потрібно з випадаючих списків вибрати концепт типу «Driver» та «Receiver» і натиснути кнопку «додати шлях». Для вилучення непотрібних шляхів з моделювання динамічного часового аналізу, потрібно обрати даний шлях у випадаючому списку та натиснути кнопку «Вилучити шлях». Для того щоб сформувати графік, потрібно вказати час та натиснути кнопку «Створити графік» (рис. 4.10).

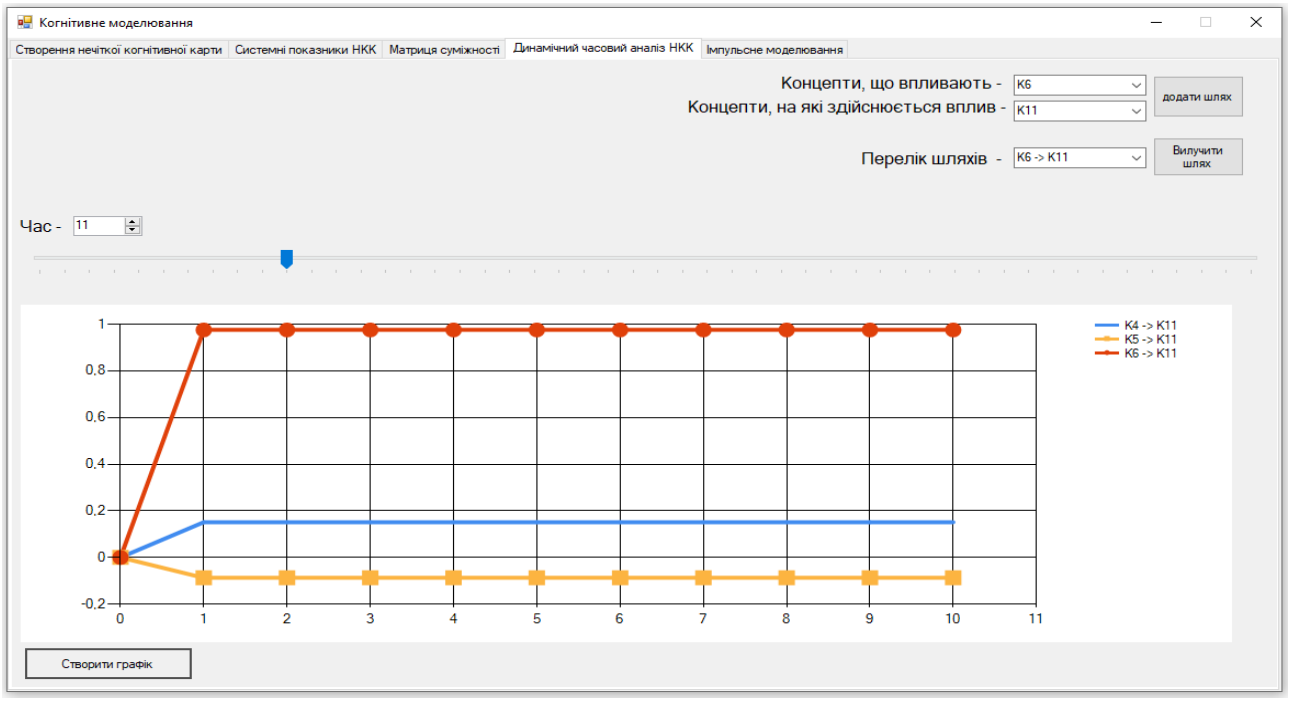


Рисунок 4.10 – Вікно динамічного часового аналізу

Для проведення імпульсного моделювання потрібно задати імпульс у досліджуваний концепт, встановити кількість ітерацій та натиснути на кнопку «Створити графік». Усі розрахунки та значення вершин на кожній з ітерацій показані у текстовому полі зліва та виводяться автоматично (рис. 4.11).

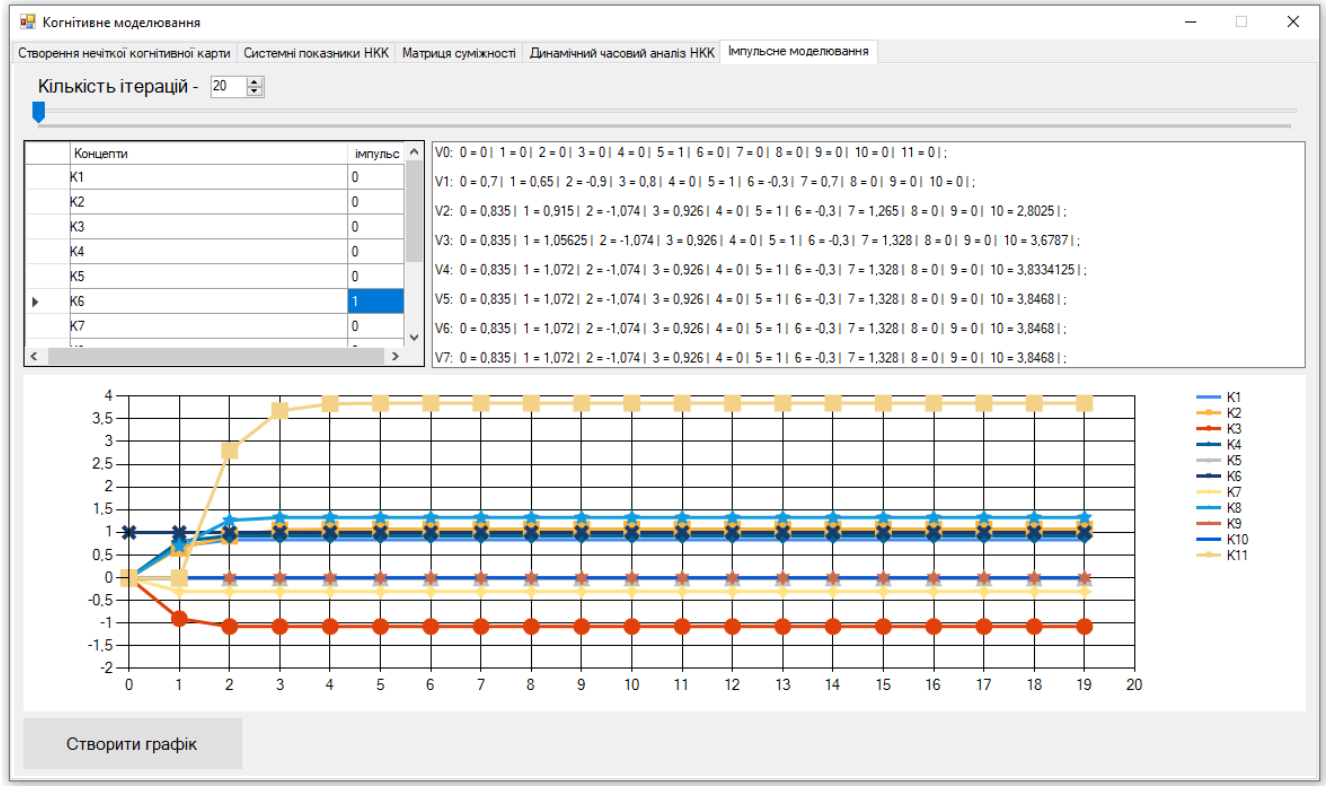


Рисунок 4.11 – Вікно імпульсного моделювання

У результаті виконання усіх запропонованих програмних модулів, отримуються усі необхідні дані для оцінювання впливу загроз на рівень захищеності досліджуваних систем за когнітивними моделями.

4.5 Висновки до розділу 4

У даному розділі проведено аналіз розроблених когнітивних моделей у часі та здійснено розробку ПЗ для оцінювання рівня захищеності систем ЗІ, що циркулює в ІС.

Зокрема, на основі динамічної каузальної алгебри визначено вплив найвагоміших концептів НКК на захищеність об’єкта КІ у різні моменти часу. Задано вектор порогів вершин, який не залежить від часу і відмежовує усі незначні впливи між концептами та вектор стану вершин, у якого досліджувана

вершина активізується ззовні та залишається активною протягом усього процесу. Визначено хвилю, що породжує процес активізації вершин та відповідних шляхів. Встановлено момент часу стабілізації процесу. Обчислено впливи вздовж усіх активізованих шляхів від досліджуваних концептів до цільового, на основі отриманих значень визначено сумарний вплив K_{15} – захищеність системи ЗІ на K_{14} – захищеність КІ в моменти часу $t = 0, 1, 2, 3, 4$: $T_{(K_{15}, K_{14})}(t) = (0; 0.456; 0.456; 1.216; 1.216)$ та сумарний вплив K_{16} – захищеність КМ на K_{14} – захищеність КІ ($t = 0, 1, 2, 3, 4, 5$): $T_{(K_{16}, K_{14})}(t) = (0; 0; 0; 0.475; 1.045; 1.045)$. Отримані дані відображено графічно.

Також проведено дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи ЗІ при впливі потенційних загроз. Побудовано матрицю транзитивного замикання НКК предметної області. Аналіз даної матриці показав, що при внесенні імпульсу в концепт K_6 – організаційне забезпечення ЗІ, концепт K_{11} – захищеність системи ЗІ максимально посилиться (до 3,8), а при внесенні імпульсу у K_5 – НСД до інформації зловмисником, цільовий концепт максимально послабиться (до 2,9). Дані концепти є найвагомішими концептами системи, що також підтверджується результатами отриманими у другому розділі роботи внаслідок проведення структурно-топологічного аналізу досліджуваної когнітивної карти. Використовуючи авторське ПЗ, побудовано графіки, що ілюструють можливі варіанти розвитку ситуацій у віртуальному середовищі.

Крім того, розроблено ПЗ для оцінювання рівня захищеності систем ЗІ на основі когнітивного підходу. Запропоновано структуру програми у вигляді семи взаємозалежних програмних модулів. Згідно запропонованої структури програми, реалізацію проведено у вигляді додатку Windows Forms на мові програмування C# з використанням платформи .Net Framework. Для ефективного та раціонального використання додатку користувачем, продемонстровано застосування програмних модулів, наведено приклад роботи програми.

ВИСНОВКИ

У роботі отримано нове вирішення актуальної наукової задачі, яка полягає у підвищенні рівня захищеності систем ЗІ на основі когнітивного моделювання з використанням НКК, а саме:

1. Розроблено когнітивні моделі для визначення рівня захищеності КМ, системи ЗІ та об'єкта КІ. Запропоновані моделі дозволяють визначити найвагоміші загрози, з точки зору вивчення даної проблеми, та проаналізувати відносну зміну рівня захищеності досліджуваних систем. Проведено структурно-топологічний аналіз побудованих НКК, результати якого свідчать про достатню їхню щільність, складність та демократичність. Визначено концепти, які мають найвищу структурну значимість та здійснено сценарне моделювання, у результаті якого при максимально позитивному впливі даних концептів, визначено, що рівень захищеності КМ підвищиться на 63 %, системи ЗІ – на 19 % та об'єкта КІ – на 2%.

2. На основі множинного регресійного аналізу підтверджено достовірність впливу загроз на рівень захищеності систем ЗІ, що циркулює в ІС, визначеного за сценарним моделюванням на основі когнітивного підходу. Для кожної із розроблених когнітивних моделей знайдено аналітичний вираз лінійної кореляційної залежності, яка існує між найвагомішими її концептами та захищеністю відповідної системи. Розраховано стандартизовані коефіцієнти регресії та коефіцієнти еластичності. Проведений аналіз отриманих значень даних коефіцієнтів надав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

3. Проведено симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта КІ. Побудовано симпліціальний комплекс, що являє собою послідовність симплексів, які впорядковані за правилом спадання їх розмірності. Визначено перший структурний вектор даного комплексу: $Q_x = \{1\,2\,3\,5\,7\,10\,12\,1\}$. Результат виконаної структуризації дозволив сформувати множину управляючих для всієї системи концептів та встановити на рівні $q = 3$

зв'язні концепти нечіткої когнітивної моделі: $\{K_{11}, K_{13}, K_{18}\}, \{K_3, K_5, K_4\}, \{K_7, K_6, K_2\}$. Вплив на взаємозв'язані всередині кожного блоку концепти даного симпліціального комплексу дозволить при найменших зусиллях підвищити рівень захищеності об'єкта КІ.

4. Здійснено ранжування загроз системі ЗІ та об'єкту КІ з використанням теорії нечітких відношень. На основі визначених рангів здійснено розбиття множини загроз на класи, які не перетинаються та еквівалентні за вагомістю. Для забезпечення захищеності досліджуваних систем запропоновано розподіл допустимих витрат у пропорційній еквівалентності рангам загроз, що сприятиме раціональному використанню ресурсів та засобів для попередження, усунення або ж зменшення сили впливу вірогідних загроз ІБ. Крім того, на основі ранжування загроз визначено допустиму інтенсивність зниження рівня захищеності системи ЗІ та об'єкта КІ, що дозволить вчасно впровадити ефективні механізми протидії загрозам, раціонально перерозподілити сили і засоби для їхньої нейтралізації.

5. Проведено динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта КІ, використовуючи апарат динамічної каузальної алгебри. Для досягнення поставленої мети задано вектор порогів вершин, який не залежить від часу і відмежовує усі незначні впливи між концептами, та вектор стану вершин, у якого досліджувана вершина активізується ззовні та залишається активною протягом усього процесу. Встановлено момент часу стабілізації процесу. Визначено μ-хвилю, що породжує процес активізації вершин та відповідних шляхів. Обчислено впливи вздовж усіх активізованих шляхів від досліджуваних концептів до цільового, на основі отриманих значень визначено сумарний вплив концепта K_{15} – захищеність системи ЗІ на K_{14} – захищеність КІ в моменти часу $t = 0, 1, 2, 3, 4$: $T_{(K_{15}, K_{14})}(t) = (0; 0.456; 0.456; 1.216; 1.216)$ та сумарний вплив K_{16} – захищеність КМ на K_{14} – захищеність КІ ($t = 0, 1, 2, 3, 4, 5$): $T_{(K_{16}, K_{14})}(t) = (0; 0; 0; 0.475; 1.045; 1.045)$. Відповідні рівні впливу у конкретні моменти часу відображено графічно.

6. Проведено дослідження імпульсних процесів на НКК для визначення зміни рівня захищеності системи ЗІ. Дана методика базується на розповсюдженні імпульсу, введеного у концепт (або декілька концептів) когнітивної карти, який, поширюючись по системі, посилюється або ж згасає. Для досягнення поставленої мети сформовано матрицю транзитивного замикання, яка відображає зміну стану кожного концепту системи у момент стабілізації імпульсного процесу. Аналіз даної матриці дозволив для простих імпульсних процесів з визначеними початковими вершинами встановити зміну рівня захищеності системи ЗІ. Крім того, серед множини усіх концептів когнітивної карти виділено найвагоміші, які унаслідок імпульсного процесу найбільшою мірою впливатимуть на захищеність досліджуваної системи. Так, при внесенні імпульсу в концепт K_6 – організаційне забезпечення ЗІ, концепт K_{11} – захищеність системи ЗІ максимально посилиться (до 3,8), а при внесенні імпульсу у K_5 – НСД до інформації зловмисником, цільовий концепт максимально послабиться (до 2,9). Дані концепти є найвагомішими концептами системи, що також підтверджується результатами отриманими внаслідок проведення структурно-топологічного аналізу досліджуваної когнітивної карти. Для наглядності еволюційного розвитку системи побудовано графіки.

7. Розроблено програмні засоби для реалізації запропонованих когнітивних моделей оцінювання рівня захищеності систем ЗІ, що циркулює в ІС. Запропоновано структуру програми у вигляді семи взаємозалежних програмних модулів. Згідно даної структури реалізацію проведено у вигляді додатку Windows Forms на мові програмування C# з використанням платформи .Net Framework. Для ефективного та раціонального використання додатку користувачем, продемонстровано застосування програмних модулів, наведено приклад роботи програми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] О. В. Салієва, та Ю. Є. Яремчук, «Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі», *Реєстрація, зберігання і обробка даних,* т. 21, № 4, с. 28–39, 2019.

[2] N. Mumtaz, A. Begum, B. Gul, S. Noor, R. Odarchenko, I. Machalin and O. Saliieva «Semantic, Digitization, Design and Implementation of Ontology in Social Internet-Services», *Conflict Management in Glodal Information Networks*, vol. 2588, pp. 228-249, 2019.

[3] О. В. Салієва, та Ю. Є. Яремчук, «Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання», *Безпека інформації*, т. 26, № 1, с. 42-49, 2020.

[4] О. В. Салієва, та Ю. Є. Яремчук, «Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень», *Захист інформації*, т. 22, № 1, с. 51–59, 2020.

[5] О. В. Салієва, та Ю. Є. Яремчук, «Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури», *Безпека інформації*, т. 26, № 2, с. 64-73, 2020.

[6] О. В. Салієва, та Ю. Є. Яремчук, «Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз», *Реєстрація, зберігання і обробка даних,* т. 22, № 2, с. 63-76, 2020.

[7] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу», *Вісник Вінницького політехнічного інституту,* № 4, с. 98-104, 2020.

[8] О. В. Салієва, та Ю. Є. Яремчук, «Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури», *Захист інформації*, т. 22, №3, с. 148–157, 2020.

[9] О. В. Салієва, та Ю. Є. Яремчук, «Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури», *Реєстрація, зберігання і обробка даних,* т. 22, №3, с. 68-75, 2020.

[10] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об’єкта критичної інфраструктури за результатами когнітивного моделювання», *Вісник Черкаського державного технологічного університету,* №3, с. 85-93, 2020.

[11] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності систем захисту інформації», *Вісник Вінницького політехнічного інституту,* №5, с. 56-62, 2020.

[12] О. В. Салієва, «Системологічне дослідження суб’єктів захисту інформації», у *Матеріалах XLV науково-технічної конференції підрозділів ВНТУ*, м. Вінниця, 2016, с. 2190-2191.

[13] О. В. Салієва, Я. Ю. Яремчук, «Порівняння моделей інформаційної безпеки за характеристиками суб’єктів», у *Матеріалах конференції «Управління знаннями та конкурентна розвідка»,* м. Харків, 2019, с. 67-68.

[14] О. В. Салієва, «Аналіз впливу загроз безпеці комп’ютерної мережі з використанням когнітивного моделювання», у *Матеріалах XLVII науково-технічної конференції підрозділів ВНТУ*, м. Вінниця, 2020, с. 2725-2726.

[15] О. В. Салієва, «Оцінювання рівня захищеності системи безпеки на основі когнітивного моделювання», у *Матеріалах всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи»*, м. Вінниця, 2020, с. 1215-1216.

[16] О. В. Салієва, «Визначення витрат на забезпечення захищеності системи захисту інформації ранжуванням загроз», у *Матеріалах VI Міжнародної науково-практичної конференції «Перспективні напрями захисту інформації»*, м. Одеса, 2020, с. 83-84.

[17] Ю. Є. Яремчук, О. В. Салієва, «Оцінювання рівня захищеності об’єкта критичної інфраструктури», у *Матеріалах науково-практичної конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання»,* м. Київ, 2020, с. 280-281.

[18] О. В. Салієва, «Визначення впливу загроз на рівень захищеності комп’ютерної мережі за когнітивною моделлю на основі регресійного аналізу», *у Матеріалах науково-технічної конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології»*, м. Київ, 2020, с. 105-106.

[19] Конституція України від 28.06.1996 р. № 254к/96–ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

[20] Про національну безпеку України: Закон України від 21 червня 2018 року №2469-19. *Відомості Верховної Ради України*. 2018. №31. Ст. 241.

[21] Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.

[22] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року №81/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

[23] Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 року №537-V. *Відомості Верховної Ради України.* 2007. № 12. Ст. 102.

[24] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. *Верховна Рада України. Законодавство України.*

[25] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. *Верховна Рада України. Законодавство України*.

[26] В. А. Ліпкан, *Теоретичні основи та елементи національної безпеки України: монографія*. Київ: Текст, 2003.

[27] А. А. Тер-Акопов, *Безопасность человека: Теоретические основы социально-правовой концепции,* Москва, Россия: МНЭПУ, 1998.

[28] В. И. Ярочкин, и Т. А. Шевцова, *Словарь терминов и определений по безопасности и защите информации,* Москва, Россия: Ось-89, 1996.

[29] В. Д. Гавловський, О. І. Коваленко, В. К. Гіжевський, В. С. Цимбалюк та ін., *Інформаційне право та інформаційна безпека. Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту*. Донецьк, Україна: КРОК, 2001.

[30] А. А. Князев, *Энциклопедический словарь СМИ*. Бишкек, Киргизстан: КРСУ, 2002.

[31] В. А. Ліпкан, *Національна безпека України: навч. посіб.* Київ, Україна: КНТ, 2009.

[32] А. І. Семенченко, *Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: монографія.* Київ: НАДУ, 2008.

[33] И. М. Ажмухамедов, *Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования: монография.* Астрахань, 2012.

[34] В. И. Ярочкин, *Информационная безопасность.* Москва, Россия: Академический Проект, Гаудеамус, 2004.

[35] *ГОСТ Р 51275-2006.* Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Введ. 2008-02-01]. Изд. Москва: Стандартинформ, 8 с., 2007.

[36] *ГОСТ Р 56205-2014. IEC/TS 62443-1-1:2009.* Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. [Введ. 2016-01-01]. Изд. Москва: Стандартинформ, 74 с., 2014.

[37] В. А. Ліпкан, Ю. Є. Максименко, та В. М. Желіховський, *Інформаційна безпека України в умовах євроінтеграції: навч. посіб.* Київ, Україна: КНТ, 2006.

[38] С. В. Кавун, В. В. Носов, та О. В. Мажай, *Інформаційна безпека: навч. посіб. Ч.1.* Харків, Україна: ХНЕУ, 2008.

[39] *ДСТУ 3396.0-96.* Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997-01-01]. Вид. офіц. Київ: Державна служба спеціального зв'язку та захисту інформації України, 40 с., 1996.

[40] А. М. Астахов, *Искусство управления информационными рисками*. Москва, Россия: ДМК Пресс, 2010.

[41] О. Литвиненко, «Проблема інформаційної безпеки в контексті міграційних процесів», *Українознавчий альманах*, Вип. 7, с. 116-117, 2017.

[42] *ДСТУ ISO/IEC 27005:2015*. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. [Чинний від 2017-01-01]. Вид. офіц. Київ: Технічний комітет зі стандартизації «Інформаційні технології», 65 с., 2015.

[43] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Введ. 2008-02-14], М.: ФСТЭК России, 16 с., 2008.

[44] Качественный анализ рисков. *Управление рисками, риск-менеджмент на предприятии.* [Электронный ресурс]. Доступно: http://www.risk24.ru/analiz2.htm. Дата обращения: Сен. 10, 2019.

[45] Количественный анализ рисков. *Управление рисками, риск-менеджмент на предприятии.* [Электронный ресурс]. Доступно: http://www.risk24.ru/analiz3.htm. Дата обращения: Сен. 05, 2019.

[46] Управление рисками. Метод CRAMM. *Треннинговый и экзаменационный центр IT Expert*. [Электронный ресурс]. Доступно: http://www.itexpert.ru/rus/ITEMS/77-33/. Дата обращения: Сен. 13, 2019.

[47] Н. Куканова, «Современные методы и средства анализа и управления рисками информационных систем компаний», *Библиотека on-line CIT*

Forum. [Электронный ресурс]. Доступно: http://citforum.ru/products/dsec/cramm/. Дата обращения: Сен. 20, 2019.

[48] Методология OCTAVE для оценки информационных рисков. [Электронный ресурс]. Доступно: http://www.risk24.ru/octave.htm. Дата обращения: Сен. 15, 2019.

[49] О. Г. Пузиренко, С. О. Івко, та О. О. Лаврут, «Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем», *Системи обробки інформації*, Вип. 8 (124), с. 128-134, 2014.

[50] Microsoft Security Assessment Tool 4.0. *Download Center Microsoft*. [Электронный ресурс]. Доступно: https://www.microsoft.com/ruru/download/details.aspx?id=12273. Дата обращения: Сен. 14, 2019.

[51] Средство оценки безопасности Microsoft Security Assessment Tool. *Технический центр безопасности Microsoft*. [Электронный ресурс]. Доступно: https://technet.microsoft.com/ru-ru/security/cc185712.aspx. Дата обращения: Сен. 08, 2019.

[52] L. Taylor, Risk analysis tools & how they work. [Online]. Available: http://www.riskwatch.com. Accessed on: Sept. 05, 2019.

[53] С. В. Разумников, «Анализ возможности применения методов OCTAVE, RISKWATCH, CRAMM для оценки рисков ИТ для облачных сервисов», *Современные проблемы науки и образования*, № 1, с. 247, 2014.

[54] И. Медведовский, Современные методы и средства анализа и контроля рисков информационных систем компаний. *Прогноз финансовых рисков*. [Электронный ресурс]. Доступно: http://www.bre.ru/security/20461.html Дата обращения: Сен. 16, 2019.

[55] С. Ф. Гончар, «Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом», *Захист інформації,* № 1 (16), с. 40-46, 2014.

[56] Г. А. Черней, «Оценка угроз безопасности автоматизированным информационным системам». [Электронный ресурс]. Доступно: http://security.ase.md/publ/ru/pubru01.html. Дата обращения: Май 20, 2019.

[57] П. В. Плетнев, и В. М. Белов, «Методика оценки рисков информационной безопасности», [Электронный ресурс]. Доступно: www.tusur.ru/filearchive/reports-magazine/2012-25-2/083. Дата обращения: Апр. 10, 2019.

[58] О. М. Степанова, та А. А. Волков, «Оцінка інформаційних ризиків в умовах розвитку інформаційної системи підприємства», *Вісник східноукраїнського національного університету імені В. Даля,* №10 (240), с. 106-110, 2017.

[59] О. Ю. Губарева, О. В. Осипов, и В. В. Пугин, «Иерархическая вероятностная модель мониторинга угрозы информационной безопасности информационной системы», *Инфокоммуникационные технологи*, т. 14, №4, с. 429-435, 2016.

[60] Ю. М. Ткач та ін., «Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу», *Захист інформації*, т. 19, №2, с. 137-142, 2017.

[61] І. С. Добринін, та Н. О. Мальцева, «Вдосконалення методики факторного аналізу інформаційних ризиків», *Системи обробки інформації,* Вип. 3 (149), с.146-150, 2017.

[62] О. Г. Корченко, та С. В. Казмірчук, «Метод оцінювання ризиків інформаційної безпеки на основі відкритих баз даних уразливостей», *Безпека інформації*, т. 22, № 2, с. 214-224, 2016.

[63] В. О. Шапорин, П. М. Тишин, Р. О. Шапорин, и Н. Б. Копытчук, «Разработка лингвистической модели оценки рисков активов информационной системы», *Восточно-Европейский журнал передовых технологий*, №4/2 (76), с. 30-35, 2015.

[64] M. Lund, B. Solhaug, and K. Stolen, «Model-Driven Risk Analysis», *Springer-Verlag*, Berlin, pp. 55–62, 2011.

[65] Р. А. Бельфер, Д. А. Калюжный, и Д. В. Тарасова, «Анализ зависимости уровня риска информационной безопасности сетей святи от экспертных данных при расчетах с использованием модели нечетких множеств», *Вопросы кибербезопасности*, №1(2), с. 33-39, 2014.

[66] I. Anikin, «Information Security Risks Assessment Method Based on AHP and Fuzzy Sets», in *Proceedings of 2nd Intl' Conference on Advanced in Engineering Sciences and Applied Mathematics (ICAESAM'2014),* Istambul (Turkey), May 4-5, pp. 11-15, 2014.

[67] И Аникин, «Нечеткая оценка факторов риска информационной безопасности», *Безопасность информационных технологий*, т. 23, №1, с. 78-87, 2016.

[68] Е. К. Баранова, и А. М. Гусев, «Методика анализа рисков информационной безопасности с использованием нечёткой логики на базе инструментария MATLAB», *Образовательные ресурсы и технологи*, № 1 (13), с. 88-96, 2016.

[69] И. В. Сибикина, «Анализ рисков информационной безопасности с использованием системы нечеткого вивода», *Научный вестник Новосибирского государственного технического университета*, № 4, с. 121–134, 2016.

[70] R. Muratkhan, B. Khabdolda, M. Zhumabekov, and A. Omarova, «Assessing information security risk with the fuzzy set theory», *Journal of Theoretical and Applied Information Technology*, vol. 96, no 11, pp. 3142-3152, 2018.

[71] С. А. Глушенко, «Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации», *Бизнес-информатика*, № 1 (39), с. 68-77, 2017.

[72] О. В. Кочетков, Т. О. Гаур, та В. М. Машін, «Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки», *Наукові праці ОНАЗ ім. О.С. Попова,* № 1, с. 97-104, 2019.

[73] О. І. Черняк, та Д. О. Сікорський, «Нечіткий підхід до оцінювання рівня інформаційних ризиків у CRM-системах», *Нейро-нечіткі технології моделювання в економіці*, № 5, с. 199–232, 2016.

[74] Н. С. Хохлов, С. В. Канавин, и А. Е. Рыбокитов, «Логико-лингвистическая нечеткая модель для оценки рисков нарушения информационной безопасности в самоорганизующихся сетях связи и управление ими», *Вестник Воронежского института МВД России*, №2, с. 144-154, 2019.

[75] В. И. Максимов, Е. К. Корноушенко, и С. В. Качаев, «Когнитивные технологии для поддержки принятия управленческих решений», *Информационное общество*, Вып. 2, с. 50-54. 1999. [Электронный ресурс]. Доступно: www.iis.ru/events/19981130/maximov.ru.html.

[76] А. Н. Пылкин, А. В. Крошилин, и С. В. Крошилина, «Методология когнитивного анализа в вопросах автоматизации управления материальными потоками», *Интеллектуальные системы*, № 2 (32), с. 138–149, 2012.

[77] В. В. Борисов, В. В. Круглов, и А. С. Федулов, *Нечеткие модели и сети.* Москва, Россия: Горячая линия, Телеком, 2012.

[78] А. А. Кулинич, «Систематизация когнитивных карт методов их анализа», *на VII Межд. науч.-практ. конф. Управление большими системами 2007*, Москва, 2007, с. 50–55.

[79] О. П. Кузнецов, А. А. Кулинич, и А. В. Марковский, «Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт», *Человеческий фактор в управлении*, с. 313–344, 2006.

[80] Ф. С. Робертс, *Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам.* Москва, Россия: Наука, 1986.

[81] B. Kosko, «Fuzzy Cognitive Maps», *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[82] В. Б. Силов, *Принятие стратегических решений в нечеткой обстановке.* Москва, Россия: ИНПРО-РЕС, 1995.

[83] В. В. Борисов, и А. С. Федулов, «Обобщенные нечеткие когнитивные карты», *Нейрокомпьютеры: разработка, применение*, №3, с. 3-20, 2004.

[84] А. С. Федулов, «Нечеткие реляционные когнитивные карты», *Известия РАН. Теория и системы управления,* №1, с. 120-132, 2005.

[85] J. Carvalho, «Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations», Computational Intelligence for Modeling, Control and Automation: Evolutionary *Computation and Fuzzy Logic for Intelligent Control, Knowledge Acquisition and Information Retrieval.* [Online]. Available: www.Inescid.pt/pt/indicadores/Ficheiros/1894.pdf.

[86] J. Salmeron, «Modelling grey uncertainty with fuzzy grey cognitive maps», *Expert Syst. Appl.*, vol. 37, no. 12, pp. 7581-7588, 2010.

[87] V. Kandasamy, and F. Smarandache, *Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps*. Xiquan: Phoenix, 2003.

[88] Y. Miao, Z. Q. Liu, C. K. Siew, and C. Y. Miao, «Dynamical cognitive network: An extension of fuzzy cognitive map», *IEEE Trans on Fuzzy Systems,* vol. 9, no. 5, pp. 760-770, 2001.

[89] E. Papageorgiou, and I. Salmeron, «Review of Fuzzy Cognitive Maps Research During the Last Decade», *IEEE Trans on Fuzzy Systems*, vol. 21, no. 1, pp. 66-79, 2013.

[90] В. И. Васильев, А. М. Вульфин, И. Б. Герасимова, и В. М. Картак, «Анализ рисков кибербезопасности с помощью нечетких когнитивных карт», *Вопросы кибербезопасности,* №2 (36), с. 11-21, 2020.

[91] И. М. Ажмухамедов, и О. М. Князева, «Оценка состояния защищенности данных организации в условиях возможности реализации угроз», *Управление и высокие технологии*, № 3 (31), с. 24-39, 2015.

[92] В. И. Васильев, А. М. Вульфин, и М. Б. Гузаиров, «Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт», *Информационные технологии*, т. 24, № 4, с. 266-273, 2018.

[93] Е. С. Степанова, И. В. Машкина, и В. И. Васильев, «Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности», *Известия*

Южного федерального университета. Технические науки, т. 112, № 11, с. 31-40, 2010.

[94] P. Szwed, and P. Skrzyński, «A new lightweight method for security risk assessment based on fuzzy cognitive maps», *International Journal of Applied Mathematics and Computer Science*, vol. 24, no. 1, pp. 213-225, 2014.

[95] В. А. Камаев, и В. В. Натров, «Моделирование и анализ состояния информационной безопасности организации», *Известия Тульского государственного университета. Технические науки,* №3, с. 148–155, 2011.

[96] В. И. Васильев, А. М. Вульфин, М. Б. Гузаиров, и А. Д. Кириллова, «Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт», *Информационные технологии*, т. 24, №10, с. 657-664, 2018.

[97] С. А. Трапизонян, и В. Н. Кармазин, «Когнитивное моделирование процесса обеспечения информационной безопасности организации», *Фундаментальные и прикладне исследования в современом мире,* № 18-1, с. 62 - 66, 2017.

[98] J. Shin et al, «Development of a cyber security risk model using Bayesian networks», *Reliability Engineering & System Safety*, vol. 134, pp. 208-217, 2015.

[99] P. Mell, and R. Harang, «Minimizing Attack Graph Data Structures», in *Tenth International Conference on Software Engineering Advances*, Barcelona, 2015, pp. 376-385.

[100] В. Г. Олифер, и Н. А. Олифер, *Компьютерные сети. Принципы, технологии, протоколы.* Санкт-Петербург, Россия: Питер, 2017.

[101] С. М. Захарченко, Т. І. Трояновська, та О. В. Бойко, *Основи побудови захищених мереж на базі обладнання компанії Cisco: навч. посіб.* Вінниця, Україна: ВНТУ, 2017.

[102] И. Ю. Перцев, и В. Н. Зинькевич, «Анализ существующих угроз компьютерной безопасности в сети», *Наука, образование и культура*, № 3, с. 9 – 12, 2015.

[103] *ГОСТ Р ИСО/МЭК 27033-3-2014* Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. [Введ. 2015-11-01]. Изд. Москва: Стандартинформ, 2014, 23 с.

[104] А. К Новохрестов, и Т. С. Степанова, «Модель классификации угроз нарушения безопасности компьютерных сетей», *Электронные средства и системы управления,* №1-2, с. 76-79, 2017.

[105] S. Gray, J. De Kok, A.E.R. Helfgott, B. O'Dwyer, R. Jordan, A. Nyaki, «Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological systems», *Ecology and Society, 20(2):11, 2015.* [Online]. Available: http://www.ecologyandsociety.org/vol20/iss2/art11.

[106] О. К. Юдін, *Інформаційна безпека. Нормативно-правове забезпечення.* Київ, Україна: НАУ - друк, 2011.

[107] Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова КМУ від 23 серпня 2016 р. № 563. *Офіційний вісник України*. 2016. № 69.

[108] А. Г. Массель, и Д. А. Гаськова, «Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов», *Онтология проектирования*, т. 9, №2(32), с.225-238, 2019.

[109] A. Leandros, K. Ki-Hyung, J. Helge etc., «Cruz Cyber security of critical infrastructures», *ICT Express*, №4, pp. 42–45, 2018.

[110] Д. С. Бірюков, та С. І. Кондратов, *Зелена книга з питань захисту критичної інфраструктури в Україні*: *зб. матеріалів міжнародних експертних нарад*. Київ, Україна: НІСД, 2015.

[111] В. Д. Козюра, та В. А. Хорошко, «Заходи протидії прихованої передачі інформації в локальних мережах», на *наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2018, с. 91-93.

[112] В. Б. Малащенко, «Теоретичні підходи до проблем та сучасних способів захисту від «інсайдерів»», *Ефективність державного управління,* Вип. 29, 2011. [Електронний ресурс]. Доступно: http://archive.nbuv.gov.ua/portal/soc_gum/Edu/2011_29/fail/malashchenko.pdf

[113] Р. М. Літнарович, *Побудова і дослідження математичної моделі за джерелами експериментальних даних методами регресійного аналізу.* Рівне, Україна: МЕГУ, 2011.

[114] Н. Ш. Кремер, *Теория вероятностей и математическая статистика : учебник и практикум для вузов.* Москва, Россия: Юрайт, 2019.

[115] Дж. Касти, *Большие системы: связность, сложность и катастрофы.* Москва, Россия: Мир, 1982.

[116] Г. В. Горелова, Е. Н. Захарова, и С. А. Радченко, *Исследование слабоструктурированных проблем социально-экономических систем: когнитивный подход: монография.* Ростов н/Д: РГУ, 2006.

[117] И. М. Ажмухамедов, «Моделирование на основе экспертных суджений процесса оценки информационной безопасности», *Вестник АГТУ. Серия: «Управление, вычислительная техника и информатика»,* №2, с.101-109, 2009.

[118] А. Г. Кащенко, «Многокритериальная оценка и ранжирование информационных рисков на основе алгоритма Мамдани», на *V Международной научно-технической конференции Кибернетика и технологи XXI века,* Воронеж, 2004, с. 81-85.

[119] А. П. Ротштейн, «Нечеткие когнитивные карты в анализе надежности», *Надежность*, №4, с. 24-31, 2019.

[120] А. П. Ротштейн, «Ранжирование элементов системы на основе нечеткого отношения влияния и транзитивного замыкания», *Кибернетика и системный анализ*, т. 53, №1, с. 68-78, 2017.

[121] Класифікація загроз інформаційній безпеці. Інформаційна безпека особистості. [Електронний ресурс]. Доступно:

https://sites.google.com/site/infobezosob/klasifikacia-zagroz-informacijnijbezpeci. Дата звернення: Бер. 25, 2020.

[122] T. Saaty, *Mathematical models of arms control and disarmament.* New York: John Willey & Sons, 1968.

[123] L. Zadeh, «Similarity relations and fuzzy orderings», *Information Sciences*, vol. 3, pp. 177-200, 1971.

[124] Z.-Q. Liu, J. Y. Zhang, «Interrogating the structure of fuzzy cognitive maps», *Soft Computing,* vol. 7, pp. 148–153, 2003.

[125] О. П. Кузнецов, А. А. Кулинич, и А. В. Марковский, «Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт», *Человеческий фактор в управлении*, с. 330-362, 2006.

ДОДАТКИ

Додаток А Модуль транзитивного замикання відношення схожості

```
var express = require('express');
var app = express();
var bodyParser = require('body-parser');
var urlencodedParser = bodyParser.urlencoded({ extended: false });
app.set('view engine', 'ejs');
app.get('/', function(req, res){
   var Matrix = require('matrix-slicer');

   var R1 = new Matrix([
      [0, 0, 0.3, 0, 0, 0, 0, 0],
      [0, 0, 0, 0.3, 0, 0, 0, 0],
      [0, 0, 0, 0, 0, 0, 0.2, 0],
      [0, 0, 0, 0, 0, 0, 0, 0.2],
      [0, 0, 0, 0.6, 0, 0, 0, 0],
      [0, 0, 0.6, 0, 0, 0, 0, 0],
      [0.5, 0, 0, 0.4, 0.5, 0, 0, 0],
      [0, 0.5, 0.4, 0, 0, 0.5, 0, 0]
   ]);

   var R2 = new Matrix([
      [0, 0, 0.3, 0, 0, 0, 0, 0],
      [0, 0, 0, 0.3, 0, 0, 0, 0],
      [0, 0, 0, 0, 0, 0, 0.2, 0],
      [0, 0, 0, 0, 0, 0, 0, 0.2],
      [0, 0, 0, 0.6, 0, 0, 0, 0],
      [0, 0, 0.6, 0, 0, 0, 0, 0],
      [0.5, 0, 0, 0.4, 0.5, 0, 0, 0],
      [0, 0.5, 0.4, 0, 0, 0.5, 0, 0]
   ]);


   var array = [];
   for (var i=0; i<8; i++){
      var row = R1.getRow(i);
      for (var j=0; j<8; j++){
         var column = R2.getColumn(j);
         for(var c=0; c< row.length; c++) {
            array.push((row[c]*column[c]).toFixed(4));
         }
      }
   }

   var new_array = [];
   var chunksize = 8;
   while (array.length) {
               var chunk = array.splice(0,chunksize);
               new_array.push(chunk);
   }

   var final_array = [];
```

```
    for (var i=0; i<new_array.length; i++){
        maxResult = Math.max.apply(null, new_array[i]);
        final_array.push(maxResult);
    }
    var konez = [];
    var chunksize = 8;
    while (final_array.length) {
                var chunk = final_array.splice(0,chunksize);
                konez.push(chunk);
    }
    var resultMatrix = new Matrix(konez);
    var sendMatrix = JSON.stringify(resultMatrix);

    var stat;
    if (JSON.stringify(resultMatrix)==JSON.stringify(R2)){
        stat = "Matrix are the same";
    }else{
        stat = "Matrix are different";
    }
    res.render('index', {status:stat});
});
app.listen(3000);
```

Додаток Б Значення непрямих впливів концепта «Захищеність комп'ютерної мережі» на концепт «Захищеність критичної інфраструктури» у різні моменти часу

$P(K_{16}, K_{14})$	$I_P(0)$	$I_P(1)$	$I_P(2)$	$I_P(3)$	$I_P(4)$	$I_P(5)$
(K_{16}, K_{15}, K_{14})	0	0	0	0,475	0,475	0,475
$(K_{16}, K_{15}, K_{18}, K_{15}, K_{14})$	0	0	0	0,23	0,23	0,23
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0	0	0,08	0,08	0,08
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{15}, K_{14})$	0	0	0	0,03	0,03	0,03
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,01	0,01	0,01
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,001	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,001	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,001	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,0001	0,0001	0,0001
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0,08	0,08	0,08
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{16}, K_{15}, K_{14})$	0	0	0	0,039	0,039	0,039
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,005	0,005	0,005
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{15}, K_{14})$	0	0	0	0,114	0,114	0,114
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,037	0,037	0,037
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,005	0,005	0,005
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,002	0,002	0,002
$(K_{16}, K_{18}, K_{15}, K_{14})$	0	0	0	0,304	0,304	0,304
$(K_{16}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0	0	0,106	0,106	0,106
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{15}, K_{14})$	0	0	0	0,04	0,04	0,04
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,013	0,013	0,013
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,002	0,002	0,002
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,0008	0,0008	0,0008
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,0008	0,0008	0,0008
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,0002	0,0002	0,0002
$(K_{16}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0,105	0,105	0,105
$(K_{16}, K_{18}, K_{13}, K_{16}, K_{15}, K_{14})$	0	0	0	0,05	0,05	0,05
$(K_{16}, K_{18}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,007	0,007	0,007
$(K_{16}, K_{24}, K_{13}, K_{15}, K_{14})$	0	0	0	0,155	0,155	0,155
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{14})$	0	0	0	0,02	0,02	0,02
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{14})$	0	0	0	0,01	0,01	0,01
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0,009	0,009	0,009
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0,002	0,002	0,002

$(K_{16}, K_{15}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0,078	0,078	0,078
$(K_{16}, K_{24}, K_{13}, K_{16}, K_{15}, K_{14})$	0	0	0	0,078	0,078	0,078
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0,009	0,009	0,009
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,03	0,03
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0002	0,0002
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,0004	0,0004
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,171	0,171
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,01	0,01
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,007	0,007
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{15}, K_{14})$	0	0	0	0	0,006	0,006
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,01	0,01
$(K_{16}, K_{15}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,1	0,1
$(K_{16}, K_{15}, K_{22}, K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,004	0,004
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,007	0,007
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0004	0,0004
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,0004	0,0004
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0001	0,0001
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,034	0,034
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0002	0,0002
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002

$(K_{16},\ K_{18},\ K_{12}, K_{16}, K_{22},\ K_{23},\ K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16},\ K_{18},\ K_{12}, K_{16}, K_{22},\ K_{23}, K_{20}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},\ K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0004	0,0004
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,0008	0,0008
$(K_{16}, K_{22},\ K_{15}, K_{14})$	0	0	0	0	0,4	0,4
$(K_{16}, K_{22},\ K_{20}, K_{15}, K_{14})$	0	0	0	0	0,035	0,035
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,016	0,016
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{16}, K_{15}, K_{14})$	0	0	0	0	0,015	0,015
$(K_{16}, K_{15}, K_{22},\ K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{22},\ K_{23},\ K_{15}, K_{14})$	0	0	0	0	0,027	0,027
$(K_{16}, K_{22}, K_{23},\ K_{21}, K_{15}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{22},\ K_{23},\ K_{20}, K_{15}, K_{14})$	0	0	0	0	0,007	0,007
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,01	0,01
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,027	0,027
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{15}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{21}, K_{15}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,05	0,05
(K_{16}, K_{17}, K_{14})	0	0	0	0	0,57	0,57
$(K_{16}, K_{22},\ K_{15}, K_{17}, K_{14})$	0	0	0	0	0,319	0,319
$(K_{16}, K_{22},\ K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,028	0,028
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{15}, K_{17},\ K_{14})$	0	0	0	0	0,013	0,013
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,012	0,012
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{16},\ K_{17}, K_{14})$	0	0	0	0	0,018	0,018
$(K_{16}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{22},\ K_{20}, K_{23}, K_{16}, K_{18}, K_{12},\ K_{17}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,021	0,021
$(K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,004	0,004
$(K_{16}, K_{22},\ K_{23},\ K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,006	0,006
$(K_{16}, K_{24}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,155	0,155
$(K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,016	0,016
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,01	0,01
$(K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,007	0,007

$(K_{16},K_{24},K_{13},K_{21},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,007	0,007
$(K_{16},K_{24},K_{13},K_{21},K_{23},K_{20},K_{15},K_{17},K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,124	0,124
$(K_{16},K_{24},K_{13},K_{20},K_{22},K_{15},K_{17},K_{14})$	0	0	0	0	0,022	0,022
$(K_{16},K_{24},K_{13},K_{20},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,007	0,007
$(K_{16},K_{24},K_{13},K_{20},K_{22},K_{21},K_{15},K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{24},K_{13},K_{20},K_{22},K_{21},K_{23},K_{15}, K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{24},K_{13},K_{20},K_{22},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{24},K_{13},K_{20},K_{22},K_{23},K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16},K_{18},K_{12}, K_{16}, K_{22},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,002	0,002
$(K_{16},K_{18},K_{12},K_{16},K_{22}, K_{23},K_{20},K_{15},K_{17},K_{14})$	0	0	0	0	0,0005	0,0005
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22},K_{23},K_{21},K_{15},K_{17}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16},K_{18},K_{12},K_{16},K_{24},K_{13},K_{15},K_{17},K_{14})$	0	0	0	0	0,01	0,01
$(K_{16},K_{18},K_{12},K_{16}, K_{24}, K_{13},K_{17},K_{14})$	0	0	0	0	0,01	0,01
$(K_{16},K_{18},K_{12},K_{16},K_{24},K_{13},K_{20},K_{15},K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{18},K_{12},K_{16},K_{24},K_{13},K_{21},K_{15},K_{17},K_{14})$	0	0	0	0	0,0007	0,0007
$(K_{16},K_{18},K_{12},K_{16},K_{24},K_{13},K_{21},K_{22},K_{15},K_{17},K_{14})$	0	0	0	0	0,0006	0,0006
$(K_{16},K_{18},K_{12},K_{16},K_{24},K_{13},K_{21},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{18}, K_{12},K_{16},K_{24},K_{13},K_{21},K_{23},K_{20},K_{15}, K_{17},K_{14})$	0	0	0	0	0,0002	0,0002
$(K_{16},K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,084	0,084
$(K_{16}, K_{18}, K_{13}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,042	0,042
$(K_{16},K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,105	0,105
$(K_{16},K_{18}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{18}, K_{17}, K_{14})$	0	0	0	0	0,304	0,304
$(K_{16}, K_{18}, K_{12}, K_{17}, K_{14})$	0	0	0	0	0,173	0,173
$(K_{16}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,085	0,085
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{17}, K_{14})$	0	0	0	0	0,048	0,048
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,032	0,032
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,027	0,027
$(K_{16}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{18},K_{12},K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16},K_{18},K_{12},K_{16},K_{22},K_{20},K_{23},K_{21},K_{15},K_{17},K_{14})$	0	0	0	0	0,0002	0,0002
$(K_{16},K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16},K_{18},K_{12},K_{16},K_{22},K_{21},K_{23},K_{15},K_{17},K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,38	0,38
$(K_{16}, K_{15}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,137	0,137
$(K_{16}, K_{15}, K_{18}, K_{17}, K_{14})$	0	0	0	0	0,228	0,228
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{17}, K_{14})$	0	0	0	0	0,13	0,13

$(K_{16}, K_{15}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,064	0,064
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{17}, K_{14})$	0	0	0	0	0,036	0,036
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,024	0,024
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,02	0,02
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0008	0,0008
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0001	0,0001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0004	0,0004
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0002	0,0002
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,008	0,008
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,01	0,01
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0005	0,0005
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0005	0,0005
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0005	0,0005
$(K_{16}, K_{15}, K_{18}, K_{12}, K_{16}, K_{24}, K_{13}, K_{21}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0001	0,0001
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,063	0,063
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,03	0,03
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,078	0,078
$(K_{16}, K_{15}, K_{18}, K_{13}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,004	0,004
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,012	0,012
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{17}, K_{14})$	0	0	0	0	0,008	0,008
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{12}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{22}, K_{20}, K_{23}, K_{16}, K_{18}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,001	0,001
$(K_{16}, K_{15}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,009	0,009

$(K_{16}, K_{15}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,09	0,09
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{17}, K_{14})$	0	0	0	0	0,14	0,14
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,077	0,077
$(K_{16}, K_{15}, K_{22}, K_{23}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,003	0,003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{22}, K_{20}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0005	0,0005
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,03	0,03
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{17}, K_{14})$	0	0	0	0	0,037	0,037
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,004	0,004
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,005	0,005
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,002	0,002
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{21}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0003	0,0003
$(K_{16}, K_{15}, K_{18}, K_{16}, K_{24}, K_{13}, K_{20}, K_{22}, K_{23}, K_{21}, K_{15}, K_{17}, K_{14})$	0	0	0	0	0,0001	0,0001

Додаток В Лістинг основних модулів програми для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах

```
using Newtonsoft.Json;
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Windows.Forms.DataVisualization.Charting;

namespace test111
{
  public partial class meinForm : Form
  {
    private Graph graph;
    private int vertexCounter;
    private Drawing drawingGraph;
    private Image vertexImage;
    private DynamicModelingOfTheImpactOfConcepts DynamicModeling;
    private ImpactSchedule[] impactSchedules;
    private Statistics statistics;
    private CognitiveModeling cognitiveModeling;
    private List<int> startV;
    private List<int> endV;
    private List<int[]> way;

    public meinForm()
    {
      InitializeComponent();

      vertexImage = Image.FromFile(@"res\vertex.png");
      graph = new Graph();
      drawingGraph = new Drawing(pictureBox, graph, vertexImage);
      DynamicModeling = new DynamicModelingOfTheImpactOfConcepts();
      statistics = new Statistics();
      cognitiveModeling = new CognitiveModeling();

      startV = new List<int>();
      endV = new List<int>();
      way = new List<int[]>();

      vertexCounter = 0;

      openFileDialog1.Filter = "Text files(*.json)|*.json|All files(*.*)|*.*";
```

```
    saveFileDialog1.Filter = "Text files(*.json)|*.json|All files(*.*)|*.*";
}

private void tabControl_Selecting(object sender, TabControlCancelEventArgs e)
{
    if (tabControl.SelectedIndex == 1)
    {
        statistics.createStatistics(graph);

        StatisticsDataGridView.Rows.Clear();

        totalComponentsTextBox.Text = statistics.totalComponents.ToString();
        totalConnectionTextBox.Text = statistics.totalConnection.ToString();
        densityTextBox.Text = statistics.density.ToString();
        driverComponentsTextBox.Text = statistics.driverComponents.ToString();
        receiverComponentsTextBox.Text = statistics.receiverComponents.ToString();
        ordinaryComponentsTextBox.Text = statistics.ordinaryComponents.ToString();
        complexityScoreTextBox.Text = statistics.complexityScore.ToString();
        hierarchyIndexTextBox.Text = statistics.hierarchyIndex.ToString();

        for (int i = 0; i < graph.Vertex.Count; i++)
        {
            StatisticsDataGridView.Rows.Add();
            StatisticsDataGridView[0, i].Value = graph.Vertex[i].name;
            StatisticsDataGridView[1, i].Value = graph.Vertex[i].indegree;
            StatisticsDataGridView[2, i].Value = graph.Vertex[i].outdegree;
            StatisticsDataGridView[3, i].Value = graph.Vertex[i].centrality;
        }

    }
    else if (tabControl.SelectedIndex == 2)
    {
        graph.initializeMatrix();
        renewal_dataGridViewVertex();
    }
    else if (tabControl.SelectedIndex == 3)
    {
        startVertexComboBox.Items.Clear();

        endVertexComboBox.Items.Clear();

        for (int i = 0; i < graph.Vertex.Count; i++)
        {
            startVertexComboBox.Items.Add(graph.Vertex[i].name);
            endVertexComboBox.Items.Add(graph.Vertex[i].name);
        }

        if (graph.Vertex.Count != 0)
        {
            startVertexComboBox.SelectedIndex = 0;
            endVertexComboBox.SelectedIndex = 0;
```

```
            }


        }
        else if (tabControl.SelectedIndex == 4)
        {
            dataPulse.Rows.Clear();
            for (int i = 0; i < graph.Vertex.Count; i++)
            {
                dataPulse.Rows.Add();
                dataPulse[0, i].Value = graph.Vertex[i].name;
            }
        }
    }
    private void renewal_dataGridViewVertex()
    {
        DataGridViewColumn columnAdjacencyTable;

        deleteComboBox.Items.Clear();

        dataGridViewVertex.Columns.Clear();
        dataGridViewVertex.RowHeadersWidth = 100;

        for (int i = 0; i < graph.Vertex.Count; i++)
        {
            columnAdjacencyTable = new DataGridViewTextBoxColumn();
            columnAdjacencyTable.DataPropertyName = ($"{graph.Vertex[i].id}:
{graph.Vertex[i].name}");
            columnAdjacencyTable.Name = (graph.Vertex[i].name);

            dataGridViewVertex.Columns.Add(columnAdjacencyTable);

            dataGridViewVertex.Rows.Add();

            dataGridViewVertex.Rows[i].HeaderCell.Value = (graph.Vertex[i].name);

            deleteComboBox.Items.Add(graph.Vertex[i].name);
        }

        for (int i = 0; i < graph.Vertex.Count; i++)
        {
            for (int j = 0; j < graph.Vertex.Count; j++)
            {
                dataGridViewVertex.Rows[i].Cells[j].Value = graph.adjacencyMatrix[i, j];
            }
        }
    }


    private void dataGridViewVertex_CellParsing(object sender,
DataGridViewCellParsingEventArgs e)
```

```
    {
        bool edgeCreate = true;

        for (int i = 0; i < graph.Edge.Count; i++)
        {
            if (graph.Edge[i].startVertex.id == e.RowIndex && graph.Edge[i].endVertex.id ==
e.ColumnIndex)
            {
                graph.Edge[i].weight = Convert.ToDouble(e.Value);
                graph.Edge[i].renewalWeight();
                edgeCreate = false;
            }
        }

        if (edgeCreate && e.Value != "")
        {
            Edge edge = new Edge();
            edge.IniInitialize(pictureBox);
            edge.startVertex = graph.Vertex[e.RowIndex];
            edge.endVertex = graph.Vertex[e.ColumnIndex];
            edge.weight = Convert.ToDouble(e.Value);

            edge.renewalWeight();

            graph.Edge.Add(edge);
        }

        graph.initializeMatrix();
    }
    private void createVertexButton_Click(object sender, EventArgs e)
    {
        createVertex($"K{vertexCounter + 1}");
    }

    private void AddVertexToDataG_Click(object sender, EventArgs e)
    {
        if (textBoxNameVerte.Text != "")
        {
            createVertex(textBoxNameVerte.Text);
            textBoxNameVerte.Text = "";

            renewal_dataGridViewVertex();
        }
    }

    private void buttonDelete_Click(object sender, EventArgs e)
    {
        for (int i = 0; i < graph.Vertex.Count; i++)
        {
            if (graph.Vertex[i].name == deleteComboBox.SelectedItem.ToString())
            {
```

```
            graph.deleteVertex(i);

            deleteComboBox.Text = "";

            break;
        }
    }

    graph.initializeMatrix();
    renewal_dataGridViewVertex();
}
private void deleteWayButton_Click(object sender, EventArgs e)
{
    if (startV.Count != 0 && endV.Count != 0 && deleteWayComboBox.Text != "")
    {
        startV.Remove(deleteWayComboBox.SelectedIndex);
        endV.Remove(deleteWayComboBox.SelectedIndex);
        way.RemoveAt(deleteWayComboBox.SelectedIndex);

        deleteWayComboBox.Items.RemoveAt(deleteWayComboBox.SelectedIndex);
        if (deleteWayComboBox.Items.Count != 0)
        {
            deleteWayComboBox.SelectedIndex = deleteWayComboBox.Items.Count - 1;
        }
        else
        {
            deleteWayComboBox.Text = "";
        }

    }
}

private void addWaybutton_Click(object sender, EventArgs e)
{
    way.Add(new int[2]);

    for (int i = 0; i < graph.Vertex.Count; i++)
    {
        if (graph.Vertex[i].name == startVertexComboBox.SelectedItem.ToString())
        {
            way[way.Count - 1][0] = i;
            startV.Add(i);
        }
        else if (graph.Vertex[i].name == endVertexComboBox.SelectedItem.ToString())
        {
            way[way.Count - 1][1] = i;
            endV.Add(i);
        }
    }

    deleteWayComboBox.Items.Add($"{graph.Vertex[way[way.Count - 1][0]].name} ->
```

```
{graph.Vertex[way[way.Count - 1][1]].name}");
            deleteWayComboBox.SelectedIndex = deleteWayComboBox.Items.Count - 1;
        }

        private void clearGraphButton_Click(object sender, EventArgs e)
        {
            graph.Clear();
            pictureBox.Invalidate();
        }

        private void CreateScheduleButton_Click(object sender, EventArgs e)
        {
            impactSchedules = new ImpactSchedule[way.Count];

            for (int i = 0; i < way.Count; i++)
            {
                impactSchedules[i] = DynamicModeling.calculationOfDynamicTimeAnalysis(graph,
trackBarIteration.Value,
                    graph.Vertex[way[i][0]], graph.Vertex[way[i][1]]);
            }

            chart1.Series.Clear();

            ChartArea chart = this.chart1.ChartAreas[0];

            chart.AxisX.LabelStyle.Format = "";
            chart.AxisY.LabelStyle.Format = "";

            chart.AxisX.LabelStyle.IsEndLabelVisible = true;

            chart.AxisX.Minimum = 0;
            chart.AxisX.Maximum = this.trackBarIteration.Value;

            chart.AxisX.Interval = 1;
            chart.AxisY.Interval = 0.2;

            for (int i = 0, s = 0; i < impactSchedules.Length; i++, s++)
            {
                chart1.Series.Add($"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}");
                chart1.Series[$"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}"].ChartType = SeriesChartType.Line;

                chart1.Series[$"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}"].BorderWidth = 4;

                if (s == 9)
                {
                    s = 0;
                }
```

```
            chart1.Series[$"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}"].MarkerSize = 15;
            chart1.Series[$"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}"].MarkerStyle = (MarkerStyle)s;

            for (int j = 0; j < impactSchedules[i].schedule.Length; j++)
            {
               chart1.Series[$"{impactSchedules[i].startVetex} ->
{impactSchedules[i].endVetex}"].Points.AddXY(j, impactSchedules[i].schedule[j]);
            }
         }

      }
      private void pulseModelingButton_Click(object sender, EventArgs e)
      {
         textBox1.Clear();

         double[] P = new double[dataPulse.Rows.Count];

         for(int i = 0; i < dataPulse.Rows.Count; i++)
         {
            P[i] = Convert.ToDouble(dataPulse[1, i].Value);
         }

         List<double[]> masResult = cognitiveModeling.Modeling(P, graph,
Convert.ToInt32(numberOfIterationsInfoCognitive.Value));

         chart2.Series.Clear();

         textBox1.Text = cognitiveModeling.text;

         var chart = chart2.ChartAreas[0];
         chart.AxisX.LabelStyle.Format = "";
         chart.AxisY.LabelStyle.Format = "";

         chart.AxisX.LabelStyle.IsEndLabelVisible = true;

         chart.AxisX.Minimum = 0;
         chart.AxisX.Maximum = Convert.ToInt32(numberOfIterationsInfoCognitive.Value);

         chart.AxisX.Interval = 1;
         chart.AxisY.Interval = 0.5;

         for (int i = 0, s = 0; i < graph.Vertex.Count; i++, s++)
         {
            chart2.Series.Add(dataPulse[0, i].Value.ToString());
            chart2.Series[dataPulse[0, i].Value.ToString()].ChartType = SeriesChartType.Line;
            chart2.Series[dataPulse[0, i].Value.ToString()].BorderWidth = 3;

            if (s == 9)
            {
```

```
            s = 0;
        }

        chart2.Series[dataPulse[0, i].Value.ToString()].MarkerSize = 15;
        chart2.Series[dataPulse[0, i].Value.ToString()].MarkerStyle = (MarkerStyle)s;

        for (int j = 0; j < Convert.ToInt32(numberOfIterationsInfoCognitive.Value); j++)
        {
            chart2.Series[dataPulse[0, i].Value.ToString()].Points.AddXY(j, masResult[j][i]);
        }
    }
}


private void saveButton_Click(object sender, EventArgs e)
{
    graph.initializeMatrix();

    if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)
        return;

    SaveGraph SaveG = new SaveGraph();

    SaveG.adjacencyMatrix = graph.adjacencyMatrix;
    for (int i = 0; i < graph.Vertex.Count; i++)
    {
        SaveG.Vertex.Add(new SaveV());

        SaveG.Vertex[i].id = graph.Vertex[i].id;
        SaveG.Vertex[i].name = graph.Vertex[i].name;
        SaveG.Vertex[i].rect = graph.Vertex[i].rect;

    }
    string json = JsonConvert.SerializeObject(SaveG, Formatting.Indented);

    string filename = saveFileDialog1.FileName;

    System.IO.File.WriteAllText(filename, json);
    MessageBox.Show("Файл збережено");
}

private void openButton_Click(object sender, EventArgs e)
{
    if (openFileDialog1.ShowDialog() == DialogResult.Cancel)
        return;

    graph.Clear();

    pictureBox.Invalidate();

    SaveGraph SaveG;
```

```
        string filename = openFileDialog1.FileName;

        string fileText = System.IO.File.ReadAllText(filename);
        SaveG = JsonConvert.DeserializeObject<SaveGraph>(fileText);

        graph.Clear();

        for (int i = 0; i < SaveG.adjacencyMatrix.GetLength(0); i++)
        {
            Vertex V = new Vertex(SaveG.Vertex[i].name, SaveG.Vertex[i].rect, SaveG.Vertex[i].id,
pictureBox);

            graph.Vertex.Add(V);
            pictureBox.Invalidate();
        }

        for (int i = 0; i < SaveG.adjacencyMatrix.GetLength(0); i++)
        {
            for (int j = 0; j < SaveG.adjacencyMatrix.GetLength(1); j++)
            {
                if (SaveG.adjacencyMatrix[i, j] != 0)
                {
                    Edge edge = new Edge();
                    edge.IniInitialize(pictureBox);
                    edge.startVertex = graph.Vertex[i];
                    edge.endVertex = graph.Vertex[j];
                    edge.weight = SaveG.adjacencyMatrix[i, j];
                    edge.renewalWeight();
                    graph.Edge.Add(edge);
                }
            }
        }
        graph.initializeMatrix();
    }

    private void numberOfIterationsInfo_ValueChanged(object sender, EventArgs e)
    {
        trackBarIteration.Value = Convert.ToInt32(this.numberOfIterationsInfo.Value);
    }

    private void trackBarIteration_ValueChanged(object sender, EventArgs e)
    {
        numberOfIterationsInfo.Value = this.trackBarIteration.Value;
    }

    private void numericUpDown1_ValueChanged_1(object sender, EventArgs e)
    {
        trackBarIterationCognitive.Value =
Convert.ToInt32(numberOfIterationsInfoCognitive.Value);
    }
```

```
        private void trackBar1_ValueChanged(object sender, EventArgs e)
        {
            numberOfIterationsInfoCognitive.Value = trackBarIterationCognitive.Value;
        }

        public void createVertex(string name)
        {
            Vertex V = new Vertex(name,
                new Rectangle(100 + vertexCounter * 10, 100 + vertexCounter * 10, 100, 30),
                vertexCounter,
                pictureBox);

            graph.Vertex.Add(V);

            pictureBox.Invalidate();

            graph.initializeMatrix();

            vertexCounter++;
        }

        private void label14_Click(object sender, EventArgs e)
        {

        }
    }
}
    class Drawing
    {

        private Graph graph;
        private Vertex Vertex;
        private Edge edge;

        private Point pointDown;

        private PictureBox pictureBox;

        private Image vertexImage;

        private bool createEdge;
        private bool mouseDown;

        private Pen pen;
        public Drawing(PictureBox p, Graph g, Image i)
        {

            pointDown = new Point();

            mouseDown = false;
```

```
        pen = new Pen(Color.Black, 2);
        pen.CustomEndCap = new AdjustableArrowCap(4.0F, 8.0F);

        vertexImage = i;
        pictureBox = p;
        graph = g;

        pictureBox.Paint += new PaintEventHandler(panelDrawVertex_Paint);
        pictureBox.MouseDoubleClick += new MouseEventHandler(PictureBox_CreateEdge);
        pictureBox.MouseClick += new MouseEventHandler(PictureBox_ClickVertex);


        pictureBox.MouseDown += new MouseEventHandler(PictureBox_MouseDown);
        pictureBox.MouseUp += new MouseEventHandler(PictureBox_MouseUp);
        pictureBox.MouseMove += new MouseEventHandler(PictureBox_MouseMove);

    }
    private void panelDrawVertex_Paint(object sender, PaintEventArgs e)
    {

        foreach (Vertex V in graph.Vertex)
        {
            V.renewal();
            e.Graphics.DrawImage(vertexImage, V?.rect ?? Rectangle.Empty);
        }

        foreach (Edge E in graph.Edge)
        {
            if (E.startVertex != null & E.endVertex != null)
            {
                E.renewalNumericLocation();
                e.Graphics.DrawLine(pen, (PointF)(E.startVertex.rect.Location),
(PointF)(E.endVertex.rect.Location));
            }
        }
    }

    private void PictureBox_MouseDown(object sender, MouseEventArgs e)
    {
        foreach (Vertex Ver in graph.Vertex)
        {
            if (Rectangle.Intersect(new Rectangle(e.X, e.Y, 0, 0), Ver.rect) != Rectangle.Empty)
            {
                Vertex = Ver;
                pointDown = Point.Subtract(e.Location, (Size)Vertex.rect.Location);
                mouseDown = true;
            }
        }

    }
```

```
    private void PictureBox_MouseUp(object sender, MouseEventArgs e)
    {
       mouseDown = false;
    }

    private void PictureBox_MouseMove(object sender, MouseEventArgs e)
    {
       if (mouseDown)
       {
          Vertex.rect.Location = Point.Subtract(e.Location, (Size)pointDown);
          pictureBox.Invalidate();
       }
    }

    private void PictureBox_ClickVertex(object sender, MouseEventArgs e)
    {
       if (e.Button == MouseButtons.Right)
       {
          for (int i = 0; i < graph.Vertex.Count; i++)
          {
             if (Rectangle.Intersect(new Rectangle(e.X, e.Y, 0, 0), graph.Vertex[i].rect) !=
Rectangle.Empty)
             {
                graph.deleteVertex(i);
                pictureBox.Invalidate();
             }
          }
       }
       if (e.Button == MouseButtons.Left && createEdge)
       {
          foreach (Vertex Ver in graph.Vertex)
          {

             if (!Ver.statesearchStatus && Rectangle.Intersect(new Rectangle(e.X, e.Y, 0, 0),
Ver.rect) != Rectangle.Empty)
             {
                graph.Edge.Add(edge);
                bool b = false;
                for (int i = 0; i < graph.Edge.Count; i++)
                {
                   if (graph.Edge[i].startVertex == edge.startVertex & graph.Edge[i].endVertex ==
Ver)
                   {
                      b = true;
                   }

                }

                if (!b)
                {
```

```
                    createEdge = false;

                    edge.IniInitialize(pictureBox);
                    edge.startVertex.statesearchStatus = false;
                    edge.endVertex = Ver;
                    edge = null;

                    pictureBox.Invalidate();
                    return;
                }
                else
                {

                    edge.startVertex.statesearchStatus = false;
                    edge = null;

                    createEdge = false;

                    graph.Edge.Remove(graph.Edge.Last());

                    return;
                }
            }

        }
    }

    }
    private void PictureBox_CreateEdge(object sender, MouseEventArgs e)
    {

        foreach (Vertex Ver in graph.Vertex)
        {
            if (!Ver.statesearchStatus && Rectangle.Intersect(new Rectangle(e.X, e.Y, 0, 0), Ver.rect)
!= Rectangle.Empty)
            {
                createEdge = true;
                edge = new Edge();
                edge.startVertex = Ver;
                Ver.statesearchStatus = true;
            }
        }
    }

  }


  class DynamicModelingOfTheImpactOfConcepts
  {
    private bool[] used;
```

```
    private double[,] adjacencyMatrix;
    private double[] initialVector;
    private double[] thresholds;
    private double[,] wave;
    private bool crutch;
    private List<int[]> ways;
    private List<int> r;
    private List<List<int[]>> sortedWays;
    private List<List<double[]>> valueOfIndirectEffectsOverTime;

    public ImpactSchedule calculationOfDynamicTimeAnalysis(Graph g, int time, Vertex startV,
Vertex endV)
    {
      ImpactSchedule result = new ImpactSchedule();
      ways = new List<int[]>();
      r = new List<int>();
      crutch = true;
      result.startVetex = startV.name;
      result.endVetex = endV.name;
      used = new bool[g.Vertex.Count];
      adjacencyMatrix = g.adjacencyMatrix;
      initialVector = new double[g.Vertex.Count];
      initialVector[startV.id] = 1;
      thresholds = new double[g.Vertex.Count];
      thresholds = FindingVertexThresholds(adjacencyMatrix, startV.id);
      wave = WaveCalculation(time, initialVector, adjacencyMatrix, thresholds);
      dfs(startV.id, endV.id);
      sortedWays = Rtiage(ways);

      valueOfIndirectEffectsOverTime = new List<List<double[]>>();

      for (int j = 0; j < time; j++)
      {
        valueOfIndirectEffectsOverTime.Add(new List<double[]>());

        for (int k = 0; k < sortedWays.Count; k++)
        {
          valueOfIndirectEffectsOverTime[j].Add(impactCalculation(j, wave, sortedWays[k],
adjacencyMatrix));
        }
      }

      result.schedule = calculationTotalImpact(valueOfIndirectEffectsOverTime);

      return result;

    }
    private double[] FindingVertexThresholds(double[,] mas, int start)
    {
      double[] result = new double[mas.GetLength(0)];
```

```
        for (int i = 0; i < mas.GetLength(0); i++)
        {
            for (int j = 0; j < mas.GetLength(1); j++)
            {
                if (i != start)
                {
                    result[i] += mas[j, i];
                }
                else
                {
                    result[i] = 0;
                }

            }
            if (result[i] < 0)
                result[i] = 0;

            result[i] = Math.Abs(result[i]);
            result[i] = Math.Floor(result[i]);
        }

        return result;
    }
    private double[,] WaveCalculation(int time, double[] initialVector, double[,] mas, double[]
thresholds)
    {
        double[,] result = new double[time, initialVector.Length];
        double[,] r = new double[1, initialVector.Length];

        for (int i = 0; i < initialVector.Length; i++)
        {
            r[0, i] = initialVector[i];
            result[0, i] = r[0, i];
        }

        for (int cycle = 1; cycle < time; cycle++)
        {
            r = MultiplyMatrix(r, mas);

            for (int i = 0; i < thresholds.Length; i++)
            {
                r[0, i] = Math.Abs(r[0, i]);
                if (r[0, i] >= thresholds[i])
                {
                    r[0, i] = 1;
                }
                else
                {
                    r[0, i] = 0;
                }
            }
```

```
      for (int i = 0; i < initialVector.Length; i++)
         result[cycle, i] = r[0, i];

   }
   return result;
}

private double[,] MultiplyMatrix(double[,] matrixA, double[,] matrixB)
{

   double[,] matrixC = new double[matrixA.GetLength(0), matrixB.GetLength(1)];

   for (var i = 0; i < matrixA.GetLength(0); i++)
   {
      for (var j = 0; j < matrixB.GetLength(1); j++)
      {
         matrixC[i, j] = 0;

         for (var k = 0; k < matrixA.GetLength(1); k++)
         {
            matrixC[i, j] += matrixA[i, k] * matrixB[k, j];
         }
      }
   }

   return matrixC;
}
private void dfs(int v, int end)
{
   used[v] = true;

   if (crutch)
   {
      used[v] = false;
      crutch = false;
   }

   r.Add(v);

   for (int u = 0; u < adjacencyMatrix.GetLength(0); u++)
   {
      if (adjacencyMatrix[v, u] != 0)
      {
         if (!used[u])
         {

            dfs(u, end);
            if (u == end)
            {
               used[u] = false;
```

```
                r.Add(u);

                int[] a = new int[r.Count];
                for (int i = 0; i < r.Count; i++)
                {
                    a[i] = r[i];
                }

                ways.Add(a);
                r.Remove(u);
            }
        }
    }
    used[v] = false;
    r.RemoveAt(r.Count - 1);

}
private List<List<int[]>> Rtiage(List<int[]> ways)
{
    List<List<int[]>> result = new List<List<int[]>>(); ;
    List<int> stack = new List<int>();
    stack.Add(0);

    for (int i = 1; i < ways.Count; i++)
    {
        for (int k = 0; k < ways.Count; k++)
        {
            if (ways[i][ways[i].Length - 2] == ways[k][ways[k].Length - 2])
            {
                for (int j = 0; j < stack.Count; j++)
                {
                    if (stack[j] != ways[i][ways[i].Length - 2])
                    {
                        stack.Add(ways[i][ways[i].Length - 2]);
                        stack = stack.Distinct().ToList();
                    }
                }
            }
        }
    }

    for (int i = 1; i < stack.Count; i++)
    {
        result.Add(new List<int[]>());
        for (int j = 0; j < ways.Count; j++)
        {
            if (ways[j].Length != 2)
            {
                if (stack[i] == ways[j][ways[j].Length - 2])
```

```
                {
                    result[i - 1].Add(ways[j]);
                }
            }

        }
    }

    return result;
}

private double[] impactCalculation(int time, double[,] waves, List<int[]> V, double[,]
matrix)
{

    double[] result = new double[V.Count];

    for (int i = 0; i < result.Length; i++)
    {
        result[i] = 1;
    }

    for (int i = 0; i < V.Count; i++)
    {
        for (int j = 1; j < V[i].Length; j++)
        {
            if (j == V[i].Length - 1)
            {
                result[i] *= matrix[V[i][j - 1], V[i][j]];
            }
            result[i] *= matrix[V[i][j - 1], V[i][j]] * waves[time, V[i][j - 1]];

        }
    }

    return result;

}

private double[] calculationTotalImpact(List<List<double[]>> value)
{
    double[] result = new double[ value.Count ];

    for (int i = 0; i < value.Count; i++)
    {
        for (int j = 0; j < value[i].Count; j++)
        {
            if (value[i][j].Length != 0)
            {
                result[i] += value[i][j].Max();
            }
```

```
            }
        }
        return result;
    }

}
class Edge
{
    public Vertex startVertex;
    public Vertex endVertex;

    public double weight;

    private PictureBox pictureBox;
    private NumericUpDown myNumericUpDown;

    public void IniInitialize(PictureBox pB)
    {
        myNumericUpDown = new NumericUpDown();
        pictureBox = pB;

        weight = 1;

        myNumericUpDown.Maximum = 1;
        myNumericUpDown.Minimum = -1;
        myNumericUpDown.Width = 60;
        myNumericUpDown.DecimalPlaces = 3;
        myNumericUpDown.Value = (decimal)weight;

        myNumericUpDown.ValueChanged += MyNumericUpDown_ValueChanged;

        pictureBox?.Controls.Add(myNumericUpDown);

    }

    private void MyNumericUpDown_ValueChanged(object sender, EventArgs e)
    {
        weight = (double)myNumericUpDown.Value;
    }

    public void renewalNumericLocation()
    {
        myNumericUpDown.Location = new Point(
            (startVertex.rect.X + endVertex.rect.X) / 2,
            (startVertex.rect.Y + endVertex.rect.Y) / 2
            );
    }

    public void renewalWeight()
    {
```

```
        if (weight > 1)
        {
            weight = 1;
        }
        else if (weight < -1)
        {
            weight = -1;
        }

        myNumericUpDown.Value = (decimal)weight;

    }

    public void remove()
    {
        pictureBox.Controls.Remove(myNumericUpDown);
    }

}

class Graph
{
    public List<Vertex> Vertex;
    public List<Edge> Edge;
    public double[,] adjacencyMatrix;

    public Graph()
    {
        Vertex = new List<Vertex>();
        Edge = new List<Edge>();
    }

    public void initializeMatrix()
    {
        adjacencyMatrix = new double[Vertex.Count, Vertex.Count];

        for (int i = 0; i < Vertex.Count; i++)
        {
            Vertex[i].id = i;
        }

        for (int i = 0; i < Edge.Count; )
        {
            if (Edge[i].weight != 0)
            {
                adjacencyMatrix[Edge[i].startVertex.id, Edge[i].endVertex.id] = Edge[i].weight;
                i++;
            }
            else
            {
                Edge[i].remove();
```

```
                Edge.RemoveAt(i);
                i = 0;
            }
        }
    }
    public void deleteVertex(int id)
    {
        for (int j = 0; j < Edge.Count;)
        {
            if (Edge[j].startVertex == Vertex[id] || Edge[j].endVertex == Vertex[id])
            {
                Edge[j].remove();
                Edge.RemoveAt(Edge.IndexOf(Edge[j]));
                j = 0;
            }
            else
            {
                j++;
            }
        }

        Vertex[id].remove();
        Vertex.RemoveAt(id);

        initializeMatrix();
    }
    public void Clear()
    {
        while (Vertex.Count != 0)
        {
            deleteVertex(0);
        }

        initializeMatrix();
    }

}

class ImpactSchedule
{
    public string startVetex;
    public string endVetex;
    public double[] schedule;
}

class SaveGraph
{
    public List<SaveV> Vertex = new List<SaveV>();
    public double[,] adjacencyMatrix;
}
}
```

```
class SaveV
{
    public Rectangle rect;
    public string name;
    public int id;
}
class Statistics
{
    public int totalComponents;
    public int totalConnection;
    public double density;
    public double complexityScore;
    public double hierarchyIndex;

    public int driverComponents;
    public int receiverComponents;
    public int ordinaryComponents;

    public void createStatistics(Graph g)
    {
        driverComponents = 0;
        receiverComponents = 0;
        ordinaryComponents = 0;
        hierarchyIndex = 0;


        if (g.Vertex.Count == 0)
        {
            return;
        }

        totalComponents = g.Vertex.Count;
        totalConnection = g.Edge.Count;

        density = Math.Round((double)totalConnection / (double)(totalComponents *
(totalComponents - 1)), 2);

        bool driver;
        bool receiver;

        for (int i = 0; i < g.Vertex.Count; i++)
        {
            driver = false;
            receiver = false;
            g.Vertex[i].outdegree = 0;
            g.Vertex[i].indegree = 0;
            for (int j = 0; j < g.Edge.Count; j++)
            {
                if (!driver)
                {
                    if (g.Vertex[i].name == g.Edge[j].endVertex.name)
```

```
            {
                driver = true;
            }
        }
        if (!receiver)
        {
            if (g.Vertex[i].name == g.Edge[j].startVertex.name)
            {
                receiver = true;
            }
        }

        if (g.Vertex[i].name == g.Edge[j].startVertex.name)
        {
            g.Vertex[i].outdegree += Math.Abs(g.Edge[j].weight);
        }

        if (g.Vertex[i].name == g.Edge[j].endVertex.name)
        {
            g.Vertex[i].indegree += Math.Abs(g.Edge[j].weight);
        }
    }

    if (!driver)
    {
        driverComponents++;
    }

    if (!receiver)
    {
        receiverComponents++;
    }

    if (receiver && driver)
    {
        ordinaryComponents++;
    }

    g.Vertex[i].centrality = g.Vertex[i].outdegree + g.Vertex[i].indegree;

}

complexityScore = (double)receiverComponents / (double)driverComponents;

double q = 0;
double h = 0;

for (int i = 0; i < g.Vertex.Count; i++)
{
    h += g.Vertex[i].outdegree;
}
```

```
        h /= totalComponents;

        for (int i = 0; i < g.Vertex.Count; i++)
        {
           q += Math.Pow(g.Vertex[i].outdegree - h, 2);
        }

        q /= totalComponents;

        hierarchyIndex = Math.Round((12 * Math.Pow(q, 2)) / (Math.Pow(totalComponents, 2) -
1), 2);

     }

  class Vertex
  {

     public Rectangle rect;
     public string name;
     public int id;

     public bool statesearchStatus;

     public double indegree;
     public double outdegree;
     public double centrality;

     public TextBox myTextBox;
     private PictureBox pictureBox;

     public Vertex(string n, Rectangle r, int i, PictureBox pB)
     {

        name = n;
        rect = r;
        id = i;
        pictureBox = pB;

        myTextBox = new TextBox();
        myTextBox.BackColor = Color.FromArgb(2, 115, 94);
        myTextBox.BorderStyle = BorderStyle.None;
        myTextBox.Text = name;
        myTextBox.Width = 50;

        myTextBox.TextChanged += MyTextBox_TextChanged;

        renewal();

        pictureBox?.Controls.Add(myTextBox);
     }
```

```
    private void MyTextBox_TextChanged(object sender, EventArgs e)
    {
      name = myTextBox.Text;
    }

    public void renewal()
    {
       myTextBox.Location = rect.Location;
    }

    public void remove()
    {
       pictureBox.Controls.Remove(myTextBox);
    }

}
```

Додаток Г Список публікацій за темою дисертації

[1] О. В. Салієва, та Ю. Є. Яремчук, «Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі», *Реєстрація, зберігання і обробка даних*, т. 21, № 4, с. 28–39, 2019.

[2] N. Mumtaz, A. Begum, B. Gul, S. Noor, R. Odarchenko, I. Machalin and O. Saliieva «Semantic, Digitization, Design and Implementation of Ontology in Social Internet-Services», *Conflict Management in Glodal Information Networks*, vol. 2588, pp. 228-249, 2019.

[3] О. В. Салієва, та Ю. Є. Яремчук, «Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання», *Безпека інформації*, т. 26, № 1, с. 42-49, 2020.

[4] О. В. Салієва, та Ю. Є. Яремчук, «Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень», *Захист інформації*, т. 22, № 1, с. 51–59, 2020.

[5] О. В. Салієва, та Ю. Є. Яремчук, «Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури», *Безпека інформації*, т. 26, № 2, с. 64-73, 2020.

[6] О. В. Салієва, та Ю. Є. Яремчук, «Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз», *Реєстрація, зберігання і обробка даних,* т. 22, № 2, с. 63-76, 2020.

[7] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу», *Вісник Вінницького політехнічного інституту,* № 4, с. 98-104, 2020.

[8] О. В. Салієва, та Ю. Є. Яремчук, «Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури», *Захист інформації*, т. 22, №3, с. 148–157, 2020.

[9] О. В. Салієва, та Ю. Є. Яремчук, «Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об'єкта критичної

інфраструктури», *Реєстрація, зберігання і обробка даних,* т. 22, №3, с. 68-75, 2020.

[10] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури за результатами когнітивного моделювання», *Вісник Черкаського державного технологічного університету,* №3, с. 85-93, 2020.

[11] О. В. Салієва, та Ю. Є. Яремчук, «Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності систем захисту інформації», *Вісник Вінницького політехнічного інституту,* №5, с. 56-62, 2020.

[12] О. В. Салієва, «Системологічне дослідження суб'єктів захисту інформації», у *Матеріалах XLV науково-технічної конференції підрозділів ВНТУ,* м. Вінниця, 2016, с. 2190-2191.

[13] О. В. Салієва, Я. Ю. Яремчук, «Порівняння моделей інформаційної безпеки за характеристиками суб'єктів», у *Матеріалах конференції «Управління знаннями та конкурентна розвідка»,* м. Харків, 2019, с. 67-68.

[14] О. В. Салієва, «Аналіз впливу загроз безпеці комп'ютерної мережі з використанням когнітивного моделювання», у *Матеріалах XLVII науково-технічної конференції підрозділів ВНТУ*, м. Вінниця, 2020, с. 2725-2726.

[15] О. В. Салієва, «Оцінювання рівня захищеності системи безпеки на основі когнітивного моделювання», у *Матеріалах всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи»*, м. Вінниця, 2020, с. 1215-1216.

[16] О. В. Салієва, «Визначення витрат на забезпечення захищеності системи захисту інформації ранжуванням загроз», у *Матеріалах VI Міжнародної науково-практичної конференції «Перспективні напрями захисту інформації»*, м. Одеса, 2020, с. 83-84.

[17] Ю. Є. Яремчук, О. В. Салієва, «Оцінювання рівня захищеності об'єкта критичної інфраструктури», у *Матеріалах науково-практичної конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання»,* м. Київ, 2020, с. 280-281.

[18] О. В. Салієва, «Визначення впливу загроз на рівень захищеності комп’ютерної мережі за когнітивною моделлю на основі регресійного аналізу», *у Матеріалах науково-технічної конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології»*, м. Київ, 2020, с. 105-106.

Додаток Д Акти впровадження результатів дисертації

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

21021, м. Вінниця, Хмельницьке шосе, 95
Тел.: (0432) 56-08-48 Факс: (0432) 46-57-72 Ел. пошта: vntu@vntu.edu.ua

16.11.20 № 11/32
на № _____

ЗАТВЕРДЖУЮ
Перший проректор з науково-педагогічної роботи по організації навчального процесу та його науково-методичного забезпечення Вінницького національного технічного університету
_____ О.М. Василевський
«16» 11 2020 р.

АКТ
про підтвердження впровадження результатів кандидатської дисертаційної роботи Салієвої Ольги Володимирівни «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» у навчальний процес

Цим актом підтверджується, що результати кандидатської дисертаційної роботи Салієвої О. В. «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» використовуються у Вінницькому національному технічному університеті під час читання лекцій, проведення практичних занять та лабораторних робіт з дисциплін «Захист комп'ютерних мереж», «Моделювання, прогнозування та менеджмент інформаційної безпеки», «Управління ризиками та аудит інформаційної безпеки», а також під час виконання курсового проектування для студентів, що навчаються за спеціальністю 125 «Кібербезпека». З метою підвищення якості навчання, у навчальний процес впроваджено розроблені когнітивні моделі для визначення рівня захищеності комп'ютерної мережі, системи захисту інформації та об'єкту критичної інфраструктури.

Заступник першого проректора з науково-педагогічної роботи з організації навчального процесу — Г. Л. Лисенко

Завідувач навчально-методичного відділу — Л. П. Громова

Декан факультету менеджменту та інформаційної безпеки — М. І. Небава

Завідувач кафедри менеджменту та безпеки інформаційних систем — В. В. Карпінець

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ ЗОНАЛЬНИЙ ВІДДІЛ ВІЙСЬКОВОЇ СЛУЖБИ ПРАВОПОРЯДКУ
Код 09765840
«16» 11 2020 р.
№ 4651
29000, м. Хмельницький, вул. Івана Франка,

Прим. № 4

ЗАТВЕРДЖУЮ
Начальник Хмельницького зонального відділу Військової служби правопорядку
полковник О. БЄХТЄРЄВ
«16» 11 2020 р.
м.п.

АКТ
про підтвердження впровадження результатів кандидатської дисертації
Салієвої Ольги Володимирівни

«16» листопада 2020 року м. Хмельницький

Комісія у складі:

голова комісії – начальник штабу - заступник начальника Хмельницького зонального відділу Військової служби правопорядку підполковник Хованець Павло Любомирович та члени комісії – начальник групи секретного документального забезпечення Хмельницького зонального відділу Військової служби правопорядку старший прапорщик Пальний В'ячеслав Володимирович, молодший спеціаліст групи секретного документального забезпечення Хмельницького зонального відділу Військової служби правопорядку старший солдат М'ясніков Денис Віталійович розглянувши матеріали дисертаційної роботи Салієвої Ольги Володимирівни склала цей акт про те, що результати дисертаційної роботи впроваджені при розробці комплексної системи захисту інформації в автоматизованій системі ІТС_5267-3.6 Хмельницького зонального відділу Військової служби правопорядку.

У кандидатській дисертації розроблено когнітивні моделі для дослідження рівня захищеності комп'ютерної мережі та системи захисту інформації в умовах реалізації загроз. Дані моделі є адаптованими до невизначеності вхідних даних та характеризуються простотою реалізації, наочністю, гнучкістю й конструктивністю.

Комісія підтверджує, що при розробці Салієвою О. В. комплексної системи захисту інформації використані такі результати її дисертаційної роботи:

– підхід до оцінювання рівня захищеності комп'ютерної мережі та системи захисту інформації на основі когнітивного моделювання з використанням нечітких когнітивних карт;

– когнітивні моделі для визначення рівня захищеності комп'ютерної мережі та системи захисту інформації;

Запропоновані когнітивні моделі дозволяють виявляти загальні тенденції зміни рівня захищеності комп'ютерної мережі та системи захисту інформації при впливі на них потенційних загроз. Крім того, надається можливість визначити у пропорційному відношенні до рангів загроз витрати на забезпечення захищеності досліджуваної системи та допустиму інтенсивність зниження рівня її захищеності.

Голова комісії: підполковник П. ХОВАНЕЦЬ

Члени комісії: старший прапорщик В.ПАЛЬНИЙ

старший солдат Д. М'ЯСНІКОВ

«16» листопада 2020 року

ЗАТВЕРДЖУЮ

Во.директора технічного відокремленого підрозділу «Південно-Західна електроенергетична система» приватного акціонерного товариства «Національна енергетична компанія «Укренерго»

В.В. ЛАЩЕНКО

«20» листопада 2020 року

АКТ
про підтвердження впровадження результатів кандидатської дисертації
Салієвої Ольги Володимирівни

«20» листопада 2020 року м. Вінниця

Комісія у складі: голова комісії – начальник виробничо-технічного відділу Жогов В.В., члени комісії – начальник відділу діагностики, кандидат технічних наук Лабзун М.П., начальник групи підтримки користувачів відділу ІТ та підтримки користувачів департаменту автоматики, інформаційних технологій та зв'язку Дудченко І.А. , керівник режимно-секретного органу та спецзв'язку Андрющенко О.С., розглянувши матеріали дисертаційної роботи «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» Салієвої Ольги Володимирівни склала цей акт про те, що результати дисертаційної роботи впроваджені при розробці комплексної системи захисту інформації в автоматизованій системі режимно-секретного органу відокремленого підрозділу «Південно-Західна електроенергетична система» приватного акціонерного товариства «Національна енергетична компанія «Укренерго» (далі за текстом – Південно-Західна ЕС).

Особливістю розробленої системи захисту є використання когнітивної моделі для дослідження рівня захищеності інформації об'єкта критичної інфраструктури, що сприятиме збільшенню швидкості обробки вхідної інформації та зменшенню часу на її опрацювання за рахунок використання доступної експертної інформації без збору і обробки статистичних даних; покращенню наочності представлення даних; вирішенню задач, що не піддаються строгій формалізації; використанню неповної, нечіткої інформацію та суб'єктивних суджень експертів предметної області; простому розширенню кількості факторів, за рахунок введення додаткових вершин і дуг графа когнітивної карти; прогнозуванню розвитку ситуацій щодо можливої реалізації потенційних загроз.

Комісія підтверджує, що при розробці Салієвою О. В. комплексної системи захисту інформації в Південно-Західній ЕС використані такі результати її дисертаційної

роботи:

– підхід до оцінювання рівня захищеності об'єкта критичної інфраструктури на основі когнітивного моделювання з використанням нечітких когнітивних карт;

– когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури.

Розроблена когнітивна модель для дослідження рівня захищеності інформації об'єкта критичної інфраструктури надала можливість прослідкувати відносну зміну захищеності досліджуваної системи при впливі загроз та визначити найвагоміші з них. На основі результатів сценарного моделювання було розроблено чіткий план управління, спрямований на підвищення захищеності інформації об'єкта критичної інфраструктури – Південно-Західної ЕС, діяльність якого є важливою для функціонування держави.

Відповідно до п. 3.5 Статуту приватного акціонерного товариства «Національна енергетична компанія «Укренерго», затвердженого наказом Міністерства фінансів України від 29 липня 2019 року № 321

«Товариство здійснює свою діяльність без застосування печатки».

Голова комісії В.В. Жогов

Члени комісії М.П. Лабзун

І.А. Дудченко

О.А. Андрющенко

ПЕНСІЙНИЙ ФОНД УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ ПЕНСІЙНОГО ФОНДУ УКРАЇНИ
У ВІННИЦЬКІЙ ОБЛАСТІ

Хмельницьке шосе, 7, м. Вінниця,21100 Тел./факс(0432) 66-02-95 E-mail gu@vn.pfu.gov.ua Код ЄДРПОУ 13322403

_____ № _____ На № _____від

ЗАТВЕРДЖУЮ
Заступник начальника
головного управління
Пенсійного фонду України
у Вінницькій області
_____М.Ю.Єрошенко
«___»_____2020р.

АКТ
про підтвердження впровадження результатів кандидатської дисертації
Салієвої Ольги Володимирівни

Комісія у складі:

голова комісії – заступник начальника управління Єрошенко Марина Юліївна та члени комісії – начальник Управління інформаційних систем та електронних реєстрів Криклива Ольга Іванівна та головний спеціаліст Відділу адміністрування інформаційних систем Управління інформаційних систем та електронних реєстрів Колосова Олена Едуардівна, розглянувши матеріали дисертаційної роботи Салієвої Ольги Володимирівни, склала цей акт про те, що результати даної дисертаційної роботи впроваджені при розробці та впровадженні комплексної системи захисту інформації в автоматизованій системі головного управління Пенсійного фонду України у Вінницький області.

Характерною особливістю розробленої системи захисту є використання когнітивних моделей для аналізу впливу загроз на рівень захищеності комп'ютерної мережі та системи захисту інформації. Це надає можливість формалізувати чисельно не вимірювальні фактори, використовувати неповну й нечітку вхідну інформацію, з легкістю інтерпретувати причинно-наслідкові зв'язки досліджуваної системи і наглядно представляти їх, використовувати суб'єктивні судження експертів.

Комісія підтверджує, що при розробці Салієвою О. В. комплексної системи захисту інформації використані такі результати її дисертаційної роботи:

– підхід до оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах на основі когнітивного моделювання з використанням нечітких когнітивних карт;

– когнітивна модель для аналізу впливу загроз на рівень захищеності комп'ютерної мережі;

– когнітивна модель для визначення рівня захищеності системи захисту інформації.

Розроблена когнітивна модель для аналізу впливу загроз на рівень захищеності комп'ютерної мережі надала можливість спрогнозувати стан мережевої безпеки, що, у свою чергу, посприяло впровадженню необхідних механізмів попередження, захисту та контролю доступу на відповідних рівнях мережевої інфраструктури. В свою чергу, когнітивна модель для визначення рівня захищеності системи захисту інформації дозволила підвищити рівень захищеності досліджуваної системи.

Голова комісії М. Ю. Єрошенко

Члени комісії О.І. Криклива

О. Е. Колосова