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.