https://doi.org/10.31649/1997-9266-2020-152-5-56-62

УДК 519.1:004.81.056.5

О. В. Салієва[1]
Ю. Є. Яремчук[1]

ДОСЛІДЖЕННЯ ІМПУЛЬСНИХ ПРОЦЕСІВ НА КОГНІТИВНІЙ КАРТІ ДЛЯ ВИЗНАЧЕННЯ ЗМІНИ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

[1]Вінницький національний технічний університет

Характерною особливістю XXI століття є впровадження високоінтелектуальних інформаційних технологій в усі сфери суспільної діяльності, яке породжує низку небезпек, пов'язаних зі стрімким розвитком різноманітних загроз. Тому наразі актуальними є задачі забезпечення надійного та безпечного функціонування систем захисту інформації та підвищення рівня їхньої захищеності. Для розв'язання таких задач важливо своєчасно виявити загрози, встановивши при цьому зміну рівня захищеності досліджуваної системи. У зв'язку з цим, у роботі пропонується провести дослідження імпульсних процесів на нечіткій когнітивній карті для визначення зміни рівня захищеності системи захисту інформації. Ця 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 матриці дозволив для простих імпульсних процесів з визначеними початковими вершинами встановити зміну рівня захищеності системи захисту інформації. Крім того, серед множини усіх концептів когнітивної карти виділено найвагоміші, які внаслідок імпульсного процесу найбільшою мірою вплинуть на захищеність досліджуваної системи. Для автоматизації імпульсного моделювання розроблено програмний засіб, який надає змогу наочно представити еволюційний розвиток системи при внесенні збурення у концепт чи декілька концептів когнітивної карти.

Результати, отримані внаслідок проведення цього дослідження, сприятимуть покращенню прогнозування розвитку ситуацій у разі реалізації ймовірних загроз, що, у свою чергу, підвищить ефективність прийняття своєчасних рішень, спрямованих на підвищення захищеності системи захисту інформації.

Ключові слова: система захисту інформації, загроза, захищеність, нечітка когнітивна карта, імпульсний процес.

Вступ

На сучасному етапі розвитку суспільства спостерігається інтенсивне впровадження інформаційних технологій у різноманітні процеси людської діяльності. Разом з тим, зростає і рівень інформаційних загроз, що зумовлює посилення вимог до захищеності систем захисту інформації, порушення функціонування яких може спричинити вкрай важкі наслідки. Тому вирішенню цього питання приділяється значна увага як українських, так і закордонних дослідників.

Зокрема, у статті [1] запропоновано алгоритм оцінювання роботи в системах захисту інформації для аналізу ризиків інсайдерських загроз та вживання заходів щодо їх зниження. У роботі [2] на основі теорії графів розроблено модель загроз, які виникають при управлінні системою захисту інформації. Автори праці [3] проаналізували актуальні загрози інформаційній безпеці, зокрема, детально дослідили методи соціальної інженерії та сформулювали рекомендації стосовно захисту від фішингових атак. З метою забезпечення інформаційної безпеки у роботі [4] розглянуто можливість впровадження теорії та методу машинного навчання для виявлення вторгнень у систему. У роботі [5] проведено детальний аналіз загроз та вразливостей кібербезпеки, у результаті чого виділено серед них ключові та визначено частоту їх виникнення. Автори праці

[6] застосували регресивні моделі для прогнозування виникнення загроз, що сприяло покращенню аналізу ризиків інформаційної безпеки.

Застосування когнітивного підходу до вирішення цієї проблематики відображається у роботі [7], де запропоновано когнітивну модель, яка базується на нечіткій когнітивній карті (НКК) [8] для визначення рівня захищеності системи захисту інформації. Проведене у цій роботі сценарне моделювання дозволяє при заданому значенні впливу конкретних загроз розглянути відносну зміну безпосередньо з'єднаних концептів, проте не надає змогу дослідити еволюційний розвиток усієї системи. Цю задачу можна вирішити за допомогою імпульсного моделювання [9], в якому об'єкт дослідження розглядається як сукупність взаємодіючих між собою динамічних процесів, що відбуваються 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. Таким чином, актуальним є визначення зміни рівня захищеності системи захисту інформації у разі впливу на неї потенційних загроз на основі імпульсного моделювання.

Метою роботи є дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту, що дозволить підвищити якість прогнозування розвитку ситуацій.

Визначення зміни рівня захищеності системи захисту інформації шляхом моделювання імпульсних процесів на когнітивній карті

Одним з широко використовуваних методів кількісного аналізу НКК є імпульсний, який надає можливість простежити як вплине збурення, внесене в одну або декілька вершин когнітивної карти, на інші вершини та систему в цілому.

Змоделюємо імпульсні процеси розповсюдження збурень, введених почергово в усі вершини НКК, запропонованої у роботі [7] (рис. 1).

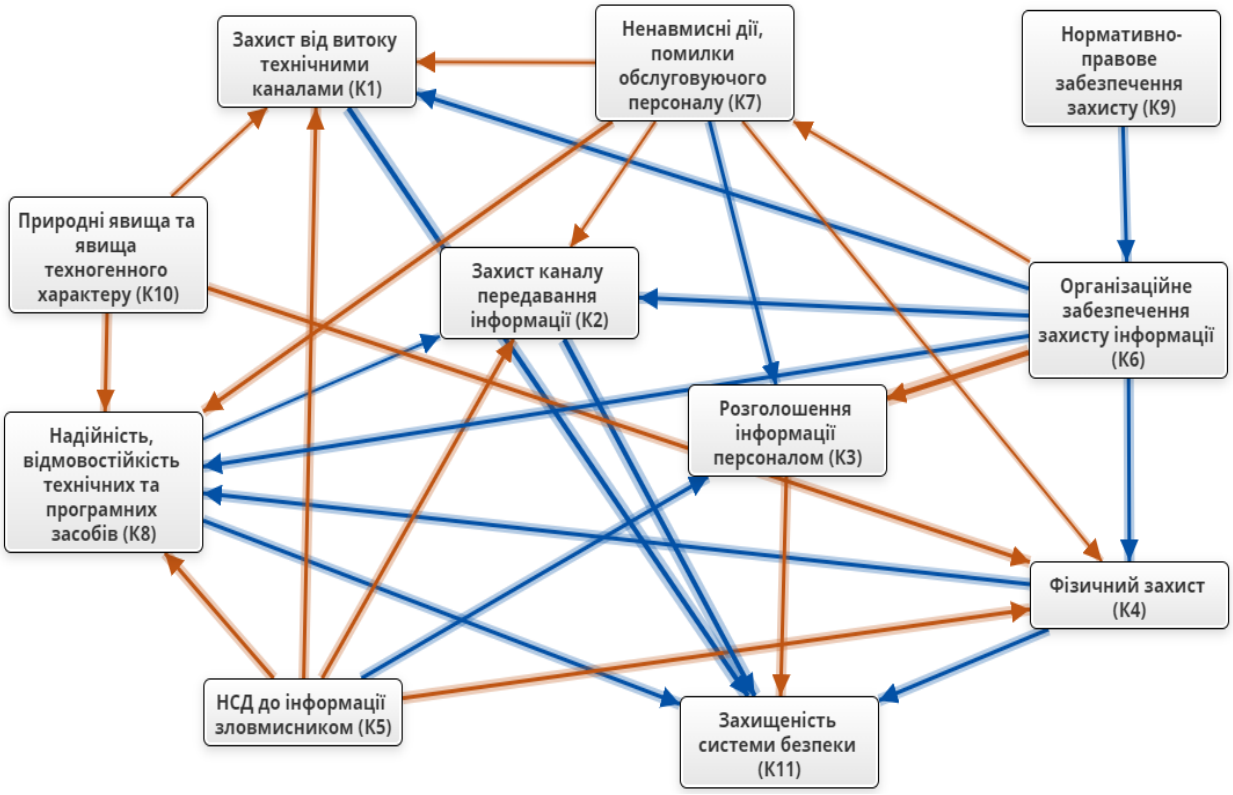

Рис. 1. Нечітка когнітивна карта для визначення рівня захищеності системи захисту інформації

Вирішимо поставлене завдання за допомогою матриці транзитивного замикання M [9]:

$$M = E + W + W^2 + ... + W^n, \quad (1)$$

де W — матриця суміжності НКК; n — порядок матриці W.

Для досліджуваної когнітивної моделі матриця суміжності матиме вигляд (табл. 1):

Таблиця 1

Матриця суміжності НКК для визначення рівня захищеності системи захисту інформації

	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

Тоді, відповідно до формули (1) отримаємо матрицю транзитивного замикання M (табл. 2).

Таблиця 2

Матриця транзитивного замикання НКК для визначення рівня захищеності системи захисту інформації

	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 [9]:

$$p_j(t) = \left\{ \text{елемент } i,\ j \text{ матриці } W^n \right\}, \tag{2}$$

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

$$V_j(t) = V_j(0) + \left\{ \text{елемент } i,\ j \text{ в матриці } E + W + W^2 + ... + W^n \right\}. \tag{3}$$

Враховуючи формулу (3) та значення елементів матриці транзитивного замикання (табл. 2), 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 безпеки 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 одно-

го стану в інший та визначити ті концепти, які найбільше послаблюватимуть або ж підсилюватимуть захищеність системи захисту інформації. Виходячи з цього, проведено аналіз значень елементів матриці транзитивного замикання досліджуваної НКК, який показав, що при внесенні імпульсу в концепт K_6 — організаційне забезпечення захисту інформації, концепт K_{11} — захищеність системи безпеки збільшиться до максимального значення — 3,8. З метою наочного представлення реакції системи захисту інформації 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. 2).

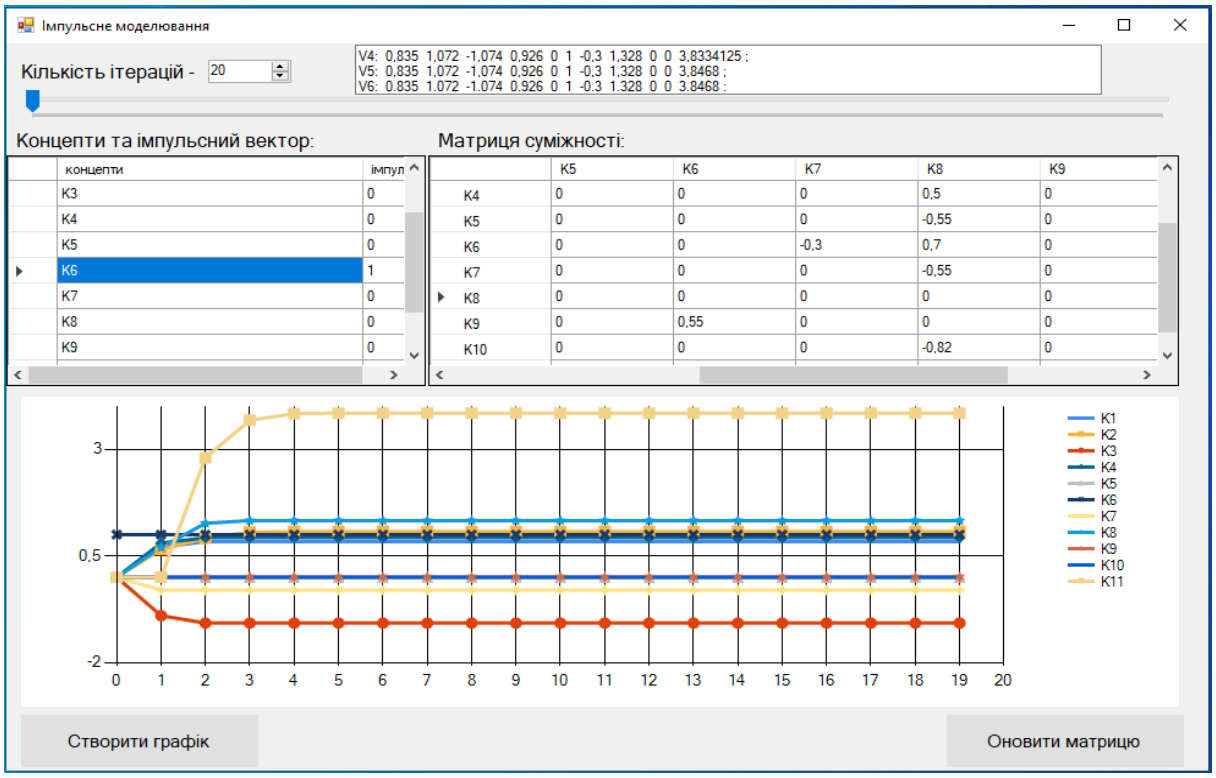

Рис. 2. Стан концептів досліджуваної системи при введенні імпульсу у вершину K_6

Аналіз графіка (рис. 2) показав, що K_{11} — захищеність системи безпеки 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, зменшаться 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 безпеки максимально послабиться (до 2,9) при внесенні імпульсу у K_5 — НСД до інформації зловмисником, та спостерігатиметься така зміна досліджуваної системи (рис. 3).

Аналіз графіка рис. 3 свідчить про те, що K_{11} — захищеність системи безпеки 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 захисту інформації та K_5 — НСД до інформації зловмисником, захищеність системи безпеки набуває екстремальних значень. Отже, ці концепти є найвагомішими концептами досліджуваної системи, що також підтверджується результатами роботи [7] внаслідок проведення структурно-топологічного аналізу когнітивної карти.

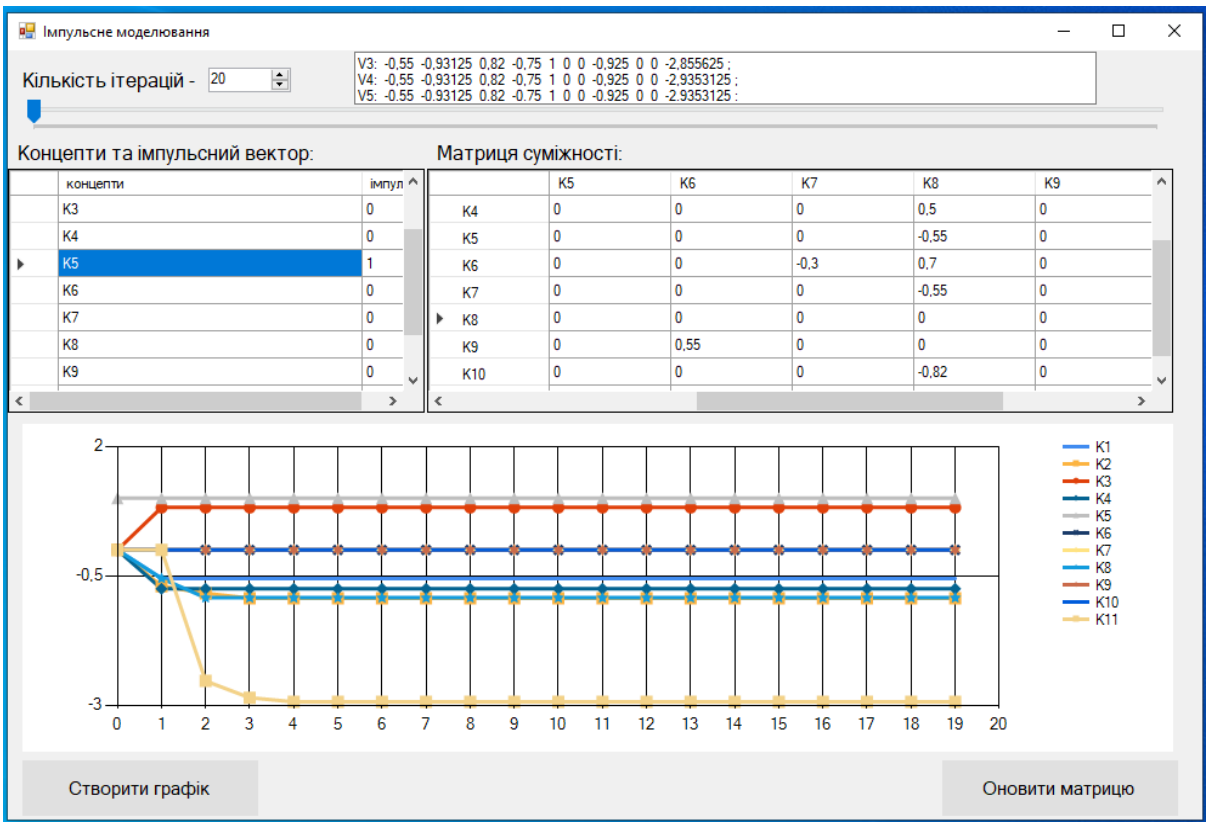

Рис. 3. Стан концептів досліджуваної системи при введенні імпульсу у вершину K_5

Отримані результати сприятимуть підвищенню якості прогнозування розвитку ситуації, що дозволить вчасно приймати необхідні рішення та вживати заходи для забезпечення захищеності систем захисту інформації.

Висновки

У роботі проведено дослідження розвитку у часі розробленої авторами когнітивної моделі для визначення зміни рівня захищеності системи захисту інформації, шляхом введення імпульсних впливів у концепти когнітивної карти. Це дослідження дає змогу прослідкувати еволюційний розвиток системи й на основі отриманих результатів підвищити ефективність прогнозування і, відповідно, прийняття управлінських рішень.

Для досягнення поставленої мети побудовано матрицю транзитивного замикання НКК предметної області. Аналіз матриці дозволив для простих імпульсних процесів з початковими вершинами K_1 (захист від витоку технічними каналами) та K_2 (захист каналу передавання інформації) встановити збільшення значення K_{11} (захищеність системи безпеки), відповідно, до 0,9 і 0,85. Водночас, для початкової вершини K_3 (розголошення інформації персоналом) захищеність зменшиться до 0,75.

Окрім того, визначено найвагоміші концепти системи, які у наслідок імпульсного процесу найбільшою мірою впливатимуть на захищеність системи безпеки. А саме K_6 (організаційне забезпечення захисту інформації) підвищить максимально захищеність до 3,8 та K_5 (НСД до інформації зловмисником) максимально знизить значення досліджуваного концепту до 2,9. Визначені найвагоміші концепти збігаються з отриманими у роботі [7] внаслідок структурно-топологічного аналізу досліджуваної когнітивної карти.

Проведений імітаційний експеримент ілюструє можливі варіанти розвитку ситуації у віртуальному середовищі за допомогою розробленого програмного засобу, який дає змогу наочно відобразити реакцію системи на розповсюдження збурення по НКК для визначення рівня захищеності системи захисту інформації. Це, у свою чергу, дозволить підвищити якість прогнозування розвитку ситуацій у разі впливу ймовірних загроз та вчасно вжити комплексні заходи (технічні, адміністративні тощо) для забезпечення захищеності досліджуваної системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] В. В. Корчинський, Халед Аль-Файюми, Ю. В. Копитін, і М. В. Копитіна, «Ризики інсайдерських загроз в системах захисту інформації підприємств,» *Наукові праці ОНАЗ ім. О. С. Попова*, № 2, с. 112-116, 2019.

[2] М. Л. Соловьев, Т. Е. Минеева, А. А. Конев, и Д. Н. Буинцев, «Модель угроз безопасности, возникающих при управлении системой защиты информации,» *Доклады ТУСУР*, т. 22, № 3, с. 31-36, 2019.

[3] Д. Мехед, Ю. Ткач, і В. Базилевич, «Дослідження технологій впливу та методів протидії фішингу,» *Захист інформації*, т. 21, № 4, с. 246-251, 2019.

[4] F. Weijian, T. Xiaoling, and W. Dominic, «Research on machine learning method and its application technology in intrusion information security detection,» *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 2, pp. 1549-1558, 2020.

[5] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, «Cyber Security Threats and Vulnerabilities: a Systematic Mapping Study,» *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171-3189, 2020.

[6] P. T. Figueira, C. L. Bravo, and J. L. R. López, «Improving information security risk analysis by including threat-occurrence predictive models,» *Computers & Security*, vol. 88, pp. 1-9, 2020.

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

[8] B. Kosko, «Fuzzy Cognitive Maps», *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[9] Ф. С. Робертс, *Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам*. Москва: Наука, 1986, 496 с.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 19.11.2020

Салієва Ольга Володимирівна — асистент кафедри менеджменту та безпеки інформаційних систем;

Яремчук Юрій Євгенович — д-р техн. наук, професор, професор кафедри менеджменту та безпеки інформаційних систем, директор Центру інформаційних технологій і захисту інформації, e-mail: yurevyar@gmail.com

Вінницький національний технічний університет, Вінниця

O. V. Saliieva[1]
Yu. Ye. Yaremchuk[1]

Investigation of Impulse Processes on a Cognitive Map to Determine Changes in the Level of Security of the Information Security System

[1]Vinnytsia National Technical University

A characteristic feature of the XXI century is the introduction of highly intelligent information technology in all spheres of public activity, which creates a number of dangers associated with the rapid development of various threats. Therefore, issues related to ensuring the reliable and secure operation of information protection systems and increasing their level of security are currently relevant. To solve these problems, it is important to identify threats in a timely manner, while establishing a change in the level of security of the studied system. In this regard, it is proposed to conduct a study of impulse processes on a fuzzy cognitive map to determine changes in the level of security of the information security system. This technique is based on the propagation of the impulse introduced into the concept (or several concepts) of the cognitive map, which spreads through the system amplifies or fades.

To achieve this goal, a matrix of transitive closure is formed, which reflects the change in the state of each system concept at the time of stabilization of the pulse process. The analysis of this matrix allowed for simple pulse processes with certain initial vertices to establish a change in the level of security of the information security system. In addition, the most important concepts of the cognitive map have been identified, which as a result of the impulse process will have the greatest impact on the security of the studied system. To automate pulse modeling, a software tool has been developed that allows to visualize the evolutionary development of the system when introducing perturbations into a concept or several concepts of the cognitive map.

The results of this study will improve the forecasting of situations in the implementation of potential threats, which, in turn, will increase the effectiveness of timely decisions aimed at improving the security of the information security system.

Keywords: information security system, threat, security, fuzzy cognitive map, impulse process.

Saliieva Olha V. — Assistant of the Chair of Management and Security of Information Systems;

Yaremchuk Yurii Ye. — Dr. Sc. (Eng.), Professor of the Chair of Management and Security of Information Systems, Head of the Center of Information Technologies and Information Security, e-mail: yurevyar@gmail.com

О. В. Салиева[1]
Ю. Е. Яремчук[1]

Исследование импульсных процессов на когнитивной карте для определения изменения уровня защищенности системы защиты информации

[1]Винницкий национальный технический университет

Характерной особенностью XXI века является внедрение высокоинтеллектуальных информационных технологий во все сферы общественной деятельности, которое порождает ряд опасностей, связанных со стремительным развитием угроз. Поэтому сейчас актуальны вопросы, касающиеся обеспечения надежного и безопасного функционирования систем защиты информации и повышения уровня их защищенности. Для решения этих задач важно своевременно выявить угрозы, установив при этом изменение уровня защищенности исследуемой системы. В связи с этим в работе предлагается провести исследование импульсных процессов на нечеткой когнитивной карте для определения изменения уровня защищенности системы защиты информации. Эта методика базируется на распространении импульса, введенного в концепт (или несколько концептов) когнитивной карты, который, распространяясь по системе, усиливается или угасает.

Для достижения поставленной цели сформирована матрица транзитивного замыкания, которая отражает изменение состояния каждого концепта системы в момент стабилизации импульсного процесса. Анализ матрицы позволил для простых импульсных процессов с определенными начальными вершинами установить изменение уровня защищенности системы защиты информации. Кроме того, определены наиболее значимые концепты когнитивной карты, которые вследствие импульсного процесса в наибольшей степени повлияют на защищенность исследуемой системы. Для автоматизации импульсного моделирования разработано программное средство, дающее возможность наглядно представить эволюционное развитие системы при внесении возмущения в концепт или несколько концептов когнитивной карты.

Результаты, полученные в результате проведения исследования, будут способствовать улучшению прогнозирования развития ситуаций при реализации вероятных угроз, что, в свою очередь, повысит эффективность принятия своевременных решений, направленных на повышение защищенности системы защиты информации.

Ключевые слова: система защиты информации, угроза, защищенность, нечеткая когнитивная карта, импульсный процесс.

Салиева Ольга Владимировна — ассистент кафедры менеджмента и безопасности информационных систем;

Яремчук Юрий Евгеньевич — д-р техн. наук, профессор, профессор кафедры менеджмента и безопасности информационных систем, директор Центра информационных технологий и защиты информации, e-mail: yurevyar@gmail.com