https://doi.org/10.31891/2307-5732-2026-361-34
УДК 637.5.02

ХЛІБОЙКО МИХАЙЛО
Західноукраїнський національний університет
https://orcid.org/0009-0000-7613-8899
e-mail: mihayloh.com@gmail.com

МОДЕЛЮВАННЯ ПРИЧИННО-НАСЛІДКОВИХ ПОДІЙ У БЕЗПЕЦІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ НЕЧІТКИХ КОГНІТИВНИХ КАРТ

У цій роботі представлено методику моделювання причинно-наслідкових зв'язків між подіями, що впливають на функціональну безпеку інформаційних систем, застосовуючи нечіткі когнітивні карти та нейро-нечіткі технології.

Ключові слова: *нечіткі когнітивні карти, нейро-нечіткі методи, причинно-наслідкове моделювання, оцінка ризиків, системи виявлення вторгнень.*

KHLIBOIKO MYKHAILO
West Ukrainian National University

MODELING CAUSE-AND-EFFECT EVENTS IN INFORMATION SYSTEMS SECURITY USING FUZZY COGNITIVE MAPS

This paper presents a methodology for modeling cause-and-effect relationships between events impacting the functional safety of information systems, utilizing fuzzy cognitive maps and neuro-fuzzy technologies. The described model and approach effectively assess the level of risk and functional safety of information systems under conditions of uncertainty, taking into account complex interactions between information assets, vulnerabilities, and cyber threats, thereby providing insights into the system's security state.

The article describes the use of fuzzy cognitive maps based on expert assessments, weight tuning through neuro-fuzzy learning, and the modeling of cyberattack scenarios. The proposed approach includes tools for modeling cyberattack scenarios, enabling the evaluation of the likelihood of successful attacks and the identification of critical system points requiring additional protection.

The method is beneficial for intrusion detection systems and the security assessment of cloud and enterprise information systems. The article also discusses the limitations of the analyzed model, namely the high quality of expert assessments and the computational complexity of analyzing large systems with numerous interconnections. To address these challenges, optimization of algorithms using neuro-fuzzy methods, particularly an adaptive neuro-fuzzy inference system, and the use of parallel computing are proposed. Future research aims to extend the model's application to Internet of Things systems, where there is potential for assessing quality and functional safety, enabling the development of new methods that account for the identified limitations and integrate with machine learning technologies.

Keywords: *fuzzy cognitive maps, neuro-fuzzy methods, cause-and-effect modeling, risk assessment, intrusion detection systems.*

Стаття надійшла до редакції / Received 07.12.2025
Прийнята до друку / Accepted 11.01.2026
Опубліковано / Published 29.01.2026

Постановка проблеми

Сучасні інформаційні системи (ІС) відіграють важливу роль в інфраструктурі організацій, але їхня комплексна структура та постійна мінливість генерують серйозні труднощі в забезпеченні безпеки. Збільшення кількості кібератак, включаючи розподілені атаки на відмову в обслуговуванні (DDoS), витоки даних та зловмисне програмне забезпечення, вказує на нагальну потребу в ефективних способах оцінки та керування ризиками безпеки. Звичайні підходи, такі як статистичні моделі або мережі Байєса, часто не можуть врахувати невизначеності та нелінійні причинно-наслідкові взаємодії, властиві для сучасних загроз. У цьому плані, нечіткі когнітивні карти (НКК) представляють собою перспективний інструмент для моделювання складних систем, що дозволяє враховувати нечіткі залежності та експертні знання.

Інтеграція нейро-нечітких методів з нечіткими когнітивними картами відкриває нові горизонти для адаптивного моделювання причинно-наслідкових подій у безпеці ІС. Ці методи дозволяють обробляти невизначеність, динамічно коригувати ваги зв’язків та покращувати точність прогнозування ризиків. У статті розглянуто теоретичні основи, запропоновано методологію побудови моделі причинно-наслідкових подій у безпеці інформаційних систем, проаналізовано результати експериментів та оцінено практичну значущість запропонованого підходу.

Аналіз досліджень та публікацій

Актуальність питання моделювання причинно-наслідкових зв'язків в безпеці інформаційних систем зумовлена стрімким ускладненням кіберзагроз та невизначеністю в процесі оцінки ризиків. Вплив штучного інтелекту на стратегії захисту інформаційних систем від нових типів кіберзагроз описано авторами у статті [1]

Нечіткі когнітивні карти зарекомендували себе як ефективний інструмент аналізу складних систем, де взаємодія між компонентами має причинний характер, що знаходить застосування в функціональній безпеці ІС, як описують автори [2, 3, 4, 5].

Запропоновані в науковій праці [6] НКК надають можливість моделювати взаємозалежності між концептами (уразливостями, загрозами, активами), використовуючи вагові матриці, що визначають ступінь їх взаємовпливу та робить їх особливо корисними в умовах невизначеності [7, 8].

Сучасні наукові дослідження свідчать про широке використання НКК в різноманітних сферах інформаційної безпеки. Наприклад, в праці [9] НКК застосовуються для оцінки ризиків кібербезпеки в телемедичних системах, де вони відображають причинні зв'язки між різними аспектами безпеки, такими як витік даних або несанкціонований доступ. Дослідження [10] продемонстрували, як НКК дають змогу розробляти сценарії кіберзагроз, враховуючи експертні оцінки, висловлені з використанням нечітких понять, що сприяє підвищенню точності прогнозування ризиків. Аналогічно, автори [11] створили модель оцінки ризиків інформаційної безпеки на основі правил, використовуючи НКК для роботи з нечіткими даними.

Інтеграція нейро-нечітких методів із НКК значно збагачує їхній потенціал. Автори [12] презентували двоступеневу модель, поєднуючи НКК із нейронними мережами для прогнозування часових рядів, яка може бути адаптована до динамічних кіберзагроз. Аналогічний підхід описаний у [13], де нейро-нечіткі методи використовуються для посилення захисту IoT-систем, моделюючи причинно-наслідкові події. У роботі [14] використали НКК, щоб створити інтелектуальну систему безпеки, враховуючи невизначеності в причинно-наслідкових зв'язках. Дослідження [15, 16] також підкреслюють розширення НКК для підвищення їх адаптивності.

Автори [17] провели систематичний огляд розширень НКК, включаючи методи обробки зашумлених даних та динамічної оптимізації. Крім того, еволюційні алгоритми для навчання НКК, описані в [18], дозволяють автоматично налаштовувати ваги зв'язків, зменшуючи залежність від суб'єктивних оцінок експертів.

НКК також знаходять застосування у моделюванні складних кіберфізичних систем, де вони аналізують взаємозв'язки між апаратними та програмними компонентами. Наприклад, автори [9] застосували НКК для оцінки стійкості інфраструктур, включаючи ІС, до зовнішніх загроз. У контексті управління кризовими ситуаціями автори [15] продемонстрували ефективність НКК у моделюванні взаємозалежностей у критичних системах, що може бути адаптовано до потреб кібербезпеки [19, 20]. В науковій статті [21] розроблено методи виявлення причинно-наслідкових зв'язків у зашумлених наборах НКК, що важливо для аналізу реальних даних у системах безпеки.

Попри значний прогрес, все ще зберігаються помітні прогалини у цій галузі. Переважна більшість існуючих моделей НКК залежить від експертних оцінок для визначення ваг між концептами, що може вносити суб'єктивність в кінцевий результат. Інтеграція нейро-нечітких систем з НКК для опрацювання динамічних загроз у реальному часі поки що не є достатньо вивченою. Також бракує моделей, здатних одночасно враховувати як технічні (вразливості, атаки), так і організаційні (політики, людський фактор) аспекти безпеки, а дослідження з масштабування НКК для великих інформаційних систем з тисячами концептів обмежені [2, 7, 11, 15].

Отже, незважаючи на великий потенціал НКК та нейро-нечітких методів у моделюванні причинно-наслідкових зв’язків у системах інформаційної безпеки, потрібні додаткові дослідження, спрямовані на автоматизацію навчання моделей, обробку динамічних даних у режимі реального часу та інтеграцію технічних та організаційних факторів [18].

Мета роботи: розглянути та проаналізувати модель на основі НКК з нейро-нечітким навчанням для оцінювання причинно-наслідкових подій у безпеці інформаційних систем.

Виклад основного матеріалу

Запропонована модель для моделювання причинно-наслідкових подій у системах інформаційної безпеки базується на нечітких когнітивних картах. Це забезпечує ефективне опрацювання невизначеностей та нелінійних взаємодій між елементами безпеки. Модель використовує нейро-нечіткі методи для адаптивного навчання та оптимізації. Такий підхід збільшує точність та стійкість моделі до змінних кібернетичних загроз.

Нечіткі когнітивні карти використовують для моделювання системи як сукупність концептів (A_i), кожен з яких описує ключовий аспект інформаційної безпеки, зокрема, уразливості, загрози, активи чи засоби протидії. У цій моделі концепти було визначено на основі аналізу типових кібернетичних атак, наприклад, DDoS-атак, витоків інформації або несанкціонованого доступу, наприклад [2]:

1. (A_1): Рівень вразливості системи.
2. (A_2): Ймовірність атаки.
3. (A_3): Цінність активу.
4. (A_4): Ефективність контрзаходів.
5. (A_5): Рівень ризику.

Кожен концепт (A_i) має значення активації:

$$A^{k+1} = f(A^k \cdot W)\,, \tag{1}$$

Рівень активації обчислюється через нечітку логіку, де 0 означає відсутність впливу, а 1 - найбільший вплив. Початкові значення ($A_i(0)$) визначаються на основі експертної оцінки або емпіричних даних, взятих з логів безпеки [8, 11].

Матриця зв’язків є основою НКК і визначає причинно-наслідкові відношення між концептами. Вона представлена як матриця ваг (W), де елемент (w_{ij} $[-1,1]$) відображає силу впливу концепту (A_i) на концепт (A_j):

1. ($w_{ij} > 0$): Позитивний вплив (зростання (A_i) сприяє зростанню (A_j)).
2. ($w_{ij} < 0$): Негативний вплив (зростання (A_i) зменшує (A_j)).
3. ($w_{ij} = 0$): Відсутність зв’язку.

Матриця (W) будується на основі експертних знань або аналізу даних. Наприклад, для системи з п’ятьма концептами матриця (W) має вигляд [6]:

$$W = \begin{bmatrix} 0 & w_{12} & w_{13} & w_{14} & w_{15} \\ w_{21} & 0 & w_{23} & w_{24} & w_{25} \\ w_{31} & w_{32} & 0 & w_{34} & w_{35} \\ w_{41} & w_{42} & w_{43} & 0 & w_{44} \\ w_{51} & w_{52} & w_{53} & w_{54} & 0 \end{bmatrix}, \quad (2)$$

Оновлення стану концептів, описане авторами [3, 4, 6], здійснюється за ітераційним правилом:

$$A_i(t+1) = f\left(\sum_{j=1}^{N} w_{ij} A_j(t)\right), \quad (3)$$

де (f) — функція активації, яка нормалізує значення в діапазоні [0, 1]. Сигмоїдна функція обрана через її здатність обробляти нелінійні залежності, що є типовим для систем безпеки.

Для адаптації вагових коефіцієнтів (w_{ij}) та поліпшення точності моделювання використовуються нейро-нечіткі підходи, зокрема адаптивна нейро-нечітка система висновку. Адаптивна нейронечітка система логічного висновку (ANFIS) поєднує в собі нечітку логіку та нейронні мережі, забезпечуючи автоматичне коригування вагових коефіцієнтів матриці (W) на основі даних для навчання. Навчання відбувається у кілька етапів:

1. Ініціалізація ваг: Початкові ваги (w_{ij}) встановлюються за експертними оцінками або випадковим чином у діапазоні [-1, 1].

2. Формування навчального набору: Використовуються історичні дані безпеки (наприклад, логи атак) для створення пар.

3. Навчання ANFIS: Нейронна мережа оптимізує функції належності нечітких множин, використовуючи алгоритм зворотнього поширення помилки або гібридний метод (градієнтний спуск, плюс метод найменших квадратів).

4. Оновлення НКК: Оптимізовані ваги застосовуються до матриці (W), після чого модель повторно обчислює стани концептів для оцінки ризиків [9, 12].

Такий підхід дає можливість моделі пристосовуватися до змін у безпеці інформаційних систем, які постійно відбуваються, зокрема, до виникнення нових слабких місць або зміни стратегій атак. Додатково, для опрацювання даних із шумом, застосовується розширення НКК , засноване на сірій теорії, що підвищує захищеність від невизначеностей [10, 14].

Для моделювання взаємопов'язаних подій у сфері безпеки інформаційних систем із використанням нечітких когнітивних карт пропонується алгоритм, що складається з трьох ключових етапів: збір інформації, встановлення причинно-наслідкових взаємодій та обчислення нечітких вагових коефіцієнтів. Цей алгоритм ґрунтується на актуальних методиках створення НКК, пристосованих до аналізу кібербезпеки [2, 4, 7].

Перший крок полягає у здобутті відомостей, що стануть основою для створення НКК. Стосовно інформаційної безпеки, ці дані можуть вміщати як експертні судження, так і аналіз логів безпеки. Експертні оцінки отримують через опитування фахівців із кібербезпеки, які визначають ключові поняття та взаємозв'язки між ними. Аналіз логів безпеки надає емпіричні дані про події, такі як спроби атак, мережевий трафік або аномалії. Логи обробляють, вдаючись до автоматизованих інструментів аналізу, таких як Splunk або ELK Stack, задля виявлення повторюваних патернів і причинно-наслідкових зв'язків. Наприклад, лог може вказати на зв’язок між невдалою аутентифікацією та подальшою DDoS-атакою, що послужить основою для побудови моделі [6, 7, 9, 11]

На основі зібраних даних будується граф НКК, де вузли (концепти) зображають складові системи безпеки, а ребра показують причинно-наслідкові взаємодії між ними. Для цього формується матриця суміжності (W), де (w_{ij}) є вагою зв'язку між концептами (A_i) та (A_j). Процес містить:

1. Визначення концептів: Експерти або алгоритми аналізу логів ідентифікують ключові змінні системи.

2. Встановлення зв’язків: На основі експертних оцінок або кореляційного аналізу логів визначаються причинні впливи. Наприклад, зростання частоти атак (A_i) може посилювати ризик втрати даних (A_j), що позначається як позитивний зв’язок ($w_{ij} > 0$).

3. Формалізація графа: Граф НКК представлено як (G = (A, W)) [3, 4, 8, 14].

Ваги визначаються двома способами:

1. Експертні оцінки: Експерти визначають ваги на основі лінгвістичних оцінок, які переводяться в числові значення через нечіткі множини.

2. Автоматизоване навчання: Нейро-нечіткі методи Hebbian learning, використовуються для оптимізації ваг на основі даних логів. Алгоритм Hebbian learning оновлює ваги за правилом, описаним в [18]:

$$w_{ij}(t+1) = w_{ij}(t) + \eta \cdot A_i(t) \cdot A_j(t), \quad (4)$$

Це дозволяє адаптувати НКК до динамічних змін у системі безпеки.

Для підтримки стабільності, ваги моделі підлягають нормалізації, а функціонування НКК перевіряється на предмет сходження до усталеного стану або циклічного режиму.

Цей алгоритм надає можливість для адаптивного моделювання причинно-наслідкових зв'язків в сфері безпеки інформаційних систем, беручи до уваги як невизначеність, так і динамічний характер загроз [2, 7, 11, 14].

Нейро-нечітке навчання виступає наріжним каменем запропонованої моделі, оскільки воно забезпечує можливість динамічної адаптації ваг нечітких когнітивних карт, надаючи їм більшу стійкість до невизначеностей та змін у середовищі інформаційних систем безпеки. У класичних НКК ваги взаємозв'язків

між концептами встановлюються на основі експертних оцінок, що потенційно призводить до статичності моделі та низької пристосованості до кіберзагроз, що постійно розвиваються. Поєднання нейронних мереж з нечіткою логікою вирішує цю проблему, даючи можливість автоматично корегувати ваги на основі даних, що надходять у реальному часі, отже, збільшуючи точність моделювання причинно-наслідкових зв'язків.

Основна концепція нейро-нечіткого навчання полягає в представленні НКК як нейронної мережі, де концепти НКК відповідають нейронам, а ваги зв'язків – синаптичним вагам. Це надає можливість застосування алгоритмів машинного навчання для оптимізації моделі. У контексті безпеки інформаційних систем цей алгоритм змінює ваги, виходячи з кореляцій між подіями: якщо активація концепту "вразливість" часто передує активації "загроза", вага зв'язку між ними зростає.

Для складніших ситуацій, коли НКК поєднується з багатокомпонентними структурами, використовується метод зворотнього поширення помилки, модифікований для розмитих мереж. Метод зворотнього поширення помилки вираховує відхилення між передбачуваними активностями НКК і фактичними подіями безпеки, а згодом передає цю помилку назад через мережу для корекції ваг.

Даний метод гарантує надзвичайну точність при моделюванні причинно-наслідкових сценаріїв, скажімо, послідовностей атак (від етапу збору даних до моменту реалізації шкідливого коду), а також дає змогу НКК швидко реагувати на нові види загроз, включно з атаками нульового дня.

Висновки з даного дослідження

Внаслідок проведеного аналізу було описано модель причинно-наслідкових подій для використання у сфері інформаційної безпеки на основі нечітких когнітивних карт з нейро-нечітким навчанням. Застосування алгоритмів Hebbian learning для навчання та зворотнього поширення дозволить скоригувати ваги НКК до динамічних даних, які охоплюють як штатні мережеві трафіки, так і різноманітні види атак.

Практична цінність розробленої моделі полягає в її можливостях для впровадження у практичні системи захисту інформаційних ресурсів. Зокрема, модель може бути інтегрована в системи виявлення вторгнень, де вона здатна прогнозувати ймовірність атак на основі раніше виявлених патернів, таких як DDoS, даючи змогу адміністраторам здійснювати профілактичні заходи у режимі реального часу. Крім того, модель придатна для оцінювання ризиків в складних середовищах, наприклад, в телемедичних системах або IoT-мережах, де невизначеність даних є значною. Завдяки можливості адаптації ваг НКК до нових видів загроз, модель гарантує постійне вдосконалення, що робить її корисним інструментом для підвищення стійкості інформаційних систем.

Література

1. Лозовський Р., Мороз А., Вплив штучного інтелекту на стратегії захисту інформаційних систем від нових типів кіберзагроз, *Вісник Хмельницького національного університету,* 2024. Vol. 3(337). P. 366-372. https://doi.org/10.31891/2307-5732-2024-337-55
2. Karatzinis, G. D., Boutalis, Y. S. A review study of fuzzy cognitive maps in engineering: Applications, insights, and future directions. *Engineering,* 2025. Vol. 6. P. 37. https://doi.org/10.3390/eng6020037
3. Mpelogianni, V., Groumpos, P. P., Marnetta P. Fuzzy cognitive maps in the service of energy efficiency. *IFAC-PapersOnLine,* 2015. Vol. 48, P. 1-6. https://doi.org/10.1016/j.ifacol.2015.12.047
4. Papageorgiou, E. I., Salmeron, J. L. Methods and Algorithms for Fuzzy Cognitive Map-based Modeling. *Fuzzy Cognitive Maps for Applied Sciences and Engineering,* 2013 Vol. 54. P. 1-28. https://doi.org/10.1007/978-3-642-39739-4_1
5. Хлібойко М.Я., Васильків Н.М., Хміль В.А., Заблоцький М.М. Нейро-нечіткі методи оцінювання якості та функціональної безпеки інформаційних систем: порівняльний аналіз та огляд сучасного стану досліджень, *Наука і техніка. Сьогодні,* 2025. Vol. 9(50). P. 1562-1573. https://doi.org/10.52058/2786-6025-2025-9(50)-1562-1572
6. Osoba, O., Kosko, B. Causal modeling with feedback fuzzy cognitive maps. In *Social-Behavioral Modeling for Complex Systems* 2019 Vol. 25. P. 1–25. https://doi.org/10.1002/9781119485001.ch25
7. Felix, G., Nápoles, G., Falcon, R., Froelich, W., Vanhoof, K., Bello R. A review on methods and software for fuzzy cognitive maps. *Artificial Intelligence Review,* 2017 Vol. 52, P. 1707–1737. https://doi.org/10.1007/s10462-016-9475-1
8. Groumpos, P. P. Fuzzy cognitive maps: Basic theories and their application to complex systems. *Studies in Fuzziness and Soft Computing,* 2010. Vol. 247 331, P. 1–22. https://doi.org/10.1007/978-3-642-03220-2_1
9. Liu X., Wang Z., Zhang S., Liu J. Novel Approach to Fuzzy Cognitive Map Based on Hesitant Fuzzy Sets for Modeling Risk Impact on Electric Power System. *International Journal of Computational Intelligence Systems*, 2019 Vol. 12(2) P. 842. https://doi.org/10.2991/ijcis.d.190722.001
10. Poleto, T., de Gusmão, A. P. H., da Silva, M. M., & Costa, A. P. C. S. Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services. *Healthcare,* 2021. Vol. 9(11), P. 1504. https://doi.org/10.3390/healthcare9111504
11. Poleto, T., de Oliveira, R. C. P., da Silva, A. L. B., & de Carvalho, V. D. H. Using fuzzy cognitive map approach for assessing cybersecurity for telehealth scenario. *Trends and Innovations in Information Systems and Technologies* 2020. Vol.1160 P. 828–837. https://doi.org/10.1007/978-3-030-45691-7_78

12. Papageorgiou, E. I., & Poczęta, K. A two-stage model for time series prediction based on fuzzy cognitive maps and neural networks. *Neurocomputing,* 2017. Vol. 232, P. 113–121. https://doi.org/10.1016/j.neucom.2016.10.072

13. Makkar A., Ghosh U., Sharma P. K., Javed A. A fuzzy-based approach to enhance cyber defence security for next-generation IoT. *IEEE Internet of Things Journal,* 2021. Vol. 10, P. 2079-2086. https://doi.org/10.1109/JIOT.2021.3053326

14. Jose L. S. A fuzzy grey cognitive maps-based intelligent security system. *IEEE International Conference on Grey Systems and Intelligent Services,* 2015. P. 29-32. https://doi.org/10.1109/GSIS.2015.7301813

15. Mohammadi, S., De Angeli, S., Boni, G., Pirlone, F., & Cattari, S. Fuzzy cognitive mapping to uncover vital urban functions and their interdependencies for disaster recovery. *Journal of Contingencies and Crisis Management*. 2025. Vol 33. P. 1-17. https://doi.org/10.1111/1468-5973.70071

16. Salmeron, J. L., Froelich, W. Dynamic optimization of fuzzy cognitive maps for time series forecasting. *Knowledge-Based Systems,* 2018 Vol. 105, P. 29–37. https://doi.org/10.1016/j.knosys.2016.04.023

17. Schuerkamp, R., & Giabbanelli, P. Extensions of fuzzy cognitive maps: A systematic review. *ACM Computing Surveys,* 2018. Vol. 53. P. 1-36. https://doi.org/10.1145/3610771

18. Froelich, W., & Salmeron, J. L. Evolutionary learning of fuzzy grey cognitive maps for the forecasting of multivariate, interval-valued time series. *International Journal of Approximate Reasoning,* 2014. Vol. 55. P. 1319-1335 https://doi.org/10.1016/j.ijar.2014.02.006

19. Christoforou, A., & Andreou, A. S. A framework for static and dynamic analysis of multi-layer fuzzy cognitive maps. *Neurocomputing,* 2017. Vol. 232. P. 133-145. https://doi.org/10.1016/j.neucom.2016.09.115

20. Rezaee, M. J., Yousefi, S., & Valipour, M. A decision system using fuzzy cognitive map and multi-group data envelopment analysis to estimate hospitals' outputs level. *Neural Computing and Applications,* 2016. Vol. 29. P. 761-777 https://doi.org/10.1007/s00521-016-2478-2

21. Y. Teng, K. Wu, J. Liu. Causal discovery from abundant but noisy fuzzy cognitive map set. *IEEE Transactions on Fuzzy Systems*. 2024. Vol. 32. P.3992-4003 https://doi.org/10.1109/TFUZZ.2024.3386823

References

1. Lozovskyi R., Moroz A., Impact of artificial intelligence on information systems protection strategies against new types of cyber threats. *Herald of Khmelnytskyi National University*. 2024. Vol. 3(337). P. 276-281. https://doi.org/10.31891/2307-5732-2024-337-55

2. Karatzinis, G. D., Boutalis, Y. S. A review study of fuzzy cognitive maps in engineering: Applications, insights, and future directions. *Engineering,* 2025. Vol. 6. P. 37. https://doi.org/10.3390/eng6020037

3. Mpelogianni, V., Groumpos, P. P., Marnetta P. Fuzzy cognitive maps in the service of energy efficiency. *IFAC-PapersOnLine,* 2015. Vol. 48, P. 1-6. https://doi.org/10.1016/j.ifacol.2015.12.047

4. Papageorgiou, E. I., Salmeron, J. L. Methods and Algorithms for Fuzzy Cognitive Map-based Modeling. *Fuzzy Cognitive Maps for Applied Sciences and Engineering,* 2013 Vol. 54. P. 1-28. https://doi.org/10.1007/978-3-642-39739-4_1

5. Khliboiko M. Y., Vasylkiv N. M., Khmil V. A., Zablotskyy M. M. Neuro-fuzzy methods for evaluating the quality and functional safety of information systems: comparative analysis and review of the current state of research. *Science and Technology. Today,* 2025. Vol. 9(50). P. 1562-1573. https://doi.org/10.52058/2786-6025-2025-9(50)-1562-1572

6. Osoba, O., Kosko, B. Causal modeling with feedback fuzzy cognitive maps. In *Social-Behavioral Modeling for Complex Systems* 2019 Vol. 25. P. 1–25. https://doi.org/10.1002/9781119485001.ch25

7. Felix, G., Nápoles, G., Falcon, R., Froelich, W., Vanhoof, K., Bello R. A review on methods and software for fuzzy cognitive maps. *Artificial Intelligence Review,* 2017 Vol. 52, P. 1707–1737. https://doi.org/10.1007/s10462-016-9475-1

8. Groumpos, P. P. Fuzzy cognitive maps: Basic theories and their application to complex systems. *Studies in Fuzziness and Soft Computing,* 2010. Vol. 247 331, P. 1–22. https://doi.org/10.1007/978-3-642-03220-2_1

9. Liu X., Wang Z., Zhang S., Liu J. Novel Approach to Fuzzy Cognitive Map Based on Hesitant Fuzzy Sets for Modeling Risk Impact on Electric Power System. *International Journal of Computational Intelligence Systems*, 2019 Vol. 12(2) P. 842. https://doi.org/10.2991/ijcis.d.190722.001

10. Poleto, T., de Gusmão, A. P. H., da Silva, M. M., & Costa, A. P. C. S. Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services. *Healthcare,* 2021. Vol. 9(11), P. 1504. https://doi.org/10.3390/healthcare9111504

11. Poleto, T., de Oliveira, R. C. P., da Silva, A. L. B., & de Carvalho, V. D. H. Using fuzzy cognitive map approach for assessing cybersecurity for telehealth scenario. *Trends and Innovations in Information Systems and Technologies* 2020. Vol.1160 P. 828–837. https://doi.org/10.1007/978-3-030-45691-7_78

12. Papageorgiou, E. I., & Poczęta, K. A two-stage model for time series prediction based on fuzzy cognitive maps and neural networks. *Neurocomputing,* 2017. Vol. 232, P. 113–121. https://doi.org/10.1016/j.neucom.2016.10.072

13. Makkar A., Ghosh U., Sharma P. K., Javed A. A fuzzy-based approach to enhance cyber defence security for next-generation IoT. *IEEE Internet of Things Journal,* 2021. Vol. 10, P. 2079-2086. https://doi.org/10.1109/JIOT.2021.3053326

14. Jose L. S. A fuzzy grey cognitive maps-based intelligent security system. *IEEE International Conference on Grey Systems and Intelligent Services,* 2015. P. 29-32. https://doi.org/10.1109/GSIS.2015.7301813

15. Mohammadi, S., De Angeli, S., Boni, G., Pirlone, F., & Cattari, S. Fuzzy cognitive mapping to uncover vital urban functions and their interdependencies for disaster recovery. *Journal of Contingencies and Crisis Management*. 2025. Vol 33. P. 1-17. https://doi.org/10.1111/1468-5973.70071

16. Salmeron, J. L., Froelich, W. Dynamic optimization of fuzzy cognitive maps for time series forecasting. *Knowledge-Based Systems,* 2018 Vol. 105, P. 29–37. https://doi.org/10.1016/j.knosys.2016.04.023

17. Schuerkamp, R., & Giabbanelli, P. Extensions of fuzzy cognitive maps: A systematic review. *ACM Computing Surveys,* 2018. Vol. 53. P. 1-36. https://doi.org/10.1145/3610771

18. Froelich, W., & Salmeron, J. L. Evolutionary learning of fuzzy grey cognitive maps for the forecasting of multivariate, interval-valued time series. *International Journal of Approximate Reasoning,* 2014. Vol. 55. P. 1319-1335 https://doi.org/10.1016/j.ijar.2014.02.006

19. Christoforou, A., & Andreou, A. S. A framework for static and dynamic analysis of multi-layer fuzzy cognitive maps. *Neurocomputing,* 2017. Vol. 232. P. 133-145. https://doi.org/10.1016/j.neucom.2016.09.115

20. Rezaee, M. J., Yousefi, S., & Valipour, M. A decision system using fuzzy cognitive map and multi-group data envelopment analysis to estimate hospitals' outputs level. *Neural Computing and Applications,* 2016. Vol. 29. P. 761-777 https://doi.org/10.1007/s00521-016-2478-2

21. Y. Teng, K. Wu, J. Liu. Causal discovery from abundant but noisy fuzzy cognitive map set. *IEEE Transactions on Fuzzy Systems*. 2024. Vol. 32. P.3992-4003 https://doi.org/10.1109/TFUZZ.2024.3386823