УДК 004.056:338 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.52

С. М. ШЕВЧЕНКО
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID: 0000-0002-9736-8623

Ю. Д. ЖДАНОВА
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID: 0000-0002-9277-4972

С. Д. МЕЛЬНИЧУК
студентка факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка
ORCID: 0009-0006-7254-3305

АВТОМАТИЗАЦІЯ КОГНІТИВНОГО МОДЕЛЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ВИКОРИСТАННЯ MENTAL MODELER ТА FCM EXPERT

Фундаментальним елементом будь-якої архітектури безпеки є оцінка ризиків. Вона дозволяє систематизувати потенційні загрози та уразливості, а також спрогнозувати деструктивний вплив на конфіденційність, цілісність і доступність інформації, що є критичним для розробки дієвих заходів захисту. У цій роботі приділено особливу увагу питанню когнітивного моделювання ризиків із застосуванням спеціалізованого програмного інструментарію, зокрема рішень Mental Modeler та FCM Expert, що дозволяють візуалізувати та математично обґрунтувати складні взаємозв'язки в системах захисту.

Проведений у роботі аналіз наукових джерел дозволив систематизувати теоретичні засади та існуючі практичні рішення для оцінки ризиків, зокрема використання SWOT-аналізу, методику експертного оцінювання, апарату теорії ігор, нечіткої логіки, а також сучасних методів машинного навчання та алгоритмів кластеризації. Встановлено, що в умовах високої невизначеності та динамічності кіберпростору нечіткі когнітивні карти (Fuzzy Cognitive Maps – FCM) є одним із найбільш перспективних підходів. Вони надають унікальну можливість поєднувати якісну експертну оцінку з кількісними методами аналізу, дозволяючи моделювати різноманітні сценарії розвитку подій для прийняття обґрунтованих управлінських рішень.

Практична значущість дослідження полягає у демонстрації можливостей автоматизації процесів моделювання за допомогою Mental Modeler та FCM Expert. У роботі детально описано розроблену архітектуру когнітивної моделі умовної організації, яка охоплює ключові вектори загроз, технічні та організаційні уразливості, а також наявні контрзаходи. На базі цієї моделі було реалізовано симуляцію сценарію фішингової атаки. Порівняльний аналіз результатів, отриманих у двох програмних середовищах, дозволив чітко розмежувати їхні функціональні ролі. Встановлено, що Mental Modeler був ефективним для початкового структурування експертних знань та швидкої візуалізації якісних тенденцій та є оптимальним для етапу мозкового штурму. В той самий час FCM Expert досяг глибшої математичної перевірки сценарію шляхом обчислення абсолютних значень стабілізації системи, зменшуючи суб'єктивність експертної оцінки.

Результати проведеного дослідження мають не лише теоретичне, а й освітнє значення. Матеріали та розроблені моделі були успішно апробовані у навчальному процесі під час викладання дисципліни «Теорія ризиків» для здобувачів спеціальності F5 «Кібербезпека та захист інформації». Це підтверджує адаптивність запропонованих методів для підготовки фахівців, здатних оперувати складними аналітичними інструментами в умовах реальних викликів цифровій безпеці.

Ключові слова: *ризики інформаційної безпеки, кіберризики, когнітивне моделювання, нечіткі когнітивні карти (FCM), MENTAL MODELER, FCM EXPERT.*

S. M. SHEVCHENKO
Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor at the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University
ORCID: 0000-0002-9736-8623

YU. D. ZHDANOVA
Candidate of Physical and Mathematical Sciences, Associate Professor,
Associate Professor at the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University
ORCID: 0000-0002-9277-4972

S. D. MELNYCHUK
Student at the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0006-7254-3305

AUTOMATION OF COGNITIVE MODELING OF INFORMATION SECURITY RISKS: EXPERIENCE OF USING MENTAL MODELER AND FCM EXPERT

A fundamental element of any security architecture is risk assessment. It allows you to systematize potential threats and vulnerabilities, as well as predict the destructive impact on the confidentiality, integrity and availability of information assets, which is critical for the development of effective protection measures. This work pays special attention to the issue of cognitive risk modeling using specialized software tools, in particular, Mental Modeler and FCM Expert solutions, which allow you to visualize and mathematically substantiate complex relationships in protection systems.

The analysis of scientific sources conducted in the work allowed to systematize theoretical foundations and existing practical solutions for risk assessment, in particular the use of SWOT analysis, expert assessment methods, game theory apparatus, fuzzy logic, as well as modern machine learning methods and clustering algorithms. It was established that in conditions of high uncertainty and dynamism of cyberspace, fuzzy cognitive maps (Fuzzy Cognitive Maps – FCM) are one of the most promising approaches. They provide a unique opportunity to combine qualitative expert assessment with quantitative analysis methods, allowing to model various scenarios of events for making informed management decisions.

The practical significance of the study lies in demonstrating the possibilities of automating modeling processes using Mental Modeler and FCM Expert. The paper describes in detail the developed architecture of the cognitive model of a conditional organization, which covers key threat vectors, technical and organizational vulnerabilities, as well as existing countermeasures. Based on this model, a simulation of a phishing attack scenario was implemented. A comparative analysis of the results obtained in the two software environments allowed us to clearly distinguish their functional roles. It was found that Mental Modeler was effective for the initial structuring of expert knowledge and rapid visualization of qualitative trends and is optimal for the brainstorming stage. At the same time, FCM Expert achieved a deeper mathematical verification of the scenario by calculating the absolute values of system stabilization, reducing the subjectivity of expert assessment.

The results of the study are not only theoretical, but also educational. The materials and developed models were successfully tested in the educational process during the teaching of the discipline "Risk Theory" for applicants for the specialty F5 "Cybersecurity and Information Protection". This confirms the adaptability of the proposed methods for training specialists capable of operating complex analytical tools in conditions of real challenges to digital security.

Key words: *information security risks, cyber risks, cognitive modeling, fuzzy cognitive maps (FCM), MENTAL MODELER, FCM EXPERT.*

Постановка проблеми

У сучасному суспільстві через стрімке зростання використання мережі Інтернет та активне поширення особистої інформації та інших конфіденційних даних у онлайн-середовищі, інформаційні активи та фінансові транзакції стають дедалі уразливішими для кіберзлочинців. Згідно звіту «Глобальний огляд кібербезпеки 2026» [1] респонденти вважають, що найпоширенішими атаками були: фішинг (включаючи вішинг та смішинг) – 62 %, шахрайство з розрахунками – 37 %, крадіжка особистих даних – 32 %. Занепокоєння викликає вплив штучного інтелекту на кібербезпеку: з одного боку, – це потужний підсилювач спроможностей, з іншого – технологічний допінг для зловмисників. Переважна більшість опитаних (87 %) констатують наявність системних уразливостей у своїх організаціях, зумовлених впровадженням технологій штучного інтелекту [1].

Оцінка ризиків інформаційної безпеки (ІБ) швидко стає необхідністю для забезпечення стійкості та цілісності системи. Попри декларативну важливість кіберзахисту, реальна кіберстійкість впроваджена лише у 2 %

організацій. Крім того, бізнес стикається з труднощами при вимірюванні ризиків: 47 % опитаних сумніваються в достовірності наявних методів оцінки кіберризиків, а ще 39 % стурбовані високим рівнем невизначеності результатів [2]. Саме тому прийняття управлінських рішень у цій сфері суттєво ускладнюється, особливо через динамічний характер загроз, високий рівень невизначеності та складність прогнозувати наслідки експлуатації уразливостей [3].

Аналіз останніх досліджень і публікацій

Оцінка ризиків інформаційної безпеки є вимогою будь-якої системи, оскільки вона закладає основу для побудови ефективної системи захисту, допомагаючи виявити потенційні загрози, уразливості та відповідні наслідки, спричинені порушенням конфіденційності, цілісності та доступності даних. У сучасній практиці зазвичай існує три типи традиційних методологій оцінки ризиків, які мають свої застосування та обмеження. Якісні методи залежать від експертної оцінки та лінгвістичних шкал для встановлення рівнів ризику, і їх зручно застосовувати, але вони є суб'єктивними. Кількісні підходи намагаються зібрати надійні числові результати, наприклад очікувані річні втрати (ALE) або середня частота виникнення інцидентів (ARO), але вони потребують великої кількості даних, які часто не є доступними через конфіденційність інформації про атаки. Гібридні методи беруть найкраще з кожної групи, дозволяючи експертам сформувати свій досвід за допомогою математичних методів в умовах невизначеності та неповних вхідних даних [4].

У дослідженні [5] автори рекомендують технологію для оцінки ризиків ІБ на поєднанні теорії графів та експертного оцінювання.

Роботи [6–8] спрямовують відповідальних за кібербезпеку в організаціях застосовувати SWOT-аналіз та експертне оцінювання для початкового аналізу ризиків інформаційних активів.

Для малого та середнього бізнесу заслуговують на увагу дослідження [9, 10]. Ці організації потребують рішень, які є економічно ефективними, простими в управлінні та відповідають їхнім обмеженим фінансовим та людським ресурсам.

Запропоновано ґрунтовний підхід науковцями [11] до кількісного оцінювання кіберризиків, що базується на використанні нейронних мереж для моніторингу стану системи та автоматизації перевірки на відповідність міжнародним стандартам ІБ.

У наступній статті [12] ініційовано комплексну методологію оцінки ризиків інформаційної безпеки на основі галузевих стандартів, експертного досвіду та інтелектуального аналізу даних. Застосування алгоритмів машинного навчання та методу кластерного аналізу к-середніх дозволило виявити приховані загрози, а розробка тезауруса та теплових карт для візуалізації виводить оцінку ризику на новий рівень точності.

У межах дослідження [13] було синтезовано комбінований метод, що дає змогу оцінювати ризики та прогнозувати динаміку цифрових валют, застосовуючи теорію ігор, апарат нечіткої логіки та обчислювальну потужність нейромережевих моделей.

Оскільки близько 95 % усіх успішних атак виникають через людську помилку, звичайні технічні заходи захисту часто виявляються недостатніми, що вимагає використання формалізованих методів моделювання сценаріїв для дослідження складних взаємозв'язків між заходами безпеки та поведінкою зловмисників [14].

Для аналізу таких систем нечіткі когнітивні карти (FCM) є одним з найперспективніших підходів, які надають спосіб моделювання з набором концепцій (вузлів) та причинно-наслідкових зв'язків між ними (зважені ребра), а також можливість аналізувати сценарії на основі принципу «що, якщо» (What-if) [4]. Саме когнітивне моделювання полягає в організації експертних знань та розумінні впливу факторів на загальний рівень безпеки організації [15-19], використання когнітивної моделі допомагає структурувати знання про систему безпеки та проводити як якісну, так і кількісну оцінку впливу різних факторів на загальну стійкість компанії [20], а метод оцінки інформаційних ризиків на підприємстві за допомогою нечітких когнітивних карт дозволяє скоротити час, необхідний для прийняття рішень щодо вибору необхідних контрзаходів у 1,5–2 рази [21].

Нині існують різні програмні інструменти для реалізації нечіткого когнітивного моделювання включаючи ті, що відрізняються аналітичними можливостями та зручністю інтерфейсу. У цій роботі будуть розглядатись два програмні інструменти: Mental Modeler – розроблений для підтримки групового прийняття рішень та спільної побудови моделей експертами, та FCM Expert – спеціалізована платформа, що використовує алгоритми машинного навчання для оптимізації топології мережі та аналізу сценаріїв. Кожен із цих інструментів має логіку обробки параметрів, що робить актуальним їхнє порівняння в умовах ідентичного сценарію кіберзагрози [22].

Формулювання мети дослідження

Метою роботи є проведення порівняльного аналізу результатів моделювання ризиків інформаційної безпеки за допомогою програмних засобів Mental Modeler та FCM Expert на прикладі сценарію фішингової атаки на віртуальну компанію «CloudGuard Systems».

Для досягнення поставленої мети передбачається розв'язання таких завдань:

1. Розглянути теоретичні засади функціонування нечітких когнітивних карт як інструменту управління ризиками.

2. Описати архітектуру когнітивної моделі уявної компанії «CloudGuard Systems», включаючи засоби захисту (PAM, навчання персоналу), уразливості та загрози.

3. Виконати моделювання сценарію фішингової атаки в програмному середовищі Mental Modeler для оцінювання ризику витоку даних.

4. Провести аналогічну симуляцію в середовищі FCM Expert із використанням його засобів сценарного аналізу.

5. Здійснити порівняльний аналіз отриманих результатів та оцінити зручність і ефективність досліджуваних інструментів для прийняття рішень у сфері кібербезпеки.

Викладення основного матеріалу дослідження

1. Методологія нечіткого когнітивного моделювання ризиків.

У сучасному середовищі кібербезпеки існує потреба в інструментах, які ефективно працюють в умовах високої невизначеності та відсутності статистичних даних. Оскільки багато компаній приховують деталі успішних атак для захисту своєї репутації, аналітики змушені базувати свої аналізи на експертних оцінках та сценаріях випадків. Для цього типу аналізу нечіткі когнітивні карти (FCM), розроблені Бартом Коско як гібрид теорії нечітких множин, нейронних мереж та когнітивного картування, виявилися найпотужнішими інструментами [23]. FCM є представленням системи у вигляді орієнтованого графа, де вузли (концепти) є факторами ризику, а зважені ребра – асоціаціями причинності.

Модель FCM дозволяє перетворювати лінгвістичні оцінки експертів (такі як «сильний вплив», «слабкий вплив») у числові ваги в діапазоні [-1,1], що дає можливість проведення обчислювальних експериментів [20]. Когнітивне моделювання корисне для демонстрації того, як формується структура загроз та для моніторингу швидкості змін з часом: як зміна одного вхідного параметра (наприклад, зрив у навчанні персоналу) вплине на інші в системі та призведе зростання ризику витоку даних. Це робить FCM потужним інструментом для проактивного захисту, де прогнозування наслідків замінює просте реагування на інциденти [15].

Аналіз системи за допомогою когнітивних карт традиційно поділяється на два взаємодоповнюючі напрями, які представлені у таблиці 1.

Таблиця 1

Напрями аналізу систем на основі нечітких когнітивних карт

Тип аналізу	Зміст дослідження	Практична цінність для кібербезпеки
Статичний	Оцінювання топології графа, розрахунок центральності концептів та щільності зв'язків мережі $\left(d = \frac{n}{N^2}\right)$	Виявлення критичних уразливостей (найбільш уразливих вузлів) та аналіз загальної архітектурної стійкості системи захисту
Динамічний	Ітераційне моделювання зміни станів концептів у часі до досягнення системою точки стабілізації	Проведення «What-if» симуляцій для прогнозування розвитку атак (наприклад фішингу) та оцінки ефективності впровадження PAM або сегментації

2. Характеристика програмного забезпечення Mental Modeler

Інструмент Mental Modeler базується на хмарних технологіях і орієнтований на підтримку прийняття рішень через залучення експертів до спільної побудови моделей [24]. Програма дозволяє швидко створювати графічні представлення складних систем та аналізувати їх за допомогою спрощеного інтерфейсу, що не потребує глибоких знань. Однак, Mental Modeler має обмеження щодо автоматизації розрахунків та відсутності вбудованих алгоритмів машинного навчання для корекції ваг зв'язків. Ключові характеристики програмного засобу Mental Modeler подані у таблиці 2.

Таблиця 2

Ключові характеристики програмного засобу Mental Modeler

Критерій	Опис можливостей
Тип інтерфейсу	Веб-орієнтована платформа (Web-based), доступна через браузер, що забезпечує швидкий доступ
Призначення	Структурування експертних знань, підтримка групового прийняття рішень та візуалізація FCM
Сценарний аналіз	Можливість запуску базових симуляцій шляхом ручної зміни початкових станів концептів
Аналітичні функції	Автоматична класифікація компонентів на Driver (засоби захисту), Ordinary (загрози та уразливості) та Receiver (результати)
Обмеження	Відсутність алгоритмів навчання ваг на основі даних; обмежені параметри налаштування функцій активації

3. Характеристика програмного комплексу FCM Expert

На відміну від інструментів, які охоплюють більш спрощені завдання, FCM Expert є просунутою платформою на базі Java, призначеною для глибокого аналізу сценаріїв та класифікації патернів. Основною перевагою цього інструменту є інтеграція алгоритмів машинного навчання (Supervised та Unsupervised Learning), які можуть бути

використані для отримання оптимізації параметрів моделі та збіжності системи. FCM Expert використовується для великих наборів даних у форматі ARFF і застосовується для складних задач прогнозування в межах великих корпоративних організацій, які можуть обробляти великі системні середовища [22]. Ключові характеристики програмного засобу Mental Modeler подані у таблиці 3.

Таблиця 3

Ключові характеристики програмного комплексу FCM Expert

Критерій	Опис можливостей
Архітектура	Об'єктно-орієнтоване десктопне ПЗ на базі Java, що забезпечує кросплатформеність та стабільність обчислень
Машинне навчання	Підтримка еволюційних алгоритмів (PSO, GA, DE) для автоматичного обчислення ваг на основі даних та оптимізації структури мережі
Гнучкість симуляції	Можливість вибору функцій активації (*Sigmoid*, *Hyperbolic Tangent*, *Saturation*) та точне налаштування параметрів збіжності
Візуалізація динаміки	Генерація ітераційних графіків (Convergence Plotter) та аналіз стабільних станів системи (атракторів)
Робота з даними	Повна підтримка форматів CSV та ARFF, що дозволяє інтегрувати реальну статистику інцидентів у когнітивну модель

Отже, використання обраних інструментів дозволяє виконати повний цикл аналізу ризиків: від концептуального проєктування системи безпеки в Mental Modeler до математично точного моделювання сценаріїв атак у FCM Expert.

4. Результати дослідження

1. Опис об'єкта дослідження. У межах проведення порівняльного експериментального дослідження об'єктом аналізу обрано інформаційну систему віртуальної компанії «CloudGuard Systems», яка спеціалізується на наданні хмарних послуг та розробляє інфраструктуру безпеки для корпоративних клієнтів. Така організація обрана через високу цінність їхніх інформаційних активів, включаючи персональні дані користувачів, вихідний код платформи та ключові бази даних. Оскільки інформація є одним з найцінніших активів сучасного підприємства, витік інформації через кібератаки може призвести до незворотних фінансових та репутаційних втрат.

У компанії налічується близько 250 співробітників в організаційній структурі, велика частина з яких має технічні спеціалізації. Однак попередній аналіз виявив ряд системних проблем. Багато співробітників можуть мати надмірний доступ (C4) через відсутність чітких регламентів, що призводить до значного розширення поверхні атаки. Наразі система захисту має мінімальні практики безпеки, а високопріоритетні технології, включаючи систему управління привілейованим доступом (PAM, C1) та глибоку сегментацію мережі (C2), ще не були належним чином впроваджені. Найслабшою ланкою залишається людський фактор. За статистикою, помилки персоналу є причиною до 95 % успішних кібератак, що робить навчання співробітників (C3) критично важливим компонентом безпеки. Для CloudGuard Systems було обрано сценарій агресивної фішингової кампанії (C6) – найбільш розповсюдженого типу загрози, що базується на методах соціальної інженерії для викрадення конфіденційних даних.

Для групування знань про систему та проведення подальшого моделювання було виділено 10 ключових концептів, які на основі методології когнітивного картування розподілені на три функціональні групи: Driver (засоби захисту), Ordinary (уразливості та загрози) та Receiver (результуючі показники). Перелік концептів та їхня характеристика наведені у Таблиці 4.

Обраний сценарій передбачає розвиток подій за принципом «найгіршого випадку»: відсутність навчання (C3 = −1) та недостатнє впровадження PAM (C1 = 0.2) створюють ідеальні умови для успішного фішингу, попри гарно розроблену сегментацію (C2 = 0.7). У поєднанні з надмірними правами доступу (C4 = 0.8), така система дозволяє зловмисникам реалізувати горизонтальне переміщення мережею, що безпосередньо впливає на цільові показники (C8, C9, C10). Таким чином, побудована модель дозволяє аналізувати не лише прямий вплив загроз, а й відсутність засобів захисту.

2. Побудова моделі та моделювання сценарію в Mental Modeler. Наступний етап дослідження передбачав побудову нечіткої когнітивної карти (FCM) для компанії CloudGuard Systems за допомогою середовища Mental Modeler. Цей інструмент є веб-орієнтованою платформою для моделювання, яка дозволяє згрупувати експертні знання у вигляді стандартизованих сценаріїв. Процес моделювання починається з перенесення визначених концептів (C1–C10) у графічне середовище та встановлення причинно-наслідкових зв'язків між ними. Згідно з методологією FCM, кожному зв'язку було присвоєно вагу в діапазоні від −1 до 1, що відображає інтенсивність та характер впливу одного фактора на інший.

Для систематизації взаємозв'язків була сформована когнітивна матриця, де були записані числові значення впливів (рис. 1).

На основі цієї матриці Mental Modeler автоматично створив орієнтований зважений граф, який візуалізує архітектуру ризиків компанії (рис. 2). Вузли представляють концепцти, а ребра представляють динамічні зв'язки.

Таблиця 4

Концептуальна структура когнітивної моделі CloudGuard Systems

Тип концепту	ID	Назва концепту	Характеристика впливу в моделі
Driver	C1	PAM (Privileged Access Management)	Засіб захисту, що мінімізує можливість зловживання привілейованими правами
	C2	Сегментація мережі	Засіб захисту, спрямований на логічне обмеження поширення атаки
	C3	Навчання персоналу (Security Awareness)	Засіб захисту, що знижує ймовірність успіху соціальної інженерії
Ordinary	C4	Надмірні права доступу	Уразливість, що критично полегшує дії зловмисника після проникнення
	C5	Відсутність сегментації	Технічна уразливість, що дозволяє безперешкодно переміщатися всередині периметра
	C6	Фішинг	Активна загроза, яка є початковим вектором більшості кібератак
	C7	Lateral Movement	Загроза, що полягає у поширенні контролю зловмисника всередині мережі компанії
Receiver	C8	Ризик витоку даних	Кінцевий негативний результат реалізації ланцюжка загроз
	C9	Рівень кібербезпеки	Інтегральний показник, що відображає ефективність вжитих заходів захисту
	C10	Операційна стабільність	Показник здатності бізнес-процесів компанії функціонувати в умовах інциденту

	C1 (PAM)	C2 (Сегментація)	C3 (Навчання)	C4 (Надмірні права)	C5 (Відсутність сегментації)	C6 (Фішинг)	C7 (Lateral Movement)	C8 (Ризик витоку)	C9 (Рівень безпеки)	C10 (Стабільність)
C1 (PAM)				-0.4			-0.1		0.4	0.1
C2 (Сегментація)					-0.5		-0.2			0.3
C3 (Навчання)				-0.1		-0.3			0.6	
C4 (Надмірні права)		-0.3					0.4	0.3		
C5 (Відсутність сегментації)	-0.1	-0.2					0.4	0.4		
C6 (Фішинг)				0.5			0.4	0.1		
C7 (Lateral Movement)		-0.3			0.4			0.3		
C8 (Ризик витоку)									-0.5	-0.5
C9 (Рівень безпеки)								-0.5		0.5
C10 (Стабільність)										

Рис. 1. Когнітивна матриця взаємовпливів факторів для CloudGuard Systems у середовищі Mental Modeler

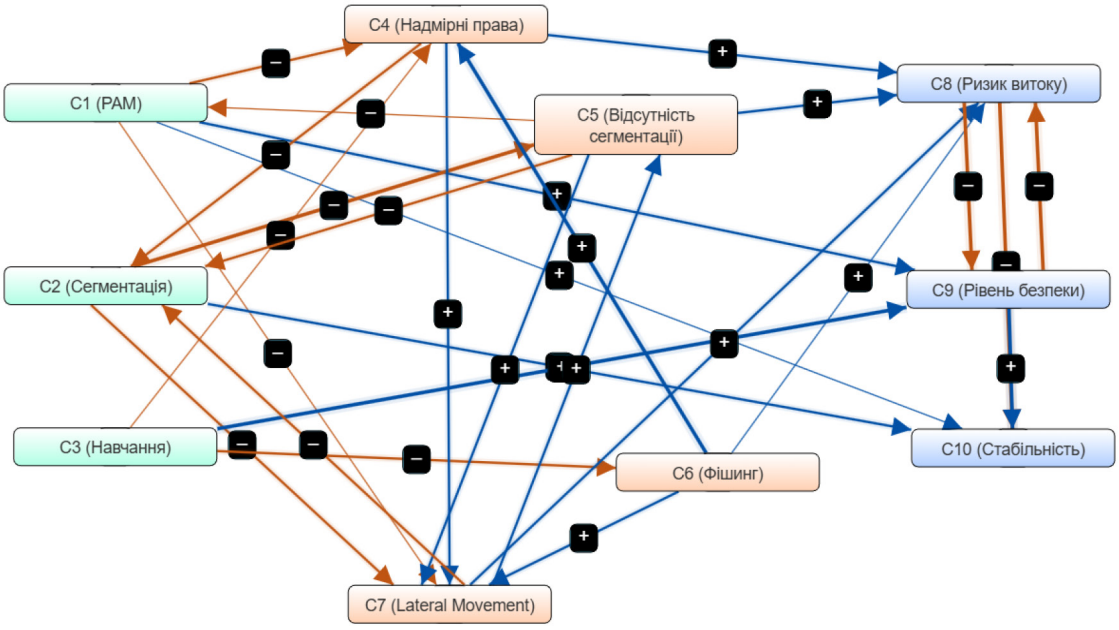

Рис. 2. Графічна візуалізація нечіткої когнітивної карти у Mental Modeler

Вихід цього графа, таким чином, може бути використаний для відображення критичних шляхів поширення атак, зокрема ланцюжок від фішингу через горизонтальне переміщення до кінцевого витоку даних.

Для оцінювання структурної складності побудованої системи було розраховано щільність зв'язків (d) за формулою $d = \frac{n}{N^2}$ $\left(\text{або } d = \frac{n}{N(N-1)}\right)$, де n – кількість зв'язків, а N – кількість концептів. Для нашої моделі з 10 концептами та 27 визначеними зв'язками показник щільності 0.3 свідчить про помірний рівень зв'язності, що вказує на наявність достатніх можливостей для проведення сценарного аналізу.

Після побудови статичної моделі було проведено динамічне моделювання зі сценарієм фішингової атаки. Початкові припущення сценарію були наступним: повна відсутність навчання персоналу (C3 = –1), надмірні права доступу (C4 = 0.8) і часткова реалізація PAM та сегментації для перевірки їх ефективності. Результати моделювання, що на рис. 3, показують, що успіх фішингу (C6) і горизонтального переміщення (C7) значно збільшився, що призвело до критичного зниження на –0.25 інтегрального рівня кібербезпеки (C9) і збільшення ризику витоку даних (C8).

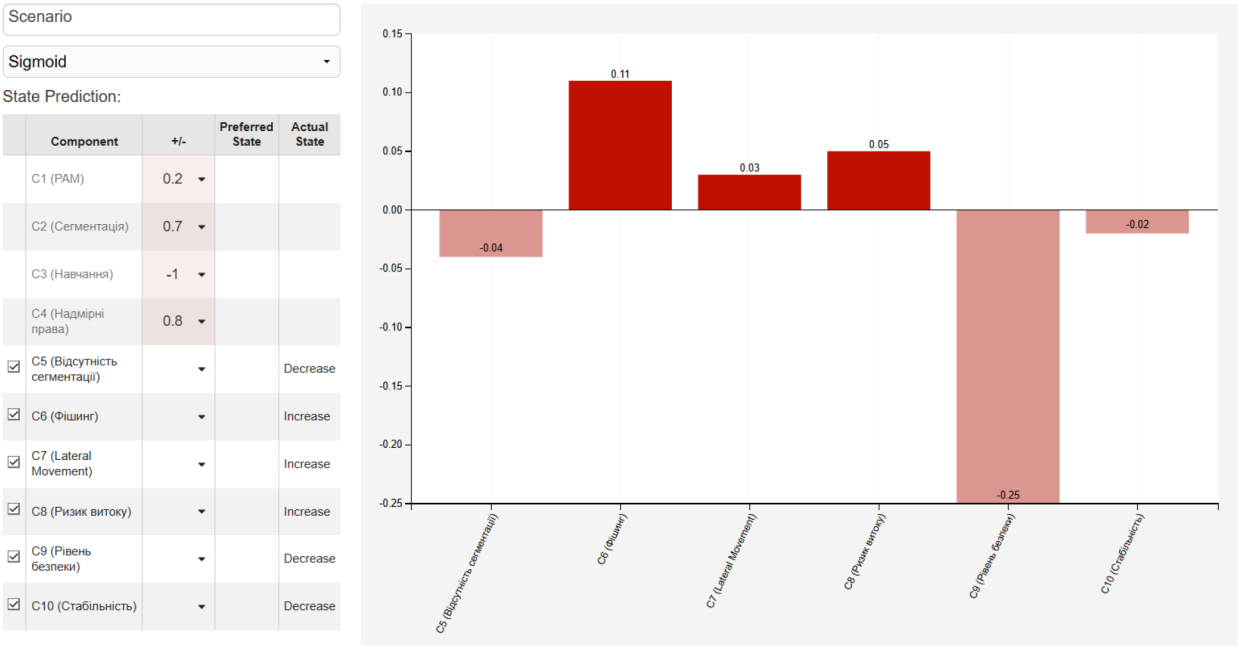

Рис. 3. Результати симуляції сценарію фішингової атаки на CloudGuard Systems у середовищі Mental Modeler

Отримані дані підтверджують, що навіть при мінімальних заходах безпеки, нехтування людським фактором (у нашому випадку навчанням) та привілейованим доступом створює передумови для реалізації критичного ризику. Результати цієї симуляції у Mental Modeler стануть основою для подальшого порівняння з обчисленнями у середовищі FCM Expert.

3. Моделювання сценарію в програмному комплексі FCM Expert. Математична логіка цього інструменту базується на розрахунку абсолютного кінцевого стану системи, що дозволяє виявити стабільні атрактори та приховані патерни в архітектурі безпеки CloudGuard Systems. У FCM Expert повинні порівнювати дельту (зміну) з рівновагою проти базової рівноваги системи під впливом зовнішніх стимулів [22].

Методологія дослідження передбачає три етапи: фіксацію базового стану, налаштування вхідних параметрів сценарію та аналіз фінальних результатів.

Першим кроком було визначено «базовий результат» – стан системи без втручання зловмисників. За умови нейтральної активації всіх концептів (0.5), система автоматично прямує до стабілізації за допомогою обраної сигмоїдної функції активації. Це дає змогу побачити природну стійкість мережі (рис. 4).

Згідно з графіком на рис. 4, за нейтральних умов рівень безпеки та ризиків стабілізується на 6-й ітерації. Кількісні дані базового стану наведені на рис. 5.

З аналізу рис. 5 видно, що у стані спокою показник «Ризик витоку даних» (C8) становить 0.7624, а «Рівень кібербезпеки» (C9) – 0.7313. Ці цифри слугують точкою відліку для оцінювання масштабу руйнівного впливу фішингової атаки.

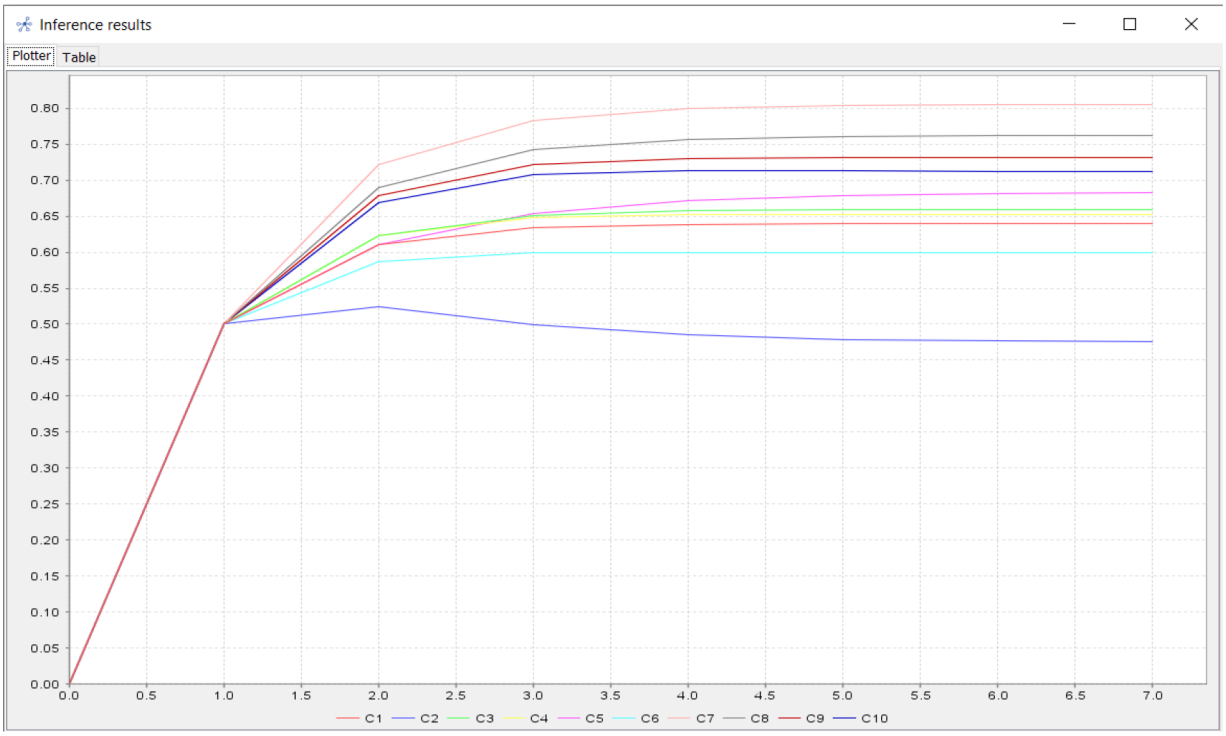

Рис. 4. Графік динаміки збіжності концептів до стабільного стану (Baseline Plotter)

Inference results

Plotter Table

Step	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
2	0.6106	0.525	0.6225	0.6225	0.6106	0.5866	0.7211	0.69	0.6792	0.6682
3	0.634	0.4999	0.6508	0.6478	0.654	0.5987	0.783	0.742	0.7215	0.7071
4	0.6384	0.485	0.6572	0.6521	0.672	0.5995	0.7989	0.7562	0.73	0.713
5	0.6391	0.4788	0.6586	0.6527	0.679	0.5993	0.8034	0.7605	0.7314	0.7129
6	0.639	0.4766	0.659	0.6527	0.6816	0.5991	0.8047	0.7619	0.7314	0.7122
7	0.639	0.4758	0.659	0.6527	0.6825	0.599	0.8052	0.7624	0.7313	0.7117

Рис. 5. Таблиця значень базового стану концептів (Inference Table – Baseline)

На основі обраного сценарію (слабка реалізація PAM, навчання та надмірні права) було виконано ініціалізацію вхідних значень для концептуальних драйверів та уразливостей (рис. 6). Значення 0.2 було присвоєно концепту C1 (PAM), що імітувало існування критично слабкої реалізації системи контролю доступу. Щодо C2 (Сегментація), значення було присвоєно 0.7, що відповідає частковій ізоляції мережі.

Для моделювання активної загрози фішингу ключовими факторами виступили відсутність навчання (C3 = –1) та експлуатація надмірних прав (C4 = 0.8) (рис. 7).

Коли була запущена ітерація, система продемонструвала чітку зміну динаміки. Графік Plotter (рис. 8) чітко показує каскадний ефект: початкові уразливості активують фішингові загрози (C6) та горизонтальне переміщення (C7), що призводить до зниження лінії показників ефективності.

Кількісне підтвердження небезпеки сценарію відображено в фінальній таблиці (рис. 9).

Симуляція FCM Expert показує, що через відсутність навченого персоналу (C3 = –1.0) та обмежений контроль доступу (C1 = 0.2), система безпеки неминуче призводить до компрометації. На 7-й ітерації модель досягла стабільного стану, що вказує на постійний процес розвитку атаки. Таким чином, надмірні привілеї в C4 (які були визначені як 0.8) дозволять зловмисникам переміщатися мережею без перешкод (C7 = 0.8234). Це чітко пояснює, як людська вразливість може стати шлюзом для експлуатації дірок у системі безпеки інфраструктури.

У кількісному аналізі сценарію катастрофічне зниження інтегрального показника «Рівень кібербезпеки» (C9) з 0.7313 до 0.3634 вказує на процес втрати контролю над захистом цього критичного активу. Водночас ризик витоку даних (C8) зріс до критичного рівня – 0.8099, що ще більше підкреслює ризик негативних наслідків без негайної інтеграції систем PAM та програм навчання. FCM Expert використовувався не лише для візуалізації напрямку змін, але й для обчислення математичної оцінки стану системи в «найгіршому сценарії», що буде слугувати основою для подальшого порівняння програмних інструментів.

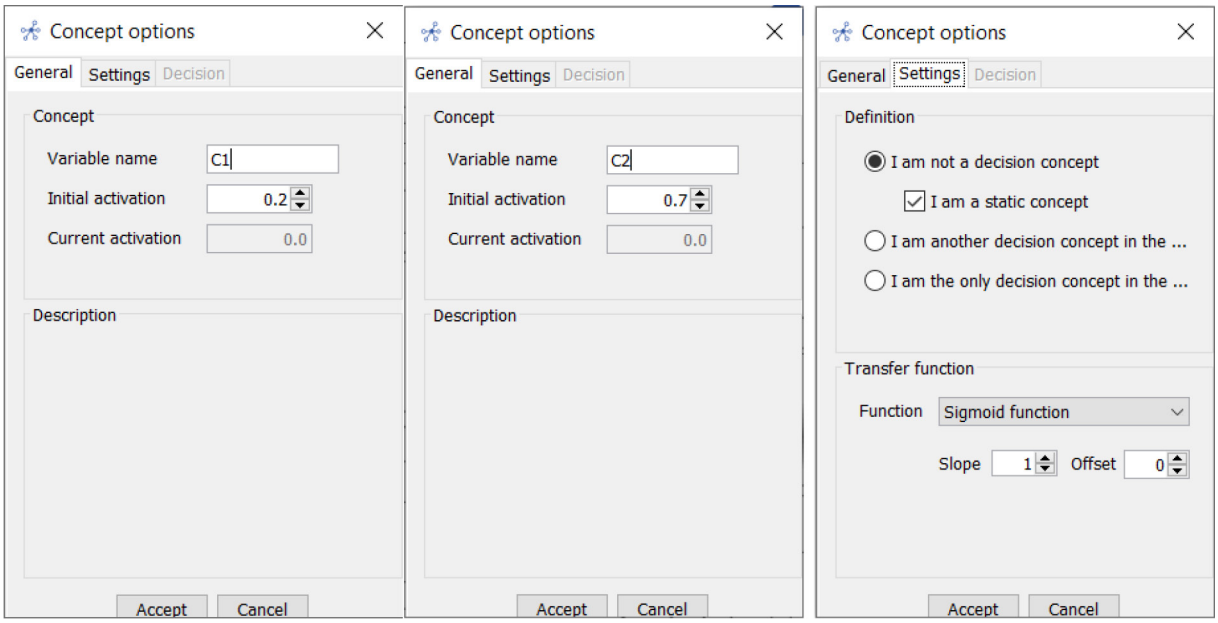

Рис. 6. Налаштування Initial activation для концептів C1 (PAM) та C2 (Сегментація)

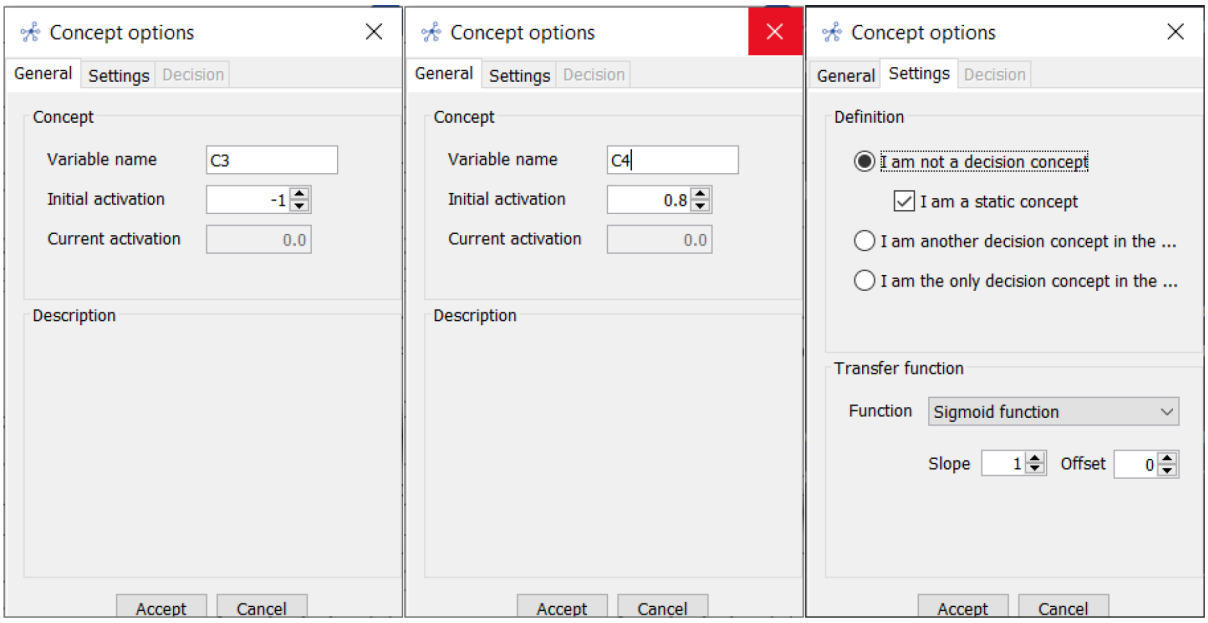

Рис. 7. Введення значень сценарію для чинників навчання (C3) та надмірних прав (C4)

4. Порівняльний аналіз результатів. Остаточний етап дослідження полягає в порівнянні результатів моделювання сценаріїв, отриманих за допомогою Mental Modeler та FCM Expert. Незважаючи на фундаментальні відмінності в алгоритмах (відносні зміни проти абсолютних значень), обидва програмні інструменти продемонстрували високий рівень кореляції в результатах, підкреслюючи критичну уразливість компанії «CloudGuard Systems» за обраним сценарієм.

Узагальнена порівняльна характеристика кількісних показників впливу атаки на цільові концепти наведена в Таблиці 5.

Аналіз даних показує, що обидва інструменти ідентифікували людський фактор (C3 = –1) та відсутність PAM (C_1) як ключові каталізатори успішної атаки. У Mental Modeler ми спостерігаємо візуалізацію, де падіння рівня безпеки (–0.25) є найсильнішим сигналом. У свою чергу, FCM Expert математично обґрунтовує це зниження, показуючи, що система не лише «погіршується», але й стабілізується на критичній точці (атракторі) з рівнем безпеки лише 0.36, що є неприйнятним для IT-компанії.

Окрім кількісних даних, було проведено оцінювання функціональних можливостей програмних засобів, що важливо для вибору інструментарію залежно від завдань аналітика (таблиця 6).

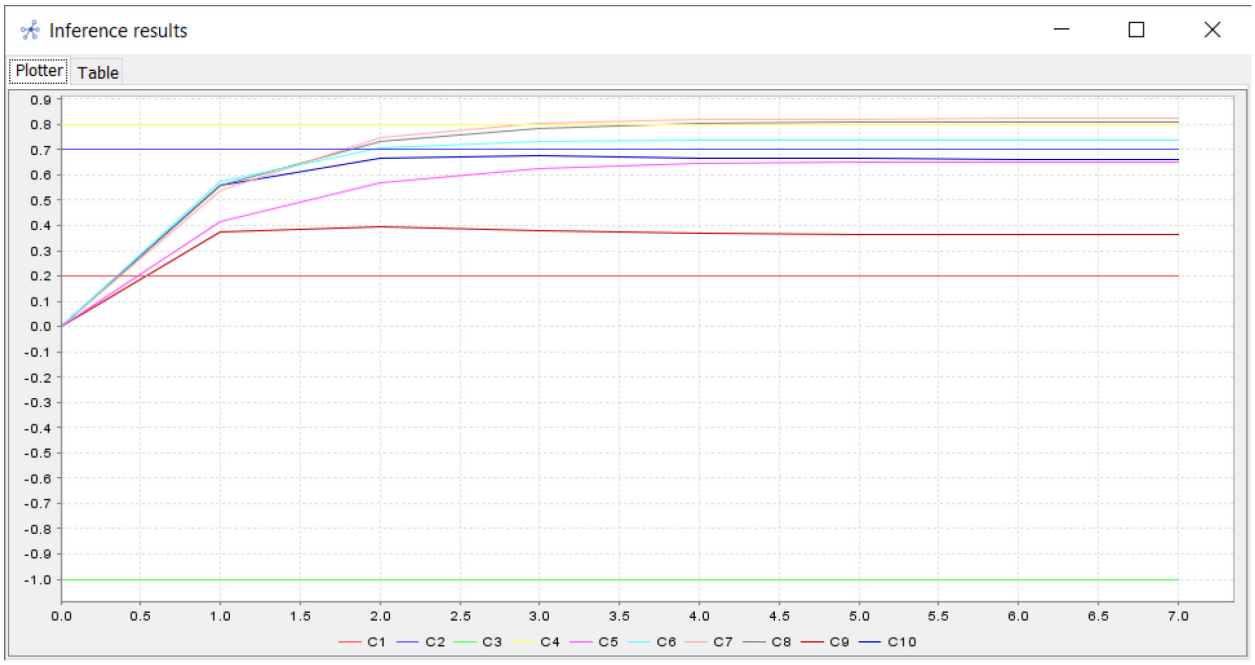

Рис. 8. Графік динаміки станів після симуляції сценарію (Scenario Plotter)

Inference results

Plotter | Table

Step	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
0	0.2	0.7	-1.0	0.8	0.0	0.0	0.0	0.0	0.0	0.0
1	0.2	0.7	-1.0	0.8	0.4134	0.5744	0.5399	0.5597	0.3729	0.5572
2	0.2	0.7	-1.0	0.8	0.5694	0.7057	0.7493	0.7307	0.3948	0.6668
3	0.2	0.7	-1.0	0.8	0.6269	0.7322	0.8052	0.7852	0.3798	0.6746
4	0.2	0.7	-1.0	0.8	0.6454	0.7373	0.8189	0.8023	0.3699	0.6686
5	0.2	0.7	-1.0	0.8	0.6509	0.7383	0.8223	0.8077	0.3656	0.6643
6	0.2	0.7	-1.0	0.8	0.6524	0.7385	0.8232	0.8093	0.3639	0.6622
7	0.2	0.7	-1.0	0.8	0.6529	0.7386	0.8234	0.8099	0.3634	0.6614

Рис. 9. Фінальні значення моделювання сценарію для CloudGuard Systems

Таблиця 5

Порівняльний аналіз результатів моделювання в Mental Modeler та FCM

Цільовий концепт	Mental Modeler (Відносна зміна)	FCM Expert (Базовий стан → Сценарій)	FCM Expert (Розрахована дельта)
C8: Ризик витоку даних	+0.05 (Зростання)	0.7624 → 0.8099	+0.0475
C9: Рівень кібербезпеки	–0.25 (Падіння)	0.7313 → 0.3634	–0.3679
C10: Стабільність	–0.02 (Зниження)	0.7117 → 0.6614	–0.0503

Таблиця 6

Порівняння функціональних особливостей Mental Modeler та FCM

Критерій	Mental Modeler	FCM Expert
Математична логіка	Фокус на дельтах (відносних змінах від початкового стану)	Фокус на абсолютних станах активації та точках стабілізації (атракторах)
Зручність інтерфейсу	Веб-орієнтований (SaaS), інтуїтивно зрозумілий, не потребує встановлення	Десктопний (Java), потребує навичок аналізу даних та налаштування параметрів
Аналіз динаміки	Спрощена візуалізація змін («What-if») у вигляді гістограм впливу	Поглиблений аналіз ітераційних кроків із візуалізацією кривих збіжності
Навчання моделі	Відсутнє (модель базується виключно на суб'єктивних оцінках експерта)	Наявні алгоритми Machine Learning (PSO, GA, DE) для корекції ваг на основі даних
Цільова аудиторія	Стейкхолдери, менеджери, фахівці нетехнічного профілю	Дослідники, аналітики кіберризиків, інженери з математичного моделювання

Як показують результати, Mental Modeler доцільно використовувати на етапі мозкового штурму та початкового структурування загроз швидкої візуалізації наслідків рішень. Однак для прийняття фінансово відповідальних рішень, таких як розрахунок точного рівня ризику або оптимізація топології захисту, FCM Expert є значно

ефективнішим завдяки можливості використовувати алгоритми машинного навчання та оцінювати збіжність системи.

Таким чином, інструменти не замінюють, а доповнюють один одного: кількісний результат у FCM Expert математично підтверджує якісні тенденції, виявлені в Mental Modeler.

Висновки

У ході виконання роботи було проведено комплексне дослідження методів оцінки ризиків інформаційної безпеки за допомогою нечіткого когнітивного моделювання на прикладі умовної компанії «CloudGuard Systems». Використання сценарію фішингової атаки дозволило наочно продемонструвати можливості програмного забезпечення для прогнозування наслідків експлуатації уразливостей в умовах високої невизначеності.

Головним результатом дослідження стало підтвердження гіпотези про те, що поєднання людського фактора (такого як відсутність навчання персоналу, C3) та архітектурних недоліків (надмірні права доступу, C4) призводить до катастрофічного зростання ризику витоку даних (C8). Моделювання показало, що навіть за наявності базової сегментації мережі, ігнорування впровадження системи PAM (C1) робить інфраструктуру прозорою для горизонтального переміщення зловмисників (C7), що підтверджується падінням інтегрального показника рівня кібербезпеки (C9) більш ніж удвічі.

Порівняння серед інструментів моделювання показало їх ключові особливості. Mental Modeler був ефективним для початкового структурування експертних знань та швидкої візуалізації якісних тенденцій та є оптимальним для етапу мозкового штурму. В той час як FCM Expert досяг глибшої математичної перевірки сценарію шляхом обчислення абсолютних значень стабілізації системи. Використовуючи певні алгоритми машинного навчання, цей інструмент зменшує суб'єктивність експертної оцінки та призводить до більш точних кількісних прогнозів, що є важливим для інвестиційних рішень, пов'язаних із захисними заходами.

Отримані дані свідчать, що інструменти не є взаємовиключними, а доповнюють один одного на різних стадіях управління ризиками.

Результати дослідження було апробовано у процесі навчання дисципліни Теорія ризиків студентів спеціальності F5 Кібербезпека та захист інформації Київського столичного університету імені Бориса Грінченка.

Перспективи подальших досліджень полягають у розробці гібридних методик, здатних інтегрувати нечіткі когнітивні карти з системами моніторингу подій безпеки (SIEM) у режимі реального часу, а також переходу від статичного аналізу сценаріїв до безперервного адаптивного управління ризиками, яке автоматично оновлює ваги зв'язків між загрозами та активами на основі реальних даних про інциденти. Також перспективним є дослідження впливу автоматизованого навчання топології мереж на точність прогнозування складних багатокрокових атак у хмарних середовищах.

Список використаної літератури

1. World Economic Forum. (2026). *Global cybersecurity outlook 2026: Insight report*. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

2. UK Government. (2025). *Cyber security breaches survey 2025*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-20254

3. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information security risk management using cognitive modeling. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3550, pp. 297–305). https://ceur-ws.org/Vol-3550/short15.pdf

4. Felix, G., Napoles Ruiz, G., Falcon, R., Froelich, W., Vanhoof, K., & Bello, R. (2017). A review on methods and software for fuzzy cognitive maps. *Artificial Intelligence Review, 52*(3), 1707–1737. https://doi.org/10.1007/s10462-017-9575-1

5. Карпович, І., Гладка, О., & Бухало, Ю. (2021). Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології, 1*(23), 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68

6. Шевченко, С. М., Жданова, Ю. Д., Спасітєлєва, С. О., & Складанний, П. М. (2020). Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека. *Кібербезпека: освіта, наука, техніка, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168

7. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Nehodenko, O. (2021). Information security risk analysis SWOT. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 309–317). http://ceur-ws.org/Vol-2923/paper34.pdf

8. Дзюба, Л., & Чмир, О. (2022). Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. *Вісник Львівського державного університету безпеки життєдіяльності, 26*, 47–54. https://doi.org/10.32447/20784643.26.2022.06

9. Шевченко, С. М., Жданова, Ю. Д., & Кравчук, К. В. (2021). Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу. *Кібербезпека: освіта, наука, техніка, 2*(14), 158–175. https://doi.org/10.28925/2663-4023.2021.14.158175

10. Шевченко, С., Жданова, Ю., & Кія, О. (2025). Напівавтоматизований інструмент багатостандартної оцінки кіберзрілості організації на основі NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8. *Кібербезпека: освіта, наука, техніка, 3*(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004

11. Палко, Д., & Мирутенко, Л. (2024). Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка, 2*(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731

12. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a flexible information security risk model using machine learning methods and ontologies. *Applied Sciences, 14*(21), 9858. https://doi.org/10.3390/app14219858

13. Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., & Zhumadilova, M. (2022). Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency. *Journal of Theoretical and Applied Information Technology, 100*(24), 7390–7404.

14. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

15. Stylios, C. D., & Groumpos, P. P. (2004). Modeling complex systems using fuzzy cognitive maps. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 34*(1), 155–162.

16. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 356–362). https://ceur-ws.org/Vol-3826/short28.pdf

17. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. *Кібербезпека: освіта, наука, техніка, 26*(2), 419–429. https://doi.org/10.28925/2663-4023.2024.26.707

18. Шевченко, С. М., Жданова, Ю. Д., & Гаркушенко, А. М. (2025). Когнітивне моделювання сценаріїв для прогнозування кіберризиків. In *Technical, agricultural and mathematical sciences: scientific trends, problems and ways of their development: collective monograph*. Boston: Primedia eLaunch. (Pp. 178–196) https://isg-konf.com/uk/information-technologies-engineering-transport-and-construction-the-latest-technologies-in-the-development-of-sciences/

19. Soner, O. (2025). Modeling and analyzing cybersecurity risk propagation in ports using fuzzy cognitive maps: System sensitivity to key threat factors. *Ocean & Coastal Management, 270*, 107857. https://doi.org/10.1016/j.ocecoaman.2025.107857

20. Papageorgiou, E. I., & Salmeron, J. L. (2012). A review of fuzzy cognitive maps research during the last decade. *IEEE Transactions on Fuzzy Systems, 21*(1), 66–79.

21. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024* (Vol. 3925, pp. 249–264).

22. Nápoles, G., et al. (2018). FCM expert: Software tool for scenario analysis and pattern classification based on fuzzy cognitive maps. *International Journal on Artificial Intelligence Tools, 27*(7), 1860010.

23. Gray, S. A., et al. (2015). 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).

References

1. World Economic Forum. (2026). *Global cybersecurity outlook 2026: Insight report*. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

2. UK Government. (2025). *Cyber security breaches survey 2025*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-20254

3. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information security risk management using cognitive modeling. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3550, pp. 297–305). https://ceur-ws.org/Vol-3550/short15.pdf

4. Felix, G., Napoles Ruiz, G., Falcon, R., Froelich, W., Vanhoof, K., & Bello, R. (2017). A review on methods and software for fuzzy cognitive maps. *Artificial Intelligence Review, 52*(3), 1707–1737. https://doi.org/10.1007/s10462-017-9575-1

5. Karpovych, I., Hladka, O., & Bukhala, Yu. (2021). Tekhnolohii modeliuvannia i otsinky ryzykiv informatsiinoi bezpeky [Technologies for modeling and assessing information security risks]. *Tekhnichni nauky ta tekhnolohii, 1*(23), 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68

6. Shevchenko, S. M., Zhdanova, Yu. D., Spasitielieva, S. O., & Skladannyi, P. M. (2020). Provedennia SWOT-analizu otsiniuvannia informatsiinykh ryzykiv yak zasib formuvannia praktychnykh navychok studentiv spetsialnosti 125 Kiberbezpeka [Conducting SWOT analysis of information risk assessment as a tool for forming practical skills of cybersecurity students]. *Kiberbezpeka: osvita, nauka, tekhnika, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168

7. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Nehodenko, O. (2021). Information security risk analysis SWOT. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 309–317). http://ceur-ws.org/Vol-2923/paper34.pdf

8. Dziuba, L., & Chmyr, O. (2022). Otsiniuvannia ryzykiv informatsiinoi bezpeky z vykorystanniam metodiv matematychnoi statystyky [Assessment of information security risks using methods of mathematical statistics]. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, 26*, 47–54. https://doi.org/10.32447/20784643.26.2022.06

9. Shevchenko, S. M., Zhdanova, Yu. D., & Kravchuk, K. V. (2021). Model zakhystu informatsii na osnovi otsinky ryzykiv informatsiinoi bezpeky dlia maloho ta serednoho biznesu [Information protection model based on information security risk assessment for small and medium-sized business]. *Kiberbezpeka: osvita, nauka, tekhnika, 2*(14), 158–175. https://doi.org/10.28925/2663-4023.2021.14.158175

10. Shevchenko, S., Zhdanova, Yu., & Kiia, O. (2025). Napiavtomatyzovanyi instrument bahatostandartnoi otsinky kiberzrilosti orhanizatsii na osnovi NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 ta CIS Controls v8 [Semi-automated multi-standard cyber maturity assessment tool based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 and CIS Controls v8]. *Kiberbezpeka: osvita, nauka, tekhnika, 3*(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004

11. Palko, D., & Myrutenko, L. (2024). Metod kompleksnoi otsinky ryzykiv kiberbezpeky v rozpodilenykh informatsiinykh systemakh [Method of comprehensive assessment of cybersecurity risks in distributed information systems]. *Kiberbezpeka: osvita, nauka, tekhnika, 2*(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731

12. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a flexible information security risk model using machine learning methods and ontologies. *Applied Sciences, 14*(21), 9858. https://doi.org/10.3390/app14219858

13. Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., & Zhumadilova, M. (2022). Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency. *Journal of Theoretical and Applied Information Technology, 100*(24), 7390–7404.

14. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

15. Stylios, C. D., & Groumpos, P. P. (2004). Modeling complex systems using fuzzy cognitive maps. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 34*(1), 155–162.

16. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 356–362). https://ceur-ws.org/Vol-3826/short28.pdf

17. Shevchenko, S. M., Zhdanova, Yu. D., Skladannyi, P. M., & Petrenko, T. (2024). Nechitki kohnityvni karty yak instrument vizualizatsii stsenariiv reahuvannia na intsydenty v systemakh bezpeky [Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems]. *Kiberbezpeka: osvita, nauka, tekhnika, 26*(2), 419–429. https://doi.org/10.28925/2663-4023.2024.26.707

18. Shevchenko, S. M., Zhdanova, Yu. D., & Harkushenko, A. M. (2025). Kohnityvne modeliuvannia stsenariiv dlia prohnozuvannia kiberryzykiv [Cognitive modeling of scenarios for predicting cyber risks]. In *Technical, agricultural and mathematical sciences: scientific trends, problems and ways of their development: collective monograph*. Boston: Primedia eLaunch. (Pp. 178–196) https://isg-konf.com/uk/information-technologies-engineering-transport-and-construction-the-latest-technologies-in-the-development-of-sciences/

19. Soner, O. (2025). Modeling and analyzing cybersecurity risk propagation in ports using fuzzy cognitive maps: System sensitivity to key threat factors. *Ocean & Coastal Management, 270*, 107857. https://doi.org/10.1016/j.ocecoaman.2025.107857

20. Papageorgiou, E. I., & Salmeron, J. L. (2012). A review of fuzzy cognitive maps research during the last decade. *IEEE Transactions on Fuzzy Systems, 21*(1), 66–79.

21. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024* (Vol. 3925, pp. 249–264).

22. Nápoles, G., et al. (2018). FCM expert: Software tool for scenario analysis and pattern classification based on fuzzy cognitive maps. *International Journal on Artificial Intelligence Tools, 27*(7), 1860010.

23. Gray, S. A., et al. (2015). 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).

Дата першого надходження статті до видання: 12.01.2026
Дата прийняття статті до друку після рецензування: 16.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026