

DOI: [10.18372/2225-5036.32.21639](https://doi.org/10.18372/2225-5036.32.21639)

ВИКОРИСТАННЯ НЕЧІТКИХ КОГНІТИВНИХ КАРТ ДЛЯ СЦЕНАРНОГО МОДЕЛЮВАННЯ ВПЛИВУ ЗАГРОЗ НА ІНФОРМАЦІЮ У БІЗНЕС-ПРОЦЕСІ

Вадим Тютюник, Ольга Тютюник

Харківський національний економічний університет імені Семена Кузнеця, Україна
Харківський національний університет радіоелектроніки, України



ТЮТЮНИК Вадим Володимирович, д.т.н., професор.

Освіта: Харківський військовий університет, 1995 рік.

Посада: професор кафедри кібербезпеки та інформаційних технологій; професор кафедри безпеки інформаційних технологій.

Наукові інтереси: національна безпека, моніторинг та антикризове управління, інформаційна безпека, автоматизовані системи безпеки.

Публікації: більше 300 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи, матеріали та тези доповідей на конференціях.

E-mail: tutunik_v@ukr.net

Orcid ID: 0000-0001-5394-6367



ТЮТЮНИК Ольга Олександрівна, к.т.н., доцент.

Освіта: Харківський національний економічний університет імені Семена Кузнеця, 2005 рік.

Посада: доцент кафедри інформатики та комп'ютерної техніки.

Наукові інтереси: системи управління безпекою, проблеми прийняття антикризових рішень.

Публікації: більше 150 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.

E-mail: olha.tiutiunyk@hneu.net

Orcid ID: 0000-0002-3330-8920

Анотація. У статті розглянуто підхід до аналізу впливу загроз і організаційно-технічних факторів на стан інформації в бізнес-процесах із використанням методу нечітких когнітивних карт (НKK). Запропоновано множину ключових концептів, що відображають зовнішні та внутрішні загрози, уразливості інформаційних систем, механізми захисту, а також наслідки порушення конфіденційності, цілісності та доступності інформації. Побудовано формалізовану матрицю впливів та граф причинно-наслідкових зв'язків між факторами, що дозволяє дослідити системні взаємозалежності в межах гіпотетичного бізнес-процесу. На основі результатів когнітивного моделювання застосовано метод сценарного аналізу для прогнозування можливих варіантів розвитку ситуації та оцінювання рівня збитків для бізнес-процесу. Отримані результати можуть бути використані як інструменти підтримки прийняття управлінських рішень у сфері забезпечення інформаційної безпеки (ІБ) з урахуванням специфіки діяльності підприємств.

Ключові слова: інформаційна безпека, бізнес-процес, нечіткі когнітивні карти, когнітивна модель, загрози інформації, уразливості, сценарний аналіз, CIA, SIEM, IDS/IPS, SOC.

Вступ. У сучасних умовах цифрової трансформації бізнес-процеси організацій стають дедалі більш складними, динамічними та взаємозалежними [1, 2]. Зростає обсяг інформаційних потоків, використання хмарних сервісів, мобільних платформ, відкритих API та гібридних інфраструктур. Це зумовлює підвищення інтенсивності, різноманітності та непередбачуваності загроз ІБ, що впливають на функціонування бізнес-процесів та якість прийняття управлінських рішень [3, 4]. Традиційні методи оцінювання ризиків і моделювання загроз часто виявляються недостатньо ефективними у ситуаціях, де характер взаємозв'язків між факторами є нечітким, нелінійним або слабо формалізованим [5–8].

Одним із перспективних підходів до аналізу складних систем з високим рівнем невизначеності є використання НKK, які дозволяють формалізувати причинно-наслідкові зв'язки між елементами системи у вигляді орієнтованого графа з ваговими зв'язками, представленими лінгвістичними змінними. Це забезпечує можливість моделювання

процесів у ситуаціях, де точні кількісні залежності відсутні або їх важко оцінити. Завдяки здатності відображати нечіткість, неповноту та експертні оцінки, НKK широко застосовуються у задачах прогнозування, підтримки прийняття рішень, аналізу ризиків та визначення впливових факторів у складних системах [9].

У контексті ІБ бізнес-процесів НKK відкривають можливості для сценарного моделювання впливу різних класів загроз на ключові властивості інформації – конфіденційність, цілісність та доступність. Моделювання дозволяє визначити найбільш критичні загрози, оцінити їхній сукупний вплив, а також проаналізувати поведінку системи у різних сценаріях – від окремих інцидентів до комбінованих атак. Це підвищує ефективність управління ризиками та створює підґрунтя для формування адаптивних стратегій захисту [10].

Метою даної статті є побудова НKK бізнес-процесу з урахуванням можливих загроз ІБ та проведення сценарного моделювання їх впливу на інформацію, що обробляється в межах процесу.

Дослідження спрямоване на визначення найбільш суттєвих загроз та оцінку їхнього впливу на інформаційні активи, що забезпечує підвищення ефективності управління ІБ.

Аналіз існуючих досліджень. Нечіткі когнітивні карти мають довгу історію розвитку від класичної концепції когнітивних карт до формалізації підходу з нечіткими ваговими зв'язками і ітераційним розповсюдженням впливу між концептами. Ця базова парадигма стала основою для широкого спектра подальших робіт з моделювання складних систем, де якісні експертні оцінки та невизначеність відіграють ключову роль [11].

За останнє десятиліття з'явилося кілька оглядових праць і систематичних оцінок, які підсумовують еволюцію методів НКК – розширення архітектури (інтеграція з імовірнісними та інтуїтивними нечіткими теоріями, методами навчання вагових матриць, гібридними підходами з машинним навчанням), а також класифікацію задач, у яких НКК застосовують для прогнозування, аналізу ризиків та підтримки рішень. Ці огляди фіксують інтенсифікацію дослідницької активності й появи формальних процедур валідації та навчання НКК [12, 13].

Серед прикладних напрямів помітно зростання застосувань НКК в аналізі ризиків та ІБ. У кількох останніх роботах було продемонстровано ефективність підходу для сценарного моделювання інцидентів (what-if аналіз), візуалізації ланцюгів впливу та ідентифікації критичних факторів у системах безпеки. Зокрема, серія праць останніх років розглядають використання НКК для моделювання сценаріїв кіберінцидентів, для оцінки ризиків у телемедичному середовищі та для системного аналізу поширення ризиків у критичних інфраструктурах. Ці дослідження показують, що НКК добре підходять для експертно-орієнтованих задач, де даних недостатньо для чисто статистичних підходів [14].

Водночас останні праці також вказують на низку методологічних питань і прогалин. По-перше, є потреба у стандартизованих підходах до отримання та валідації ваг (опитування експертів, агрегування оцінок, застосування алгоритмів навчання) та в дослідженнях щодо чутливості результатів моделювання до різних процедур квантифікації нечіткості. По-друге, хоча існують приклади застосування НКК до окремих IT-сценаріїв, відносно менше робіт присвячено детальному моделюванню впливу загроз саме на інформацію в межах структурованих бізнес-процесів – тобто на поділені ролі, точки обробки й передачі інформації, а також на виміри CIA (конфіденційність, цілісність, доступність) у контексті процесу. Це створює дослідницьке вікно для нашої роботи, а саме розробити процедурно підкріплену НКК, орієнтовану на бізнес-процесні артефакти та сценарний аналіз загроз [15].

Крім того, останні огляди і приклади впровадження демонструють такі тренди, які важливо врахувати: 1) комбінування НКК із методами машинного навчання для автоматичного уточнення ваг; 2) використання лінгвістичних змінних і розширених нечітких теорій для вираження експертної невизначеності; 3) інтеграція

НКК у сценарну аналітику та інструменти підтримки прийняття рішень. Ці напрямки слугують методологічною опорою для запропонованого підходу й визначають можливі шляхи подальшого розвитку моделі (наприклад, гібридне навчання ваг та валідація на реальних кейсах бізнес-процесів) [16].

Таким чином, результати проведеного літературного аналізу підтверджують доречність застосування НКК для сценарного моделювання загроз у сфері ІБ, але одночасно виявляє нестачу цільових досліджень, що прямо поєднують НКК з формалізованим описом бізнес-процесів та кількісною оцінкою впливу на властивості інформації (Confidentiality, Integrity, Availability; CIA). Це обґрунтовує наукову новизну та практичну значимість нашого дослідження.

Основна частина дослідження. Нечіткі когнітивні карти є розвитком класичних когнітивних карт, які розроблені для відображення причинно-наслідкових зв'язків у складних соціально-економічних системах. Подальший розвиток концепції базується на інтегруванні у модель апарат нечіткої логіки та дав математичне формулювання взаємодії між концептами. НКК ґрунтуються на уявленні системи у вигляді орієнтованого графа, де вузли відповідають концептам (факторам), а дуги – причинно-наслідковим зв'язкам, що мають напрямок та вагу. У НКК ваги зв'язків задаються не точними числовими значеннями, а нечіткими оцінками, що описують рівень впливу за допомогою лінгвістичних змінних («слабкий», «помірний», «сильний», «критичний»). Це дозволяє моделювати системи, у яких характер взаємодій є нечітким, динамічним або недостатньо формалізованим. Нечіткі ваги відображають експертні судження та забезпечують гнучкість у представленні невизначеності.

Формально НКК описується матрицею вагових коефіцієнтів $W = \{w_{ij}\}$, де w_{ij} – величина та напрямок впливу концепту C_j на C_i . Значення ваг можуть бути додатними (підсилюючий вплив), від'ємними (послаблюючий вплив) або нульовими (відсутність зв'язку). Динаміка системи визначається шляхом ітераційного оновлення вектора станів $A(t)$, який відображає поточні значення концептів. Типовий процес моделювання базується на рекурентному співвідношенні $A(t+1) = f(A(t)W)$, де $f()$ – функція активації (порогова, сигмоїдна, лінійна), що нормалізує значення концептів у заданому діапазоні. Особливістю НКК є здатність моделювати ланцюгові впливи, зворотні зв'язки, каскадні ефекти та поведінку системи в умовах неповних даних. Це робить НКК ефективним інструментом для аналізу складних систем, де традиційні статистичні підходи не забезпечують достатньої точності або вимагають обсягів даних, які недоступні. Так, у сфері ІБ НКК дозволяють формалізувати взаємозв'язки між загрозами, уразливостями, характеристиками

інформації та елементами бізнес-процесів. Моделювання на основі НКК забезпечує можливість аналізу сценаріїв загроз, їх сукупного впливу, оцінювання стійких режимів системи та виявлення концептів, що мають найбільший вплив на властивості інформації.

Бізнес-процес є цілісною послідовністю операцій, взаємодій та інформаційних потоків, спрямованих на досягнення певного результату або створення цінності для споживача. У контексті ІБ особливу важливість становить аналіз того, яка інформація формується, зберігається, передається та обробляється на кожному етапі процесу, а також які суб'єкти, ресурси та технічні засоби залучені до цих операцій. Це дозволяє ідентифікувати потенційні точки впливу загроз та визначити вразливі ланки, що мають істотний вплив на властивості інформації – конфіденційність, цілісність і доступність. У типовому бізнес-процесі можна виділити такі структурні елементи: 1) інформаційні об'єкти (дані клієнтів, облікові записи, транзакційні дані, службові повідомлення); 2) функціональні дії (створення, модифікація, передача, зберігання, видалення інформації); 3) суб'єкти (персонал, автоматизовані системи, зовнішні користувачі, партнери); 4) технічна інфраструктура (сервери, мережеві пристрої, канали зв'язку, хмарні сервіси); 5) контрольно-захисні механізми (аутентифікація, аудит, шифрування, політики доступу).

Аналіз бізнес-процесу ґрунтується на визначенні точок, де можливе виникнення загроз: при доступі користувачів, у каналах комунікації, під час збереження даних, в інтерфейсах взаємодії між сервісами, а також у місцях перетину прав доступу різних суб'єктів. Для цілей побудови НКК доцільно застосувати класифікацію загроз, що охоплює ключові категорії впливу на інформацію у бізнес-процесі, а саме: 1) технічні загрози, що пов'язані з технологічними компонентами процесу, серед яких перехоплення трафіку та несанкціоноване прослуховування каналів зв'язку, модифікація

даних під час передачі, шкідливе втручання в інформаційні системи (використання експлойтів, злом облікових записів) та порушення доступності через DDoS-атаки або технічні збої. Ці загрози безпосередньо впливають на стан інформації, порушуючи цілісність, конфіденційність або доступність у межах конкретних етапів бізнес-процесу; 2) організаційні загрози, що охоплюють помилки персоналу, недоліки процедур, порушення політик безпеки, відсутність регламентів і невідповідність між ролями та рівнями доступу. Оскільки бізнес-процеси передбачають залучення багатьох учасників, людський фактор часто стає одним із провідних джерел інцидентів. Наслідки таких загроз проявляються у некоректній обробці даних, випадковому витоку чи ненавмисному видаленні інформації; 3) соціоінженерні загрози, що мають на меті отримання доступу до інформації шляхом психологічного впливу на співробітників. Серед поширених сценаріїв – фішингові атаки, підроблені запити, маніпулятивні комунікації. Вразливість до соціоінженерних атак визначає ймовірність компрометації облікових даних або критичної інформації, яка далі впливає на всі наступні етапи бізнес-процесу. 4) внутрішні загрози включають дії співробітників, партнерів або користувачів, які мають легітимний доступ до системи, але використовують його зловмисно або недоброчесно. Оскільки внутрішній порушник має знання структури бізнес-процесу та доступ до ключових даних, його вплив є особливо небезпечним і важко прогнозованим. Такі загрози найчастіше призводять до суттєвого порушення цілісності та конфіденційності інформації. 5) комбіновані загрози у сучасних умовах рідко проявляються ізольовано та частіше вони взаємодіють у комплексі. Комбіновані загрози є особливо важливими для моделювання за допомогою НКК, оскільки вони створюють багатоетапні ланцюги впливу, характер яких складно передбачити традиційними методами.

Таблиця 1

Когнітивна матриця впливу факторів на інформації у бізнес-процесі

	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}
F_1	0	0	0	0	0	0	0	0	0	+1	+1	+1	0
F_2	0	0	0	0	0	0	0	0	0	+1	+1	+1	0
F_3	+1	+1	0	0	0	0	0	0	0	0	0	0	0
F_4	0	0	0	0	0	0	0	0	0	-1	0	0	0
F_5	0	0	0	0	0	0	0	0	0	0	-1	0	0
F_6	0	0	0	0	0	0	0	0	0	0	0	0	0
F_7	0	-1	0	0	0	0	0	0	0	0	0	0	0
F_8	0	-1	0	0	0	0	0	0	0	0	0	0	0
F_9	-1	0	0	0	0	0	0	0	0	0	0	0	0
F_{10}	0	0	0	0	0	-1	0	0	0	0	0	0	+1
F_{11}	0	0	0	0	0	-1	0	0	0	0	0	0	+1
F_{12}	0	0	0	0	0	-1	0	0	0	0	0	0	+1
F_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0

Забезпечення належного рівня ІБ в організації потребує комплексного врахування факторів, що формують як загрозове середовище, так і внутрішню стійкість інформаційних систем. У цьому дослідженні визначено тринадцять ключових концептів ($F_1 - F_{13}$), кожен з яких відіграє суттєву роль у функціонуванні бізнес-процесів та збереженні властивостей інформації – конфіденційності, цілісності та доступності. Цими концептами (факторами), що взаємопов'язані у відповідності до даних табл. 1, є: F_1 – зовнішні загрози; F_2 – внутрішні загрози; F_3 – уразливості інформаційних систем; F_4 – захищеність каналів передачі інформації; F_5 – якість обробки та зберігання даних; F_6 – рівень захищеності інформації у бізнес-процесі; F_7 – політики інформаційної безпеки; F_8 – рівень підготовки персоналу; F_9 – система моніторингу та виявлення атак; F_{10} – порушення конфіденційності інформації; F_{11} – порушення цілісності інформації;

F_{12} – порушення доступності інформації; F_{13} – рівень збитків для бізнес-процесу.

Матрицю впливів сформовано у строго формалізованому вигляді, де значення зв'язків між факторами, що впливають на стан інформації у гіпотетичному бізнес-процесі, інтерпретуються таким чином: значення $+1$ відповідає позитивному (підсилюючому) впливу; значення -1 – негативному (стримувальному) впливу; значення 0 – відсутності безпосереднього причинно-наслідкового зв'язку між відповідними концептами. У разі адаптації запропонованої когнітивної моделі до умов конкретного підприємства та його бізнес-процесів, числові значення зв'язків між концептами доцільно визначати у неперервному діапазоні значень $[-1; +1]$, з урахуванням експертних оцінок фахівців у сфері ІБ та специфіки функціонування відповідної організаційно-технічної системи. Результати, наведені у табл. 1, стали підґрунтям для побудови графа впливу факторів на стан інформації у гіпотетичному бізнес-процесі з використанням методу НКК. Отриману модель впливів у графічному вигляді подано на рис. 1.

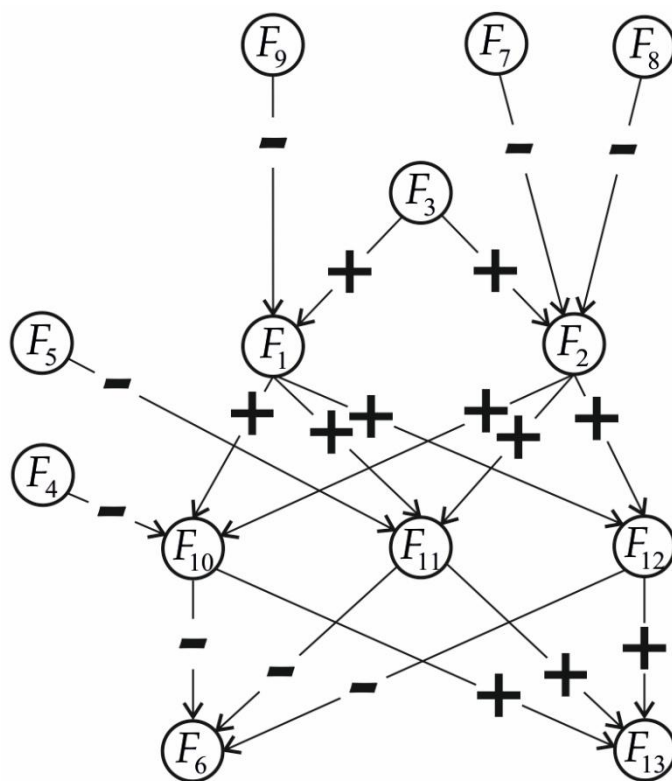


Рис. 1. Концептуальна модель впливу факторів на стан інформації в бізнес-процесі, побудована з використанням методу нечітких когнітивних карт

Концептуальна модель, подана на рис. 1, описує причинно-наслідкові зв'язки між факторами, що впливають на стан інформації в бізнес-процесі, за наступними напрямками: вплив загроз і уразливостей; організаційні та технічні фактори; наслідки для бізнес-процесу. Отже, першу групу

становлять зовнішні загрози (F_1), що включають кібератаки, хактивізм, вірусні інфекції, DDoS-атаки та фішингові кампанії. Вони формують первинний тиск на інформаційні активи організації та є найбільш поширеним джерелом інцидентів. Другу групу складають внутрішні загрози (F_2), пов'язані з

людським фактором: діями інсайдерів, помилками персоналу, недотриманням процедур або свідомим зловживанням повноваженнями. На відміну від зовнішніх атак, внутрішні загрози часто мають прихований характер і можуть спричиняти значні ушкодження інформації.

Ключовою умовою виникнення як зовнішніх, так і внутрішніх загроз є наявність уразливостей інформаційних систем (F_3). До них належать прогалини в архітектурі, застаріле або неправильно налаштоване програмне забезпечення, застосування слабких паролів та відсутність регулярних оновлень. Уразливості створюють додаткові можливості для реалізації атак і підвищують ймовірність їх успішності.

Важливим стабілізуючим чинником є захищеність каналів передачі інформації (F_4), яка включає застосування криптографічних механізмів, сегментацію мереж, використання технологій VPN (Virtual Private Network) та систем контролю доступу. Ефективні механізми захисту каналів значною мірою знижують ризик перехоплення, модифікації чи підробки даних у процесі їхнього транспортування. Аналогічно, якість обробки та зберігання даних (F_5) визначає здатність системи забезпечувати незмінність інформації, коректність операцій, своєчасне резервне копіювання та контроль версій.

Фактор F_6 відображає множину даних, що циркулюють у діяльності організації: операційних, фінансових, персональних, аналітичних та управлінських. Стан цієї інформації є інтегральним критерієм того, наскільки надійно функціонує бізнес-процес і наскільки він захищений від дестабілізуючих впливів.

Організаційний рівень моделі характеризується політиками ІБ (F_7), які охоплюють регламенти, стандарти та процедурні інструкції, і визначають правила взаємодії персоналу з інформаційними ресурсами. Їх ефективність безпосередньо залежить від рівня підготовки персоналу (F_8), що включає знання принципів кібергігієни, усвідомлення загроз і вміння реагувати на інциденти. Низький рівень обізнаності співробітників є одним з головних факторів виникнення інцидентів безпеки.

Технічний рівень контролю представлений системами моніторингу та виявлення атак (F_9), зокрема: системою централізованого збору, кореляції, аналізу та зберігання подій ІБ, що надходять з різномірних джерел інформаційної інфраструктури (Security Information and Event Management; SIEM); системою виявлення та запобігання вторгненням, призначені для моніторингу мережевого та/або хостового трафіку з метою ідентифікації ознак несанкціонованої активності, відомих атак або аномальної поведінки (Intrusion Detection System/Intrusion Prevention System; IDS/IPS); організаційно-технічним центром

управління подіями та інцидентами ІБ, що забезпечує безперервний моніторинг стану захищеності інформаційних ресурсів, аналіз подій безпеки, координацію реагування на інциденти та підтримку процесів прийняття рішень у режимі реального часу (Security Operations Center; SOC). Ці системи відіграють ключову роль у ранньому виявленні аномалій, зменшенні часу реагування на інциденти та запобіганні масштабних порушень.

Фактори F_{10} – F_{12} описують результат впливу загроз і уразливостей на інформацію у бізнес-процесі (F_6). Порушення конфіденційності (F_{10}) проявляється у витокі або несанкціонованому розголошенні даних. Порушення цілісності (F_{11}) призводить до спотворення, модифікації або знищення інформації, а порушення доступності (F_{12}) – до блокування або затримки виконання бізнес-процесів. Сукупний вплив цих порушень визначає рівень збитків для бізнес-процесу (F_{13}), що включає фінансові втрати, зниження продуктивності, репутаційні наслідки та витрати на відновлення.

Результати проведеного моделювання стали основою для прогнозування впливу факторів на стан інформації в бізнес-процесі з використанням методу сценарного аналізу. Застосування сценарного аналізу дозволяє прогнозувати можливі траєкторії розвитку досліджуваної ситуації, ідентифікувати та оцінювати рівень невизначеності, пов'язаної з дією ключових концептів, що визначають рівень захищеності інформації. У свою чергу, отримані результати створюють підґрунтя для формування обґрунтованих управлінських рішень, спрямованих на запобігання або мінімізацію негативного впливу на стан інформації в бізнес-процесі.

Для проведення аналізу НКК необхідно враховувати всі прямі та опосередковані взаємовпливи між концептами системи. З цією метою, на основі побудованої когнітивної карти, у роботі виконано аналіз основних системних показників, що ґрунтується на використанні матриці суміжності, яка формалізує структуру причинно-наслідкових зв'язків між концептами. Матриця суміжності дозволяє кількісно описати інтенсивність і напрям впливів, а також врахувати сукупний ефект багатокрокових взаємодій у системі, що є необхідною умовою для адекватного аналізу динаміки та поведінки досліджуваної моделі впливу факторів на стан інформації в бізнес-процесі. В представленій на рис. 1 моделі, у якості активаційної (нелінійної) функції застосовано функцію гіперболічного тангенсу, тому стан кожного концепту обчислювався як

$$A_i^{(t+1)} = \tanh\left(\sum_j A_j^{(t)} w_{ji}\right), \text{ де } A_j - \text{стан концепту,}$$

w_{ji} – вага зв'язку, $\tanh()$ – функція обмеження.

Особливістю застосування такого виду функції обмеження значення концептів у діапазоні $[-1; +1]$ є

те, що вона добре підходить для моделювання складних систем в умовах виникнення різного роду загроз небезпек, а також дозволяє формалізувати позитивні й негативні сценарії. Результати оцінок впливу факторів на інформації у бізнес-процесі наведено у табл. 2.

Серед представлених в табл. 2 результатів, показник впливу (outdegree) концепту характеризує ступінь його активного впливу на інші елементи системи та визначається як сума абсолютних значень вихідних зв'язків відповідного концепту, а саме

$$I_i = \sum_{j=1}^n |w_{ij}|, \text{ де } n - \text{кількість концептів у}$$

когнітивній карті. Високі значення цього показника свідчать про домінуючу роль у формуванні динаміки системи відіграють концепти F_1 і F_2 . Показник чутливості (indegree) концепту відображає ступінь залежності його стану від впливів інших концептів і визначається як сума абсолютних

$$\text{значень вхідних зв'язків, а саме } S_i = \sum_{j=1}^n |w_{ji}|.$$

Концепти F_6 , F_{10} , F_{11} , F_{12} та F_{13} , які характеризуються високою чутливістю, є найбільш уразливими до змін у системі та суттєво реагують на варіації зовнішніх і внутрішніх факторів. Для узагальненої оцінки ролі концепту використовується показник центральності (centrality), який враховує як активний, так і пасивний вплив: $C_i = I_i + S_i$. Показник центральності дозволяє ідентифікувати ключові концепти системи, що відіграють визначальну роль у її функціонуванні та формуванні сценаріїв розвитку. Цими концептами в представлений на рис. 1 моделі є концепти типу ordinary, а саме F_1 , F_2 , F_{10} , F_{11} та F_{12} .

Таблиця 2

Значущість впливу факторів на інформації у бізнес-процесі

Component	Indegree	Outdegree	Centrality	Type
F_1 – зовнішні загрози	2	3	5	ordinary
F_2 – внутрішні загрози	2	3	5	ordinary
F_3 – уразливості інформаційних систем	0	2	2	driver
F_4 – захищеність каналів передачі інформації	0	1	1	driver
F_5 – якість обробки та зберігання даних	0	1	1	driver
F_6 – рівень захищеності інформації у бізнес-процесі	3	0	3	receiver
F_7 – політики інформаційної безпеки	0	1	1	driver
F_8 – рівень підготовки персоналу	0	1	1	driver
F_9 – система моніторингу та виявлення атак	0	1	1	driver
F_{10} – порушення конфіденційності інформації	3	2	5	ordinary
F_{11} – порушення цілісності інформації	3	2	5	ordinary
F_{12} – порушення доступності інформації	3	2	5	ordinary
F_{13} – рівень збитків для бізнес-процесу	3	0	3	receiver

З метою поглибленого аналізу результатів когнітивного моделювання роботі було застосовано метод сценарного аналізу, який дозволяє дослідити можливі варіанти розвитку ситуації залежно від зміни інтенсивності впливу ключових факторів, а також забезпечує формування альтернативних траєкторій розвитку стану інформації в бізнес-процесі та дає змогу оцінити чутливість системи до дії загроз, уразливостей і компенсуючих організаційно-технічних заходів. Тому, у межах дослідження у роботі розглянуто три узагальнені сценарії.

Сценарій 1, так званий «Базовий сценарій», який характеризується середнім рівнем зовнішніх і внутрішніх загроз за умови наявності мінімально необхідного комплексу організаційних та технічних заходів захисту. За цього сценарію вплив факторів $F_1 - F_3$ частково компенсується дією факторів $F_4 - F_9$, що дозволяє підтримувати прийнятний рівень захищеності інформації у бізнес-процесі (F_6). Рівень збитків для бізнес-процесу (F_{13}) у цьому випадку може бути оцінено як помірний та контрольований.

Сценарій 2 – «Критичний сценарій». Цей сценарій передбачає зростання інтенсивності зовнішніх (F_1) та внутрішніх загроз (F_2) на тлі наявних уразливостей інформаційних систем (F_3) і недостатньої ефективності механізмів захисту, таких як F_4 – F_8 . За таких умов компенсуючий вплив організаційних і технічних факторів є недостатнім, що призводить до порушень конфіденційності (F_{10}), цілісності (F_{11}) та доступності інформації (F_{12}). У результаті рівень захищеності інформації у бізнес-процесі (F_6), а рівень збитків для бізнес-процесу (F_{13}) суттєво зростає, що може спричинити збій у функціонуванні критично важливих процесів та значні фінансові й репутаційні втрати.

Сценарій 3 – «Оптимістичний сценарій». Цей сценарій ґрунтується на підвищенні ефективності організаційно-технічних заходів захисту, зокрема впровадженні актуальних політик ІБ (F_7), підвищенні рівня підготовки персоналу (F_8) та розвитку систем моніторингу і виявлення атак (F_9). За такого сценарію негативний вплив загроз і уразливостей істотно зменшується, а порушення властивостей інформації мають поодинокий або локальний характер. Це забезпечує мінімальний рівень збитків для бізнес-процесу та підвищує загальну стійкість системи.

Таким чином, результати сценарного аналізу підтверджують доцільність використання когнітивної моделі як інструменту підтримки прийняття управлінських рішень у сфері ІБ. Отримані сценарії дозволяють не лише оцінити поточний стан захищеності інформації, а й обґрунтувати напрями підвищення ефективності захисних заходів з урахуванням специфіки бізнес-процесів.

Висновки

1. Розроблено та досліджено когнітивну модель впливу факторів на стан інформації в бізнес-процесі, побудовану з використанням методу НКК. Запропонований підхід дозволяє формалізувати складні причинно-наслідкові зв'язки між зовнішніми та внутрішніми загрозами, уразливостями інформаційних систем, організаційно-технічними заходами захисту та наслідками для бізнес-процесів. Визначено множину ключових концептів, що відображають як джерела ризиків, так і компенсуючі фактори, які впливають на конфіденційність, цілісність та доступність інформації. Побудована матриця впливів дала змогу формалізувати характер взаємодії між концептами та слугувала основою для побудови графа впливу факторів у межах гіпотетичного бізнес-процесу.

2. Застосування сценарного аналізу на основі результатів когнітивного моделювання дозволило оцінити можливі варіанти розвитку ситуації за різних умов функціонування системи ІБ. Отримані сценарії продемонстрували, що рівень збитків для

бізнес-процесу істотно залежить від узгодженості дій організаційних і технічних механізмів захисту та їх здатності компенсувати негативний вплив загроз і уразливостей. Практична цінність запропонованого підходу полягає у можливості його адаптації до умов конкретного підприємства шляхом уточнення значень зв'язків між концептами на основі експертних оцінок. Це створює підґрунтя для використання когнітивної моделі як інструменту підтримки прийняття управлінських рішень у сфері забезпечення ІБ бізнес-процесів. Подальші дослідження доцільно спрямувати на кількісну інтерпретацію ваг зв'язків між факторами, інтеграцію запропонованої моделі з методами оцінювання ризиків, а також апробацію підходу на реальних бізнес-процесах з урахуванням галузевої специфіки.

Література

- [1] Ортинський В.Л., Керницький І.С., Живко З.Б., Керницька М.І., Гук О.В., Шимечко Г.І., Живко М.О. Економічна безпека підприємств. Київ: Алтера, 2011. 704 с. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/369610579_EKONOMICNA_BEZPEKA_PIDPRIEMSTVA_SUTNIST_STRUKTURA_TA_MECHANIZM_ZABEZPECENNA
- [2] Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Правління Національного банку України. 28.09.2017. 95. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/v0095500-17#Text>
- [3] Волот О. Інформаційна та кібернетична безпека сучасного підприємства: за безпечення та моделювання. Центральноукраїнський науковий вісник. Економічні науки. 2019. 3(36). 238–247. [Електронний ресурс]. Режим доступу: [https://doi.org/10.32515/2663-1636.2018.3\(36\).238-247](https://doi.org/10.32515/2663-1636.2018.3(36).238-247)
- [4] Шостак Л.В., Помазун О.О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. Цифрова економіка та економічна безпека. 2024. 5(14). 160–165.
- [5] Онищенко С.В., Ківшик О.П. Управління інформаційною безпекою стратегічно важливих підприємств в умовах викликів й загроз. Економіка і регіон. 2022. 3(86). 80–85. [Електронний ресурс]. Режим доступу: [https://doi.org/10.26906/EiR.2022.3\(86\).2817](https://doi.org/10.26906/EiR.2022.3(86).2817)
- [6] Валіулліна З.В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. Вісник Дніпропетровського університету. Серія: Менеджмент інновацій. 2016. 6. 34–43.
- [7] Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. Київ: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с. [Електронний ресурс]. Режим доступу: https://duikt.edu.ua/uploads/1_1240_28693628.pdf
- [8] Tiutiunyk V., Tiutiunyk O., Teslenko O., Brynza N. Peculiar Properties of Creating a System of Support to Make Anti Crisis Decisions by Experts of the Situational Center at the Cyber Protection Object. 3rd International Scientific and Practical Conference on Information Security and Information Technologies. 2021. 3200. 47–56. [Електронний ресурс]. Режим доступу: http://repositc.nuczu.edu.ua/bitstream/123456789/14239/1/DRF_2021_Tiutiunyk_ENG.pdf
- [9] Тютюнник В.В., Тютюнник О.О., Усачов Д.В. Особливості застосування нечітких когнітивних карт для сценарного моделювання функціонування критичної інфраструктури в умовах надзвичайних ситуацій воєнного

характеру. Modern Information Technologies in the Sphere of Security and Defence. 2025. 3(54). 93–102. [Електронний ресурс]. Режим доступу: <https://sit.nuou.org.ua/article/view/338904>

[10] Chernysh I., Makhovka V., Lobach L. Management of Information Security of the Enterprise in the Conditions of Dynamic Business Environment. Economics and Business Administration. Economics and Region. 2020. 1(76). 106–112.

[11] Мілявський Ю.Л. Когнітивне моделювання складних систем. Проектування та аналіз когнітивних моделей. Київ. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». 2025. 39. [Електронний ресурс]. Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/3c03af72-c07a-4a10-bc76-4b7e37d9bae8/content>

[12] Papageorgiou E.I., Salmeron J.L. Review study on Fuzzy Cognitive Maps and their applications during the last decade. IEEE International Conference on Fuzzy Systems. 2011. 828–835. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/230750770_A_Review_of_Fuzzy_Cognitive_Maps_Research_During_the_Last_Decade

[13] Stylios C.D., Groumpos P.P. Modeling Complex Systems Using Fuzzy Cognitive Maps. IEEE Transactions on Systems, Man, and Cybernetics. 2004. 34. 1. 155–162. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/3412335_Modeling_Complex_Systems_Using_Fuzzy_Cognitive_Maps

[14] Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. Сучасний захист інформації. 2024. 2(58), 103–108. [Електронний ресурс]. Режим доступу: <https://doi.org/10.31673/2409-7292.2024.020012>

[15] Шевченко С.М., Жданова Ю.Д., Гаркушенко А.М. Когнітивний підхід в інформаційній та кібербезпеці. Кібербезпека: освіта, наука, техніка. 2025. 1(29). 854–866. [Електронний ресурс]. Режим доступу: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/945/775>

[16] Сікора Л.С., Лиса Н.К., Павлюк О.М., Сабат В.І., Федевич О.Ю. Інформаційні та логіко-когнітивні підходи до формування кібербезпеки техногенних інфраструктур з урахуванням рівня ризиків. Scientific Bulletin of UNFU. 2023. 33. 1. 71–81.

УДК 003.26:004.056.55:621.39(045)

Tiutiunyk V, Tiutiunyk O. Application of Fuzzy Cognitive Maps for Scenario-Based Modeling of Threat Impacts on Information in Business Processes

Abstract. This paper presents an approach to analyzing the impact of threats and organizational–technical factors on the state of information within business processes using the fuzzy cognitive map methodology. A set of key concepts is defined to represent external and internal threats, vulnerabilities of information systems, protective mechanisms, and the consequences of violations of information confidentiality, integrity, and availability. A formally structured influence matrix is developed, where causal relationships between concepts are described using positive, negative, and neutral interactions, serving as the basis for constructing a cognitive influence graph for a hypothetical business process. The proposed cognitive model enables the identification of systemic interdependencies between risk-generating factors and compensating security controls, allowing a comprehensive assessment of information security resilience. Based on the results of cognitive modeling, scenario analysis is applied to forecast possible trajectories of system behavior under varying threat intensities and levels of protection effectiveness. Several generalized scenarios are considered, including baseline, critical, and optimistic scenarios, which differ in the balance between threats, vulnerabilities, and security measures. The obtained results demonstrate that the level of damage to business processes is largely determined by the coherence and maturity of organizational and technical security mechanisms, as well as their ability to mitigate the negative impact of threats and vulnerabilities. The proposed approach can be adapted to specific enterprises by refining the weights of causal relationships through expert assessments, which enables its practical application as a decision support tool in information security management.

Keywords: information security, business process, fuzzy cognitive maps, cognitive modeling, threat analysis, information system vulnerabilities, scenario analysis, CIA triad, SIEM, IDS/IPS, SOC.

Тютюник Вадим Володимирович, професор кафедри кібербезпеки та інформаційних технологій, професор кафедри безпеки інформаційних технологій.

Tiutiunyk Vadym, Professor of the Department of Cybersecurity and Information Technologies, Professor of the Department of Information Technology Security.

Тютюник Ольга Олександрівна, доцент кафедри інформатики та комп'ютерної техніки.

Tiutiunyk Olha, Associate Professor of the Department of Computer Science and Computer Engineering.

Дата надходження:

26.01.2026

Дата прийняття:

18.03.206

Дата публікації:

22.04.2026