УДК 004.002+658.5 **DOI: 10.33042/3083-6727-2026-1-196-22-33**

В.В. Тютюник[1,2], О.О. Тютюник[1]

[1]*Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна*
[2]*Харківський національний університет радіоелектроніки, Харків, Україна*

СЦЕНАРНЕ КОГНІТИВНЕ МОДЕЛЮВАННЯ ВПЛИВУ ЗАГРОЗ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЗАПРОВАДЖЕННЯ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

У статті розроблено та досліджено когнітивну модель сценаріїв впливу загроз на інформаційну безпеку об'єктів критичної інфраструктури в умовах воєнного стану з урахуванням нелінійних причинно-наслідкових зв'язків та сценарного характеру розвитку загроз з метою підтримки прийняття управлінських рішень.

Ключові слова: *інформаційна безпека; об'єкти критичної інфраструктури; когнітивне моделювання; сценарне моделювання; воєнний стан; загрози інформаційній безпеці; антикризове управління.*

Постановка проблеми

В умовах повномасштабної збройної агресії та запровадження правового режиму воєнного стану в Україні суттєво зростає роль об'єктів критичної інфраструктури (ОКІ) у забезпеченні життєдіяльності держави, суспільства та економіки [1–3]. Функціонування таких об'єктів безпосередньо залежить від стану інформаційної безпеки (ІБ), оскільки порушення процесів обробки, зберігання та передавання інформації може призвести до значних соціально-економічних, техногенних і безпекових наслідків [4–6].

Особливістю сучасних умов є комплексний характер загроз ІБ ОКІ, що поєднують кібернетичні атаки, фізичний вплив на інфраструктурні елементи, інформаційно-психологічні операції, а також організаційні та кадрові ризики. Вплив зазначених загроз має нелінійний характер, супроводжується наявністю зворотних зв'язків і каскадних ефектів, що суттєво ускладнює їх аналіз та прогнозування за допомогою традиційних методів оцінювання ризиків [7–9].

У наукових дослідженнях значна увага приділяється питанням захисту критичної інфраструктури, кібербезпеки та управління ризиками. Водночас недостатньо опрацьованими залишаються підходи, які дозволяють враховувати взаємозалежність загроз, динаміку їх розвитку та сценарний характер впливу на ІБ в умовах воєнного стану. Це зумовлює необхідність застосування інструментів когнітивного моделювання, зокрема нечітких когнітивних карт (НКК), що забезпечують формалізований опис складних причинно-наслідкових зв'язків між елементами системи [10, 11].

Когнітивне сценарне моделювання дозволяє не лише ідентифікувати ключові загрози ІБ, але й оцінити їх системний вплив на стійкість функціонування ОКІ за різних сценаріїв розвитку подій. Використання такого підходу створює підґрунтя для підтримки прийняття управлінських рішень у сфері ІБ в умовах високої невизначеності та обмеженості ресурсів.

З огляду на зазначене, актуальним є дослідження, спрямоване на розроблення когнітивної моделі сценаріїв впливу загроз на ІБ ОКІ в умовах введення в державі правового режиму воєнного стану. Це і обумовило мету наших досліджень.

Аналіз останніх досліджень і публікацій

Проблематика забезпечення ІБ ОКІ є предметом активних досліджень як у вітчизняній, так і в зарубіжній науковій літературі. Особлива увага приділяється питанням аналізу загроз, оцінювання ризиків та прогнозування наслідків їх реалізації в умовах зростаючої складності, взаємозалежності та динамічності сучасних соціально-технічних систем.

У класичних підходах до аналізу ризиків ІБ широко застосовуються імовірнісні методи, логіко-імовірнісні моделі, дерева відмов і атак, байєсівські мережі, а також методи багатокритеріального аналізу. Однак зазначені підходи здебільшого орієнтовані на статичний аналіз і не повною мірою враховують нелінійні причинно-наслідкові зв'язки, наявність зворотних зв'язків і сценарний характер розвитку загроз, що є характерним для функціонування ОКІ [12, 13].

У зв'язку з цим у світовій науці активно розвивається напрям застосування когнітивного моделювання, зокрема НКК (Fuzzy Cognitive Maps, FCM), для аналізу складних систем безпеки. У фундаментальних роботах з теорії FCM зазначається, що когнітивні карти дозволяють формалізувати

експертні знання у вигляді орієнтованих графів із зваженими зв'язками, що дає змогу поєднувати якісний і кількісний аналіз та здійснювати імітаційне моделювання сценаріїв розвитку системи [14, 15].

Зарубіжні дослідження демонструють ефективність використання FCM для оцінювання кіберризиків і загроз у критичних інфраструктурах різного призначення, зокрема енергетичних системах, транспортних вузлах, портових комплексах і промислових системах управління. У таких роботах когнітивні карти застосовуються для виявлення ключових факторів ризику, аналізу каскадних ефектів та визначення критичних вузлів, порушення яких може призвести до суттєвого зниження рівня ІБ. Окремий напрям іноземних досліджень пов'язаний із інтеграцією когнітивних карт із методами оцінювання вразливостей і сценарного аналізу кібератак на промислові системи управління (ICS/SCADA). У таких підходах когнітивні моделі дозволяють відобразити взаємозв'язки між активами, уразливостями, загрозами та заходами захисту, а також моделювати різні сценарії розвитку атак і оцінювати їх системний вплив [16–18].

Також когнітивне моделювання активно використовується у дослідженнях ІБ в галузях, де критичність інформації є особливо високою, зокрема в охороні здоров'я, телекомунікаціях та системах електронного урядування. У цих роботах підкреслюється здатність FCM-підходу враховувати людський фактор, організаційні аспекти та управлінські рішення, що є суттєвим для аналізу загроз у реальних умовах експлуатації [19].

Узагальнюючи результати аналізу іноземних джерел, можна зробити висновок, що когнітивні та нечіткі когнітивні моделі є одним із найбільш перспективних інструментів для сценарного аналізу загроз ІБ критичної інфраструктури. Водночас більшість існуючих робіт зосереджені на мирний час або стандартні умови функціонування систем і не враховують специфіку правового режиму воєнного стану, який характеризується підвищеною інтенсивністю загроз, обмеженістю ресурсів і необхідністю швидкого прийняття рішень.

Таким чином, аналіз наукових публікацій свідчить про наявність наукової прогалини, пов'язаної з недостатнім опрацюванням питань когнітивного сценарного моделювання впливу загроз на ІБ ОКІ саме в умовах воєнного стану, що зумовлює актуальність і доцільність проведення даного дослідження.

Формулювання мети статті

З огляду на зростання інтенсивності та складності загроз ІБ ОКІ в умовах воєнного стану, а також необхідність урахування нелінійних причинно-наслідкових зв'язків і сценарного характеру їх розвитку, метою статті є розроблення та дослідження когнітивної моделі сценаріїв впливу загроз на ІБ ОКІ в умовах воєнного стану з метою підтримки прийняття управлінських рішень.

Для досягнення поставленої мети у статті передбачається розв'язання таких завдань: 1) проаналізувати особливості загроз ІБ ОКІ в умовах воєнного стану; 2) сформувати перелік ключових факторів і загроз, що впливають на ІБ; 3) побудувати когнітивну модель причинно-наслідкових зв'язків між загрозами, інформаційними процесами та станами ІБ; 4) здійснити сценарне моделювання впливу загроз за різних умов розвитку подій; 5) оцінити системні показники когнітивної моделі з метою ідентифікації критичних факторів; 6) обґрунтувати можливості практичного використання отриманих результатів для підтримки прийняття рішень у сфері ІБ.

Виклад основного матеріалу

Теоретико-методологічні засади класифікації ОКІ та загроз інформаційній безпеці в умовах воєнного стану. Захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз є важливою задачею в умовах нерівномірного розподілу по території держави критичної інфраструктури, з низкою життєвоважливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, зокрема: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (у тому числі постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність [20–22].

Виходячи за даними рис. 1, ОКІ являють собою складні соціально-технічні системи, порушення функціонування яких може призвести до значних негативних наслідків для національної безпеки, економіки та життєдіяльності населення. В умовах воєнного стану особливого значення набуває класифікація ОКІ з урахуванням їх функціонального призначення, рівня критичності, характеру інформаційних процесів та спектра загроз ІБ [23, 24].

Класифікація ОКІ за функціональним

призначенням базується на визначені множини об'єктів у вигляді:

$$OCI = \{o_1, o_2, ..., o_n\}. \quad (1)$$

Тоді за функціональним призначенням визначається розбиття:

$$OCI = \bigcup_{k=1}^{K} OCI_k, \quad (2)$$

де OCI_k – підмножина об'єктів відповідного сектору критичної інфраструктури (енергетична інфраструктура; транспортна інфраструктура; інформаційно-телекомунікаційна інфраструктура; фінансово-банківська система; системи водопостачання та водовідведення; охорона здоров'я та екстрені служби; державне управління та оборонний сектор).

Класифікація за рівнем критичності ОКІ базується на тому, що для кожного об'єкта $o_i \in OCI$ вводиться показник критичності:

$$K(o_i) \in \{K_N, K_R, K_L\}, \quad (3)$$

де K_N – національний рівень, K_R – регіональний рівень, K_L – локальний рівень. Рівень критичності визначається масштабом можливих наслідків порушення функціонування об'єкта та використовується як ваговий коефіцієнт під час сценарного аналізу загроз.

Рис. 1. Схема класифікації ОКІ з позицій ІБ в умовах запровадження правового режиму воєнного стану

Класифікація за характером інформаційних процесів та з точки зору ІБ кожен ОКІ характеризується домінуючим типом інформаційних процесів:

$$IP(o_i) \in \{ICS, IS, DIS\}, \quad (4)$$

де *ICS* – автоматизовані системи управління та промислові системи (ICS/SCADA), *IS* – інформаційно-аналітичні системи, *DIS* – розподілені інформаційні системи та мережі зв'язку. Цей критерій є ключовим для формування переліку загроз та визначення структури когнітивної моделі, оскільки тип інформаційних процесів безпосередньо впливає на вразливість об'єкта.

В свою чергу, функціонування ОКІ в умовах воєнного стану характеризується суттєвою зміною середовища безпеки, що супроводжується зростанням інтенсивності, різноманітності та взаємопов'язаності загроз ІБ. Запровадження правового режиму воєнного стану зумовлює не лише підвищені вимоги до безперервності роботи таких об'єктів, але й накладає додаткові організаційні, правові та ресурсні обмеження, які безпосередньо впливають на стан ІБ.

Однією з ключових особливостей воєнного стану є поєднання кібернетичних, фізичних та інформаційно-психологічних загроз, які реалізуються комплексно та часто синхронізовано. Кібернетичні загрози включають цілеспрямовані атаки на інформаційні системи та мережі ОКІ, зокрема атаки типу DDoS, впровадження шкідливого програмного забезпечення, компрометацію облікових даних, атаки на промислові системи управління та автоматизовані системи управління технологічними процесами. Такі атаки можуть призводити до порушення доступності, цілісності та конфіденційності інформації, що циркулює в критично важливих процесах.

Фізичні загрози в умовах воєнного стану набувають особливої актуальності та пов'язані з можливістю безпосереднього ураження інфраструктурних об'єктів, каналів зв'язку, центрів обробки даних, енергетичних і телекомунікаційних вузлів. Руйнування або пошкодження фізичних елементів інфраструктури призводить до порушення інформаційних процесів зберігання та передавання даних, а також створює умови для вторинних кібернетичних інцидентів і каскадних відмов.

Вагомим чинником у системі загроз є людський фактор, який у період воєнного стану посилюється через підвищене психоемоційне навантаження, дефіцит кваліфікованого персоналу, ротацію кадрів і необхідність залучення тимчасових або недостатньо підготовлених працівників. Це підвищує ймовірність помилок оператора, порушення регламентів безпеки

та успішної реалізації атак соціальної інженерії.

Окрему групу становлять інформаційно-психологічні загрози, спрямовані на дезінформацію, маніпуляцію та підрив довіри до інформації, що використовується в процесах управління ОКІ. Поширення недостовірної або спотвореної інформації може призводити до ухвалення помилкових управлінських рішень, що опосередковано впливає на стійкість функціонування об'єктів і рівень їх ІБ.

Умови воєнного стану також передбачають зміну організаційних та управлінських процесів, зокрема централізацію управління, обмеження доступу до інформації, пріоритетність виконання окремих функцій і перерозподіл ресурсів. З одного боку, такі заходи спрямовані на підвищення рівня захищеності, а з іншого – можуть створювати додаткові ризики, пов'язані з перевантаженням систем управління, зниженням гнучкості та затримками в обміні інформацією.

Таким чином, загрози ІБ ОКІ в умовах воєнного стану мають системний, багатофакторний та динамічний характер. Їхній вплив проявляється через складні причинно-наслідкові зв'язки між технічними, організаційними та людськими компонентами системи. Тому, класифікація за типами загроз в умовах воєнного стану через множину загроз ІБ для об'єкта o_i може бути представлена як

$$T(o_i) = \{T_c, T_p, T_h\}, \quad (5)$$

де T_c – кібернетичні загрози, T_p – фізичні загрози, T_h – гібридні загрози.

Для кількісного аналізу введено вектор загроз:

$$T(o_i) = \{t_c, t_p, t_h\}, \quad (6)$$

де кожна компонента $t_j \in [0;1]$ відображає інтенсивність відповідного типу загроз.

З урахуванням наведених критеріїв кожен ОКІ може бути описаний узагальненим кортежем:

$$o_i = \langle OCI_k, K(o_i), IP(o_i), T(o_i) \rangle. \quad (7)$$

Запропонована формалізація дозволяє уніфікувати опис різнорідних ОКІ, використовувати класифікаційні ознаки як вхідні параметри когнітивної моделі та формувати сценарії впливу загроз з урахуванням специфіки воєнного стану. Так, розроблена класифікація створює методичну основу для подальшого когнітивного сценарного моделювання впливу загроз на ІБ ОКІ.

Когнітивне моделювання впливу загроз на інформаційну безпеку ОКІ в умовах воєнного стану. В роботі когнітивну модель подано на рис. 2 у вигляді орієнтованого зваженого графа:

$$G = \langle C, E, W \rangle, \quad (8)$$

де $C = \{c_1, c_2, ..., c_n\}$ – множина концептів, $E \subseteq C \times C$ – множина орієнтованих зв'язків між концептами, $W = \{w_{ij}\}$ – множина ваг зв'язків, $w_{ij} \in [-1;1]$.

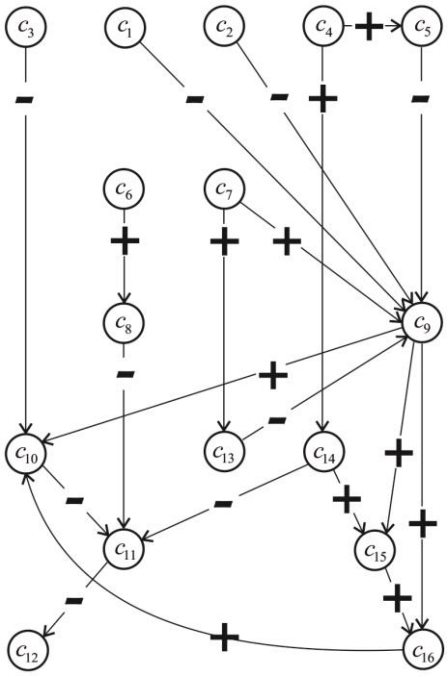

Рис. 2. Когнітивна модель сценарного впливу загроз на ІБ ОКІ в умовах запровадження правового режиму воєнного стану

З урахуванням специфіки функціонування ОКІ в умовах введення правового режиму воєнного стану множина концептів формується з чотирьох логічних груп.

Перша група – концепти-загрози (Driver-concepts):

$$C_D = \{c_1, c_2, c_3, c_4, c_5\}, \quad (9)$$

де c_1 – кібератаки на інформаційні системи ОКІ, c_2 – фізичне ураження об'єктів інфраструктури, c_3 – порушення телекомунікаційних каналів, c_4 – інформаційно-психологічні впливи, c_5 – інсайдерські загрози. Дані концепти є зовнішніми по відношенню до системи та ініціюють сценарії впливу.

Друга група – концепти умов воєнного стану (Ordinary-concepts):

$$C_W = \{c_6, c_7, c_8, c_9\}, \quad (10)$$

де c_6 – обмеженість ресурсів, c_7 – централізація управління, c_8 – дефіцит кваліфікованого персоналу, c_9 – підвищена інтенсивність зовнішніх загроз. Ці концепти виступають як підсилювачі або демпфери впливів.

Третя група – концепти інформаційної безпеки (Ordinary-concepts):

$$C_{IB} = \{c_{10}, c_{11}, c_{12}, c_{13}\}, \quad (11)$$

де c_{10} – конфіденційність інформації, c_{11} – цілісність інформації, c_{12} – доступність інформації, c_{13} – стійкість інформаційних систем.

Четверта група – концепти наслідків (Receiver-concepts):

$$C_R = \{c_{14}, c_{15}, c_{16}\}, \quad (12)$$

де c_{14} – порушення функціонування ОКІ, c_{15} – соціально-економічні збитки, c_{16} – зниження рівня національної безпеки.

Матрицю зв'язків між загрозами, умовами функціонування, інформаційними процесами та наслідками для ОКІ в умовах правового режиму воєнного стану сформовано у строго формалізованому вигляді. Зокрема, значення +1 відповідає позитивному (підсилюючому) впливу одного концепту на інший; значення –1 – негативному (стримувальному) впливу; значення 0 – відсутності безпосереднього причинно-наслідкового зв'язку між відповідними концептами. Отримані результати формалізації взаємовпливів наведено у табл. 1. Водночас, у разі адаптації запропонованої когнітивної моделі до умов функціонування конкретного ОКІ, числові значення зв'язків між концептами доцільно визначати у неперервному діапазоні значень $w_{ij} \in [-1;1]$, що дає змогу більш точно відобразити інтенсивність причинно-наслідкових впливів. Оцінювання вагових коефіцієнтів w_{ij} у такому випадку рекомендується здійснювати з використанням експертних оцінок фахівців у сфері ІБ, з урахуванням специфіки функціонування відповідної організаційно-технічної системи, рівня її критичності, галузевих особливостей та умов воєнного стану. Застосування неперервної шкали значень дозволяє підвищити адекватність когнітивної моделі та забезпечити більш гнучке сценарне моделювання впливу загроз на ІБ ОКІ.

Таблиця 1.

Когнітивна матриця зв'язків між загрозами, умовами функціонування, інформаційними процесами та наслідками для ОКІ в умовах запровадження правового режиму воєнного стану

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
c_1	0	0	0	0	0	0	0	0	–1	0	0	0	0	0	0	0
c_2	0	0	0	0	0	0	0	0	–1	0	0	0	0	0	0	0
c_3	0	0	0	0	0	0	0	0	0	–1	0	0	0	0	0	0
c_4	0	0	0	0	+1	0	0	0	0	0	0	0	0	+1	0	0
c_5	0	0	0	0	0	0	0	0	–1	0	0	0	0	0	0	0
c_6	0	0	0	0	0	0	0	–1	0	0	0	0	0	0	0	0
c_7	0	0	0	0	0	0	0	0	+1	0	0	0	+1	0	0	0
c_8	0	0	0	0	0	0	0	0	0	0	–1	0	0	0	0	0
c_9	0	0	0	0	0	0	0	0	0	+1	0	0	0	0	+1	+1
c_{10}	0	0	0	0	0	0	0	0	0	0	–1	0	0	0	0	0
c_{11}	0	0	0	0	0	0	0	0	0	0	0	–1	0	0	0	0
c_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
c_{13}	0	0	0	0	0	0	0	0	–1	0	0	0	0	0	0	0
c_{14}	0	0	0	0	0	0	0	0	0	0	–1	0	0	0	+1	0
c_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1
c_{16}	0	0	0	0	0	0	0	0	0	+1	0	0	0	0	0	0

У якості активаційної (нелінійної) функції в когнітивній моделі застосовано функцію гіперболічного тангенса, що забезпечує обмеження значень станів концептів у скінченному інтервалі. З урахуванням цього стан кожного концепту c_i на k-ій ітерації обчислюється за співвідношенням

$$x_i^{(t+1)} = f\left(\sum_{j=1}^{n} w_{ji} x_j^{(k)}\right), \quad f(z) = \tanh(z), \qquad (13)$$

де $x_j^{(k)}$ – стан i-то концепту, w_{ji} – ваговий коефіцієнт впливу j-го концепту на i-й, $f()$ – функція обмеження.

Особливістю застосування гіперболічного тангенса є те, що значення станів концептів обмежуються діапазоном $x_i \in [-1;1]$, що робить цю функцію доцільною для моделювання складних організаційно-технічних систем в умовах виникнення різнотипних загроз і небезпек. Такий підхід дозволяє формалізувати як позитивні (підсилюючі), так і негативні (деструктивні) сценарії розвитку ситуації, а також забезпечує стійкість обчислювального процесу під час ітераційного сценарного аналізу. Результати оцінювання впливу факторів на загрози, умови функціонування, інформаційні процеси та наслідки для ОКІ в умовах правового режиму воєнного стану наведено у табл. 2.

Таблиця 2.

Значущість впливу факторів на загрози, умови функціонування, інформаційні процеси та наслідки для ОКІ в умовах запровадження правового режиму воєнного стану

Component	Indegree	Outdegree	Centrality	Type
c_1 – кібератаки на інформаційні системи ОКІ	0	1	1	driver
c_2 – фізичне ураження ОКІ	0	1	1	driver
c_3 – порушення телекомунікаційних каналів	0	1	1	driver
c_4 – інформаційно-психологічні впливи	0	2	2	driver
c_5 – інсайдерські загрози	1	1	2	ordinary
c_6 – обмеженість ресурсів	0	1	1	driver
c_7 – централізація управління	0	2	2	driver
c_8 – дефіцит кваліфікованого персоналу	1	1	2	ordinary
c_9 – підвищена інтенсивність зовнішніх загроз	5	3	8	ordinary
c_{10} – конфіденційність інформації	3	1	2	ordinary
c_{11} – цілісність інформації	3	1	4	ordinary
c_{12} – доступність інформації	1	0	1	receiver
c_{13} – стійкість інформаційних систем	1	1	2	ordinary
c_{14} – порушення функціонування ОКІ	1	2	3	ordinary
c_{15} – соціально-економічні збитки	2	1	3	ordinary
c_{16} – зниження рівня національної безпеки	2	1	3	ordinary

Серед результатів, наведених у табл. 2, показник впливу (outdegree) концепту характеризує ступінь його активного впливу на інші елементи системи. Даний показник визначається як сума абсолютних значень усіх вихідних зв'язків відповідного концепту та обчислюється за формулою

$$Out_i = \sum_{j=1}^{n} |w_{ij}|, \qquad (14)$$

де n – кількість концептів у когнітивній карті.

Показник чутливості (indegree) концепту відображає ступінь залежності його стану від впливів інших концептів системи та визначається як сума абсолютних значень усіх вхідних зв'язків:

$$In_i = \sum_{j=1}^{n} |w_{ji}|. \qquad (15)$$

Для узагальненої оцінки ролі концепту в когнітивній моделі використовується показник центральності (centrality), який враховує як активний, так і пасивний вплив концепту:

$$C_i = Out_i + In_i . \quad (16)$$

Показник центральності дозволяє ідентифікувати ключові концепти системи, що відіграють визначальну роль у її функціонуванні, поширенні загроз та формуванні сценаріїв розвитку ІБ ОКІ в умовах правового режиму воєнного стану.

За даними табл. 2 запропонована когнітивна модель відображає причинно-наслідкові зв'язки між загрозами, умовами функціонування, інформаційними процесами та наслідками для ОКІ в умовах правового режиму воєнного стану. На початковому рівні моделі розміщені driver-концепти, що описують ключові деструктивні фактори та умови воєнного часу. Їх активізація призводить до зростання інтенсивності загроз та безпосередньо впливає на центральний концепт c_9, який агрегує стан ІБ ОКІ. Центральний концепт c_9 виконує роль системного вузла трансформації, через який реалізується вплив як загроз, так і захисних та організаційних заходів. Подальше поширення впливів відбувається через інформаційно-управлінський контур, що включає рівень довіри до інформації (c_{15}) та якість управлінських рішень (c_{16}). Наслідки реалізації загроз акумулюються у receiver-концептах c_{10}, c_{11} та c_{12} які відображають зниження стійкості об'єктів, масштаб негативних наслідків та соціально-економічні втрати. Наявність зворотних зв'язків у моделі забезпечує відображення адаптивного характеру системи та можливості компенсації негативних впливів шляхом управлінських рішень.

Розроблена когнітивна модель дозволяє здійснювати сценарне моделювання розвитку ситуацій, оцінювати чутливість інформаційної безпеки до окремих загроз та обґрунтовувати пріоритетні напрями підвищення стійкості ОКІ в умовах введення правового режиму воєнного стану. Результати сценарного моделювання впливу загроз на ІБ ОКІ в умовах воєнного стану дозволяють виявити системні закономірності поширення негативних впливів, а також визначити ключові фактори, що формують стійкість або вразливість досліджуваної системи.

Так, порівняльний аналіз базового, кризового та катастрофічного сценаріїв показав, що зі зростанням інтенсивності загроз спостерігається нелінійний характер змін станів концептів. Навіть помірне підвищення активності driver-концептів за наявності несприятливих умов воєнного стану призводить до суттєвого зниження показників доступності та стійкості інформаційних систем. У кризовому сценарії зафіксовано ефект каскадного поширення впливів, коли первинні кібернетичні або фізичні загрози через систему опосередкованих зв'язків спричиняють порушення функціонування ОКІ. Це підтверджує доцільність врахування непрямих впливів у межах когнітивного підходу.

Аналіз системних показників впливу, чутливості та центральності дозволив ідентифікувати критичні вузли когнітивної моделі. Концепти, пов'язані з доступністю та стійкістю інформаційних систем, мають найвищі значення центральності, що свідчить про їх визначальну роль у забезпеченні стабільності функціонування ОКІ. Driver-концепти, що відповідають кібернетичним атакам і фізичному ураженню об'єктів, демонструють максимальні значення показника впливу. Натомість receiver-концепти, які відображають соціально-економічні наслідки та рівень національної безпеки, характеризуються високою чутливістю, що робить їх індикаторами критичного стану системи.

Отримані результати свідчать, що з точки зору управління ризиками доцільно зосереджувати захисні заходи не лише на нейтралізації окремих загроз, але й на підвищенні стійкості ключових концептів з високою центральністю. Такий підхід дозволяє зменшити системний ефект негативних впливів навіть у разі реалізації кризових сценаріїв [25]. Крім того, когнітивна модель може використовуватися як інструмент підтримки прийняття рішень для оцінювання ефективності різних стратегій забезпечення ІБ ОКІ [26].

Крім того, результати моделювання підтверджують, що умови воєнного стану відіграють роль підсилювальних факторів, які знижують адаптивні можливості системи ІБ. Обмеженість ресурсів, дефіцит персоналу та централізація управління зменшують ефективність реагування на загрози та прискорюють перехід системи у кризовий або катастрофічний стан. Так, навіть за однакового рівня загроз, ІБ ОКІ в умовах воєнного стану є значно вразливішою порівняно з мирним часом.

Алгоритм антикризового управління інформаційною безпекою ОКІ та практичні рекомендації. На основі результатів когнітивного сценарного моделювання впливу загроз на ІБ ОКІ в умовах воєнного стану в роботі сформульовано комплекс практичних рекомендацій, спрямованих на підвищення стійкості інформаційних систем та зменшення негативних наслідків реалізації кризових сценаріїв.

Так, з огляду на високі значення показників центральності концептів доступності та стійкості інформаційних систем доцільно спрямовувати першочергові захисні заходи саме на ці компоненти. До таких заходів належать: резервування критичних інформаційних ресурсів; використання відмовостійких архітектур; сегментація мереж та

ізоляція критичних компонентів. Такий підхід дозволяє зменшити системний ефект поширення загроз навіть за умов їх ескалації.

Для мінімізації впливу загроз, що виступають ініціаторами негативних сценаріїв, рекомендовано: впроваджувати багаторівневі системи кіберзахисту (Defense in Depth); посилювати контроль доступу до інформаційних систем ОКІ; застосовувати регулярний моніторинг подій безпеки та засоби раннього виявлення атак. Особливу увагу слід приділяти захисту автоматизованих систем управління та промислових мереж, які є найбільш уразливими в умовах воєнного стану.

Результати сценарного моделювання свідчать, що обмеженість ресурсів та дефіцит кваліфікованого персоналу значно знижують ефективність заходів ІБ. У зв'язку з цим доцільно: автоматизувати процеси реагування на інциденти; впроваджувати спрощені, але надійні процедури управління безпекою; забезпечувати перехресну підготовку персоналу для виконання критичних функцій.

Запропоновану когнітивну модель доцільно використовувати як інструмент підтримки прийняття рішень під час: планування заходів захисту інформаційної інфраструктури; оцінювання ефективності альтернативних стратегій безпеки; прогнозування наслідків реалізації нових або комбінованих загроз. Це дозволяє переходити від реактивного до проактивного управління ІБ ОКІ.

В умовах же воєнного стану особливої актуальності набуває протидія гібридним загрозам. Для цього рекомендовано: поєднувати заходи кібербезпеки та фізичного захисту; забезпечувати узгодженість дій технічних і організаційних підрозділів; впроваджувати сценарні навчання на основі результатів когнітивного моделювання.

Практична реалізація результатів сценарного когнітивного моделювання представлено на рис. 3 у вигляді розробленого керуючого алгоритму антикризового управління ІБ ОКІ, що базується на чинних нормативно-правових документах України, зокрема постановах Кабінету Міністрів України, нормативних актах Національного банку України та державних стандартах (ДСТУ), і орієнтований на функціонування в умовах воєнного стану.

Розроблений керуючий алгоритм антикризового управління ІБ ОКІ в умовах правового режиму воєнного стану має ієрархічну поетапну структуру та реалізується у вигляді послідовності взаємопов'язаних етапів, що забезпечують системний підхід до ідентифікації загроз, моделювання їх впливу та вибору ефективних управлінських рішень.

На першому етапі здійснюється ідентифікація ОКІ та його нормативна класифікація відповідно до чинного законодавства України. На цьому етапі визначається галузева належність об'єкта, рівень його критичності, склад інформаційних активів та вимоги регуляторних органів до забезпечення інформаційної та кібернетичної безпеки.

Другий етап передбачає ідентифікацію та структуризацію загроз, що можуть впливати на ІБ ОКІ в умовах воєнного стану. Загрози класифікуються за основними групами: кібернетичні, інформаційно-психологічні, організаційні, а також фізичні та техногенні. Така структуризація забезпечує повноту охоплення деструктивних факторів та формує основу для подальшого формалізованого аналізу.

На третьому етапі здійснюється побудова когнітивної моделі взаємозв'язків між загрозами, умовами функціонування, інформаційними процесами та наслідками для ОКІ. Формується матриця прямих і сумарних впливів, визначаються ключові концепти та їх роль у системі, а також кількісні характеристики взаємовпливів, що дозволяє перейти до сценарного аналізу.

Рис. 3. Керуючий алгоритм антикризового управління ІБ ОКІ в умовах запровадження правового режиму воєнного стану

Четвертий етап полягає у сценарному моделюванні антикризових ситуацій. На основі когнітивної моделі та матриці впливів аналізуються можливі сценарії розвитку подій, зокрема базові, кризові та критичні сценарії. Для кожного сценарію оцінюється динаміка зміни станів концептів і ступінь загрози ІБ ОКІ.

П'ятий етап передбачає вибір антикризових управлінських впливів. На цьому етапі визначаються найбільш ефективні заходи протидії

загрозам, спрямовані на ключові концепти когнітивної моделі, з урахуванням результатів

Шостий етап включає реалізацію обраних управлінських рішень та організацію безперервного моніторингу стану ІБ. Здійснюється контроль виконання заходів, фіксація інцидентів, збір показників ефективності та актуалізація інформації про поточний стан системи.

Сьомий етап спрямований на оцінювання ефективності впроваджених антикризових заходів та коригування алгоритму управління. На основі отриманих результатів проводиться аналіз досягнення цільових показників, уточнюються параметри когнітивної моделі та сценарії, а також формується зворотний зв'язок для підвищення адаптивності системи в умовах динамічних загроз воєнного часу.

Висновки

1. Удосконалено підхід до аналізу впливу загроз на ІБ ОКІ в умовах воєнного стану на основі когнітивного сценарного моделювання для дослідження інтенсивності кібернетичних, фізичних та гібридних загроз, які мають системний характер та здатні спричиняти каскадні порушення функціонування критично важливих об'єктів. У результаті дослідження сформовано класифікацію ОКІ з позицій інформаційної безпеки, яка враховує функціональне призначення, рівень критичності, характер інформаційних процесів та специфіку загроз у період воєнного стану. Запропонована класифікація створює методичну основу для формалізованого опису об'єктів у межах когнітивних моделей.

2. Побудовано когнітивну модель впливу загроз на ІБ ОКІ у вигляді нечіткої когнітивної карти, що дозволяє враховувати як прямі, так і опосередковані причинно-наслідкові зв'язки між загрозами, умовами воєнного стану, властивостями ІБ та наслідками їх порушення. Визначено множину концептів та виконано їх класифікацію за роллю у моделі. Запропоновано систему системних показників, зокрема показники впливу, чутливості та центральності, що дозволяють ідентифікувати ключові концепти когнітивної моделі та оцінити їх роль у формуванні ризиків для ІБ. Показано, що концепти, пов'язані з доступністю та стійкістю інформаційних систем, мають вирішальне значення для забезпечення стабільного функціонування ОКІ.

3. Розроблено керуючий алгоритм антикризового управління ІБ ОКІ в умовах запровадження правового режиму воєнного стану, який реалізується у вигляді послідовності взаємопов'язаних етапів, що включають ідентифікацію об'єкта та його нормативну сценарного аналізу та обмежень, пов'язаних з ресурсами й нормативними вимогами. класифікацію, структуризацію загроз (кібернетичних, інформаційно-психологічних, організаційних, фізичних і техногенних), побудову когнітивної моделі та матриці сумарних впливів, сценарне моделювання антикризових ситуацій, вибір управлінських впливів, їх реалізацію та моніторинг, а також оцінювання ефективності із подальшим коригуванням прийнятих рішень, що забезпечує адаптивність системи управління ІБ ОКІ в умовах динамічних загроз воєнного часу.

4. На основі отриманих результатів сформульовано практичні рекомендації щодо підвищення ІБ ОКІ, орієнтовані на пріоритезацію захисних заходів, зменшення впливу ключових загроз та підвищення стійкості інформаційних систем. Запропонований підхід може бути використаний як інструмент підтримки прийняття рішень у сфері захисту критичної інфраструктури в умовах воєнного стану. Напрямами подальших досліджень є розширення когнітивної моделі за рахунок кількісних показників ефективності захисних заходів, інтеграція статистичних даних інцидентів ІБ, а також розроблення програмних засобів автоматизованого сценарного аналізу для ОКІ різних секторів.

Література

1. *Про критичну інфраструктуру: Закон України. 16.11.2021. 1882-IX. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#top*
2. *Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. За ред. О.М. Суходолі. Київ. Національний інститут стратегічних досліджень. 2020. 28. [Електронний ресурс]. Режим доступу: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastructury_0.pdf*
3. *Єрменчук О.П. Оцінка загроз критичній інфраструктурі як важлива складова частини діяльності із захисту державної безпеки. Національний юридичний журнал: теорія і практика. 2018. 6. 50–54. [Електронний ресурс]. Режим доступу: http://www.jurnaluljuridic.in.ua/archive/2018/6/part_1/11.pdf*
4. *Про основні засади забезпечення кібербезпеки України: Закон України. 05.10.2017. 2163-VIII. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text*
5. *Про Стратегію кібербезпеки України: Указ Президента України Про рішення Ради національної безпеки і оборони України. 14.05.2021. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text*
6. *Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова кабінету міністрів України. 19.06.2019. 518. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text*
7. *Ruban I., Tiutiunyk V., Zabolotnyi V., Tiutiunyk O. Vulnerability Assessment of Cyber Defense Objects Based on*

a Risk Oriented Approach. Ukrainian Scientific Journal of Information Security. 2020. 26. 3. 145–155. [Електронний ресурс]. Режим доступу: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/14947

8. Яременко О.І., Страхніцький Я.О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. Державне управління: удосконалення та розвиток. 2022. 1. [Електронний ресурс]. Режим доступу: https://www.dy.nayka.com.ua/pdf/1_2022/40.pdf

9. Хаустова В.Є., Трушкіна Н.В. Загрози розвитку критичної інфраструктури: сутність і класифікація. Проблеми економіки. 2025. 3(65). 89–104. [Електронний ресурс]. Режим доступу: https://www.problecon.com/export_pdf/problems-of-economy-2025-3_0-pages-89_104.pdf

10. Салієва О.В., Яремчук Ю.Є. Симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта критичної інфраструктури. Реєстрація, зберігання і обробка даних. 2020. 22. 3. 68–75. [Електронний ресурс]. Режим доступу: http://jnas.nbuv.gov.ua/article/UJRN-0001200603

11. Брежнєв Є.В., Фесенко Г.В., Харченко В.С. Методологічні засади оцінювання та забезпечення безпеки критичних інформаційних інфраструктури. Радіоелектронні і комп'ютерні системи. 2018. 4. 78–85. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/recs_2018_4_10

12. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. Київ. Альфа Реклама. 2019. 176.

13. Євсєєв В.О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць Харківського національного університету Повітряних Сил. 2016. 4. 168–172. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_4_35

14. Кожедуб Ю., Василенко С., Максимець А., Гирда В. Концептуальна модель захисту інформації об'єктів критичної інформаційної інфраструктури України. Information Technology and Security. 2021. 9. 2(17). 151–164. [Електронний ресурс]. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/8046302f-a889-4c0b-9a69-325cd3b0b1ef/content

15. Мурасов Р.К., Мельник Я.В. Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України. Modern Information Technologies in the Sphere of Security and Defence. 2023. 1(46). 41–44. [Електронний ресурс]. Режим доступу: https://sit.nuou.org.ua/article/view/280288/289997

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

17. 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://romisatriawahono.net/lecture/rm/survey/softcomputing/Papageorgiou%20-%20Fuzzy%20Cognitive%20Maps%20Research%20-%202013.pdf

18. Rotshtein A.P., Katielnikov D.I. Fuzzy cognitive map vs regression. Cybernetics and Systems Analysis. 2021. 57(4). 605–616. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/s10559-021-00385-3

19. 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.

20. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України. 09.10.2020. 1109. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

21. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України. 22.07.2022. 821. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

22. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України. 14.10.2022. 1174. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text

23. Про правовий режим воєнного стану: Закон України. 12.05.2015. 389-VIII. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/389-19#Text

24. Тютюник В.В., Тютюник 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

25. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. 1(43). 41–52. [Електронний ресурс]. Режим доступу: http://repositsc.nuczu.edu.ua/handle/123456789/15894

26. Tiutiunyk V., Tiutiunyk O., Teslenko O., Brynza N. Peculiar Properties of Creating a System of Support to Make AntiCrisis 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://repositsc.nuczu.edu.ua/bitstream/123456789/14239/1/DRF_2021_Tiutiunyk_ENG.pdf

References

1. On Critical Infrastructure: Law of Ukraine. 16.11.2021. 1882-IX. Available at: https://zakon.rada.gov.ua/laws/show/1882-20#top

2. State system of protection of critical infrastructure in the system of ensuring national security: analytical supplement. Edited by O.M. Sukhodoly. Kyiv. National Institute for Strategic Studies. 2020. 28. Available at: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastructury_0.pdf

3. *Yermenchuk O.P. Assessment of threats to critical infrastructure as an important component of activities to protect state security. National Legal Journal: Theory and Practice. 2018. 6. 50–54. Available at: http://www.jurnaluljuridic.in.ua/archive/2018/6/part_1/11.pdf*

4. On the Basic Principles of Ensuring Cybersecurity in Ukraine: Law of Ukraine. 05.10.2017. 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine On the Decision of the National Security and Defense Council of Ukraine. 05/14/2021. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text

6. On approval of General requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine. 06/19/2019. 518. Available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

7. Ruban I., Tiutiunyk V., Zabolotnyi V., Tiutiunyk O. Vulnerability Assessment of Cyber Defense Objects Based on a Risk Oriented Approach. Ukrainian Scientific Journal of Information Security. 2020. 26. 3. 145–155. Available at: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/14947

8. Yaremenko O.I., Strahnitsky Ya.O. Theoretical and methodological foundations of ensuring the system of protection of critical infrastructure of the state. Public administration: improvement and development. 2022. 1. Available at: https://www.dy.nayka.com.ua/pdf/1_2022/40.pdf

9. Khaustova V.E., Trushkina N.V. Threats to the development of critical infrastructure: essence and classification. Problems of economy. 2025. 3(65). 89–104. Available at: https://www.problecon.com/export_pdf/problems-of-economy-2025-3_0-pages-89_104.pdf

10. Salieva O.V., Yaremchuk Y.E. Simplistic analysis of the structure of a cognitive model for studying the security of a critical infrastructure object. Data registration, storage and processing. 2020. 22. 3. 68–75. Available at: http://jnas.nbuv.gov.ua/article/UJRN-0001200603

11. Brezhnev E.V., Fesenko G.V., Kharchenko V.S. Methodological principles of assessing and ensuring the security of critical information infrastructure. Radioelectronic and computer systems. 2018. 4. 78–85. Available at: http://nbuv.gov.ua/UJRN/recs_2018_4_10

12. Honchar S.F. Assessing cybersecurity risks of information systems of critical infrastructure facilities: monograph. Kyiv. Alfa Reklama. 2019. 176.

13. Yevseyev V.O. Possible ways to improve the protection of critical infrastructure of Ukraine taking into account world experience. Collection of scientific papers of the Kharkiv National University of the Air Force. 2016. 4. 168–172. Available at: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_4_35

14. Kozhedub Yu., Vasylenko S., Maksymets A., Hyrda V. Conceptual model of information protection of critical information infrastructure objects of Ukraine. Information Technology and Security. 2021. 9. 2(17). 151–164. Available at: https://ela.kpi.ua/server/api/core/bitstreams/8046302f-a889-4c0b-9a69-325cd3b0b1ef/content

15. Murasov R.K., Melnyk Ya.V. Assessment of cyberspace security of critical infrastructure facilities of Ukraine. Modern Information Technologies in the Sphere of Security and Defence. 2023. 1(46). 41–44. Available at: https://sit.nuou.org.ua/article/view/280288/289997

16. Milyavskyi Y.L. Cognitive modeling of complex systems. Design and analysis of cognitive models. Kyiv. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". 2025. 39. Available at: https://ela.kpi.ua/server/api/core/bitstreams/3c03af72-c07a-4a10-bc76-4b7e37d9bae8/content

17. 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. Available at: https://romisatriawahono.net/lecture/rm/survey/softcomputing/Papageorgiou%20-%20Fuzzy%20Cognitive%20Maps%20Research%20-%202013.pdf

18. Rotshtein A.P., Katielnikov D.I. Fuzzy cognitive map vs regression. Cybernetics and Systems Analysis. 2021. 57(4). 605–616. Available at: https://doi.org/10.1007/s10559-021-00385-3

19. Sikora L.S., Lysa N.K., Pavlyuk O.M., Sabat V.I., Fedevich O.Yu. Informational and logical-cognitive approaches to the formation of cybersecurity of technogenic infrastructures taking into account the level of risks. Scientific Bulletin of UNFU. 2023. 33. 1. 71–81.

20. Some issues of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine. 09/10/2020. 1109. Available at: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

21. On approval of the Procedure for monitoring the level of security of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine. 07/22/2022. 821. Available at: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

22. On approval of the Regulations on information exchange between entities of the national critical infrastructure protection system: Resolution of the Cabinet of Ministers of Ukraine. 10/14/2022. 1174. Available at: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text

23. On the legal regime of martial law: Law of Ukraine. 12.05.2015. 389-VIII. Available at: https://zakon.rada.gov.ua/laws/show/389-19#Text

24. Tiutiunyk V.V., Tiutiunyk O.O., Usachov D.V. Peculiarities of using fuzzy cognitive maps for scenario modeling of critical infrastructure functioning in conditions of military emergencies. Modern Information Technologies in the Sphere of Security and Defence. 2025. 3(54). 93–102. Available at: https://sit.nuou.org.ua/article/view/338904

25. Tiutiunyk V.V., Yashchenko O.A., Ruban I.V., Tiutiunyk O.O. Features of the functioning of the system of situational centers at different stages of the development of emergency situations. Modern information technologies in the field of security and defense. 2022. 1(43). 41–52. Available at: http://repositsc.nuczu.edu.ua/handle/123456789/15894

26. Tiutiunyk V., Tiutiunyk O., Teslenko O., Brynza N. Peculiar Properties of Creating a System of Support to Make AntiCrisis 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. Available at: http://repositsc.nuczu.edu.ua/bitstream/123456789/14239/1/DRF_2021_Tiutiunyk_ENG.pdf

Рецензент: член-кореспондент Національної академії наук України, доктор технічних наук, професор, ПОПОВ Олександр Олександрович, директор Центру інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України

Автор: ТЮТЮНИК Вадим Володимирович
доктор технічних наук, професор
Харківський національний економічний університет імені Семена Кузнеця
Харківський національний університет радіоелектроніки
E-mail – tutunik_v@ukr.net
ID ORCID: https://orcid.org/0000-0001-5394-6367

Автор: ТЮТЮНИК Ольга Олександрівна
кандидат технічних наук, доцент
Харківський національний економічний університет імені Семена Кузнеця
E-mail – olha.tiutiunyk@hneu.net
ID ORCID: https://orcid.org/0000-0002-3330-8920

SCENARIO-BASED COGNITIVE MODELING OF THE IMPACT OF THREATS ON THE INFORMATION SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES UNDER THE INTRODUCTION OF THE LEGAL REGIME OF MARTIAL LAW

V. Tiutiunyk [1,2], O. Tiutiunyk [1]
[1] Simon Kuznets Kharkiv National University of Economics
[2] Kharkiv National University of Radio Electronics

Considering the growing intensity and complexity of threats to the information security of critical infrastructure facilities under martial law, as well as the need to account for nonlinear cause-and-effect relationships and the scenario-based nature of their development, the article develops and investigates a cognitive model of threat impact scenarios on the information security of critical infrastructure facilities. The proposed approach is aimed at supporting managerial decision-making in the field of crisis management of information security under the legal regime of martial law.

The approach to analyzing the impact of threats on the information security of critical infrastructure facilities under martial law has been improved based on cognitive scenario modeling, which enables the study of the intensity of cyber, physical, and hybrid threats that have a systemic nature and are capable of causing cascading disruptions in the functioning of critically important facilities. As a result of the study, a classification of critical infrastructure facilities from the perspective of information security has been developed, taking into account their functional purpose, level of criticality, nature of information processes, and the specific characteristics of threats during martial law. The proposed classification provides a methodological basis for the formalized description of facilities within cognitive models and enhances the validity of scenario-based analysis.

A cognitive model of the impact of threats on the information security of critical infrastructure facilities has been developed in the form of a fuzzy cognitive map, which makes it possible to account for both direct and indirect cause-and-effect relationships between threats, martial law conditions, information security properties, and the consequences of their violation. The set of model concepts has been defined and their classification according to functional roles within the system has been carried out. A system of systemic indicators has been proposed, including indicators of influence, sensitivity, and centrality, which enable the identification of key concepts of the cognitive model and the assessment of their role in the formation of information security risks. It has been shown that concepts related to the availability and resilience of information systems are of decisive importance for ensuring the stable functioning of critical infrastructure facilities.

A control algorithm for crisis management of information security of critical infrastructure facilities under the legal regime of martial law has been developed, implemented as a sequence of interrelated stages. The algorithm includes identification of the facility and its regulatory classification; structuring of threats (cyber, information-psychological, organizational, physical, and technogenic); construction of a cognitive model and a matrix of cumulative influences; scenario-based modeling of crisis situations; selection and implementation of control actions; monitoring of the information security state; and evaluation of effectiveness with subsequent adjustment of decisions made. The proposed algorithm ensures the adaptability of the information security management system of critical infrastructure facilities under dynamic wartime threats.

Keywords: *information security; critical infrastructure objects; cognitive modeling; scenario modeling; martial law; information security threats; crisis management.*

Дата надходження статті: 18.01.2026
Дата прийняття до друку: 15.03.2026
Дата публікації статті: 23.03.2026

Автори заявляють про відсутність конфлікту інтересів.