ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СЦЕНАРНОГО КОГНІТИВНОГО МОДЕЛЮВАННЯ ДЛЯ АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Тютюник В. В.[1,2], Тютюник О. О.[1]
[1]Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
[2]Харківський національний університет радіоелектроніки, Харків, України

У сучасних наукових дослідженнях значна увага приділяється проблемам захисту критичної інфраструктури (КІ), забезпечення кібербезпеки та управління ризиками. Водночас недостатньо розробленими залишаються підходи, що дозволяють комплексно враховувати взаємозалежність загроз, динаміку їх розвитку та сценарний характер впливу на інформаційну безпеку (ІБ) в умовах воєнного стану. Це обумовлює необхідність застосування методів, здатних адекватно відображати складні причинно-наслідкові зв'язки в системах із високим рівнем невизначеності. Одним із таких інструментів є когнітивне моделювання, зокрема апарат нечітких когнітивних карт (НКК), який забезпечує формалізоване представлення взаємодії факторів впливу та дозволяє здійснювати сценарний аналіз розвитку загроз [1].

Метою доповіді є дослідження та розроблення підходу до сценарного моделювання впливу загроз на ІБ об'єктів критичної інфраструктури (ОКІ) із застосуванням НКК.

У доповіді наведено результати дослідження та розроблення підходу до сценарного моделювання впливу загроз на ІБ КІ з використанням НКК. Так, 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 [3].

В роботі когнітивну модель подано на рис. 1 у вигляді орієнтованого зваженого графа: $G = \langle C, E, W \rangle$, 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, $w_{ij} \in [-1;1]$.

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): $C_D = \{c_1, c_2, c_3, c_4, c_5\}$, 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.

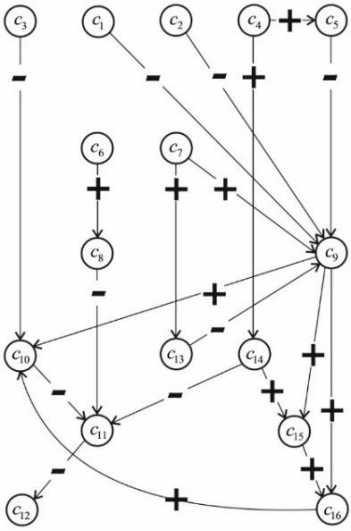

Рис. 1. Когнітивна модель сценарного впливу загроз на ІБ ОКІ в умовах запровадження правового режиму воєнного стану

Друга група – концепти умов воєнного стану (Ordinary-concepts): $C_W = \{c_6, c_7, c_8, c_9\}$ 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): $C_{IB} = \{c_{10}, c_{11}, c_{12}, c_{13}\}$, де c_{10} – конфіденційність інформації, c_{11} – цілісність інформації, c_{12} – доступність інформації, c_{13} – стійкість інформаційних систем.

Четверта група – концепти наслідків (Receiver-concepts): $C_R = \{c_{14}, c_{15}, c_{16}\}$, де c_{14} – порушення функціонування ОКІ, c_{15} – соціально-економічні збитки, c_{16} – зниження рівня національної безпеки.

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 [4, 5]. Крім того, когнітивна модель може використовуватися як інструмент підтримки прийняття рішень для оцінювання ефективності різних стратегій забезпечення ІБ ОКІ [6, 7].

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.

Список літератури

1. 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

2. 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

3. Тютюник В.В., Тютюник О.О. Сценарне когнітивне моделювання впливу загроз на інформаційну безпеку об'єктів критичної інфраструктури в умовах запровадження правового режиму воєнного стану. *Комунальне господарство міст. Серія: Інформаційні технології та інженерія*. 2026. Т. 1. Вип. 196. С. 22–33. DOI: https://doi.org/10.33042/3083-6727-2026-1-196-22-33

4. 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. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-41-52