

ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Запропоновано когнітивну модель, яка дозволяє оцінити рівень захищеності об'єкта критичної інфраструктури. Здійснено структурно-топологічний аналіз даної моделі та визначено найвагоміші її концепти. Проведено сценарне моделювання впливу даних концептів на захищеність об'єкта критичної інфраструктури.

Summary. A cognitive model has been proposed to assess the level of protection of a critical infrastructure object. The structural-topological analysis of this model is carried out and its most important concepts are defined. Scenario modeling of the impact of these concepts on the security of critical infrastructure is performed.

Ключові слова: інформаційна безпека, критична інфраструктура, когнітивне моделювання.

Одним із найважливіших пріоритетів держави є захист об'єктів критичної інфраструктури (КІ), виведення з ладу або руйнування яких може мати негативний вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв. У зв'язку із цим варто звернути увагу на забезпечення безпеки об'єктів КІ при впливі на них ймовірних загроз. Причому дана задача характеризується високим ступенем невизначеності, складністю строгої формалізації та має суб'єктивний характер. Тому для її вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечіткої когнітивної карти (НКК).

Враховуючи актуальність досліджуваної проблеми, запропоновано когнітивну модель для оцінювання рівня захищеності об'єкта критичної інфраструктури, який відноситься до класу об'єктів, що передбачає доступ до мережі Інтернет та відображає максимальне представлення структурних складових.

Для побудови когнітивної моделі було визначено експертним шляхом структуру НКК предметної області, тобто склад її концептів, причинно-наслідкові зв'язки між ними та силу впливу між кожною парою концептів.

Встановлено структурно-топологічні властивості розробленої НКК, проаналізовано такі показники структурної складності як

щільність (коефіцієнт кластеризації), індекс ієрархії та центральність концептів. Так, отримане значення щільності НКК ($d = 0,18$), свідчить про достатню складність розробленої моделі, а значення індексу ієрархії ($h = 0,16$) відображає високу демократичність досліджуваної системи.

Розрахунок показників центральності показав, що найбільш високу структурну значимість мають концепти: «Інсайдерський вплив» ($td = 11,6$), «Захищеність комп'ютерної мережі» ($td = 9,2$) та «Захищеність системи безпеки» ($td = 8,39$). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу у досліджуваній НКК.

Максимально посилюючи негативний вплив кожного з найвагоміших концептів окремо, здійснено моделювання сценаріїв, у результаті запуску яких, відображається відносна зміна захищеності об'єкта КІ. Зокрема, при посиленні інсайдерського впливу, зниженні захищеності комп'ютерної мережі та системи безпеки спостерігатиметься послаблення захищеності КІ відповідно на 0,03; 0,06 та 0,44 відносні одиниці. Проведене сценарне моделювання дозволяє отримати прогноз розвитку досліджуваної ситуації, проаналізувавши вплив найвагоміших концептів НКК на захищеність КІ.

Розроблена когнітивна модель є гнучкою та легко адаптується до змін за рахунок введення нових концептів та встановлення зв'язків між ними.

Висновки. Таким чином, використовуючи когнітивний підхід, розроблено модель для оцінювання рівня захищеності об'єкта КІ. Проведено структурно-топологічний аналіз побудованої НКК, який свідчить про її достатню складність та високу демократичність, тобто адаптивність до змін зовнішнього середовища. Крім того, визначено найвагоміші концепти досліджуваної системи та проведено сценарне моделювання в результаті якого визначено відносну зміну рівня захищеності об'єкта КІ.

Отримані дані сприятимуть прогнозуванню розвитку конкретних ситуацій, необхідному для вчасного прийняття управлінських рішень щодо підвищення рівня захищеності досліджуваного об'єкта, порушення функціонування якого може призвести до розвитку надзвичайних ситуацій, здатних паралізувати життєдіяльність як окремих міст, так і усєї держави в цілому.

