НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 24

Київ – 2024

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 19 від 24 грудня 2024 р.)

Інформаційні технології та безпека. Матеріали XXIV Міжнародної науково-практичної конференції ІТБ-2024. – Київ: Інжиніринг. – 202 с. ISBN: 978-617-8180-00-3

До збірника увійшли матеріали доповідей, представлених на XXIII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2024, 19 грудня 2024 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпеки та живучості критичних інфраструктур, технологіям штучного інтелекту; розробки та застосування аналітичних систем на основі відкритих джерел інформації, комп'ютерного моделювання складних систем, аналізу та прогнозування процесів мережевої взаємодії; створення сучасних інтелектуальних технології підтримки прийняття рішень.

Для фахівців в області комп'ютерних наук, інформаційних технологій, інформаційної і кібернетичної безпеки, захисту інформації, а також для здобувачів освіти вищої школи відповідних спеціальностей.

ISBN 978-617-8180-00-3

ТЕНЗОРНА МОДЕЛЬ ПРЕДСТАВЛЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ярослав Дорогий[1], Владислав Кравчук[2], Василь Цуркан[3]
[1] *Донецький національний технічний університет, cisco.rna@gmail.com, 0000-0003-3848-9852*
[2] *Донецький національний технічний університет, vladkrava15@ukr.net, 0009-0000-7929-6796*
[3] *Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, v.v.tsurkan@gmail.com, 0000-0003-1352-042X*

У роботі розглядається тензорна модель для опису критичної інфраструктури, яка дозволяє аналізувати багатовимірні залежності між компонентами системи, їх характеристиками, взаємозв'язками та ризиками. Запропонована модель використовує тензори для представлення атрибутів компонентів, функціональних взаємодій та загроз, забезпечуючи системний підхід до аналізу та прогнозування поведінки інфраструктури. Особлива увага приділяється математичним методам, таким як розклади тензорів і оптимізація ризиків, що дозволяють ідентифікувати вразливості системи та розробляти стратегії захисту. Наведені математичні вирази деталізують запропоновану модель, а також її застосування для підвищення стійкості та ефективності функціонування КІ.

Ключові слова: тензорна модель, критична інфраструктура, багатовимірний аналіз, оптимізація ризиків, розклад тензорів, система захисту, оцінка вразливості.

Вступ

Тензорний підхід до моделювання критичної інфраструктури (КІ) забезпечує ефективний засіб для багатовимірного аналізу складних систем. Критична інфраструктура [1] охоплює різні підсистеми, включаючи енергетичний сектор, транспортні мережі, інформаційно-комунікаційні технології, систему охорони здоров'я та фінансові послуги, які характеризуються складними взаємозв'язками як між собою, так і з зовнішнім середовищем.

Завдяки тензорній моделі можливо врахувати численні взаємозв'язки між елементами системи $C = \{C_1, C_2, \dots, C_n\}$, їх характеристиками $A = \{A_1, A_2, \dots, A_m\}$ та зовнішніми впливами $P = \{P_1, P_2, \dots, P_p\}$, що забезпечує більш точний аналіз та прогнозування.

Основи тензорного представлення критичної інфраструктури

Тензорна модель дозволяє подати дані про КІ у вигляді багатовимірної структури $T \in R^{n \times m \times p}$, де кожен вимір відповідає конкретному аспекту системи. Елементи критичної інфраструктури $C_i \in C$, такі як електростанції, транспортні вузли чи дата-центри, представляються у вигляді множини компонентів. Їхні характеристики $A_j \in A$, наприклад, потужність, рівень загроз чи продуктивність, моделюються через набір атрибутів. У тривимірному тензорі кожен елемент відображає стан конкретної компоненти у визначений момент часу або у певному просторовому контексті. Наприклад, компонента тензора $T(i, j, k)$ відображає стан j-го атрибута i-го елемента у k-й точці часу або просторі.

Для аналізу взаємозв'язків між компонентами системи вводиться додатковий тензор взаємодії $R \in R^{n \times n \times q}$, де q — типи взаємозв'язків. Наприклад, $R(i, j, k)$ представляє взаємодію між елементами C_i і C_j через k-й канал зв'язку (енергетичний, інформаційний чи транспортний), що моделює функціональні зв'язки, такі як енергетичний обмін, інформаційні потоки чи транспортна доступність. Такий підхід дозволяє ідентифікувати, як одна частина системи впливає на інші в реальному часі. Крім того, врахування множини загроз за допомогою спеціалізованого тензора ризиків створює умови для моделювання впливу негативних факторів, таких як кібератаки, природні катастрофи чи техногенні аварії. Загрози моделюються через тензор ризиків $\Theta \in R^{n \times m \times l}$, де l — типи загроз. Значення $\Theta(i, j, k)$ описує ризик для j-го атрибута i-го компонента через k-й тип загрози.

Загальна модель описується як функція (1):

$$T = f(C, A, P, R, \Theta), \tag{1}$$

де f – оператор, що відображає взаємодію між компонентами, атрибутами, просторово-часовими координатами, типами взаємозв'язків та ризиками.

Функціональні можливості моделі

Однією з ключових переваг тензорної моделі є можливість глибокого аналізу залежностей у КІ. Використовуючи розклади тензорів такі як розклад Такера [2] або CP-розклад [3], можна виділити основні взаємозв'язки між компонентами та атрибутами, визначити приховані залежності та кластери, а також ідентифікувати найуразливіші елементи системи.

Наприклад, для розкладу Такера маємо (2):

$$T \approx G \times_1 U^{(1)} \times_2 U^{(2)} \times_3 U^{(3)}, \qquad (2)$$

де G — ядро, $U^{(1)}, U^{(2)}, U^{(3)}$ — матриці факторів для різних вимірів.

Для оцінки загроз використовується тензорне множення початкового тензора характеристик T із тензором ризиків Θ (3):

$$T' = T \odot \Theta, \qquad (3)$$

де T'(i, j, k) відображає вплив ризиків на відповідні характеристики.

Модель дозволяє прогнозувати поведінку системи під впливом різних факторів, таких як зміна навантаження, атаки чи збої, шляхом моделювання змін у відповідних тензорах.

Зокрема, операції над тензорами дають змогу оцінити потенційний вплив загроз або оптимізувати ресурси для зменшення ризиків.

Практичне застосування тензорної моделі

Тензорний підхід до моделювання критичної інфраструктури може бути використаний у різних сценаріях. Він забезпечує ефективний інструмент для аналізу вразливості системи, виявляючи компоненти з найбільшим рівнем ризику. Наприклад, модель дозволяє оцінювати вразливість системи через максимальні ризики (4):

$$R_{\max} = \max_{i,j,k} \Theta\,(i, j, k). \qquad (4)$$

Модель також дозволяє прогнозувати ефекти загроз, що виникають, і оцінювати їхній вплив на функціонування системи. Наприклад, у разі виявлення потенційної кібератаки можна оцінити її вплив на інформаційні системи, транспортні вузли та енергетичні ресурси. Прогнозування впливу загроз здійснюється

через оцінку змін компонентів системи, наприклад, обчислюючи відхилення (5):

$$\Delta T(i,j,k) = T'(i,j,k) - T(i,j,k). \quad (5)$$

Крім того, тензорний підхід корисний для оптимізації процесів у КІ. Завдяки багатовимірній структурі моделі можливо визначити, які ресурси та дії необхідно перерозподілити для мінімізації негативних наслідків загроз або для забезпечення сталого функціонування системи в умовах кризових ситуацій. Для оптимізації ресурсів використовуються критерії мінімізації сукупного ризику (6):

$$\text{Min} \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} \Theta(i,j,k). \quad (6)$$

Висновки

Тензорна модель є потужним інструментом для аналізу, прогнозування та оптимізації критичної інфраструктури. Вона забезпечує системний підхід до вивчення взаємозв'язків у багатовимірному просторі, враховуючи не лише характеристики компонентів, але й їхню взаємодію, ризики та зовнішні впливи. Застосування такого підходу сприяє підвищенню стійкості та ефективності функціонування КІ, особливо в умовах загрозливого середовища та високого рівня взаємозалежності між її компонентами.

[1] Я. Ю. Дорогий, В. В. Мохор, І. О. Козлюк, В. В. Цуркан, "Критична інфраструктура: вразливості, загрози, ризики," Тези доповідей. ІІ міжнародна науково-практична конференція «Інформаційні технології та взаємодії», Kyiv, pp. 46-47, 2015.

[2] F. Stolf and A. Canale, "Bayesian Adaptive Tucker Decompositions for Tensor Factorization," 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2411.10218.

[3] T. G. Kolda and B. W. Bader, "Tensor Decompositions and Applications," SIAM Review, vol. 51, no. 3, pp. 455–500, 2009. [Online]. Available: https://doi.org/10.1137/07070111X.