НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2025»

Збірник матеріалів конференції
26 березня 2025 р.

Київ – 2025

УДК 620.9 + 349 + 004 + 003.26

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол № 3 від 27.03.2025)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Відповідальний за випуск:
В.О. Артемчук

Usage of blockchain technologies in energetics – 2025: collection of materials of the scientific and practical conference, Kyiv, March 26, 2025, PIMEE of NAS of Ukraine. - 2025. - 84 p.

Використання блокчейн технологій в енергетиці – 2025 : збірник матеріалів науково-практичної конференції, м. Київ, 26 березня 2025 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 84 с.

ЗМІСТ

Я.Ю. Дорогий, В.В. Цуркан, В.С. Кравчук

ТЕНЗОРНА МОДЕЛЬ ОЦІНКИ РЕЗУЛЬТАТИВНОСТІ ПЕНТЕСТУ НА РІЗНИХ ЕТАПАХ РОЗГОРТАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті пропонується тензорна модель для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Модель дозволяє оцінити ефективність захисту системи в процесі тестування, налаштування та після розгортання в продуктивному середовищі, що допомагає виявити потенційні слабкі місця на кожному з етапів. Оцінка проводиться за допомогою трьох основних показників: результативності тестів, адаптивності засобів захисту та ефективності захисту. Використання такої моделі дозволяє точніше і комплексно аналізувати стан захисту на різних етапах розгортання інфраструктури.

Вступ. Актуальність використання тензорного аналізу для дослідження критичних інфраструктур обумовлена зростанням складності та взаємозалежності сучасних технологічних систем. Критична інфраструктура, яка охоплює енергетичні мережі, телекомунікації, фінансові та транспортні системи, стає все більш уразливою до кібератак і технічних збоїв. У зв'язку з цим виникає необхідність у нових підходах для комплексного аналізу безпеки таких систем, які дозволяють ефективно оцінити та забезпечити їх надійність і стійкість до загроз. Тензорний аналіз пропонує потужний інструмент для моделювання та аналізу складних взаємозв'язків між елементами критичної інфраструктури, що дозволяє більш точно передбачати можливі вразливості та загрози, що обговорюється в роботі [1].

Застосування тензорного аналізу в контексті пентестінгу критичних інфраструктур дозволяє детально вивчити та візуалізувати залежності між різними компонентами системи, такими як апаратне забезпечення, програмне забезпечення, мережеві ресурси та фізична безпека. Це відкриває нові можливості для виявлення потенційних слабких місць на ранніх етапах розгортання та експлуатації інфраструктури. Тензорні моделі дозволяють обчислювати результативність засобів захисту, їх адаптивність до змін середовища та ефективність у реальному часі, що є критично важливим для оцінки ризиків і мінімізації загроз у складних системах. Такий підхід розглядається у статті [2], де визначаються основні параметри та характеристики тензорного аналізу для пентестів.

Модель, запропонована в цій статті, спрямована на розширення можливостей тензорного аналізу для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Оцінка результативності пентесту проводиться з урахуванням ключових аспектів тестування на різних етапах, що дозволяє більш ефективно виявляти уразливості, оцінювати їх вплив на загальну безпеку та підвищувати стійкість інфраструктур до зовнішніх і внутрішніх загроз. Подібні сценарії

дослідження та оцінки результативності пентесту розглядаються в роботі [3], де детально аналізуються різні стратегії застосування тензорних моделей для оцінки ефективності захисту критичної інфраструктури.

Модель оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Оцінка результативності пентесту на різних етапах розгортання критичної інфраструктури є важливою для визначення слабких місць в системі безпеки та забезпечення надійності інфраструктури. Математична модель оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури може враховувати такі фактори, як кількість виявлених уразливостей, час на їх усунення, рівень їх критичності, а також вартість потенційного збитку від кожної вразливості.

Нехай визначено наступні тензори:

1. Тензор результативності тестів S: $S_{i,j,k,l}$ вказує на результативність тестів на кожному етапі розгортання інфраструктури, наприклад, на етапі тестування, налаштування або після розгортання в продуктивному середовищі. Даний тензор може відображати рівень виявлених уразливостей або кількість вдало проведених тестів. Нехай $S_{i,j,k,l}$ визначає результативність тестів на етапі i для компонента j з уразливістю k на етапі l.

2. Тензор адаптивності засобів захисту A: $A_{i,j,k,l}$ відображає адаптивність засобів захисту на різних етапах розгортання. Тензор визначає, наскільки ефективно система може реагувати на нові або змінювані уразливості на кожному з етапів. Нехай $A_{i,j,k,l}$ визначає адаптивність засобів захисту на етапі i для компонента j з уразливістю k на етапі l.

3. Тензор ефективності захисту R: $R_{i,j,k,l}$ оцінює ефективність захисту на кожному етапі та для кожної уразливості. Він також допомагає виявити найбільш вразливі етапи в процесі пентесту, тобто ті етапи, де захист є найбільш слабким. Нехай тоді $R_{i,j,k,l}$ відображає ефективність захисту на етапі i для компонента j з уразливістю k на етапі l.

Індекси тензорів визначають наступне:

- i – етапи розгортання інфраструктури, наприклад:
  - $i = 1$ – тестування,
  - $i = 2$ – налаштування,
  - $i = 3$ – продуктивне середовище.
- j – компоненти критичної інфраструктури, такі як сервери, мережі, бази даних, операційні системи тощо.
- k – типи уразливостей для кожного компонента.
- l – етапи пентесту, наприклад:
  - $l = 1$ – попереднє тестування,
  - $l = 2$ – тестування в умовах атаки,
  - $l = 3$ – тестування після атаки.

Опишемо математичну модель на базі введених позначень.

Для кожного етапу i, результативність тестів для компонентів критичної інфраструктури можна виразити наступним чином (1):

$$S_i = \frac{\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} S_{i,j,k,l}}{M \cdot L}, \quad (1)$$

де:

$S_{i,j,k,l}$ – результативність тестів для компонента j на етапі i для уразливості k на етапі l,

M – кількість компонент критичної інфраструктури,

L – кількість видів уразливостей.

Адаптивність засобів захисту на етапі i для кожного компонента j з уразливістю k можна оцінити так (2):

$$A_i = \frac{\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} A_{i,j,k,l}}{M \cdot L}, \quad (2)$$

де $A_{i,j,k,l}$ – адаптивність засобів захисту для компонента j на етапі i.

Ефективність захисту на кожному етапі i можна оцінити наступним чином (3):

$$R_i = \sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} R_{i,j,k,l}, \quad (3)$$

де $R_{i,j,k,l}$ – ефективність захисту для компонента j на етапі i.

Загальна результативність пентесту по всіх етапах розгортання критичної інфраструктури можна отримати як середнє значення результативності для кожного етапу (4):

$$E_{\text{total}} = \frac{1}{N}\sum_{i=1}^{N} S_i\,, \quad (4)$$

де N – кількість етапів розгортання.

Потенційний збиток від усіх уразливостей розгорнутої критичної інфраструктури можна оцінити через (5):

$$C_{\text{damage}} = \sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} R_{i,j,k,l} \cdot D_{i,j,k,l}, \quad (5)$$

де

$D_{i,j,k,l}$ – потенційний збиток від експлуатації уразливості для компонента j на етапі i.

Представлена тензорна модель дозволяє зберігати та обробляти складні взаємозв'язки між різними етапами розгортання критичними інфраструктури, уразливостями та засобами захисту. Врахування таких факторів, як адаптивність засобів захисту та результативність тестів на різних етапах, дозволяє більш точно оцінювати вразливості на кожному етапі розвитку критичної інфраструктури та запобігати потенційним загрозам. Такий підхід дозволяє вчасно виявити слабкі місця і підвищити рівень захисту на кожному з етапів розгортання інфраструктури.

Висновки. У результаті проведеного дослідження тензорного аналізу для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури отримані важливі результати, які можуть значно підвищити ефективність забезпечення безпеки таких систем. Використання тензорних моделей дозволяє враховувати складні взаємозв'язки між різними компонентами інфраструктури, що дає змогу точніше оцінити ефективність засобів захисту на кожному етапі розгортання, починаючи від тестування і налаштування до експлуатації в продуктивному середовищі.

Розроблена модель, яка оцінює результативність пентесту на основі тензорних структур, дозволяє виявляти потенційні уразливості та загрози на різних етапах розвитку системи. Це дає можливість не лише своєчасно коригувати стратегії захисту, а й значно зменшити ймовірність виникнення критичних помилок, які можуть призвести до серйозних збоїв у роботі інфраструктури. Завдяки адаптивним тензорним моделям забезпечується висока ефективність аналізу і надійність системи захисту на всіх етапах її життєвого циклу.

Перспективи подальших досліджень в даному напрямку пов'язані з удосконаленням тензорних моделей для більш детальної оцінки впливу кожного етапу розгортання на загальну безпеку критичної інфраструктури. Крім того, важливим напрямком є інтеграція таких моделей з іншими методами та технологіями, зокрема з машинним навчанням і штучним інтелектом, для забезпечення більш точного прогнозування і своєчасної реакції на нові загрози та вразливості..

1. Дорогий Я.Ю., Цуркан В.В., Кравчук В.С. Тензорна модель представлення критичної інфраструктури / Я.Ю. Дорогий, В.В. Цуркан, В.С. Кравчук // Інформаційні технології та безпека. Матеріали XXIV Міжнародної науково-практичної конференції ІТБ-2024. – Київ: Інжиніринг. – с. 97-100. – doi: 10.5281/zenodo.14592839.

2. Дорогий Я.Ю., Кравчук В.С. Використання тензорного аналізу для задач пентестінгу / Я.Ю. Дорогий, В.С. Кравчук // Сучасний стан та перспективи розвитку науки, освіти і технологій: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 4 січня 2025 р.): у 2 ч. – Кременчук: ЦФЕНД, 2025. – Ч. 2. – с. 62-63. – doi: 10.5281/zenodo.14698727.

3. Дорогий Я.Ю., Кравчук В.С. Сценарії дослідження пентесту на базі тензорних моделей / Я.Ю. Дорогий, В.С. Кравчук // Традиційні та інноваційні підходи до наукових досліджень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції, м. Дрогобич, 31 січня, 2025 р. / Міжнародний центр наукових досліджень. – Вінниця: ТОВ «УКРЛОГОС Груп, 2025. – с. 304-307. – doi: 10.5281/zenodo.14777058.