ЗБІРНИК НАУКОВИХ ПРАЦЬ

З МАТЕРІАЛАМИ VIII МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

31 СІЧНЯ 2025 РІК

М. ДРОГОБИЧ, УКРАЇНА

«ТРАДИЦІЙНІ ТА ІННОВАЦІЙНІ ПІДХОДИ ДО НАУКОВИХ ДОСЛІДЖЕНЬ»

ЗБІРНИК НАУКОВИХ
ПРАЦЬ З МАТЕРІАЛАМИ
VIII МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

ТРАДИЦІЙНІ ТА ІННОВАЦІЙНІ ПІДХОДИ ДО НАУКОВИХ ДОСЛІДЖЕНЬ

31 січня 2025 рік
м. Дрогобич, Україна

Вінниця, Україна
«UKRLOGOS Group»
2025

УДК 082:001
Т 65

Організація, від імені якої випущено видання:
ГО «Міжнародний центр наукових досліджень»
Номер запису організації в Єдиному реєстрі громадських об'єднань: 1499141.

Голова оргкомітету: Сотник С.Г.

Верстка: Білоус Т.В.
Дизайн: Бондаренко І.В.

Рекомендовано до видання Вченою Радою Інституту науково-технічної інтеграції та співпраці. Протокол № 4 від 30.01.2025 року.

*Конференцію зареєстровано Державною науковою установою у сфері управління Міністерства освіти і науки «Український інститут науково-технічної експертизи та інформації» в базі даних науково-технічних заходів України на поточний рік та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (**Посвідчення № 364 від 12.06.2024**).*

*Збірник наукових праць з матеріалами конференції видано офіційно суб'єктом видавничої справи зі **Свідоцтвом ДК № 7860 від 22.06.2023**.*

Т 65 **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. — 562 с.

ISBN 978-617-8440-29-9
DOI 10.62731/mcnd-31.01.2025

Викладено матеріали учасників VIII Міжнародної наукової конференції «Традиційні та інноваційні підходи до наукових досліджень», яка відбулася 31 січня 2025 року у місті Дрогобич.

УДК 082:001

ISBN 978-617-8440-29-9

СЦЕНАРІЇ ДОСЛІДЖЕННЯ ПЕНТЕСТУ НА БАЗІ ТЕНЗОРНИХ МОДЕЛЕЙ

Кравчук Владислав Сергійович
ORCID ID: 0009-0000-7929-6796
аспірант науково-навчального інституту
комп'ютерно-інформаційних технології та автоматизації
ДВНЗ «Донецький національний технічний університет», Україна

Дорогий Ярослав Юрійович
ORCID ID: 0000-0003-3848-9852
д-р. техн. наук, професор, професор кафедри прикладної математики
та інформатики науково-навчального інституту комп'ютерно-
інформаційних технологій та автоматизації
ДВНЗ «Донецький національний технічний університет», Україна

Вступ. Забезпечення кібербезпеки в умовах сучасного інформаційного середовища вимагає комплексного підходу до аналізу ефективності засобів захисту. Одним із ключових інструментів для цього є пентест [1], що дозволяє моделювати різні сценарії атак та оцінювати здатність системи реагувати на потенційні загрози. Використання математичних тензорних моделей [2] забезпечує можливість багатовимірного аналізу, що враховує різні аспекти захищеності системи: типи атак, адаптивність засобів захисту, рівень прав доступу користувачів, етапи розгортання інфраструктури та інтенсивність атак. У рамках дослідження представлено п'ять основних сценаріїв, що дозволяють дослідити ефективність пентесту та побудувати комплексну модель аналізу кібербезпеки.

Розглянемо основні варіанти сценаріїв дослідження пентесту, використовуючи математичну модель тензора результативності пентесту. Для кожного сценарію враховуються різні аспекти пентесту, що відображаються через тензори аналізу сценаріїв та адаптивності засобів захисту.

Сценарій 1. Оцінка ефективності засобів захисту в залежності від різних типів атак. У цьому сценарії можна оцінити, як адаптивність засобів захисту змінюється в залежності від типу атаки. Тензор результативності пентесту тут буде використаний для порівняння

результатів, отриманих під час різних атак, таких як фішинг, DDoS-атаки або атаки через вразливості в програмному забезпеченні.

В даному сценарії тензор:

– $S_{i,j,k,l}$ відображатиме ймовірність успішного виконання атаки в різних сценаріях (наприклад, атака через уразливості на різних рівнях мережі або в програмному забезпеченні).

– $A_{i,j,k,l}$ описуватиме адаптивність засобів захисту до цих атак (як система захисту адаптується до кожного типу атаки).

– $R_{i,j,k,l}$ надасть інформацію про ефективність пентесту для кожної комбінації типу атаки та адаптивності захисту.

Сценарій 2. Оцінка результативності пентесту для різних груп користувачів (захист на рівні прав доступу). В цьому сценарії аналізується, як різні групи користувачів (наприклад, адміністратори, кінцеві користувачі, гості) впливають на рівень безпеки в системах. Тензор результативності пентесту можна використовувати для виявлення слабких місць у захисті в залежності від рівня прав доступу користувачів.

За даним сценарієм:

– $S_{i,j,k,l}$ буде показувати рівень успішності атак на систему для різних категорій користувачів.

– $A_{i,j,k,l}$ оцінюватиме ефективність засобів захисту для кожної групи користувачів.

– $R_{i,j,k,l}$ дозволить оцінити, як рівень прав доступу впливає на захищеність системи та вразливість до атак.

Сценарій 3. Оцінка результативності пентесту на різних етапах розгортання інфраструктури. У цьому сценарії можна оцінити ефективність захисту системи на різних етапах її розгортання, наприклад, під час тестування, в ході налаштування або після розгортання в продуктивному середовищі. Це дозволить виявити можливі слабкі місця в захисті, які можуть бути упущені на певних етапах.

В даному сценарії:

– $S_{i,j,k,l}$ буде вказувати на результативність тестів на кожному етапі (наприклад, під час тестування на етапі налаштування або після розгортання).

– $A_{i,j,k,l}$ де відображати адаптивність засобів захисту на різних етапах розгортання.

– $R_{i,j,k,l}$ допоможе оцінити ефективність захисту та виявити найбільш вразливі етапи в процесі пентесту.

Сценарій 4. Оцінка результативності пентесту після оновлення програмного забезпечення або змін у політиках безпеки. Після оновлення програмного забезпечення або змін у політиках безпеки можна оцінити ефективність пентесту для визначення, як ці зміни впливають на рівень захисту.

В сценарії тензор моделі:

– $S_{i,j,k,l}$ відображатиме рівень вразливості до атак до та після оновлень або змін у політиках.

– $A_{i,j,k,l}$ буде оцінювати адаптивність захисту до нових уразливостей або змін.

– $R_{i,j,k,l}$ дозволить порівняти ефективність захисту до та після змін, що дасть розуміння про покращення чи погіршення результатів пентесту.

Сценарій 5. Оцінка захищеності системи при різних рівнях складності атак (інтенсифікація атак). У цьому сценарії оцінюється, як система реагує на різні рівні складності атак, від простих до складних, що дозволить зрозуміти, наскільки ефективно працює захист при більш інтенсивних і складних атаках.

Для цього:

– $S_{i,j,k,l}$ описуватиме різні рівні складності атак (від простих до складних).

– $A_{i,j,k,l}$ оцінюватиме адаптивність засобів захисту на кожному рівні складності.

– $R_{i,j,k,l}$ дозволить побудувати картину того, як система реагує на різні типи атак та як зміни в складності атак впливають на результативність пентесту.

Кожен з наведених сценаріїв дозволяє досліджувати ефективність пентесту за допомогою тензора результативності, що дозволяє зважити кілька факторів одночасно, таких як тип атаки, адаптивність захисту, рівень прав доступу та етапи розгортання інфраструктури. Тензор результативності забезпечує комплексний підхід до аналізу безпеки системи в різних умовах і дозволяє здійснити більш точну оцінку захищеності.

Висновки. Використання тензорів сприяє аналізу ефективності засобів захисту залежно від типів атак, прав доступу користувачів, етапів розгортання інфраструктури, змін у політиках безпеки та рівня складності атак. Такий багатовимірний підхід дає змогу своєчасно виявляти вразливості, адаптувати засоби захисту та підвищувати загальний рівень кібербезпеки.

Список використаних джерел:

1. Дорогий, Я.Ю., & Кравчук, В. С. (2025). Використання тензорного аналізу для задач пентестінгу. *Сучасний стан та перспективи розвитку науки, освіти і технологій: Збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 4 січня 2025 р.)* (Ч. 2, с. 62–63). Кременчук: ЦФЕНД. https://doi.org/10.5281/zenodo.14698727.
2. Дорогий, Я.Ю., Цуркан, В. В., & Кравчук, В. С. (2024). Тензорна модель представлення критичної інфраструктури. *Інформаційні технології та безпека: Матеріали XXIV Міжнародної науково-практичної конференції ІТБ-2024* (с. 97–100). Київ: Інжиніринг. https://doi.org/10.5281/zenodo.14592839.