УДК 004.056:514.742

Кравчук В.С., аспірант
Дорогий Я.Ю., д.т.н., професор
Донецький національний технічний університет
Цуркан В.В., к.т.н., доцент
КПІ ім. Ігоря Сікорського

КРИТЕРІЙ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Анотація. У цих тезах розглядається підхід до формалізації критерію ефективності захисту критичної інфраструктури шляхом інтеграції практичних метрик тестування на проникнення (MTTD, MTTR, VDR, ROI) у багатовимірну тензорну модель кібербезпеки. Показано, як показники операційного охоплення, технічної ефективності та швидкості реагування математично відображаються на параметри тензорів ресурсів, вразливостей, загроз та засобів захисту. Запропоновано комплексний критерій, який дозволяє не лише оптимізувати технічні параметри захисту, але й оцінити економічну рентабельність інвестицій (ROI) у розрізі зниження загального тензора ризику.

Вступ. Формалізація поняття ефективності кіберзахисту є критично важливою вимогою для сучасних організацій та критичної інфраструктури. Традиційно ефективність оцінюється за допомогою практичних метрик безпеки (таких як рівень виявлення вразливостей, час на усунення тощо). З іншого боку, для системного аналізу складних інфраструктур передові дослідження пропонують використовувати тензорний аналіз, який дозволяє математично описати взаємозв'язки між загрозами, вразливостями та ресурсами [1, 2]. Об'єднання цих двох підходів — перенесення кількісних метрик (KPI) у площину багатовимірних тензорних характеристик — дозволяє створити динамічний, вимірюваний та математично обґрунтований критерій ефективності захисту.

Аналіз літературних джерел. В основі практичної оцінки кібербезпеки лежать стандартизовані методології (PTES, OSSTMM), які формалізують процес виявлення вразливостей. Для вимірювання ефективності цього процесу застосовують метрики швидкості (MTTD, MTTR), метрики технічної ефективності (VDR, рівень хибних спрацьовувань) та показники ROI. Водночас для математичного моделювання безпеки критичної інфраструктури застосовується 4-вимірна тензорна модель [1, 2]. Ця модель оперує тензорами ресурсів (R), загроз (Z), вразливостей (V) та засобів захисту (G), дозволяючи розраховувати результуючий тензор ризику Rr та моделювати

адаптивне зниження загроз у часі [1]. Однак, для набуття практичної цінності, абстрактні параметри цих тензорів потребують наповнення реальними метриками безпеки.

Основна частина. Комплексний критерій ефективності захисту формується через проектування практичних показників ефективності (метрик) на відповідні компоненти тензорної моделі:

1. Метрики охоплення та частоти у тензорі ресурсів (R). Метрика охоплення портфеля (Portfolio Coverage) безпосередньо визначає повноту формування тензора ресурсів Ri,j,k,l [1]. Якщо охоплення під час аналізу чи пентесту становить менше 100%, виникає "сліпа зона", яка генерує неврахований (прихований) тензор ризику. Метрика частоти тестування (Test Cadence) зі свого боку визначає інтервал дискретизації для оновлення матриць стану в системі.

2. Технічна ефективність та достовірність тензора вразливостей (V). Показник рівня виявлення вразливостей (Vulnerability Discovery Rate — VDR) та рівень хибних спрацьовувань (False Positive Rate) виступають індикаторами точності побудови тензора вразливостей Vi,j,k,l, що описує складність та потенційний вплив недоліків [1]. Високий VDR зменшує кількість невідомих елементів тензора V, забезпечуючи об'єктивність моделі. Низький рівень хибних спрацьовувань гарантує, що ймовірність спрацьовування засобів захисту (Pg) з тензора G [1] не буде марно витрачатися на хибні загрози.

3. Метрики швидкості (MTTD, MTTR) у часовій динаміці загрози. Для оцінки часового аспекту ефективності в тензорному аналізі застосовується функція часової динаміки: Zi,j,k,l'(t)= Zi,j,k,le-βt, де — коефіцієнт згасання загрози, а t — час після виявлення [1]. Практичні часові метрики — середній час до виявлення (MTTD) та середній час на усунення (MTTR) — є обернено пропорційними до коефіцієнта beta. Ефективна система захисту забезпечує мінімальні значення MTTD та MTTR, що математично максимізує . Це гарантує швидке експоненційне зниження впливу загрози на систему [1].

4. Економічна ефективність (ROI) у тензорі захисту (G). Тензор засобів захисту Gi,j,k,l містить вимір вартості імплементації інструменту — Cgv [13, 14]. Економічна ефективність захисту розраховується через моделювання рентабельності інвестицій (ROI). У рамках тензорної моделі ROI обчислюється як відношення зниженого потенційного збитку (різниця початкового тензора ризику Rr та залишкового Rr' після застосування засобів захисту G до фінансових витрат Cgv: ROI =fRr- Rr'– CgvCgv, де |Rr| — монетизована оцінка тензора ризику на основі цінності ресурсу Vr з тензора R [1]).

Формалізований критерій ефективності. З урахуванням наведених метрик, глобальний критерій ефективності захисту полягає у такому налаштуванні тензора засобів захисту (G), яке:

1. Мінімізує глобальний тензор ризику [1]:

$$Rr = fIi,j,k,lVi,j,k,lGi,j,k,l$$

2. Максимізує швидкість згасання загрози шляхом системного зменшення метрик MTTD та MTTR.

3. Забезпечує максимальне значення ROI за умови збереження заданого рівня охоплення активів (Portfolio Coverage).

Висновки. Інтеграція практичних метрик тестування на проникнення та реагування на інциденти (VDR, MTTD, MTTR, ROI) в абстрактну тензорну модель перетворює її на потужний аналітичний інструмент. Це дозволяє формалізувати критерій ефективності кіберзахисту не як статичну констатацію наявності захисних систем, а як динамічний процес. Математично ефективність виражається у здатності тензора засобів захисту мінімізувати результуючий тензор ризику з урахуванням швидкості реакції (MTTR) та економічної доцільності (ROI). Такий комплексний критерій забезпечує керівництво організацій дієвими показниками для оптимізації бюджету на кібербезпеку.

Список використаних джерел

1. Dorohyi I., Kravchuk V.S., Tsurkan V.V., Berdychenko I.O. Application of tensor analysis for cybersecurity tasks in critical infrastructure. Інформаційні технології та безпека. Матеріали XXV Міжнародної науково-практичної конференції ІТБ-2025. Київ: Інжиніринг. с. 179-182.

2. Dorohyi I., Kravchuk V., Tsurkan V. Tensor Model for Representing Critical Infrastructure. CEUR Workshop Proceedings. 2024. URL: https://ceur-ws.org/Vol-4068/paper9.pdf (дата звернення: 23.03.2026).