ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП ТА УПРАВЛІННЯ

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції

20-21 листопада 2025 р.

Міністерство освіти і науки України
Вінницький національний технічний університет
Національна академія Державної прикордонної
служби України ім. Богдана Хмельницького
Вінницький національний медичний університет ім. М.І. Пирогова
Державний заклад вищої освіти «Університет менеджменту освіти»
Державний податковий університет
Комунальний заклад вищої освіти “Вінницька академія безперервної освіти”
Сумський обласний інститут післядипломної педагогічної освіти
Інститут комп'ютерних систем і технологій "Індустрія 4.0"
ім. П. Н. Платонова
Університет Бельсько-Бяльський (Польща)
Люблінська політехніка (Польща)

«ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП ТА УПРАВЛІННЯ»

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції
20-21 листопада 2025 р.

Суми/Віннця
НІКО/КЗВО «Вінницька академія безперервної освіти»
2025

УДК 004
ББК 32.97
Е50

Рекомендовано до видання Вченою радою КЗВО «Вінницька академія безперервної освіти» (протокол № 8 від 25.11.2025 р.)

Електронні інформаційні ресурси: створення, використання, доступ та управління. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2025 р. – Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2025. – 420 с.

ISBN 978-617-7422-25-8

Збірник містить матеріали Міжнародної науково-практичної Інтернет конференції «Електронні інформаційні ресурси: створення, використання, доступ та управління. Матеріали збірника подано у авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей. Матеріали відтворюються зі збереженням змісту, орфографії та синтаксису текстів, наданих авторами.

УДК 004
ISBN 978-617-7422-25-8

ДОРОГИЙ ЯРОСЛАВ,
доктор технічних наук, професор,
Донецький національний технічний університет, Дрогобич, Україна
КРАВЧУК ВЛАДИСЛАВ,
аспірант,
Донецький національний технічний університет, Дрогобич, Україна
ЦУРКАН ВАСИЛЬ,
кандидат технічних наук, доцент,
КПІ ім. Ігоря Сікорського, Київ, Україна

ТЕНЗОРНА МОДЕЛЬ ВЗАЄМОДІЇ КОМАНД RED/BLUE/PURPLE

Анотація. У статті представлено тензорну модель симуляції взаємодії команд Red, Blue та Purple у контексті тривалих сценаріїв пентестингу та кіберзахисту критичної інфраструктури. Запропоновано формальну динамічну систему, що відображає вплив атакувальних і захисних дій на стани активів та враховує аналітичну роль команди Purple як посередника у виробленні рекомендаційних політик. Показано, що використання тензорного представлення забезпечує можливість моделювання складних часово-просторових залежностей, зменшує розмірність даних і підтримує навчання в умовах змагального середовища (minimax / adversarial RL). Запропонована модель може бути використана для оцінювання ефективності стратегій

кіберзахисту за допомогою метрик TTD, TTR та Cumulative Impact..
Ключові слова: Red team, Blue team, Purple team, пентестинг, тензорна модель, симуляція атак, кіберзахист, adversarial learning.

Abstract. The paper presents a tensor-based model for simulating the interaction of Red, Blue, and Purple teams in the context of long-term penetration testing and critical infrastructure cybersecurity scenarios. A formal dynamic system is proposed to represent the impact of offensive and defensive actions on asset states while accounting for the analytical role of the Purple team as a mediator in developing recommendation policies. It is shown that the use of tensor representation enables the modeling of complex spatio-temporal dependencies, reduces data dimensionality, and supports learning in a competitive environment (minimax / adversarial RL). The proposed model can be applied to evaluate the effectiveness of cybersecurity strategies using metrics such as TTD, TTR, and Cumulative Impact.
Keywords: Red team, Blue team, Purple team, pentesting, tensor model, attack simulation, cybersecurity, adversarial learning.

Вступ. Розвиток сучасних кіберзагроз характеризується зростанням їхньої складності, тривалістю атакувальних кампаній і мультиагентністю дій. Традиційні методи пентестингу не завжди дозволяють адекватно оцінити поведінку захисних систем у динаміці, особливо в умовах змінного середовища та тривалого часу реагування. Підхід, заснований на взаємодії команд Red, Blue та Purple, орієнтований на створення ітераційного циклу навчання між атакувальною, оборонною та аналітичною складовими.

Моделювання таких процесів у вигляді тензорних систем дає змогу інтегрувати часові, просторові та функціональні зв'язки між об'єктами кіберінфраструктури, підвищити точність прогнозування наслідків атак і оптимізувати симуляцію тривалих сценаріїв (від тижнів до місяців). Такий підхід відкриває можливості для побудови адаптивних систем кіберзахисту, що навчаються у процесі взаємодії між командами різних ролей.

Аналіз літературних джерел. У роботі [1] подано тензорну модель представлення критичної інфраструктури, у якій формалізовано взаємозв'язки між об'єктами, процесами та ризиками у вигляді тривимірного тензора станів. Автори продемонстрували застосування Tucker-розкладів для зменшення розмірності даних та моделювання довготривалих процесів у кіберфізичних системах. Запропонований підхід може бути адаптований для побудови симуляційних моделей взаємодії Red/Blue/Purple команд у контексті кіберзахисту критичної інфраструктури.

Дослідження [2] описує симуляційне середовище CybORG, створене для навчання автономних агентів у сфері кіберзахисту. Це середовище моделює взаємодію команд Red і Blue на основі сценаріїв, що відтворюють реальні кіберінциденти, та дає змогу оцінювати ефективність алгоритмів виявлення й реагування. Автори підкреслюють, що застосування методів reinforcement learning у кібербезпеці потребує чіткої формалізації дій, станів і функцій винагород, а також урахування тривалих часових епізодів під час моделювання.

У роботі [3] представлено оновлену версію цього середовища – CybORG++, яка усуває недоліки попередньої архітектури. Дослідники реалізували розширений набір агентів, зокрема додали Purple-компонент, і запропонували стандартизований набір метрик для оцінювання поведінки системи (Detection Rate, Time-to-Detect, Recovery Time). Робота робить суттєвий внесок у відтворення реалістичних сценаріїв взаємодії команд Red/Blue/Purple та демонструє потенціал симуляційних підходів для тестування стратегій кіберзахисту.

У публікації [4] уперше застосовано концепцію adversarial reinforcement learning для моделювання кіберконфліктів. Запропоновано стохастичну гру між атакувальною та оборонною сторонами, у межах якої кожна сторона навчається оптимальній стратегії дій. Автори встановили, що зі збільшенням кількості змінних (типів активів, варіантів атак, обмежень ресурсів) завдання набуває високої розмірності, тому для зниження складності доцільно застосовувати методи факторизації станів.

І, нарешті, звіт [5] присвячено аналізу впровадження Purple-команд у корпоративних середовищах. Автори доводять, що співпраця між Red і Blue командами через аналітичний шар Purple дозволяє скоротити середній час виявлення інцидентів на 30–40% і підвищити ефективність використання ресурсів центрів моніторингу безпеки (SOC). Це підтверджує доцільність моделювання Purple-компоненти як аналітичного елемента у симуляційних моделях кіберзахисту.

Нарешті, у роботі [5] подано тензорну модель представлення критичної інфраструктури, у якій формалізовано взаємозв'язки між об'єктами, процесами та ризиками у вигляді тривимірного тензора станів. Автори продемонстрували застосування Tucker-розкладів для зменшення розмірності даних та моделювання довготривалих процесів у кіберфізичних системах. Запропонований підхід може бути адаптований для побудови симуляційних моделей взаємодії Red/Blue/Purple команд у контексті кіберзахисту критичної інфраструктури.

Тензорна модель. Нехай модель має наступні параметри:

– T - кількість часових кроків (наприклад, дні або години): $t = 1, \dots, T$.

– N - кількість критичних активів/вузлів (сервери, ПЛК, БД тощо).

– F - кількість описових фіч стану для кожного активу (конфігурація, вразливість, навантаження, доступність тощо).

– P - розмірність простору атак (типи атак/вектори).

– Q - розмірність простору захисних дій / ремедіацій.

– S - розмірність спостережень / телеметрії (лог-події, метрики SIEM, алерти).

І нехай, основні вектори та тензори моделі мають наступний вид:

– станова тензор-матриця: $\mathcal{X} \in R^{T\times N\times F}$, де $\mathcal{X}_{t,i,:}$ - вектор стану активу i у часі t.

– дії червоної команди (атаки): $\mathcal{A}^{\mathcal{R}} \in R^{T\times N\times P}$. $\mathcal{A}^{\mathcal{R}}_{t,i,p}$ - інтенсивність/наявність атаки типу p на актив i в час t.

– дії синьої команди (захист): $\mathcal{A}^{\mathcal{B}} \in R^{T\times N\times Q}$. $\mathcal{A}^{\mathcal{B}}_{t,i,q}$ - захисна дія q (ремедіація, патч, сегментація).

– підтримка аналітики / purple: параметризована функція Φ_θ (тензор-параметри θ) яка транслює спостереження в поради/політики для Blue; її ефективність моделюється коефіцієнтом $\eta_\theta \in [0,1]$.

Спостереження та телеметрія моделі описуються наступний чином:

– $\mathcal{O} \in R^{T\times S}$. $\mathcal{O}_{t,:}$ - агреговані спостереження у час t (лог-події, аномалії).

Модель також передбачає наявність шуму та непередбачуваних факторів Ξ_t.

Далі розглянемо модель взаємолії команд.

Модель взаємодії команд. У запропонованій моделі Red/Blue/Purple взаємодія формалізована як тензорна динамічна система (1):

$$\mathcal{X}_{t+1} = f(\mathcal{X}_t, \mathcal{A}^{\mathcal{R}}_t, \mathcal{A}^{\mathcal{B}}_t) + \Xi_t, \quad (1)$$

де $\mathcal{X}_t$ – стан активів, $\mathcal{A}^{\mathcal{R}}_t$ та $\mathcal{A}^{\mathcal{B}}_t$ - дії атакуючої та захисної сторін відповідно, а Ξ_t – шум або непередбачувані фактори. Purple-команда представлена параметризованою функцією Φ_θ, яка генерує рекомендації для Blue-команди на основі історії спостережень.

Модель підтримує навчання у режимі змагальної оптимізації (2):

$$\min_{\pi^B,\Phi_\theta} \max_{\pi^R} J(\pi^B, \Phi_\theta; \pi^R), \quad (2)$$

де функція втрат включає метрики ефективності кіберзахисту (TTD, TTR, Cumulative Impact).

Застосування тензорних розкладів (Tucker, CP) дає змогу зменшити обчислювальну складність та зберегти структурні зв'язки між часом, активами та характеристиками.

Практична реалізація передбачає симуляцію протягом 12 тижнів для 200 активів і 10 ознак стану кожного, із застосуванням факторизованих політик π_R, π_B та Purple-рекомендацій Φ_θ. Такий підхід дає змогу досліджувати поведінку кіберзахисту на макрорівні, включаючи економічні аспекти, часову реакцію та надійність аналітичних порад.

Висновки. Розроблена тензорна модель взаємодії команд Red/Blue/Purple формує основу для проведення довготривалих симуляцій пентестингових сценаріїв із урахуванням багатовимірних зв'язків між активами, діями та телеметричними даними. Запропонований підхід поєднує математичну строгість ігрових моделей із гнучкістю методів машинного навчання, що дає змогу аналітично оцінювати результативність стратегій кіберзахисту. Подальші дослідження можуть бути зосереджені на адаптації моделі до реальних SOC-даних та автоматизованому навчанні політик Purple-команди.

Список використаних джерел

1. Тензорна модель представлення критичної інфраструктури [Текст] / Я. Ю. Дорогий, В. В. Цуркан, В. С. Кравчук // Тези доповідей XXIV Міжнародної науково-практичної конференції «Інформаційні технології та безпека» (ІТБ-2024). – Київ : Інжиніринг, 2024. – С. 97–100. – DOI: 10.5281/zenodo.14592839.

2. CybORG: A Gym for the Development of Autonomous Cyber Agents [Текст] / M. Standen, M. Lucas, D. Bowman, T. J. Richer, J. Kim, D. Marriott. – arXiv preprint arXiv:2108.09118. – 2021. – Режим доступу: https://arxiv.org/abs/2108.09118.

3.CybORG++: An Enhanced Gym for the Development of Autonomous Cyber Agents [Текст] / H. Emerson, L. Bates, C. Hicks, V. Mavroudis. – arXiv preprint arXiv:2410.16324. – 2024. – Режим доступу: https://arxiv.org/abs/2410.16324.
4. Adversarial Reinforcement Learning in a Cyber Security Simulation [Текст] / R. Elderman, L. J. J. Pater, A. S. Thie, M. M. Drugan, M. A. Wiering // Proceedings of the 9th International Conference on Agents and Artificial Intelligence (ICAART). – 2017. – Режим доступу: https://surl.li/ahdser.
5. IDC MarketScape: Worldwide Incident Readiness Services Assessment [Текст] / Secureworks. – Secureworks Report. – 2021. – Режим доступу: https://surl.li/vqxage.