Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра автоматики і телекомунікацій

Донецький науковий центр НАН України і МОН України

«ТАК»

Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Дрогобич, 18-19 листопада 2025 р.)

Дрогобич
ДВНЗ «ДонНТУ»
2025

УДК 621.39+681+004
Т 15

Рекомендовано до друку Вченою радою ДВНЗ «Донецький національний технічний університет», протокол №12 від 27.11.25

Редакційна колегія:
Вікторія Воропаєва, к.т.н., професор, перший проректор з науково-педагогічної роботи ДонНТУ;
Гліб Ступак, ст. викл. кафедри автоматики і телекомунікацій, керівник мережної академії Cisco ДонНТУ, голова клубу підприємництва YEP!Club DNTU;
Валерій Поцепаєв, к.т.н., доц., завідувач кафедри автоматики і телекомунікацій ДонНТУ;
Наталія Маслова, к.т.н., доц., к.т.н., доцент кафедри прикладної математики і інформатики ДонНТУ;
Сергій Ковальов, к.т.н., доц., в.о. завідувача кафедри електронної техніки і комп'ютерної інженерії ДонНТУ;
Олександр Колларов, к.т.н., доц., завідувач кафедри електричної інженерії ДонНТУ;
Едуард Петелін, к.т.н., доц., директор навчально-наукового інституту комп'ютерно-інформаційних технологій та автоматизації ДонНТУ;
Олена Кучер, к.ф.-м.н., в.о. директора Донецького наукового центру НАН України і МОН України;
Володимир Ставицький, к.т.н., інженер-програміст вбудованих систем, ТОВ «РЗА СИСТЕМЗ»;
Семен Батир, к.т.н., провідний інженер-розробник Ring Ukraine.

Відповідальність за зміст, новизну та оригінальність наданого матеріалу несуть автори.

Т 15 **«ТАК»**: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, Дрогобич, 18-19 листопада 2025р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. – Дрогобич: ДВНЗ «ДонНТУ», 2025. – 142 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрою автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

© ДВНЗ «ДонНТУ», 2025

МОДЕЛЮВАННЯ RED/BLUE/PURPLE КОМАНД ДЛЯ ЗАДАЧ ПЕНТЕСТИНГУ

Дорогий Ярослав Юрійович[1] , доктор технічних наук, доцент,
yaroslav.dorohyi@donntu.edu.ua;
Кравчук Владислав Сергійович[1] , аспірант, vladkrava15@gmail.com
Цуркан Василь Васильович[2] , кандидат технічних наук, доцент,
v.v.tsurkan@gmail.com
[1] Донецький національний технічний університет, Дрогобич, Україна
[2] КПІ ім. Ігоря Сікорського, Київ, Україна

Вступ

Сучасні кіберзагрози характеризуються зростанням складності, тривалістю атакових кампаній та мультиагентністю дій. Традиційні методи пентестингу не завжди дозволяють адекватно оцінити поведінку захисних систем у динаміці. Підхід, заснований на взаємодії Red, Blue та Purple команд, спрямований на створення ітеративного циклу навчання між атакувальною, оборонною та аналітичною складовими. Моделювання таких процесів у вигляді тензорних систем дозволяє інтегрувати часові, просторові та функціональні зв'язки між об'єктами, а також оптимізувати процес симуляції тривалих сценаріїв (від тижнів до місяців).

Аналіз літературних джерел

Дослідження [1] пропонує симуляційне середовище CybORG, розроблене для тренування автономних агентів кіберзахисту. Середовище реалізує взаємодію Red і Blue команд на основі сценаріїв, що імітують реальні атаки, дозволяючи розробникам оцінювати ефективність алгоритмів виявлення та реагування. Автори доводять, що застосування reinforcement learning у кібербезпеці потребує формалізації дій, станів і нагород, а також моделювання тривалих епізодів.

Дослідження [2] презентує оновлену версію середовища – CybORG++, що усуває обмеження попередньої архітектури. Автори впроваджують розширений набір агентів, зокрема Purple-компонент, та описують стандартизований набір метрик для оцінки поведінки системи (Detection Rate, Time-to-Detect, Recovery Time). Робота є важливим кроком до відтворення реалістичних сценаріїв взаємодії Red/Blue/Purple команд і підтверджує ефективність симуляцій як методу тестування стратегій захисту.

У праці [3] вперше застосовано підхід adversarial reinforcement learning для моделювання кіберконфлікту. Пропонується стохастична гра між атакувальною та оборонною сторонами, де кожна з них навчається оптимальній політиці дій. Автори показали, що при збільшенні кількості змінних (кількість активів, типів атак, обмеження ресурсів) проблема стає високовимірною, тому для зменшення складності доцільно використовувати методи факторизації станів.

Дослідження [4] розкриває роль моделювання та симуляції у підтримці

кібероборони. Автори наголошують, що симуляційні системи мають враховувати часову динаміку атак і відновлення систем. Запропонована методика оцінювання кіберстійкості організацій включає врахування латентних періодів виявлення та метрики відновлення.

У звіті [5] проаналізовано впровадження Purple-команд у корпоративних середовищах. Автори доводять, що колаборація між Red і Blue командами через аналітичний шар Purple знижує середній час виявлення інцидентів на 30–40% та оптимізує використання ресурсів SOC. Цей висновок підкреслює практичну значущість моделювання Purple-компоненти як аналітичного модуля в симуляційних середовищах.

Нарешті, у роботі [6] запропоновано тензорну модель представлення критичної інфраструктури. Автори формалізують взаємозв'язки між об'єктами, процесами та ризиками у вигляді тримірного тензора станів і демонструють застосування Tucker-розкладів для зменшення розмірності даних. Запропонована методика дозволяє моделювати довготривалі процеси в кіберфізичних системах і може бути безпосередньо адаптована до симуляцій Red/Blue/Purple сценаріїв.

Модель взаємодії команд

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

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

де $\mathcal{X}_t$ – стан активів, $\mathcal{A}_t^{\mathcal{R}}$ та $\mathcal{A}_t^{\mathcal{B}}$ - 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):

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

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 моделювання Red/Blue/Purple команд створює основу для довготривалих симуляцій пентестингових сценаріїв із урахуванням багатовимірних взаємодій між активами, діями та телемет-

рією. Запропонований підхід об'єднує математичну строгість ігрових моделей і гнучкість машинного навчання, дозволяючи аналітично оцінювати ефективність захисних стратегій. Подальші дослідження можуть бути спрямовані на адаптацію моделі до реальних SOC-даних та автоматизоване навчання політик Purple-команди.

Література

1.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.

2.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.

3. 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.

4. Modeling and Simulation to Support Cyber Defense [Текст] / S. Damodaran, N. Wagner // The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. – 2019. – Vol. 17, Issue 1. – DOI: 10.1177/1548512919856543.

5. IDC MarketScape: Worldwide Incident Readiness Services Assessment [Текст] / Secureworks. – Secureworks Report. – 2021. – Режим доступу: https://surl.li/vqxage.

6. 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.

Анотація

У роботі розглянуто тензорну модель симуляції взаємодії Red, Blue та Purple команд у контексті тривалих сценаріїв пентестингу та кіберзахисту критичної інфраструктури. Запропоновано формальну динамічну систему, що описує вплив атакувальних і захисних дій на стани активів, а також роль аналітичного посередника (Purple team) у рекомендаційних політиках. Показано, що тензорне представлення дозволяє моделювати складні часово-просторові залежності, знижує розмірність даних та підтримує навчання у змагальному середовищі (minimax / adversarial RL). Модель може бути застосована для оцінки ефективності стратегій кіберзахисту через метрики TTD, TTR та Cumulative Impact.

Ключові слова: Red team, Blue team, Purple team, пентестинг, тензорна модель, симуляція атак, кіберзахист, adversarial learning.

Abstract

The paper examines a tensor-based simulation model of the interaction between Red, Blue, and Purple teams in the context of long-term penetration testing and critical infrastructure cybersecurity. A formal dynamic system is proposed to describe the impact of offensive and defensive actions on asset states, as well as the role of the analytical intermediary (Purple team) in recommendation policies. It is shown that the tensor representation makes it possible to model complex spatiotemporal dependencies, reduce data dimensionality, and support learning in an adversarial environment (minimax / adversarial RL). The model can be applied to assess the effectiveness of cybersecurity strategies through such metrics as TTD, TTR, and Cumulative Impact.

Keywords: Red team, Blue team, Purple team, penetration testing, tensor model, attack simulation, cybersecurity, adversarial learning.