INFORMATION PLATFORM "CENTER FOR INNOVATIVE THINKING"
UKRAINIAN INSTITUTE OF SCIENTIFIC STRATEGIES
EUROPEAN UNION RESEARCH DEPARTMENT
SCIENTIFIC AND PUBLISHING CENTER "PROGRESS"

OXFORD 2026:
SCIENCE AND EDUCATION TODAY

PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

JULY 17-19, 2026
OXFORD, UNITED KINGDOM

INFORMATION PLATFORM "CENTER FOR INNOVATIVE THINKING"
UKRAINIAN INSTITUTE OF SCIENTIFIC STRATEGIES
EUROPEAN UNION RESEARCH DEPARTMENT
SCIENTIFIC AND PUBLISHING CENTER "PROGRESS"

OXFORD 2026:
SCIENCE AND EDUCATION TODAY

PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC
AND PRACTICAL CONFERENCE

July 17-19, 2026

Oxford, United Kingdom

This edition was approved for publication on July 31, 2026.

Published in A4 format online on website:
https://naukainfo.com/conference?id=140

Publisher: Sole proprietor Soloviov O. V. Certificate of registration in the State Register of Publishers, Manufacturers, and Distributors of Publishing Products series DK № 8227, dated April 23, 2025.

Oxford, United Kingdom
2026

UDC 001.3-048.35:0/9](06)

Proceedings of the International scientific and practical conference “Oxford 2026: Science and Education Today” (July 17-19, 2026) / Publisher website: www.naukainfo.com. - Oxford, United Kingdom, 2026. - 160 p.

ISBN 978-617-8680-85-5
https://doi.org/10.64828/conf-140-2026

The recommended citation for this publication is:

Shevchenko T. G. Research into the specifics of the development of performing arts in Ukraine under martial law // Oxford 2026: Science and Education Today : proceedings of the International scientific and practical conference (July 17-19, 2026). - Oxford, United Kingdom : naukainfo.com, 2026. - Pp. 15-21. - URL: https://naukainfo.com/conference?id=140

Editor
Soloviov O. V.

M.Sc.Ed., M.P.A., Hon. PhD, Academic Advisor,
Head of the European Union Research Department,
Ukrainian Institute of Scientific Strategies

The collection of scientific articles is a scientific and practical publication that includes research papers by students, postgraduate students, Candidates and Doctors of Sciences, researchers, and practitioners from Ukraine, Europe, neighboring countries, and beyond. The articles reflect studies of processes and changes in the structure of modern science. This collection is intended for students, postgraduate and doctoral candidates, educators, researchers, practitioners, and all those interested in current trends in the development of modern science.

E-mail: journal@naukainfo.com

Publisher website: https://www.naukainfo.com

FIRE AND CIVIL SAFETY

CHEMISTRY, CHEMICAL AND BIOENGINEERING

ECOLOGY AND ENVIRONMENTAL PROTECTION TECHNOLOGIES

INFORMATION TECHNOLOGIES AND SYSTEMS

PHYSICAL AND MATHEMATICAL SCIENCES

PHILOLOGY AND JOURNALISM

PEDAGOGY AND EDUCATION

DOI: https://doi.org/10.64828/conf-140-2026-4
УДК 004.056:004.89

Ланде Дмитро Володимирович
доктор технічних наук, професор
Гончаров Денис Констянтинович
Литвин Микита Романович
студенти
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна

КОГНІТИВНИЙ КІБЕРПОЛІГОН НА ОСНОВІ СЕМАНТИЧНОГО ЦИФРОВОГО ДВІЙНИКА

Анотація. Запропоновано концепцію когнітивного кіберполігону нового покоління, призначеного для підтримки прийняття рішень у сфері кібербезпеки. На відміну від традиційних кіберполігонів, орієнтованих переважно на моделювання заздалегідь визначених сценаріїв атак і навчання персоналу, запропонований підхід забезпечує автоматичне формування альтернативних сценаріїв реагування відповідно до поточного стану інформаційної інфраструктури, актуального інформаційного контексту та поставлених цілей забезпечення безпеки. Архітектура системи інтегрує цифровий опис мережі, орієнтовану семантичну мережу знань, Retrieval-Augmented Generation, великі мовні моделі та багатоагентний аналіз у єдину платформу підтримки прийняття рішень. Запропоновано двосторонній алгоритм побудови контекстної семантичної підмережі, який незалежно виконує пряме розширення від поточного стану системи та зворотне розширення від заданої цілі безпеки. Отримані сценарії оцінюються багатоагентною системою віртуальних експертів на основі великих мовних моделей, що забезпечує їх багатокритеріальне ранжування та пояснення сформованих рекомендацій. Працездатність підходу підтверджено експериментом на тестовій корпоративній мережі.

Ключові слова: когнітивний кіберполігон, семантична мережа, великі мовні моделі, Retrieval-Augmented Generation, багатоагентна система, підтримка прийняття рішень.

Вступ

Стрімке ускладнення сучасної інформаційної інфраструктури, широке впровадження хмарних сервісів, кіберфізичних систем, Інтернету речей та технологій штучного інтелекту супроводжується постійним зростанням кількості й складності кіберзагроз. Багато сучасних атак реалізуються як багатоступеневі кампанії, що використовують численні взаємопов'язані техніки, швидко змінюють тактику та активно спираються на інформацію відкритих джерел.

Традиційні кіберполігони (Cyber Range) успішно використовуються для моделювання інформаційних систем, перевірки засобів захисту та підготовки персоналу [1, 2]. Проте більшість існуючих платформ реалізує лише виконання заздалегідь сформованих сценаріїв. Формування нових сценаріїв реагування, врахування поточного стану мережі, актуальних відомостей про кіберзагрози та нормативних вимог залишаються завданням людини-аналітика. Використання цифрових двійників дозволило істотно підвищити реалістичність таких платформ, наблизивши їх до реальних виробничих інформаційних систем [3]. Завдяки цьому сучасні кіберполігони широко застосовуються для дослідження вразливостей, оцінювання кіберстійкості, навчання персоналу, перевірки процедур реагування та випробування нових засобів захисту.

Одночасно інтенсивно розвиваються великі мовні моделі (LLM) [4], Retrieval-Augmented Generation (RAG) [5], семантичні мережі та графи знань. Проте зазначені технології найчастіше використовуються окремо: графи знань – для представлення інформації, великі мовні моделі – для генерації текстових відповідей, а RAG – для підвищення достовірності відповідей мовних моделей. Їх інтеграція в єдину систему підтримки прийняття рішень досі залишається недостатньо дослідженою.

Метою роботи є розроблення концепції когнітивного кіберполігону, що забезпечує автоматичний синтез, оцінювання та ранжування альтернативних сценаріїв реагування на основі орієнтованих семантичних мереж, двостороннього формування контекстної семантичної мережі, багатоагентного аналізу із застосуванням великих мовних моделей.

Архітектура когнітивного кіберполігону із семантичним цифровим двійником

Запропонований когнітивний кіберполігон розглядається як інтелектуальна система підтримки прийняття рішень, що інтегрує цифровий двійник інформаційної інфраструктури, бази знань про кіберзагрози, механізми Retrieval-Augmented Generation, семантичні мережі та великі мовні моделі.

Функціонування системи починається з формування цифрового опису мережевої інфраструктури, який містить відомості про активи, конфігурацію обладнання, програмне забезпечення, мережеві сервіси, відкриті порти, засоби захисту та відомі вразливості. Одночасно формується інформаційний контекст за рахунок інтеграції даних із відкритих джерел, баз CVE, MITRE ATT&CK, рекомендацій CERT-UA та нормативних документів.

На основі інтегрованих даних будується глобальна орієнтована семантична мережа $G = (V, E)$, де множина вершин описує сутності предметної області (активи, вразливості, техніки атак, механізми захисту, нормативні вимоги, ресурси), а множина орієнтованих ребер відображає причинно-наслідкові, функціональні та технологічні залежності між ними.

Сукупність цифрового опису інформаційної інфраструктури, глобальної семантичної мережі та актуального інформаційного контексту утворює семантичний цифровий двійник інформаційної системи $D_S = (A, G, C)$, де A – цифровий опис активів і конфігурації інформаційної системи, G – глобальна орієнтована семантична мережа предметної області, C – актуальний інформаційний контекст, сформований засобами Retrieval-Augmented Generation. Саме семантичний цифровий двійник є інформаційною основою подальшого автоматичного синтезу альтернативних сценаріїв реагування.

На відміну від традиційних графів атак, побудована мережа використовується не лише як модель представлення знань, а як універсальна когнітивна модель предметної області, що забезпечує подальший синтез альтернативних сценаріїв реагування (Рис. 1).

Контекстна семантична підмережа та багатоагентне оцінювання

Для конкретної задачі підтримки прийняття рішень аналізується не вся глобальна мережа, а лише її контекстна підмережа

$$G_C = \Phi(G, C),$$

де C визначає поточний інформаційний контекст, який включає початковий стан системи, цільовий стан, обмеження та релевантний корпус документів.

Формування контекстної підмережі здійснюється двостороннім алгоритмом. На першому етапі виконується пряме розширення від поточного стану інформаційної системи, тоді як на другому – незалежне зворотне розширення від визначеної цілі безпеки. Після узгодження двох отриманих підмереж формується єдина причинно-наслідкова модель, у якій автоматично визначаються альтернативні маршрути переходу між початковим і цільовим станами.

Отримані маршрути інтерпретуються як альтернативні сценарії реагування.

Подальший аналіз здійснюється багатоагентною системою, побудованою на основі великих мовних моделей. Кожний агент спеціалізується на окремому аспекті аналізу: технічній реалізованості, оцінці кіберризику, ресурсному забезпеченні, відповідності нормативним вимогам, можливості практичного впровадження та повноті процедур реагування.

На відміну від багатьох сучасних застосувань LLM, мовні моделі не використовуються для генерації сценаріїв. Їх функцією є виключно оцінювання вже сформованих альтернатив, пояснення отриманих результатів та інтеграція експертних оцінок.

Загальний процес підтримки прийняття рішень описується композицією трьох операторів

$$D_S \xrightarrow{\Phi} G_C \xrightarrow{\Theta} P \xrightarrow{\Gamma} P^*,$$

де оператор Φ формує контекстну семантичну підмережу, оператор Θ синтезує множину альтернативних сценаріїв P, а оператор Г виконує їх багатоагентне оцінювання та ранжування, формуючи впорядковану множину P^*.

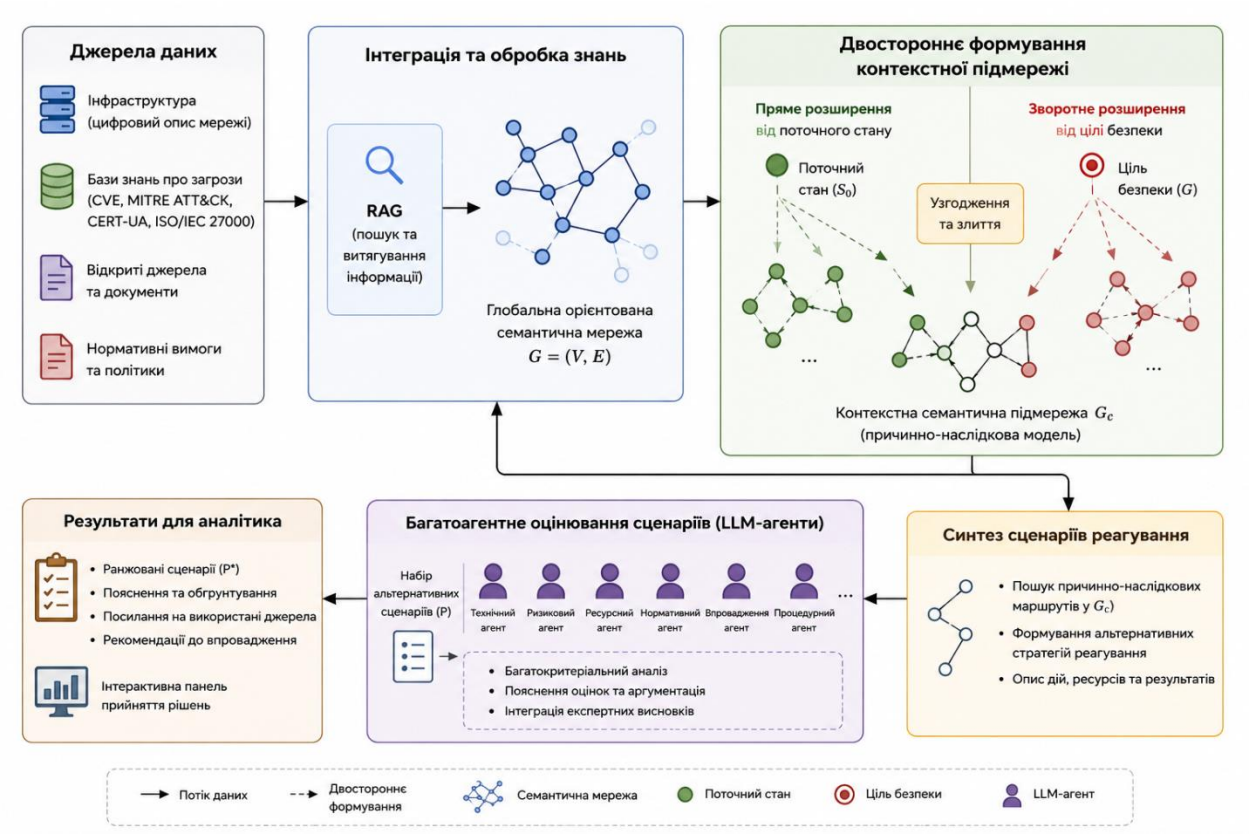

Рис 1. Архітектура когнітивного кіберполігону

Експериментальна перевірка

Експериментальне дослідження проводилося на тестовій корпоративній мережі, що містила 12 вузлів та 26 мережевих зв'язків [6], [7]. До її складу входили робочі станції користувачів і адміністраторів, вебсервер, сервер баз даних, Active Directory, мережеве сховище, SIEM, бездротова точка доступу, маршрутизатор, комутатор та міжмережевий екран.

Для кожного вузла було сформовано цифровий опис, що містив характеристики програмного забезпечення, конфігурації операційної системи, відкритих сервісів, відомих вразливостей і засобів захисту. Додатково інтегрувалися відомості з баз CVE, MITRE ATT&CK, CERT-UA та нормативних документів ISO/IEC 27000.

У результаті побудовано глобальну семантичну мережу, що містила 32 вершини та 48 орієнтованих зв'язків.

Для сценарію компрометації вебсервера було автоматично сформовано контекстну семантичну підмережу, яка містила лише 6 вершин і 16 зв'язків, що відповідало скороченню області аналізу приблизно на 81 % без втрати релевантної інформації.

Подальший синтез сценаріїв дозволив автоматично сформувати дванадцять альтернативних стратегій реагування. Їх оцінювання здійснювалося шістьма віртуальними агентами, які використовували єдиний інформаційний контекст, сформований засобами Retrieval-Augmented Generation. Для кожної альтернативи система автоматично формувала пояснення, що містило причинно-наслідковий ланцюг, використані фрагменти семантичної мережі та нормативні документи, які обґрунтовували запропоновані рішення.

Проведений експеримент підтвердив працездатність запропонованої концепції та продемонстрував можливість автоматичного формування й ранжування сценаріїв реагування без попереднього програмування конкретних алгоритмів дій.

Висновки

Запропоновано концепцію когнітивного кіберполігону, що інтегрує цифровий опис інформаційної інфраструктури, орієнтовані семантичні мережі, технології Retrieval-Augmented Generation, великі мовні моделі та багатоагентний аналіз у єдину систему підтримки прийняття рішень.

Наукова новизна роботи полягає у використанні двостороннього алгоритму побудови контекстної семантичної підмережі, який забезпечує автоматичний синтез альтернативних сценаріїв

реагування, та у функціональному розділенні процесів побудови сценаріїв і їх експертного оцінювання.

Експериментальна перевірка підтвердила працездатність запропонованого підходу та показала перспективність його застосування як у навчальних кіберполігонах, так і в інтелектуальних системах підтримки прийняття рішень для захисту корпоративних інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Kovačević, I., Katulić, F., Mamut, M. and Groš, S., 2025, June. Survey of Open Source Technologies for Building Cyber Ranges for Exercises and Trainings. In 2025 MIPRO 48th ICT and Electronics Convention (pp. 788-793). IEEE. DOI: 10.1109/MIPRO65660.2025.11131978
2. Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P. and Fujdiak, R., 2025. Lessons learned from using cyber range to teach cybersecurity at different levels of education. Technology, Knowledge and Learning. DOI: 10.1007/s10758-025-09840-y
3. Hosamo, H.H., Nielsen, H.K., Alnmr, A.N., Svennevig, P.R. and Svidt, K., 2022. A review of the Digital Twin technology for fault detection in buildings. Frontiers in Built Environment, 8, p.1013196. DOI: 10.3389/fbuil.2022.1013196
4. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3, DOI: 10.5281/zenodo.14278893
5. Zhao, P., Zhang, H., Yu, Q., Wang, Z., Geng, Y., Fu, F., Yang, L., Zhang, W., Jiang, J. and Cui, B., 2026. Retrieval-augmented generation for ai-generated content: A survey. Data Science and Engineering, pp.1-29. 10.1007/s41019-025-00335-5
6. Oleksii Novikov, Dmytro Lande, and Lesia Alekseichuk. Assessment of Corporate Network Penetration Scenarios Based on Iterative Link Weight Determination Using the MRRW-PageRank Method. Proceedings of the Workshop on Cryptology and Data Security (WCDS 2025) co-located with SMICS 2025. Lviv, Ukraine, October 16.18, 2025. https://ceur-ws.org/Vol-4191/paper2.pdf
7. Lande D., Novikov O., Alekseichuk L. Application of Large Language Models for Assessing Parameters and Possible Scenarios of Cyberattacks on Information and Communication Systems // Theoretical and Applied Cyber Security. Vol. 6 No. 1 (2024). DOI: 10.20535/tacs.2664-29132024.1.315242.