



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**



**НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**



THEORETICAL AND APPLIED CYBERSECURITY

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4



Київ – 2026

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ**

**THEORETICAL AND APPLIED
CYBERSECURITY**

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4

Київ – 2026

*Рекомендовано до друку Вченою радою
НН ФТІ КПІ ім. Ігоря Сікорського
(протокол № 9 від 29 червня 2026 р.)*

Theoretical and Applied Cybersecurity. Матеріали IV Всеукраїнської науково-практичної конференції (TACS-2026). – Київ: Інжиніринг. – 186 с. ISBN 978-617-8180-08-9

До збірника увійшли матеріали доповідей, представлених на IV Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2026, 28 травня 2026 р., м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпечного функціонування кібернетичного та інформаційного простору, безпеки промислових систем та систем критичної інфраструктури, математичних і технічних проблем кібернетичної безпеки, запобігання і протидії кібератакам, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації, застосування штучного інтелекту.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

Редакційна колегія:

*О.М. Новіков, д.т.н., професор, член-кор. НАН України;
Д.В. Ланде, д.т.н., професор; С.А. Смирнов, к.т.н., с.н.с.;
А.Ш. Апішева, к.психол.н.; А.В. Напрєсько*

ISBN 978-617-8180-08-9

© НН ФТІ
КПІ ім. Ігоря Сікорського,
2026

© Колектив авторів, 2026

БАГАТОАГЕНТСЬКИЙ СЕМАНТИЧНИЙ АНАЛІЗ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ

Ланде Д.В., Рибак О.О.

*Національний технічний університет України “Київський
політехнічний інститут імені Ігоря Сікорського”,
Київ, Україна,
dwlande@gmail.com, rybak.oleksandr01@gmail.com*

Запропоновано метод багатоагентського семантичного аналізу для підтримки прийняття рішень у сфері кібербезпеки. Метод поєднує інформаційний пошук у відкритих джерелах, формування корпусу релевантних документів, доповнену пошуком генерацію, побудову семантичної мережі, генерацію сюжетних ланцюжків та їх ранжування. Добір документів виконується аналітиком у системі CyberAggreghator, а велика мовна модель забезпечує їх структуроване опрацювання та побудову семантичної мережі.

Ключові слова: багатоагентський аналіз, семантична мережа, підтримка прийняття рішень, доповнена пошуком генерація, CyberAggreghator, OSINT, великі мовні моделі, кібербезпека.

Вступ

Сучасні задачі підтримки прийняття рішень у кібербезпеці потребують побудови цілісної моделі проблемної ситуації, що відображає зв'язки між загрозами, вразливостями, засобами захисту та варіантами реагування. Великі мовні моделі здатні узагальнювати інформацію й формувати гіпотези, однак без зовнішнього контексту можуть використовувати недостатньо перевірені знання. Тому актуальним є їх поєднання з корпусом релевантних документів, відібраних з відкритих джерел [1].

Етапи реалізації методу

Запропонований метод передбачає послідовне виконання кількох етапів. На першому етапі аналітик формує проблемний запит і здійснює пошук у системі CyberAggreghator. Пошукові запити можуть містити ключові слова, синоніми, часові обмеження, мову, типи джерел і тематичні фільтри. Результатом є масив релевантних документів: новинні повідомлення, пости, аналітичні матеріали, повідомлення про інциденти або інші тексти з відкритих електронних джерел.

На другому етапі здійснюється підготовка документів до аналізу: очищення тексту, усунення дублікатів, визначення мови, сегментація на фрагменти, виділення сутностей і первинних тематичних ознак.

На третьому етапі велика мовна модель використовується для побудови або розширення семантичної мережі на основі опису проблеми, виявлених сутностей і фрагментів релевантних документів. Це відповідає логіці доповненої пошуком генерації, за якої модель враховує зовнішній корпус документів [1]. Семантична мережа подається як граф, де вузли відповідають поняттям, а ребра відображають зв'язки між ними.

Багатоагентність методу полягає у розподілі аналітичного процесу між спеціалізованими ролями. Агент збору даних відповідає за формування пошукових профілів і добір документів; агент фільтрації та індексації виконує очищення й підготовку корпусу; агент семантичного аналізу виділяє поняття та зв'язки; агент генерації ланцюжків формує можливі сценарії вирішення проблеми; агент-оцінювач ранжує їх за визначеними критеріями; агент-інтерпретатор пояснює отримані результати для особи, що ухвалює рішення [2].

Сюжетний ланцюжок у межах методу розглядається як упорядкований шлях від вузла проблеми до вузла бажаного результату через проміжні вузли, що відображають причини, ризики, засоби впливу, обмеження та практичні дії. Наприклад, для проблеми фішингу такий ланцюжок

може мати вигляд: “фішинг – викрадення облікових даних – автентифікація – стійка багатофакторна автентифікація – зниження компрометації”. Оцінювання таких ланцюжків може здійснюватися за критеріями релевантності, достовірності, очікуваного впливу, ризику, вартості, практичної застосовності та рівня підтримки джерелами [3].

Висновки

У роботі запропоновано метод багатоагентського семантичного аналізу для підтримки прийняття рішень у сфері кібербезпеки. Він поєднує інформаційний пошук, підготовку корпусу документів, побудову семантичної мережі, формування сюжетних ланцюжків та їх ранжування.

Практичне значення методу полягає у формуванні впорядкованих і пояснюваних сценаріїв дій. Використання CyberAggreghator та великої мовної моделі підвищує керованість, відтворюваність і джерельну простежуваність результатів.

Список використаних джерел

1. Y. Gao та ін. “ Retrieval-Augmented Generation for Large Language Models: A Survey”, 18 December 2023. [Online]. <https://arxiv.org/pdf/2312.10997>
2. T. Guo та ін. “ Large Language Model Based Multi-Agents: A Survey of Progress and Challenges”, 2024. [Online]. <https://arxiv.org/pdf/2402.01680>
3. O. Novikov, D. Lande, L. Alekseichuk, “Assessment of Corporate Network Penetration Scenarios Based on Iterative Link Weight Determination Using the MRRW-PageRank Method”, 2025. [Online]. <https://ceur-ws.org/Vol-4191/paper2.pdf>