



**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. Напрєнко*

ISBN 978-617-8180-08-9

© НН ФТІ
КПІ ім. Ігоря Сікорського,
2026

© Колектив авторів, 2026

ПОРІВНЯННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ, МЕТОДУ АНАЛІЗУ МЕРЕЖ І ПІДХОДУ «ВІД СЕРЕДНЬОГО РІВНЯ» ДЛЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КІБЕРБЕЗПЕЦІ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Свобода І. М., Ланде Д. В.

*КПІ ім. Ігоря Сікорського, Фізико-технічний інститут,
Київ, Україна,
i.svoboda@kpi.ua; dwlande@gmail.com*

У роботі порівнюються три підходи до побудови систем підтримки прийняття рішень (СППР) у кібербезпеці із застосуванням агентів на основі великих мовних моделей (LLM): метод аналізу ієрархій (MAI), метод аналізу мереж (MAM) та підхід “від середнього рівня” (middle-out) із двоспрямованим пошуком. Показано, що MAI та MAM визначають пріоритети альтернатив, а підхід “від середнього рівня” готує перевірювану основу для вибору критеріїв, альтернатив і зв’язків між ними.

Ключові слова: кібербезпека, система підтримки прийняття рішень, метод аналізу ієрархій, метод аналізу мереж, двоспрямований пошук, великі мовні моделі, віртуальні експерти.

Вступ

Рішення у сфері кібербезпеки часто приймаються за умов неповноти даних, обмеженості ресурсів, суперечливості критеріїв та високої вартості помилки. Формальною основою для таких задач є MAI [1] та MAM [2]. Агенти на основі LLM можуть формувати пояснення, матриці парних порівнянь і причинні зв’язки, однак без формальної процедури їхні відповіді залишаються попередніми судженнями. Попередні роботи підтверджують доцільність такого напрямку [3]-[5]. Мета

роботи - уточнити ролі трьох підходів у спільній СППР, а не розглядати їх як рівнозначні альтернативи.

Ролі підходів у СППР

МАІ доцільно застосовувати, коли задачу можна подати як ієрархію “мета - критерії - альтернативи” [1]. LLM-агенти можуть пропонувати критерії, формувати парні порівняння за шкалою Сааті та пояснювати підстави суджень, а СППР - агрегувати відповіді й контролювати коефіцієнт узгодженості. Типовий приклад - вибір першочергової дії для окремого інциденту. Перевага МАІ - прозорість; обмеження - слабе врахування взаємного впливу критеріїв.

МAM доцільний, коли залежності між критеріями, альтернативами та наслідками є істотною частиною задачі [2]. У кібербезпеці це типово: сегментація мережі впливає на моніторинг, моніторинг - на швидкість реагування, реагування - на доступність сервісів. LLM-агенти можуть попередньо формувати групи “загрози - активи - засоби захисту - обмеження - наслідки”, але кожне судження має бути пов’язане з джерелом або експертним обґрунтуванням. МAM краще описує мережеву природу кіберзахисту, проте потребує ретельнішої перевірки.

Підхід “від середнього рівня” не є третім способом визначення пріоритетів нарівні з МАІ та МAM. Його роль - підготувати предметну структуру задачі. Початковим вузлом може бути техніка MITRE ATT&CK для промислових систем керування (ATT&CK for ICS) [6], кіберподія, актив, уразливість або засіб захисту. Двоспрямований пошук рухається вгору до управлінської мети, ризику та наслідків, і вниз до індикаторів, журналів подій, технічних перевірок і заходів протидії. Отже, цей підхід визначає, що саме треба оцінювати і чому.

Приклад застосування

Для об’єкта критичної інфраструктури початковою точкою може бути техніка ATT&CK for ICS або подія зі звіту центру операцій безпеки (SOC). LLM-агенти

виділяють активи, наслідки, засоби захисту та джерела доказів; непідтверджені зв'язки вилучаються. Якщо структура задачі деревоподібна, її доцільно передати до MAI. Якщо є сильні зворотні впливи між сегментацією, доступом, журналюванням, резервним копіюванням і навчанням персоналу, ті самі вузли слід передати до MAM.

Комбінована схема та рекомендації

Запропонована схема має чотири етапи: 1) LLM-агенти будують початковий граф “подія - доказ - актив - наслідок - засіб захисту” на основі опису інциденту, ATT&CK for ICS, STIX (Structured Threat Information Expression) [7] або внутрішньої онтології; 2) перевіряються джерела, критерії та альтернативи; 3) обирається метод: MAI - для локальної ієрархічної задачі, MAM - для задачі зі зворотними зв'язками; 4) обчислюються пріоритети, перевіряється узгодженість матриць і формується пояснення “доказ - критерій - судження - пріоритет - рекомендація”. Практична рекомендація: спочатку застосовувати підхід “від середнього рівня” для постановки задачі, а потім переходити до MAI або MAM залежно від структури залежностей.

Висновки

Порівняння показує, що MAI, MAM і підхід “від середнього рівня” розв'язують різні частини задачі СППР. MAI є базовим методом для швидкого й прозорого вибору альтернатив за відносно незалежними критеріями. MAM слід застосовувати тоді, коли взаємозалежність засобів захисту, активів, загроз і організаційних обмежень впливає на результат. Підхід “від середнього рівня” варто використовувати перед MAI або MAM як засіб побудови доказової структури. Висновки LLM-агентів мають розглядатися як перевірювані попередні судження з посиланням на джерело, обґрунтування, матрицю порівнянь і результат перевірки узгодженості.

Список використаних джерел

1. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill International Book Company, 1980. 287 p.
2. Saaty T. L. Decision Making with Dependence and Feedback: The Analytic Network Process. Pittsburgh: RWS Publications, 1996. 370 p.
3. Svoboda I., Lande D. AI Agents in Multi-Criteria Decision Analysis: Automating the Analytic Hierarchy Process with Large Language Models. SSRN, 2024. DOI: 10.2139/ssrn.5069656.
4. Svoboda I. Automating Cybersecurity Decision-Making with AI and the Analytic Hierarchy Process. Theoretical and Applied Cybersecurity. 2025. Vol. 7, No. 2. P. 91-97. DOI: 10.20535/tacs.2664-29132025.2.338865.
5. Lande D., Alekseichuk L., Svoboda I., Strashnoy L. Methodology of a Swarm of Virtual Experts for Evaluating the Weight of Connections in Networks. Theoretical and Applied Cybersecurity. 2024. Vol. 6, No. 2. P. 25-33. DOI: 10.20535/tacs.2664-29132024.2.319946.
6. MITRE ATT&CK. ICS Matrix. MITRE. URL: <https://attack.mitre.org/matrices/ics/> (дата звернення: 27.05.2026).
7. OASIS. STIX Version 2.1 Errata 01. Edited by Rich Piazza, Emily Ratliff, Stephan Relitz, Christian Studer. 02 April 2025. OASIS Committee Specification Draft 01. URL: <https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.html> (дата звернення: 27.05.2026).