

МАТЕРІАЛИ

IV Міжнародної науково-практичної конференції “КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНСТИТУЦІЙ ТА ПОДОЛАННЯ КРИЗОВИХ СТАНІВ”

18 листопада 2025 року

Київ – Тернопіль – Краків

**Матеріали IV Міжнародної науково-практичної конференції
“Кібербезпека державних інституцій та подолання кризових станів”:**
(Київ – Тернопіль – Краків): ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. 475 с.

У матеріалах IV Міжнародної науково-практичної конференції “Кібербезпека державних інституцій та подолання кризових станів” опубліковано тези доповідей в яких висвітлюються питання дослідження, аналізу й узагальнення нових теоретичних і практичних результатів у сферах кіберзахисту державних інформаційних ресурсів, розвитку сучасних електронних комунікацій, застосування штучного інтелекту та інформаційних технологій у забезпеченні кібербезпеки, криптографії та захисту даних, а також питання формування професійних компетентностей фахівців сектору безпеки й оборони України, розвитку лідерства та освітніх практик в умовах воєнного стану.

РЕЦЕНЗЕНТИ:

Олександр ПУЧКОВ	к.філос.н., професор, Заслужений працівник освіти України
Сергій КОНЮШОК	к.т.н., доцент
Владислав ГОЛЬ	к.т.н., професор
Вадим РОМАНЕНКО	к.т.н., доцент
Дмитро МОГИЛЕВИЧ	д.т.н., професор
Олена УВАРКІНА	д.філос.н., професор, Заслужений працівник освіти України
Ігор СУБАЧ	д.т.н., професор, Заслужений працівник освіти України
Ярослав ЗІНЧЕНКО	к.т.н., с.н.с.

*Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 4 від 17.11.2025)*

Віра ГИРДА;
Дмитро ЛАНДЕ, д.т.н., професор

СЕМАНТИЧНИЙ НЕТВОРКІНГ ЯК ІНСТРУМЕНТ ДЛЯ ОЦІНЮВАННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ

Анотація. Запропоновано методику оцінювання достовірності інформації на основі семантичного нетворкінгу та генеративного штучного інтелекту.

Summary. A method of assessing the reliability of information based on semantic networking and generative artificial intelligence is proposed.

Ключові слова: кібербезпека, великі мовні моделі, семантичний нетворкінг.

Методика включає в себе застосування великих мовних моделей та семантичного нетворкінгу для виявлення фейкової інформації та надання узагальненої оцінки.

Методика оцінки достовірності інформації включає такі етапи:

1. Проведення семантичного аналізу та формування семантичної мережі подій новинного повідомлення у вигляді орієнтованого графа зв'язків між подіями;
2. Визначення рівня достовірності кожного типу зв'язків за допомогою промт-інжинірингу із використанням декількох великих мовних моделей, які функціонують як "ансамбль штучних експертів".
3. Розрахунок інтегральної оцінки достовірності з урахуванням вагових коефіцієнтів, які відповідають ступеню довіри до певного типу зв'язку.

Висновки. Практичний експеримент підтвердив ефективність методики: отримана інтегральна оцінка достовірності дозволила чітко розмежувати правдиві та фейкові повідомлення, виявивши слабкі місця у їхній структурі.

Отримані результати свідчать про перспективність використання комбінованих методів штучного інтелекту в аналізі медіаконтенту, а також про можливість подальшого розвитку цього напрямку в галузі кібербезпеки

Розроблена технологія може стати основою для створення інструментів автоматизованого аналізу інформаційних загроз, підвищення цифрової грамотності населення та забезпечення інформаційної стійкості суспільства