



РЕЦЕНЗІЯ

Міжнародний конкурс
студентських робіт зі
штучного інтелекту 2025

II тур
Перший етап

на наукову роботу

назва Методика виявлення кібератак/кіберінцидентів

у системах управління інформацією та подіями безпеки

із застосуванням генеративного штучного інтелекту

шифр Бетельгейзе

представлену на Міжнародний конкурс студентських робіт зі штучного інтелекту

№ з/п	Характеристики та критерії оцінки рукопису наукової роботи	Рейтингова оцінка. Максимальна кількість балів (за 120-бальною шкалою)	Бали
1	Актуальність проблеми	10	10,00
2	Новизна та оригінальність ідей	15	13,00
3	Використані методи дослідження	15	13,00
4	Теоретичні наукові результати	10	8,75
5	Практична направленість результатів	20	20,00
6	Рівень використання наукової літератури та інших джерел інформації	5	3,75
7	Ступінь самостійності роботи	10	10,00
8	Якість оформлення	5	5,00
9	Наукові публікації	10	8,50
10	Недоліки роботи (пояснення зниження максимальних балів у пунктах 1-9): Робота присвячена застосуванню великих мовних моделей (LLM) у сфері кібербезпеки для автоматизації аналізу подій безпеки. Ідея інтеграції генеративного ШІ з інструментами типу Wazuh та Shuffle є актуальною й має практичний потенціал. Проте реалізація базується переважно на адаптації відомих підходів, що обмежує рівень наукової новизни (рівень конференційної публікації). До сильних сторін роботи належить практична орієнтація та продемонстроване якісне покращення часу аналізу подій (скорочення на 97%). Разом із тим, кількісне оцінювання ефективності є недостатнім: відсутні основні статистичні метрики точності, повноти (precision, recall), F1-score, а також показники хибних спрацьовувань (False Positives / False Negatives). Це ускладнює об'єктивне порівняння з іншими методами у сфері кіберзахисту. Експериментальна база обмежена: тестування проведено на невеликій вибірці (близько 70 логів) у межах однієї інфраструктури, що не дозволяє узагальнити результати або підтвердити стабільність методики у різних середовищах SIEM/SOAR. Недостатньо деталізовано описано архітектуру генеративного модуля та механізми взаємодії з GPT4Free (g4f): відсутні формальні схеми, опис структури промптів, обробки багатомовних журналів, контролю якості відповідей ШІ чи порівняння з альтернативними LLM (наприклад, OpenAI API або Mistral). Це знижує можливість повторного відтворення результатів іншими дослідниками.		

№ з/п	Характеристики та критерії оцінки рукопису наукової роботи	Рейтингова оцінка. Максимальна кількість балів (за 120-бальною шкалою)	Бали
	Теоретична частина обмежується адаптацією існуючих методів без їх подальшого розвитку. Бракує аналізу шаблонів ланцюжків подій, що могло б підвищити глибину дослідження. У бібліографії переважають технічна документація та веб-ресурси; кількість саме наукових джерел є недостатньою. Загальна оцінка: робота має практичну цінність і демонструє компетентність автора у застосуванні сучасних інструментів, проте потребує суттєвого поглиблення експериментальної та наукової складових для досягнення рівня академічного дослідження.		
10.1	Наявність розробленого програмного забезпечення, у т.ч. веб-сервісу, мобільного застосунку	10	10,00
10.2	Рівень отриманих практичних результатів наукової роботи	10	9,25
Сума балів			111,25

Загальний висновок рекомендується для захисту на ПНПК
(рекомендується, не рекомендується для захисту на науково-практичній конференції)

Рецензенти члени Конкурсної комісії напряму «Обробка природної мови»

«07» листопада 2025 року