МАТЕРІАЛИ
VIII науково-практичної конференції курсантів (студентів),
аспірантів, докторантів та молодих учених
“АКТУАЛЬНІ ПИТАННЯ
ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ”

18 червня 2025 року

Київ – 2025

УДК 621

Матеріали VIII науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем". Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. 516 с.

У матеріалах VIII науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем" опубліковано тези доповідей, в яких висвітлюються питання дослідження, аналізу й узагальнення нових теоретичних і практичних результатів у сфері кібербезпеки, новітніх інформаційних технологій, штучного інтелекту та електронних комунікацій, підготовки офіцерів для сектору безпеки та оборони а також залучення здобувачів вищої освіти до активної наукової діяльності.

РЕЦЕНЗЕНТИ:

Олександр ПУЧКОВ	К.філос.н., професор
Сергій КОНЮШОК	К.т.н., доцент
Владислав ГОЛЬ	К.т.н., професор
Вадим РОМАНЕНКО	К.т.н., доцент
Дмитро МОГИЛЕВИЧ	Д.т.н., професор
Ірина КОНОВА	К.т.н., доцент
Ігор СУБАЧ	Д.т.н., професор
Ярослав ЗІНЧЕНКО	К.т.н., с.н.с.

Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 13 від 16.06.2025).

Секція № 4 "Новітні інформаційні технології та штучний інтелект в сфері кібербезпеки"

Володимир ПИЛИПЕНКО;
Артем ІЩЕНКО

ВИКОРИСТАННЯ ТА ЗАСТОСУВАННЯ MICROSOFT SECURITY COPILOT В КІБЕРБЕЗПЕЦІ

Анотація. Microsoft Security Copilot є рішенням на основі генеративного штучного інтелекту, призначеним для підвищення ефективності та можливостей фахівців з кібербезпеки. Кіберпомічник дозволяє використовувати «природну мову» для розслідування інцидентів, аналізу загроз та керування станом безпеки. Інтегруючись із широким спектром продуктів Microsoft та сторонніми сервісами, Security Copilot надає глибокий контекст даних, прискорюючи реакцію на кібератаки.

Summary. Microsoft Security Copilot is a generative AI-powered solution designed to enhance the efficiency and capabilities of cybersecurity professionals. It enables the use of «natural language» for investigating incidents, analyzing threats, and managing security posture. Integrating with a wide range of Microsoft products and third-party services, Security Copilot provides deep data context, accelerating response to cyberattacks.

Ключові слова: Кібербезпека, Microsoft Security Copilot, Штучний інтелект, Розслідування інцидентів, Управління ризиками.

У сучасних реаліях кібербезпеки організації стикаються зі зростаючою частотою атак та браком кваліфікованих кадрів. Фахівцям з безпеки складно обробляти великі обсяги інформації та швидко реагувати на загрози. Microsoft Security Copilot позиціонується як помічник зі штучним інтелектом, що використовує можливості GPT та великий досвід Microsoft у сфері кібербезпеки для вирішення цих проблем.

Security Copilot функціонує як інтерфейс природною мовою до даних безпеки організації. Він доступний як самостійний продукт (Standalone experience) та інтегрується в інші продукти Microsoft Security (Embedded experience). Вбудовані можливості доступні в таких інструментах, як Microsoft Defender XDR8, Microsoft Intune, Microsoft Entra, Microsoft Purview, Microsoft Sentinel, Azure Firewall та Microsoft Defender Threat Intelligence. Також підтримується інтеграція зі сторонніми сервісами через плагіни, наприклад, ServiceNow.

На відміну від стандартних великих мовних моделей (LLM), Security Copilot доповнює їхнє навчання специфічними навичками безпеки. Він використовує підхід, що називається "grounding" (уземлення), який покращує специфіку вхідних запитів, роблячи відповіді

більш релевантними та дієвими. Цей процес включає доступ до даних через плагіни з організаційно-специфічної інформації, авторитетних джерел та глобальної аналітики загроз. Microsoft застосовує метод Low-Rank Adaptive fine-tuning (LoRA) для налаштування LLM на завдання кібербезпеки, такі як аналіз, виявлення, реагування та узагальнення. Рішення також використовує актуальну аналітику загроз (evergreen Threat Intelligence) з отриманням даних у режимі реального часу. Для обробки даних використовується AI суперкомп'ютер у Azure.

Основні сценарії використання Security Copilot включають:

Розслідування та усунення загроз безпеки: Швидке отримання контексту інцидентів, узагальнення попереджень та покрокові вказівки для реагування. Дозволяє прискорити дослідження.

Аналіз скриптів та генерація запитів KQL: Можливість аналізувати підозрілі скрипти, отримуючи покроковий опис тактик експлойту, а також створювати запити на мові Kusto Query Language (KQL) за допомогою природної мови для полювання на загрози.

Оцінка ризиків та управління станом безпеки: Надання ширшої картини стану середовища з пріоритезацією ризиків.

Підготовка звітів для зацікавлених сторін: Генерація зрозумілих звітів, адаптованих для різної аудиторії, включаючи нетехнічні підсумки для керівництва.

Завдяки інтеграції з різними джерелами даних. та вбудованим специфічним навичкам (Promptbooks), Security Copilot може значно прискорити процеси розслідування. Він може допомогти аналітикам, навіть якщо вони не є експертами у всіх галузях, надаючи контекст з підключених служб. Рішення підтримує стан сесії (stateful experience), дозволяючи легко повертатися до попередніх розслідувань та обмінюватися контекстом з командою.

Висновки. Microsoft Security Copilot демонструє потенціал генеративного ШІ для трансформації операцій кібербезпеки. Він допомагає подолати виклики, пов'язані зі зростанням складності загроз та нестачею ресурсів, підвищуючи ефективність захисників на "машинній швидкості та масштабі". Надаючи єдиний інтерфейс природною мовою до різноманітних джерел даних безпеки. та автоматизуючи складні завдання, такі як аналіз скриптів чи генерація запитів KQL., Security Copilot робить передові можливості кібербезпеки більш доступними та дозволяє командам швидше реагувати на інциденти.

VIII науково-практична конференція курсантів (студентів), аспірантів, докторантів та молодих учених

“АКТУАЛЬНІ ПИТАННЯ ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ”

Збірник матеріалів науково-практичної конференції

18 червня 2025 року

Підписано до друку 16.06.2025 Формат 60х84/8 Папір офсетний
Гарнітура «timesnewroman» Друк – різограф
Ум.друк. Арк. –32,25. Обл. Вид. Арк. –32,25.