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

з нагоди 20-ї річниці утворення
Державної служби спеціального зв’язку та захисту
інформації України

23 червня 2026 року

Київ – 2026

УДК 621

Матеріали IX науково-практичної конференції студентів, курсантів, аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем". Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2026. 581с.

У матеріалах IX науково-практичної конференції студентів, курсантів, аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем" опубліковано тези доповідей, в яких висвітлюються питання дослідження, аналізе та узагальнення нових теоретичних і практичних наукових результатів у сферах кібербезпеки, кіберзахисту, інформаційних технологій та електронних комунікацій. Підвищення професійної підготовки майбутніх офіцерів сектору безпеки і оборони шляхом формування лідерських якостей і фахових компетентностей в умовах сучасних безпекових викликів, зокрема правового режиму воєнного стану. Залучення здобувачів вищої освіти до активної наукової діяльності з використанням новітніх інформаційних технологій і штучного інтелекту в сфері кібербезпеки.

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
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 22.06.2026).

СЕКЦІЇ КОНФЕРЕНЦІЇ

Секція № 1 “Актуальні питання кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури.”
ГОЛЬ Владислав Дмитрович, завідувач Спеціальної кафедри № 1, к.т.н., професор – керівник секції

Секція № 2 “ Формування лідерських якостей та фахових компетентностей майбутніх офіцерів сектору безпеки і оборони України в умовах правового режиму воєнного стану.”
РОМАНЕНКО Вадим Петрович, завідувач Спеціальної кафедри № 2, к.т.н., доцент – керівник секції

Секція № 3 “Пріоритетні напрями розвитку спеціальних електронних інформаційно-комунікаційних систем”
МОГИЛЕВИЧ Дмитро Ісакович, завідувач Спеціальної кафедри № 3, д.т.н., професор – керівник секції

Секція № 4 “Імплементація інформаційно-комунікаційних систем у формуванні психологічних, комунікаційних і кібернетичних компетентностей офіцерів”
КОНОНОВА Ірина Віталіївна, завідувач Спеціальної кафедри № 4, к.т.н., доцент – керівник секції

Секція № 5 “Новітні інформаційні технології та штучний інтелект в сфері кібербезпеки ”
СУБАЧ Ігор Юрійович, завідувач Спеціальної кафедри № 5, д.т.н., професор – керівник секції

Артем ПЕДУНОВ;
Дмитро ЛАНДЕ, д. т. н., професор

ПОБУДОВА КОНТУРУ LLMSECOPS НА БАЗІ ELASTIC ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА СПЕЦИФІЧНІ АТАКИ НА ВЕЛИКІ МОВНІ МОДЕЛІ

Анотація. У роботі демонструється підхід до побудови контуру безпеки LLMSecOps для захисту локальних великих мовних моделей (LLM) від атак відповідно до аналізу OWASP GenAI Security (Q2 2026). Продемонстровано архітектуру на основі Elastic Security (ELK-стек) із інтеграцією open-source сенсорів LLM Guard, Meta Prompt Guard та ModelScan для виявлення prompt injection, jailbreak та витоку даних у реальному часі.

Summary. This paper presents an approach to building an LLMSecOps security framework to protect on-premises large language models (LLMs) from attacks, in accordance with the OWASP GenAI Security analysis (Q2 2026). It demonstrates an architecture based on Elastic Security (ELK stack) with the integration of open-source sensors LLM Guard, Meta Prompt Guard, and ModelScan to detect prompt injection, jailbreak, and data leaks in real time.

Ключові слова: LLMSecOps, Elastic Security, prompt injection, jailbreak, LLM Guard, OWASP GenAI, захист ШІ, SIEM.

Впровадження великих мовних моделей у корпоративних системах створило ризик загроз на які не поширюються традиційні метди захисту. Аналізуючи публікацію OWASP GenAI Security (Q2 2026) визначено, що найкритичнішими вразливостями великих мовних моделей визначено: prompt injection (LLM01), витік чутливих даних (LLM02) та компрометація постачальника моделей (LLM03). Відсутність спеціалізованої телеметрії та механізмів виявлення таких загроз створює потребу розробки відповідної системи моніторингу.

За результатами дослідження було створено архітектуру LLMSecOps (рис. 1) яка базується на Elastic Security (та містить Elasticsearch + Kibana + Logstash) та було реалізовує чотирирівневу модель. Рівень сенсорів охоплює LLM Guard - проксі-шар фільтрації запитів і виявлення витоків даних. Meta Prompt Guard використаний як класифікатор jailbreak-спроб. ModelScan виконує роль аудитора файлів моделей на шкідливий код до завантаження у датасет. Elastic Agent збірає системні та прикладні логи.

На рівні обробки в Logstash створено конвеєри парсингу JSON/GELF-логів. Ключові поля індексації: prompt_risk_score, sensitive_data_detected, jailbreak_attempt_type, model_latency_ms. Нормалізація за Elastic Common Schema має сумісність зі стандартними правилами виявлення та кореляцію із загальносистемними подіями безпеки.

Виявлення атак відбувається через Elastic Detection Rules (EQL/KQL) за трьома класами. (1) Adversarial Attack Protection - аномальна частота API-запитів та паттерни автоматизованих атак. (2) Prompt Injection Detection - сигнатурний та поведінковий аналіз. (3) Data Leakage Protection - моніторинг вихідного контенту на персональні дані та дані захист яких обумовлений законом. Алертинг інтегрується через Webhook та Elastic Actions.

У середовищі Kibana було спроєктовано дашборд AI Security Posture Management зі статистикою загроз за поділом на типи атак, станом LLM-інстансів та рівнем відповідності AI Governance-політикам. Повна локалізація даних периметрі, відсутність ліцензійних витрат та масштабованість через підключення нових моделей до існуючого Elasticsearch-кластеру являється ключовими перевагами рішення.

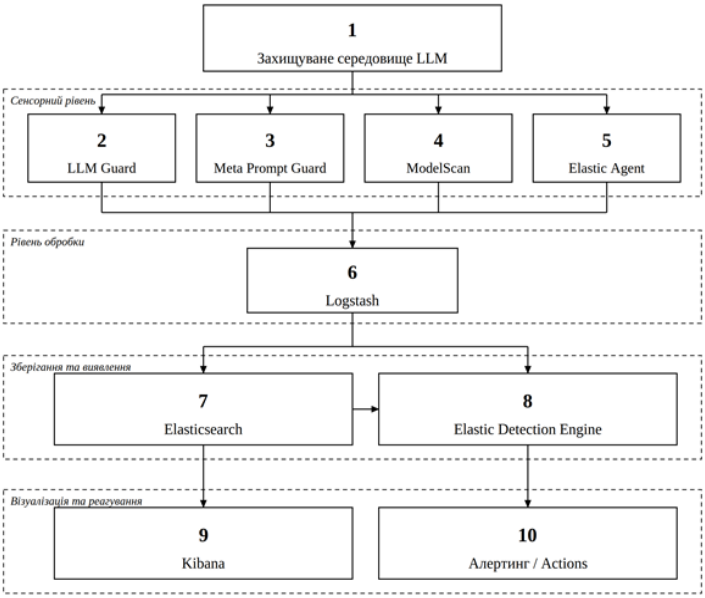

Рис. 1. Архітектура контуру LLMSecOps на базі Elastic Security

Порівняльний аналіз показує, що пропрієтарні платформи (Microsoft Azure AI Content Safety, AWS Guardrails) вимагають передачі даних до хмари постачальника, що є неприйнятним для систем з закритим контуром, комерційні SIEM-системи (Splunk, IBM QRadar) не мають вбудованих коннекторів для LLM-телеметрії та потребують значних ліцензійних витрат . ELK-стек поєднуючи з відкритими LLM-сенсорами має схожу функціональність без зазначених обмежень.

Верифікація ефективності проведено за методологією Red Team з використанням фреймворку PyRIT : 500 синтетичних атакових сценаріїв за OWASP LLM Top 10 показали Recall = 0.91 для прямих prompt injection та Recall = 0.84 для непрямих ін'єкцій через RAG-контекст. Серед поточних обмежень - залежність від актуальності сигнатурних баз LLM Guard та потреба в перенавчанні класифікатора на власних даних організації. Перспективами в данному дослідженні є інтеграція пояснюваного ШІ (XAI) для інтерпретації алертів та розширення підходу на мультимодальні моделі.

Практичне розгортання запропонованого контуру передбачає горизонтальне масштабування Elasticsearch-кластеру за схемою зберігання “hot-warm-cold”, що оптимізує вартість утримання індексів LLM-телеметрії для ретроспективного аналізу інцидентів. Конвеєр LLM Guard → Logstash → Elasticsearch вбудовується у MLOps-процеси організації (MLSecOps), забезпечуючи безперервний контроль безпеки на всіх етапах життєвого циклу від завантаження моделі до її промислової експлуатації.

Окрему увагу приділено відповідності нормативним вимогам. Дашборд AI Security Posture Management співвідносить виявлені події з контрольними заходами NIST AI Risk Management Framework, вимогами Регламенту ЄС щодо штучного інтелекту (EU AI Act) та стандарту ISO/IEC 42001 стосовно систем управління ШІ що забезпечує не лише технічне виявлення атак, а й управлінську прозорість життєвого циклу LLM у регульованих галузях.

Висновки. Запропонований контур LLMSecOps на базі Elastic Security надає комплексний моніторинг загроз для LLM-систем без пропрієтарних рішень. Інтеграція LLM Guard, Meta Prompt Guard та ModelScan з Elastic Detection Engine підтвердила практичну ефективність (Recall = 0.91) при захисті від актуальних векторів атак OWASP GenAI Security. Результати мають теоретичну цінність у систематизації підходів до захисту ШІ та практичну значущість при розгортанні корпоративних LLM.

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

Збірник матеріалів науково-практичної конференції
23 червня 2026 року

Підписано до друку 22.06.2026 Формат 60x84/8 Папір офсетний
Гарнітура «timesnewroman» Друк – різограф
Ум.друк. Арк. –32,25. Обл. Вид. Арк. –32,25.