МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Мелітопольський державний педагогічний університет
імені Богдана Хмельницького
Київський столичний університет імені Бориса Грінченка
Полтавський національний педагогічний університет імені В.Г. Короленка
Хортицька національна навчально-реабілітаційна академія
Сілезька академія, Польща
Riga Technical University Liepaja Academy

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА НАУЦІ

Збірник наукових праць
V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

21 травня 2026 року

Запоріжжя, 2026

УДК 004:[378+001](062.552)

Рекомендовано Вченою радою Мелітопольського державного педагогічного університету імені Богдана Хмельницького (протокол № 17 від 23.06.2026 р.)

Редакційна колегія:
Наталя ФАЛЬКО, докторка психологічних наук, професорка, ректорка, Мелітопольський державний педагогічний університет імені Богдана Хмельницького.
Владислав КРУГЛИК, доктор педагогічних наук, професор кафедри інформатики і кібернетики, Мелітопольський державний педагогічний університет імені Богдана Хмельницького.
Ірина КРАШЕНІННІК, докторка філософії, доцентка, завідувачка кафедри інформатики і кібернетики, Мелітопольський державний педагогічний університет імені Богдана Хмельницького.
Юрій СІЦИЛІЦИН, доктор філософії, доцент кафедри інформатики і кібернетики, Мелітопольський державний педагогічний університет імені Богдана Хмельницького.
Альона ЧОРНА, кандидатка педагогічних наук, доцентка кафедри інформатики і кібернетики, Мелітопольський державний педагогічний університет імені Богдана Хмельницького.

Інформаційні технології в освіті та науці: збірник наукових праць V міжнародної науково-практичної конференції (Запоріжжя, 21 травня 2026 р.) / за заг. ред. В. С. Круглика. – Запоріжжя: МДПУ ім. Б. Хмельницького, 2026. – 696 с.

ISBN 978-617-8757-01-4
DOI: https://doi.org/10.33842/bkmspu_ites2026

До збірника ввійшли матеріали, присвячені актуальним проблемам цифрової трансформації суспільства та окремих сфер його функціонування, а також інноваційного розвитку освіти. Збірник буде корисним науково-педагогічним працівникам, аспірантам та студентам.

У матеріалах конференції збережено орфографію та пунктуацію авторів. За достовірність та оригінальність матеріалу відповідальність покладається на авторів.

© МДПУ імені Богдана Хмельницького, 2026
© Кафедра інформатики і кібернетики, 2026
© Автори публікацій, 2026

ТОПОЛОГІЧНА ЕКСТРАКЦІЯ МОД ТЕНЗОРІВ ДЛЯ СТІЙКОГО ШІ-КЕРОВАНОГО ПЕНТЕСТИНГУ ВЕБ-ЗАСТОСУНКІВ

Кравчук Владислав Сергійович
аспірант
ДВНЗ «Донецький національний технічний університет»

Дорогий Ярослав Юрійович
доктор технічних наук, професор
завідувач кафедри штучного інтелекту та кібербезпеки
ДВНЗ «Донецький національний технічний університет»

У сучасних умовах забезпечення безпеки веб-застосунків є однією з найактуальніших задач IT-галузі. Традиційні основані на правилах сканери та навіть сучасні моделі машинного навчання (RNN, CNN, Graph Neural Networks) мають суттєві обмеження: вони погано узагальнюються на нові багатостадійні атаки, потребують ручного підбору гіперпараметрів і не враховують мультимасштабну топологічну структуру даних.

У роботі запропоновано новий фреймворк **TopoCP**, який інтегрує топологічний аналіз даних з тензорним розкладом для автоматичної, шумостійкої екстракції ознак у системах пентестингу веб-застосунків

керованих ШІ. Основна ідея полягає в заміні традиційного виділення ознак на топологічно-регуляризований тензорний розклад.

Спочатку трафік веб-застосунків моделюється як гетерогенний граф токенів. Кожен HTTP-запит парситься на семантичні токени (назви параметрів, значення, заголовки, методи тощо), яким присвоюються категоріальні мітки. Ребра графа поєднують два типи залежностей: синтаксичні (з дерева парсингу HTTP-запиту) та темпоральні (в межах ковзного вікна сесії). Ад'яцентна матриця формується як зважене поєднання цих залежностей.

На побудованому графі застосовується субрівнева фільтрація за вагою структурної важливості вузлів. За допомогою персистентної гомології (0-вимірної – компоненти зв'язності) обчислюються діаграми персистенції, які фіксують «народження» та «смерть» топологічних ознак на різних масштабах. Для подальшої векторизації діаграми перетворюються в ландшафти персистенції – кусочно-лінійні функції, що представляють топологічну структуру даних у вигляді векторів.

Трафік організовується у тензор третього порядку (сесії × токени × часові вікна). Замість традиційного CP-розкладу з фіксованим рангом пропонується топологічно-регуляризований канонічний поліадичний розклад. Ландшафти персистенції використовуються для автоматичного визначення оптимального рангу: спектральна енергія ландшафтів визначає внутрішню розмірність маніфолду даних, а спеціальний регуляризаційний член (на основі кумулятивної топологічної енергії) штрафує ранги, що не відповідають стабільним топологічним структурам. Оптимізаційна задача розв'язується методом обмеженого пошуку по сітці під час офлайн-навчання.

Отримані низькорангові тензорні фактори замінюють сирі вектори трафіку в downstream-моделях класифікації (лінійний SVM). Така заміна забезпечує фокусування аналізу виключно на атаках зі стабільними топологічними характеристиками, природну фільтрацію шуму та автоматичну адаптацію до змінних патернів трафіку без ручного тюнінгу гіперпараметрів.

Експериментальна валідація проводилася на об'єднаному датасеті, що включає CIC-IDS2017 (веб-атаки), CSE-CIC-IDS2018 (хмарні сценарії) та CSIC 2010 HTTP (синтетичні атаки). Порівняння здійснювалося з бейзлайнами: RawTF, PCA, StaticCP (фіксований ранг R=10) та AutoCP

(CORECONDIA). Запропонований метод ТороСР продемонстрував найкращі результати:

- точність – 0,942 ± 0,008;
- прецизія – 0,938 ± 0,010;
- повнота – 0,948 ± 0,008;
- F1-міра – 0,943 ± 0,007.

Це перевищує найкращий бейзлайн (AutoCP) на 3,1 % за F1-мірою. Абляційне дослідження регуляризаційного коефіцієнта підтвердило, що оптимальне значення забезпечує автоматичний вибір рангу, який найкраще відповідає стабільним топологічним ознакам.

Візуалізація t-SNE латентних факторів сесій показала чітку сепарабельність класів (benign, SQLi, XSS, Command Injection), на відміну від бейзлайнів, де спостерігалося перекривання кластерів.

Запропонований підхід має високий потенціал для інтеграції в реальні пайплайни безпеки, оскільки усуває потребу в ручному виборі рангу тензора, підвищує інтерпретованість (тензорні фактори прямо вказують на ключові токени атак) та забезпечує стійкість до шуму. Серед подальших викликів у дослідженні можна визначити масштабованість для реального часу та шляхи її досягнення (приблизна персистентна гомологія, batch-обробка, апаратне прискорення).

Таким чином, інтеграція топологічного аналізу даних з тензорним розкладом відкриває нову парадигму виділення ознак для надійних систем автоматизованого пентестингу веб-застосунків.

Список використаних джерел

1. Bubenik P. Statistical topological data analysis using persistence landscapes. *Journal of Machine Learning Research*. 2015. Vol. 16, no. 1. P. 77–102.

2. Salem M., Mrian M. AI-Driven Penetration Testing: Automating Exploits with LLMs and Metasploit – A VSFTPD Case Study. *International Conference on New Trends in Information and Communication Technology*. 2025.

3. Dhadi S. P. R., Reddy J., Prasad G. N. R. Cognitive Attack Topology (CAT): A Topological Framework for Modeling and Detecting Human-Centric Cyber Attacks. *Preprints.org*. 2026.

4. Aizpurua B., Palmer S., Orús R. Tensor networks for explainable machine learning in cybersecurity. *Neurocomputing*. 2025.

5. Khan Z. I., Afzal M. M., Shamsi K. N. A comprehensive study on CICIDS2017 dataset for intrusion detection systems. *International Research Journal of Advanced Engineering Hub*. 2024.