НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

Редакційна колегія:

ГОРБАЧЕНКО Станіслав, д.е.н., професор

СОКОЛОВ Артем, д.т.н., професор

АХМАМЕТЬЄВА Ганна, к.т.н., доцент

РАЗІНКІН Нікіта, асистент кафедри

© НУ «Одеська юридична академія», 2025

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

Editorial Board:

GORBACHENKO Stanislav, Doctor of Economics, Professor

SOKOLOV Artem, Doctor of Engineering, Professor

AKHMAMETYEVA Anna, Candidate of Engineering, Associate Professor

RAZINKIN Nikita, Assistant

© National University "Odesa Law Academy", 2025

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

8. Abiona O. O., Oladapo O. J., Modupe O. T., Oyeniran O. C., Adewusi A. O., Komolafe A. M. The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline. *World Journal of Advanced Engineering Technology and Sciences*. 2024. Vol. 11, No. 2. P. 127-133. DOI: https://doi.org/10.30574/wjaets.2024.11.2.0093
9. Zhao X., Hoda R., Clear T., MacDonell S. G. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software*. 2024. Vol. 214. 112059. DOI: https://doi.org/10.1016/j.jss.2024.112059
10. Akbar M. A., Smolander K., Mahmood S., Alsanad A. Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*. 2022. Vol. 147. 106894. DOI: https://doi.org/10.1016/j.infsof.2022.106894

Ключові слова: безпека Android, Kotlin, Jetpack Compose, криптографія мобільних застосунків, DevSecOps, вразливості застосунків, захист даних.
Keywords: Android security, Kotlin, Jetpack Compose, mobile application cryptography, DevSecOps, application vulnerabilities, data protection.

КОНЦЕПЦІЯ ТА РОЗГОРТАННЯ ВИСОКОІНТЕРАКТИВНОГО ХАНІПОТУ НА НА ОСНОВІ ЕМУЛЯЦІЇ ЛЕГІТИМНОГО ВЕБСЕРВЕРА (NGINX)

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Ханіпотом (медовим горщиком) називають спеціальний пасивний засіб захисту — по суті, пастку, що є приманкою для шкідливого програмного забезпечення. По суті, це — спеціалізований пасивний засіб збору розвідувальних даних, що є приманкою для зловмисників та шкідливого ПЗ, основне завдання якого виявляти нові й цільові атаки Zero-day, які погано піддаються розпізнаванню традиційними методами [1].

Існуючі рішення для ханіпотів традиційно поділяються на дві основні категорії: низькоінтерактивні та високоінтерактивні. Низькоінтерактивні ханіпоти, як-от Cowrie (для емуляції SSH) або Dionaea (для мережевих сервісів), швидко емулюють лише необхідні аспекти реального сервісу, що робить їх економічними, але водночас вкрай вразливими до автоматизованого розпізнавання досвідченими ботами та зловмисниками. Натомість, високоінтерактивні ханіпоти використовують повну віртуалізацію операційної системи або сервісу, що вимагає значно більших ресурсів, але надає максимально детальні та цінні розвідувальні дані про поведінку атакуючого. Більшість готових комерційних та open-source рішень часто є гібридами, які намагаються знайти баланс між ресурсоємністю та глибиною взаємодії, проте їхня широка відомість і типові мережеві відбитки є головною вразливістю [2].

Сучасне шкідливе програмне забезпечення (malware) характеризується, з одного боку, постійним удосконаленням методів атаки та еволюцією засобів нападу, з іншого — високим рівнем використання автоматичних, практично “бездумних” засобів атаки [3].

Ботнети являють собою децентралізовані мережі, які складаються з мільйонів скомпрометованих пристроїв, включаючи традиційні сервери, робочі станції, а також пристрої Інтернету речей (IoT), що мають мінімальний рівень захисту. Саме широке використання IoT як вектора атаки стало ключовим фактором зростання ботнет-активності (зафіксовано зростання на 25% у 2023 році). Ботнети, такі як Torpig Mebroot або TorrentLocker, забезпечують зловмисників масштабованою платформою для розповсюдження шкідливого ПЗ, спаму та проведення DDoS-атак. Крім того, такі угруповання, як Volt Typhoon, використовують ботнети для прихованого проникнення та закріплення в мережах критичної інфраструктури, що вимагає вкрай складних методів виявлення, які не здатні забезпечити традиційні сигнатурні засоби[4].

Широке використання систем LLM призвело до того, що боти, з одного боку, швидко вдосконалюються та змінюються. З іншого боку, використання LLM значною мірою стандартизує та “шаблонізує” техніки, що використовуються ботами. У звіті [5] вказується вплив усіх перелічених вище факторів. Автоматизований трафік перевищив людський: Вперше автоматизований трафік (боти) становив 51% від усього інтернет-трафіку, перевищивши людський (49%). При цьому шкідливі боти (які часто є частиною ботнетів) зросли до 37% від усього веб-трафіку (це шостий рік поспіль зростання). Автори звіту роблять висновок про те, що доступність інструментів ШІ сприяла зростанню простих бот-атак (вони зросли до 45% усіх бот-атак), оскільки ШІ знизив поріг входу для зловмисників. Вплив ШІ двоякий: зростання простих, шаблонізованих атак (45% бот-трафіку, за Imperva) збільшує загальний шум, але ШІ також дозволяє ботам будь-якого класу швидше адаптуватися та мімікрувати, що робить їх більш ухильними (advanced evasion) від традиційних засобів захисту. Такий стан справ вимагає використання нетрадиційних засобів, що доповнюють традиційні (IDS/IPS/Firewalls).

Швидка еволюція та простота арсеналу сторони, що атакує, вимагає такого ж швидкого виявлення та аналізу атак. Це висуває ханіпоти, як систему, що дозволяє швидко зібрати інформацію та виявити можливі методи атаки, на перший план. Однією з проблем пропонованих готових рішень є їхня широка відомість — зокрема зловмисникам, що дозволяє вибудовувати системи протидії таким пасткам.

Пропонована система використовує як фронтенд вебсервер Nginx. Така схема дозволяє отримати одразу кілька переваг. Перше — це суттєва економія ресурсів як у процесі розробки ханіпоту (не потрібно створювати

блок, що відповідає за взаємодію з вебпротоколами), так і в процесі експлуатації (Nginx розрахований на максимізацію продуктивності та добре справляється там, де потрібне кешування), друге — використання реального вебсервера з усіма його властивостями та ознаками дозволяє замаскувати цільове призначення медової пастки та ввести атакуючого в оману. Використання реального, надійно сконфігурованого вебсервера дозволяє точно імітувати мережевий відбиток (network fingerprint) легітимної системи. Nginx генерує реалістичні заголовки відповідей (HTTP response headers) та обробляє мережеві запити з очікуваною швидкістю та поведінкою, що значно ускладнює автоматизоване виявлення пастки на основі відомих сигнатур, які використовують досвідчені зловмисники.

Системи, що використовують цю ідею в пілотному варіанті, були розгорнуті 27 липня 2025 року. На 01 листопада 2025 року було зібрано 136615 записів. Цікавим побічним ефектом експлуатації системи стала можливість проспостерігати в режимі реального часу зростання активності ботнетів, пов’язане з кількома великими DDoS-атаками: атаку на Cloudflare 2-го вересня [6], та атаку на сервери MMORPG Albion Online (офіційний звіт на форумі компанії [7]) 23 липня (рис.1).

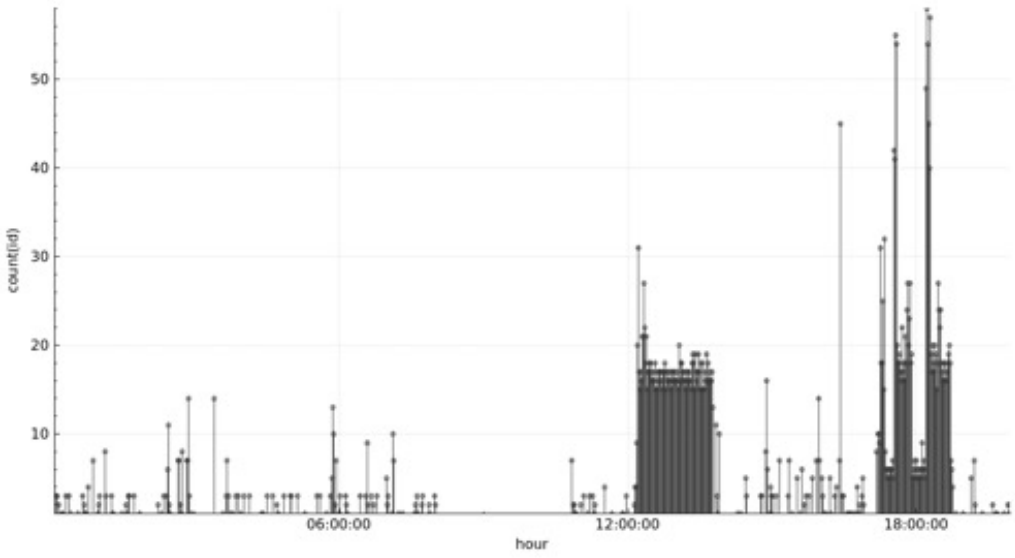

Рисунок 1 – Кількість атак 23-го липня 2025 року

Надалі така інформація може бути використана для прогнозування нових DDoS-атак, оскільки їхній початок, можливо, пов’язаний зі зростанням загальної активності ботнету, яку може виявляти пропонований ханіпот.

Список використаних джерел:

1. *Morić Z., Dakić V., Regvart D.* Advancing Cybersecurity with Honeypots and Deception Strategies // Informatics. MDPI, 2025. Т. 12. 14.
2. *Zou J., Sun Z., Ku C., Li X., Dahbura A.* WiP: Developing High-interaction Honeypots to Capture and Analyze Region-Specific Bot Behaviors // Proceedings of the Hot Topics in Security and Privacy (HotSoS). JHU Information Security Institute, 2024.

3. *Insikt Group, Recorded Future*. 2024 Malicious Infrastructure Report: Threat Intelligence Report. — Recorded Future, 2025.
4. *USTelecom*. Botnet and IoT Security Trends 2024: Industry Report. — USTelecom, 2024. — URL: https://ustelecom.org/wp-content/uploads/2024/03/USTelecom-Botnet-and-Security-Trends-2024.pdf.
5. *Imperva Threat Research, Thales*. 2025 Bad Bot Report: The Rapid Rise of Bots and The Unseen Risk for Business: Annual Report. — Imperva, 2025. — URL: https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/.
6. *SecurityOnline Info*. The Largest DDoS Attack in History: Cloudflare Fights Back. — https://securityonline.info/the-largest-ddos-attack-in-history-cloudflare-fights-back/, 2025.
7. *Sandbox Interactive, Albion Online Forum*. Resolved: Ongoing DDoS Attack & Compensation (Forum Post). — https://forum.albiononline.com/index.php/Thread/214699-Resolved-Ongoing-DDoS-Attack-Compensation/#post1442554, 2025.

Ключові слова: ханіпот, високоінтерактивний, nginx, ботнет, виявлення атак, zero-day, мережевий відбиток, емуляція, кібербезпека, автоматизований трафік, вебсервер, розвідувальні дані, ddos-атака, маскування, шкідливе пз, віртуалізація, журналювання, мережева інфраструктура, критична інфраструктура, сигнатури.
Keywords: honeypot, high-interaction, nginx, botnet, attack detection, zero-day, network fingerprint, emulation, cybersecurity, automated traffic, web server, threat intelligence, ddos attack, deception, malware, virtualization, logging, network infrastructure, critical infrastructure, signatures

МІЖНАБОРНЕ ТЕСТУВАННЯ МЕТОДУ KNN+TF-IDF У ЗАДАЧІ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ

Коробейнікова Тетяна
к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»
Кравчук Назар
аспірант, асистент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»

У сучасних вебзастосунках, що характеризуються великою кількістю динамічних інтеграцій і складною структурою даних, ризик появи ін'єкційних атак (SQLi, XSS, ін'єкцій команд) залишається одним із ключових викликів для систем кіберзахисту. Традиційні сигнатурні рішення IDS/WAF часто не здатні ефективно розпізнавати обфусковані або нові варіанти атак, тоді як моделі глибинного навчання вимагають значних обчислювальних ресурсів і не завжди забезпечують прозорість прийняття рішень. У попередній роботі нами було показано, що поєднання алгоритму k-найближчих сусідів (KNN) із TF-IDF-представленням текстових навантажень і додатковими структурно-статистичними ознаками дозволяє досягти високої ефективності виявлення ін'єкцій (до 99,77% точності та F_1=0,998) при низьких ресурсних витратах.

ЗМІСТ