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».

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».

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)

5. Нефедченко О., Алексахіна Т., Плохута Т. Евристичне навчання та штучний інтелект: сучасні тенденції у вищій освіті у вивченні іноземних мов. *Науковий вісник Вінницької академії безперервної освіти.* 2025. № 7. С. 164-169. DOI: https://doi.org/10.32782/academ-ped.psyh-2025-1.22

Ключові слова: LLM, чат-бот, Gemini, GPT-4, навчання.
Keywords: LLM, chatbot, Gemini, GPT-4, education.

ІНТЕГРАЦІЯ ФУНКЦІОНАЛУ ЧАТ-БОТІВ У СИСТЕМИ МОНІТОРИНГУ ВЕБ-СЕРВЕРІВ ДЛЯ ЗМЕНШЕННЯ ЧАСУ РЕАКЦІЇ НА КІБЕРЗАГРОЗИ

Бойко Віктор

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

Наконечний Микита

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному глобальному кіберпросторі зростаюча складність та частота виникнення кіберзагроз для веб-серверів становить суттєві складнощі для безперервного забезпечення роботи організацій що на них покладаються, також ліквідація наслідків та відновлення бізнес-процесів після інциденту це великі фінансові та репутаційні збитки. Одна з найголовніших причин зростання витрат на ліквідацію наслідків кіберінцидент, репутаційних, фінансових полягає у тривалому часі на виявлення та реагування на кіберінциденти.

Згідно дослідженням середній час реагування на кіберінцидент перебуває у межах 192 діб, якщо час виявлення кіберінциденту не перевищує 200 діб, то витрати на ліквідацію його наслідків будуть на 30% меншими у порівнянні з більш тривалими виявленнями, наприклад у США це різниця між 5,01 млн. та 3,87 млн. доларів сша [2]. Затримки у реагуванні дають змогу зловмисникам розширювати свій доступ та переривати бізнес-процеси. Одними з основних причин таких затримок як зазначено у статті становлять такі чинники як [1]. Великий обсяг кібератак та інцидентів, через постійні спроби атаки на сервер організаціям важко знайти коли і яка саме яка кіберзагроза з усіх виявлених була успішно реалізована зловмисником. Обмеження бюджету та знань, організації середнього та малого бізнесу можуть просто не мати необхідних бюджетів для підтримки постійного штату спеціалістів з кіберзахисту або не розуміти як захистити себе від кіберзагроз, навіть великі організації можуть бути вразливими до такого через скорочення бюджету. Недостаток інструментів, через який спеціалісти що реагують на

кіберінцидент не отримавши необхідний контекст втрачають час на аналіз незначних подій, ігноруючи або пропускаючи потенційно критичні інциденти.

Однак сучасні технології автоматизації моніторингу показують позитивну тенденцію щодо зменшення середнього часу реакції на кіберінциденти, у середньому на 6 днів у порівнянні з 2024 роком, що підтверджує правильність обраного методу. Проте такий результат хоч має позитивну тенденцію але все ще не є достатнім для своєчасного виявлення та нейтралізації загроз, що залишає простір для шкідливих дій потенційного зловмисника у межах півроку. Саме тому поєднання функціоналу чат-боту дозволить удосконалити систему автоматизованого моніторингу, та надати спеціалістам з кіберзахисту необхідний інструмент для своєчасного виявлення кіберінцидентів [2].

Для реалізації автоматичної системи моніторингу необхідно дотримуватись основної мети такої системи виявлення індикаторів компрометації на різних етапах з дотриманням стандартів, що дозволить швидко реагувати на потенцыйні кіберінциденти та зменшувати потенційні витрати на їх подальшу нейтралізацію. Робота такої системи складається з ключових фаз [3]:

- Збору даних – налаштування захоплення логів системи, мережі та технічних.
- Об'єднання даних – обробка виявлених подій для виявлення зв'язків між різними джерелами.
- Аналіз даних – виявлення аномальної активності у оброблених даних
- Вживання заходів – реагування на інцидент та усунення загроз, ліквідація наслідків.

Робота такої системи зустрічається з такими викликами, як великий обсяг оброблювальних даних, брак ресурсів та навичок персоналу в організаціях, складність аналізу та відокремлення логів за їх важливістю з отриманої інформації.

Для вирішення наведених викликів у системах моніторингу кібербезпеки дедалі частіше застосовуються автоматизовані інструменти, зокрема чат-боти які можуть бути реалізовані як з застосуванням штучного інтелекту так і реалізовані функціонально іінтегрований у систему моніторингу чат-бот буде виконувати ключові функції, своєчасного виявлення кіберінциденту на ранніх етапах, скорочення часу реакції через автоматичний аналіз подій у логах системи, пристроїв та мережі, координацію дій щодо нейтралізації загрози та реагування на кіберінцидент, а також збір та кореляцію що налаштовується через інтеграцію з SIEM (Security Information and Event Management) системами [4]. Зважаючи на необхідність чіткого порядку дій, та встановлених алгоритмів для аналізу і реагування на кіберінцидент, доцільним є використання

функціонального чат-боту, який буде працювати на основі статичних правил та шаблонів. Чат-боти такого типу забезпечують прямий контроль над процесами та спрощують керування завдяки передбачуваний логіці, знижуючи ризик непередбачуваних дій характерних для ШІ-систем. До переваг функціональних чат-ботів також відносять швидке налаштування, прозорість роботи, економію ресурсів мережі бо вони не потребують спеціального апаратного забезпечення для функціонування або часу на навчання та перенавчання. Чат-бот реалізований функціональним методом може автоматично генерувати сповіщення про подію та передавати їх для подальшого аналізу.

У цій доповіді пропонується доповнити системи автоматизованого моніторингу за веб-серверами, інтеграцією з функціональним чат-ботом який функціонує на основі визначених статичних правил та шаблонів. Такий підхід дозволяє вирішити питання надто високого часу реагування на кіберінциденти, підвищити ефективність виявлення кіберзагроз, сприяти централізованому управлінню подіями. Маючи можливість інтеграції з SIEM для збору аналізу і кореляції логів сервера. Основні функції включатимуть: автоматичне сканування логів на наявність аномалій, генерацію оповіщень та передачу їх до спеціалістів з кіберзахисту організації.

Список використаних джерел:

1. Verizon business – 2025 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/Tc9a/reports/2025-dbir-data-breach-investigations-report.pdf
2. AI driven cybersecurity chatbot for incident response. URL: https://ijarcce.com/wp-content/uploads/2024/05/IJARCCE.2024.13509.pdf
3. Cyber Security Monitoring and Logging Guide. URL: https://www.crest-approved.org/wp-content/uploads/2022/04/Cyber-Security-Monitoring-Guide.pdf
4. Tidmarsh D. The 3 Biggest Cyber Incident Response Challenges. URL: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/incident-response-challenges/

Ключові слова: SIEM, MTTI, MTTD, MTTR, управління кіберінцидентами, реагування на інциденти, виявлення інцидентів, автоматизація, моніторинг подій, час реагування, чат-бот, ChatOps, веб-сервери, аналіз трафіку.
Keywords: SIEM, MTTI, MTTD, MTTR, cybersecurity incident management, incident response, incident detection, automatization, event monitoring, response time, chatbot, ChatOps, web-servers, traffic analysis.

ЗМІСТ