Міністерство освіти і науки України
Івано-Франківський національний технічний університет нафти і газу
Інститут інформаційних технологій
Кафедра комп'ютерних систем і мереж

**Лизан Юрій Володимирович**

**УДК 004.05**

# БАКАЛАВРСЬКА РОБОТА

## Розробка ШІ-агента на основі фреймворку CrewAI для виявлення вразливостей API на прикладі проекту-гри RESTaurant API Game

Комп'ютерна інженерія
(назва освітньої програми)

123 - Комп'ютерна інженерія
(шифр і назва спеціальності)

Робота містить результати власних досліджень, використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело:

Здобувач освітнього ступеня _____ *Лизан Ю.В.*_____
(підпис, ініціали та прізвище здобувача)

Науковий керівник _____ *Пашкевич О.П., доцент*_____
(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

**Допущено до захисту**
Завідувач кафедри КСМ

*д.т.н.,професор*_____*С.І. Мельничук*
(посада) (підпис) (дата) (ініціали та прізвище)

**Івано-Франківськ – 2025 рік**

**Івано-Франківський національний технічний університет нафти і газу**
(повне найменування вищого навчального закладу)

Інститут *інформаційних технологій*

Кафедра *комп'ютерних систем і мереж*

Освітній ступінь *бакалавр*

Спеціальність *123 – Комп'ютерна інженерія*
(шифр і назва)

**ЗАТВЕРДЖУЮ**
**Завідувач кафедри КСМ**
**(С.І. Мельничук)**
**«___» _____ 2025 року**

# З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

**Лизану Юрію Володимировичу**
**(прізвище, ім'я, по батькові)**

1. **Тема проекту (роботи)** ***Розробка ШІ-агента на основі фреймворку CrewAI для виявлення вразливостей API на прикладі проекту-гри RESTaurant API Game***

**керівник проекту (роботи)** *Пашкевич О.П., доцент.*
**(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)**

затверджені наказом вищого навчального закладу від
«_05_ *» травня 2025 року № _275/7____*

**2. Строк подання студентом роботи** *12 червня 2025 р*.

**3. Вихідні дані до роботи** *Матеріали і результати отримані під час проходження переддипломної практики, методичні вказівки, технічна література.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити). 1. Аналіз сучасних методів виявлення вразливостей API та підходи розробки агентів ШІ. 2. Розробка технічного задвання для агента ШІ. 3. Розробка агента ШІ 4. Перевірка працездатності та продуктивності агента.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

**6. Консультанти розділів роботи**

| Розділ | **Прізвище, ініціали та посада консультанта** | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання 29.01.2025 р. .

## КАЛЕНДАРНИЙ ПЛАН

| **№ з/п** | **Назва етапів дипломного проекту (роботи)** | **Строк виконання етапів проекту (роботи)** | **Примітка** |
|---|---|---|---|
| 1 | Аналіз сучасних методів виявлення вразливостей API та підходи розробки агентів ШІ | *Лютий, 2025* | |
| 2 | Розробка технічного задвання для агента ШІ | *Березень- квітень 2025* | |
| 3 | Розробка агента ШІ | *Квітень-травень, 2025* | |
| 4 | Перевірка працездатності та продуктивності агента | *Травень, 2025* | |
| 5 | Оформлення роботи | *Червень, 2025* | |
| | | | |
| | | | |
| | | | |

**Студент** _____ *Лизан Ю.В.*
(підпис) (прізвище та ініціали)

**Керівник роботи** _____ *Пашкевич О.П.*
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Дослідження присвячене розробці агента штучного інтелекту (ШІ) для виявлення та усунення вразливостей у програмних інтерфейсах (API) у контрольованому середовищі, зокрема в Damn Vulnerable RESTaurant API. Робота акцентує увагу на зростанні складності та частоти кіберзагроз, підкреслюючи ключову роль ШІ у підвищенні рівня кібербезпеки, зокрема у захисті API. Агент ШІ, створений на базі фреймворку CrewAI та з використанням моделі Grok 3, автономно виявляє, виправляє та документує вразливості, такі як порушення авторизації на рівні об’єктів (BOLA), порушення автентифікації, підробка запитів на стороні сервера (SSRF) та інші, що входять до списку OWASP API Security Top 10. Агент застосовує методи машинного навчання, статичний аналіз коду (SAST) за допомогою інструментів, таких як Semgrep, та аналіз поведінки для виявлення аномалій і прогнозування потенційних загроз. Практичне значення роботи полягає у створенні автоматизованого рішення для кібербезпеки, яке може бути використано розробниками, етичними хакерами та інженерами з безпеки для вдосконалення навичок розробки безпечних API та тестування. Інтеграція агента в процеси DevSecOps та гейміфікований підхід до навчання підвищують його цінність у навчальних і професійних середовищах. Дослідження підкреслює важливість проактивних стратегій на основі ШІ для захисту цифрової інфраструктури від нових кіберзагроз, відповідаючи регуляторним вимогам, таким як GDPR та CCPA. Результати демонструють здатність агента ефективно вирішувати складні вразливості та створювати детальні звіти, відкриваючи шлях до масштабованої та адаптивної кібербезпеки.

**Ключові слова**: штучний інтелект, кібербезпека, захист API, виявлення вразливостей,

## ABSTRACT

The research focuses on the development of an artificial intelligence (AI) agent designed to detect and mitigate vulnerabilities in Application Programming Interfaces (APIs) within a controlled environment, specifically the Damn Vulnerable RESTaurant API. The study addresses the growing complexity and frequency of cyber threats, emphasizing the critical role of AI in enhancing cybersecurity, particularly in API protection. The AI agent, built using the CrewAI framework and powered by the Grok 3 model, autonomously identifies, fixes, and documents vulnerabilities such as Broken Object Level Authorization (BOLA), Broken Authentication, and Server-Side Request Forgery (SSRF), among others listed in the OWASP API Security Top 10. The agent leverages machine learning techniques, static code analysis (SAST) with tools like Semgrep, and behavioral analysis to detect anomalies and predict potential threats. The practical significance of the work lies in its contribution to automated cybersecurity solutions, offering a tool for developers, ethical hackers, and security engineers to practice secure API development and testing. The agent's integration into DevSecOps pipelines and its gamified approach to learning enhance its applicability in educational and professional settings. The research underscores the importance of proactive, AI-driven strategies to safeguard digital infrastructure against evolving cyber threats, aligning with regulatory requirements like GDPR and CCPA. The results demonstrate the agent's ability to effectively resolve complex vulnerabilities while generating detailed reports, paving the way for scalable and adaptive cybersecurity solutions.



**Keywords**: artificial Intelligence, cybersecurity, API Security, vulnerability detection