УДК 004.056.5:004.4

ІМПЛЕМЕНТАЦІЯ МЕТОДІВ DEVSECOPS В РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В СВІТЛІ СУЧАСНИХ ЗАГРОЗ

Приходько Я. О.
Науковий керівник – к.т.н., доц. Вечур О. В.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна
e-mail: yan.prykhodko.cpe@nure.ua

This work is devoted to the analysis of the key information security challenges for IT startups and consideration on the implementation of the DevSecOps methods and instruments to ensure secure development and data security. It analyzes the modern threats database in order to find the correlation to the DevSecOps instruments that mitigate corresponding security risks which provides a possibility for IT-companies to concentrate on specific aspects of security measures implementation based on the limitations caused by modern company environments and teams.

У сучасному інформаційному середовищі, де IT-стартапи стають ключовим елементом інноваційного розвитку, питання інформаційної безпеки набувають особливої актуальності та значення. Інформаційна безпека не лише захищає конфіденційні дані та інтелектуальну власність, але й впливає на довіру клієнтів, інвесторів та партнерів. У світлі сучасних загроз, забезпечення належного рівня безпеки вимагає обізнаності, ефективного використання ресурсів і відповідних стратегій [1].

Відповідь на сучасні кіберзагрози стає надзвичайно важливою у світлі сучасних загроз інформаційній безпеці. Для впровадження та забезпечення відповідного рівня інформаційної безпеки в IT-стартапах, розробники все частіше звертаються до DevSecOps практик. Однією з ключових переваг DevSecOps є можливість виявлення вразливостей на ранніх стадіях розробки, що дозволяє запобігати серйозним проблемам безпеки в майбутньому. Основні принципи DevSecOps включають [2]: зміщення безпеки вліво (на початок життєвого циклу розробки); тренінги з безпеки та культура робочого місця; спостереження (observability) та моніторинг; моделювання загроз та тестування безпеки; аналіз і визначення пріоритетів та усунення наслідків.

З метою ідентифікації та кластеризації метою ідентифікації та кластеризації загроз можна використати базу загальновідомих вразливостей інформаційної безпеки (Common Vulnerabilities and Exposures) [4]. Це дозволить пов'язати загрози з інструментами DevSecOps [3], що мають найбільшу актуальність та зрозуміти і пріоритезувати заходи безпеки, необхідні для інформаційних систем.

Для аналізу використовуються датасет Kaggle “CVE (Common Vulnerabilities and Exposures)” [4] та основні особливості з датасету CVE:

числовий рейтинг вразливості (cvss) та текстовий опис вразливостей (summary). Виконується очищення та підготовка даних. Текстові дані перетворюються в числовий формат за допомогою TF-IDF векторизації, щоб вони могли бути проаналізовані за допомогою алгоритмів машинного навчання. Застосовується метод Principal Component Analysis (PCA) [5] для зменшення розмірності комбінованих даних (текст + cvss), щоб спростити візуалізацію та аналіз. Формула PCA:

$$X\,pca = XW, \tag{1}$$

де X – вихідні дані, W – матриця ваг головних компонент.

Використовуючи метод кластеризації K-Means, дані розділяються на кластери, що представляють групи вразливостей з подібними характеристиками. Формула k-середніх:

$$arg\,min \sum_{i=1}^{k} \sum_{x \in S_i} \left\| x - \mu_i \right\|^2 \tag{2}$$

де S_i – і-тий кластер, x – точки даних, μ_i – центроїд і-того кластера.

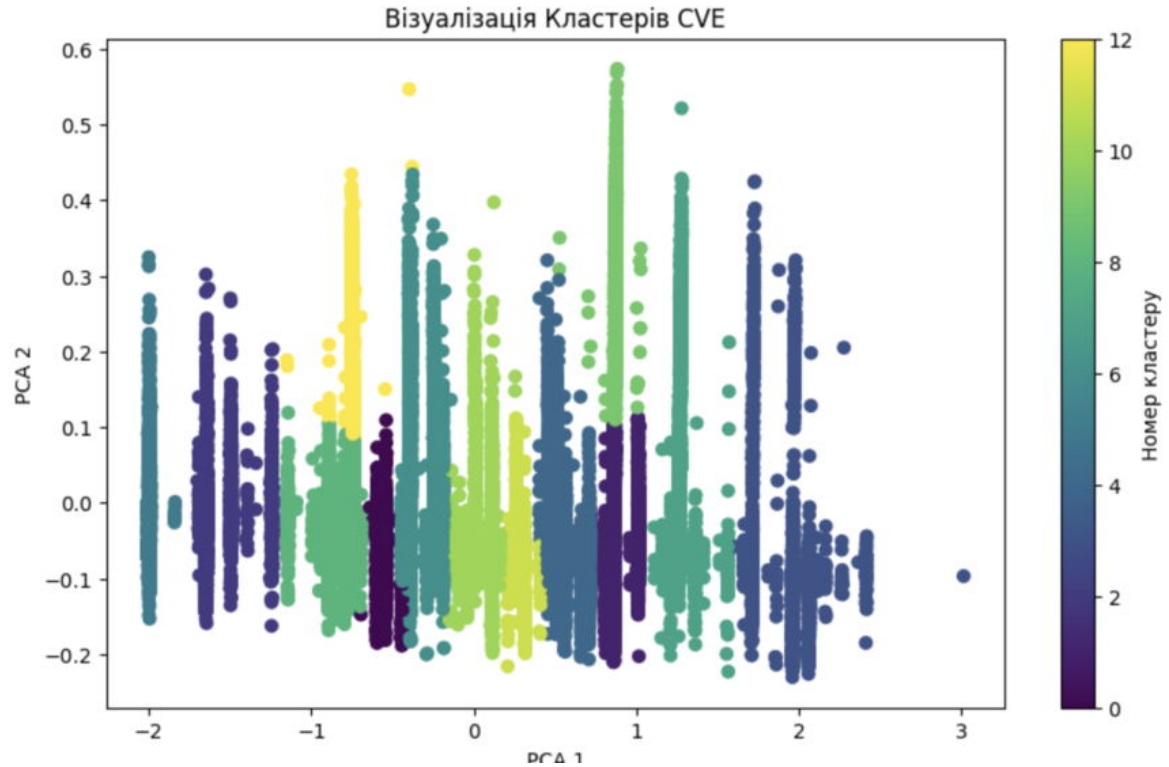

Рисунок 1 – Візуалізація результатів кластеризації

Дані, що були розподілені на кластери, марковані для відповідності інструментам DevSecOps[3] на основі ознак вразливостей (ключів) із бази загальновідомих вразливостей, відсортовані за рівнем актуальності відображено у таблиці 1:

Таблиця 1 – Результати кластеризації та відповідні інструменти

Кластер	Актуальність	Кількість вразливостей	Інструмент (назва)
5	10.000000	4504	Інструменти зберігання секретів
2	9.224815	7577	Інструменти сканування коду
8	7.582385	9479	Інструменти захисту мережі
12	7.501287	4847	Інструменти зберігання та перегляду логів
0	7.171997	3375	Інструменти зберігання та перегляду метрик
6	6.716870	12930	Інструменти тестування на проникнення

Таким чином, за результатами кластеризації, відповідно до актуальності інструментів, що покривають велику кількість DevSecOps, для усунення та запобігання загальновідомих загроз при впровадженні інформаційної безпеки проекту програмного забезпечення особливу увагу слід зосередити на інструментах для зберігання секретів, сканування коду, захисту мережі, моніторингу, а також інструментах тестування на проникнення. Це допомагає встановити пріоритети в інвестиціях у інструменти безпеки та стратегії DevSecOps.

Список використаних джерел:

1. Ayman Elsawah. “5 Problems With Startup Security” : вебсайт URL: https://www.lastweekasavciso.com/p/5-problems-with-startup-security (дата звернення 04.02.2024).

2. Microsoft. “What is DevSecOps?” : вебсайт. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops (дата звернення 04.02.2024).

3. Bright Security. “DevSecOps: Quick Guide to Process, Tools, and Best Practices : вебсайт. URL: https://www.hackerone.com/knowledge-center/devsecops-quick-guide-process-tools-and-best-practices (дата звернення 04.02.2024).

4. Kaggle. “CVE (Common Vulnerabilities and Exposures)” : вебсайт URL: – https://www.kaggle.com/datasets/andrewkronser/cve-common-vulnerabilities-and-exposures?select=cve.csv (дата звернення 04.02.2024).

5. Christopher M. Bishop "Pattern Recognition and Machine Learning": 1st ed. 2006. Corr. 2nd printing 2011; Springer New York publisher. – 738 p.