УДК 004.415

ВИКОРИСТАННЯ DOCKER ДЛЯ СПРОЩЕННЯ РОЗРОБКИ ТА ДЕПЛОЮ ЗАСТОСУНКІВ

Косенко М.А.
e-mail: mykola.kosenko@nure.ua
Харківський національний університет радіоелектроніки, кафедра РТІКС
м. Харків, Україна

This article explores the role of Docker in modern application development and deployment. It discusses the advantages of containerization, the process of creating and managing containers, and the international regulatory frameworks that impact software deployment. The study highlights the importance of using standardized environments for development and ensures efficient, scalable, and portable application deployment.

У сучасній розробці програмного забезпечення важливо забезпечити узгоджене середовище на всіх етапах життєвого циклу застосунку. Docker став потужним інструментом, що спрощує ці процеси завдяки технології контейнеризації. Використання ізольованих середовищ гарантує стабільну роботу застосунків на різних платформах, усуваючи проблеми сумісності, які традиційно ускладнюють роботу розробників. Завдяки інкапсуляції всіх залежностей, бібліотек і конфігурацій у контейнер, Docker забезпечує плавний перехід від розробки до тестування і продакшн-середовища.

Однією з ключових переваг Docker є здатність ефективно масштабувати застосунки. Завдяки контейнеризації розробники можуть швидко розгортати кілька екземплярів програми для задоволення зростаючих потреб користувачів. Це особливо важливо для архітектур, заснованих на мікросервісах, де кожен компонент працює незалежно у власному контейнері. Такий підхід підвищує надійність і підтримуваність системи, зменшуючи ризик загального збою.

Окрім розробки та розгортання, важливими аспектами залишаються безпека та відповідність міжнародним стандартам. Регулювання у сфері захисту даних і кібербезпеки, такі як Загальний регламент про захист даних (GDPR, Regulation (EU) 2016/679), Закон США про перенесення та відповідальність медичного страхування (HIPAA, Public Law 104-191) і Директива про платіжні послуги 2 (PSD2, Directive (EU) 2015/2366), встановлюють жорсткі вимоги до обробки персональних даних. Крім того, Рамкова програма кібербезпеки Національного інституту стандартів і технологій США (NIST Cybersecurity Framework) та рекомендації Агентства з кібербезпеки та інфраструктурної безпеки США (CISA) визначають найкращі практики захисту контейнеризованих середовищ. Можливості Docker щодо впровадження надійних механізмів безпеки, таких як контроль доступу, шифрування мережевих з'єднань і регулярне сканування на вразливості, допомагають організаціям відповідати цим вимогам та захи-

щати конфіденційні дані.

Для ефективного використання Docker розробники зазвичай створюють Dockerfile, який визначає середовище застосунку та його залежності. Цей файл слугує основою для створення образу Docker, що може бути запущений на будь-якому пристрої з Docker. Після створення контейнерів їх можна легко запускати, гарантуючи однаковість середовищ розробки, тестування та продакшну. Для застосунків, що складаються з кількох сервісів, Docker Compose дозволяє зручно керувати взаємопов'язаними контейнерами.

Вплив Docker на сучасну розробку програмного забезпечення важко переоцінити. Використання стандартизованих середовищ мінімізує розбіжності між етапами розробки та продакшну. Контейнеризація сприяє підвищенню ефективності, спрощує процеси деплою та покращує безпеку, роблячи Docker незамінним інструментом у сучасній розробці застосунків. Організації та розробники, що впроваджують Docker у свої робочі процеси, отримують переваги у вигляді гнучкості, масштабованості та відповідності міжнародним стандартам кібербезпеки і захисту даних.

Список використаних джерел:

1. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191. [Електронний ресурс]. – Режим доступу: https://www.hhs.gov/hipaa

3. Payment Services Directive 2 (PSD2) – Directive (EU) 2015/2366. [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/eli/dir/2015/2366/oj

4. National Institute of Standards and Technology (NIST) Cybersecurity Framework.. [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework

5. Cybersecurity & Infrastructure Security Agency (CISA). Cyber Hygiene Services. [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/cyber-hygiene-services