УДК 004.056
Шевченко В.Ф.[1], Киричек Г.Г.[2]
[1] студ. гр. КНТ-515м НУ «Запорізька політехніка»
[2] доц. НУ «Запорізька політехніка»

# РИЗИКИ ТА СТРАТЕГІЯ БЕЗПЕКИ ПРИ РОЗГОРТАННІ КОНТЕЙНЕРИЗОВАНИХ ДОДАТКІВ У ХМАРНИХ СЕРЕДОВИЩАХ

Сучасна парадигма розробки програмного забезпечення базується на принципах мікросервісної архітектури та широкому використанні контейнерних технологій, зокрема таких платформ, як Kubernetes та Docker [1]. Контейнеризація забезпечує гнучкість, масштабованість і швидкість розгортання додатків, однак одночасно формує нові виклики у сфері кібербезпеки. Актуальність дослідження зумовлена необхідністю побудови ефективних механізмів захисту в умовах інтеграції хмарних середовищ із корпоративною інфраструктурою, зокрема системами управління ідентифікацією та доступом.

Метою роботи є аналіз основних ризиків безпеки контейнеризованих додатків у хмарних середовищах та розробка ефективних стратегій їх мінімізації. Для досягнення поставленої мети визначено такі задачі: ідентифікація ключових загроз; аналіз вразливостей контейнерних середовищ; дослідження механізмів контролю доступу та формування багаторівневої моделі захисту. Об'єктом дослідження виступають процеси розгортання та експлуатації контейнеризованих додатків у хмарних середовищах. Предметом дослідження є методи та засоби забезпечення безпеки контейнерної інфраструктури.

У роботі проведено комплексний аналіз ризиків інформаційної безпеки, що виникають при використанні контейнеризованих технологій у хмарних середовищах [2]. Розглянуто основні вектори атак, пов'язані з використанням платформ контейнеризації та оркестрації, а також запропоновано багаторівневу модель захисту на основі концепції Defense in Depth. Особливу увагу приділено інтеграції хмарних сервісів із корпоративними системами управління ідентифікацією, що дозволяє підвищити рівень контролю доступу та мінімізувати ризики несанкціонованого доступу. Запропоновано інтегровану модель безпеки контейнеризованих середовищ, яка поєднує механізми централізованого управління ідентифікацією з технологіями динамічного моніторингу та аналізу вразливостей, що дозволяє підвищити рівень захищеності хмарної інфраструктури [3]. Експлуатація контейнерних середовищ, таких як Containerd, супроводжується низкою критичних загроз. По-перше, використання неперевірених або застарілих образів із публічних репозиторіїв може призводити до впровадження вразливостей, ідентифікованих у базах CVE. По-друге, існує ризик компрометації ізоляції

контейнерів, що дозволяє зловмиснику отримати доступ до кінцевої операційної системи через експлуатацію спільного ядра. По-третє, значну небезпеку становлять помилки конфігурації, зокрема запуск контейнерів із надлишковими привілеями. Додатково, відсутність належної мережевої сегментації сприяє реалізації атак типу горизонтального переміщення всередині кластера. Для забезпечення належного рівня безпеки доцільно застосовувати багаторівневу модель захисту Defense in Depth, яка передбачає поєднання організаційних та технічних заходів. Ключовим елементом є централізоване управління ідентифікацією (IAM), яке реалізується через інтеграцію з корпоративними каталогами, зокрема Active Directory. Використання протоколів LDAP, SAML та OIDC забезпечує федеративне управління ідентифікацією. Це дозволяє реалізувати централізовану автентифікацію та ефективне рольове управління доступом, синхронізуючи корпоративні групи з ролями у кластері.

Практична апробація запропонованих підходів здійснена на прикладі проєкту «Vision Link», у межах якого реалізовано розгортання сервера BigBlueButton із інтеграцією в LDAP-інфраструктуру. Такий підхід забезпечує автоматичне управління доступом до ресурсів: деактивація облікового запису користувача в каталозі призводить до негайного блокування доступу до всіх пов'язаних сервісів, що суттєво знижує ризики інсайдерських загроз. На технологічному рівні ефективними є підходи Shift Left, які передбачають інтеграцію засобів сканування вразливостей, таких як Trivy та Clair, у CI/CD пайплайни. Додатково застосовуються інструменти runtime-захисту, зокрема Falco, які дозволяють виявляти аномальну поведінку в реальному часі.

Проведений аналіз показав, що безпека контейнеризованих додатків у хмарних середовищах є комплексною задачею, яка потребує поєднання технічних і організаційних заходів. Основними ризиками є вразливості образів, порушення ізоляції, надлишкові привілеї та недостатня мережна сегментація. Запропонована модель Defense in Depth із інтеграцією IAM та RBAC, а також використання сучасних інструментів сканування і моніторингу, дозволяє суттєво знизити рівень загроз.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Burns B., Grant B., Oppenheimer D., Brewer E., Wilkes J. Borg, Omega, and Kubernetes: Lessons learned from three container-management systems over a decade. *Queue*, 2016. 14.1. P.70-93. DOI: https://doi.org/10.1145/2898442.2898444

2. Киричек Г.Г., Тягунова М.Ю., Смірнов В.В. Реалізація технологій для розгортання програм у контейнері. *Таврійський науковий вісник. Серія:*

*Технічні науки*. 2023. №6. С.26-34. DOI: https://doi.org/10.32782/tnv-tech.2023.6.4

3. Придибайло О. Б., Придибайло Р. В. Роль контейнеризації у хмарних обчисленнях. *Зв'язок*, 2025. №4. С.92-98. DOI: https://doi.org/10.31673/2412-9070.2025.042607