

Секція 1

**ДОСЛІДЖЕННЯ ШЛЯХІВ ПІДВИЩЕННЯ БЕЗПЕКИ В
КОНТЕЙНЕРАХ KUBERNETES: АНАЛІЗ ТА ПРАКТИЧНІ
РЕКОМЕНДАЦІЇ**

Власов Ю. О.

Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Узун Д. Д.

Актуальність. З ростом використання Kubernetes у хмарних середовищах збільшується і ймовірність потенційних атак на безпеку даних. Розуміння та управління безпекою в Kubernetes стає ключовою проблемою для забезпечення стійкості системи від можливих загроз. Результат також показує, що 94% організацій стикалися принаймні з одним інцидентом безпеки за останні 12 місяців, серед яких 69% проблем безпеки пов'язані з неправильною конфігурацією [1]. З моменту свого започаткування у 2014 році Kubernetes встановив себе як фактичний інструмент для автоматизованої оркестрації контейнерів [2]. Хвиля вразливостей ядра Linux, таких як Dirty COW, які можуть бути використані для виходу з контейнерів, збільшила страхи щодо недостатньої ізоляції контейнерів [3]. Додатково, згідно з доповіддю IBM про вартість порушення захищеності даних, середні витрати на наслідки порушення захищеності даних у 2023 році становлять 4,35 мільйона доларів, що на 13% більше, ніж у 2020 році, що ілюструє масштаб цих проблем безпеки [4].

Метою даного дослідження є аналіз інструментів та методів забезпечення безпеки в Kubernetes та розробка практичних рекомендацій щодо підвищення рівня безпеки в масштабованих кластерах.

Основні положення. Аналізуючи ринок хмарних технологій, виявлено, що Kubernetes стає основним інструментом для розгортання та управління додатками в хмарних та гібридних середовищах. Однак, зростання використання Kubernetes призводить до збільшення кількості потенційних атак та вразливостей, що потребує комплексного підходу до забезпечення безпеки. Для ефективного захисту середовища виконання програм у Kubernetes використовуються різноманітні інструменти та підходи. На етапах до та під час виконання програми активно використовуються такі засоби: Kubesec, OPA GateKeeper, Falco, AppArmor Seccomp, та ін. Крім того, принципи, такі як принцип найменшого доступу, захист на всіх рівнях і безпека на основі дизайну, є ключовими стратегіями у розробці безпечних систем [5]. У роботі проведено аналіз переваг та недоліків різних

інструментів, а також надано рекомендації з їх ефективного використання для комплексного захисту системи від потенційних загроз на всіх етапах роботи та обслуговування.

Висновки. Дослідження показує необхідність постійного вдосконалення стратегій безпеки в Kubernetes та активної участі спеціалістів у забезпеченні безпеки в хмарних середовищах. Рекомендації безпеки включають у себе використання інструментів моніторингу загроз, виявлення вразливостей та заходів з підвищення безпеки в масштабованих Kubernetes-кластерах.

Список літератури

1. Shamim S. I. Mitigating security attacks in kubernetes manifests for security best practices violation. ESEC/FSE '21: 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, м. Athens Greece. New York, NY, USA, 2021. DOI: <https://doi.org/10.1145/3468264.3473495>.
2. Security Misconfigurations in Open Source Kubernetes Manifests: An Empirical Study / A. Rahman та ін. ACM Transactions on Software Engineering and Methodology. 2023. DOI: <https://doi.org/10.1145/3579639>.
3. Viktorsson W., Klein C., Tordsson J. Security-Performance Trade-offs of Kubernetes Container Runtimes. 2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), France, 2020. DOI: <https://doi.org/10.1109/mascots50786.2020.9285946> (дата звернення: 01.05.2024).
4. IBM Data Breach. *IBM*. URL – <https://www.ibm.com/reports/data-breach> (дата звернення: 01.05.2024).
5. Saltzer J. H., Schroeder M. D. The protection of information in computer systems. Proceedings of the IEEE. 1975. Volume 63(9). Page 1278–1308. DOI: <https://doi.org/10.1109/proc.1975.9939>.

Відомості про авторів

Власов Юрій Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.vlasov@student.csn.khai.edu
 Узун Дмитро Дмитрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, d.uzun@csn.khai.edu