ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБРОБКИ ВЕЛИКИХ ДАНИХ У МУЛЬТИТЕНАНТНИХ ХМАРНИХ АРХІТЕКТУРАХ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ ВИРОБНИЧИХ СИСТЕМ

Сердюк Н.М., Вольгуст М.С.

Харківський національний університет
радіоелектроніки, Україна.

E-mail: nataliya.serdyuk@nure.ua,
maksym.volhust@nure.ua

Abstract

This paper addresses the problem of ensuring cybersecurity in multitenant cloud architectures applied to intelligent manufacturing systems. The study focuses on mechanisms of data isolation and access control, which are essential for protecting information and maintaining operational stability under conditions of continuous production. Key security tools such as Kubernetes Namespaces, Network Policies, Role-Based Access Control (RBAC), and TLS encryption are analyzed in the context of preventing unauthorized access and mitigating cyber threats. A practical example based on the operation of heat exchangers in the food industry demonstrates the effectiveness of multitenant architectures in avoiding data leakage, ensuring fault tolerance, and maintaining system reliability under peak loads or potential cyberattacks. The results confirm that multitenant cloud systems can simultaneously solve the tasks of big data management and the formation of resilient cyber defense strategies for industrial enterprises.

Інтелектуальні виробничі системи генерують великі обсяги даних у реальному часі, що створює значні виклики для їхньої обробки, зберігання та захисту. Мультитенантна архітектура хмарних систем дозволяє вирішувати проблему масштабування та забезпечувати ефективний розподіл обчислювальних ресурсів між клієнтами [1]. Водночас саме мультитенантність створює нові виклики для кібербезпеки, оскільки підвищується ризик витоку або несанкціонованого доступу до даних. Особливу небезпеку становлять можливі кібератаки на хмарну інфраструктуру, які можуть призвести не лише до економічних втрат, а й до порушення безперервності технологічних процесів та блокування критичного обладнання.

Метою роботи є аналіз та удосконалення механізмів ізоляції даних і контролю доступу в мультитенантних хмарних системах з урахуванням актуальних кіберзагроз, а також оцінка їх ефективності для забезпечення безпеки інтелектуальних виробничих процесів.

Для досягнення поставленої мети необхідно:

- проаналізувати особливості функціонування мультитенантних хмарних архітектур у виробничих середовищах;
- ідентифікувати основні кіберзагрози, пов’язані з обробкою великих даних у мультитенантних системах;
- визначити механізми ізоляції даних та контролю доступу, що забезпечують багаторівневий захист інформації;
- оцінити практичну ефективність застосування цих механізмів на прикладі виробничих процесів;
- розробити рекомендації щодо підвищення стійкості та захищеності хмарних систем в умовах кіберзагроз.

Мультитенантна архітектура дозволяє одночасно обслуговувати кілька виробничих підрозділів чи клієнтів на спільній інфраструктурі. Завдяки контейнеризації та оркестрації (Docker, Kubernetes)

система забезпечує ізоляцію середовищ, динамічне масштабування ресурсів і підтримку безперервності виробничих процесів навіть у режимі пікових навантажень.

Серед ключових загроз можна визначити: витік даних між тенантами, несанкціонований доступ до критичної інформації, компрометація облікових записів користувачів, перехоплення або модифікація даних у мережі, а також атаки на бази даних і сенсорні системи, що можуть призвести до спотворення виробничих параметрів та аварійних зупинок [2].

Так, виробнича лінія з обслуговування теплообмінників у харчовій промисловості. працює у режимі безперервного навантаження та генерує великі масиви даних від десятків сенсорів: температуру, тиск, швидкість потоку теплоносія [3]. Традиційна інформаційна система при пікових навантаженнях часто стикається з перевантаженням бази даних та уповільненням обробки запитів, переривання чи спотворення даних сенсорів унаслідок кібератаки може призвести до аварії обладнання. А мультитенантна архітектура з багаторівневим захистом зменшує ці ризики. У мультитенантній архітектурі завдяки ізоляції середовищ кожен підрозділ підприємства отримує власний контейнер із виділеними ресурсами. Якщо одна лінія виробництва різко збільшує обсяг даних, система автоматично масштабує кількість контейнерів і розподіляє навантаження без впливу на інші підрозділи. У результаті підприємство уникає простоїв, забезпечує своєчасне технічне обслуговування обладнання та знижує ризик аварійних зупинок виробництва.

Але однією з ключових проблем мультитенантних систем є загроза несанкціонованого доступу або витоку даних. Для її вирішення застосовуються кілька рівнів захисту:

- ізоляція середовищ у Kubernetes, що використовує Namespaces для кожного тенанта та дозволяє відокремлювати обчислювальні процеси та уникати взаємного впливу;
- мережеві політики (Network Policies), які контролюють взаємодію між контейнерами та запобігають доступу одного клієнта до ресурсів іншого;
- Role-Based Access Control (RBAC), що визначає права доступу користувачів відповідно до їхніх ролей, забезпечуючи суворе дотримання політик безпеки;
- шифрування TLS гарантує захист даних при передачі між підсистемами та зовнішніми сервісами.

Завдяки цим механізмам мультитенантна архітектура може підтримувати високу надійність і конфіденційність навіть за умов великої кількості одночасних клієнтів. Основні засоби забезпечення кібербезпеки у мультитенантних хмарних середовищах наведені у табл.1.

Таблиця 1. Основні засоби забезпечення кібербезпеки у мультитенантних хмарних середовищах

Механізм	Призначення	Приклад реалізації	Роль у кіберзахисті
Namespaces (Kubernetes)	Ізоляція середовищ для кожного тенанта	Виділення ресурсів	Запобігає перетину даних між клієнтами та проникненню зловмисних процесів
Network Policies	Контроль мережевих з'єднань	Заборона доступу між контейнерами	Блокує несанкціоновану взаємодію, зменшує ризик lateral movement у разі атаки
RBAC	Розмежування прав доступу користувачів	Ролі «адмін», «тенант»	Мінімізує наслідки компрометації облікових записів, обмежує можливості зловмисників
TLS-шифрування	Захист даних при передачі	HTTPS, gRPC secure	Унеможливлює перехоплення та модифікацію даних у мережі

Таким чином, до основних механізмів ізоляції даних та контролю доступу, що забезпечують багаторівневий захист інформації віднесено Namespaces у Kubernetes, які забезпечують ізоляцію середовищ; мережеві політики (Network Policies), що обмежують взаємодію контейнерів; контроль доступу на основі ролей (RBAC), який мінімізує наслідки компрометації облікових записів; а також TLS-шифрування для захисту даних при передаванні у мережі.

На прикладі експлуатації теплообмінників у харчовій промисловості продемонстровано, що мультитенантна архітектура з багаторівневим захистом дозволяє уникати перевантажень і простоїв, своєчасно масштабувати ресурси, гарантувати конфіденційність даних сенсорів і мінімізувати ризики аварійних зупинок навіть у випадку спроб зовнішнього втручання чи кібератаки.

Рекомендовано впроваджувати багаторівневу модель кіберзахисту з комбінацією механізмів ізоляції, контролю доступу та шифрування; застосовувати постійний моніторинг і аудит безпеки в Kubernetes-середовищах; інтегрувати AI/ML-алгоритми для виявлення аномалій у роботі виробничих систем; а також адаптувати архітектуру під вимоги міжнародних стандартів кібербезпеки для промислових підприємств України та ЄС.

Мультитенантні хмарні системи демонструють високу ефективність в управлінні великими даними інтелектуальних виробництв. Використання контейнеризації та оркестрації забезпечує ізоляцію середовищ, динамічний розподіл ресурсів і надійний захист даних у режимі реального часу. Практичне застосування, зокрема у виробничих лініях теплообмінників у харчовій та енергетичній промисловості, підтверджує здатність такої архітектури підтримувати безперервну роботу обладнання навіть при різкому зростанні навантажень. Система дозволяє уникати простоїв, підвищує стабільність і безпеку процесів, а також знижує витрати на інфраструктуру завдяки спільному використанню ресурсів. Запропонована архітектура відповідає сучасним вимогам кібербезпеки до хмарних виробничих систем і може стати основою для формування стратегії кіберзахисту промислових підприємств. Подальші дослідження можуть бути спрямовані на інтеграцію більш складних AI/ML-рішень для прогнозування технічних збоїв та нейтралізації кіберзагроз.

*Л*ітература

1. Serdiuk N., Volhust M. Advantages of the cloud information system architecture with multitenant support // XI International conference "Information Technology and Implementation" (IT&I-2024) satellite conference. – Kyiv, Ukraine, 21 November 2024. – [Електронний ресурс]. – Режим доступу: http://iti.fit.univ.kiev.ua/en/archive/

2. Сердюк Н.М., Вольгуст М.С. Ефективне управління великими даними в інтелектуальних виробництвах через мультитенантні хмарні системи // Наукові праці Донецького національного технічного університету, серія "Проблеми моделювання та автоматизації проектування". – 2025. – №1 (21). – [Електронний ресурс]. – Режим доступу: https://pmap.donntu.edu.ua/uk/issues/no121-2025

3. Ilyunin O., Bezsonov O., Rudenko S., Serdiuk N., Udovenko S., Kapustenko P., Plankovsky S., Arsenyeva O. The neural network approach for estimation of heat transfer coefficient in heat exchangers considering the fouling formation dynamic // Thermal Science and Engineering Progress. – 2024. – Vol. 51. – P. 102615. – [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2451904924002336