УДК 004.056.5:004.738.5

КІБЕРЗАХИСТ МІКРОСЕРВІСНОЇ IIOT-АРХІТЕКТУРИ ВИРОБНИЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Уляна ПАНОВИК[1,2], Богдана ФЕДИНА[1,2], Діана РІВНЯК[1]
[1]Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Анотація. *Розглянуто підхід до кіберзахисту виробничих інформаційних систем на основі мікросервісної архітектури IIoT. Запропоновано багаторівневу модель, що поєднує VPN, TLS, Zero Trust Policy Engine, контейнерну ізоляцію та моніторинг з аудитом. Такий підхід забезпечує захищене передавання даних, автентифікацію сервісів і контроль поведінки компонентів. Модель формує єдиний захисний контур від сенсорів до хмарних сервісів, підвищуючи стійкість і довіру до промислових даних.*

Ключові слова: *кіберзахист, IIoT, мікросервісна архітектура, Zero Trust, TLS, VPN, контейнерна безпека.*

Abstract. *The approach to cybersecurity of industrial information systems based on a microservice IIoT architecture is considered. A multilayer model is proposed that combines VPN, TLS, Zero Trust Policy Engine, container isolation, and monitoring with auditing. This approach ensures secure data transmission, service authentication, and component behavior control. The model forms a unified security contour from sensors to cloud services, increasing resilience and trust in industrial data.*

Keywords: *cybersecurity, IIoT, microservice architecture, Zero Trust, TLS, VPN, container security*

Сучасні виробничі системи переходять до архітектури IIoT, де сенсори, контролери та аналітичні модулі взаємодіють через мікросервісні інтерфейси. Така децентралізація підвищує гнучкість, але й збільшує ризики — від доступу до даних сенсорів до атак на контейнери. Традиційні засоби, як VPN чи TLS, захищають лише канали зв'язку, не контролюючи довіру між сервісами. Тому актуальним стає багаторівневий підхід до кіберзахисту з урахуванням контексту взаємодії елементів. Використання принципу security-by-design дозволяє вбудовувати захист у мікросервіси, API-шлюзи та політики доступу, поєднуючи шифрування, контроль ресурсів і виявлення аномалій.

У промислових системах IIoT безпека охоплює всі рівні — від сенсорів до хмарних сервісів. Висока взаємопов'язаність компонентів, динамічне масштабування контейнерів і використання відкритих протоколів (MQTT, REST API) створюють нові вектори атак, недоступні для класичних методів захисту. Оскільки кожен мікросервіс має власні політики доступу та автономне розгортання, ефективний кіберзахист потребує комплексного підходу, що поєднує мережеві, прикладні та поведінкові технології [1].

Базовими механізмами захисту в IIoT-системах залишаються VPN і TLS технології. VPN забезпечує створення захищених тунелів між вузлами, ізоляцію від публічних мереж і захист управлінських команд. Сучасні рішення (WireGuard, OpenVPN) відзначаються високою швидкодією, однак не усувають ризик внутрішніх атак, тому використовуються як частина багаторівневого захисту. TLS гарантує конфіденційність і автентичність даних у мікросервісних обмінах, зокрема через сертифікати X.509. Його реалізація у брокерах MQTT чи API-шлюзах потребує належного керування ключами та ротації сертифікатів, інакше можливе створення лише ілюзії безпеки без фактичного контролю ідентичності [2].

Концепція Zero Trust Architecture (ZTA) усуває довіру за замовчуванням: кожен запит автентифікується й авторизується незалежно від джерела. У IIoT це означає цифрову ідентичність для кожного сенсора, шлюзу чи сервісу, а рішення про доступ приймає Policy Engine, що знижує ризик внутрішніх атак. Контейнерна безпека (Docker, Kubernetes, AppArmor, SELinux, Falco) ізолює мікросервіси й контролює їхню поведінку, запобігаючи поширенню компрометацій. IDS/IPS аналізують трафік і виявляють аномалії на рівні edge-пристроїв. Таким чином, поєднання VPN, TLS, Zero Trust, контейнерної ізоляції та IDS/IPS формує проактивну, багаторівневу систему кіберзахисту IIoT.

Виробнича система на базі IIoT — це багаторівнева структура, де апаратні, комунікаційні й аналітичні компоненти взаємодіють через мікросервіси. Така архітектура підвищує гнучкість, але створює нові вразливості, тому захист має охоплювати всі рівні. Зазвичай виокремлюють три: польовий, edge/gateway і центральний. Польовий рівень охоплює сенсори й контролери, що потребують локального шифрування та автентифікації. Edge-рівень — шлюзи, брокери MQTT/AMQP і мікросервіси, де використовуються VPN, TLS, контейнерна ізоляція й Zero Trust. Центральний рівень включає аналітику, бази даних і SCADA/HMI з реалізацією RBAC, IDS/IPS та аудиту. Ефективний кіберзахист досягається лише інтеграцією цих рівнів — від достовірності даних до захищеного управління.

Побудова кіберзахисту виробничої IIoT-системи повинна розпочинатися ще на етапі її проєктування, коли визначаються логіка взаємодії сервісів, канали обміну даними та механізми автентифікації. Концепція security-by-design передбачає інтеграцію безпеки не як додаткового модуля, а як невід'ємної частини архітектури — із закладеними політиками шифрування, контролю доступу та моніторингу. У межах запропонованої моделі кіберзахисту мікросервісної IIoT-архітектури використовуються взаємопов'язані рівні безпеки, які формують єдину захисну оболонку системи: VPN, TLS, Zero Trust Policy Engine, контейнерна ізоляція та моніторинг і аудит (рис.1).

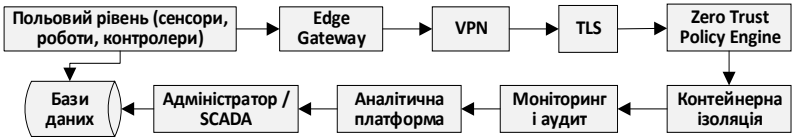

Рисунок 1 – Модель кіберзахисту мікросервісної IIoT-архітектури

Перший рівень VPN формує захищений тунель між вузлами та серверами, запобігає перехопленню трафіку й гарантує безпечний доступ через публічні мережі. Для промислових систем ефективними є легковагові протоколи WireGuard або OpenVPN. Другий рівень TLS забезпечує шифрування даних і взаємну автентифікацію мікросервісів, а централізована система PKI з ротацією сертифікатів гарантує цілісність як зовнішнього, так і внутрішнього трафіку. Третій рівень Zero Trust Policy Engine контролює доступ, перевіряючи кожен запит за контекстом і станом пристроїв, що запобігає внутрішнім загрозам. Четвертий рівень контейнерна ізоляція забезпечує безпечне виконання мікросервісів через обмеження привілеїв, контроль ресурсів і перевірку образів, запобігаючи поширенню атак між контейнерами. П'ятий рівень моніторинг і аудит здійснює постійний аналіз поведінки системи за допомогою IDS/IPS і SIEM, формуючи зворотний зв'язок із Policy Engine для адаптації політик безпеки в реальному часі.

Представлена модель кіберзахисту мікросервісної IIoT-архітектури забезпечує безпечну взаємодію польових пристроїв, шлюзів і аналітичних сервісів. Вона об'єднує п'ять рівнів — VPN, TLS, Zero Trust Policy Engine, контейнерну ізоляцію та моніторинг — у єдиний захисний контур від збору даних до управління процесами. VPN і TLS гарантують захищене передавання даних, Zero Trust контролює динамічний доступ, контейнерна ізоляція запобігає поширенню атак, а моніторинг і аудит забезпечують постійний контроль. Така інтегрована структура підвищує стійкість, керованість і довіру до промислових даних без потреби складної централізованої перевірки

Література

1. Пановик У. Захист інформації в автоматизованих системах на основі концептуальної моделі з формалізованою оцінкою ефективності. *Кібербезпека: освіта, наука, техніка»*, 2025. 4(28), с. 307–320. URL: https://doi.org/10.28925/2663-4023.2025.28.798

2. Zhukabayeva T. et al. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*. 2025. Vol. 25, no. 1. P. 213. URL: https://doi.org/10.3390/s25010213