

Аналіз принципів нульової довіри для побудови кіберфізичної системи віддаленого моніторингу та керування промисловим обладнанням

Ярослав Белий, Дмитро Гурін

Кафедра КІТАРБІ, Харківський національний університет радіоелектроніки, УКРАЇНА,
Харків, пр. Науки, 14, email: yaroslav.bielyi@nure.ua

Анотація: Проведено аналіз застосування принципів нульової довіри у кіберфізичних системах віддаленого моніторингу та керування промисловим обладнанням. Розглянуто особливості ОТ/ІоТ-середовищ, механізми автентифікації, авторизації, сегментації та безперервного контролю. Визначено вимоги до архітектури захищеного віддаленого доступу.

Ключові слова: кіберфізична система, нульова довіра, промислове обладнання, віддалений доступ, ОТ.

I. Вступ

Цифровізація промисловості та поширення технологій Industrial Internet of Things сприяють інтеграції технологічного обладнання, засобів автоматизації, периферійних обчислювальних вузлів і хмарних сервісів у єдині кіберфізичні системи. Віддалений моніторинг дає змогу оперативно отримувати технологічні параметри, діагностувати стан обладнання та скорочувати час реагування на відмови. Водночас функції дистанційного керування безпосередньо впливають на фізичний процес, тому компрометація каналу доступу може мати наслідки не лише для конфіденційності даних, а й для доступності, цілісності та безпеки виробництва [1].

Традиційна модель захисту, заснована переважно на довірі до внутрішнього мережевого периметра, недостатньо відповідає умовам сучасної ІТ/ОТ-конвергенції. Віддалені оператори, сервісні організації, мобільні робочі місця та ІоТ-пристрої формують велику кількість точок доступу. Концепція Zero Trust передбачає відсутність неявної довіри до користувача або пристрою лише через його мережеве чи фізичне розташування; автентифікація й авторизація мають передувати встановленню сеансу доступу до ресурсу [2].

Метою роботи є аналіз принципів нульової довіри та існуючих підходів до їх застосування в системах віддаленого моніторингу й керування промисловим обладнанням, визначення переваг, обмежень та вимог, які доцільно врахувати при подальшому розробленні відповідної кіберфізичної системи.

II. Особливості віддаленого доступу до промислового обладнання

Операційні технології (ОТ) охоплюють програмовані системи та пристрої, що безпосередньо взаємодіють із фізичним середовищем і здійснюють моніторинг або керування процесами. Для них характерні підвищені вимоги до доступності, передбачуваності часових характеристик,

безперервності роботи та функціональної безпеки [1]. Це відрізняє ОТ від типових інформаційних систем і обмежує пряме перенесення частини ІТ-механізмів кіберзахисту.

У типовій кіберфізичній системі віддаленого обслуговування можна виділити рівень промислового обладнання та PLC, локальний ОТ-сегмент, шлюз або edge-вузол, комунікаційну інфраструктуру та віддалений клієнт. Інформаційний потік моніторингу переважно спрямований від обладнання до оператора, тоді як команди керування формують зворотний потік і потребують жорсткішого контролю.

Основними ризиками віддаленого доступу є компрометація облікових даних, несанкціоноване використання привілейованих функцій, підключення скомпрометованого пристрою, перехоплення або модифікація трафіку, а також поширення атаки між ІТ-та ОТ-сегментами. CISA окремо рекомендує обмежувати мережеву експозицію систем керування, ізолювати їх від бізнес-мереж і застосовувати захищені механізми віддаленого доступу [3].

III. Принципи Zero Trust у кіберфізичній системі

Відповідно до NIST SP 800-207, об'єктом захисту в архітектурі Zero Trust є ресурс, а не мережевий сегмент. Доступ надається окремо для конкретного сеансу та повинен визначатися політикою з урахуванням суб'єкта, пристрою, ресурсу й доступної контекстної інформації [2]. Для промислової кіберфізичної системи це означає, що сам факт підключення до корпоративної мережі або VPN не повинен автоматично надавати право керувати технологічним обладнанням.

Ключовими механізмами є сильна автентифікація користувача і пристрою, принцип найменших привілеїв, мікросегментація, захист усіх каналів обміну, журналювання подій і постійне оцінювання стану активів. Архітектура NIST також виділяє Policy Engine, який приймає рішення щодо доступу, та Policy Administrator, який забезпечує виконання цього рішення [2].

Для задачі керування доцільно розмежувати щонайменше режими перегляду телеметрії, діагностики, зміни конфігурації та безпосереднього формування керуючих впливів. Такий підхід зменшує наслідки компрометації окремого облікового запису та дозволяє формувати політики відповідно до критичності операції.

IV. Аналіз підходів до захищеного віддаленого доступу

Найпростішим підходом є використання VPN у поєднанні з міжмережним екраном. Його перевагами є поширеність і відносна простота інтеграції. Проте VPN переважно створює захищений мережевий канал і сам по собі не реалізує повну модель Zero Trust: після встановлення тунелю необхідні додаткові механізми контролю того, до яких саме ресурсів і функцій має доступ суб'єкт. Крім того, рівень захисту залежить від стану кінцевого пристрою [3].

Другий підхід передбачає рольове керування доступом (RBAC). Права визначаються роллю користувача, наприклад оператор, інженер або адміністратор. Перевагою є зрозуміла модель адміністрування, однак статична роль не завжди враховує контекст сеансу: тип пристрою, його стан, місце підключення, час, критичність ресурсу або аномальну поведінку.

Більш гнучким є атрибутний або політико-орієнтований контроль доступу, за якого рішення формується з урахуванням сукупності параметрів. У дослідженнях IoT запропоновано багаторівневі Zero Trust-архітектури, що забезпечують деталізовану авторизацію як у мережевому, так і в edge-доміні та підтримують динамічну реконфігурацію політик [4]. Це особливо важливо для промислового середовища, де частина обладнання може використовувати застарілі або пропрієтарні протоколи.

Проведений аналіз показує, що для системи віддаленого моніторингу та керування доцільно відокремлювати контур отримання телеметрії від контуру формування керуючих команд. Доступ до кожного ресурсу має визначатися окремою політикою, а рішення про дозвіл повинно враховувати ідентичність користувача, стан клієнтського пристрою, критичність операції та поточний контекст.

Узагальнено рішення про доступ можна представити функцією

$$A(t) = F(I, D(t), R, O, C(t)), \quad (1)$$

де I – підтверджена ідентичність суб'єкта; $D(t)$ – поточний стан пристрою; R – запитуваний ресурс; O – тип операції; $C(t)$ – контекст доступу. На відміну від статичного дозволу, така модель допускає повторну оцінку політики під час сеансу та відкриття доступу при зміні умов.

Практична архітектура може містити захищений шлюз між зовнішньою мережею та ОТ-сегментом, сервіс ідентифікації, механізм багатофакторної автентифікації, модуль прийняття політик, точку примусового застосування рішень, журнал аудиту та засоби моніторингу мережевої активності. Для legacy-обладнання, яке не підтримує сучасні механізми автентифікації, контроль доцільно переносити на проміжний edge-шлюз.

Особливе значення має принцип fail-safe: відмова компонента кіберзахисту або втрата зовнішнього з'єднання не повинні переводити технологічний процес у небезпечний стан. NIST наголошує, що заходи захисту ОТ необхідно впроваджувати з урахуванням

специфічних вимог до продуктивності, надійності та безпеки фізичного процесу [1].

Таблиця 1. Порівняння підходів до організації віддаленого доступу

	Переваги	Обмеження	Відповідність ZT
VPN	Захист каналу; поширеність	Довіра після підключення без додаткових політик	Часткова
RBAC	Просте керування ролями	Статичність прав; слабкий контекст	Середня
ABAC/динамічні політики	Контекстний і деталізований доступ	Складність політик та інтеграції	Висока
ZT + сегментація + моніторинг	Безперервний контроль; обмеження латерального руху	Вища складність впровадження	Висока

V. Формування вимог до архітектури кіберфізичної системи

Особливе значення має принцип fail-safe: відмова компонента кіберзахисту або втрата зовнішнього з'єднання не повинні переводити технологічний процес у небезпечний стан. NIST наголошує, що заходи захисту ОТ необхідно впроваджувати з урахуванням специфічних вимог до продуктивності, надійності та безпеки фізичного процесу [1].

VI. Переваги та обмеження застосування Zero Trust

Основною перевагою Zero Trust є зменшення залежності безпеки від місця підключення. Компрометація одного вузла або облікового запису не повинна автоматично відкривати доступ до інших ресурсів. Деталізовані політики дозволяють обмежувати права конкретною операцією, а постійний моніторинг забезпечує додаткові дані для виявлення аномалій.

Разом із тим впровадження Zero Trust в ОТ має низку обмежень. Промислові системи можуть містити обладнання з тривалим життєвим циклом, застарілими протоколами та обмеженими обчислювальними ресурсами. Надмірна кількість перевірок або невдало розташовані засоби контролю здатні збільшувати затримку, а помилка політики – впливати на

доступність технологічної функції. Тому міграція повинна бути поетапною та спиратися на інвентаризацію активів, сегментацію й аналіз ризиків.

Окремою проблемою є баланс між кібербезпекою та експлуатаційною придатністю. Для аварійних і сервісних сценаріїв необхідно заздалегідь визначити контрольовані процедури доступу, журналювання та відновлення, не створюючи неконтрольованих обхідних механізмів.

VII. Напрями подальшого розроблення

Результати аналізу можуть бути використані для розроблення кіберфізичної системи, в якій віддалений клієнт не взаємодіє з PLC або іншим промисловим обладнанням безпосередньо. Запит проходить через точку контролю доступу, а його виконання дозволяється лише після перевірки користувача, пристрою, запитуваної операції та поточного контексту.

Подальше дослідження доцільно спрямувати на формалізацію набору атрибутів для динамічної авторизації, розроблення структури edge-шлюзу, вибір протоколів обміну телеметрією та командами, а також експериментальну оцінку затримки, доступності та стійкості системи до несанкціонованих запитів. Окремо необхідно дослідити механізм безпечного відкликання активного сеансу та реакцію системи на зміну рівня довіри до пристрою.

У межах подальшої реалізації доцільно також формалізувати модель загроз. Для віддаленого керування критичними є викрадення облікових даних, підміна клієнтського пристрою, компрометація шлюзу, повторне відтворення команд, ескаляція привілеїв та латеральне переміщення між сегментами. Zero Trust не усуває ці загрози автоматично, але змінює принцип побудови захисту: кожний запит оцінюється відносно конкретного ресурсу та контексту, а успішна автентифікація не розглядається як безумовна довіра на весь час роботи.

Для промислового обладнання важливим є розмежування інформаційних та керуючих ресурсів. Наприклад, віддалений спеціаліст може отримати доступ до архіву параметрів і діагностичних повідомлень без права змінювати уставки PLC. Перехід до режиму керування може вимагати повторної автентифікації, додаткового підтвердження або погодження локальним оператором. Таким чином, політика формується не лише для користувача, а для конкретної операції над конкретним ресурсом.

VIII. Критерії оцінювання запропонованого підходу

Для переходу від аналітичного огляду до практичного розроблення системи необхідно визначити набір показників, за якими можна оцінювати ефективність застосування принципів Zero Trust. Першою групою є показники кібербезпеки: частка заблокованих неавторизованих запитів, кількість успішних спроб доступу з невідповідним контекстом, час виявлення зміни стану клієнтського пристрою та час відкликання активного сеансу. Ці параметри

характеризують здатність системи підтримувати політику найменших привілеїв не тільки в момент встановлення з'єднання, а й у процесі його використання.

Друга група показників повинна характеризувати вплив механізмів захисту на технологічну складову. До неї доцільно віднести додаткову затримку формування та передачі команди, час автентифікації й авторизації, доступність сервісу моніторингу, частоту помилкових відмов у доступі та поведінку системи при втраті зв'язку з компонентом прийняття політик. Для ОТ-середовища ці показники є принциповими, оскільки підвищення рівня захищеності не повинно порушувати допустимі часові характеристики та безпечний стан фізичного процесу.

Під час експериментального дослідження доцільно сформулювати декілька типових сценаріїв. Базовий сценарій передбачає легітимне підключення авторизованого оператора з довіреного пристрою. Інші сценарії можуть включати спробу використання правильних облікових даних із невідомого пристрою, звернення до ресурсу поза межами наданих повноважень, зміну атрибутів пристрою під час активного сеансу та повторне використання раніше перехопленого запиту. Окремо необхідно перевірити доступ до функцій моніторингу й керування, оскільки наслідки несанкціонованого читання телеметрії та формування керуючої команди мають різний рівень критичності.

Результатом такого експерименту має бути не лише підтвердження факту блокування атаки, а й визначення компромісу між рівнем деталізації політик та експлуатаційними характеристиками системи. Це дозволить обґрунтувати, які перевірки необхідно виконувати для кожного запиту, які можуть здійснюватися періодично, а які доцільно переносити на edge-рівень для зменшення затримки.

IX. Висновки

Проведено аналіз підходів до організації віддаленого моніторингу та керування промисловим обладнанням із застосуванням принципів нульової довіри. Встановлено, що традиційні механізми мережевого захисту, зокрема VPN і периметрова фільтрація, залишаються корисними компонентами, але не забезпечують повної реалізації Zero Trust без додаткової ідентифікації, деталізованої авторизації, сегментації та безперервного контролю.

Для кіберфізичної системи доцільним є поєднання багатofакторної автентифікації, динамічних політик доступу, edge-шлюзу, ізоляції ОТ-ресурсів та журналювання. При цьому механізми кіберзахисту мають враховувати вимоги технологічного процесу до доступності, затримок і функціональної безпеки.

Отримані результати формують основу для подальшого розроблення архітектури кіберфізичної системи віддаленого моніторингу та керування промисловим обладнанням, а також алгоритмів контекстної оцінки довіри та динамічного прийняття рішень щодо доступу.

Перелік посилань

- [1] K. Stouffer et al., "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev. 3, 2023. doi: 10.6028/NIST.SP.800-82r3.
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207.
- [3] Cybersecurity and Infrastructure Security Agency, "Configuring and Managing Remote Access for Industrial Control Systems," CISA, recommended practice.
- [4] A. Tedeschi et al., "A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures," *Electronics*, vol. 12, no. 3, art. 566, 2023. doi: 10.3390/electronics12030566.
- [5] S. Liu et al., "Security Control of Cyber-Physical Systems under Cyber Attacks: A Survey," *Sensors*, vol. 24, no. 12, art. 3815, 2024. doi: 10.3390/s24123815
- [6] YEVSIEIEV, V., & GURIN, D. (2026). Development of a model for constructing the optimal trajectory of the gripping device of a collaborative robot-manipulator taking into account the influence of the cargo mass and energy consumption. *Open Information and Computer Integrated Technologies*, 0(107), 224-240. <https://doi.org/10.32620/oikit.2026.107.15>
- [7] Industry 5.0 та колаборативна робототехніка: динамічний опис навколишнього середовища роботів-маніпуляторів з використанням мови Python: монографія / І. Ш. Невлюдов, В. В. Євсєєв, С. С. Максимова. – Харків : Видавництво Іванченка І. С., 2026. – 279 с. <https://doi.org/10.30837/978-617-8332-95-2>
- [8] Attar, H., Abu-Jassar, A., Hafez, M., Al-Sharo, Y. M., Yevsieiev, V., & Lyashenko, V. (2025, December). Model of Spatial Localization and Identification Objects in the Working Area Collaborative Robot. In 2025 Asian Conference on Communication and Networks (ASIANComNet) (pp. 1-6). IEEE.
- [9] Nevliudov, I., Vladyslav, Y., & Horovyi, K. (2026). MODEL OF THE TECHNOLOGICAL PROCESS OF WEDGE BONDING BASED ON FEK DELVOTEC 6400 IN THE PRODUCTION OF HYBRID ELECTRONIC MODULES. Collection of Scientific Papers «SCIENTIA», (June 12, 2026; Chicago, USA), 170–173.
- [10] Nevliudov, I., Yevsieiev, V., Maksymova, S., Gopejenko, V., & Kosenko, V. DEVELOPMENT OF MATHEMATICAL SUPPORT FOR ADAPTIVE CONTROL FOR THE INTELLIGENT GRIPPER OF THE COLLABORATIVE ROBOT MANIPULATOR. *Advanced Information Systems*. 2025 9(3), P. 57–65. DOI: <https://doi.org/10.20998/2522-9052.2025>
- [11] Amer Abu-Jassar, Hassan Al-Sukhni, Yasser Al-Sharo, Svitlana Maksymova, Vladyslav Yevsieiev, Vyacheslav Lyashenko, Building a Route for a Mobile Robot Based on the BRRT and A*(H-BRRT) Algorithms for the Effective Development of Technological Innovations. *International Journal of Engineering Trends and Technology*. 2024. Vol. 72, no. 11, P. 294-306, DOI: <https://doi.org/10.14445/22315381/IJETT-V72I11P129>.
- [12] Невлюдов, І. Ш., Євсєєв, В. В., Максимова, С. С., & Теслюк, С. І. (2026). Numerical simulation of mobile robotic platform route construction in dynamic space using QR tags. *Open Information and Computer Integrated Technologies*, (108), 218-235.
- [13] Yevsieiev V. Digital Twin in Modeling and Control of Collaborative Robots: Analysis, Comparison and Application Recommendations / V. Yevsieiev, S. Starikova // *Computer-integrated technologies, automation and robotics 2026 : Proceedings of III st All-Ukrainian Conference*, May 14-15, 2026. - Kharkiv : [electronic version], 2026. - P. 89-92.
- [14] Yevsieiev V. Digital Twins of Collaborative Robotic Systems for Decision Support in Emergency Situations / V. Yevsieiev, S. Svetlana // *Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations (ICSTRO-2026) : Proceedings of I-st All-Ukrainian Conference*, February 12-23, 2026. – Kharkiv, 2026. - P. 153-156.
- [15] Attar, H., Abu-Jassar, A., Hafez, M., Al-Sharo, Y. M., Yevsieiev, V., & Lyashenko, V. (2025, December). Model of Spatial Localization and Identification Objects in the Working Area Collaborative Robot. In 2025 Asian Conference on Communication and Networks (ASIANComNet) (pp. 1-6). IEEE.
- [16] Ababneh, J., Abu-Jassar, A., Hamdan, H., Hafez, M., Yevsieiev, V., & Lyashenko, V. (2025, December). Determining the Trajectory of a Mobile Robot Using Chaotic Dynamical Systems. In 2025 Asian Conference on Communication and Networks (ASIANComNet) (pp. 1-7). IEEE.
- [17] Hamdan, M., Ababneh, J., Hafez, M., Abu-Jassar, A., Yevsieiev, V., & Lyashenko, V. (2025, December). Collaborative Manipulator Adaptive Path Planning with Human Presence and Comfort Zone Consideration. In 2025 Asian Conference on Communication and Networks (ASIANComNet) (pp. 1-8). IEEE.
- [18] Attar, H., Abu-Jassar, A., Hamdan, M., Hafez, M., Yevsieiev, V., & Lyashenko, V. (2025, December). Stochastic Model of Collaborative Robot Interaction in a Manufacturing Environment. In 2025 Asian Conference on Communication and Networks (ASIANComNet) (pp. 1-6). IEEE.
- [19] Yevsieiev, V., Maksymova, S., Kulish, S., & Voloshyn, Y. (2025, November). Models and Method for Decentralized Control of Group of Collaborative Robot Manipulators in Single Working Area with Human Operator. In *Conference on Integrated Computer Technologies in Mechanical Engineering–Synergetic Engineering* (pp. 401-424). Cham: Springer Nature Switzerland.
- [20] Nevliudov, I., Yevsieiev, V., Maksymova, S., Gopejenko, V., & Kosenko, V. (2025). Development of mathematical support for adaptive control for the intelligent gripper of the collaborative robot manipulator. *Advanced Information Systems*, 9(3), 57-65.