4. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, № 4. P. 2347–2376.

УДК 004.94:681.5

КОНЦЕПЦІЯ ЦИФРОВИХ ДВІЙНИКІВ (DIGITAL TWINS) В АВТОМАТИЗОВАНИХ СИСТЕМАХ МОНІТОРИНГУ ТА ДІАГНОСТИКИ

Вадим Співак

Миколаївський національний аграрний університет, м. Миколаїв, Україна

Забезпечення надійності, відмовостійкості та безперебійності роботи складних технологічних комплексів є пріоритетним завданням сучасної інженерії та автоматизації [1]. В умовах стрімкого впровадження концепції «Індустрія 4.0» однією з найбільш проривних технологій цифрової трансформації є концепція цифрових двійників (Digital Twins). Як зазначають у своєму дослідження M. Grieves та J. Vickers, які стояли біля витоків цієї технології, цифровий двійник - це не просто статична тривимірна модель, а динамічна віртуальна копія фізичного об'єкта, яка еволюціонує разом з ним протягом усього життєвого циклу завдяки безперервному обміну даними [1].

Метою роботи є обґрунтування доцільності та розробка концептуальних підходів до застосування технології цифрових двійників у складі інтелектуальних систем діагностики й управління промисловим та агропромисловим обладнанням.

Традиційні підходи до технічного обслуговування базуються на регламентних (планово-попереджувальних) ремонтах або на ремонтах за фактом поломки (реактивне обслуговування). Обидві стратегії є економічно неефективними: перша призводить до заміни ще придатних деталей, а друга - до тривалих аварійних простоїв. Згідно з дослідженнями F. Tao та співавторів, перехід до предиктивного технічного обслуговування (Predictive Maintenance) неможливий без створення єдиного інформаційного середовища, де фізичний об'єкт безперервно обмінюється даними зі своєю віртуальною копією [2].

У науковій літературі, зокрема у фундаментальному огляді W. Kritzinger та ін., прийнято розрізняти три рівні інтеграції цифрових моделей, які визначають ступінь автоматизації систем моніторингу [3]:

1. Цифрова модель (Digital Model) - передбачає ручний обмін даними між фізичним об'єктом та його віртуальною копією (застосовується на етапі проєктування).

2. Цифрова тінь (Digital Shadow) - характеризується одностороннім автоматичним потоком даних від фізичного об'єкта до цифрової моделі, що дозволяє здійснювати моніторинг, але без зворотного керуючого впливу.

3. Цифровий двійник (Digital Twin) - найвищий рівень інтеграції, що базується на повністю автоматизованому двосторонньому потоці даних, де рішення віртуальної моделі автоматично імплементуються у фізичне середовище [3].

Розроблена нами концептуальна архітектура системи моніторингу передбачає використання саме повноцінного цифрового двійника. Телеметричні дані (температура, спектр вібрацій, споживаний струм) з реального обладнання через промислові IoT-шлюзи безперервно надходять до хмарного середовища, де розгорнуто цифрову копію [4]. На базі цих даних віртуальна модель постійно синхронізує свій внутрішній стан з фізичним оригіналом.

Ключовим механізмом інтелектуальної діагностики є постійне паралельне порівняння реакції реального об'єкта та цифрового двійника на однакові керуючі впливи. Оскільки цифрова модель імітує роботу «ідеально справного» механізму, будь-яка нев'язка між реальними сенсорними даними та розрахунковими показниками моделі свідчить про початок деградації вузлів [2]. Для аналізу цих відхилень система використовує алгоритми машинного навчання (зокрема, рекурентні нейронні мережі), що дозволяє ідентифікувати тип несправності та розрахувати залишковий корисний ресурс (Remaining Useful Life - RUL) об'єкта [4].

У контексті агропромислового виробництва використання таких технологій відкриває можливості для створення цифрових двійників цілих технологічних ліній (наприклад, елеваторних комплексів чи ліній переробки сировини). Q. Qi та співавтори доводять, що інтеграція технології Digital Twins з системами аналізу Великих даних здатна підвищити загальну ефективність обладнання (OEE) на 15–20 % за рахунок оптимізації режимів роботи [4].

Отже, впровадження цифрових двійників в автоматизовані інформаційні системи моніторингу формує принципово новий рівень управління кіберфізичними системами [1]. Це дозволяє здійснити перехід до обслуговування обладнання за фактичним станом, що мінімізує фінансові втрати від непередбачених простоїв та підвищує експлуатаційну безпеку підприємства [2].

Список використаних джерел

1. Grieves M., Vickers J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary perspectives on complex systems. Springer, Cham, 2017. P. 85–113.

2. Tao F., Zhang H., Liu A., Nee A. Y. C. Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics. 2019. Vol. 15, № 4. P. 2405–2415.

3. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine. 2018. Vol. 51, № 11. P. 1016–1022.

4. Qi Q., Tao F., Hu T., Anwer N., Liu A., Wei Y., Wang L., Nee A. Y. C. Enabling technologies and tools for digital twin. Journal of Manufacturing Systems. 2021. Vol. 58. P. 3–21.

УДК 004.056:004.7

DEVELOPMENT OF ADAPTIVE ACCESS CONTROL POLICIES FOR MULTI-CLOUD ENVIRONMENTS IN DISTRIBUTED INFORMATION SYSTEMS

Dmytro Hleba

Institute of Special Communications and Information Protection,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

Abstract. This paper investigates the challenges and prospects of developing adaptive access control policies for distributed information systems operating in multi-cloud environments. It analyzes key information security threats associated with cloud migration, as well as the limitations of traditional static access control models. The advantages of transitioning to dynamic attribute-based models (ABAC) and Zero Trust architecture are identified. Particular attention is paid to mechanisms for continuous monitoring of user context, automated policy updating, and enhancing the overall resilience of the infrastructure against modern cyberattacks.

Keywords: multi-cloud environments, cybersecurity, access control, adaptive policies, distributed information systems, Zero Trust, ABAC, identity management.

Research Relevance: The current stage of corporate information technology development is characterized by a massive transition to multi-cloud architectures. Organizations simultaneously use resources from various providers (e.g., AWS, Azure, Google Cloud) to optimize costs and ensure the uninterrupted operation of distributed systems. However, such infrastructure fragmentation leads to an expanded attack surface, loss of centralized control, and difficulties in managing access rights. Traditional static Role-Based Access Control (RBAC) models are no longer capable of effectively protecting data in conditions of highly dynamic connections, Bring Your Own Device (BYOD) practices, and remote work. The relevance of this research stems from the urgent need to develop and implement adaptive access control mechanisms capable of responding in real time to context changes and risk levels within multi-cloud ecosystems.

Research Objective: The aim of this study is to analyze the principles of building adaptive access control policies in multi-cloud environments, develop approaches for integrating dynamic risk assessment