УДК 004.056
М. Копач; Ю. Скоренький, к.ф.-м.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ЦИФРОВИХ ДВІЙНИКІВ ВИРОБНИЧИХ ЛІНІЙ МЕТАЛООБРОБНИХ ПІДПРИЄМСТВ

UDC 004.056
M. Kopach; Yu. Skorenkyy, Ph.D., Assoc. Prof.

STUDY OF VULNERABILITIES OF DIGITAL TWINS OF THE METAL PROCESSING ENTERPRIZES

Ключові слова: інформаційна безпека, промисловий інтернет речей, вразливості.
Key words: information security, industrial internet of things, vulnerability.

Поява Інтернету речей (Internet of Things, IoT) проклала шлях до нових можливостей для вдосконалення промислових процесів за допомогою інтеграції та складного керування машинами та приводами, обладнаними датчиками. У технологічних процесах промисловий Інтернет речей дає виробникам можливість отримати всебічне уявлення про кожен етап виробничого процесу, сприяючи коригуванням у реальному часі для забезпечення безперебійного виробництва та зниження ймовірності дефектів і збоїв, спричинених людськими помилками, відповідно до принципів Індустрії 4.0. Позитивні наслідки інтелектуального виробництва виходять за рамки виробничих операцій, обладнання та оптимізації запасів. Цифрові близнюки (Digital Twin, DT), які широко використовуються в Індустрії 4.0 для моделювання та керування виробничими процесами [1], є віртуальними копіями фізичних об’єктів або систем. Перевага використання цифрових двійників для малого та середнього бізнесу полягає в можливості оптимізувати виробничі процеси, забезпечити навчання персоналу та розширити можливості моделювання, виправдовуючи розробку ресурсомісткого, але важливого програмного забезпечення, призначеного для моделювання та навчання.

Для металообробного виробництва з високим рівнем цифровізації промислове моделювання на основі даних дозволяє розробити відповідну архітектуру цифрового двійника. Зібрані дані та оброблена інформація є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

В даній роботі представлено аналіз вразливостей [2] промислових цифрових двійників, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Література

1. Skorenky Yu. et al. Development of digital twin interface for Industry 4.0 production line. CEUR Workshop Proceedings, 2024, 3742, pp. 358–369
2. R. Khan, K. McLaughlin, D. Laverty, S. Sezer. STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc. (2018) 1-6. URL: https://doi.org/10.1109/ISGTEurope.2017.8260283