УДК 004.056
М.Р. Карпець – ст. гр. СБмз-61, Ю.Л. Скоренький к.ф.-м.н., доц.
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПЛАТФОРМ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

M. Karpets, Dr. Yu. Skorenkyy

STUDY OF VULNERABILITIES OF THE INDUSTRIAL INTERNET OF THINGS PLATFORMS

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

Широке впровадження цифрових платформ може призвести до нових спільних бізнес-моделей, які сприятимуть сталому розвитку [1, 2]. Питання безпеки застосування пристроїв інтернету речей має надзвичайну актуальність, оскільки дані є одним з найбільш важливих виробничих ресурсів Індустрії 5.0.

Інтелектуальне виробництво може надавати різноманітні дані, включаючи фізичні дані про матеріали та візуальні дані, дані керування процесом і дані про машину тощо. Щоб безпечно керувати даними з кіберфізичної системи пристроїв IoT з обмеженими ресурсами, потокова великомасштабна платформа обміну даними має бути належним чином розроблена. Інформаційна безпека та захист конфіденційності стають критичними вимогами та заслуговують на особливу увагу в контексті Індустрії 5.0.

Для інтелектуальних виробничих процесів і агрегатів в системах Індустрії 5.0 використовують цифрові двійники, які моделюють реальні виробничі лінії та процеси, дозволяють обробляти дані на місці або транслювати дані в хмарні сервіси для підтримки прийняття рішень на основі математичних моделей, що характеризують споживання ресурсів і якість і кількість результатів процесу. Рівень безпеки для промислового цифрового двійника в хмарних/граничних середовищах має бути ретельно спроектований і належним чином розроблений. Захист IDT в цілому та кожного пристрою IoT зокрема вимагає вирішення багатьох загроз інформаційній безпеці та кібербезпеці. Зібрані дані та оброблена інформація в IDT є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

В даній роботі представлено аналіз вразливостей промислових цифрових платформ, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Література

1. Skorenky Yu. et al. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. *CEUR Workshop Proceedings*, 2023, 3468, pp. 12–23.

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