УДК 004.056;004.032.26
Kyrychenko O.V.[1], Vasylenko O.V.[2]

[1] студ. гр. БК-815м НУ «Запорізька політехніка»
[2] доц. НУ «Запорізька політехніка»

DEFENSE SYSTEM FOR SENSOR NODES OF CYBER-PHYSICAL SYSTEMS

The rapid development of the Industry 4.0 paradigm and the massive implementation of Internet of Things (IoT) technologies have led to the formation of complex cyber-physical systems (CPS) [1]. Today, CPS are the foundation of critical infrastructure: from smart grids and automated production lines to life support systems and autonomous transport. The main feature of such systems is the deep integration of computational (cybernetic) processes with the physical environment. However, this integration generates fundamentally new vectors of cyber threats aimed not at stealing information, but at destabilizing or destroying physical objects. Traditional information security methods (firewalls, antivirus software, classical cryptography) focus on protecting data in transit (in the communication channel) and preventing unauthorized access to higher-level IT infrastructure.

However, they prove vulnerable to intelligent attacks at the lowest, hardware level – the level of sensor nodes [2]. If an attacker gains the ability to manipulate the analog signal in the physical environment or replace the measuring sensor itself (False Data Injection, Stealthy, Replay attacks), the microcontroller's cryptographic mechanisms will encrypt the compromised data, and the control system will accept them as legitimate.

Analysis of real incidents (e.g., the Stuxnet virus) [3] proves the critical need to transition to end-to-end verification systems that confirm not only the cryptographic integrity of packets but also the physical authenticity of the measurements themselves [4]. That is why the development of comprehensive, multi-level securi-

ty systems based on a hardware "root of trust" and semantic analysis using AI methods is a highly relevant scientific and practical task.

The aim of the work is the development and software modeling of a conceptual multi-level cyber defense architecture for sensor nodes of cyber-physical systems, which provides comprehensive verification of measurement data using hardware key generation, active sensing methods, and semantic analysis based on adaptive filters and recurrent neural networks.

To achieve this aim, the following research tasks were formulated and solved: to analyze the specifics of data collection in information and measurement systems and classify modern vectors of intelligent attacks on the hardware level of CPS (FDI, Stealthy, Replay); to investigate existing practical approaches to ensuring the hardware integrity of end nodes, in particular the use of Physical Unclonable Functions (PUF); to consider the mathematical apparatus of anomaly detection based on the physics of processes (Physics-based Detection) and methods of active watermarking of analog signals; to design a conceptual multi-level security architecture combining isolated execution of cryptographic operations (TrustZone) with dynamic semantic analysis; to develop and justify a mathematical model of an adaptive residual detection threshold for the classical Kalman filter and an extended digital twin based on an LSTM neural network; to perform a software simulation of the developed architecture to confirm its effectiveness under conditions of non-stationary noise and stealthy cyberattacks.

The object of the research is the processes of collection, primary processing, cryptographic protection, and transmission of measurement information from end sensor nodes to control controllers within cyber-physical systems.

The subject of the research is the methods, algorithms, and comprehensive engineering solutions for ensuring data integrity, reliability, and hardware authenticity based on PUF technologies, Kalman filters, and Long Short-Term Memory (LSTM) neural networks.

Research methods. In the process of performing the work, the following were applied: methods of system analysis (to form a multi-level security architecture); automatic control theory (to describe the dynamics of CPS in the state space); mathematical statistics (to calculate residuals and adaptive detection thresholds); machine learning (to approximate non-linear physical processes using LSTM); cryptographic information protection methods; and computer modeling methods (for software simulation of the developed monitoring algorithms).

Practical significance of the obtained results.

The proposed architectural model and adaptive detection algorithms can be used as a theoretical and algorithmic foundation for developing real security monitoring systems at critical infrastructure facilities, which will significantly increase their cyber resilience against intelligent physical-layer attacks.

REFERENCES

1. Henderson K., Salado A. Value and benefits of model-based systems engineering (MBSE): Evidence from the literature. *Systems Engineering*. 2021. Vol. 24. P. 51–66. DOI: 10.1002/sys.21566.

2. Pasupuleti M. K. Modeling and Simulation with MATLAB, Simulink, and Python [Online resource]. 2026. URL: https://www.researchgate.net/publication/399882757 (дата звернення: 14.03.2026).

3. Digital Twins as a Tool for Strategic Planning and Sustainability in Industry [Online resource]. 2025. URL: https://www.researchgate.net/publication/385612345_Digital_Twins_Siemens_Xcelerator (дата звернення: 14.03.2026).