УДК 621.316:004.056 Економіка і енергозбереження

RESEARCH OF TECHNICAL SOLUTIONS FOR CYBERSECURITY OF POWER SYSTEMS WITH INTEGRATED RENEWABLE ENERGY SOURCES

[1] Pavlenko V., [2] Volianyk O.
[1] National University of Life and Environmental Sciences of Ukraine
[2] Kyiv National University of Technologies and Design

The energy infrastructure now is facing new challenges due to integrating renewable energy sources, the decarbonisation of the economy, and the need to ensure a stable electricity supply. As cyber-physical systems (CPS) become more prevalent in the energy sector, they introduce additional vulnerabilities to cyber threats. These threats pose the risk of financial losses and threaten the smooth operation of critical energy infrastructure. In this context, safeguarding energy systems from cyberattacks has become an urgent priority, especially as digitalisation continues transforming the energy landscape.

Numerous risks accompany the integration of CPS into modern energy systems. Existing security protocols do not always meet the requirements of the dynamic cyber environment, making it challenging to implement new technologies. Third, the high cost of integrating protective technologies and adapting them to existing systems poses a significant barrier to adopting solutions in the industry. Finally, insufficient development of real-time forecasting tools limits the ability to detect and prevent attacks promptly.

The most common types of cyberattacks faced by modern cyber-physical energy systems and effective protection methods are shown in Table 1.

Table 1 - Common Types of Cyberattacks on Cyber-Physical Energy Systems

Attack Type	Description Protection	Method Common	Vulnerabilities
DoS/DDoS	Overloading the network with many requests and blocking services	Implementation of IDS/IPS systems to detect and block attacks	Unsecured network infrastructure and inadequate traffic filtering
FDI (False Data Injection)	Injecting false data into control systems leads to incorrect decisions	Machine learning algorithms are used to detect anomalies in data	Lack of data validation and anomaly detection systems
SQL Injection	Exploiting vulnerabilities in databases for unauthorised access or data modification	Use of prepared statements, Object-Relational Mapping, and encryption	SQL vulnerabilities, improper input validation, and insecure database access
Replay	Reusing recorded data to create the illusion of regular system operation	Real-time data synchronisation using Phasor Measurement Units	Lack of data timestamping and session management
Man-in-the-middle	Intercepting data between two parties for manipulation or unauthorised access	Data encryption and use of SSL/TLS certificates for secure communications	Weak encryption protocols and improper certificate handling
Phishing	Social engineering to gain confidential information (passwords, access)	Employee training and use of anti-phishing solutions	Lack of security awareness and poor access control practices
Malware	Introduction of malicious software to disrupt system operations or steal data	Use of antivirus programs and regular system updates	Insufficient endpoint protection and outdated software

A multi-layered approach incorporating technical, organisational, and software measures is essential to enhance the cybersecurity of power systems. A promising area is adopting next-generation SCADA systems with protective modules such as encryption, multi-factor authentication, and advanced intrusion detection systems (IDS). Integrating Phasor Measurement Units (PMUs) ensures microsecond data synchronisation, providing better visibility and faster emergency response.

Implementing multi-agent systems with blockchain protection enhances resilience by reducing the risk of data compromise and enabling rapid recovery after attacks. Machine learning algorithms for monitoring reduce false positives by 30% compared to traditional detection systems. Integrating PMUs reduces emergency response time by 15% by providing precise, synchronised data, allowing faster actions in critical situations.

Adopting cybersecurity standards like ISO 27001 boosts the credibility of energy systems, attracting investment for infrastructure development. Training systems that simulate risks help operators develop the necessary skills to maintain stability during crises.

Ensuring cybersecurity in energy systems is crucial for Smart Grid development. Future research should focus on creating adaptive management systems, implementing artificial intelligence for automated monitoring, and developing scalable solutions for integrating decentralised systems into national grids. Studying the impact of cybersecurity on large energy systems, especially during mass failures caused by attacks on decentralised elements, is important. Researching energy storage systems' integration into cyber-physical networks will improve stability during peak periods. Long-term, developing international standards for unifying cybersecurity approaches for critical infrastructure is essential.

Developing cybersecurity technologies will ensure power grid stability, enhance efficiency, and create the foundation for sustainable energy development. The growing dependence on interconnected cyber-physical systems increases the attack surface. As renewable energy sources like wind and solar power are integrated, managing decentralised generation has become more complex, requiring sophisticated security methods to protect data exchanged between generation sites, storage systems, and grid operators.

For instance, IoT devices in wind farms and solar arrays can become entry points for attackers if not secured. Energy storage systems, crucial for balancing supply and demand, are also vulnerable to cyber threats leading to cascading outages. Communication infrastructure within Smart Grids is especially vulnerable as more sensitive data is transferred, requiring robust encryption and authentication measures.

AI and machine learning are crucial for identifying and mitigating cyber threats. Machine learning models can detect abnormal patterns and trigger automated responses, preventing widespread damage. AI can also monitor system behaviour, predict vulnerabilities, and help energy providers take preventive measures. Blockchain technology secures energy systems by providing a decentralised ledger that records all transactions, making it difficult for hackers to alter data without detection. Blockchain ensures transparency and trust, particularly in decentralised networks and renewable energy markets. For instance, it could track the ownership and origin of renewable energy certificates, offering a verifiable history of energy production and facilitating the integration of distributed energy resources (DERs).

The future of energy systems lies in integrating renewable sources, smart grids, and advanced cybersecurity technologies. Implementing solutions like machine learning, blockchain, and next-generation SCADA systems will significantly strengthen energy systems' resilience to cyber threats, ensuring stability, efficiency, and sustainability in the energy sector.

References

1. Pavlenko V., Volianyk O., Ponomarenko I., Danylchenko D. Research of the prospects for the development of smart energy systems technology using distributed databases // Energetics and Automation. 2024. №5. URL: https://www.journals.nubip.edu.ua/index.php/Energiya/article/view/51318.

2. Darlington, Eze, Ekechukwu., Peter, Simpa. (2024). 1. The future of Cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions. Computer science & IT research journal.