Література:

1. Zhang Y., & Wang J. Adaptive Sleep Mode Algorithms in IoT for Improved Energy Efficiency. *Journal of Internet Technology*, 24(2), 2023. P. 205–212. doi:10.1109/JIT.2023.108.

2. Lee S., Kim H., & Park D. Optimizing MQTT for IoT Systems: A Survey of Energy-efficient Protocols. *IEEE Communications Surveys & Tutorials*, 25(1), 2023, P. 34–50. doi:10.1109/COMST.2023.1234567.

3. Patel R., & Bansal R. Edge AI for IoT Systems: A Review of Energy-efficient Architectures. *Sensors*, 23(5), 2023, 4567. doi:10.3390/s23054567.

4. Gupta, A., & Mehta, S. Security Optimization in IoT: Lightweight Encryption Techniques. IEEE Access, 10, 2022, 122345-122357. doi: 10.1109/ ACCESS.2022.1245678.

DOI https://doi.org/10.36059/978-966-397-522-1-127

ANALYSIS OF THE DEPENDENCE OF DISTRIBUTED ENTERPRISES ON THE STABLE FUNCTIONING OF ENERGY AND COMMUNICATION SYSTEMS

Khniunin S. H.
Candidate of Technical Sciences, Associate Professor,
Department of Information Technologies
International Humanitarian University
Odesa, Ukraine

Shvedu M. I.
2nd-year undergraduate student
in the speciality 125 – Cybersecurity and Information Protection
International Humanitarian University
Odesa, Ukraine

Despite the ongoing war, Ukraine continues to implement its long-term National Strategic Plan for Digital Development, including action plans for its implementation during 2025–2027 [1]. This effort extends beyond the mere automation of existing processes via computers; it represents a fundamental transformation of interaction, labour, production, and the consumption of information and services – a vital step towards deeper integration into the European community.

However, the troubling global landscape in recent years has exposed a dangerous dependency of both transnational distributed enterprises [2] and entire nations on the stable functioning of energy and communication systems.

Let us consider the major incidents involving damage to both power and communication infrastructure that occurred between 2023 and 2025.

Damage to the Estlink 2 cable between Finland and Estonia on 25 December 2024 [3]; further damage to cables between Sweden and Lithuania, and Finland and Germany in November 2024 [4]; damage to a submarine telecommunications cable in the Baltic Sea within Sweden's economic zone in February 2025 [5]. Since October 2023, at least 11 instances of submarine cable damage have been recorded in the Baltic Sea, raising concerns over potential acts of sabotage [6].

Between January and February 2025, Taiwan experienced four undersea cable disruption incidents – three domestic and one international [7–9].

A widespread network failure on 28 April 2025 affected several European countries – including Spain, Portugal, France, Belgium, and Andorra – paralysing public transport and halting train services. Preliminary estimates by experts suggest the incident may have resulted in financial losses ranging from €2.25 to €4.5 billion [10–13].

The failure of the Intelsat 33e communication satellite, built by Boeing and operated by Intelsat, which occurred on 19 October 2024 while in geostationary orbit, led to a complete cessation of communication services for customers across Europe, Africa, and parts of Asia. Intelsat confirmed the total loss of the satellite [14–15].

This analysis leads to a concerning conclusion: the dependency of both transnational distributed enterprises and entire nations on the stable operation of energy and communication systems is critical – and extremely dangerous. This vulnerability becomes increasingly apparent in today's world, where globalisation and digitalisation continue to expand.

Interruptions in energy supply or communication networks affect numerous facets of life:

– They lead to substantial economic losses – halting production, disrupting supply chains, causing data loss and customer attrition (at the national level, this may result in reduced GDP, inflation, financial market instability, and social unrest).

– They paralyse daily life – disrupting work, education, access to healthcare, communication with loved ones, and the reception of essential information.

– They become instruments of political coercion and blackmail – dependency on critical infrastructure renders countries vulnerable to cyberattacks, sabotage, and even military aggression.

– The complexity and interdependence of modern energy and communication systems create new vectors for systemic disruption – a minor

software error or a successful cyberattack can trigger cascading failures across the entire infrastructure.

Recognising this dangerous dependency is the first step towards identifying new solutions and developing comprehensive strategies at both national and international levels. These should aim to enhance the resilience of critical infrastructure, diversify sources of energy and communication, strengthen cybersecurity, improve backup and recovery systems, and foster international cooperation in securing critical infrastructure.

Bibliography:

1. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (дата звернення: 18.05.2025).

2. Khniunin S.H., Shvedu M.I. Ensuring the Security of Information Systems in Distributed Enterprises in Conditions of Unstable Communication System Operations // Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку : Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь : Liha-Pres, 2025. Ч. 2. С. 144–146. DOI: 10.36059/978-966-397-491-0-42

3. The Guardian: Sixty-mile drag mark found near damaged Baltic Sea cable, says Finland. URL: https://www.theguardian.com/world/2024/dec/30/finnish-investigators-into-suspected-sabotage-find-100km-trail-on-baltic-sea-bed (дата звернення: 18.05.2025).

4. New York Post: Russia accused of cutting, sabotaging undersea cables in the Baltic Sea. URL: https://nypost.com/2024/11/19/world-news/russia-accused-of-cutting-sabotaging-undersea-cables-in-the-baltic/ (дата звернення: 18.05.2025).

5. Reuters: Finland, Sweden investigate suspected sabotage of Baltic Sea telecoms cable. URL: https://www.reuters.com/world/europe/sweden-investigates-possible-breach-undersea-cable-baltic-sea-prime-minister-2025-02-21/ (дата звернення: 18.05.2025).

6. AP News: At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard. URL: https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125 (дата звернення: 18.05.2025).

7. Reuters: Taiwan detains China-linked cargo ship after undersea cable disconnected. URL: https://www.reuters.com/world/asia-pacific/taiwan-detains-china-linked-cargo-ship-after-undersea-cable-disconnected-2025-02-25/ (дата звернення: 18.05.2025).

8. Al Jazeera: Taiwan charges captain of China-linked ship with damaging subsea cable. URL: https://www.aljazeera.com/news/2025/4/11/taiwan-charges-

captain-of-china-linked-ship-with-damaging-subsea-cable (дата звернення: 18.05.2025).

9. Global Taiwan Institute: Countering China's Subsea Cable Sabotage. URL: https://globaltaiwan.org/2025/03/countering-chinas-subsea-cable-sabotage/ (дата звернення: 18.05.2025).

10. Reuters: Spain, Portugal switch back on, seek answers after biggest ever blackout. URL: https://www.reuters.com/world/europe/spains-power-generation-nearly-back-normal-after-monday-blackout-says-grid-2025-04-29/ (дата звернення: 18.05.2025).

11. Apagão: electricidade regressa de norte a sul do país. URL: https://www.publico.pt/2025/04/28/economia/noticia/apagao-geral-rede-electrica-portugal-2131164?#110130 (дата звернення: 18.05.2025).

12. Reuters: No sign of cyberattack on grid operator during Spain's blackout, minister says. URL: https://www.reuters.com/world/europe/no-sign-cyberattack-grid-operator-during-spains-blackout-minister-says-2025-05-14/?utm_source=chatgpt.com (дата звернення: 18.05.2025).

13. EuroNews: Europe's 'wake up call': What lessons can be learned from Spain and Portugal's power outage? URL: https://www.euronews.com/next/2025/04/29/europes-wake-up-call-what-lessons-need-to-be-learned-from-spain-and-portugals-power-outage?utm_source=chatgpt.com (дата звернення: 18.05.2025).

14. Intelsat Reports IS-33e Satellite Loss. URL: https://www.intelsat.com/newsroom/intelsat-reports-is-33e-satellite-loss/ (дата звернення: 18.05.2025).

15. TheVerge: A satellite made by Boeing just fell apart in space. URL: https://www.theverge.com/2024/10/22/24277073/intelsat-33e-boeing-satellite-fell-apart-space (дата звернення: 18.05.2025).