Тетяна Запорожець, доктор наук з державного управління, доцент, професор кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка
Tetyana Zaporozhets, Doctor of Science of Public Administration, Associate Professor, Professor of Global and National Security Department, Educational and Scientific Institute of Public Administration and Civil Service Taras Shevchenko National University of Kyiv
ORCID ID https://orcid.org/0000-0003-1914-9481

КІБЕРСТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ОНОВЛЕНІ СТРАТЕГІЇ ЗАХИСТУ В УМОВАХ ЗРОСТАЮЧИХ ЗАГРОЗ
CYBER RESISTANCE OF CRITICAL INFRASTRUCTURE: UPDATED PROTECTION STRATEGIES IN THE CONDITIONS OF GROWING THREATS

The article highlights current challenges in the field of critical infrastructure cybersecurity, emphasizing the importance of a comprehensive approach to its protection. The increasing number of cyberattacks on essential sectors threatens economic, social, and political stability, especially due to the use of outdated technologies in critical systems. The example of Singapore's Masterplan OT 2024 initiative illustrates the importance of coordination between government agencies, the private sector, and research centers to enhance cyber resilience and serve as a model for improving cybersecurity and ensuring critical infrastructure resilience against emerging cyber threats. The program focuses on developing specialist skills and implementing standardized security protocols to enable rapid responses to cyber threats. Special emphasis is placed on building a cybersecurity culture among citizens through educational programs and information campaigns.

Keywords: critical infrastructure, cybersecurity, cyber resilience, Masterplan OT 2024, comprehensive approach, cybersecurity culture

Сучасні загрози у сфері кібербезпеки критичної інфраструктури виходять за межі технічних викликів, оскільки зачіпають економічну, соціальну та навіть політичну стабільність країн. Значне зростання випадків кібератак на інфраструктуру життєзабезпечення свідчить про необхідність цілеспрямованої та системної роботи в цій галузі.

На сьогодні немає єдиного міжнародного агентства з кібербезпеки, проте в різних країнах існують організації, що активно працюють у сфері захисту критичної інфраструктури на міжнародному рівні. Наприклад, Агентство кібербезпеки та інфраструктурної безпеки США (CISA) [1] надає керівництво та координує зусилля для захисту критичних секторів у партнерстві з іншими країнами. CISA активно бере участь у міжнародних ініціативах, щоб реагувати на кіберзагрози глобального рівня, підкреслюючи важливість співпраці та обміну інформацією між державними й приватними організаціями.

Також Європейське агентство з кібербезпеки (ENISA) [2] є одним з провідних регуляторів у цій галузі для країн ЄС, яке сприяє розвитку стандартів безпеки та здійснює моніторинг кіберзагроз. Важливу роль у координації зусиль відіграє і організація Interpol [3], яка об’єднує правоохоронні органи різних країн у боротьбі з кіберзлочинністю та загрозами критичним об’єктам інфраструктури.

Різноманітність і масштаб загроз підкреслюють, що вразливості критичних секторів можуть впливати на громадський порядок, економічну стабільність і навіть національну обороноздатність. Крім того, старіючі технології, що використовуються в багатьох галузях інфраструктури, стають значним фактором ризику, оскільки не завжди відповідають сучасним вимогам до кібербезпеки. Системи операційних технологій, які часто управляють фізичними процесами в енергетиці, водопостачанні та транспорті, були створені переважно з акцентом на фізичну, а не на кібербезпеку. Це робить їх вразливими для сучасних кіберзагроз, включаючи атаки, що можуть призвести до серйозних наслідків, таких як збої в електропостачанні, перебої в транспортній системі чи втручання в системи водопостачання.

Міжнародне співробітництво і координація між секторами критичної інфраструктури є важливим аспектом побудови надійної кіберстійкості. Одним із прикладів ефективної координації є сингапурський Masterplan OT 2024 (Operational Technology Cybersecurity Masterplan 2024) [4], у якому акцентується на важливості об’єднання зусиль державних установ, приватного сектору, дослідницьких центрів і освітніх установ. Такий підхід дає змогу не тільки ефективніше використовувати наявні ресурси, але й створює сприятливі умови для розробки нових інструментів кіберзахисту.

Одним із ключових напрямів, який підтримується Masterplan OT 2024, є посилення технічних навичок і професійної компетентності фахівців у сфері OT-кібербезпеки. Зростаюча потреба у кваліфікованих кадрах, здатних захистити критичну інфраструктуру від складних і еволюціонуючих кіберзагроз, вимагає значних інвестицій у навчання та підготовку фахівців. Окрім того, для забезпечення безпеки важливо, щоб усі учасники процесу мали уніфіковані протоколи обміну інформацією та спільні стандарти безпеки, що сприятиме швидкому реагуванню на загрози і зменшенню ризиків.

Кібербезпека критичної інфраструктури неможлива без належного рівня обізнаності суспільства щодо питань безпеки, ризиків і необхідності дотримання певних норм і стандартів у щоденній діяльності. Masterplan OT 2024 прагне створити культуру кібербезпеки, зосереджуючись на вихованні відповідального ставлення до кіберзагроз серед усіх верств населення. Такі ініціативи включають інформаційні кампанії, освітні програми та розвиток загальних стандартів безпеки для організацій різних рівнів.

Формування культури кібербезпеки є стратегічною потребою, оскільки забезпечити стійкість перед сучасними загрозами можливо лише завдяки комплексному підходу. Ефективна кібербезпека вимагає не лише технічних рішень, але й змін у свідомості та поведінці суспільства [5]. Такі зміни сприяють довготривалій стійкості інфраструктури та ефективності державних і приватних зусиль щодо протидії кіберзагрозам.

Отже, оновлений Masterplan OT 2024 є важливим стратегічним кроком у напрямі підвищення кібербезпеки критичної інфраструктури Сінгапуру. Він об'єднує інтереси різних секторів і сприяє взаємодії між учасниками екосистеми кібербезпеки, підвищуючи загальний рівень захисту від сучасних загроз. Це підкреслює необхідність комплексного підходу до кіберстійкості, який враховує технічні, соціальні та організаційні аспекти захисту.

Masterplan OT 2024 може стати прикладом для інших країн, оскільки демонструє важливість інтегрованих рішень для зміцнення стійкості критичної інфраструктури та формування стійкого суспільства перед новітніми кіберзагрозами.

Список використаних джерел

1. US Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/

2. The European Union Agency for Cybersecurity, ENISA. https://www.enisa.europa.eu/about-enisa

3. Interpol. Strategic Framework 2022-2025. https://www.interpol.int/Who-we-are/Strategy/Strategic-Framework-2022-2025

4. Singapore updates OT Masterplan 2024 to bolster national cybersecurity defense. URL : https://industrialcyber.co/industrial-cyber-attacks/singapore-updates-ot-masterplan-2024-to-bolster-national-cybersecurity-defense/

5. Kyle Chin. Developing a Culture of Cybersecurity Within Your Organization. URL : https://www.upguard.com/blog/developing-a-culture-of-cybersecurity