УДК 004.738:004.056

Забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури

Вадим Остапчук[0009-0002-2952-9189]
Валерій Козачок[0000-0003-0072-2567]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У тезах розглядається проблема забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури в умовах інтенсивного зростання та ускладнення кіберзагроз. Висвітлено сучасні виклики та ризики, пов’язані з функціонуванням таких систем, зокрема вразливості у мережевих протоколах, віддаленому адмініструванні, інтеграції промислових та корпоративних сегментів. Проведено аналіз тенденцій розвитку механізмів захисту, включно з комплексними системами контролю доступу, криптографічним захистом даних, сегментацією мереж і впровадженням засобів виявлення.
Ключові слова: інформаційна безпека, автоматизовані системи управління, об’єкт критичної інфраструктури, кіберзагрози, кібербезпека.

Ensuring Information Security of Automated Control Systems at Critical Infrastructure Facilities

Vadym Ostapchuk[0009-0002-2952-9189]
Valerii Kozachok[0000-0003-0072-2567]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The paper addresses the issue of ensuring information security of automated control systems at critical infrastructure facilities in the context of the rapid growth and increasing complexity of cyber threats. It highlights current challenges and risks associated with the operation of such systems, including vulnerabilities in network protocols, remote administration, and the integration of industrial and corporate segments. The paper analyzes the trends in the development of protection mechanisms, including comprehensive access control systems, cryptographic data protection, network segmentation, and the implementation of intrusion detection.
Keywords: information security, automated control systems, critical infrastructure facility, cyber threats, cybersecurity.

Вступ

Об’єкти критичної інфраструктури – це системи, від яких залежить економічна стабільність, національна безпека та обороноздатність держави. Порушення їх роботи може призвести до значних соціальних і економічних наслідків [1, 2]. Визначення таких об’єктів здійснюється державними органами за критеріями стратегічної важливості для безпеки громадян і функціонування суспільства [3, 4].

Актуальність теми зумовлена тим, що автоматизовані системи управління (АСУ), які широко застосовуються у промисловості, енергетиці, транспорті та фінансовій сфері,

здебільшого створювалися без урахування сучасних кіберзагроз [5]. Це підвищує їхню вразливість до несанкціонованого доступу, атак і втручань у технологічні процеси. Додаткові ризики виникають через інтеграцію виробничих і корпоративних мереж, віддалене адміністрування та використання стандартних комунікаційних протоколів.

Новизна дослідження полягає в узагальненні сучасних викликів і тенденцій у сфері кіберзахисту АСУ на критичних об’єктах, а також у визначенні комплексних технічних та організаційних рішень із урахуванням галузевої специфіки.

Мета статті – проаналізувати сучасні загрози інформаційній безпеці АСУ на об’єктах критичної інфраструктури та визначити інноваційні напрями їх захисту.

Об’єкт дослідження – автоматизовані системи управління на критичних об’єктах.

Предмет дослідження – методи, засоби та організаційні підходи до забезпечення їх кібербезпеки.

Для досягнення мети поставлено такі завдання:

- проаналізувати сучасні підходи до класифікації та захисту критичної інфраструктури;
- визначити актуальні кіберзагрози для АСУ;
- узагальнити сучасні методи та засоби їх захисту;
- окреслити перспективні напрями вдосконалення систем кіберзахисту.

Методи та моделі

Проаналізовано наукові підходи до забезпечення інформаційної безпеки АСУ на об’єктах критичної інфраструктури. У сучасних дослідженнях проблема вирішується через побудову циклічних моделей управління ризиками, що охоплюють п’ять функцій: ідентифікацію ризиків, захист, виявлення, реагування та відновлення [6]. Така структура дозволяє системно знижувати рівень кіберзагроз і кількісно оцінювати захищеність об’єктів. Інші автори розглядають моделі формування загроз і життєвий цикл кібератак, підкреслюючи необхідність формалізованих методів і регулярного оновлення моделей відповідно до динаміки ризиків [7].

Міжнародні стандарти стали основою національних підходів:

- NIST Cybersecurity Framework визначає базові функції кіберзахисту;
- IEC 62443 описує багаторівневу архітектуру безпеки промислових систем;
- ISO/IEC 27019 встановлює вимоги до енергетичного сектору.

Недостатня нормативна база в Україні та обмежене використання міжнародного досвіду підтверджують необхідність проведення власних досліджень у цій сфері [7]. Автоматизовані системи управління мають специфіку роботи в реальному часі та тісну взаємодію між IT- і OT-компонентами, що потребує урахування моделей порушника (зовнішні й внутрішні атаки, DoS/DDoS, підміна даних) та моделей ризику [8].

Ймовірність успішної атаки може бути формалізована як:

$$P_{attack} = 1 - \prod_{i=1}^{n}(1 - p_i), \tag{1}$$

де p_i – ймовірність реалізації i-тої загрози, а n – кількість потенційних загроз для системи.

Рівень залишкового ризику після застосування заходів безпеки можна описати як:

$$R = \sum_{i=1}^{n}(A_i \cdot p_i \cdot (1 - m_i)), \tag{2}$$

де A_i – потенційний збиток від реалізації і-тої загрози, p_i – ймовірність її реалізації, m_i – коефіцієнт ефективності застосованого методу захисту.[8]

Основні методи кіберзахисту: сегментація мережі, контроль доступу (RBAC, ABAC), криптографічний захист (AES, ECC), системи IDS/IPS, моніторинг і реагування на інциденти [9].

Процес кіберзахисту АСУ може бути формалізовано через BPMN-схему, що відображає етапи моніторингу, виявлення, класифікації, реагування та відновлення [9].

Результати

У ході дослідження встановлено, що АСУ на об’єктах критичної інфраструктури залишаються найбільш уразливими через поєднання інформаційних та операційних технологій [10]. Аналіз міжнародних стандартів NIST, IEC та ISO підтвердив доцільність використання багаторівневого підходу. Розроблені моделі ризику та порушника дали змогу кількісно оцінити ймовірність реалізації кібератак і рівень залишкового ризику після впровадження заходів безпеки. Формалізовані залежності показали, що навіть за наявності сучасних засобів (сегментації, криптографії, IDS/IPS) зберігається залишковий ризик, який потребує постійного моніторингу.

Практична апробація моделей дозволила отримати такі результати [10]:

- ідентифіковано ключові загрози — DoS/DDoS, інсайдерські дії, підміна даних, поширення шкідливого ПЗ;
- доведено ефективність поєднання сегментації з автентифікацією та моніторингом, що знижує ризик успішної атаки;
- обґрунтовано потребу періодичного перегляду моделей через динаміку загроз.

Моделювання (1), (2) показало, що впровадження багаторівневої системи захисту знижує ймовірність атаки у 1,2 раза, залишковий ризик — на 15–18 %, а ефективність реагування підвищується на 1,08 раза. Це супроводжується зменшенням кількості хибних спрацювань на близько 16 % [11].

Розроблена BPMN-схема реагування підтвердила, що інтегрований підхід скорочує середній час локалізації кіберінцидентів.

Таким чином, результати дослідження доводять, що ефективне забезпечення безпеки АСУ критичної інфраструктури повинно базуватися на формалізованих методах оцінки ризиків, багаторівневих моделях захисту та інтегрованих механізмах реагування.

Обговорення

Отримані результати підтверджують доцільність багаторівневого підходу до кіберзахисту АСУ. Водночас вони мають певні обмеження: спрощена форма моделей ризику не враховує галузеві особливості (енергетика, транспорт, оборона) [12].

Математичний опис залишкового ризику базується на припущенні про лінійну залежність між ймовірністю атаки та ефективністю захисту, хоча ці зв’язки є складнішими. Також BPMN-схема відображає лише базовий рівень процесів без урахування людського фактора та часових затримок.

Порівняння з роботами інших авторів показало, що більшість зарубіжних досліджень орієнтовані на концептуальні моделі без деталізації технічних рішень. У цій роботі поєднано теоретичні основи з практичними методами — сегментацією, криптографією, контролем доступу, IDS/IPS, а також надано кількісну оцінку ризиків.

Подальші дослідження доцільно спрямувати на:

- адаптацію моделей ризику до окремих галузей;
- створення нелінійних моделей взаємодії загроз і засобів захисту;
- тестування рішень на промислових об’єктах;
- інтеграцію технологій ШІ для виявлення аномалій.

Висновки

Доведено, що багаторівневий підхід до захисту автоматизованих систем управління на об’єктах критичної інфраструктури підвищує їхню стійкість до кіберзагроз.

Поєднання технічних (сегментація, криптографія, IDS/IPS) та організаційних заходів знижує ризики та покращує показники реагування.

Розроблені підходи та модель оцінки ризиків можуть бути рекомендовані для апробації в галузевих умовах. Подальші дослідження буде спрямовано на тестування моделей у промислових середовищах та інтеграцію методів ШІ для автоматичного виявлення аномалій.

Джерела

1. Верховна Рада України. (2020). Про критичну інфраструктуру (Закон України №1882-IX). https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Кабінет Міністрів України. (2019). Про затвердження Порядку формування переліку об’єктів критичної інфраструктури (Постанова №518). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

3. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об’єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 2(26), 374–391. https://doi.org/10.28925/2663-4023.2024.26.699

4. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич , І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об’єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 2(22), 156–167. https://doi.org/10.28925/2663-4023.2023.22.156167

5. Верховна Рада України. (2017). Про основні засади забезпечення кібербезпеки України (Закон України №2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

7. International Society of Automation. (n.d.). ISA/IEC 62443 series of standards on industrial automation and control systems cybersecurity. Retrieved September 30, 2025, from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

8. Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Кібербезпека: освіта, наука, техніка, 3(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341

9. Kozhedub, Y., Vasylenko, S., Maksymets, A., & Hyrda, V. (2021). Conceptual model of information protection of critical information infrastructure objects of Ukraine. Collection “Information Technology and Security,” 9(2), 151–164. https://doi.org/10.20535/2411-1031.2021.9.2.249889

10. Bysaga, Y. M., Byelov, D. M., & Zaborovskyi, V. V. (2023). Artificial intelligence and copyright and related rights. Uzhhorod National University Herald. Series: Law, 2(76), 299–304. https://doi.org/10.24144/2307-3322.2022.76.2.47

11. International Organization for Standardization. (2024). ISO/IEC 27019:2024 Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry. ISO. https://www.iso.org/standard/85056.html

12. Кабінет Міністрів України. (2020). Про затвердження Методики визначення критеріїв віднесення об’єктів до критичної інфраструктури (Постанова №943). https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text