ЛІТЕРАТУРА

1. Захисні споруди цивільного захисту. Зі зміною № 1 та №2 : ДБН В.2.2-5:2023. [Чинний від 01.04.2025]. *Мінрозвитку України*, 2023. 115 с.
2. Raisa Barbosa, Mohamad Issa, Sidelmo Silva, & Adrian Ilinca. Variable Speed Diesel Electric Generators: Technologies, Benefits, Limitations, Impact on Greenhouse Gases Emissions and Fuel Efficiency. *Journal of Energy and Power Technology*. 2022. Vol. 4, Issue 1. PP. 1-23. https://doi.org/10.21926/jept.2201003.
3. Razak S., and Normanyo E. Modelling and Simulation of an Electric Motor-Generator Set for Internal Combustion Engine Replacement. *Applications of Modelling and Simulation*/. 2021. Vol. 5. PP. 134–144. http://arqiipubl.com/ojs/index.php/AMS_Journal/article/view/271.

УДК 004.056:355.48

ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ ЧЕРЕЗ ВДОСКОНАЛЕННЯ ПРОЦЕСІВ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Валентина ЯЩУК к.е.н., доцент, Валерія БАЛАЦЬКА доктор філософії (PhD)
Львівський державний університет безпеки життєдіяльності, Україна

Сучасний стан розвитку цифрового середовища зумовлює трансформацію підходів до забезпечення інформаційної безпеки держави, зокрема у сфері захисту критичної інформаційної інфраструктури. Зростання інтенсивності та складності кіберзагроз, а також їх цілеспрямований характер щодо об’єктів державного управління, енергетики, транспорту та фінансової системи актуалізує необхідність переходу від традиційної моделі захисту до концепції кіберстійкості.

Кіберстійкість у цьому контексті доцільно розглядати як інтегральну властивість критичної інформаційної інфраструктури, що забезпечує здатність системи запобігати кіберінцидентам, ефективно їх виявляти, оперативно реагувати та відновлювати функціонування з мінімальними втратами. Ключовим елементом реалізації цієї здатності виступає система управління інцидентами інформаційної безпеки, яка забезпечує перехід від реактивного до проактивного та адаптивного управління загрозами.

Недосконаліть процесів реагування на інциденти є однією з основних причин зниження ефективності функціонування систем захисту. У більшості випадків це проявляється у фрагментарності процедур, відсутності уніфікованих протоколів взаємодії, недостатній автоматизації аналізу подій та обмеженій інтеграції між суб’єктами кібербезпеки. Як наслідок, збільшується час виявлення інцидентів (MTTD) та реагування на них (MTTR), що критично впливає на стійкість державних систем.

Удосконалення процесів реагування на інциденти передбачає їх стандартизацію, формалізацію та інтеграцію у загальну систему управління інформаційною безпекою. Такий підхід забезпечує узгодженість дій усіх суб’єктів кібербезпеки, зменшення часу реагування на інциденти та підвищення рівня керованості процесами протидії кіберзагрозам. Стандартизація процесів реагування полягає у приведенні їх у відповідність до міжнародно визнаних норм і рекомендацій, зокрема ISO/IEC 27001, ISO/IEC 27035 та NIST SP 800-61. У межах цього підходу визначаються єдині принципи класифікації інцидентів, розробляються типові сценарії реагування, встановлюються ролі та відповідальність учасників процесу, а також формуються показники ефективності, зокрема час виявлення та реагування на інциденти. Це створює основу для уніфікації процесів та забезпечує можливість ефективної міжвідомчої взаємодії.

Формалізація процесів реагування передбачає їх детальне документування та закріплення у внутрішніх нормативних актах організації або держави. До таких документів

належать політики реагування на інциденти, регламенти дій, стандартні операційні процедури, матриці ескалації та сценарії реагування на типові загрози. Формалізований підхід охоплює всі етапи життєвого циклу інциденту, включаючи його виявлення, реєстрацію, аналіз, локалізацію, ліквідацію наслідків, відновлення функціонування систем та проведення постінцидентного аналізу. Це дозволяє забезпечити відтворюваність процесів, зменшити вплив людського фактора та створити передумови для проведення аудиту й оцінювання ефективності системи реагування.

Разом з тим важливим напрямом підвищення кіберстійкості є розвиток організаційно-технічної інфраструктури реагування, зокрема центрів моніторингу та реагування на інциденти. Їх ефективність визначається не лише технологічним рівнем, але й ступенем інтеграції з національною системою кібербезпеки, наявністю чітко визначених процедур взаємодії та обміну інформацією. У цьому контексті особливу роль відіграє міжвідомча координація, яка забезпечує консолідацію зусиль державних органів, приватного сектору та міжнародних партнерів.

Підвищення кіберстійкості критичної інформаційної інфраструктури держави досягається через вдосконалення процесів реагування на інциденти, що передбачає ефективну взаємодію між SOC як центрами безперервного моніторингу та первинного реагування і CERT як спеціалізованими командами координації, аналізу та реагування на кіберінциденти на національному та міжвідомчому рівнях. Основна різниця між SOC (Security Operations Center) та CERT (Computer Emergency Response Team) полягає у їхніх функціях, завданнях та методах роботи та наведена в табл. 1.

Таблиця 1

Порівняльна характеристика SOC (Security Operations Center) та CERT (Computer Emergency Response Team)

Критерій	SOC	CERT
Функції	відповідає за постійний моніторинг систем безпеки, виявлення загроз та інцидентів у реальному часі, а також за їхню первинну обробку.	спеціалізується на реагуванні на кіберінциденти, вирішенні кризових ситуацій, аналізі виявлених загроз та розробці стратегій та методів їхнього вирішення.
Область діяльності	зазвичай орієнтований на постійне моніторинг внутрішніх мереж та систем організації або компанії.	може бути внутрішньою чи зовнішньою командою, яка відповідає за реагування на інциденти в різних організаціях або галузях.
Час реакції	реагує на події в реальному часі, намагаючись виявити та припинити загрози якнайшвидше.	може бути активований після виявлення серйозних кіберінцидентів для проведення розслідування та реагування на них.
Аналіз інцидентів	зазвичай використовує автоматизовані системи та методи для виявлення та аналізу загроз.	зазвичай використовує більш ретельний аналіз та дослідження для визначення походження та масштабу кіберінцидентів

Комплексна реалізація зазначених підходів сприяє суттєвому підвищенню ефективності реагування на інциденти, зокрема скороченню часу їх виявлення та нейтралізації, підвищенню точності аналізу загроз і зменшенню негативних наслідків для інформаційних систем. У ширшому контексті це забезпечує підвищення рівня кіберстійкості критичної інформаційної інфраструктури держави, оскільки дозволяє не лише протидіяти кіберзагрозам, але й забезпечувати стабільність функціонування систем в умовах їх реалізації.

Таким чином, підвищення кіберстійкості критичної інформаційної інфраструктури держави безпосередньо залежить від рівня зрілості процесів управління інцидентами. Їх удосконалення має здійснюватися на основі комплексного підходу, що поєднує стандартизацію процедур, розвиток інституційної спроможності, впровадження сучасних технологій аналізу та забезпечення ефективної координації між усіма суб’єктами кібербезпеки. Саме така інтегрована модель дозволяє забезпечити стійкість державних інформаційних систем в умовах постійно зростаючих кіберзагроз.

ЛІТЕРАТУРА

1. Polotai, O., Brych, T., Kukharska, N., Yashchuk, V., & Tkachenko, A. (2025). Інтеграція систем виявлення вторгнень у структуру корпоративної мережі: Підходи, виклики та ефективність реагування на інциденти. Кібербезпека: освіта, наука, техніка**,** (1(29))**,** 405–418. https://doi.org/10.28925/2663-4023.2025.29.889
2. Yashchuk, V. I. (2024). Роль та місце Стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. In Moderní aspekty vědy: XLII (pp. 259–286). Mezinárodní Ekonomický Institut s.r.o. https://doi.org/10.52058/42-2024
3. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Integrative approach to the analysis, modeling, and ensuring cyber security of critical information infrastructure under modern threats. Baltic Journal of Economic Studies**,** 11(2), 273–286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286

УДК 628.17:628.74:628.16

ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ ПРОТИПОЖЕЖНОГО ВОДОПОСТАЧАННЯ ТА ВОДООЧИЩЕННЯ В УМОВАХ ПОШКОДЖЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Олександр СІПКО, Богдан ТИЩЕНКО
Національний університет цивільного захисту України

В умовах війни забезпечення безперебійного функціонування систем водопостачання набуває особливого значення для цивільного захисту населення та підтримання функціональної стійкості критичної інфраструктури. Пошкодження магістральних трубопроводів, насосних станцій, резервуарів, споруд водопідготовки, систем електроживлення та автоматизованого керування призводить не лише до порушення господарсько-питного водопостачання, а й до ускладнення гасіння пожеж, ліквідації наслідків надзвичайних ситуацій та забезпечення населення водою нормативної якості [3,4]. За таких умов системи протипожежного водопостачання та водоочищення доцільно розглядати як взаємопов’язані складові безпеки територій і об’єктів.

Для об’єктів критичної інфраструктури зазначена проблема є суттєвою, оскільки порушення функціонування систем водопостачання безпосередньо впливає на безперервність надання життєво важливих послуг, ефективність аварійного реагування та рівень захищеності населення [3]. У сучасних умовах пошкодження інженерних мереж може бути наслідком бойових дій, пожеж, вибухів, відключення електроенергії, ускладнення логістики ремонтно-відновлювальних робіт та дефіциту обслуговуючого персоналу. Це зумовлює необхідність переходу від традиційного підходу до експлуатації систем водопостачання до підходу, орієнтованого на резервування, автономізацію та готовність до функціонування в аварійному режимі [3,4].

Однією з найбільш вразливих складових є система зовнішнього протипожежного водопостачання. Руйнування водопровідної мережі, пошкодження пожежних гідрантів, зниження тиску, відмова насосного обладнання або втрата доступу до окремих ділянок мережі істотно зменшують фактичну витрату води на пожежогасіння [2]. Наслідком цього є збільшення часу розгортання пожежно-рятувальних підрозділів, потреба у підвозі води, використанні альтернативних джерел водозабору та зростання ризику поширення пожежі на суміжні об’єкти. Для об’єктів критичної інфраструктури локальна відмова зовнішнього протипожежного водопостачання може спричинити каскадний розвиток небезпечних подій, що підвищує вимоги до надійності та резервування системи [2,3].