УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.101

ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРВІЙНИ

Дорофєєва К. І.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: dorofieieva.kseniia@nure.ua

The current issues of protecting critical infrastructure facilities in the context of cyber warfare is considered. In addition, the importance of continuously updating and improving protection measures to effectively counter rapidly changing cyber threats is considered. The threats that affect the security of critical infrastructure in the conditions of cyber warfare have been identified The importance of paying attention to this issue and emphasizing the need for continuous improvement of cybersecurity strategies to ensure the continuity of critical infrastructure in the era of digital threats is described.

В умовах війни захист об’єктів критичної інфраструктури є одним із важливих пріоритетів держави. В сучасних умовах відбувається й кібервійна, у зв’язку з чим ризики для інфраструктури суттєво зростають. Адже саме від стану захищеності її об’єктів багато у чому залежить і національна безпека. Тому численні та цілеспрямовані кібератаки ворога спрямовані, у першу чергу, на підрив основ національної безпеки країни, насамперед, шляхом заподіяння шкоди державним інформаційним ресурсам та об’єктам критичної інфраструктури [1].

Здійснення заходів з кіберзахисту передбачає [2-5]:

- ідентифікацію – виявлення реальних і потенційних кіберзагроз для запобігання та їх нейтралізації;
- захист – розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем;
- виявлення – проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;
- реагування – вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізацію їх можливих наслідків, удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та співрозмірності можливостей таких систем реальним та потенційним ризикам;

- відновлення – поновлення штатного режиму функціонування інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення передумов для проведення розслідування за наслідками кібератаки.

Під час забезпечення функціонування базисної інфраструктури кіберзахисту забезпечується:

- захист у кіберпросторі національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;
- захист об’єктів критичної інфраструктури;
- захист інтересів громадянина та суспільства у кіберпросторі;
- здійснення заходів з формування культури кібербезпеки в установах, на об’єктах критичної інфраструктури і підприємствах;
- інформування громадян про кіберінциденти.

Головним завданням технологічної інфраструктури кіберзахисту є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, в тому числі шляхом: збору, аналізу, оцінювання, узагальнення та поширення інформації про кіберінциденти; надання методичної допомоги іншим суб’єктам кіберзахисту; взаємного інформування суб’єктів кіберзахисту про нові реальні та потенційні загрози; створення умов для відповідального та довіреного обміну інформацією між суб’єктами кіберзахисту всіх секторів кіберзахисту [1, 4, 5].

Об’єкти критичної інфраструктури – це стратегічно важливі підприємства та установи, необхідні для функціонування суспільства країни та її економіки. Захист об’єктів критичної інфраструктури – комплексне та пріоритетне завдання держави в умовах сьогодення.

Список використаних джерел

1. Yevseiev, Serhii, et al. "Development of a concept for building a critical infrastructure facilities security system." Eastern-European Journal of Enterprise Technologies 3.9 (2021): 111.
2. Іваненко О.І. Підхід до національної оцінки ризиків для критичної інфраструктури. Вісник ХНТУ. 2020. № 2(73). С. 9-22.
3. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ "ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.
4. Про затвердження Положення про організаційно-технічну модель кіберзахисту. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 01.03.2024).
5. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 04.03.2024).