**Дуліна О.В.,**
к.ю.н., доцент, доцент кафедри публічного управління та регіоналістики
Навчально-науковий інститут публічної служби та управління
Національного університету «Одеська політехніка»
м. Одеса

# РИЗИК-ОРІЄНТОВАНЕ УПРАВЛІННЯ ІНФРАСТРУКТУРНОЮ БЕЗПЕКОЮ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Аналіз ситуації показує, що в наслідок агресії РФ руйнування об'єктів критичної інфраструктури спричинило серйозні втрати для економіки та держави в цілому. Багато об'єктів, таких як електростанції, водопровідні системи, транспортні мережі та комунікаційна інфраструктура, залишаються позбавленими функціональності або працюють на мінімальному рівні продуктивності через руйнування та несправності [3]. Крім того, аналіз вітчизняної та світової практики свідчить, що кризи які впливають на роботу критично важливих об’єктів інфраструктури можуть виникнути у зв’язку з пандемією, кліматичними ризиками та іншими природними небезпеками, кібератаками чи терористичними атаками.

У Стратегії забезпечення державної безпеки від 16 лютого 2022 року № 56/2022 [5] об’єкти критичної інфраструктури згадані серед об’єктів забезпечення державної безпеки нарівні з державним суверенітетом, конституційним ладом і територіальною цілісністю країни, що свідчить про високий рівень їх значимості.

У зв’язку з чим важливим завданням для органів місцевої влади, функціональних органів, визначених відповідальними за функціонування окремих державних систем захисту та реагування, операторів критичної інфраструктури - є впровадження заходів зі зниження ризику як невід'ємної частини стратегій і програм у сфері захисту та безпеки інфраструктурних об’єктів і збільшення стійкості держави до негативного впливу загроз.

Концепцію створення державної системи захисту критичної інфраструктури [2] передбачено на місцевому та об’єктовому рівнях розроблення, затвердження і виконання місцевих програм забезпечення захисту та стійкості критичної

інфраструктури, програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням доступу до життєво важливих ресурсів. Згідно методичних рекомендацій уповноважених органів розробка зазначених програмних документів відбувається на основі ідентифікації та аналізу ризиків та загроз об'єктам інфраструктури.

У 2023 році в Україні затверджено Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури (КІ) [4], одними з основних стратегічних цілей якого визначено створення системи координації, взаємодії суб'єктів національної системи захисту КІ, впровадження управління ризиками КІ; налагодження функціонування системи обміну інформацією під час реагування на загрози та кризові стани.

Ризики та загрози інфраструктурним об'єктам класифікують на матеріальні ризики, до яких відносяться фізичні та природні ризики для частин активів, критичних для функціонування об'єкта критичної інфраструктури; ризики кібербезпеки та інформаційної безпеки; ризики, пов'язані з людським фактором – ризики, які створює персонал (працівники) об'єкта критичної інфраструктури; ризики ланцюжка постачання.

Організація управління ризиками безпеки включає:

- визначення вихідних даних щодо функціонування об'єкту критичної інфраструктури (область застосування, внутрішні і зовнішні чинники, критерії щодо управління ризиками безпеки);
- визначення суб'єктів національної системи захисту критичної інфраструктури, які виконують завдання/заходи щодо управління ризиками безпеки; визначення методів, інструментів та механізмів, які використовуються в ході управління ризиками безпеки;
- ідентифікацію та планування ресурсів, необхідних для управління ризиками безпеки, зокрема людські, інформаційні, фінансові, матеріально-технічні. Вкрай важливим є визначення засобів та заходів щодо забезпечення комунікації в ході управління

ризиками безпеки.

Ризик-орієнтоване мислення дає змогу управлінцям швидко адаптуватися до змін і реагувати на кризові моменти у світі, країні  чи в компанії вчасно та адекватно загрозам. Метою оцінювання безпеки об’єктів інфраструктури є встановлення можливих ризиків та негативних наслідків їх прояву для інфраструктурних об’єктів. При проведенні оцінки негативних наслідків надзвичайних ситуацій на об’єктах критичної інфраструктури має враховуватися шкода для життя і здоров’я людей, виражена через кількість постраждалих, травмованих, загиблих, евакуйованих. Управління ризиками на об'єктах критичної інфраструктури є складним завданням, що потребує комплексного підходу. Один з ключових аспектів цього управління – це управління проєктними ризиками. Це означає врахування можливих проблем, які можуть виникнути на будь-якому етапі реалізації спеціальних проєктів – від планування до введення в експлуатацію і подальшого функціонування.

У контексті захисту національної безпеки, об’єкти КІ є основою життя і безпеки країни, тому їх захист стає пріоритетним завданням у разі воєнного конфлікту чи надзвичайної ситуації [1].

Отже, багатоаспектність проблем захисту критичної інфраструктури детермінує необхідність систематичного аналізу ризиків в управлінні безпекою (ризик-аналізу) [6]. Особливість критичного ризик-аналізу полягає в тому, що розглядаються потенційно негативні наслідки, які можуть виникнути у результаті відмови в роботі технічних систем, збоїв або помилок з боку персоналу об’єкта та ін. Система управління ризиками безпеки на об’єктах критичної інфраструктури має являти собою сукупність задокументованих і затверджених політики, правил, методик і процедур управління ризиками безпеки, які визначають порядок дій оператора критичної інфраструктури, спрямованих на здійснення систематичного процесу вимірювання, моніторингу, контролю, звітування та обробки ризиків безпеки, в тому числі Паспорт безпеки на об’єкт критичної інфраструктури.

**Список використаних джерел:**


1. Бубела Т.З., Мельник М.Я., Назаровець О.Б., Рудик Ю.І Аналіз визначень та нормативних вимог системи захисту об’єкта критичної інфраструктури. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 29. С. 119-127. https://doi.org/https://doi.org/10.32447/20784643.29.2024.13

2. Концепція створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12. 2017р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

3. Магомедов А. О. Ризики та загрози для об’єктів критичної інфраструктури та шляхи їх подолання. *Інвестиції: практика та досвід*. No 15. 2024. С.216-221. URL: https://www.nayka.com.ua/index.php/investplan/article/view/4320/4355

4. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". Указ Президента України від 16.02.2022 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/ 2022#Text

6. Яременко О., Страхніцький Я. Визначення та управління загрозами у структурі державної політики. *Університетські наукові записки*, 2022, № 3 (87), С. 73-82. URL: file:///C:/Users/Asus/Downloads/359-Article%20Text-629-4-10-20220817%20(1).pdf