

СЕКЦІЯ «СИСТЕМНИЙ АНАЛІЗ ТА ОБЧИСЛЮВАЛЬНА МАТЕМАТИКА»

УДК 005.21:351.86:711.4

Бахрушин В.Є.

проф. НУ «Запорізька політехніка»

СИСТЕМНИЙ АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПРИФРОНТОВИХ МІСТ

Захист критичної інфраструктури є важливим складником діяльності органів державної влади, у т.ч. ЦВА, місцевого самоврядування, відповідних підприємств, установ та організацій у період воєнного стану. Поняття критичної інфраструктури визначено Законом України «Про критичну інфраструктуру» [1]. Цей Закон системно описує основні засади, мету і завдання державної політики у сфері захисту критичної інфраструктури, рівні управління системою захисту, критерії зарахування об'єктів до критичної інфраструктури тощо. При цьому функції з визначення порядку віднесення конкретних об'єктів до критичної структури, створення і використання відповідного реєстру покладено на Кабінет Міністрів України. До критичної інфраструктури прифронтових міст, зокрема належать органи державного управління та місцевого самоврядування, системи енергозабезпечення, включно із постачанням теплової енергії, водопостачання та водовідведення, транспортна інфраструктура, електронні комунікації, продовольче забезпечення, охорона здоров'я, електронні комунікації, установи, що надають фінансові послуги, деякі промислові підприємства та ін. Для цих груп існують як спільні, так і специфічні загрози, ризики та методи захисту. Також варто зазначити, що виокремлені групи об'єктів не є незалежними одна від одної. Руйнування або істотне пошкодження об'єктів одного із складників критичної інфраструктури веде до суттєвих порушень роботи інших складників.

Як свідчить практика останніх війн, зокрема російсько-української війни, військової операції США та Ізраїлю проти Ірану, одним з основних об'єктів атак стає енергетична інфраструктура. Для цього є очевидні підстави. Її руйнування унеможливорює чи істотно ускладнює функціонування практично всієї іншої критичної інфраструктури. За даними DiXi Group [2] від 24.02.2022 до початку 2026 р. лише під час масованих обстрілів енергетичну інфраструктуру України атакували близько 2900 російських ракет та 12700 ударних дронів. При цьому близько 12800 атак відбулися у 2025-2026 р. Відповідно до звіту КШЕ [3], на початок 2026 р. загальні збитки в енергетичному секторі становили \$75,3 млрд. по доходах і \$15,1 млрд по доданій вартості. Ці дані не враховують непрямі втрати в

інших секторах, зумовлені значним скороченням генерації електроенергії та видобутку й переробки енергоресурсів, знищенням значної частини засобів передачі електроенергії тощо та відповідними обмеженнями на їх споживання. Також вони не враховують втрати через те, що деякі потужні виробники опинилися на тимчасово окупованій території. Серед інших складників критичної інфраструктури найбільш постраждалими за фінансовими втратами, кількістю знищених/пошкоджених об'єктів та кількістю атак є портова та залізнична інфраструктура, заклади охорони здоров'я. Слід зазначити, що значно більших втрат зазнали об'єкти, що не належать до критичної інфраструктури, але є важливими для життєдіяльності прифронтових міст. Значна частка їх втрат пов'язана з пошкодженням чи знищенням критичної інфраструктури.

Сьогодні найчастіше обговорюють прямі ризики, пов'язані з атаками ракетами, ударними БПЛА, КАБами на об'єкти критичної інфраструктури. Для запобігання таким ризикам використовують різні підходи від знищення підприємств, що виготовляють відповідну зброю, складів, пускових установок до їх збиття під час польоту чи примусової посадки або відхилення від цілі. Для створення ефективних систем захисту необхідно використовувати всі опції, але вибір конкретних засобів і підходів має визначатися з використанням оптимізаційних моделей та врахуванням пріоритетів захисту конкретних об'єктів, даних про імовірність враження визначених цілей, доступності і вартості конкретних засобів враження тощо. Для багатьох об'єктів критичної інфраструктури не менш важливими є ризики, зумовлені хакерськими атаками, фінансовою неспроможністю, відсутністю матеріальних, кадрових та інших ресурсів, необхідних для ефективного захисту, тощо.

Для вирішення наявних проблем варто використовувати методи та інструменти системного аналізу (прийняття багатокритеріальних рішень за умов невизначеності, SWOT, PESTLE, оптимізації, прогнозування тощо), моделювання складних систем, аналізу даних, штучного інтелекту та ін.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20/conv#n410> (дата звернення : 14.04.2026).
2. DiXi Group. URL: <https://dixigroup.org/en/over-four-years-of-full-scale-war-russia-has-launched-more-than-60-massive-attacks-on-ukraines-energy-sector> (дата звернення : 14.04.2026).
3. KSE-Institute. URL: https://kse.ua/wp-content/uploads/2026/02/KSE-Institute_Losses-2026-Report-en-2.pdf (дата звернення : 08.04.2026).