Класифікація загроз критичній інфраструктурі України під час війни

Павло Пасічник, канд. техн. наук, доцент [1] (ORCID: 0000-0001-8499-6949)
Олексій Варварчук, магістр [1] (ORCID: 0009-0005-6904-1868), **Андрій Широков,** аспірант[1] (ORCID: 0009-0008-0602-7083)
[1] *Київський національний університет будівництва і архітектури , Україна*

АНОТАЦІЯ

У статті розглянуто сутність критичної інфраструктури (КІ) як системи об'єктів, мереж та ресурсів, що мають вирішальне значення для національної безпеки, економіки, охорони здоров'я, довкілля та життєзабезпечення населення. Наведено перелік основних секторів КІ, зокрема енергетика, транспорт, зв'язок, водопостачання, медицина та цифрові фінансові системи. Особливу увагу приділено аналізу загроз, що постають перед КІ в умовах війни, зокрема під час російсько-українського збройного конфлікту. Окреслено класифікацію загроз: фізичні, кіберзагрози, соціально-політичні, техногенні, природні та комбіновані. Проаналізовано характер кожного типу загроз, їхні джерела, приклади реалізації та потенційні наслідки. Зазначено, що хоча фізичне знищення об'єктів КІ є головною загрозою в умовах війни, не менш небезпечними є соціально-політичні та техногенні ризики, які посилюються під час воєнного стану. Зроблено висновок про необхідність посилення державної політики у сфері безпеки критичної інфраструктури, пошуку нових рішень і адаптації систем захисту до сучасних викликів.

Ключові слова: критична інфраструктура; види загроз для критичної інфраструктури під час війни; техногенні катастрофи..

1. ВСТУП

У сучасних умовах, коли Україна перебуває в стані повномасштабної війни, питання захисту критичної інфраструктури набуває особливої актуальності. Від стійкості та безперебійного функціонування таких об'єктів, як енергетичні станції, транспортні вузли, системи зв'язку та водопостачання, залежить не лише національна безпека, а й життя мільйонів громадян. Складність сучасних загроз — від ракетних ударів до кібератак і соціальних заворушень — вимагає системного підходу до аналізу ризиків та розробки ефективних механізмів захисту. У даній роботі розглянуто основні види загроз для критичної інфраструктури, їх джерела, приклади та наслідки в умовах воєнного та мирного часу.

2. МЕТА

Метою доповіді є проаналізувати основні загрози для критичної інфраструктури України в умовах воєнного стану та окреслити напрями її захисту з урахуванням сучасних викликів.

3. ОСНОВНА ЧАСТИНА

Критична інфраструктура (КІ) – об'єкти, системи, мережі, ресурси, які мають вирішальне значення для національної безпеки, оборони, охорони здоров'я, економіки, екології, безпеки життя і здоров'я громадян [1]. До КІ можна віднести об'єкти енергетики (АЕС, ТЕЦ, ТЕС, трансформаторні підстанції, тепломережі тощо), нафтогазова галузь (НГПЗ, компресорні станції, газорозподільчі станції, газосховища, інфраструктура родовищ тощо), транспортної інфраструктури (залізниця, мости та тунелі, порти, аеропорти та вокзали, тощо), водопровідні системи (насосні станції, водопідйоми, очисні споруди тощо), системи зв'язку (базові станції мобільного зв'язку, антенно-щоглові споруди, передавачі тощо), медичні заклади (лікарні, перинатальні центри, лабораторії тощо), платіжні системи (цифрова інфраструктура), аварійно-рятувальні служби і т.і.[2] Під час російсько-української війни удари по критичній інфраструктурі України є регулярним явищем, не зважаючи на Женевські чи Гаазькі конвенції, Римський статут чи заклики ООН. Захист ключових інфраструктурних об'єктів є невід'ємною складової державної політики та оборонної стратегії України.

Головною загрозою під час бойових дій для критичної інфраструктури звісно є дії ворога, проте не варто нехтувати і загрозами, які присутні в мирний час, адже їх вплив та небезпека може кратно підсилюватися під час війни. Так, спеціалісти визначають наступні загрози для критичної інфраструктури: фізичні, кібер-, соціально-політичні, техногенні, природні та комбіновані [2,3,4]. Класифікацію загроз приведено в таблиці 1.

Таблиця1. Класифікація загроз для критичної інфрастуктури

Вид	Джерело	Приклади
Фізичні	Ворог	Ракетні та дронові удари по енергетичним об'єктам України
Кіберзагроза	Ворог, терористи, хакерські групи	DDoS – атака на Київстар, Укрзалізницю і т.і.
Соціально-політичні	Суспільство, люди	Страйк шахтарів, перекриття трас державного значення, розповсюдження паніки через дезінформацію
Техногенна	Технології, людський фактор, час	Аварія на ЧАЕС, пориви газопроводів чи теплотрас
Природна	Пиродні явища	Снігові замети на дорогах, повені, лісові пожежі тощо
Комбінована	Ворог	Фізична атака на інфраструктуру + дезінформаційна кампанія

Фізичні загрози – це можливість прямого фізичного пошкодження об'єктів КІ. До таких загроз можна віднести: навмисні ракетні, артилерійські, дронові атаки чи авіаудари; терористичні акти та диверсії у вигляді підпалів чи підривів. Такі загрози, як правило, реалізуються під час безпосередньо воєнних дій або стадії підготовки до них або ж терористичними організаціями чи психічнохворими індивідами.

Кіберзагрози –це будь-яка потенційна дія в цифровому середовищі, яка може завдати шкоди інформаційним системам, даним, мережам або ІТ-інфраструктурі, а також порушити їхню конфіденційність, цілісність або доступність. Прикладами таких загроз є DDoS-атаки (підвищене навантаження на сайт чи сервер), провадження шкідливого програмного забезпечення, несанкціоновані проникнення в різні системи, зливи даних тощо. Джерелами кіберзагрози є ворожі спецслужби, кіберзлочинні угруповування, окремі хакери та ін. [5,6]

Соціально-політичні загрози – це загрози, які провокуються людським фактором, державною політикою чи соціальною напругою. Основним чинником таких загроз є масові протести (блокування доріг, захоплення об'єктів, страйки працівників), недолугість політичної системи (перехід контролю над об'єктами КІ), зовнішній політичний тиск (торгові блокади, санкції тощо), провокації ворожих спецслужб (дезінформація, шпигунство, зливи тощо), передвиборча нестабільність. Соціально-політичні загрози є важкопередбачцваними та можуть мати великий суспільний резонанс, що супроводжується панікою або навіть економічним шоком.[5,6,7]

Техногенні та природні загрози є загрозами мирного часу, боротьбу з якими держава, суб'єкти господарювання та населення веде на постійній основі, проте військові дії можуть підсилювати їх ефект [7,8]. Так, не зважаючи на можливість підприємств критичної інфраструктури бронювати співробітників, велика кількість висококваліфікованого персоналу залучаються до безпосерднього захисту держави у лавах сил оборони. Це призводить до зниження якості управління та обслуговування об'єктів КІ. В той же час постійні фізичні атаки на ключові інфраструктурні об'єкти змушують експлуатувати обладнання, мережі та перш за все людей в екстремальних умовах, не дотримуючись певних технологічних регламентів, законів про працю тощо. Все це провокує підвищення ризику техногенних катастроф на об'єктах КІ та недостатньої підготовки до можливих природніх загроз.

Комбіновані загрози для критичної інфраструктури як раз найбільш характерні для періодів збройної агресії, адже сукупність факторів різного походження дають найбільш нищивний ефект. Так, атака на фізичні потужності в сукупності з атакою на систему управління значно масштабують ефект цих акт. На думку авторів, комбіновані загрози є найбільш небезпечними та тими, що визначають націленість ворогів на тотальне нищення держави та її основної функції – захисту громадян.

4. ВИСНОВКИ

Таким чином, підсумовуючи вище зазначене, можна сказати, що під час війни важливим та пріоритетним вектором безпекової політики нашої держави має збереження стійкості національної критичної інфраструктури та пошук нових ефективних рішень щодо її захисту.

Список літератури

[1] Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.10.2025).

[2] Бірюков Д. С., Кондратов С. І Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / ред. О.М. Суходолі. К. : НІСД, 2016. 176 с.

[3] Грічанінов Г. Ф. Актуальні проблеми модернізації ризиків і загроз критичних інфраструктур.URL: http://www.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/ article/15026.3.1.002.pdf. (дата звернення: 28.09.2025)

[4] Бірюков Д. С. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки: Аналітична записка. URL: file:///C:/Users/Student/Desktop/nivanb_2015_3-4_14.pdf (дата звернення : 28.09.2025)

[5] Handbook on Securing Cyber-Physical Critical Infrastructure. Elsevier, 2012. URL: https://doi.org/10.1016/c2011-0-04434-4 (date of access: 04.10.2025).

[6] Лядовська В. М., Рябий М. О., Гнатюк С. О. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів. Зв'язок. 2014. №4. С. 3□7.

[7] Critical infrastructure protection / ed. by United States. Government Accountability Office. New York : Nova Science, 2008.

[8] Уряднікова І. В., Чумаченко С. М., Кармазін С. В.,Тесленко О. М. Застосування експертно-аналітичних методівдля оцінювання ризиків надзвичайних ситуацій на об'єктахкритичної інфраструктури. Науковий вісник Академіїмуніципального управління. Серія : Техніка. 2015. Вип. 1.С. 206-218.