УДК 351.865

О. Л. Назаренко, О. М. Головань, В. В. Рудинський

ЩОДО ПИТАННЯ ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Питання захисту критичної інфраструктури в умовах воєнного стану набуває першочергового значення. Критична інфраструктура включає в себе об'єкти, системи й мережі, безперебійна робота яких життєво важлива для функціонування держави, економіки та добробуту громадян. Оцінювання вразливості таких об'єктів дає змогу виявити слабкі місця в системі безпеки, запобігти потенційним атакам і забезпечити ефективне планування заходів реагування у межах забезпечення державної безпеки.

Запропоновано науково обґрунтований підхід до оцінювання вразливості об'єктів критичної інфраструктури України в умовах воєнного стану з урахуванням сучасних загроз (воєнних, кібернетичних, диверсійних).

Ключові слова: *об'єкти критичної інфраструктури, вразливості, ризики, загрози.*

Постановка проблеми. Об'єкти критичної інфраструктури (ОКІ) є ключовими елементами забезпечення стабільного функціонування держави, суспільства, економіки й національної безпеки. Саме ці об'єкти стають пріоритетними цілями для противника, що зумовлює необхідність їх надійного захисту та своєчасного реагування на потенційні загрози. Важливо насамперед оцінити їхню вразливість, аби своєчасно виявляти слабкі місця, посилювати захист і швидко реагувати на можливі небезпеки.

Застосування високотехнологічних засобів ураження, зокрема безпілотних літальних апаратів (БПЛА), засобів радіоелектронної боротьби, а також широкомасштабних кібератак, істотно підвищує рівень ризиків для елементів критичної інфраструктури. Тому особливого значення набуває оцінювання вразливості таких об'єктів, що дає змогу виявити потенційно слабкі місця у системі безпеки, здійснити пріоритизацію заходів захисту й розробити ефективні стратегії реагування.

Попри актуальність зазначеної проблематики, в Україні сьогодні потребує вдосконалення методика оцінювання вразливості ОКІ, яка має бути адаптована до умов воєнного стану. Підходи, що застосовуються, є фрагментарними, а в окремих випадках і застарілими, оскільки розроблені в контексті мирного періоду. Крім того, практична реалізація заходів із захисту інфраструктури часто не має системного характеру, що знижує загальний рівень національної безпеки.

Отже, існує нагальна потреба у науково обґрунтованому підході до оцінювання вразливості ОКІ, який би враховував специфіку сучасних воєнних загроз, включав міждисциплінарні методи аналізу й забезпечував підґрунтя для прийняття рішень у сфері безпеки держави. У сучасному контексті оцінювання вразливості об'єктів критичної інфраструктури набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Проведено огляд керівних документів, наукових джерел і публікацій стосовно оцінювання вразливості, стану захисту й потенційних загроз для об'єктів критичної інфраструктури, зокрема в Україні. У наказі [1] затверджено порядок проведення оцінювання вразливості ядерних установок та ядерних матеріалів. Наказом [2] затверджена методика, критерії та показники оцінювання стану захищеності об'єктів критичної інфраструктури від епідемій, кіберзахисту та визначення рівня захисту від економічного тероризму. Критерії оцінювання і загрози критичній інфраструктури визначено у науковій статті [3]. Авторами праці [4] запропонована методика оцінювання ризиків і загроз об'єктам критичної інфраструктури під час вогневого впливу противника. У статті [5] розглянуто методику оцінювання загроз і ризиків для ОКІ за сценаріями розвитку надзвичайних ситуацій. Методику оцінювання захищеності кіберпростору об'єктів критичної інфраструктури запропоновано у праці [6].

Зазначені публікації висвітлюють різні оціночні аспекти ОКІ, зокрема методи ідентифікації, управління ризиками, кібербезпеку й використання сучасних технологій для моніторингу і захисту. Однак у керівних документах і дослідженнях [1 – 6] бракує уваги питанням оцінювання вразливості ОКІ в умовах воєнного стану.

Метою статті є вдосконалення науково обґрунтованого підходу до оцінювання вразливості об'єктів критичної інфраструктури України в умовах воєнного стану з урахуванням сучасних загроз (воєнних, кібернетичних, диверсійних).

Для досягнення поставленої мети вирішено такі часткові завдання дослідження: проаналізовано сучасний стан проблеми оцінювання вразливості об'єктів критичної інфраструктури в науковій і практичній площині; ідентифіковано основні види загроз для об'єктів критичної інфраструктури, актуальні в умовах військового конфлікту; визначено ключові критерії та індикатори вразливості ОКІ; розроблено методичний підхід до оцінювання вразливості з урахуванням комплексного аналізу ризиків; досліджено можливості інтеграції сучасних технологій (GIS, штучного інтелекту, систем раннього виявлення тощо) у процес оцінювання та моніторингу вразливості; запропоновано рекомендації щодо підвищення стійкості й захищеності об'єктів критичної інфраструктури на національному рівні.

Виклад основного матеріалу. Оцінювання вразливості об'єктів критичної інфраструктури – це процес виявлення, аналізу та пріоритизації слабких місць у фізичних і кібернетичних компонентах інфраструктури з урахуванням міжсистемних взаємозв'язків, які можуть бути використані противником для знищення або виведення з ладу об'єктів критичної інфраструктури. Цей процес передбачає ідентифікацію ОКІ, аналіз та оцінювання ризиків, визначення ймовірності загроз і їх впливу на об'єкт. Здійснюється дослідження фізичних, технічних, кібернетичних, організаційних і людських чинників безпеки.

Першим кроком ідентифікації об'єктів критичної інфраструктури є визначення, які саме об'єкти входять до складу критичної інфраструктури. Це можуть бути: енергетичні системи (електростанції, підстанції, газогони); транспортні вузли (мости, залізничні станції, аеропорти); об'єкти зв'язку й телекомунікацій; водопостачання і каналізаційні системи; медичні установи, урядові будівлі, інформаційні центри тощо. Ідентифікація ОКІ являє собою один із ключових етапів формування ефективної системи їх захисту та оцінювання вразливості. Визначення таких об'єктів дає змогу здійснити пріоритизацію ресурсів, сконцентрувати зусилля на найбільш значущих елементах і забезпечити адресне планування заходів безпеки.

Згідно із Законом [7] до об'єктів критичної інфраструктури належать матеріальні й віртуальні елементи систем, що мають важливе значення для національної безпеки, економіки, охорони здоров'я, довкілля та суспільного життя. Це енергетичні об'єкти, транспорт, зв'язок, ІТ-системи, об'єкти охорони здоров'я, водопостачання, фінансові інститути тощо.

Ідентифікація об'єктів критичної інфраструктури має ґрунтуватися на визначених критеріях значущості, як-от: масштаби потенційних наслідків у разі їх виходу з ладу; ступінь залежності інших об'єктів або систем від їхнього функціонування; можливість швидкого відновлення; значення для обороноздатності й безпеки держави.

У сучасній практиці до ідентифікації ОКІ застосовуються такі підходи [8]:

– секторальний аналіз, який передбачає оцінювання об'єктів у межах окремих сфер (енергетика, транспорт, охорона здоров'я тощо);

– матричний підхід, що базується на оцінюванні взаємозалежностей між об'єктами та можливості каскадного ефекту;

– інформаційно-аналітичний підхід, що включає оброблення великих масивів даних про інфраструктуру з використанням ГІС-технологій і систем підтримки прийняття рішень;

– інтегрований ризик – орієнтований підхід, який передбачає одночасний облік рівня загроз, уразливостей та можливих наслідків.

У Європейському Союзі (ЄС) для ідентифікації ОКІ функціонує система EPCIP (Європейська програма захисту критичної інфраструктури), яка передбачає обов'язкову ідентифікацію «Європейських критичних інфраструктур» (ECI) за погодженими критеріями. У США ідентифікація проводиться за 16 секторами критичної інфраструктури в межах програми NIPP (National Infrastructure Protection Plan). Обидві системи наголошують на пріоритетності ідентифікації залежностей і вразливих точок у міжгалузевій взаємодії.

В умовах війни процес ідентифікації ускладнюється такими чинниками: обмежений доступ до актуальної інформації з міркувань безпеки; постійна зміна конфігурації інфраструктурної мережі через руйнування та релокацію; наявність прихованих або нестандартних об'єктів, що відіграють критичну роль; недосконаліть методик і брак єдиної державної інформаційної платформи.

Задля підвищення ефективності ідентифікації ОКІ в Україні впроваджено стандартизовані критерії оцінювання значущості, а також розроблено інтегровану національну інформаційну систему ідентифікації та моніторингу [9, 10].

Успішна ідентифікація об'єктів критичної інфраструктури вимагає інтегрованого підходу, що враховує як національне законодавство, так і міжнародні практики, ризик-орієнтовані методи, взаємозалежності між об'єктами, а також упровадження сучасних інформаційно-аналітичних інструментів. Особливої актуальності це завдання набуває в умовах воєнного стану, коли критична інфраструктура не лише забезпечує життєдіяльність суспільства, а й безпосередньо впливає на обороноздатність держави.

Комплексне оцінювання вразливості ОКІ [1, 11] неможливе без глибокого аналізу потенційних загроз. На цьому етапі визначаються джерела загроз, їхня природа, можливі сценарії розвитку, рівень впливу на об'єкти, а також імовірність їх виникнення. Усі загрози можна умовно класифікувати на три основні групи: природні, техногенні та антропогенні.

Природні й техногенні загрози [12, 13], хоча й не пов'язані з навмисною людською діяльністю, можуть завдати значної шкоди об'єктам критичної інфраструктури, спричиняючи масштабні перебої у їх функціонуванні. Антропогенні загрози виникають через свідому або несвідому діяльність людини.

До природних загроз належать явища, що виникають унаслідок природних процесів і не залежать від людської діяльності. Так, землетруси потенційно здатні вивести з ладу стратегічно важливі об'єкти, особливо у сейсмічно активних зонах: уразливі інженерні споруди, трубопроводи, електростанції, мости. Повені загрожують об'єктам, розташованим поблизу річок, водойм або в низинній місцевості. Порушення у роботі систем водопостачання, каналізації, електропостачання можуть спричинити масштабні гуманітарні та екологічні наслідки. Пожежі (особливо лісові) здатні пошкодити енергетичні мережі, телекомунікаційні вежі, логістичні вузли. У контексті змін клімату частота й інтенсивність природних катаклізмів зростає, що вимагає врахування нових факторів ризику в системах моніторингу й реагування.

Техногенні загрози пов'язані з несправностями, збоями чи аваріями через технічний стан об'єктів або людські помилки: аварії на підприємствах (наприклад, хімічних заводах, атомних електростанціях) можуть спричинити каскадні ефекти на суміжні елементи інфраструктури; збої в роботі систем енергопостачання або інформаційних мереж призводять до порушення життєво важливих функцій (зв'язку, охорони здоров'я, безпеки); вибухи, витоки газу, обвали трапляються через зношення обладнання, нехтування технікою безпеки чи виснаження ресурсу матеріалів. Особливість техногенних загроз полягає в тому, що вони можуть мати кумулятивний характер: незначний збій у роботі однієї системи спричиняє масштабні відмови в інших.

До наступної групи загроз, що становлять небезпеку для ОКІ, належать антропогенні загрози. Це найнебезпечніша й динамічна група загроз, пов'язана з навмисною або ненавмисною діяльністю людини. У сучасних умовах воєнного стану саме такі загрози в Україні є найбільш актуальними. До антропогенних загроз відносять: терористичні акти, що вчиняються з метою дестабілізації, спричинення паніки, завдання шкоди життєво важливим об'єктам (водопостачання, зв'язок, електростанції тощо); військові атаки, зокрема ракетні удари, обстріли, захоплення стратегічних вузлів, диверсії (значний ризик становлять системи транспортування енергоносіїв, мости, аеропорти, логістичні центри); кібератаки (злами IT-інфраструктури, атаки на системи управління (SCADA), виведення з ладу баз даних, каналів комунікації). Дедалі серйознішими стають загрози з боку БПЛА, застосовувані ворогом як для розвідки, так і для безпосереднього ураження ОКІ (електропідстанцій, нафтобаз, складів, об'єктів ППО).

Усі антропогенні загрози характеризуються високим ступенем непередбачуваності, швидкістю реалізації та здатністю спричиняти значні соціальні, економічні й безпекові наслідки.

Аналіз загроз дає змогу не лише ідентифікувати потенційно небезпечні впливи на ОКІ, але й формувати відповідні сценарії реагування і захисту. В умовах гібридної війни пріоритетним стає врахування саме антропогенних загроз, зокрема з боку новітніх засобів ураження – кіберзасобів і БПЛА. Водночас не варто ігнорувати природні й техногенні чинники, які часто є тригерами послідовних аварій у комплексних інфраструктурних системах. Основні критерії й показники, які можна використовувати для оцінювання стану захищеності об'єктів критичної інфраструктури, визначено в наказі [2].

Для ефективного планування заходів безпеки й підвищення стійкості ОКІ вирішального значення набуває оцінювання їх вразливості. Воно дає змогу визначити, наскільки об'єкт здатний протистояти

зовнішнім впливам, а також вчасно виявити загрози й мінімізувати наслідки надзвичайних ситуацій. Таке оцінювання має ґрунтуватися на комплексному підході, що враховує технічний, організаційний, кадровий і технологічний аспекти.

Першим важливим чинником є оцінювання вразливості фізичного стану об'єкта і наявність інженерних бар'єрів, здатних запобігати загрозам або зменшувати наслідки їх впливу. Оцінюється ступінь зношення будівель, інженерних мереж, опорних конструкцій, захисних укріплень, наявність протиударних, протипожежних або герметичних елементів. Важливо також брати до уваги адаптованість інфраструктури до можливих змін, зокрема здатність витримувати ударну хвилю чи перебої в енергопостачанні.

Наступний чинник – рівень охорони та фізичної безпеки ОКІ. Він включає в себе організацію фізичної охорони об'єкта, наявність постів спостереження, контрольно-пропускних пунктів, захисту по периметру, систем контролю доступу та сигналізації. Аналізується також взаємодія між службами безпеки об'єкта й Сил безпеки і оборони України [14]. Охорона об'єктів критичної інфраструктури вимагає комплексного підходу та скоординованої взаємодії між усіма складовими сектору безпеки і оборони України. До суб'єктів Національної системи захисту критичної інфраструктури належать:

– Збройні Сили України (ЗСУ);
– Служба безпеки України (СБУ);
– Національна гвардія України (НГУ) [15];
– Національна поліція України (НПУ);
– Державна служба з надзвичайних ситуацій (ДСНС);
– Державна прикордонна служба України (ДПСУ);
– органи місцевого самоврядування;
– приватний сектор та оператори критичної інфраструктури;
– міжнародні партнери, союзники та ін.

Ефективний захист ОКІ залежить від налагодженого механізму комунікації, спільного аналізу загроз, обміну інформацією та узгодженого реагування на загрози. Збройні Сили України є основною силовою структурою, яка здійснює захист стратегічно важливих об'єктів, військових баз та державних установ від повітряних загроз.

Для підвищення якості підготовки здійснюється розвиток стратегій і навчань, а саме:

– проведення спільних навчань із союзниками-країнами НАТО для поліпшення тактики охорони й оборони ОКІ;
– розроблення й упровадження новітніх технологій і тактичних рішень.

Спільна робота СБУ, НГУ, НПУ та ДСНС є ключовим елементом забезпечення безпеки критичної інфраструктури. Ефективна охорона має виконувати не лише пасивну, а й активну функцію – бути здатною оперативно реагувати на порушення чи загрози [16].

Уразливість значною мірою зменшується за наявності такого чинника, як сучасні системи виявлення загроз: і фізичних (відеоспостереження, сенсорні мережі, охоронні датчики), і кіберзагроз (системи мережевого моніторингу, IDS/IPS, аналіз поведінки). Особливу роль відіграють інтегровані системи реагування, здатні автоматично виявляти і класифікувати загрозу, ініціювати процедури безпеки або передавати сигнал тривоги відповідним службам.

Рівень кваліфікації персоналу та його підготовленість до реагування на надзвичайні ситуації в ОКІ – один із ключових чинників оцінювання їх вразливості. Людський фактор критично важливий для забезпечення безпеки ОКІ. Рівень підготовки персоналу, знання алгоритмів дій у кризових ситуаціях, наявність регулярних навчань і тренувань безпосередньо впливають на здатність працівників об'єкта оперативно реагувати на загрози. Оцінюється також наявність планів евакуації, процедур ліквідації наслідків надзвичайних ситуацій, доступність засобів індивідуального захисту та медичної допомоги.

Оцінювання вразливості ОКІ має здійснюватися систематично й багатоаспектно. Недостатній рівень захищеності за хоча б одним із наведених чинників значно підвищує ризики функціонального збою чи руйнування об'єкта. Тому ефективне управління вразливістю потребує не лише технічних рішень, а й організаційної зрілості, міжвідомчої взаємодії та постійного оновлення систем безпеки відповідно до змін середовища загроз [17, 18].

Важливим напрямом дослідження у процесі оцінювання вразливості об'єктів критичної інфраструктури є оцінювання наслідків ураження. Оцінювання потенційних наслідків ураження ОКІ – невід'ємний складник аналізу ризиків і стратегічного планування безпеки. Цей етап передбачає визначення масштабу і глибини впливу інциденту – як безпосереднього, так і опосередкованого – на

життєдіяльність населення, економіку, функціонування суміжних систем, а також на соціально-політичну стабільність регіону й держави загалом.

Ураження об'єктів критичної інфраструктури може спричиняти прямі й опосередковані наслідки для здоров'я, безпеки та умов життя населення. Так, ураження енергетичних об'єктів може призвести до такого: перебої в електропостачанні житлових районів, лікарень, систем опалення у зимовий період; руйнування систем водопостачання або каналізаційних систем, що створює ризики для санітарно-епідеміологічного стану; пошкодження транспортної інфраструктури, що ускладнює евакуацію, постачання гуманітарної допомоги та екстрених служб; стрес і паніка серед населення, які в умовах тривалого дефіциту ресурсів можуть призвести до зростання рівня соціальної напруженості та порушень громадського порядку.

Наслідки ураження інфраструктури в економічному вимірі можуть бути колосальними. Вони охоплюють: прямі втрати – витрати на відновлення зруйнованих об'єктів, відшкодування збитків, тимчасові заходи безпеки; непрямі втрати – зупинення виробництва, зниження обсягів транспортування, втрата робочих місць, падіння податкових надходжень; тривалі економічні ефекти – зниження інвестиційної привабливості регіону, порушення логістичних ланцюгів, девальвація стратегічних активів (наприклад, у сільському господарстві через втрату доступу до зрошення чи енергоживлення). Такі збитки можуть бути як регіонального, так і національного масштабу.

Порушення роботи суміжних об'єктів або систем критично впливає на загальну стійкість і безпеку основного об'єкта. У процесі оцінювання вразливості міжсистемні зв'язки потребують особливої уваги. Критична інфраструктура являє собою складну взаємозалежну систему, де вихід із ладу одного елемента здатен спричинити каскадні відмови в інших. Так, ураження підстанції електропередачі може зупинити роботу водоканалів, лікарень і транспорту; атака на вузол зв'язку – паралізувати системи оповіщення та координації дій у надзвичайних ситуаціях; виведення з ладу залізничного вузла – зірвати постачання паливно-енергетичних ресурсів до інших областей.

Соціальна й політична дестабілізація суттєво впливає на рівень безпеки об'єкта, тому її потенційні наслідки слід обов'язково брати до уваги під час оцінювання вразливості. Наслідки ураження можуть вийти далеко за межі матеріальних втрат і перейти у сферу соціальної й політичної безпеки. Можливі такі прояви: зниження довіри громадян до державних інституцій у разі нездатності запобігти кризі або швидко на неї відреагувати; посилення панічних настроїв, протестна активність, зростання впливу деструктивних інформаційних кампаній; використання інцидентів зовнішніми або внутрішніми силами для політичної маніпуляції чи ескалації конфліктів; порушення міжнародних зобов'язань України тощо. Особливо це стосується стратегічних об'єктів, ураження яких викликає широкий суспільний резонанс: медичних установ, урядових будівель або енергетичних об'єктів тощо.

Оцінювання наслідків ураження дає змогу не лише виміряти рівень потенційних збитків, а й установити пріоритети захисту ОКІ. У планах безпеки та стратегіях реагування до об'єктів, ураження яких спричиняє одночасний вплив на кілька сфер (гуманітарну, економічну, соціальну), має бути підвищена увага. Такий аналіз формує й підґрунтя для розроблення сценаріїв кризового управління та ефективного розподілу ресурсів у разі надзвичайної ситуації.

Отже, оцінювання вразливості об'єктів критичної інфраструктури є фундаментальним інструментом для забезпечення їхньої стійкості, своєчасного реагування на загрози і мінімізації наслідків надзвичайних ситуацій.

Оцінювання вразливості ОКІ передбачає застосування різних методик [19, 20], які дають змогу комплексно аналізувати ризики та їх потенційний вплив на безпеку. Існують декілька підходів до такого оцінювання. Умовно можна виділити кількісні, якісні та інтегровані методи.

Кількісні методи дають змогу отримати об'єктивні числові показники ризиків і ймовірностей ураження, що важливо для прийняття обґрунтованих рішень щодо захисту ОКІ. Цей підхід базується на використанні математичних моделей, імовірнісного аналізу та сценарного моделювання. Можливо чисельно визначити рівень ризику або вразливості об'єкта, а також оцінити ефективність заходів щодо його захисту. Найпоширеніші такі кількісні методи.

1. Метод імовірнісного оцінювання ризиків (Probabilistic Risk Assessment, PRA) дає змогу врахувати всі можливі сценарії розвитку подій і визначити ймовірність кожного з них.

2. Аналіз дерев відмов (Fault Tree Analysis, FTA) та аналіз потоків подій (Event Tree Analysis, ETA) використовується для ідентифікації критичних точок і ланцюгів відмов.

3. Методи багатокритеріальної оптимізації дають змогу одночасно оцінювати декілька факторів впливу (наприклад, стан захисту, надійність систем, логістичні зв'язки тощо).

4. Моделювання сценаріїв впливу використовується для прогнозування наслідків різних загроз.

Якісні методи ґрунтуються на експертному оцінюванні, аналітичних спостереженнях та описовому аналізі, що дає змогу враховувати складні, недостатньо формалізовані фактори впливу на вразливість ОКІ. Якісне оцінювання вразливості ґрунтується на експертних судженнях, контекстному аналізі та використанні структурованих методик збирання інформації. Цей підхід особливо корисний у випадках, коли бракує даних для математичного аналізу. До основних якісних методів належать такі.

1. SWOT-аналіз (Strengths, Weaknesses, Opportunities, Threats) дає змогу виявити сильні і слабкі сторони об'єкта, зовнішні загрози й можливості для захисту.

2. Метод DELPHI полягає у багатоетапному опитуванні експертів для досягнення консенсусу в оцінках.

3. Структуровані інтерв'ю та опитування використовуються для збирання думок фахівців з експлуатації, безпеки та управління ОКІ.

4. Метод аналітичних ієрархій (AHP) дає змогу структурувати складні рішення та оцінювати вразливість за кількома параметрами.

Інтегровані методи поєднують елементи кількісного і якісного аналізу, забезпечуючи більш повну та збалансоване оцінювання вразливості поєднанням точних даних і експертних суджень. У сучасній практиці найефективнішими вважаються інтегровані методи оцінювання вразливості, що поєднують кількісні та якісні підходи. Такий підхід забезпечує:

– більш повну картину вразливості об'єкта завдяки включенню як об'єктивних, так і суб'єктивних даних;

– підвищену достовірність результатів, оскільки уможливлює зменшення похибки, властивої кожному з методів окремо;

– можливість адаптації до різних типів інфраструктури і загроз.

Інтегровані методи часто реалізуються у формі моделей, які поєднують різні джерела даних і підходи до аналізу. Зокрема такі моделі можуть бути втілені у вигляді GIS-систем, інформаційно-аналітичних платформ або цифрових двійників об'єктів, що дає змогу постійно оновлювати дані і здійснювати моніторинг уразливості в реальному часі.

Аналіз методів оцінювання вразливості є визначальним елементом у формуванні цілісного підходу до безпеки, оскільки дає можливість не лише визначати рівень небезпеки для об'єктів, а й планувати ефективні заходи протидії.

Приклади вразливості в умовах воєнного стану показують, як зовнішні загрози здатні критично впливати на функціонування об'єктів критичної інфраструктури, акцентуючи на необхідності системного підходу до їх оцінювання і захисту. Повномасштабне військове вторгнення в Україну, що розпочалося у 2022 р., кардинально змінило підходи до забезпечення безпеки ОКІ. Військові дії, які супроводжуються системними атаками на ОКІ, продемонстрували їх підвищену вразливість до широкого спектру загроз (від фізичного знищення до інформаційного впливу).

У період з 2022 р. і дотепер російська федерація здійснила велику кількість масованих ракетних і дронових атак по об'єктах енергетики. Метою цих ударів було виведення з ладу таких ключових елементів енергосистеми країни, як теплові електростанції (ТЕС), підстанції магістрального рівня, трансформаторні станції, об'єкти генерації та диспетчерського управління. Унаслідок атак мільйони українців зазнали тривалих відключень електроенергії, теплопостачання і водопостачання. Це продемонструвало високу вразливість енергетичної інфраструктури до точкових ракетних ударів і ударів дронів-камікадзе, а також обмеженість резервних потужностей у системі.

Ураження транспортної інфраструктури в умовах військового конфлікту призводить до порушення логістичних ланцюгів, обмеження мобільності сил оборони й ускладнення евакуаційних і гуманітарних операцій, що робить її однією з найуразливіших ланок критичної інфраструктури. Неодноразово цілями ракетних атак ставали залізничні вузли, мости, а також логістичні хаби. Так, пошкодження залізничного полотна у Дніпропетровській, Київській та Львівській областях затримувало транспортування вантажів. Руйнування мостів і залізничних переїздів у прифронтових регіонах ускладнило евакуацію мирного населення й постачання боєприпасів. Удар по вокзалу у Краматорську у квітні 2022 р. призвів до численних жертв серед цивільного населення. Наведені приклади демонструють, наскільки вразливою є транспортна інфраструктура до високоточної зброї та якими можуть бути гуманітарні й військові наслідки її ураження.

Кібератаки на цифрову інфраструктуру в умовах воєнного стану [21] можуть спричинити порушення зв'язку, втрату доступу до критичних даних, збої в роботі енергетичних, фінансових та

управлінських систем, що робить її однією з ключових зон уразливості сучасної критичної інфраструктури.

Окрім фізичних атак у 2022–2025 рр. значно активізувалися кібератаки на державні і приватні інформаційні системи. Найрезонансніші приклади: атаки на урядові портали та бази даних (зокрема, портали «Дія», державні реєстри); злами банківських систем і порушення роботи платіжної інфраструктури; DDoS-атаки на телекомунікаційні компанії, що ускладнювало зв'язок і координацію в умовах надзвичайних ситуацій. Такі атаки демонструють критичну залежність управлінських і фінансових структур від цифрових сервісів, а також брак повноцінної цифрової кіберрезервної інфраструктури.

Наведені вище приклади свідчать про те, що в умовах війни об'єкти критичної інфраструктури стають системними цілями противника, а їх знищення або виведення з ладу спричиняє широкі соціальні, економічні та гуманітарні наслідки. Перегляду потребують традиційні підходи до захисту ОКІ, необхідні впровадження нових технологій моніторингу, протидії та відновлення, а також інтеграція компоненти безпеки у стратегічне планування держави.

Висновки

Отже, оцінювання вразливості становить критично важливий складник забезпечення безпеки об'єктів критичної інфраструктури, особливо в умовах воєнного стану. Проведення її оцінювання дає змогу: виявити найбільш уразливі компоненти інфраструктури; формувати обґрунтовані плани модернізації і зміцнення об'єктів; визначати пріоритетні напрями для інвестування у захисні технології; розробляти ефективні сценарії реагування та ліквідації наслідків надзвичайного стану.

В умовах постійної загрози з боку сучасних технологій війни Україні необхідно посилювати власну систему оцінювання й моніторингу вразливості. Доцільно впроваджувати: інтегровані моделі оцінювання, що поєднують кількісні та якісні підходи; системи раннього попередження та автоматизованого аналізу ризиків; міжвідомчу координацію у сфері захисту критичної інфраструктури; міжнародний досвід і стандарти.

Комплексне й систематичне оцінювання вразливості має стати підґрунтям для формування національної стратегії безпеки критичної інфраструктури в контексті забезпечення державної безпеки, здатної протистояти загрозам сучасної гібридної війни.

Напрямом подальших досліджень є огляд світових практик протидії загрозам об'єктам критичної інфраструктури, урахування міжнародного досвіду та можливість адаптації світових стандартів до українського контексту.

Перелік джерел посилання

1. Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів : наказ Державного комітету ядерного регулювання України № 169 від 30.11.2010 р. URL: https://surl.li/ulwcqv (дата звернення: 07.04.2025).
2. Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.01.2025 р. № 17. URL: https://surl.lu/vyxbiv (дата звернення: 07.04.2025).
3. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Економіка.* 2015. № 4 (37). С. 83–93. URL: https://surl.li/prjzyq (дата звернення: 07.04.2025).
4. Капля І. В., Тертишний Б. В. Методика оцінювання загроз об'єктам критичної інфраструктури під час вогневого впливу противника. *Social Development and Security.* 2024. № 5 (14). С. 215–221. DOI: https://doi.org/10.33445/sds.2024.14.5.21.
5. Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій / Р. К. Мурасов та ін. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 3 (48). С. 35–43. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-35-43.
6. Мурасов Р. К., Мельник Я. В. Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 1 (46). С. 41–44. DOI: https://doi.org/ 10.33099/2311-7249/2023-46-1-41-44.

7. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. *Відомості Верховної Ради України*. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 07.04.2025).

8. Toliupa S., Parkhomenko I., Antoniuk V. (2021). Method for Identification of Critical Information Infrastructure Objects of the State. In: Proceedings of the 1st International Workshop on Cyber Hygiene – CyberHygiene 2021. *CEUR Workshop Proceedings*, vol. 3179, pp. 262–271.

9. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23. URL: https://surli.cc/kznhgg (дата звернення: 07.04.2025).

10. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього : Постанова Кабінету Міністрів України від 28.04.2023 р. № 415. URL: https://surl.li/lmhjfw (дата звернення: 07.04.2025).

11. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 22.07.2022 р. № 821. URL: https://surl.li/qgwnjm (дата звернення: 07.04.2025).

12. Онопрієнко О. С., Споришев К. О. Зміст завдань сил Національної гвардії України при виникненні надзвичайної ситуації внаслідок аварій на гідротехнічних спорудах. *Державне управління: удосконалення та розвиток*. 2018. № 5. С. 243 – 247.

13. Герасименко О. М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Право*. 2024. Вип. 3 (84). С. 257–263.

14. Protecting Ukraine′s critical infrastructure from drone threats: the role of security and defence forces / Nazarenko O. L. et al. *Actual Issues of Modern Science. European Scientific e-Journal*. Ostrava. 2025. No. 37. URL: https://eiid.eu/ftpgetfile.php?id=248 (дата звернення: 01.06.2025).

15. Назаренко О. Л. Особливості охорони об'єктів критичної інфраструктури підрозділами Національної гвардії України. *Актуальні проблеми діяльності складових сектору безпеки і оборони України в умовах особливих правових режимів: поточний стан та шляхи вирішення* : матеріали II Міжнар. наук.-практ. конференція (м. Харків, 20 берез. 2025 р.). Харків, 2025. С. 370 – 371.

16. Яременко О. І., Страхніцький Я. О. Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. *Університетські наукові записки*. 2022. № 3 (87). С. 73–82. DOI: https://doi.org/10.37491/UNZ.87.6.

17. Шаптала С. О., Романенко Є. О., Хращевський Р. В. Використання лазерів для протидії безпілотним літальним апаратам. *Наука і техніка сьогодні. Техніка.* 2023. № 11 (25). С. 617–629. URL: https://surl.li/ejtqpz (дата звернення: 17.04.2025).

18. Шумигай О. В., Єрмоленко О. В. Сучасний стан багатофункціональних засобів та комплексів радіоелектронної боротьби. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2020. № 3 (5). С. 119–125. DOI: https://doi.org/10.37701/dndivsovt.5.2020.14.

19. Мурасов Р., Мельник Я., Марко В. Порівняння існуючих методик оцінювання загроз і ризиків для потенційно-небезпечних об'єктів критичної інфраструктури в зоні ведення бойових дій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 3 (45). С. 32–36. DOI: https://doi.org/10.33099/2311-7249/2022-45-3-32-36.

20. Ozkan C., Singelee D. Evidence-Based Threat Modeling for ICS. *arXiv preprint arXiv:2411.19759*. 2024. URL: https://arxiv.org/abs/2411.19759 (дата звернення: 17.04.2025).

21. Ковальчук В. В., Сидоренко І. М. Система кіберзахисту об'єктів критичної інфраструктури в умовах війни. *Науковий вісник КІНГУ*. 2024. № 2. С. 43–48. DOI: https://doi.org/10.59226/2786-6920.2.2024.43-48.

Стаття надійшла до редакції 05.06.2025 р.

UDC 351.865

O. Nazarenko, O. Holovan, V. Rudynskyi

ON THE ISSUE OF ASSESSING THE VULNERABILITY OF CRITICAL INFRASTRUCTURE OBJECTS IN WARTIME CONDITIONS

In modern conditions, especially during wartime, the issue of protecting critical infrastructure is of paramount importance. Assessing the vulnerability of such facilities allows identifying weaknesses in the security system, preventing potential attacks and ensuring effective planning of response measures within the framework of ensuring state security.

Despite the relevance of this issue, Ukraine currently needs to improve a comprehensive methodology for assessing the vulnerability of critical infrastructure facilities adapted to martial law conditions. Existing approaches are fragmented and, in some cases, outdated, having been developed in the context of peacetime. In addition, the practical implementation of infrastructure protection measures is often not systematic, which can affect the overall level of national security.

Thus, there is an urgent need for a scientifically based approach to assessing the vulnerability of CI that would take into account the specifics of modern military threats, include interdisciplinary methods of analysis and provide a basis for decision-making in the field of state security. Thus, the assessment of the vulnerability of critical infrastructure is of particular relevance in the current context.

The assessment of the vulnerability of critical infrastructure facilities involves an analysis of their security and physical safety, which includes physical protection measures, access control, surveillance and alarm systems, as well as effective interaction between the facility's security forces and the entities of the National System of Critical Infrastructure Protection of Ukraine, including the Armed Forces of Ukraine, the Security Service of Ukraine, the National Guard of Ukraine, the National Police of Ukraine, the State Emergency Service, the State Border Guard Service of Ukraine, local authorities, and other relevant entities.

The article discusses the issue of assessing the level of vulnerability of critical infrastructure facilities and proposes a systematic and multidimensional approach to threat analysis. The possible consequences of damage to critical infrastructure for the population, including the risks of social and political destabilization, are proved. Methods for assessing the vulnerability of critical infrastructure facilities and examples of their vulnerability in wartime are presented. The results of international practice are presented and an analysis of potential threats to critical infrastructure is conducted.

Keywords: *critical infrastructure facilities, vulnerabilities, risks, threats, cybersecurity.*

НАЗАРЕНКО Олег Леонідович – кандидат військових наук, доцент кафедри забезпечення державної безпеки, Національна академія Національної гвардії України
https://orcid.org/0000-0001-7579-0658

ГОЛОВАНЬ Олег Михайлович – кандидат військових наук, доцент начальник кафедри забезпечення державної безпеки, Національна академія Національної гвардії України
https://orcid.org/0000-0002-7290-8021

РУДИНСЬКИЙ Віталій Вікторович – доктор філософії, начальник кафедри управління діями підрозділів військової розвідки та Сил спеціальних операцій, Військова академія (м. Одеса)
https://orcid.org/0000-0003-2066-865X