Підготовка об’єктів критичної інфраструктури до захисту від збройних сил країни агресора

Preparation of Critical Infrastructure Facilities for Protection Against the Armed Forces of the Aggressor State

Олег Соколовський
старший науковий співробітник науково-дослідного відділу проблем розвитку та застосування частин і підрозділів військової розвідки та Сил спеціальних операцій, e-mail: bizoklop@ukr.net, ORCID ID: 0009-0002-5234-2590

Військова академія, м. Одеса, Україна

Oleg Sokolovsky
Senior Research Fellow of the Research Department on the Development and Employment of Military Intelligence Units and Special Operations Forces, e-mail: bizoklop@ukr.net, ORCID ID: 0009-0002-5234-2590

Military Academy, Odessa, Ukraine

Received: December 06, 2025 | Revised: December 20, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/sds.2025.15.6.12

Мета роботи. Аналіз чинників, що впливають на підготовку об’єктів критичної інфраструктури до оборони та їх захист під час ведення наступальних дій противником, вироблення пропозицій щодо удосконалення захисту об’єктів критичної інфраструктури та участь в ньому центральних та місцевих державних органів влади.

Метод дослідження. У процесі дослідження використано комплекс загальнонаукових і спеціальних методів, зокрема аналіз і синтез нормативно-правових актів у сфері національної безпеки та захисту критичної інфраструктури, логіко-структурний і порівняльний аналіз для побудови та зіставлення моделей захисту, системний підхід для оцінювання ролі критичної інфраструктури у забезпеченні стійкості держави, а також узагальнення практичного досвіду з метою розроблення прикладних рекомендацій щодо підготовки об’єктів і територій до оборони в умовах воєнного стану.

Результати дослідження. За результатами дослідження визначено основні загрози об’єктам критичної інфраструктури в умовах збройної агресії, виявлено недоліки чинної системи їх захисту в мирний і воєнний час та обґрунтовано необхідність створення ефективної координаційної вертикалі. Визначено роль ГШ Збройних Сил України, Міністерства внутрішніх справ, Національної гвардії України й органів державної влади у забезпеченні захисту об’єктів критичної інфраструктури та запропоновано практичні заходи з підготовки об’єктів і територій до оборони, у тому числі із залученням сил руху опору.

Теоретична цінність дослідження. Теоретична цінність дослідження полягає в поглибленні наукових уявлень про захист критичної інфраструктури як складову національної безпеки й оборонного планування в умовах збройного конфлікту, а також у розвитку положень військової науки щодо асиметричних форм боротьби та забезпечення стійкості держави під час воєнного стану.

Практична цінність дослідження. Практична цінність дослідження визначається можливістю використання його результатів у діяльності органів державної влади та військового управління при вдосконаленні нормативно-правового забезпечення захисту критичної інфраструктури, у процесі оборонного і мобілізаційного планування, організації оборони об’єктів і територій, а також у підготовці офіцерських кадрів та фахівців сектору безпеки і оборони України.

Тип статті. теоретичний.

Purpose. The purpose of the study is to analyze the factors influencing the preparation of critical infrastructure facilities for defense and their protection during the adversary’s offensive operations, to develop proposals for improving the protection of critical infrastructure facilities, and to determine the role of central and local public authorities in this process.

Method. The study employs a set of general scientific and specialized methods, including analysis and synthesis of regulatory and legal acts in the field of national security and critical infrastructure protection; logical-structural and comparative analysis to develop and compare protection models; a systems approach to assess the role of critical infrastructure in ensuring state resilience; and the generalization of practical experience to formulate applied recommendations for preparing facilities and territories for defense under martial law.

Findings. The study identifies the main threats to critical infrastructure facilities under conditions of armed aggression, reveals shortcomings in the existing protection system in both peacetime and wartime, and substantiates the need to establish an effective coordination hierarchy. The roles of the General Staff of the Armed Forces of Ukraine, the Ministry of Internal Affairs, the National Guard of Ukraine, and public authorities in ensuring the protection of critical infrastructure facilities are defined, and practical measures for preparing facilities and territories for defense, including the involvement of resistance movement forces, are proposed.

Theoretical implications. The theoretical contribution of the study lies in deepening scholarly understanding of critical infrastructure protection as a component of national security and defense planning in conditions of armed conflict, as well as in advancing military science perspectives on asymmetric forms of warfare and state resilience during martial law.

Practical implications. The practical implications of the study consist in the applicability of its findings for public authorities and military command bodies in improving the regulatory framework for critical infrastructure protection, in defense and mobilization planning, in organizing the defense of facilities and territories, and in the training of officers and specialists of Ukraine’s security and defense sector.

Type of article: theoretical.

Ключові слова: оборонна сфера, рух опору, планування, оперативне середовище, об’єкти критичної інфраструктури, мирний та воєнний час.

Key words: Defense Sector, Resistance Movement, Planning, Operational Environment, Critical Infrastructure Facilities, Peacetime and Wartime.

Вступ

Захист і підготовка до оборони об'єктів критичної інфраструктури від дій окупаційних військ держави-агресора на території України є важливим елементом боротьби за суверенітет і територіальну цілісність держави. Актуальність зазначеної проблематики зумовлена тим, що на сучасному етапі противник систематично здійснює вогневий вплив на об'єкти критичної інфраструктури та намагається захопити їх у разі проведення наземних наступальних операцій. Водночас, як засвідчив досвід останніх років, національна система захисту об'єктів критичної інфраструктури (далі — ОКІ) була орієнтована переважно на виклики мирного часу та не забезпечувала наявності чіткого алгоритму їх захисту в умовах надзвичайного і воєнного стану [1].

Захист ОКІ становить собою комплексну систему заходів, спрямованих на забезпечення їх безпеки, стійкості та безперебійного функціонування, що є складовою національної безпеки України. Така система передбачає ідентифікацію та категоризацію об'єктів критичної інфраструктури, визначення актуальних загроз їх функціонуванню, упровадження інженерно-технічних, організаційних і кіберзахисних заходів, а також координацію дій між органами державної влади, органами місцевого самоврядування, суб'єктами господарювання незалежно від форми власності та інститутами громадянського суспільства [1; 5].

Теоретичні основи дослідження

Підготовка об'єктів критичної інфраструктури до захисту під час організації оборони як ключового елементу асиметричної боротьби в умовах війни є важливою складовою стратегічного планування оборонних операцій. Зазначена проблематика перебуває в полі досліджень військової науки та охоплює питання тактики, оперативного мистецтва і стратегії ведення бойових дій.

Відповідно до Закону України «Про критичну інфраструктуру» (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України. Віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну та екологічну значущість для забезпечення оборони держави, безпеки громадян, суспільства і правопорядку. До таких критеріїв, зокрема, належать: забезпечення реалізації життєво важливих функцій і надання життєво важливих послуг; наявність загроз функціонуванню об'єктів; імовірність виникнення кризових ситуацій унаслідок несанкціонованого втручання, дії людського чинника або природних лих; тривалість робіт, необхідних для ліквідації наслідків і повного відновлення штатного режиму функціонування [1].

Досвід інших держав у розвитку систем захисту об'єктів критичної інфраструктури свідчить, що ключовими елементами таких систем є чітке визначення переліку критичних об'єктів, а також закріплення відповідальності за їх захист за конкретними органами державної влади та посадовими особами. Водночас у більшості країн основними джерелами ризиків тривалий час розглядалися передусім терористичні загрози та загрози у сфері кібербезпеки.

У Сполучених Штатах Америки об'єкти критичної інфраструктури законодавчо визначаються як сукупність фізичних або віртуальних систем і засобів, настільки важливих для держави, що їх виведення з ладу або знищення може призвести до катастрофічних наслідків у сферах оборони, економіки, охорони здоров'я та національної безпеки. Центральним органом, відповідальним за захист критичної інфраструктури, є Міністерство внутрішньої безпеки США. У 2018 році в його структурі було створено Агентство з кібербезпеки та безпеки інфраструктури як виконавчий орган оперативного рівня, уповноважений на протидію загрозам критичній інфраструктурі.

У Великій Британії законодавство у сфері захисту критичної інфраструктури також орієнтоване на пріоритетність протидії терористичним і кіберзагрозам. До об'єктів критичної інфраструктури віднесено системи телекомунікацій, банківського і фінансового секторів, водопостачання, енергозабезпечення та інші об'єкти, що мають ключове значення для економіки країни. У 1999 році було створено спеціалізований координаційний центр із безпеки національної інфраструктури як складову системи Міністерства внутрішніх справ, який у 2007 році було реорганізовано в окремий урядовий центр із захисту національної критичної інфраструктури.

У Франції координація діяльності у сфері захисту критичної інфраструктури покладена на прем'єр-міністра, а на організаційному рівні відповідні функції здійснює Генеральний секретаріат з оборони і національної безпеки. Згідно із Законом про захист основних економічних секторів від 2014 року № 6600/SGDSN/PSE/HSN до критичних і таких, що потребують захисту, віднесено всі сектори, які забезпечують базові соціальні та економічні процеси держави, зокрема державне управління, судочинство, збройні сили, сільське господарство, електронні комунікаційні системи, енергетику, космічну діяльність, водні ресурси, промисловість, охорону здоров'я та транспорт.

У Німеччині поняття об'єктів критичної інфраструктури визначено в Національній стратегії захисту критичної інфраструктури, де до них віднесено організаційні та фізичні структури і об'єкти, що є настільки життєво важливими для суспільного й економічного існування нації, що порушення їх функціонування може призвести до суттєвих прогалин у системі державної безпеки або інших тяжких наслідків. Ключовими критеріями віднесення об'єктів до критичної інфраструктури визначено інтереси нації та безпеку держави. Координаційні функції у цій сфері покладено на Федеральне міністерство внутрішніх справ, а також на спеціалізований орган виконавчої влади, завданням якого є моніторинг вразливостей інфраструктури та розроблення рекомендацій щодо її захисту.

У 2025 році уряд Республіки Польща ухвалив постанову, якою заборонено передавати в оренду об'єкти критичної інфраструктури для здійснення на них господарської діяльності суб'єктам недержавної форми власності [2].

Водночас покладання функцій захисту об'єктів критичної інфраструктури в Україні на Державну службу спеціального зв'язку та захисту інформації України не вирішує, а ускладнює наявні проблеми, оскільки зазначений орган не наділений достатніми інструментами впливу та не має реальних важелів взаємодії з Силами оборони України, зокрема Збройними Силами України та Національною гвардією України. Рада національної безпеки і оборони України, яка відповідно до Конституції України здійснює координацію і контроль у сфері національної безпеки, також не спроможна самостійно повноцінно виконувати ці функції через відсутність належних законодавчих і управлінських механізмів впливу на органи державної влади.

Ефективне здійснення зазначених функцій Кабінетом Міністрів України ускладнюється відсутністю в системі органів виконавчої влади чітко вибудуваної інституційної вертикалі, а також невирішеністю питань залучення до захисту об'єктів критичної інфраструктури збройних формувань, які мають необхідну номенклатуру озброєння та військової техніки. У цьому контексті ключовою проблемою залишається відсутність чіткого законодавчого визначення ролі, місця та завдань Генерального штабу Збройних Сил України у сфері захисту об'єктів критичної інфраструктури в мирний і воєнний час.

Постановка проблеми

Досвід засвідчує, що зверхнє ставлення до підготовки населення, територій та об'єктів критичної інфраструктури до дій груп руху опору не дало змоги в перші дні широкомасштабної збройної агресії завдати противнику таких втрат, які могли б змусити його відмовитися від реалізації поставлених цілей принаймні на окремих оперативних напрямках. Станом на

сьогодні противник не відмовився від зазіхань на нові території України, що зумовлює об'єктивну необхідність ретельної підготовки населення та оперативного середовища для ефективних дій груп руху опору із захисту об'єктів критичної інфраструктури [5].

Дослідження зазначеної проблематики та вироблення дієвих пропозицій щодо організації системи захисту об'єктів критичної інфраструктури є основним завданням, яке ставить перед собою автор у цій публікації. Чинна система захисту виявилася неготовою до функціонування в умовах воєнного часу та до ефективного реагування на притаманні йому загрози, насамперед щодо збройного ураження об'єктів критичної інфраструктури в ході бойових дій [1].

Подальші спроби Російської Федерації знищити українські енергетичні та інші критично важливі об'єкти зумовлюють необхідність ухвалення органами державної влади України невідкладних управлінських рішень та вжиття термінових практичних заходів, спрямованих на їх збереження, захист і оперативне відновлення.

У зв'язку з цим виникає потреба у проведенні ґрунтовного наукового аналізу окреслених питань з метою формування обґрунтованих висновків і внесення відповідних змін до нормативно-правових та керівних документів. Окремим завданням дослідження є впровадження отриманих результатів у навчальні плани та програми підготовки офіцерських кадрів для забезпечення належного рівня готовності до виконання бойових завдань у визначених районах і на об'єктах критичної інфраструктури.

Результати

Основними аспектами захисту критичної інфраструктури є: визначення та категоризація об'єктів; оцінювання ризиків; системні заходи безпеки; кіберзахист; координація та взаємодія; система раннього виявлення загроз; ведення єдиного реєстру; міжнародне співробітництво [1].

Станом на сьогодні чинна система координації та контролю у сфері захисту об'єктів критичної інфраструктури потребує вдосконалення як для воєнного, так і для мирного часу. Як і на початку повномасштабної війни, покладання зазначених функцій на Державну службу спеціального зв'язку та захисту інформації України, яка не наділена достатніми інструментами впливу та не має дієвих механізмів взаємодії із Силами оборони України (Збройними Силами України, Національною гвардією України), не розв'язує проблеми, а лише ускладнює її. Рада національної безпеки і оборони України, що відповідно до Конституції України здійснює координацію і контроль у сфері національної безпеки, також не може повноцінно виконувати зазначене завдання за відсутності належних законодавчих та управлінських механізмів впливу на органи державної влади [1].

Організація руху опору проти окупаційних сил охоплює комплекс заходів, спрямованих на забезпечення ефективного спротиву окупаційній владі, збереження національної ідентичності та підтримання стійкості держави, і безпосередньо залежить від наявності в потенційних районах окупації об'єктів критичної інфраструктури, які противник намагатиметься знищити або захопити [5].

Роботу з організації оборони та розгортання мережі опору необхідно здійснювати з урахуванням напрямків і конкретних об'єктів критичної інфраструктури, на ураженні чи захопленні яких противник зосереджуватиме основні зусилля. Таку діяльність доцільно розпочинати в мирний час і активізувати в загрозливий період, виходячи з оцінювання ймовірного характеру дій власних Сил оборони та сил противника. Це дає змогу діяти превентивно, випереджаючи противника та ускладнюючи досягнення ним поставлених цілей. Зазначена робота має проводитися на всіх рівнях — як Силами оборони, так і органами державної влади та місцевого самоврядування, із залученням керівництва підприємств різних форм власності та з дотриманням режиму обмеження інформації: коло осіб, обізнаних із завданнями, має бути чітко визначеним і функціонально необхідним [5].

Перелік секторів критичної інфраструктури та суб'єктів, відповідальних за формування і реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, визначається Кабінетом Міністрів України. У разі потреби внесення змін Кабінет Міністрів України переглядає та коригує зазначений перелік відповідно до критеріїв критичності, установлених законом [1].

До життєво важливих функцій та/або послуг, порушення яких може спричинити негативні наслідки для національної безпеки України, належать, зокрема: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (у тому числі постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин і забезпечення сталого функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспорт; оборона і державна безпека; правопорядок і правосуддя (включно з триманням під вартою); цивільний захист і служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність [1] (див. табл. 1; також узагальнення заходів — [2]).

Одним із напрямів організації руху опору є підготовка територій та об'єктів інфраструктури для сприяння діям сил руху опору. Особливу увагу слід приділяти створенню й підготовці формувань, які діятимуть на шляхах висування противника до важливих економічних та потенційно небезпечних об'єктів критичної інфраструктури у взаємодії з підрозділами протиповітряного прикриття [5].

Підготовка територій для сприяння діям сил руху опору має здійснюватися в мирний час, у загрозливий період, а також у ході ведення противником бойових дій. До підготовки територій та об'єктів критичної інфраструктури доцільно залучати органи державної влади, органи місцевого самоврядування та підприємства всіх форм власності. На законодавчому рівні доцільно визначити вимоги до оснащення будівель, об'єктів і комунікацій з метою можливості їх використання підрозділами Сил оборони в оборонному бою. Передбачаються, зокрема: підготовка місць укриття для особового складу та майна груп опору; створення (або інженерне пристосування) елементів економічної інфраструктури, які в умовах бойових дій можуть виконувати функцію штучних фортифікаційних перешкод і знижувати темпи просування колон техніки противника (водні перешкоди, насадження, інженерні бар'єри тощо); спорудження (за встановленими вимогами) об'єктів, що можуть бути використані як довготривалі вогневі споруди для унеможливлення просування противника до критично важливих об'єктів [5].

В умовах бойових дій уразливість об'єктів критичної інфраструктури негативно впливає на стійкість держави та її здатність до опору [1].

В Україні модель захисту критичної інфраструктури розвивається з 2014 року — від початку збройної агресії Російської Федерації. У 2021 році було ухвалено Закон України «Про критичну інфраструктуру», яким врегульовано низку питань, зокрема: створення реєстру об'єктів, що потребують захисту; покладання координації та контролю в цій сфері на Кабінет Міністрів України; визначення органів виконавчої влади, відповідальних за захист у мирний час (Державна служба спеціального зв'язку та захисту інформації України) та у воєнний час (Генеральний штаб Збройних Сил України), тощо [1]. Водночас, як засвідчує практичний досвід, домінування підходів «мирного часу» не забезпечувало наявності чіткого алгоритму захисту критичної інфраструктури в умовах воєнного стану, що призводило до втрат окремих об'єктів та підприємств, зокрема на територіях Луганської й Донецької областей, а також до несвоєчасної евакуації частини промислових потужностей [1].

Подальші спроби російської федерації знищити українські енергетичні та інші критично важливі об'єкти вимагають від органів державної влади ухвалення рішень і вжиття термінових практичних заходів щодо їх збереження та оперативного відновлення. Водночас ключовими

завданнями залишаються: ухвалення й імплементація нормативно-правових рішень у сфері захисту критичної інфраструктури; удосконалення процедур категоризації; розроблення критеріїв безпеки та стійкості; підготовка планів захисту [1; 2].

Закон України "Про Збройні Сили України" (ст. 1, розд. I) визначає, що Збройні Сили України виконують завдання з протиповітряного прикриття важливих об'єктів, перелік яких визначається Кабінетом Міністрів України. Закон України "Про правовий режим воєнного стану" (ст. 4, п. 7) передбачає спрямування, координацію та контроль за діяльністю обласних військових адміністрацій з питань захисту критичної інфраструктури та здійснення заходів правового режиму воєнного стану Генеральним штабом Збройних Сил України. Закон України "Про оборону України" (ст. 13, розд. II) визначає, що органи державної влади, органи військового управління, місцеві державні адміністрації, органи місцевого самоврядування, підприємства, установи й організації узгоджують дії з Генеральним штабом ЗСУ та забезпечують проведення заходів щодо розвитку системи зв'язку, шляхів, транспорту, інших об'єктів інфраструктури і територій [1]. Водночас деталізація зазначених законодавчих норм у Положенні про Генеральний штаб ЗСУ відсутня; окремий координаційний орган у його складі не створено, що негативно впливає на реалізацію функцій захисту та розподіл відповідальності [1].

Для належного унормування функцій і завдань державних органів та суб'єктів господарювання у сфері захисту критичної інфраструктури доцільним є внесення змін до Закону України "Про правовий режим воєнного стану", з огляду на те, що в період воєнного стану відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування надаються додаткові повноваження [1]. Військове командування видає обов'язкові до виконання накази і директиви з питань забезпечення оборони, громадської безпеки й порядку, здійснення заходів правового режиму воєнного стану та визначає сили і засоби, на які покладаються відповідні завдання. Військові адміністрації на територіях, де введено воєнний стан, разом із військовим командуванням запроваджують і здійснюють заходи оборони, цивільного захисту, громадської безпеки і порядку, захисту критичної інфраструктури, а також охорони прав і законних інтересів громадян. При цьому спрямування, координацію та контроль за діяльністю обласних військових адміністрацій щодо забезпечення оборони, громадської безпеки й порядку, захисту критичної інфраструктури та дотримання правового режиму воєнного стану здійснює Генеральний штаб ЗСУ, а з інших питань — Кабінет Міністрів України в межах повноважень [1]. Серед заходів правового режиму воєнного стану (ст. 8 Закону) передбачено завдання "встановлювати (посилювати) охорону об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення, і вводити особливий режим їх роботи" [1].

Крім того, у Законі України "Про національну безпеку України" доцільно чіткіше визначити повноваження Міністерства оборони України щодо захисту об'єктів критичної інфраструктури в умовах ведення бойових дій (зокрема шляхом уточнення Плану оборони України та його складових), що дасть змогу оперативніше реагувати на зміни в оперативному середовищі [1]. До ймовірних сценаріїв залучення Сил безпеки і Сил оборони до виконання завдань з оборони держави доцільно також включити захист ОКІ, що забезпечить ефективніший розподіл сил і засобів під час планування оборонних операцій [1].

Кожен об'єкт критичної інфраструктури має бути завчасно оцінений фахівцями та підготовлений до оборони з урахуванням пропозицій військового командування, підрозділи якого здійснюватимуть його утримання. Підготовку об'єкта до оборони слід розпочинати з далеких підступів до нього, які проходять територіями місцевих громад; отже, представники місцевої влади мають бути залучені до процесів планування і підготовки територій до оборони [1].

Недостатньо лише спланувати й підготувати оборону об'єкта: у мирний час необхідно розробити алгоритм дій та матеріально-технічне забезпечення для евакуації обладнання і персоналу в безпечні райони, а в окремих випадках — передбачити заходи щодо підготовки

об’єкта до контрольованого виведення з ладу/знищення за визначеними процедурами [1].

Найважливішим завданням є захист ОКІ від ударів з повітря (ракетних ударів, атак ударних БпЛА). Маскування, заглиблення (укриття) ключових елементів, зміна режимів функціонування, розосередження компонентів, дублювання функцій структурними елементами підприємства мають бути інтегровані в загальний задум забезпечення стійкості та збереження працездатності [1; 2].

За практичним досвідом, одна з бригад ТрО отримала перелік об’єктів, які необхідно було взяти під охорону та оборону. Перелік налічував майже 200 об’єктів в обласному центрі, тоді як спроможності бригади не були розраховані на таку кількість. Після ретельного аналізу списку в обласній державній адміністрації було встановлено, що близько 30% позицій становили приватні дрібні підприємства, які не відповідали критеріям критичності. Водночас низку дійсно критичних підприємств не було включено до переліку, а їх керівництво помилково вважало, що може організувати оборону силами внутрішньої служби безпеки або приватної охоронної структури, зокрема групами швидкого реагування мінімального складу та з обмеженим озброєнням [1].

Шляхи посилення захисту об’єктів критичної інфраструктури

- розроблення чітких критеріїв віднесення об’єктів до критичної інфраструктури [1; 2];
- упровадження системних заходів підвищення безпеки ОКІ з боку органів державної влади та керівників підприємств державного і приватного секторів із належним ресурсним забезпеченням [1; 2];
- обладнання критично важливих об’єктів захисними спорудами, підземними комунікаціями/приміщеннями, шляхами евакуації з урахуванням маскувальних можливостей від наземного та повітряного противника [2];
- розосередження майданчиків для персоналу та місць зберігання вибухонебезпечних матеріалів [2];
- розбудова інтегрованої системи протиповітряної і протиракетної оборони для захисту критичної інфраструктури та енергетичного сектору, а також уточнення завдань підрозділів ППО/ПРО під час бойових дій [1; 2];
- узгодження дій органів влади всіх рівнів щодо прикриття ОКІ, чіткий розподіл відповідальності за моніторинг, захист і своєчасне ухвалення рішень [1; 2];
- ретельне планування охорони й оборони ОКІ, визначення загроз та виділення сил і засобів для протидії [1];
- відпрацювання довідників і настанов із застосування підрозділів Сил оборони під час оборони ОКІ; вивчення тактики противника; проведення командно-штабних навчань і практичних тренувань [2].

Таблиця – Сектори критичної інфраструктури та система їх захисту

Сектори критичної інфраструктури	**Система захисту (узагальнено)**
Урядування та публічні (адміністративні) послуги	Має здійснюватися удосконалення законодавства та уніфікація критеріїв критичності і процедур категоризації
Енергозабезпечення (у т.ч. теплова енергія)	Слід забезпечити функціонування чіткої координаційної вертикалі через КМУ та профільний координаційний центр
Водопостачання та водовідведення	Має бути розмежовано повноваження координації і контролю між КМУ та РНБО з постійним моніторингом
Продовольче забезпечення	Доцільно визначити провідного координатора: у мирний час — МВС, у воєнний — МО та ГШ ЗСУ
Охорона здоров’я	Слід здійснювати планування захисту з визначенням необхідних сил і засобів та їх резервування

Сектори критичної інфраструктури	Система захисту (узагальнено)
Фармацевтична промисловість	Має бути покладено охорону об’єктів на НГУ як спроможний інструмент мирного і воєнного часу
Виробництво вакцин, біолабораторії	Доцільно планувати оборону об’єктів із залученням ЗСУ та інших складових Сил оборони
Інформаційні послуги, електронні комунікації	Слід упроваджувати довідники і настанови щодо оборони з урахуванням тактики противника
Фінансові послуги	Має здійснюватися регулярна підготовка органів управління та підрозділів (навчання, тренування)
Транспортне забезпечення	Доцільно забезпечити міжвідомчу взаємодію та чіткий розподіл відповідальності
Оборона, державна безпека	Має бути інтегровано захист ОКІ в оборонне планування та розподіл сил і засобів
Правопорядок і правосуддя	Слід запроваджувати посилені режимні заходи та спеціальні режими роботи об’єктів
Цивільний захист і служби порятунку	Має забезпечуватися безперервність функцій, резервування та готовність до відновлення
Космічна діяльність і технології	Доцільно закріпити інституційну відповідальність і інтеграцію в державні програми стійкості
Хімічна промисловість	Слід посилювати фізичний захист і інженерну стійкість залежно від рівня критичності
Дослідницька діяльність	Має плануватися безперервність функціонування, збереження даних і обладнання

Примітка. Таблицю складено на основі положень Закону України “Про критичну інфраструктуру” та узагальнених аналітичних матеріалів щодо захисту об’єктів критичної інфраструктури в умовах збройної агресії (1; 2).

Слід відмітити що в разі ретельно відпрацьованих зазначених вище питань всіма вказаними структурами особливу увагу потрібно приділити саме підготовці підрозділів які будуть безпосередньо здійснювати оборону об’єктів критичної інфраструктури а також органам управління і планування які отримають визначень завдання.

Висновки

Система захисту критичної інфраструктури України потребує якнайшвидшого комплексного та системного вдосконалення, що, з урахуванням сучасних воєнних загроз, доцільно реалізувати за такими основними напрямами:

1. **Удосконалення законодавства України** у сфері захисту об’єктів критичної інфраструктури з урахуванням умов воєнного стану та досвіду збройної агресії Російської Федерації [1].
2. **Створення чіткої координаційної вертикалі**, відповідальної за захист об’єктів критичної інфраструктури, що передбачає формування профільного координаційного центру при Кабінеті Міністрів України на чолі з Прем’єр-міністром або Віце-прем’єр-міністром. До складу такого центру мають увійти центральні органи виконавчої влади, відповідальні за відповідні сектори критичної інфраструктури та їх захист. Центр має затверджувати перелік об’єктів, що підлягають захисту, плани їх захисту, склад необхідних сил і засобів, а також нормативно-правові акти з відповідної проблематики та узгоджувати з Генеральним штабом Збройних Сил України плани захисту таких об’єктів [1; 2].
3. **Покладання на Міністерство внутрішніх справ України** координаційних функцій щодо

захисту об’єктів критичної інфраструктури у мирний час та загрозливий період, що обґрунтовується наявністю у його підпорядкуванні збройних формувань Національної гвардії України, здатних виконувати відповідні завдання [1; 5].

4. **Покладання на Національну гвардію України** завдань з охорони об’єктів критичної інфраструктури як на структуру, що має необхідні сили і засоби та може ефективно застосовуватися в мирний час, загрозливий період і під час дії воєнного стану [1; 5].
5. **Покладання на Генеральний штаб Збройних Сил України** завдань щодо розроблення планів захисту й оборони об’єктів критичної інфраструктури, які залучаються в умовах воєнного стану, а також визначення складу сил і засобів Збройних Сил України та інших складових Сил оборони, що мають бути задіяні для посилення захисту (оборони) таких об’єктів [1].
6. **Розмежування завдань координації та контролю** у сфері захисту об’єктів критичної інфраструктури між Кабінетом Міністрів України та Радою національної безпеки і оборони України, що передбачає посилення контрольних функцій РНБО України та запровадження системи постійного моніторингу стану захисту об’єктів критичної інфраструктури [1].
7. **Розроблення і відпрацювання довідників та настанов** щодо застосування підрозділів Сил оборони під час ведення оборони об’єктів критичної інфраструктури, систематичне вивчення тактики дій підрозділів противника, а також проведення командно-штабних навчань з органами управління і практичних тренувань з підрозділами, залученими до захисту об’єктів критичної інфраструктури [2; 5].

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Про критичну інфраструктуру : Закон України № 1882-IX від 16.11.2021. Відомості Верховної Ради України (ВВР). 2022. № 16. Ст. 146. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Як удосконалити захист об’єктів критичної інфраструктури України. Оборонно-промисловий кур’єр : інформаційне агентство. 25.02.2025. URL: https://opk.com.ua/
3. Про внесення змін до деяких законів України щодо удосконалення системи підготовки громадян України до військової служби : Закон України № 3724-IX від 22.05.2024. Відомості Верховної Ради України (ВВР). 2024. № 31. Ст. 229. URL: https://zakon.rada.gov.ua/laws/show/3724-20#Text
4. Про внесення змін до деяких законів України щодо уточнення завдань та основ підготовки і ведення національного спротиву : Закон України № 2024-IX від 27.01.2022. Відомості Верховної Ради України (ВВР). 2023. № 14. Ст. 35. URL: https://zakon.rada.gov.ua/laws/show/2024-20#Text
5. Про основи національного спротиву : Закон України № 1702-IX від 16.07.2021. Відомості Верховної Ради України (ВВР). 2021. № 41. Ст. 339. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text
6. Кілька фактів про Рух опору та Сили спеціальних операцій ЗСУ. Espreso.tv (укр.). 29.07.2023. URL: https://espreso.tv/den-sso-kilka-faktiv-pro-rukh-oporu-ta-sili-spetsialnikh-operatsiy-zsu

7. Командувач ССО: Рух опору діє на всіх операційних напрямках. Українська правда (укр.). 10.01.2023. URL: https://www.pravda.com.ua/news/2023/01/10/7384226/

References

1. Verkhovna Rada of Ukraine. (2021, November 16). *Pro krytychnu infrastrukturu* [Law of Ukraine No. 1882-IX]. https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Oboronno-promyslovyi kurier. (2025, February 25). *Yak udoskonalyty zakhyst obiektiv krytychnoi infrastruktury Ukrainy*. https://opk.com.ua/
3. Verkhovna Rada of Ukraine. (2024, May 22). *Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo udoskonalennia systemy pidhotovky hromadian Ukrainy do viiskovoi sluzhby* [Law of Ukraine No. 3724-IX]. https://zakon.rada.gov.ua/laws/show/3724-20#Text
4. Verkhovna Rada of Ukraine. (2022, January 27). *Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo utochnennia zavdan ta osnov pidhotovky i vedennia natsionalnoho sprotyvu* [Law of Ukraine No. 2024-IX]. https://zakon.rada.gov.ua/laws/show/2024-20#Text
5. Verkhovna Rada of Ukraine. (2021, July 16). *Pro osnovy natsionalnoho sprotyvu* [Law of Ukraine No. 1702-IX]. https://zakon.rada.gov.ua/laws/show/1702-20#Text
6. Espreso.tv. (2023, July 29). *Kilka faktiv pro rukh oporu ta syly spetsialnykh operatsii ZSU*. https://espreso.tv/den-sso-kilka-faktiv-pro-rukh-oporu-ta-sili-spetsialnikh-operatsiy-zsu
7. Ukrainska Pravda. (2023, January 10). *Komanduvach SSO: Rukh oporu diie na vsikh operatsiinykh napriamkakh*. https://www.pravda.com.ua/news/2023/01/10/7384226/