DOI 10.52363/2414-5866-2025-1-33
УДК 35.07:355.01

Шевченко К.Р., *магістр, БНАУ, м. Біла Церква,*
ORCID: 0009-0005-1774-4174

Shevchenko K., *Master's degree, Bila Tserkva National Agrarian University, Bila Tserkva*

МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ ПРИ ЗАХИСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОЇ АГРЕСІЇ

MECHANISMS OF PUBLIC ADMINISTRATION IN THE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES IN THE CONTEXT OF MILITARY AGGRESSION

У статті досліджено питання, що стосуються відповідальності складових єдиної державної системи цивільного захисту для забезпечення належного рівня безпеки об'єктів критичної інфраструктури в умовах воєнної агресії. Встановлено основні критерії небезпеки об'єктів критичної інфраструктури, які визначають їх стан безпеки. Визначено основні принципи функціонування державної системи захисту об'єктів критичної інфраструктури. Розкрито функціональну відповідальність основних елементів державного управління на рівні регіону та визначено суб'єктно-об'єктні взаємодії між критеріями безпеки об'єктів критичної інфраструктури та органами державного управління.

Ключові слова: *механізми державного управління, об'єкти критичної інфраструктури, єдина державна система цивільного захисту, воєнний стан, комісія з техногенно-екологічної безпеки та надзвичайним ситуаціям.*

The article examines the issues related to the responsibility of the components of the unified state civil defense system to ensure an adequate level of security of critical infrastructure facilities in the context of military aggression. The main criteria of critical infrastructure facilities hazard that determine their security status are established. The basic principles of the functioning of the state system of critical infrastructure protection are determined. The functional responsibility of the main elements of public administration at the regional level is revealed and the subject-object interactions between the criteria for the security of critical infrastructure and public administration bodies are determined.

Keywords: *mechanisms of public administration, critical infrastructure facilities, unified state system of civil protection, martial law, commission on technogenic and ecological safety and emergency situations.*

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

Постановка проблеми. При військовій агресії, такі об’єкти як електростанції, насосні водопостачання, метрополітен, лікарні, підприємства по виробництву військового та харчового призначення стають основними цілями ракетних атак. Такі об’єкти відносяться до об’єктів критичної інфраструктури [8]. Окрім ракетних обстрілів такі об’єкти підлягають постійним диверсійним та терористичним атакам. Виходячи з того, що вони забезпечують функціонування найбільш чуттєвих ланок життєзабезпечення держави, їх безпека є пріоритетним завданням держави. В Україні функції забезпечення безпеки об’єктів критичної інфраструктури покладено на Єдину державну систему цивільного захисту (ЄДСЦЗ) [4]. Однак до ЄДСЦЗ входить велика кількість державних органів та служб різного підпорядкування, відповідно координація їх діяльності та розподіл повноважень та відповідальності є складною проблемою. Особливо питання ускладнюється в умовах військової агресії та під час функціонування воєнного стану.

Аналіз останніх досліджень і публікацій. Єдиною державною системою цивільного захисту є сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади, які забезпечують реалізацію державної політики у сфері цивільного захисту [7]. Вивчення нормативно-правової бази України у сфері захисту критичної інфраструктури свідчить про необхідність удосконалення законодавства та координації між державними і приватними структурами. Зокрема, в аналітичній доповіді Національного інституту стратегічних досліджень підкреслюється важливість розробки єдиної державної політики у цій сфері та впровадження стратегічних підходів до управління ризиками [9].

Дослідження загроз об'єктам критичної інфраструктури в умовах воєнного стану акцентують увагу на необхідності розробки алгоритмів для класифікації загроз з урахуванням національного та міжнародного досвіду. Це дозволяє більш ефективно ідентифікувати та реагувати на потенційні ризики [3]. З огляду на зростаючу кількість кібератак, особливо з боку російських окупантів, дослідники наголошують на необхідності посилення кіберзахисту об'єктів критичної інфраструктури. Так, в роботі [6] авторами узагальнено систему заходів, спрямованих на підвищення стійкості до кібератак, зокрема в енергетичній галузі. Ефективний захист критичної інфраструктури неможливий без належної підготовки фахівців та координації між різними відомствами. Ефективність проведення міжвідомчих навчань, спільних тренувань та занять для підвищення кваліфікації персоналу продемонстровано в роботі [2].

Аналіз досвіду зарубіжних країн у сфері захисту критичної інфраструктури вказує на важливість адаптації міжнародних стандартів та практик до українських реалій. Зокрема, вивчається досвід країн-членів ЄС та НАТО щодо побудови систем захисту та стійкості критичної інфраструктури [1].

Таким чином, захист об'єктів критичної інфраструктури під час війни є багатофакторним завданням, що вимагає комплексного підходу, включаючи вдосконалення нормативно-правової бази, посилення кібербезпеки, підготовку персоналу та адаптацію міжнародного досвіду. Подальші дослідження та практичні заходи повинні бути спрямовані на підвищення стійкості та безпеки критичної інфраструктури України в умовах воєнного стану.

Постановка завдання. Метою статті є визначення взаємозв'язків та ступеня відповідальності складових єдиної державної системи цивільного захисту при забезпеченні безпеки об'єктів критичної інфраструктури при військовій агресії.

Виклад основного матеріалу. Адміністративно-правове забезпечення заходів із захисту та підвищення стійкості об'єкта критичної інфраструктури є ключовим елементом діяльності оператора критичної інфраструктури. Для належного функціонування системи безпеки об'єкта необхідно забезпечити наявність ряду обов'язкових документів і підтверджень. Передусім, на об'єкті має бути створено структурний підрозділ режимно-секретного органу (РСО), який відповідатиме за захист інформації з обмеженим доступом. Обов'язковим є також оформлення паспорта безпеки об'єкта, погодженого відповідним секторальним органом, та загальної характеристики об'єкта критичної інфраструктури, що містить основні відомості про його функціонування. Оператор повинен мати документацію, яка відображає ідентифіковані проектні загрози на національному, секторальному (у разі затвердження) та об'єктовому рівнях, а також плани захисту об'єкта відповідно до кожного з цих рівнів. Окремо мають бути розроблені вимоги до організації захисту об'єкта, а також об'єктовий план заходів щодо забезпечення його стійкості. Важливо, щоб були реалізовані рекомендації, сформульовані за підсумками попереднього моніторингу безпеки.

У сфері ризик-менеджменту оператор зобов'язаний мати правила управління ризиками безпеки, план локалізації та ліквідації наслідків аварій, а також документи, що стосуються інформаційної безпеки, включно з політикою управління ризиками, методикою оцінювання та оброблення ризиків. Кожна особа, відповідальна за захист об'єкта, повинна діяти згідно з посадовими інструкціями.

Крім того, оператор критичної інфраструктури повинен забезпечити безперервну взаємодію з підприємствами, які надають життєво важливі послуги, зокрема централізоване водопостачання, водовідведення, теплопостачання, енергозабезпечення, зв'язок, транспорт, медичну допомогу та охорону. Така взаємодія має бути підтверджена чинними договорами. Усі плани захисту об'єкта необхідно погодити з відповідними функціональними органами, а також забезпечити належне фінансування заходів безпеки і матеріально-технічну спроможність для їх реалізації. Сукупність вищезазначених заходів формує основу ефективної системи захисту об'єкта критичної інфраструкту-

ри, особливо актуальної в умовах загроз воєнного характеру.

В умовах воєнного стану питання фінансування та міжвідомчої взаємодії щодо захисту об'єктів критичної інфраструктури набувають особливої ваги та стратегічного значення. З огляду на підвищений рівень загроз – зокрема ймовірність збройних атак, диверсій, ракетних ударів, кібератак, порушення логістичних та енергетичних ланцюгів – держава та оператори критичної інфраструктури мають діяти в умовах постійної мобілізаційної готовності, забезпечуючи безперервне функціонування об'єктів, що підтримують життєдіяльність суспільства. У період дії воєнного стану забезпечення належного рівня фінансування системи захисту критичної інфраструктури стає не просто операційною задачею, а безпосередньо пов'язаним із національною безпекою. Держава може застосовувати механізми пріоритетного бюджетного фінансування, перерозподілу коштів, спрощеного доступу до резервів та ресурсів оборонного призначення. Особливої актуальності набуває формування стратегічних запасів ресурсів, у тому числі пального, техніки, обладнання, медикаментів, продовольства тощо [5].

Крім того, в умовах воєнного стану важливо передбачити гнучкість фінансування, що дозволяє оперативно реагувати на зміни ситуації, здійснювати екстрене відновлення пошкодженої інфраструктури та підтримувати її резервні потужності. Значну роль відіграють також залучення міжнародної допомоги, іноземного фінансування та участь у програмах партнерської підтримки безпеки.

Взаємодія з іншими суб'єктами національної системи в умовах воєнного стану дозволяє додатково підвищити її стійкість. В умовах збройної агресії міжвідомча взаємодія переходить у режим постійної координації, оперативного обміну інформацією та спільного прийняття рішень у реальному часі. Кожен об'єкт критичної інфраструктури стає потенційною мішенню, тому інтеграція оператора у систему територіальної оборони, сил безпеки і оборони має бути забезпечена не лише формально, а й на практиці.

Забезпечення стійкого зв'язку з військово-цивільними адміністраціями, силами оборони, розвідкою, СБУ, ДСНС, поліцією, кібервійськами та іншими державними структурами є ключовою умовою для ефективного функціонування об'єкта критичної інфраструктури в умовах воєнного стану. Такий зв'язок має бути не лише технічно захищеним, але й організаційно інтегрованим у спільну систему управління безпековими процесами.

Обмін інформацією про загрози та ризики у режимі реального часу дозволяє оперативно оновлювати ситуаційну картину, виявляти потенційні вектори атак, координувати запобіжні дії, а також оптимізувати реагування у разі реального інциденту. У воєнний період така інформація може мати статус обмеженого доступу або навіть таємну класифікацію, тому організація її обігу потребує участі режимно-секретних органів (РСО) та чітко визначених процедур. Особливу роль відіграє створення умов для діяльності підрозділів

безпеки на території об’єкта – зокрема, розміщення мобільних пунктів спостереження, забезпечення прихованого доступу для сил спецпризначення, резервного електропостачання, укриттів, систем відеоспостереження та оперативного зв’язку. Об’єкти критичної інфраструктури мають бути здатні не лише протистояти загрозам самостійно, але й діяти в повній синергії з державними силовими структурами.

Крім того, в умовах воєнного стану реагування на інциденти та ліквідація їх наслідків відбувається у тісній взаємодії з регіональними штабами оборони, координаційними центрами та оперативними групами. Така взаємодія передбачає не лише спільне реагування, а й участь у плануванні, прогнозуванні та відпрацюванні сценаріїв можливого розвитку подій.

Важливо зазначити, що навіть неушкоджений об’єкт критичної інфраструктури може стати вразливим, якщо порушена його логістика, енергозабезпечення чи комунікаційна інтеграція з іншими елементами системи. Тому взаємодія повинна включати також співпрацю з постачальниками послуг – водоканалами, електромережами, транспортом, медичними установами – які забезпечують мінімально необхідні умови для життєдіяльності об’єкта в умовах надзвичайного або бойового навантаження.

Узагальнюючи зазначене вище, в умовах воєнного стану ефективність системи захисту критичної інфраструктури прямо залежить від трьох складових: гарантованого фінансування, наявності оперативних резервів, та стійкої багаторівневої взаємодії з державними структурами, правоохоронними органами та іншими операторами критичної інфраструктури. Їхнє поєднання забезпечує не лише фізичну стійкість об’єкта, але й його функціональну безперервність – що є одним із ключових чинників національної безпеки в умовах війни.

З метою створення ефективної, стійкої та взаємодіючої системи захисту критичної інфраструктури в Україні, слід визначити ключові принципи, що формують методологічне та організаційне підґрунтя її функціонування. Ці принципи мають бути фундаментом для розроблення політик, нормативно-правових актів, процедур управління ризиками, а також взаємодії між усіма зацікавленими сторонами.

Виходячи із отриманих вище результатів до основних принципів функціонування національної системи захисту критичної інфраструктури можна віднести:

Єдність методологічних засад – передбачає застосування уніфікованих підходів, стандартів та інструментів для ідентифікації, оцінки ризиків, управління інцидентами та реагування на загрози критичній інфраструктурі. Це забезпечує цілісність та узгодженість дій усіх суб’єктів системи.

Координованість – означає узгодження дій між органами державної влади, обласними, місцевими органами, суб’єктами господарювання та іншими учасниками процесу для досягнення спільної мети – забезпечення

безпеки критичної інфраструктури. Центральну роль у координації відіграє уповноважений орган, який забезпечує міжвідомчу взаємодію.

Державно-приватне партнерство – визнає ключову роль приватного сектору, який володіє, експлуатує або управляє значною частиною критичних об'єктів, у забезпеченні їх захисту. Співпраця між державою і бізнесом ґрунтується на довірі, обміні інформацією, спільному плануванні заходів реагування та підвищенні стійкості об'єктів.

Безпека, захист та охорона інформації з обмеженим доступом – передбачає запровадження заходів щодо запобігання несанкціонованому доступу, розголошенню або втраті інформації, що стосується вразливостей, загроз, інцидентів або планів захисту критичних об'єктів. Інформаційна безпека є невід'ємною складовою загального рівня захисту.

Далі розглянемо складові ЄДС ЦЗ на прикладі військово-цивільної адміністрації області та визначемо їх суб'єктно-об'єктну взаємодію з критеріями безпеки об'єктів критичної інфраструктури.

Під час дії воєнного стану в Україні захист критичної інфраструктури набуває особливої ваги та здійснюється в умовах підвищених ризиків, пов'язаних із військовими діями, загрозами терористичного характеру, кібератаками, порушенням логістики, енергетичної стабільності та соціального порядку. У таких умовах значно посилюється роль органів виконавчої влади, місцевого самоврядування, силових структур і служб цивільного захисту. У прифронтових областях, які перебувають в зоні підвищеної небезпеки, особливо важливою є чітка і злагоджена взаємодія всіх суб'єктів системи безпеки та реагування.

Голова обласної військово-цивільної адміністрації (ВЦА) та одночасно голова регіональної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій (ТЕБ та НС) здійснює загальне керівництво заходами із захисту критичної інфраструктури, приймає стратегічні рішення та координує взаємодію всіх залучених структур. У воєнний час його рішення мають пріоритетне значення і можуть мати обов'язковий характер для органів місцевої влади та підприємств, незалежно від форми власності.

Звичайно що у прифронтових регіонах визначальну роль у механізмах державного управління відіграють представники міністерства оборони України. Їхня участь забезпечує стабільність, координацію та ефективне управління в регіоні, де ведуться бойові дії або існує реальна загроза їх початку. Військові структури відповідають за організацію оборони території, утримання ліній фронту, мінування місцевості та проведення бойових операцій. У межах ВЦА вони визначають зони з особливим режимом доступу, контролюють евакуаційні маршрути, розміщення військових підрозділів та оборонних об'єктів.

Окрему увагу військові приділяють охороні критичної інфраструктури – об'єктів енергетики, водопостачання, транспорту, зв'язку, медицини.

Разом із підрозділами Національної гвардії, поліції та інших силових органів вони здійснюють патрулювання, охорону стратегічних об'єктів, контроль на блокпостах, перевірку документів, боротьбу з диверсійно-розвідувальними групами. В умовах бойових дій військові забезпечують супровід гуманітарних вантажів, охорону евакуаційних колон, участь у розгортанні польових шпиталів, облаштуванні укриттів та пунктів тимчасового розміщення населення. Директор Департаменту цивільного захисту ВЦА, як заступник голови регіональної комісії, відповідає за організацію системи цивільного захисту, забезпечує функціонування регіональних планів реагування, проводить моніторинг і координацію дій на місцях. У воєнний час його діяльність включає управління евакуаційними заходами, цивільною обороною та оповіщенням населення.

Начальник Головного управління ДСНС у області, який також є заступником голови регіональної комісії (за згодою), організовує рятувальні операції, роботи з розмінування, ліквідацію наслідків обстрілів та інших надзвичайних ситуацій, що виникають унаслідок військових дій.

Керівники структурних підрозділів ВЦА – департаментів охорони здоров'я, освіти, економіки, промисловості, ЖКГ, агрополітики, фінансів, соціального захисту, екології – забезпечують безперебійне функціонування відповідних галузей критичної інфраструктури. В умовах воєнного стану вони здійснюють оперативну координацію з військовими, силовими структурами та гуманітарними організаціями для забезпечення базових потреб населення.

Особливої ваги набуває роль Департаменту оборонної та мобілізаційної роботи, який координує питання мобілізації, резервування, залучення людських і матеріальних ресурсів для потреб оборони, забезпечує взаємодію з військовими формуваннями.

Силові структури (СБУ, Нацполіція, прокуратура, Нацгвардія, прикордонна служба), які входять до складу комісії за згодою, здійснюють охорону об'єктів критичної інфраструктури, контрдиверсійні заходи, забезпечують громадський порядок, виявляють та нейтралізують загрози. Інші учасники, як-то начальник регіонального центру з гідрометеорології, керівник залізниці, очільники лабораторних центрів, екологічних та санітарних служб, забезпечують безперервний обмін критично важливою інформацією, підтримку логістичних шляхів, контроль за епідеміологічною ситуацією, станом довкілля, водопостачанням та безпечністю продуктів харчування.

Таким чином, система захисту критичної інфраструктури в умовах воєнного стану функціонує як багаторівнева структура з чітким розподілом повноважень і завдань, де кожен посадовець несе відповідальність за конкретний напрям дій, а ефективність захисту забезпечується лише за умови постійної взаємодії, інформаційного обміну, оперативного реагування та централізованого управління.

Висновки. Роль держави у забезпеченні захисту та стійкості об'єктів критичної інфраструктури є стратегічно визначальною і багатогранною. Вона полягає не лише у створенні нормативно-правової бази, а й у координації, контролі, фінансуванні та безпосередньому управлінні процесами захисту в умовах загроз, зокрема воєнної агресії.

По-перше, держава виступає ініціатором та гарантом розробки законодавчих і нормативних актів, які визначають вимоги до суб'єктів критичної інфраструктури щодо безпеки, стійкості, реагування на надзвичайні ситуації та інформаційного захисту. Вона визначає критерії критичності об'єктів, правила ідентифікації загроз та порядок взаємодії між органами влади й операторами інфраструктури.

По-друге, через уповноважені органи держава забезпечує моніторинг, контроль і нагляд за дотриманням стандартів безпеки. Це стосується погодження паспортів безпеки, планів захисту, перевірки готовності до реагування та координації дій у разі виникнення кризових ситуацій.

По-третє, держава здійснює міжвідомчу координацію, забезпечує єдину систему реагування на загрози, розробляє національні та секторальні стратегії безпеки, а також сприяє створенню спроможностей для захисту об'єктів, які мають важливе значення для функціонування суспільства та економіки.

По-четверте, фінансове та ресурсне забезпечення безпеки критичної інфраструктури також є обов'язком держави. Це особливо важливо у воєнний час, коли оператори можуть потребувати додаткових ресурсів для підтримки своєї стійкості.

Загалом, держава виконує роль регулятора, координатора, партнера і гаранта національної безпеки, що дозволяє забезпечити єдність, ефективність і цілеспрямованість заходів із захисту критичної інфраструктури.

Список використаних джерел:

1. Братель С. Г. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури // Теоретичні та практичні аспекти забезпечення національної безпеки. 2023. № 3. С. 261–265.
2. Гаврись А. П., Філіппова В. В., Тур Н. Ю. Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану // Bulletin of Lviv State University of Life Safety. – 2024. – № 30. – С. 173–187.
3. Герасименко О. М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану // Науковий вісник Ужгородського національного університету. – 2024. – С. 257–263.
4. Кодекс цивільного захисту України: Закон України від 02.10.2012 № 5403-VI. Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text.
5. Комісарова Н.О., Крутіков П.Д. Система кіберзахисту об'єктів критичної інфраструктури в умовах ведення війни // Науковий вісник Київського інституту Національної гвардії України. 2024. № 2. С. 43–48.

6. Мануйлов Я.С. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни // Інформація і право. 2023. № 1(44). С. 154–167.

7. Про затвердження Порядку ідентифікації об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.01.2014 № 11 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#Text.

8. Про критичну інфраструктуру: Закон України від 21.09.2024 № 1882-IV. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

9. Хрутьба В.О., Зюзюн В.І., Неведров Д.С. Огляд науково-теоретичних аспектів безпеки об'єктів критичної інфраструктури транспорту // Вісник Національного технічного університету «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. 2019. № 2(1327). С. 60–65.

References:

1. Bratel, S. G. (2023). Experience of foreign countries in the field of ensuring the security of critical infrastructure facilities. Theoretical and Practical Aspects of National Security, (3), 261–265.

2. Havrys, A. P., Filippova, V. V., & Tur, N. Yu. (2024). Information analysis of critical infrastructure protection systems during martial law. Bulletin of Lviv State University of Life Safety, (30), 173–187.

3. Herasymenko, O. M. (2024). Threats to critical infrastructure facilities of Ukraine under martial law. Scientific Bulletin of Uzhhorod National University, 257–263.

4. Verkhovna Rada of Ukraine. (2012). Code of Civil Protection of Ukraine: Law of Ukraine of 02.10.2012 No. 5403-VI [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/5403-17#Text

5. Komissarova, N. O., & Krutikov, P. D. (2024). The system of cyber defense of critical infrastructure in the conditions of war. Scientific Bulletin of the Kyiv Institute of the National Guard of Ukraine, (2), 43–48.

6. Manuilov, Y. S. (2023). Ensuring cybersecurity of critical infrastructure facilities in cyber warfare. Information and Law, 1(44), 154–167.

7. Cabinet of Ministers of Ukraine. (2014). On Approval of the Procedure for Identification of Critical Infrastructure Objects: Resolution No. 11 dated 09.01.2014. Retrieved from https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#Text.

8. Verkhovna Rada of Ukraine. (2024). On Critical Infrastructure: Law of Ukraine of 21.09.2024 No. 1882-IV [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.

9. Khrutba, V. O., Ziuziun, V. I., & Nedvedrov, D. S. (2019). Review of scientific and theoretical aspects of security of critical transport infrastructure facilities. Bulletin of the National Technical University “KhPI”. Series: Strategic Management, Portfolio, Program and Project Management, 2(1327), 60–65.

дата надходження статті: 25.04.2025
дата прийняття статті: 19.05.2025
дата публікації: 25.06.2025