DOI: 10.46972/2076-1546.2026.30.10

УДК 351.86:355.4

В. А. Каптур, канд. техн. наук, ст. наук. співроб.
Окремий спеціальний центр електронної підтримки Командування Сухопутних військ Збройних Сил України
https://orcid.org/0000-0003-4200-1151

Є. П. Подкалюк
Інститут прикладних систем управління Національної академії наук України
https://orcid.org/0009-0009-4236-2986

ФОРМУВАННЯ ТА ОБҐРУНТУВАННЯ СТРУКТУРИ ТИПОВОЇ КОНЦЕПЦІЇ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНОЇ ВІЙНИ

У статті розглянуто проблематику забезпечення захисту об'єктів критичної інфраструктури в умовах сучасних воєнних загроз. Наведено основні фактори, що впливають на рівень безпеки таких об'єктів в умовах використання засобів повітряного нападу (наприклад, безпілотних літальних апаратів), диверсійних дій та інших деструктивних впливів. Також проаналізовано підходи до оцінювання рівня захищеності та формування систем безпеки для цих об'єктів.

Розглянуто вплив сучасних воєнних загроз на функціонування стратегічно важливих елементів інфраструктури держави, зокрема енергетичних підприємств, об'єктів видобувної галузі, транспортних вузлів і систем зв'язку. Проаналізовано роль безпілотних літальних апаратів, використання яких суттєво підвищує ризики порушення функціонування об'єктів критичної інфраструктури, як одного з ключових засобів ведення сучасних бойових дій.

На основі результатів проведеного аналізу обґрунтовано необхідність формування типової концепції захисту об'єктів критичної інфраструктури, яка може використовуватися як методична основа для створення комплексних систем безпеки таких об'єктів в умовах сучасної війни. У роботі запропоновано структуру концепції, що включає: аналіз загроз, прикладів атак та наявних систем захисту; оцінювання об'єкта критичної інфраструктури, зокрема його інженерних особливостей; формування підсистем моніторингу повітряної обстановки, впливу на безпілотні літальні апарати та пасивного захисту; вибір обладнання та встановлення обсягів захисту; визначення пріоритетів; організаційні заходи безпеки та оцінювання ефективності функціонування системи захисту.

Метою роботи є формування та обґрунтування структури типової концепції захисту об'єктів критичної інфраструктури в умовах сучасних воєнних загроз.

Отримані результати можуть бути використані під час розроблення програм захисту вразливих об'єктів та формування практичних рекомендацій щодо підвищення їх стійкості до сучасних загроз.

Ключові слова: *критична інфраструктура; захист об'єктів; воєнні загрози; безпілотний літальний апарат; система безпеки; концепція захисту.*

Постановка проблеми в загальному вигляді. Сучасні воєнні конфлікти передбачають активне застосуванням високотехнологічних засобів ураження, наприклад, безпілотних літальних апаратів (БпЛА), а також крилатих та балістичних ракет. Однією з ключових цілей атак із застосуванням таких засобів дедалі частіше стають об'єкти критичної інфраструктури, до яких належать енергетичні об'єкти, підприємства видобувної галузі, транспортні вузли, системи зв'язку та інші стратегічно важливі елементи функціонування економіки й обороноздатності країни [3, 4].

Досвід ведення бойових дій в Україні демонструє, що вразливість об'єктів критичної інфраструктури до комплексних атак із повітря та інших видів впливу може призводити до значних економічних втрат, порушення стабільності функціонування систем управління та створення загроз для національної безпеки. Особливої актуальності набуває питання забезпечення належного рівня захисту таких об'єктів від новітніх загроз, зокрема масованого застосування БпЛА та високоточної зброї [1, 5].

Аналіз сучасних досліджень показує, що питання підвищення рівня безпеки об'єктів критичної інфраструктури порушені в [5, 6], де запропоновано науково-методичні підходи до оцінювання рівня безпеки таких об'єктів на основі використання комплексу технічних засобів захисту від БпЛА та ракетного озброєння. У публікації [7] розглянуто особливості застосування методів оцінювання спроможностей систем захисту об'єктів в умовах повітряних загроз. У свою чергу, у роботах [2, 8] проаналізовано питання використання сучасних технологій, зокрема безпілотних систем, для забезпечення охорони та моніторингу об'єктів.

Водночас результати проведених досліджень свідчать про відсутність єдиного узагальненого підходу до формування типової концепції захисту об'єктів критичної інфраструктури в умовах сучасних воєнних загроз. Це зумовлює необхідність розроблення вимог до структури та змісту такої концепції, яка б враховувала сучасні ризики, технологічні можливості засобів захисту, а також організаційні та економічні аспекти забезпечення безпеки стратегічно важливих об'єктів.

Аналіз останніх досліджень і публікацій. Питання забезпечення безпеки об'єктів критичної інфраструктури в умовах сучасних воєнних загроз є предметом дослідження багатьох науковців і фахівців у галузі національної безпеки, оборонних технологій та систем захисту. Значна увага приділяється аналізу можливих загроз для таких об'єктів, оцінюванню їх вразливостей та розробленню ефективних підходів до формування систем захисту.

У роботі [1] проаналізовано сучасний стан розвитку питання захисту об'єктів із застосуванням інженерних боєприпасів, що дозволяє визначити основні напрями вдосконалення наявних підходів до забезпечення безпеки стратегічно важливих об'єктів. При цьому акцент зроблено на питаннях організації інженерного захисту та підвищення стійкості об'єктів до різних видів ураження.

У [3] розглянуто особливості застосування різних засобів захисту критичної інфраструктури під час збройної агресії з боку рф. Автор проаналізував практичний досвід функціонування систем захисту в умовах воєнного стану та визначив основні проблеми, що виникають у ході забезпечення безпеки стратегічно важливих об'єктів.

Важливим напрямом досліджень є розроблення методів оцінювання ефективності систем захисту критичних об'єктів в умовах протидії засобам повітряного нападу. Зокрема, у публікації [4] запропоновано системний підхід до цього питання, який передбачає комплексне врахування різних факторів, що впливають на рівень захищеності об'єктів.

Окрему групу досліджень становлять роботи, присвячені оцінюванню рівня безпеки об'єктів критичної інфраструктури на основі використання комплексних систем захисту. Так, у [5, 6] запропоновано науково-методичні підходи до визначення рівня безпеки таких об'єктів із застосуванням інтегрованих систем захисту від БпЛА, крилатих та балістичних ракет. Вони передбачають використання комплексу технічних засобів, що забезпечують виявлення, ідентифікацію та нейтралізацію повітряних загроз.

У статті [7] розглянуто можливості використання методу оцінювання спроможностей для вирішення завдань захисту вразливих об'єктів від повітряного нападу, який дозволяє оцінювати ефективність систем захисту з урахуванням їх функціональних можливостей та наявних ресурсів.

Крім того, у сучасних дослідженнях висвітлено питання використання новітніх технологій для забезпечення охорони та моніторингу таких об'єктів. Зокрема, у роботах [2, 8] проаналізовано можливості застосування безпілотних технологій та методів оцінювання вразливості таких об'єктів в умовах воєнного стану.

Питання захисту об'єктів критичної інфраструктури також активно розглядають у міжнародній практиці. Зокрема, у країнах Європейського Союзу реалізується Європейська програма захисту (European Programme for Critical Infrastructure Protection – EPCIP), яка передбачає ідентифікацію об'єктів, оцінювання ризиків їх функціонування, а також розроблення та впровадження заходів підвищення їх стійкості до різних типів загроз [9].

У країнах НАТО питання захисту критичної інфраструктури досліджуються як складова забезпечення національної та колективної безпеки. Відповідні підходи передбачають проведення комплексного аналізу загроз, оцінювання вразливостей об'єктів, підвищення рівня їх стійкості та організацію взаємодії між державними органами, військовими структурами й операторами критичної інфраструктури [10].

Крім того, у Сполучених Штатах Америки широко застосовують модель обміну інформацією про загрози для вразливих об'єктів на основі діяльності спеціалізованих центрів обміну та аналізу інформації (Information Sharing and Analysis Centers – ISAC). Основною метою таких центрів є забезпечення оперативного обміну інформацією про потенційні загрози, вразливості та інциденти між державними структурами й операторами інфраструктури [11].

Формулювання завдання дослідження. Аналіз наукових публікацій свідчить, що, попри значну кількість досліджень, присвячених окремим аспектам забезпечення безпеки

критичної інфраструктури, питання формування узагальненої типової концепції захисту таких об'єктів у сучасних умовах залишається недостатньо опрацьованим. Це зумовлює необхідність подальших досліджень у цьому напрямі, зокрема щодо визначення основних вимог до структури та змісту такої концепції.

Метою статті є формування основних вимог до типової концепції захисту об'єктів критичної інфраструктури в умовах сучасних воєнних загроз. Для досягнення поставленої мети необхідно здійснити аналіз сучасних підходів до забезпечення безпеки таких об'єктів, розглянути основні загрози їх функціонуванню в умовах війни, а також запропонувати структуру типової концепції їх захисту з урахуванням сучасних технічних, організаційних та економічних аспектів забезпечення безпеки.

Виклад основного матеріалу

Сучасні загрози для об'єктів критичної інфраструктури в умовах війни

У сучасних умовах ведення бойових дій об'єкти критичної інфраструктури стають одними з основних цілей для противника, оскільки їх ураження може суттєво вплинути на функціонування економіки, енергетичної системи, транспортних мереж та систем управління. До них належать підприємства енергетичного сектора, об'єкти видобувної галузі, транспортні вузли, системи зв'язку, а також інші елементи інфраструктури, що забезпечують життєдіяльність держави та її обороноздатність [3, 8].

Досвід сучасної війни в Україні свідчить, що засоби повітряного нападу, зокрема крилаті та балістичні ракети, а також БпЛА різних типів стали основними для ураження об'єктів критичної інфраструктури. Масоване застосування таких засобів дозволяє противнику здійснювати атаки на значній відстані та створювати неабиякі ризики для функціонування стратегічно важливих об'єктів [5, 6].

Особливу небезпеку становить широке використання БпЛА, які можуть застосовуватися як для проведення розвідки, так і для безпосереднього ураження об'єктів інфраструктури. Завдяки відносно низькій вартості, можливості масового застосування та складності своєчасного виявлення безпілотні системи стають одним із найбільш поширених інструментів ведення сучасної війни [2, 5].

Крім засобів повітряного нападу, вразливі об'єкти інфраструктури можуть зазнавати впливу інших видів загроз, зокрема диверсійних дій, кібератак, а також порушення функціонування систем управління та зв'язку. Комплексний характер цих загроз значно ускладнює забезпечення належного рівня захисту стратегічно важливих об'єктів [1, 4].

У зв'язку з цим виникає необхідність формування комплексних систем захисту об'єктів критичної інфраструктури, які повинні включати як технічні засоби протидії сучасним загрозам, так і організаційні заходи, спрямовані на підвищення стійкості функціонування таких об'єктів в умовах воєнного часу. При цьому важливим завданням є розроблення узагальненого підходу до організації захисту, що дозволить систематизувати наявні рішення та забезпечити їх ефективне застосування для різних типів об'єктів.

Необхідність формування типової концепції захисту об'єктів критичної інфраструктури

Забезпечення належного рівня захисту об'єктів критичної інфраструктури в умовах сучасних воєнних загроз є складним багатокомпонентним завданням, що потребує

системного підходу до організації заходів безпеки. Аналіз наукових досліджень показує, що відомі підходи до забезпечення безпеки об'єктів здебільшого спрямовані на вирішення таких окремих завдань: оцінювання вразливості об'єктів, визначення ефективності технічних засобів захисту, аналіз окремих типів загроз [4–7].

Водночас практичний досвід функціонування підприємств критичної інфраструктури свідчить, що заходи безпеки часто формуються з урахуванням специфіки окремих галузей, що призводить до різнорідності підходів до організації систем захисту та ускладнює їх комплексне застосування [3, 8].

У сучасних умовах збройного протистояння значна частина загроз має комплексний характер, поєднуючи застосування засобів повітряного нападу, безпілотних систем, диверсійних дій та кібернетичних атак. Це зумовлює необхідність створення багаторівневих систем захисту, що включатимуть технічні, організаційні та управлінські заходи забезпечення безпеки вразливих об'єктів [5–7].

Отже, актуальним завданням є формування типової концепції захисту об'єктів критичної інфраструктури, яка могла б стати методичною основою для розроблення систем безпеки різних об'єктів з урахуванням їх функціонального призначення та особливостей експлуатації. Вона повинна визначати основні принципи організації захисту, структуру системи безпеки та перелік ключових заходів, спрямованих на запобігання, виявлення та нейтралізацію загроз.

Пропозиції щодо структури типової концепції захисту об'єктів критичної інфраструктури

З урахуванням характеру сучасних воєнних загроз, результатів наукових досліджень у сфері захисту критичної інфраструктури, а також практичного досвіду організації безпеки підприємств енергетичного сектора доцільним є формування типової концепції захисту, яка може бути використана як методична основа для розроблення систем безпеки різних об'єктів.

Типова концепція захисту вразливих об'єктів може включати декілька взаємопов'язаних структурних складових, кожна з яких спрямована на вирішення окремих завдань забезпечення безпеки. Для наочного відображення взаємозв'язку основних елементів запропонованої концепції на рис. 1 наведено узагальнену структурну схему формування системи захисту об'єктів критичної інфраструктури.

Першим етапом є **аналіз загроз та можливих сценаріїв атак**, що передбачає визначення потенційних способів ураження об'єкта критичної інфраструктури, зокрема застосування БпЛА, ракетного озброєння, диверсійних дій або кібернетичних атак [5–7]. Це дозволить визначити найбільш імовірні сценарії впливу на об'єкт та сформувати відповідні заходи протидії.

Другим важливим елементом концепції є **характеристика об'єктів, що підлягають захисту**. На цьому етапі формується типова модель вразливого об'єкта з урахуванням площі території, конфігурації периметра, особливостей інженерних систем, мереж електроживлення, режиму функціонування та інших параметрів, що можуть впливати на побудову системи захисту.

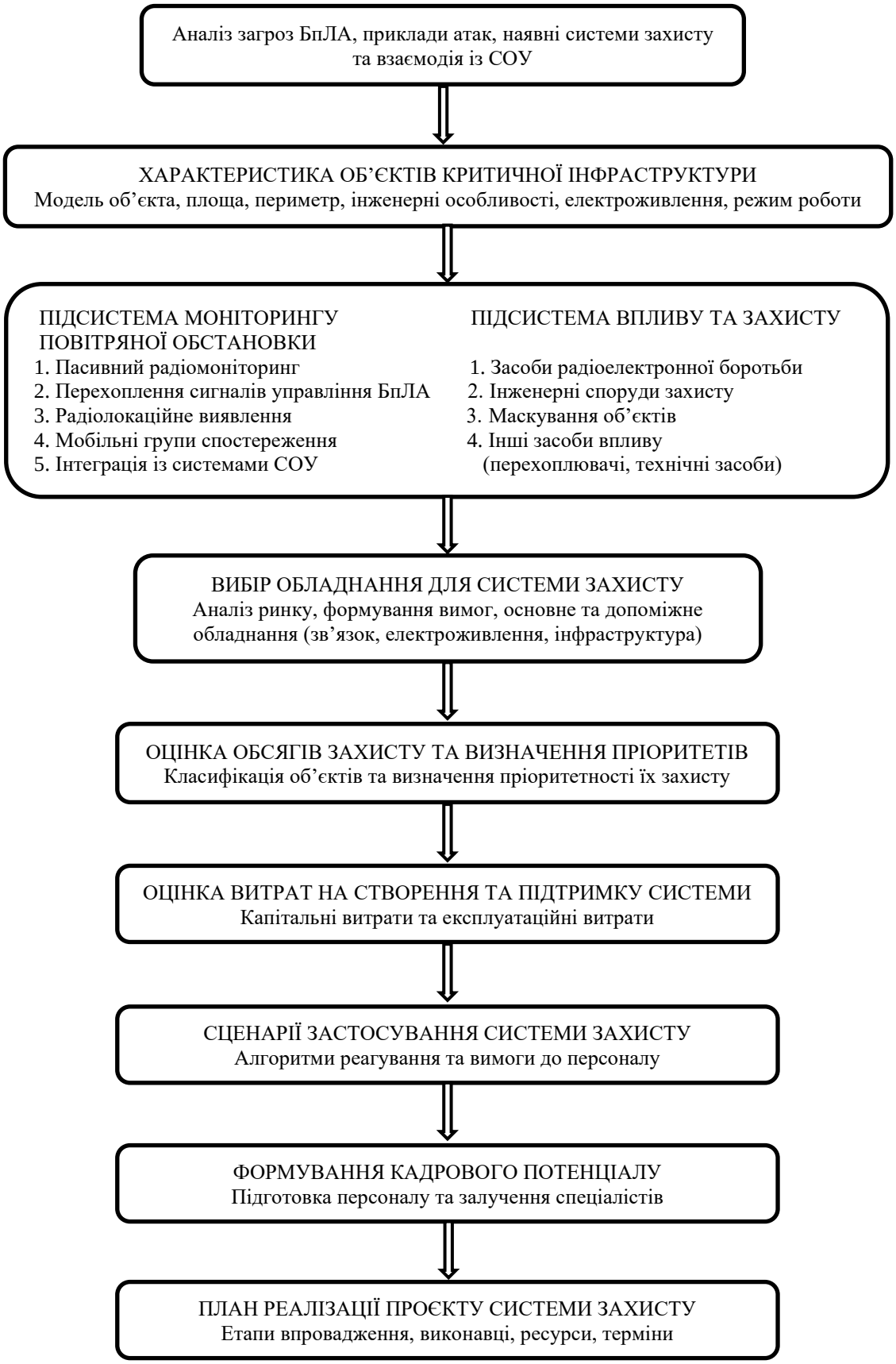

Рис. 1. Узагальнена структура типової концепції захисту об'єктів критичної інфраструктури

Як приклад об’єкта критичної інфраструктури можна розглядати підприємства енергетичного та видобувного сектору, зокрема газовидобувні комплекси. Їх особливістю є значна площа території, наявність великої кількості технологічного обладнання та безперервний режим функціонування, що підвищує їх вразливість до атак із застосуванням БпЛА або диверсійних дій.

У зв’язку з цим під час формування системи захисту для таких об’єктів особливу увагу доцільно приділяти організації систем раннього виявлення повітряних загроз, захисту ключових технологічних вузлів та забезпеченню взаємодії з підрозділами Сил оборони України (СОУ).

Наступним елементом є **формування підсистеми моніторингу повітряної обстановки**, яка може включати засоби пасивного контролю електромагнітного спектра, системи виявлення сигналів управління БпЛА, радіолокаційні засоби спостереження, а також бути інтегрованою із системами ситуаційної обізнаності СОУ (за її наявності). Використання таких засобів дозволяє забезпечити своєчасне виявлення повітряних загроз та підвищити ефективність реагування на можливі атаки.

Важливим елементом є **формування підсистеми впливу на ворожі БпЛА та підсистеми пасивного захисту**, до складу яких можуть входити засоби радіоелектронного подавлення, інженерні споруди захисту, системи маскування, а також інші технічні засоби протидії повітряним загрозам. Узагальнений алгоритм реагування системи захисту на виявлення ворожих БпЛА має такий вигляд:

1) виявлення загрози;
2) ідентифікація типу БпЛА;
3) оцінювання рівня загрози;
4) прийняття рішення щодо реагування;
5) застосування засобів протидії (радіоелектронної боротьби / інших засобів нейтралізації);
6) оцінювання результатів реагування.

Окремим напрямом є **вибір технічного обладнання для побудови системи захисту**, що передбачає формування вимог до технічних засобів, аналіз доступних рішень на ринку та визначення найбільш ефективних варіантів їх застосування.

Також важливим елементом концепції є **визначення пріоритетів захисту об’єктів**, зокрема оцінювання критичності різних елементів інфраструктури та встановлення черговості впровадження заходів безпеки з урахуванням обмеженості ресурсів.

Завершальним етапом формування концепції є **оцінювання технічної та економічної ефективності системи захисту**, що включає визначення орієнтовних капітальних та експлуатаційних витрат на створення і підтримку систем безпеки, а також оцінювання доцільності впровадження окремих технічних рішень.

Отже, запропонована структура типової концепції дозволяє систематизувати основні напрями забезпечення безпеки об’єктів критичної інфраструктури та створює основу для подальшого розроблення практичних моделей організації їх захисту в умовах сучасних воєнних загроз. Такий підхід ґрунтується на комплексному поєднанні заходів моніторингу повітряної обстановки, технічних засобів протидії загрозам, організаційних заходів безпеки та економічного обґрунтування створення системи захисту.

На відміну від відомих запропонована структура типової концепції забезпечує інтеграцію підсистем моніторингу повітряної обстановки, впливу на БпЛА, пасивного захисту, організаційних заходів та оцінювання ефективності в єдину функціонально узгоджену систему, що дозволяє реалізувати комплексний підхід до організації захисту об’єктів критичної інфраструктури в умовах сучасних воєнних загроз.

Висновки

1. Наведений у статті аналіз наукових публікацій показав, що, незважаючи на те, що об’єкти критичної інфраструктури є пріоритетними цілями в умовах сучасної війни, досі відсутній узагальнений підхід до формування комплексної концепції їх захисту.

2. Наукова новизна дослідження полягає у формуванні узагальненої структури типової концепції захисту об’єктів критичної інфраструктури, яка, на відміну від відомих підходів, забезпечує інтеграцію підсистем моніторингу повітряної обстановки, впливу на БпЛА, пасивного захисту, організаційних заходів та оцінювання ефективності в єдину функціонально узгоджену систему.

3. Достовірність отриманих результатів забезпечується аналізом наукових праць, публічних джерел та узагальненням практичного досвіду функціонування об’єктів критичної інфраструктури в умовах сучасної війни, а практична цінність роботи полягає в можливості використання запропонованого підходу як методичної основи для розроблення систем захисту об’єктів різних типів з урахуванням їх функціональних особливостей, рівня критичності та характеру загроз.

Подальші дослідження доцільно спрямувати на розроблення моделей оцінювання технічної та економічної ефективності систем захисту об’єктів критичної інфраструктури, а також на створення типових моделей організації їх захисту з урахуванням специфіки різних галузей та умов функціонування.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Аналіз стану розвитку питання захисту об’єктів критичної інфраструктури з використанням інженерних боєприпасів. URL: https://pdfs.semanticscholar.org/90e1/ecac6d9deb28362c03111c3a5777290c984d.pdf (дата звернення: 10.01.2026).

2. Застосування безпілотних технологій для охорони об'єктів критичної інфраструктури. URL: https://www.researchgate.net/publication/391692931_zastosuvanna_bezpilotnih_tehnologij_dla_ohoroni_ob'ektiv_kriticnoi_infrastrukturi (дата звернення: 12.01.2026).

3. Ліла Є. Аналіз засобів захисту критичної інфраструктури під час агресії з боку рф. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/25669/1/Ліла%20Євген.pdf (дата звернення: 10.01.2026).

4. Системний підхід до оцінювання ефективності системи захисту об’єктів критичної інфраструктури в умовах протидії ураженню їх засобами повітряного нападу. URL: http://znp.dndia.org.ua/index.php/znp/article/view/99/127 (дата звернення: 15.01.2026).

5. Науково-методичний підхід щодо оцінювання безпеки критичної інфраструктури на основі комплексу засобів захисту її об'єктів від БпЛА і крилатих ракет / С. М. Чумаченко, О. П. Кутовий , В. А. Попель та ін. // Вчені записки Таврійського нац. ун-ту ім. В. І. Вернадського.

Серія: Технічні науки. 2023. Т. 34 (73), № 1. С. 144–154. https://doi.org/10.32782/2663-5941/2023.1/22

6. Комплексний підхід до визначення рівня безпеки критичної енергетичної інфраструктури на основі інтегральної системи захисту її об'єктів від БпЛА та крилатих і балістичних ракет / С. М. Чумаченко, О. П. Кутовий , О. Г. Гуйда та ін. // Вчені записки Таврійського нац. ун-ту ім. В. І. Вернадського. Серія: Технічні науки. 2023. Т. 34 (73), № 2 (1). С. 261–267. https://doi.org/10.32782/2663-5941/2023.2.1/41

7. Особливості використання методу, що базується на оцінюванні спроможностей, для вирішення завдань захисту об'єктів критичної інфраструктури України від нападу з повітря / М. Дєнєжкін, І. Романенко, В. Башинський, Т. Побережець // Military science. 2025. Vol. 3, №. 1. С. 353–364. URL: http://nbuv.gov.ua/UJRN/milsc_2025_3_1_30 (дата звернення: 10.01.2026).

8. Щодо питання оцінювання вразливості об’єктів критичної інфраструктури в умовах воєнного стану. URL: https://sts.nangu.edu.ua/article/view/336731 (дата звернення: 10.02.2026).

9. European Commission. European Programme for Critical Infrastructure Protection (EPCIP). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0786 (last accessed: 14.01.2026).

10. NATO. Resilience and Critical Infrastructure Protection. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm (last accessed: 10.02.2026).

11. Information Sharing and Analysis Center (ISAC). URL: https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center (last accessed: 10.01.2026).

Стаття надійшла до редакції 19.03.2026.
Прийнято до друку 20.04.2026.
Дата публікації 30.06.2026.

REFERENCES

1. *Analiz stanu rozvytku pytannia zakhystu obiektiv krytychnoi infrastruktury z vykorystanniam inzhenernykh boieprypasiv [Analysis of the State of Development of the Issue of Protecting Critical Infrastructure Objects Using Engineering Munitions]*. (n. d.). Retrived from https://pdfs.semanticscholar.org/90e1/ecac6d9deb28362c03111c3a5777290c984d.pdf [in Ukrainian].

2. *Zastosuvannia bezpilotnykh tekhnolohii dlia okhorony obiektiv krytychnoi infrastruktury. [Application of Unmanned Technologies for the Protection of Critical Infrastructure Facilities]*. (n. d.). Retrived from https://www.researchgate.net/publication/391692931_zastosuvanna_bezpilotnih_tehnologij_dla_ohoroni_obektiv_kriticnoi_infrastrukturi [in Ukrainian].

3. Lila, Ye. (n. d.). *Analiz zasobiv zakhystu krytychnoi infrastruktury pid chas ahresii z boku rf [Analysis of Critical Infrastructure Protection Tools During the Aggression of the rf]*. Retrived from http://repositsc.nuczu.edu.ua/bitstream/123456789/25669/1/Lila%20Ievhen.pdf [in Ukrainian].

4. *Systemnyi pidkhid do otsiniuvannia efektyvnosti systemy zakhystu obiektiv krytychnoi infrastruktury v umovakh protydii urazhenniu yikh zasobamy povitrianoho napadu [System Approach to Assessing the Effectiveness of the Critical Infrastructure Protection System under Conditions of Countering Air Attack Weapons]*. (n. d.). Retrived from http://znp.dndia.org.ua/index.php/znp/article/view/99/127 [in Ukrainian].

5. Chumachenko, S. M., Kutovyi, O. P., & Popel, V. A., et al. (2023). Naukovo-metodychnyi pidkhid shchodo otsiniuvannia bezpeky krytychnoi infrastruktury na osnovi kompleksu zasobiv zakhystu yii obiektiv vid BpLA i krylatykh raket [Scientific and Methodological Approach to Assessing the Security of Critical Infrastructure Based on a Complex of Protection Means Against UAVs and Cruise Missiles]. *Vcheni zapysky Tavriiskoho nats. un-tu im. V. I. Vernadskoho. Seriia: Tekhnichni nauky [Scientific Notes of V. I. Vernadsky Tavriya National University. Series: Technical Sciences], 34* (73), 1, 144–154. https://doi.org/10.32782/2663-5941/2023.1/22 [in Ukrainian].

6. Chumachenko, S. M., Kutovyi, O. P., Huida, O. H. et al. (2023). Kompleksnyi pidkhid do vyznachennia rivnia bezpeky krytychnoi enerhetychnoi infrastruktury na osnovi intehralnoi systemy zakhystu yii obiektiv vid BpLA ta krylatykh i balistychnykh raket [Comprehensive Approach to Determining the Security Level of Critical Energy Infrastructure Based on an Integrated System of Protection Against UAVs and Cruise and Ballistic Missiles]. *Vcheni zapysky Tavriiskoho nats. un-tu im. V. I. Vernadskoho. Seriia: Tekhnichni nauky [Scientific Notes of V. I. Vernadsky Tavriya National University. Series: Technical Sciences], 34* (73), 2 (1), 261–267. https://doi.org/10.32782/2663-5941/2023.2.1/41 [in Ukrainian].

7. Dieniezhkin, M., Romanenko, I., Bashynskyi, V., & Poberezhets, T. (2025). Osoblyvosti vykorystannia metodu, shcho bazuietsia na otsiniuvanni spromozhnostei, dlia vyrishennia zavdan zakhystu obiektiv krytychnoi infrastruktury Ukrainy vid napadu z povitria [Features of Using a Capability-Based Assessment Method for Solving the Tasks of Protecting Critical Infrastructure Objects of Ukraine from Air Attack]. *Military science, 3*, 1, 353–364. Retrived from http://nbuv.gov.ua/UJRN/milsc_2025_3_1_30 [in Ukrainian].

8. Shchodo pytannia otsiniuvannia vrazlyvosti obiektiv krytychnoi infrastruktury v umovakh voiennoho stanu [On the Issue of Assessing the Vulnerability of Critical Infrastructure Facilities under Martial Law Conditions]. (n. d.). Retrived from https://sts.nangu.edu.ua/article/view/336731 [in Ukrainian].

9. European Commission. European Programme for Critical Infrastructure Protection (EPCIP). (n. d.). Retrived from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0786

10. NATO. Resilience and Critical Infrastructure Protection. (n. d.). Retrived from https://www.nato.int/cps/en/natohq/topics_132722.htm

11. Information Sharing and Analysis Center (ISAC). (n. d.). Retrived from https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center

V. A. Kaptur, Y. P. Podkaliuk

FORMATION AND SUBSTANTIATION OF THE STRUCTURE OF A TYPICAL CONCEPT FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES UNDER MODERN WARFARE CONDITIONS

The paper addresses the problem of ensuring the protection of critical infrastructure facilities under conditions of modern military threats. The main factors affecting the level of security of such facilities are identified, including the use of air attack means (in particular, unmanned aerial vehicles), sabotage activities, and other destructive impacts. An analysis of

scientific and public sources that consider approaches to assessing the level of protection and developing security systems for such facilities is also carried out.

The impact of modern military threats on the functioning of strategically important elements of state infrastructure, including energy enterprises, extractive industry facilities, transport hubs, and communication systems, is examined. The role of unmanned aerial vehicles as one of the key means of modern warfare is analyzed, the use of which significantly increases the risks of disruption in the functioning of critical infrastructure facilities.

Based on the conducted analysis, the necessity of forming a typical concept for the protection of critical infrastructure facilities is substantiated. Such a concept can be used as a methodological basis for the development of integrated security systems under modern warfare conditions. The paper proposes the structure of this concept, which includes threat analysis, analysis of attack scenarios and existing protection systems, assessment of the facility from the perspective of its engineering characteristics, formation of subsystems for airspace monitoring, counteraction to unmanned aerial vehicles and passive protection, selection of equipment, assessment of protection scope and prioritization, organizational security measures, and evaluation of the effectiveness of the protection system.

The aim of the study is to develop and substantiate the structure of a typical concept for the protection of critical infrastructure facilities under modern military threats.

The obtained results can be used in the development of protection programs for vulnerable facilities and in the formulation of practical recommendations aimed at increasing their resilience to modern threats.

Keywords: *critical infrastructure; infrastructure protection; military threats; unmanned aerial vehicles; security systems; protection concept.*