https://doi.org/10.35668/2520-6524-2026-3-07
УДК 355.469.5:623.746

**М. В. ІЩУК,** директор Департаменту ресурсного забезпечення
**В. Л. СИДОРЕНКО,** д-р техн. наук, проф.
**О. Г. ДОЦЕНКО,** д-р філософії, ст. дослідн.
**С. Ю. ОГУРЦОВ,** канд. техн. наук, с. н. с.

# СТВОРЕННЯ ЄДИНОЇ ІННОВАЦІЙНОЇ ЕКОСИСТЕМИ БПЛА–НРК ДЛЯ ПОСИЛЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

***Резюме.*** *У статті розглянуто можливість створення єдиної інноваційної екосистеми "безпілотні літальні апарати – наземні роботизовані комплекси" (БПЛА–НРК) як перспективного напряму підвищення стійкості критичної інфраструктури України в умовах воєнного стану. Актуальність такого підходу зумовлена активним застосуванням безпілотних систем проти об'єктів енергетики, транспорту та водопостачання, що потребує своєчасного виявлення загроз і оперативного реагування. Об'єктом дослідження є система забезпечення стійкості критичної інфраструктури України, предметом — архітектура та механізми функціонування єдиної екосистеми БПЛА–НРК. Методологічне підґрунтя дослідження становлять системний і порівняльний види аналізу, структурно-функціональне моделювання, сценарний аналіз та оцінювання ефективності організаційно-технічних рішень. Запропонована модель передбачає інтеграцію сенсорів, засобів радіоелектронної боротьби, БПЛА, наземних роботизованих комплексів і засобів кіберзахисту через центральну цифрову платформу Mission Control. Така архітектура формує єдиний інформаційний простір, у якому дані від різнорідних джерел можуть використовуватися для формування ситуаційної картини та підтримки прийняття рішень. Розглянуто також взаємодію локальних засобів захисту об'єктів із загальнодержавною системою протиповітряної оборони та питання підготовки операторів і персоналу із застосуванням цифрових навчальних засобів. Практичне значення результатів полягає в можливості використання запропонованої моделі під час створення та модернізації систем захисту енергетичних, транспортних і водогосподарських об'єктів, а також удосконалення організаційно-правових механізмів застосування безпілотних і роботизованих систем.*

***Ключові слова:*** *єдина екосистема БПЛА–НРК, критична інфраструктура, цифрова платформа, інформаційно-аналітична система, стійкість, безпілотні системи, наземні роботизовані комплекси, РЕБ, Mission Control, DELTA, кіберзахист.*

## ВСТУП

В умовах повномасштабної війни критична інфраструктура України залишається одним із ключових об'єктів впливу противника. Удари по енергетичних, транспортних, водогосподарських та інших об'єктах мають не лише безпосередні матеріальні наслідки, а й створюють ланцюгові ризики для функціонування економіки та життєзабезпечення населення [1; 2].

Особливого значення набуло широке застосування БПЛА. Їхня відносно невисока вартість, можливість масованого використання, різноманітність конструкцій і способів управління ускладнюють традиційні підходи до захисту об'єктів. Дані щодо атак на енергетичну інфраструктуру України у 2025–2026 рр. свідчать про необхідність подальшого розвитку систем, здатних забезпечувати не лише реагування на вже виявлену загрозу, а й постійний моніторинг ситуації та координацію доступних ресурсів [3–5].

Важливим напрямом розвитку систем захисту є посилення взаємодії між об'єктами критичної інфраструктури та державною системою протиповітряної оборони. Відповідні організаційні механізми створюють передумови для переходу від ізольованого захисту окремих підприємств до більш узгодженої системи протидії повітряним загрозам [6–8].

Водночас ефективність сучасних технічних засобів значною мірою залежить від якості інформаційного забезпечення. Дані від радарів, камер, безпілотних платформ, наземних сенсорів та інших джерел мають своєчасно надходити до системи управління, узгоджуватися та використовуватися для формування цілісної картини ситуації. У цьому контексті практичний інтерес становить розвиток цифрових систем

 ISSN 2520-6524, e-ISSN 3041-1726

ситуаційної обізнаності, зокрема DELTA, а також досвід використання подібних підходів у міжнародних багатодоменних системах [9–13].

Таким чином, сучасні умови потребують переходу від сукупності окремих технічних засобів до інтегрованої цифрової екосистеми, у якій сенсори, БПЛА, НРК, засоби радіоелектронної боротьби та кіберзахисту функціонують як взаємопов'язані складники єдиного інформаційно-управлінського середовища.

## ПОСТАНОВКА ПРОБЛЕМИ

Одним із головних обмежень сучасних підходів до захисту критичної інфраструктури залишається фрагментарність використання технічних засобів. Радари, відеокамери, системи радіоелектронної боротьби (РЕБ), безпілотні апарати та наземні роботизовані комплекси можуть функціонувати в межах окремих контурів управління. За таких умов інформацію від різних джерел не завжди використовують своєчасно, а ефективність реагування значною мірою залежить від оператора [14].

Характер сучасних загроз, навпаки, потребує скорочення часу між виявленням потенційної небезпеки, її оцінюванням і формуванням рішення щодо реагування. Це особливо актуально для великих технологічно складних об'єктів критичної інфраструктури.

Україна вже має практичний досвід застосування цифрових систем ситуаційної обізнаності, безпілотних платформ і засобів РЕБ. Проте комплексна модель, у якій повітряний, наземний і кібернетичний компоненти функціонують у межах єдиного інформаційно-управлінського контуру, потребує подальшого наукового опрацювання.

**Метою** дослідження є розроблення концептуальної моделі єдиної інноваційної екосистеми БПЛА–НРК для підвищення стійкості критичної інфраструктури України в умовах воєнного стану. Об'єктом дослідження є система забезпечення стійкості критичної інфраструктури України. Предметом дослідження є архітектура та механізми функціонування єдиної екосистеми БПЛА–НРК. У роботі використано методи системного аналізу, структурно-функціонального моделювання, сценарного та порівняльного аналізу, а також оцінювання ефективності запропонованих організаційно-технічних рішень.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання захисту критичної інфраструктури в умовах воєнного стану досліджують як в Україні, так і за кордоном. Значна частина наукових та аналітичних робіт зосереджена на оцінюванні ризиків, фізичному захисті об'єктів, протидії безпілотним системам, застосуванні РЕБ і розвитку цифрових систем управління [1–20].

Окремий напрям становлять дослідження мережево-центричних концепцій. Досвід CJADC2 (американська концепція мережево-центричного командування та управління військами) демонструє тенденцію до інтеграції інформації та ресурсів різних доменів у межах єдиного цифрового середовища [9]. Аналогічні тенденції простежуються в багатодоменних експериментах НАТО, зокрема REPMUS, де значну увагу приділяють взаємодії автономних платформ та обміну інформацією між ними [10; 15]. Український досвід розвитку цифрових систем ситуаційної обізнаності, насамперед DELTA, становить окремий практичний інтерес. Він демонструє можливість використання цифрової платформи як основи для об'єднання інформації від різних джерел і підтримки управлінських рішень [11–13].

Водночас більшість наявних досліджень розглядає окремі компоненти системи захисту. Недостатньо опрацьованим залишається питання комплексної інтеграції сенсорного шару, БПЛА, НРК, засобів РЕБ та кіберзахисту безпосередньо в контексті захисту об'єктів критичної інфраструктури [14; 16].

Отже, наукова проблема полягає не у відсутності окремих технологій, а насамперед у недостатній розробленості підходів до їх системного поєднання в єдиному інформаційно-аналітичному середовищі.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

### *Архітектура цифрової інформаційно-аналітичної екосистеми БПЛА–НРК*

Запропоновану екосистему розглядають як багаторівневу інформаційно-технічну систему, призначену для постійного моніторингу об'єкта критичної інфраструктури, виявлення потенційних загроз, оцінювання ситуації та координації доступних засобів реагування.

Основу архітектури становлять три взаємопов'язані домени:

1) *повітряний домен* — безпілотні літальні апарати різного призначення;

2) *наземний домен* — наземні роботизовані комплекси та інші роботизовані засоби;

3) *кібернетичний домен* — засоби захисту інформаційної інфраструктури, обміну даними та забезпечення кіберстійкості.

Над цими компонентами функціонує центральний інформаційно-управлінський рівень *Mission Control*, концептуально близький до підходів, реалізованих у цифрових системах типу DELTA [11–13; 17]. Важливим складником є

*сенсорний шар*, який забезпечує первинне отримання інформації. До нього можуть належати стаціонарні радари, відеокамери, датчики стану інженерних конструкцій, волоконно-оптичні сенсори та інші засоби моніторингу.

Наступним рівнем є засоби реагування, до яких належать БПЛА, НРК та системи РЕБ. Їхнє використання визначається конкретною ситуацією, характером загрози та встановленими правилами застосування. Центральна цифрова платформа забезпечує збирання й первинне оброблення інформації, її візуалізацію, формування ситуаційної картини та інформаційну підтримку оператора.

Запропонована архітектура передбачає інтеграцію сенсорного шару, повітряного, наземного та кібернетичного доменів у єдиному інформаційно-управлінському середовищі. Центральним елементом системи є цифрова платформа Mission Control, що забезпечує збирання, інтеграцію та візуалізацію інформації від різнорідних джерел, а також інформаційну підтримку прийняття рішень. Структурно-функціональну взаємодію ключових компонентів екосистеми наведено на **рис. 1**.

Відповідно до **рис. 1**, головною особливістю запропонованої моделі є не просто наявність окремих технічних засобів, а їхнє об'єднання в єдиний інформаційний контур. Такий підхід дає змогу забезпечити взаємний обмін інформацією між сенсорним шаром, повітряними та наземними платформами, засобами протидії та кіберзахисту. У результаті формується цілісна ситуаційна картина, яку можна використовувати для оцінювання ситуації та підтримки прийняття рішень оператором.

Інформаційні потоки в запропонованій архітектурі мають бути двонапрямними. З одного боку, сенсори та автономні платформи передають інформацію до центральної системи, а з іншого — після її аналізу оператор або відповідні автоматизовані модулі формують завдання для окремих компонентів. Таким чином, БПЛА та НРК розглядають не як ізольовані технічні одиниці, а як елементи єдиного функціонального середовища.

***Інтеграція інформації та підтримка прийняття рішень***

Ключовою перевагою запропонованої архітектури є можливість об'єднання даних від


**Рис. 1.** Архітектура єдиної інноваційної екосистеми БПЛА–НРК для забезпечення стійкості критичної інфраструктури

**Джерело:** розроблено авторами.

 ISSN 2520-6524, e-ISSN 3041-1726

різних джерел. Інформація з радарів, камер, БПЛА та наземних сенсорів надходить до центральної системи, де здійснюють її узгодження, первинне оброблення та візуалізацію. У загальному вигляді інформаційний цикл можна подати такою послідовністю:

*виявлення → передавання даних → об'єднання інформації → аналіз → оцінювання загрози → формування рішення → реагування → контроль результату.*

Така схема відповідає загальній логіці цифрових систем ситуаційної обізнаності та мережево-центричного управління [9–13].

Застосування алгоритмів штучного інтелекту може бути доцільним на етапах виявлення та класифікації об'єктів, пошуку аномалій, прогнозування розвитку ситуації та формування рекомендацій оператору. Водночас остаточне рішення щодо застосування сил і засобів має залишатися в межах визначеного організаційного та правового контуру.

Отже, цифрова платформа виконує не лише функцію передавання інформації, а й роль *інформаційно-аналітичного інтегратора*, що забезпечує узгоджене функціонування окремих компонентів системи.

***Механізми підвищення стійкості критичної інфраструктури***

Стійкість об'єкта критичної інфраструктури доцільно розглядати як його здатність своєчасно виявляти загрозу, зберігати або швидко відновлювати головні функції після впливу небезпечних чинників та адаптуватися до зміни характеру небезпеки. У запропонованій моделі підвищення стійкості можна забезпечувати поєднанням:

- постійного моніторингу території та технологічних об'єктів;
- раннього виявлення потенційних загроз;
- використання засобів радіоелектронної протидії в межах визначених повноважень;
- застосування безпілотних платформ для спостереження та виконання спеціалізованих завдань;
- використання НРК у ситуаціях, де присутність людини є небажаною або небезпечною;
- резервування каналів зв'язку та інформаційних ресурсів;
- кіберзахисту систем управління та технологічної інфраструктури.

Особливого значення набуває принцип *багаторівневості*. Вихід із ладу одного компонента не має автоматично призводити до припинення функціонування всієї системи. Тому архітектура має передбачати резервні канали зв'язку, дублювання критично важливих сенсорів і можливість роботи окремих елементів у локальному режимі.

***Оцінювання потенційної ефективності***

Для попереднього оцінювання запропонованого підходу можна використовувати методику *"ефективність — вартість"*, що враховує не лише прямі витрати на створення системи, а й потенційне зменшення збитків унаслідок порушення функціонування об'єкта.

Проведене сценарне моделювання дає змогу розглядати можливе зниження вразливості окремих об'єктів на 50–65 % як перспективний орієнтир за умови комплексного застосування запропонованих компонентів. Водночас цей діапазон варто трактувати саме як *результат моделювання*, а не як гарантований показник для всіх типів об'єктів критичної інфраструктури.

Економічне оцінювання також потрібно здійснювати з урахуванням особливостей конкретного об'єкта: його площі, рівня загроз, кількості сенсорів, типів безпілотних платформ, інфраструктури зв'язку та вимог до резервування.

***Порівняння підходів***

Порівняння фрагментарного та інтегрованого підходів до захисту критичної інфраструктури наведено в **табл. 1**.

Наведене порівняння підтверджує, що головна перевага екосистемного підходу полягає не в окремій перевазі певного типу БПЛА чи НРК, а в *системній взаємодії компонентів та інтеграції інформації*.

***Підготовка операторів і населення***

Окремим складником екосистеми має стати система підготовки персоналу. Навіть технологічно досконала система не забезпечить необхідного рівня стійкості без підготовлених операторів, здатних правильно інтерпретувати інформацію та діяти відповідно до визначених процедур.

Для операторів критичної інфраструктури доцільно передбачити використання симуляторів, цифрових двійників об'єктів і сценарного навчання, що надає можливість відпрацьовувати дії в умовах, наближених до реальних без створення додаткових ризиків для персоналу та обладнання.

Підготовка населення має бути зорієнтована насамперед на правильну поведінку під час повітряних загроз, дотримання сигналів оповіщення, евакуаційних процедур і правил взаємодії з екстреними службами.

Таким чином, людський фактор доцільно розглядати не лише як потенційне джерело помилок, а як важливий складник цифрової системи, який потребує належної інформаційної та організаційної підтримки.

*Таблиця 1*

**Порівняння фрагментарного та інтегрованого підходів до захисту критичної інфраструктури**

| Параметр | Фрагментарний підхід | Запропонована екосистема БПЛА–НРК |
|---|---|---|
| Організація системи | Окремі засоби та контури управління | Єдиний інформаційно-управлінський контур |
| Обмін інформацією | Переважно між окремими системами | Інтегрований обмін даними |
| Моніторинг | Локальний | Багаторівневий |
| Використання БПЛА | Виконання окремих завдань | Частина єдиної системи |
| Використання НРК | Автономні або спеціалізовані завдання | Координоване застосування |
| РЕБ | Окремий компонент | Інтегрований компонент системи захисту |
| Кіберзахист | Переважно окремий контур | Вбудований у загальну архітектуру |
| Підтримка прийняття рішень | Значна залежність від оператора | Аналітична підтримка оператора |
| Масштабування | Обмежене | Модульне |

**Джерело:** розроблено авторами.

***Правове та організаційне забезпечення***

Практичне впровадження екосистеми БПЛА–НРК потребує відповідного нормативного та організаційного забезпечення. Насамперед необхідно визначити порядок взаємодії операторів критичної інфраструктури з державними органами та військовим командуванням, процедури обміну інформацією, вимоги до захисту даних і відповідальність учасників системи [8; 18–20].

Перспективним напрямом є подальше нормативне врегулювання використання безпілотних систем поблизу об'єктів критичної інфраструктури, зокрема з питань організації повітряного простору та потенційного застосування принципів U-Space. Водночас інтеграція підприємств критичної інфраструктури до відповідних державних систем має здійснюватися з урахуванням розмежування повноважень, вимог кібербезпеки та режиму доступу до інформації.

Отже, технічна інтеграція без відповідної організаційної та правової інтеграції не забезпечить повноцінного функціонування екосистеми.

## ВИСНОВКИ

Проведене дослідження дає підстави розглядати створення єдиної інноваційної екосистеми БПЛА–НРК як перспективний напрям підвищення стійкості критичної інфраструктури України в умовах воєнного стану.

На відміну від підходу, за якого БПЛА, НРК, сенсори, засоби РЕБ і кіберзахист розглядають як окремі компоненти, запропонована модель передбачає їхнє функціональне об'єднання в єдиний *інформаційно-управлінський контур*. Його центральним елементом є цифрова платформа Mission Control, що забезпечує інтеграцію інформації, формування ситуаційної картини та підтримку прийняття рішень.

Таким чином, у результаті дослідження:

1) проаналізовано сучасні загрози для критичної інфраструктури, пов'язані, зокрема з широким застосуванням безпілотних систем і комбінованими способами впливу на об'єкти;

2) запропоновано структурно-функціональну архітектуру єдиної екосистеми БПЛА–НРК, що охоплює сенсорний шар, повітряний, наземний і кібернетичний домени, засоби РЕБ і центральну цифрову платформу Mission Control;

3) обґрунтовано доцільність переходу від окремого застосування технічних засобів до інтегрованого інформаційного середовища, у якому дані від різних джерел можна використовувати для формування єдиної ситуаційної картини;

4) запропоновано багаторівневий підхід до підвищення стійкості критичної інфраструктури, що передбачає поєднання моніторингу, раннього виявлення загроз, технічних засобів протидії, роботизованих систем, резервування та кіберзахисту;

5) показано, що потенційний ефект від упровадження запропонованої моделі доцільно оцінювати не лише за кількістю виявлених або

нейтралізованих загроз, а й за показниками безперервності функціонування об'єкта, часу реагування, вартості відновлення та здатності системи працювати в умовах часткової відмови її компонентів.

Подальші дослідження доцільно спрямувати на розроблення математичних моделей оцінювання стійкості екосистеми, визначення критеріїв оптимального розподілу ресурсів, дослідження безпечної взаємодії автономних платформ, удосконалення алгоритмів підтримки прийняття рішень та нормативне забезпечення інтеграції безпілотних систем у загальну архітектуру захисту критичної інфраструктури.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Споришев К. О. Функціонування та захист об'єктів критичної інфраструктури в умовах воєнного стану. *Наукові інтереси України*. 2026. № 2 (19). С. 531–539. DOI: https://doi.org/10.52058/3041-1793-2026-2(19)-531-539.
2. Залож В. В., Торічний В. О., Глуздань О. П. Аналіз ризиків у сфері захисту критичної інфраструктури Державної прикордонної служби України в умовах воєнного стану. *Національні інтереси України*. 2025. № 8 (13). С. 130–141. DOI: https://doi.org/10.52058/3041-1793-2025-8(13)-130-141.
3. Attacks against Ukraine's energy infrastructure and update on the human rights situation in Ukraine, 1 December 2025 — 31 May 2026. *United Nations.* 2026. URL: https://ukraine.un.org/en/318327-attacks-against-ukraine%E2%80%99s-energy-infrastructure-and-update-human-rights-situation-ukraine-1.
4. Russian drones swarm smaller Ukrainian power stations, data shows. *Reuters.* 2026. URL: https://www.reuters.com/business/aerospace-defense/russian-drones-swarm-smaller-ukrainian-power-stations-data-shows-2026-05-08/.
5. Ukraine — Fifth Rapid Damage and Needs Assessment (RDNA5): February 2022 — December 2025. Washington, DC: *World Bank Group*. 2026. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099022026094036395?utm_source=chatgpt.com.
6. 30 Ukrainian companies cleared to form private air defense units. *Kyiv Post*. Official website. 2026. URL: https://www.kyivpost.com/post/77770.
7. Воєнна критична інфраструктура отримує "свою" ППО, але не поза державою, а всередині її контуру. *Вчасно.* 2026. URL: https://vchasno.org.ua/ukraine/krytychna-infrastruktura-otrymuie-svoiu-ppo-ale-ne-poza-derzhavoiu-a-vseredyni-ii-konturu/.
8. Thirty companies have already joined the private air defence initiative. *Ministry of Defence of Ukraine*. 2026. URL: https://mod.gov.ua/en/news/thirty-companies-have-already-joined-the-private-air-defense-initiative.
9. Does Ukraine already have functional CJADC2 technology? *Center for Strategic & International Studies.* 2026. URL: https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.
10. NATO demonstrates new technologies at REPMUS/Dynamic Messenger 2025. *NATO.* 2025. URL: https://www.nato.int/en/multimedia/multimedia/videos/2025/09/25/nato-demonstrates-new-technologies-at-repmus-dynamic-messenger-2?utm_source=chatgpt.com.
11. Система DELTA ЗСУ фіксує щодня понад 6600 уражених цілей. *Міністерство оборони України.* 2026. URL: https://mod.gov.ua/news/u-boiovii-systemi-delta-shchodnia-fiksuietsia-ponad-6-600-urazhenykh-vorozhykh-tsilei.
12. UKR: How 'Mission Control' software centralizes drone warfare. *Arsenal.* 2026. URL: https://www.arsenal.eu/p/ukr-how-mission-control-software-centralizes-drone-warfare.
13. Ukrainian DELTA technology becomes core command platform in NATO exercises. *Ukrainska Pravda.* 2025. URL: https://www.pravda.com.ua/eng/news/2025/10/03/8001085/.
14. Shmyhal says first critical infrastructure sites already have EW systems. *Ukrinform.* 2025. URL: https://www.ukrinform.net/rubric-economy/4074709-shmyhal-says-first-critical-infrastructure-sites-already-have-ew-systems.html.
15. Ukraine to arm energy companies to shoot down Russian missiles. *Euromaidan Press.* 2025. URL: https://euromaidanpress.com/2025/11/20/ukraine-to-arm-energy-companies/.
16. When the drone war reaches the reactor fence: Ukraine and the cyber-physical front. *Complex Discovery.* 2026. URL: https://complexdiscovery.com/when-the-drone-war-reaches-the-reactor-fence-ukraine-and-the-cyber-physical-front/.
17. Понад 6,6 тисячі уражених цілей щодня: у DELTA показали масштаби роботи українських дронів. *АрміяInform.* 2026. URL: https://armyinform.com.ua/2026/07/31/ponad-66-tysyachi-urazhenyh-czilej-shhodnya-u-delta-pokazaly-masshtaby-roboty-ukrayinskyh-droniv/.
18. Журба Н. Правове регулювання БПЛА цивільного призначення у контексті захисту та стійкості критичної інфраструктури. *Пропілеї права та безпеки*. 2025. № 8, С. 211–213. DOI: https://doi.org/10.32620/pls.2025.8.53.
19. Критичне зволікання: скалічені робітники чекають на справедливість. *Дзеркало тижня. ZN.ua.* 2026. URL: https://zn.ua/ukr/LAW/kritichne-zvolikannja-skalicheni-robitniki-chekajut-na-spravedlivist.html.
20. Про реалізацію експериментального проекту щодо нового будівництва, реконструкції, капітального ремонту, ремонту та інших інженерно-технічних заходів із захисту об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури: Постанова Кабінету міністрів України від 07 лют. 2025 р. № 142. URL: https://zakon.rada.gov.ua/laws/show/142-2025-%D0%BF#Text.


## REFERENCES


1. Sporyshev, K. O. (2026). Funktsionuvannia ta zakhyst obiektiv krytychnoi infrastruktury v umovakh voiennoho stanu [Functioning and protection of critical infrastructure facilities under martial law]. *Naukovi interesy Ukrainy* [Scientific Interests of Ukraine], *2* (19), 531-539. DOI: https://doi.org/10.52058/3041-1793-2026-2(19)-531-539 [in Ukr.].
2. Zalozh, V. V., Torichnyi, V. O., & Hluzdan, O. P. (2025). Analiz ryzykiv u sferi zakhystu krytychnoi infrastruktury Derzhavnoi prykordonnoi sluzhby Ukrainy v umovakh voiennoho stanu [Risk analysis in the field of protection of critical infrastructure of the State Border Service of Ukraine under martial law]. *Natsionalni interesy Ukrainy* [National interests of

Ukraine], *8* (13), 130-141. DOI: https://doi.org/10.52058/3041-1793-2025-8(13)-130-141 [in Ukr.].
3. (2026). Attacks against Ukraine's energy infrastructure and update on the human rights situation in Ukraine, 1 December 2025 — 31 May 2026. *UN.* Retrieved from: https://ukraine.un.org/en/318327-attacks-against-ukraine%E2%80%99s-energy-infrastructure-and-update-human-rights-situation-ukraine-1.
4. (2026). Russian drones swarm smaller Ukrainian power stations, data shows. *Reuters.* Retrieved from: https://www.reuters.com/business/aerospace-defense/russian-drones-swarm-smaller-ukrainian-power-stations-data-shows-2026-05-08/.
5. (2026). Ukraine — Fifth Rapid Damage and Needs Assessment (RDNA5): February 2022 — December 2025. *World Bank.* Washington, DC: World Bank Group. Retrieved from: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099022026094036395?utm_source=chatgpt.com.
6. (2026). 30 Ukrainian companies cleared to form private air defense units. *Kyiv Post.* Retrieved from: https://www.kyivpost.com/post/77770.
7. (2026). Voienna krytychna infrastruktura otrymuie "svoiu" PPO, ale ne poza derzhavoiu, a vseredyni yii konturu [Military critical infrastructure receives "its" air defense, but not outside the state, but within its contour]. *Vchasno* [In a timely manner]. Retrieved from: https://vchasno.org.ua/ukraine/krytychna-infrastruktura-otrymuie-svoiu-ppo-ale-ne-poza-derzhavoiu-a-vseredyni-ii-konturu/.
8. (2026). Thirty companies have already joined the private air defence initiative. *Ministry of Defence of Ukraine.* Retrieved from: https://mod.gov.ua/en/news/thirty-companies-have-already-joined-the-private-air-defense-initiative.
9. (2024). Does Ukraine already have functional CJADC2 technology? *Center for Strategic & International Studies.* Retrieved from: https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.
10. (2025). NATO demonstrates new technologies at REPMUS/Dynamic Messenger 2025. *NATO.* Retrieved from: https://www.nato.int/en/multimedia/multimedia/videos/2025/09/25/nato-demonstrates-new-technologies-at-repmus-dynamic-messenger-2?utm_source=chatgpt.com/
11. (2026). Systema DELTA ZSU fiksuie shchodnia ponad 6600 urazhenykh tsilei [The AFU DELTA system records over 6,600 hit targets daily]. *Ministerstvo oborony Ukrainy* [Ministry of Defence of Ukraine]. Retrieved from: https://mod.gov.ua/news/u-boiovii-systemi-delta-shchodnia-fiksuietsia-ponad-6-600-urazhenykh-vorozhykh-tsilei.
12. (2026). UKR: How 'Mission Control' software centralizes drone warfare. *Arsenal.* Retrieved from: https://www.arsenal.eu/p/ukr-how-mission-control-software-centralizes-drone-warfare.
13. (2025). Ukrainian DELTA technology becomes core command platform in NATO exercises. *Ukrainska Pravda.* Retrieved from: https://www.pravda.com.ua/eng/news/2025/10/03/8001085/.
14. (2025). Shmyhal says first critical infrastructure sites already have EW systems. *Ukrinform.* Retrieved from: https://www.ukrinform.net/rubric-economy/4074709-shmyhal-says-first-critical-infrastructure-sites-already-have-ew-systems.html.
15. (2025). Ukraine to arm energy companies to shoot down Russian missiles. *Euromaidan Press.* Retrieved from: https://euromaidanpress.com/2025/11/20/ukraine-to-arm-energy-companies/.
16. (2026). When the drone war reaches the reactor fence: Ukraine and the cyber-physical front. *Complex Discovery.* Retrieved from: https://complexdiscovery.com/when-the-drone-war-reaches-the-reactor-fence-ukraine-and-the-cyber-physical-front/.
17. (2026). Ponad 6,6 tysiachi urazhenykh tsilei shchodnia: u DELTA pokazaly masshtaby roboty ukrainskykh droniv [Over 6.6 thousand targets hit daily: DELTA showed the scale of the work of Ukrainian drones]. *ArmiiaInform* [ArmyInform]. Retrieved from: https://armyinform.com.ua/2026/07/31/ponad-66-tysyachi-urazhenyh-czilej-shhodnya-u-delta-pokazaly-masshtaby-roboty-ukrayinskyh-droniv/ [in Ukr.].
18. Zhurba, N. (2025). Pravove rehuliuvannia BPLA tsyvilnoho pryznachennia u konteksti zakhystu ta stiikosti krytychnoi infrastruktury [Legal regulation of civil UAVs in the context of protection and resilience of critical infrastructure]. *Propilei prava ta bezpeky* [Propylaea of law and security], *8*, 211-213. DOI: https://doi.org/10.32620/pls.2025.8.53 [in Ukr.].
19. (2026). Krytychne zvolikannia: skalicheni robitnyky chekaiut na spravedlyvist [Critical delay: Crippled workers wait for justice]. *ZN.ua.* Retrieved from: https://zn.ua/ukr/LAW/kritichne-zvolikannja-skalicheni-robitniki-chekajut-na-spravedlivist.html [in Ukr.].
20. (2025). Pro realizatsiiu eksperymentalnoho proektu shchodo novoho budivnytstva, rekonstruktsii, kapitalnoho remontu, remontu ta inshykh inzhenerno-tekhnichnykh zakhodiv iz zakhystu obiektiv krytychnoi infrastruktury palyvno-enerhetychnoho sektoru krytychnoi infrastruktury: Postanova Kabinetu ministriv Ukrainy vid 07.02.2025 № 142 [On the implementation of a pilot project on new construction, reconstruction, overhaul, repair and other engineering and technical measures to protect critical infrastructure facilities of the fuel and energy sector of critical infrastructure: Resolution of the Cabinet of Ministers of Ukraine dated 07.02.2025 No. 142]. Retrieved from: https://zakon.rada.gov.ua/laws/show/142-2025-%D0%BF#Text [in Ukr.].

*Під час підготовки цієї статті автори використовували інструменти ШІ ChatGPT для пошуку і аналізу інформаційних джерел за визначеною тематикою, створення рисунку за докладним описом і часткового покращання стилю роботи. Усі результати були перевірені, відредаговані та затверджені авторами.*

**M. V. ISHCHUK,** Director of the Department of Resource Provision
**V. L. SYDORENKO,** D. Sc. in Engineering, Professor
**O. H. DOTSENKO,** PhD, Senior Researcher
**S. Yu. OHURTSOV,** PhD in Engineering, Senior Researcher

## DEVELOPMENT OF A UNIFIED INNOVATIVE UAV–UGRS ECOSYSTEM FOR ENHANCING THE RESILIENCE OF CRITICAL INFRASTRUCTURE UNDER MARTIAL LAW

***Abstract.*** *The article examines the possibility of developing a unified innovative ecosystem of unmanned aerial vehicles and unmanned ground robotic systems (UAV–UGRS) as a promising approach to enhancing the resilience of Ukraine's critical infrastructure under martial law. The relevance of this approach is driven by the increasing use of unmanned systems against energy, transport, and water supply facilities, which requires timely threat detection and rapid response. The object of the study is the resilience assurance system of Ukraine's critical infrastructure, while the subject is the architecture and functional mechanisms of a unified UAV–UGRS ecosystem. The methodological framework includes systems and comparative analysis, structural-functional modelling, scenario analysis, and assessment of the effectiveness of organizational and technical solutions. The proposed model provides for the integration of sensors, electronic warfare systems, UAVs, unmanned ground robotic systems, and cybersecurity capabilities through a central digital platform, Mission Control. This architecture forms a unified information environment in which data from heterogeneous sources can be used to develop a situational picture and support decision-making. The study also considers the interaction between local protection capabilities at critical infrastructure facilities and the national air defence system, as well as the training of operators and personnel using digital training tools. The practical significance of the results lies in the potential application of the proposed model in the development and modernization of protection systems for energy, transport, and water infrastructure facilities, as well as in improving organizational and legal mechanisms for the use of unmanned and robotic systems.*

***Keywords:*** *unified UAV–UGRS ecosystem, critical infrastructure, digital platform, information-analytical system, resilience, unmanned systems, unmanned ground robotic systems, electronic warfare, Mission Control, DELTA, cybersecurity.*

**ІНФОРМАЦІЯ ПРО АВТОРІВ**

**Іщук Максим Валерійович** — директор Департаменту ресурсного забезпечення, Державна служба України з надзвичайних ситуацій; вул. О. Гончара, 55, м. Київ, 01601; ishchuk_maksym@nuczu.edu.ua; ORCID: 0009-0004-0170-1201

**Сидоренко Володимир Леонідович** — д-р техн. наук, проф., пров. н. с., Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України; вул. Вишгородська, 21, м. Київ, Україна, 04074; sydorenko_volodymyr@nuczu.edu.ua; ORCID: 0000-0002-4584-486X (автор для листування)

**Доценко Олександр Григорович** — д-р філософії, ст. дослідн., начальник відділу, Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України; вул. Вишгородська, 21, м. Київ, Україна, 04074; dotsenko_oleksandr@nuczu.edu.ua; ORCID: 0000-0001-7437-8733

**Огурцов Сергій Юрійович** — канд. техн. наук, с. н. с., заступник начальника інституту, Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України; вул. Вишгородська, 21, м. Київ, Україна, 04074; ohurtsov_serhii@nuczu.edu.ua; ORCID: 0000-0003-3224-9436

**INFORMATION ABOUT THE AUTHORS**

**Ishchuk M. V.** — Director of the Department of Resource Provision, State Emergency Service of Ukraine; 55, O. Honchara Str., Kyiv, Ukraine, 01601; ishchuk_maksym@nuczu.edu.ua; ORCID: 0009-0004-0170-1201

**Sydorenko V. L.** — D. Sc. in Engineering, Professor, Leading Researcher, Institute of Scientific Research on Civil Protection of the National University of Civil Protection of Ukraine; 21, Vyshhorodska Str., Kyiv, Ukraine, 04074; sydorenko_volodymyr@nuczu.edu.ua; ORCID: 0000-0002-4584-486X (correspondence author)

**Dotsenko O. H.** — PhD, Senior Researcher, Department Head, Institute of Scientific Research on Civil Protection of the National University of Civil Protection of Ukraine, 21, Vyshhorodska Str., Kyiv, Ukraine, 04074; dotsenko_oleksandr@nuczu.edu.ua; ORCID: 0000-0001-7437-8733

**Ohurtsov S. Yu.** — PhD in Engineering, Senior Researcher, Deputy Director of the Institute, Institute of Scientific Research on Civil Protection of the National University of Civil Protection of Ukraine, 21, Vyshhorodska Str., Kyiv, Ukraine, 04074; Ukraine; ohurtsov_serhii@nuczu.edu.ua; ORCID: 0000-0003-3224-9436



*Надійшла до редакції 03.09.2026*
*Прийнята до друку 11.09.2026*
*Опубліковано 30.09.2026*