СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ»

ІНСТИТУТ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНОГО ЮРИДИЧНОГО
УНІВЕРСИТЕТУ ІМЕНІ ЯРОСЛАВА МУДРОГО

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Матеріали V Всеукраїнської науково-практичної конференції

(м. Харків, 23 квітня 2026 року)

Випуск № 5

м. Харків 2026 р.

УДК 351.74-057.36
А 43

Рекомендовано до видання Вченою радою
Інституту СБУ Національного юридичного університету імені Ярослава Мудрого
(протокол № 50 від «01» червня 2026 року)

Редакційна колегія вважає за доцільне повідомити, що не всі положення і висновки окремих авторів є безперечними. Разом з тим, їх публікація здійснюється з метою забезпечення плюралізму наукової думки і публічного обговорення.

Матеріали друкуються мовою оригіналу. За виклад, зміст і достовірність матеріалів, а також використання наукових джерел без відповідного посилання відповідають автори.

Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони: матеріали V Всеукраїнської науково-практичної конференції, м.Харків, 23 квітня 2026 року. м. Харків: 2026. 517 с.

У збірнику представлено матеріали V Всеукраїнської науково-практичної конференції, присвяченій обговоренню та вирішенню низки проблемних питань, забезпечення службово-бойової діяльності сил сектору безпеки і оборони України. Зокрема тези доповідей та виступів стосувались впровадження досвіду та стандартів армій країн-членів НАТО, удосконаленню рівня тактичної, вогневої, спеціальної фізичної та медико-тактичної підготовки у процесі підготовки персоналу для сектору безпеки і оборони України; міжвідомчої взаємодії у діяльності сил сектору безпеки і оборони та посилення комунікаційних зв’язків; удосконалення системи безпеки та захисту для об'єктів критичної інфраструктури України; забезпечення психологічної підтримки та гендерної рівності у діяльності сил сектору безпеки і оборони України під час виконання оперативно-службових та/або службово-бойових завдань

Видання адресоване представникам сектору безпеки і оборони України, вченим, науковим та науково-педагогічним працівникам, здобувачам освіти, а також іншим особам, до предмету зацікавленості яких відносяться порушені теми.

СЕКЦІЯ 3
УДОСКОНАЛЕННЯ СИСТЕМИ БЕЗПЕКИ ТА ЗАХИСТУ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

СЕКЦІЯ 4
ЗАБЕЗПЕЧЕННЯ ПСИХОЛОГІЧНОЇ ПІДТРИМКИ ТА ГЕНДЕРНОЇ РІВНОСТІ У ДІЯЛЬНОСТІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ ПІД ЧАС ВИКОНАННЯ ОПЕРАТИВНО-СЛУЖБОВИХ ТА/АБО СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ

Рамка управління ризиками: багаторівнева авторизація, кібер- і РЕБ-підготовка, незмінні логи, навчання і сертифікація персоналу.

Висновки:

Інтеграція АБСДК і розгляд концепту АДРК-СР відкривають значні стратегічні можливості для підвищення оборонної ефективності України. Однак ці технології повинні впроваджуватися в рамках чіткої політичної санкції, законодавчої і юридичної підоснови, кібер- та РЕБ-стійкої архітектури, прозорих процедур аудиту й навчання персоналу. Український мілітарний кіберпанк — це доктрина перемоги, що поєднує техніку, кадри й культуру у єдину систему оборони та стратегічної автономії України.

Список використаних джерел:

1. Клепар І.І., Самарай В.П., Череп'ян Ю.І. "Автономні бойові системи дистанційного керування». Збірка доповідей до Київ: Національний Університет оборони України, 2025.
2.Амосов М.М. Алгоритмы разума. Київ: Наукова думка, 1979.
3.Амосов М.М. Человек и машина. Київ: Здоров'я, 1983.
4.Глушков В.М. Введение в кибернетику. Київ: Наукова думка, 1964.
5. Глушков В.М. Основы автоматизированных систем управления. Москва: Наука, 1972.
6.Женевські конвенції 1949 року та Додаткові протоколи 1977 року. Міжнародне гуманітарне право. Женева, 1949–1977.
7. NATO Standardization Office. Autonomous Systems in Defence: Policy and Risk Management Framework. Brussels: NATO, 2024.
8. OECD. Artificial Intelligence in Defence Applications: Ethical and Legal Considerations. Paris: OECD, 2023.
9. Український інститут майбутнього. Кібербезпека та оборонні технології: стратегічні виклики для України. Київ: УІМ, 2024.
10. World Economic Forum. Future of Autonomous Weapons Systems. Geneva: WEF, 2023.

Середа Д.В.
Старший науковий співробітник науково-дослідного сектору досліджень та статистики пожеж науково-дослідного центру нормативно-технічного регулювання ІНДЦЗ Національного університету цивільного захисту України
Коваль Р.Р.
Начальник науково-дослідного сектору досліджень та статистики пожеж науково-дослідного центру нормативно-технічного регулювання ІНДЦЗ Національного університету цивільного захисту України,
доктор філософії
Несенюк Л.П.
Науковий співробітник науково-дослідного сектору досліджень та статистики пожеж науково-дослідного центру нормативно-технічного регулювання ІНДЦЗ Національного університету цивільного захисту України

ПРОГНОЗУВАННЯ РИЗИКІВ ТА ЗАБЕЗПЕЧЕННЯ ПРОТИПОЖЕЖНОГО ЗАХИСТУ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення стійкості та безпеки об'єктів критичної інфраструктури (далі - ОКІ) є

фундаментальною передумовою стабільності національної економіки, соціального добробуту та обороноздатності держави, особливо в умовах тривалої воєнної агресії [1]. Критична інфраструктура охоплює широкий спектр систем, від енергетичного сектору, включаючи атомні, гідро- та вітрові електростанції, до транспортних мереж, систем охорони здоров'я та інформаційно-комунікаційних технологій. Функціональна цілісність цих об'єктів безпосередньо впливає на здатність держави щодо життєзабезпечення населення, що робить їх першочерговими цілями для різного роду загроз, включаючи техногенні катастрофи, пожежі та військові удари [2]. Сучасний етап розвитку систем цивільного захисту вимагає переходу від реагування на надзвичайні ситуації до превентивних заходів щодо управління ризиками, що базується на глибокому аналізі вразливостей та впровадженні науково обґрунтованих методик оцінки стану захищеності. Актуальність дослідження зумовлена необхідністю уніфікації підходів до оцінювання безпеки сучасних та інтеграції прогнозування ризиків у загальну систему цивільного захисту від надзвичайної ситуації воєнного характеру [3]. Метою даної роботи є обґрунтування процедури та розробка критеріїв для комплексного оцінювання стану захищеності ОКІ, що дозволить мінімізувати наслідки надзвичайних ситуацій та підвищити загальну стійкість держави. Також, важливим аспектом є врахування міжнародних стандартів та програм, таких як PPRD East 3, що дозволяють інтегрувати вітчизняну систему цивільного захисту у європейський безпековий простір [4, 5].

Аналітичний огляд нормативно-правової бази України базується на системному аналізі, зокрема, згідно документу [3], який визначає порядок віднесення об'єктів до критичної інфраструктури та їх категоризацію за чотирма рівнями критичності: від об'єктів державного значення до локальних установ. Важливим елементом правового регулювання є розробка паспортів безпеки та планів захисту, які стають обов'язковими для операторів ОКІ відповідно до наказів ДСНС України, спрямованих на протидію загрозам національного рівня, таким як пожежі та вибухи [6, 7]. В умовах повномасштабного вторгнення рф значна частина інфраструктури зазнала критичних руйнувань, що вимагає використання даних Реєстру пошкодженого та знищеного майна для точного прогнозування необхідних ресурсів для відновлення та захисту [8]. Це зумовлює необхідність створення гнучкої системи оцінювання, яка могла б адаптуватися до динамічних умов ведення бойових дій та нових типів озброєння, що застосовуються проти інфраструктурних об'єктів.

Методологічна основа оцінювання стану захищеності ОКІ передбачає ідентифікацію критичних елементів та аналіз потенційних ризиків, що охоплюють природні та антропогенні впливи [2]. Однією з найбільш ефективних систем аналізу вразливостей є методологія CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability), яка дозволяє проводити якісну та кількісну оцінку ймовірності атак ворога на ОКІ [9]. Ця методика дозволяє оцінити об'єкт за шістьма основними параметрами: критичність (вплив на систему при виведенні з ладу), доступність (ступінь проникності), відновлюваність (час на ремонт), вразливість (стійкість до зовнішніх впливів), ефект (політичні або економічні наслідки) та розпізнаваність (ступінь ідентифікованості цілі). Застосування цієї системи у сфері цивільного захисту дає змогу фахівцям ДСНС та адміністраціям об'єктів раціонально розподіляти обмежені ресурси для зміцнення найбільш вразливих ділянок.

Оцінювання стану захищеності об’єкта критичної інфраструктури визначається у відсотковому еквіваленті за показниками критичності та вразливості.

Відносний загальний показник стану захищеності ОКІ (SO, %) визначаємо за формулою (1):

$$SO = G \, x \, 100 \, / \, FS, \, \% \qquad (1)$$

де, G - проміжна оцінка стану захищеності. Визначається як сума балів за результатом оцінювання кількості виявлених недоліків.

FS - коефіцієнт стану безпеки ОКІ. Приймається залежно від всієї кількості наявних критеріїв стану безпеки за показниками пожежна, техногенна безпека та цивільний захисту [10].

Розроблений алгоритм оцінювання базується на перевірці виконання нормативних вимог та індивідуальних концепцій протипожежного захисту [6]. У разі виявлення невідповідностей складаються протоколи, де фіксується рівень виконання кожного заходу. Загальна оцінка стану захищеності диференціюється залежно від відсотка невиконаних показників: якщо порушення становлять менше 10% за будь-яким із критеріїв, об'єкту присвоюється статус «Обмежено забезпечує», а при перевищенні цього порогу - «Не забезпечує». Важливо підкреслити, що відсутність на об'єкті передбаченої захисної споруди автоматично призводить до незадовільної оцінки за критерієм цивільного захисту. Система оцінювання також включає перевірку стану джерел протипожежного водопостачання, працездатності систем автоматичної пожежної сигналізації та пожежогасіння, а також укомплектованості персоналу засобами індивідуального захисту.

Комплексний підхід до безпеки ОКІ також включає концепцію «Країна-фортеця», яка передбачає посилення інженерного захисту від повітряних атак та диверсій. Це вимагає тісної співпраці між науковими установами, державними органами та операторами критичної інфраструктури для постійного оновлення моделей прогнозування ризиків у відповідь на появу нових типів загроз. Використання міжнародного досвіду, зокрема програм PPRD East 3 та рекомендацій UNDRR, сприяє впровадженню стандартів щодо раннього запобігання та покращенню готовності до каскадних ризиків, коли одна аварія провокує серію наступних загроз [4, 12]. Оцінювання повинно бути циклічним процесом, що включає етапи планування, реалізації захисних заходів, аудиту результатів та корекції стратегії безпеки.

Важливим компонентом є також цифровізація процесів моніторингу безпеки. Створення цифрових двійників ОКІ дозволяє моделювати різні сценарії аварій, включаючи пожежі, вибухи та обвалення конструкцій, без ризику для реального об'єкта. Це дає змогу оптимізувати плани евакуації персоналу та маршрути висування підрозділів ДСНС. Окрім того, впровадження автоматизованих систем раннього виявлення загроз (наприклад, датчиків вібрації, тепловізійних камер тощо) дозволяє значно скоротити час реагування, що є важливим фактором для мінімізації збитків на енергетичних та промислових об'єктах. Наукова новизна дослідження полягає у розробці комплексних показників, що поєднують технічні параметри надійності обладнання з організаційними аспектами цивільного захисту.

Результатом проведеного дослідження є наукове обґрунтування комплексної методики оцінки стану захищеності ОКІ, яка вперше в Україні інтегрує загрози воєнного характеру з традиційними критеріями пожежної та техногенної безпеки. Розроблений алгоритм оцінювання забезпечує прозорий та уніфікований інструментарій для підрозділів ДСНС та органів місцевого самоврядування, що дозволяє здійснювати регулярний моніторинг стійкості ОКІ та оперативно реагувати на зміни безпекового середовища. Практична реалізація запропонованих підходів сприятиме мінімізації людських та матеріальних втрат у разі виникнення надзвичайних ситуацій, а також прискорить відновлення життєво важливих функцій держави у післякризовий період. Подальші дослідження мають бути спрямовані на вдосконалення математичних моделей оцінки вразливостей, адаптацію коефіцієнтів безпеки до нових технологічних процесів у секторі критичної інфраструктури.

Список використаних джерел

1. Про Стратегію національної безпеки України: Указ Президента України від 26 травня 2015 р. № 287/2015. *Офіційний вісник України.* 2015. № 43, Ст. 14.
2. Чумаченко С. М., Троцько В. В. (2017) Оцінювання загроз об'єктам критичної інфраструктури. Науковий вісник: цивільний захист та пожежна безпека. № 1. С. 41-47.
3. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. Офіційний вісник України. 2020 № 93, Ст. 9.

4. Prevention, Preparedness and Response to Natural and Man-made Disasters in Eastern Partnership Countries (PPRD East 3). - Режим доступу : www. URL: https://www.pprdeast3.eu/.
5. PPRD East 3: New Phase for Programme on Resilience to Disasters // Civil Protection Knowledge Network – [Електронний ресурс]. - Режим доступу : www. URL: https://civil-protection-knowledge-network.europa.eu/projects-exercises/pprd-east-3/.
6. План захисту із забезпечення цивільного захисту, пожежної та техногенної безпеки на об’єктах критичної інфраструктури та протидії проєктній загрозі національного рівня «Пожежі та вибухи»: Наказ ДСНС від 08.12.2023 № 986.
7. Деякі питання паспортизації об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 4 серпня 2023 р. № 818. Офіційний вісник України. 2023. №77. Ст. 112.
8. Загальна сума збитків, завдана інфраструктурі України через війну, станом на січень 2024 року [Електронний ресурс] / Kyiv school of economics. - Режим доступу : www. URL: https://kse.ua/ua/about-the-school/news/zagalna-suma-zbitkiv-zavdana-infrastrukturi-ukrayini-zrosla-do-mayzhe-155-mlrd-otsinka-kse-institute-stanom-na-sichen-2024-roku/
9. Labaj, L. (2011). The CARVER Methodology: The Evolution of the CIA’s Offensive Targeting Methodology into the Security Industry’s Definitive Vulnerability Assessment Tool. Journal of Counterterrorism & Homeland Security International, – 17(4).
10. Цивільний захист в умовах війни: колективна монографія / за загальною редакцією Дмитра Бондаря. Львів: ЛДУБЖД, 2025. 524 с
11. Hazard Definition & Review of Classification. Technical Report // United Nations Office for Disaster Risk Reduction (UNDRR) and International Science Council (ISC) – [Технічний звіт]. 2021. – 123 с.

Скиданенко В.В.
науковий співробітник науково-дослідного відділу територіальної оборони Наукового центру Сухопутних військ
Касаткін Є.В.
начальник науково-дослідного відділу територіальної оборони Наукового центру Сухопутних військ
Беззубцева Т.Г.
старший науковий співробітник науково-дослідного відділу територіальної оборони Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

ЩОДО ЗАКОНОДАВЧИХ КОЛІЗІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Відповідно до положень Закону України «Про критичну інфраструктуру» [1], її захист є складовою частиною забезпечення національної безпеки України. Цей захист організується та здійснюється як в мирний час так і в умовах кризових ситуацій. Особливості захисту об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, правового режиму надзвичайного та воєнного стану, особливого періоду регулюються законами України «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період» та «Про оборону України», а також окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об’єктів критичної інфраструктури [2–5]. Крім того, діяльність у сфері захисту об’єктів критичної інфраструктури регламентується також іншою нормативно-