

Л. Я. Мунтян,
к. т. н., доцент, доцент кафедри морфології та громадського здоров'я,
ЧНУ імені Петра Могили
ORCID ID: <https://orcid.org/0000-0001-8456-4564>

DOI: 10.32702/2306-6814.2025.20.276

УПРАВЛІННЯ РИЗИКАМИ БЕЗПЕКИ КОМУНАЛЬНИХ СЛУЖБ ПІД ЧАС БОЙОВИХ ДІЙ

L. Muntian,
PhD in Technical Sciences, Associate Professor, Associate Professor of the Department
of Morphology and Public Health, Petro Mohyla Black Sea National University

MANAGING SECURITY RISKS FOR PUBLIC UTILITIES DURING COMBAT OPERATIONS

Актуальність даного дослідження зумовлена безпрецедентним характером повномасштабної збройної агресії та критичною вразливістю міської критичної інфраструктури (водо-, тепло-, енерго- та газопостачання) в умовах інтенсивних бойових дій. Життєзабезпечення громад, яке покладається на безперебійне функціонування комунальних служб, стає прямим чинником національної безпеки та виживання цивільного населення. Руйнування або виведення з ладу цих об'єктів внаслідок цілеспрямованих ворожих атак (ракетних ударів, диверсій, кібератак) призводить до гуманітарної катастрофи та економічної деградації. Існуючі міжнародні та національні методики управління ризиками безпеки (зокрема, стандарти ISO) виявилися недостатньо адаптованими до специфіки високоінтенсивного військового тиску, що підкреслює необхідність розробки нових науково-методичних засад.

Метою статті є розробка науково-методичних засад, адаптованих моделей та практичних рекомендацій щодо підвищення ефективності управління ризиками безпеки комунальних служб для забезпечення їхньої функціональної стійкості та безперервності життєзабезпечення громад в умовах збройної агресії.

Методологія дослідження включає систематизацію, порівняльний аналіз, класифікацію, а також застосування системного та структурно-функціонального підходів. Проведено аналіз наукових праць українських та зарубіжних вчених, що вивчають проблеми безпеки критичної інфраструктури, зокрема в контексті гібридних загроз та воєнних конфліктів.

У результаті проведеного дослідження було систематизовано функціональність комунальних служб у воєнний час; обґрунтовано статус комунальних служб як критично важливих елементів системи національної безпеки; вперше для цілей безпекового менеджменту в умовах війни розроблено класифікацію воєнних ризиків для комунальних об'єктів. Ризики розподілено на п'ять взаємопов'язаних груп, що охоплюють увесь спектр загроз; уточнено сутність управління ризиками безпеки в контексті бойових дій.

Практичне значення дослідження полягає у створенні теоретичної бази для розробки адаптованої багаторівневої моделі оцінки кумулятивного ризику та наданні конкретних практичних рекомендацій для управлінського персоналу комунальних підприємств та органів державної влади щодо вдосконалення механізмів міжвідомчої взаємодії з цивільним захистом і військовими підрозділами.

The relevance of this research is dictated by the ongoing full-scale war in Ukraine and the critical vulnerability of urban Critical Infrastructure (CI), particularly utility services responsible for water, heating, electricity, and gas supply. Hostilities, especially in densely populated areas, pose the most severe and complex threats to the civilian population, leading to mass casualties, large-scale destruction, and systemic failure of life support systems. CI objects have been established as primary targets for persistent and asymmetric enemy attacks (including missile strikes, sophisticated cyberattacks, and sabotage). The continuous, high-intensity military pressure necessitates a radical reevaluation of traditional risk mitigation strategies. Conventional security risk management methodologies, such as international standards ISO 31000 and ISO 27000, are primarily designed for peacetime, natural disasters, or low-intensity threats, and they critically fail to account for the unique characteristics of managing risks during active armed conflict.

The aim of this article is to develop scientific and methodological principles, tailored risk assessment models, and concrete practical recommendations for significantly enhancing the functional resilience and ensuring the operational continuity of municipal utility services during ongoing armed aggression.

The methodology employed in the research combines a systematic approach with structural-functional and comparative analysis. It involves the rigorous systematization of existing national legislation and international security concepts regarding CI. Crucially, the methodology includes the generalization of practical operational experiences gathered from Ukrainian utility services functioning under continuous shelling and emergency conditions, which informed the development of a specialized five-group risk classification.

The key findings confirm that maintaining the functional stability of utility services is not merely an economic concern but a critical national security issue and a prerequisite for civilian survival. The study establishes that the operational role of utility services has fundamentally shifted from routine maintenance to urgent operational-rescue activities. The central achievement of this research is the development of a comprehensive classification of war-specific security risks affecting municipal utilities. These risks are categorized into five interconnected groups to address the multifaceted nature of the threats.

The practical value of the research is substantial, providing the essential theoretical foundation for the subsequent development and verification of a practical multi-level model for assessing cumulative war risks. The ultimate practical application lies in formulating concrete recommendations for managerial personnel of utility companies and governmental bodies, focusing on implementing immediate preventive, protective, and restorative measures, as well as optimizing inter-agency coordination mechanisms between utility services, civil defense units, and military-civil administrations for rapid and coordinated response.

Ключові слова: ризики, управління ризиками, безпека, комунальні служби, стратегії реагування, оперативне реагування.

Key words: risks, risk management, safety, utilities, response strategies, rapid response.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Повномасштабна війна в Україні триває вже четвертий рік. Бойові дії в міських умовах стали в наш час невід'ємною її частиною. Фахівці вважають, що з погляду завдання шкоди цивільному населенню бойові дії в містах є, напевно, найнебезпечнішою формою війни. Адже вони несуть із собою смерть і поранення, руйнують будівлі та інфраструктуру, впливають на системи життєзабезпечення та освіти.

Під час повномасштабних бойових дій на території України особливу роль у збереженні життєдіяльності

громад відіграють працівники комунальних служб. Саме вони у воєнний час забезпечують базову інфраструктуру: воду, світло, газ, медичну допомогу, евакуацію постраждалих та розмінування територій.

В умовах воєнного конфлікту традиційні комунальні служби змінюють свою функціональність: їхні працівники не тільки виконують професійні обов'язки, але й діють в умовах підвищеного ризику для життя. Бойові дії ускладнюють доступ до об'єктів, порушують логістику, руйнують інфраструктуру, створюють постійну небезпеку від мін, снарядів, авіаударів тощо.

Під час бойових дій комунальні служби мають забезпечувати безперебійне функціонування життєво важливої інфраструктури. Головним їх завданням є підтри-

мання роботи систем водопостачання, водовідведення, електропостачання, теплопостачання та інших критично важливих послуг. Діяльність комунальних служб в умовах бойових дій є складною, оскільки вона вимагає забезпечення безперебійної роботи критичної інфраструктури, швидкого реагування на пошкодження та відновлення послуг, а також захисту персоналу і забезпечення життєдіяльності населення, зокрема шляхом виконання норм споживання та надання пільг учасникам бойових дій [7, с. 75].

Актуальність даного дослідження зумовлена низкою критичних чинників, що мають як національне безпекове, так і глобальне соціально-економічне значення.

Комунальна інфраструктура (енерго-, газо-, вода- та теплопостачання, водовідведення) має критичне значення для життєдіяльності та є основою стійкості будь-якого суспільства. Її безперебійне функціонування є не лише питанням комфорту, а й виживання цивільного населення, особливо в умовах воєнного часу. Руйнування або вихід із ладу об'єктів критичної інфраструктури внаслідок бойових дій призводить до: гуманітарної катастрофи (масові захворювання, відсутність опалення взимку, дефіцит питної води тощо) та економічної деградації (зупинка підприємств, порушення логістичних ланцюгів та фінансової стабільності тощо) [7, с. 80].

Слід зазначити, що сучасні військові конфлікти характеризуються асиметричними діями, де об'єкти комунальної інфраструктури стають першочерговими цілями для ворожих атак (ракетні удари, кібератаки, диверсії). Це вимагає кардинального перегляду традиційних, мирних підходів до управління ризиками та розробки спеціалізованих протоколів стійкості, що здатні забезпечити оперативне відновлення та захист систем в умовах постійної загрози. Адже існуючі на сьогодні міжнародні та національні методики управління ризиками безпеки (наприклад, ISO 31000, ISO 27000) були розроблені переважно для мирного часу та не враховують специфіку постійного, високоінтенсивного військового тиску.

Зазначимо, що на даний час відсутні науково обґрунтовані, адаптовані моделі та практичні рекомендації щодо оцінки кумулятивного (накопичувального) ризику пошкоджень; організації ефективної взаємодії між комунальними службами, військовими та цивільним захистом; прийняття рішень про перехід на резервні та автономні системи живлення.

Отже дослідження, спрямовані на розробку науково-методичних засад, які дозволять мінімізувати втрати, забезпечити функціональну стійкість комунальних служб та зберегти життя і здоров'я громадян в умовах збройної агресії є своєчасними та актуальними.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналізуючи літературні джерела з теми дослідження, можна відмітити різні підходи в цій сфері. Наприклад, О. Охріменко та Р. Попов [10, с. 2], Н. Паньків та А. Чернишова [12, с. 68], І. Пирога та М. Пирога [14, с. 119], С. Шевченко та О. Кукурудз [19, с. 2], а також О. Шпатакова, Р. Іваненко та М. Погребиський [20, с. 1] наголошують на важливості ефективного відновлення критичної інфраструктури для стабільності та економічного розвитку України після завершення війни.

Ризик — це невід'ємна складова людської діяльності, за якої існує невпевненість у результатах того чи того рішення або процесу. Останніми десятиліттями застосування концепту ризику поширюється на значно більшу кількість сфер життя сучасного суспільства. Слід зазначити, що в українській науці проблеми ризику найбільш розроблені в економічному аспекті (інвестиційні ризики, механізми ризик-менеджменту, підприємницькі ризики, ризики господарської діяльності тощо). Данім аспектам присвячено багато досліджень, а саме праці таких Л. Бондаренко, А. Грищенко, М. Дамаскіна, О. Колот, В. Кривошеїн, А. Пехник, Н. Скопенко, М. Степура, О. Таран [13, с. 34].

Вивченням змісту та сутності понять "ризик", "загроза", "небезпека", а також їх співвідношенням займалися багато вчених: І. Бойко [2, с. 95], М. Копитко та Н. Літвін [9, с. 6], С. Лаптев [8, с. 35-39], Г. Пазеєва [11, с. 20-25] та інші.

Статистичну оцінку ризиків вивчали В. Вітлінський та В. Скілько [4, с. 385], О. Рижено [16, с. 2], В. Фішун [18, с. 1]. Зарубіжна вчена Катаріна Дідріх [22, с. 383], а також Каміло М. та Овертон М. [21, с. 1] вивчали актуальні проблеми ризик-менеджменту.

Вивченню основних загроз для критичної інфраструктури та способів ефективної протидії їм присвячені дослідження таких українських вчених як: О. Верголяс, який показує важливість інтеграції новітніх технологій та підходів для забезпечення безпеки ключових об'єктів, особливо у контексті зростання гібридних загроз [3, с. 1]. І. Уряднікова та В. Заплатинський [17, с. 2], Д. Бірюков, С. Кондратов, О. Насвіт та О. Суходоля [1, с. 2].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою цієї статті є розробка науково-методичних засад та практичних рекомендацій щодо підвищення ефективності управління ризиками безпеки комунальних служб для забезпечення їхньої функціональної стійкості та безперервності життєзабезпечення громад в умовах збройної агресії. Для досягнення цієї мети були поставлені такі завдання:

— проаналізувати та систематизувати існуючі національні та міжнародні підходи до управління ризиками безпеки критичної інфраструктури (зокрема, ISO 31000, ISO 27000), визначивши їхню недостатність та обмеження для застосування в умовах високоінтенсивного військового тиску;

— узагальнити практичний досвід функціонування, відновлення та реагування комунальних служб в Україні під час повномасштабної війни, ідентифікувавши типові операційні моделі загроз та пошкоджень об'єктів критичної інфраструктури;

— розробити комплексну класифікацію та багаторівневу модель оцінки специфічних воєнних ризиків для комунальних об'єктів (фізичні, операційні, кадрові, кібернетичні, біологічні та екологічні), зважаючи на їхню критичність.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Комунальні служби (або житлово-комунальні служби) — це сукупність підприємств, установ та організацій,

Таблиця 1. Ключові ознаки та функції комунальних служб

Ознака	Пояснення
Життєзабезпечення	Надання послуг, відсутність яких створює загрозу життю, здоров'ю населення та нормальному функціонуванню держави.
Сфери діяльності	Водопостачання та водовідведення, теплопостачання (опалення), газопостачання, електропостачання (як частина системи, що забезпечує комунальні потреби), вивіз та утилізація побутових відходів.
Безперервність	Необхідність функціонування в режимі 24/7, що вимагає високої стійкості та швидкої відновлюваності, особливо в умовах надзвичайних ситуацій чи військового конфлікту.
Критичність	Згідно з Законом України «Про критичну інфраструктуру» [5, с. 1], об'єкти комунальних служб (особливо централізовані системи) відносяться до критично важливих елементів національної безпеки.

Джерело: сформовано на основі [7, 5].

незалежно від форми власності, які забезпечують життєво необхідні потреби населення, об'єктів соціальної сфери та економіки шляхом надання безперервних послуг та управління відповідною інфраструктурою. Комунальні служби є складовою частиною критичної інфраструктури країни.

У мирний час ці служби виконують планові та аварійні роботи, забезпечуючи стабільну роботу інфраструктури. Проте у період воєнних дій ситуація кардинально змінюється. Під обстрілами, у зруйнованих районах, без доступу до ресурсів, ці працівники змушені продовжувати свою роботу, часто — у бронежилетах, шоломах, без зв'язку та під загрозою постійних обстрілів.

Основними завданнями комунальних служб у зоні бойових дій є:

- відновлення енергопостачання та водопостачання після обстрілів;
- заміна пошкоджених ділянок мереж (електро-, газо-, водопостачання);
- рятувальні та медичні операції серед постраждалих;
- усунення вибухонебезпечних предметів;
- психологічна та технічна допомога населенню.

Ці служби стають частиною стратегії національної безпеки, адже без забезпечення базових послуг неможливо говорити про стійкість тилу, підтримку армії та збереження життів цивільного населення.

Ключові ознаки та функції комунальних служб наведено у таблиці 1.

Основними аспектами функціонування комунальних служб у зоні бойових дій є:

1. Забезпечення безперебійної роботи критичної інфраструктури. Пріоритетом є підтримання функціонування систем електро-, водопостачання, водовідведення та газопостачання.

2. Швидке реагування та відновлення. Комунальні служби мають оперативно реагувати на пошкодження мереж та об'єктів інфраструктури, спричинені бойовими діями, та здійснювати їх відновлення для забезпечення мешканців відповідними послугами.

3. Захист персоналу. Необхідно вживати заходи для захисту життя та здоров'я працівників комунальних служб, адже їх робота є надзвичайно важливою для підтримки функціонування населених пунктів.

4. Ефективне використання ресурсів. В умовах бойових дій існує потреба в економному використанні ресурсів та плануванні роботи для забезпечення стабільного функціонування в умовах дефіциту.

5. Виконання соціальних зобов'язань. Комунальні служби мають забезпечувати надання пільг учасникам бойових дій та членам їхніх сімей, які передбачені Законом України "Про статус ветеранів війни, гарантії їх соціального захисту" [6, с. 10]. Зокрема, це стосується 75 % знижки на оплату житлово-комунальних послуг та використання палива в межах норм споживання.

Автором було визначено основні ризики для комунальних служб під час ведення бойових дій. Їх можна поділити на декілька груп.

1. Фізичні та техногенні ризики (пряма загроза інфраструктурі). Ці ризики пов'язані з безпосереднім руйнівним впливом військових дій (табл. 2).

Таблиця 2. Фізичні та техногенні ризики

Ризик	Опис
Пряме руйнування об'єктів	Ушкодження або повне знищення критичних об'єктів (насосних станцій, котелень, електропідстанцій, газорозподільних пунктів) внаслідок ракетних, артилерійських ударів, авіаційних бомбардувань.
Вторинні (техногенні) аварії	Виникнення великих техногенних катастроф через руйнування (наприклад, пошкодження гребель, резервуарів з хімікатами на очисних спорудах), що призводить до забруднення навколишнього середовища.
Забруднення території	Мінна небезпека, наявність нерозірваних боєприпасів та уламків, що унеможливає або значно ускладнює проведення ремонтних та відновлювальних робіт.
Пошкодження мереж	Масштабні пориви підземних і надземних комунікацій (водогони, теплотраси, газопроводи) через ударні хвилі, вибухи або рух важкої військової техніки.

Джерело: сформовано на основі [1, 3, 7].

Таблиця 3. Операційні та логістичні ризики

Ризик	Опис
Дефіцит ресурсів	Гострий брак палива, електроенергії (через обмеження), хімічних реагентів для очищення води, а також критичних матеріалів та запасних частин для ремонту.
Порушення логістики	Неможливість доставити ремонтні бригади, обладнання або матеріали через зруйновані дороги, блокпости, комендантську годину або близькість лінії фронту.
Перебої з комунікацією	Порушення зв'язку (телефонного, інтернет) між диспетчерськими службами, ремонтними бригадами та органами влади, що ускладнює координацію дій.
Ризик саботажу/диверсій	Загроза цілеспрямованих дій ворожих диверсійно-розвідувальних груп (ДРГ) на важливих, але не повністю захищених об'єктах.

Джерело: сформовано на основі [1, 3, 7].

2. Операційні та логістичні ризики (перерва в роботі). Ці ризики стосуються порушення безперервності виробничих процесів та управління (табл. 3).

3. Кадрові та соціальні ризики (людський фактор). Ризики, пов'язані з персоналом комунальних служб та населенням (табл. 4).

4. Кібернетичні та управлінські ризики (системна вразливість). Ризики, що стосуються інформаційної безпеки та ефективності менеджменту (табл. 5).

5. Біологічні та екологічні ризики (санітарна та довгочасна загроза). Ця група ризиків пов'язана з порушенням санітарно-епідеміологічної безпеки та забруднен-

ням навколишнього середовища внаслідок бойових дій, що прямо впливає на роботу комунальних служб (табл. 6).

Ця група ризиків підкреслює, що управління безпекою комунальних служб під час війни не обмежується лише ремонтом пошкоджень, але й включає критичну функцію санітарного та екологічного захисту.

Управління ризиками безпеки (Risk Security Management) — це систематичний, безперервний процес ідентифікації, оцінки, аналізу, обробки (пом'якшення) та моніторингу загроз і вразливостей, які можуть негативно вплинути на функціонування, цілісність та стійкість об'єкта, системи чи організації. Метою є мінімізація збитків, забезпечення безперервності бізнесу та досягнення стратегічних цілей шляхом впровадження відповідних стратегій, політик та заходів безпеки.

Постанова КМУ "Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності" [15, с. 1—2] дає таке визначення поняття "ризик безпеки на об'єктах критичної інфраструктури" — можливість виникнення інциденту безпеки критичної інфраструктури/порушення стану захищеності критичної інфраструктури, що становить загрозу для за-

Таблиця 4. Кадрові та соціальні ризики

Ризик	Опис
Безпека персоналу	Висока ймовірність поранення або загибелі працівників під час виконання службових обов'язків (ремонтні роботи під обстрілами, пересування в небезпечних зонах).
Кадровий дефіцит	Відтік кваліфікованого персоналу (мобілізація, евакуація, відмова працювати в зоні бойових дій), що призводить до критичної нестачі фахівців.
Соціальна напруга	Зростання невдоволення населення через відсутність життєво необхідних послуг, що ускладнює роботу комунальників та місцевої влади.
Психологічний стан	Психологічне вигорання, стрес, паніка серед персоналу, що знижує ефективність прийняття рішень та якість виконання робіт.

Джерело: сформовано на основі [1, 3, 7].

Таблиця 5. Кібернетичні та управлінські ризики

Ризик	Опис
Кібератаки	Атаки на системи SCADA, мережеве обладнання та офісні комп'ютерні мережі комунальних підприємств, спрямовані на порушення управління або виведення з ладу обладнання.
Неефективне планування	Використання мирних планів аварійного реагування, які не відповідають специфіці воєнних загроз, що призводить до затримок у відновленні.
Фінансові ризики	Критичне зниження надходжень від оплати послуг, неможливість залучити інвестиції або кредити для відновлення та ремонту в умовах високих воєнних ризиків.
Правовий/регуляторний ризик	Невизначеність або складність правового режиму роботи в зоні бойових дій, на окупованих/деокупованих територіях, що ускладнює закупівлі, фінансування та координацію.

Джерело: сформовано на основі [1, 3, 7].

Таблиця 6. Біологічні та екологічні ризики

Ризик	Опис	Вплив на комунальні служби
Поширення інфекційних хвороб	Виникнення спалахів холери, дизентерії, гепатиту А та інших кишкових інфекцій через змішування стічних вод із питною водою внаслідок пошкодження мереж водопостачання та каналізації.	Критичне навантаження на очисні споруди та системи знезараження води; необхідність екстреної дезінфекції мереж.
Робота в заражених районах	Необхідність проведення ремонтних робіт у зонах витоків каналізації (біологічне зараження), розливів палива, хімікатів (хімічне зараження) або місцях, забруднених уламками, що містять токсичні речовини.	Вимагає спеціального захисного обладнання, навчання персоналу протоколам біологічної та хімічної безпеки.
Небезпечні біологічні матеріали	Робота з трупамі (людей чи тварин), що перебували у комунікаціях, під завалами або поблизу об'єктів інфраструктури, що становить епідеміологічну загрозу для ремонтних бригад.	Потреба у швидкій та безпечній утилізації (спільно з ДСНС/медичними службами) та знезараженні прилеглих територій і комунікацій.
Забруднення водних джерел	Потрапляння продуктів горіння, вибухівки та хімічних речовин військового походження у водозабори, річки та підземні води, що робить водопостачання непридатним.	Вимагає оперативного моніторингу якості води та переходу на альтернативні або резервні джерела, що збільшує операційні ризики.

Джерело: сформовано на основі [1, 3, 7].

безпечення функціональності, безперервності роботи, відновлюваності, цілісності та стійкості об'єктів критичної інфраструктури. Там же знаходимо визначення поняття "управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності" — це діяльність, спрямована на запобігання виникненню інциденту та мінімізацію можливих наслідків у разі його настання.

Серед основних компонентів управління ризиками безпеки можна виділити наступні:

- ідентифікація ризиків — це процес визначення того, які саме загрози (наприклад, ракетний удар, кібератака, диверсія) існують та які вразливості (старе обладнання, відсутність резервування, непідготовлений персонал) роблять комунальні служби чутливими до цих загроз. Як результат — створення повного реєстру потенційних загроз;

- оцінка та аналіз ризиків. На цьому етапі визначається ймовірність виникнення загрози та потенційний вплив (збиток), який вона може спричинити (фінансовий, екологічний, гуманітарний). Ризики ранжуються за пріоритетом (від високого до низького). Як результат — визначення критичних ризиків, що потребують негайної уваги;

- обробка (пом'якшення) ризиків — це розробка та впровадження заходів, спрямованих на зменшення ймовірності або впливу ризиків. Існує чотири основні стратегії: уникнення — усунення діяльності, яка створює ризик, наприклад, зупинка роботи в особливо небезпечній зоні; зменшення (контроль) — впровадження заходів захисту, наприклад, бетонування критичних вузлів, резервування систем; передача (страхування) — перекладання фінансового тягаря на третю сторону; прийняття — свідоме рішення прийняти низький або несуттєвий ризик, не вживаючи додаткових заходів;

- моніторинг та контроль. Зважаючи на те, що умови бойових дій постійно змінюються, необхідно безперервно відстежувати ефективність вжитих заходів та регулярно переоцінювати ризики. Це дозволяє вчасно адаптувати стратегії захисту. Як результат — актуалізація планів реагування та захисних протоколів.

Отже, управління ризиками безпеки комунальних служб під час бойових дій слід розглядати як процес, сфокусований на забезпеченні стійкості, тобто, здатність не лише протистояти загрозам, а й швидко відновлювати функціональність після атаки чи пошкодження. Це вимагає інтеграції військових, цивільних та технічних аспектів безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Комунальні служби — це суб'єкти господарювання, які експлуатують технічні системи та мережі критичної інфраструктури (водоканали, тепломережі, газові та енергетичні об'єкти), забезпечуючи безперервне надання життєво необхідних послуг населенню та

промисловості. Їхня безпека та стійкість є прямим чинником національної безпеки, що вимагає спеціалізованого управління ризиками в умовах збройного конфлікту.

Автором було підтверджено, що забезпечення функціональної стійкості комунальних служб (водо-, тепло-, енергопостачання) під час збройної агресії є не лише економічним, а й критичним питанням національної безпеки та виживання цивільного населення. Чинні міжнародні та національні методики управління ризиками (наприклад, ISO 31000) виявилися недостатньо адаптованими до специфіки високоінтенсивного військового тиску та комплексних загроз.

Систематизовано функції комунальних служб у воєнний час, підкресливши, що їхня діяльність кардинально змінюється: від планової до оперативно-рятувальної, що вимагає від персоналу діяти в умовах підвищеного ризику. Обґрунтовано, що комунальні служби є складовою частиною критичної інфраструктури, що вимагає спеціалізованих безпекових протоколів.

Вперше для цілей управління безпекою проведено класифікацію воєнних ризиків для комунальних служб, розподілену на 5 взаємопов'язаних груп:

- фізичні та техногенні (пряме руйнування, вторинні аварії);
- операційні та логістичні (дефіцит ресурсів, порушення логістики);
- кадрові та соціальні (безпека персоналу, кадровий дефіцит);
- кібернетичні та управлінські (атаки на SCADA, неефективне планування);
- біологічні та екологічні (поширення інфекцій, робота в заражених районах). Ця класифікація є базою

для розробки адаптованої моделі оцінки кумулятивного ризику.

Управління ризиками безпеки в контексті бойових дій визначено як систематичний і безперервний процес, сфокусований не лише на запобіганні, а й на швидкому відновленні функціональності після інциденту. Це вимагає інтеграції військових, цивільних та технічних аспектів для забезпечення операційної стійкості.

Визначено, що науково обгрунтовані адаптовані моделі та практичні рекомендації щодо оцінки кумулятивного ризику, а також ефективної організації взаємодії комунальних служб з військовими та цивільним захистом, наразі відсутні. Це підтверджує необхідність подальшої роботи в рамках цього дослідження для розробки конкретних превентивних і відновлювальних заходів. Наступним етапом дослідження має стати розробка та верифікація багаторівневої моделі оцінки воєнних ризиків на основі представленої класифікації та надання конкретних рекомендацій для управлінського персоналу комунальних підприємств та органів державної влади щодо підвищення їхньої стійкості.

Література:

- Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. (2015). Зелена книга з питань захисту критичної інфраструктури в Україні. Національний інститут стратегічних досліджень. Київ. URL: https://cdn-regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf (дата звернення: 20.09.2025).
- Бойко І. В. (2017). Дефініції "ризик", "загроза", "небезпека" як об'єкти наукових досліджень у напрямі економічної безпеки підприємства. Приазовський економічний вісник. Випуск 5 (05). 94—98. URL: http://rev.kpi.zp.ua/journals/2017/5_05_uk/20.pdf (дата звернення: 20.09.2025).
- Верголяс О. О. (2020). Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. Coolyanews.info. URL: <https://coolyanews.info/reformuvannya-sistemi-zahistu-ta-pidvischennya-stiijkostii-kritichnoyi-infrastrukturi-ukrayinii-v-rozriizi-aktual.html> (дата звернення: 25.09.2025).
- Вітлінський В. В., Скіцько В. І. (2018). Ризик-менеджмент ланцюгів постачання в умовах цифрової економіки. Бізнес Інформ. № 4. 384—392. URL: http://nbuv.gov.ua/UJRN/binf_2018_4_55 (дата звернення: 25.09.2025).
- Закон України "Про критичну інфраструктуру" № 1882-IX від 16 листопада 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 22.09.2025).
- Закон України "Про статус ветеранів війни, гарантії їх соціального захисту" № 3551-XII від 22 жовтня 1993 року. URL: <https://zakon.rada.gov.ua/laws/show/3551-12#Text> (дата звернення: 22.09.2025).
- Ковальов К. Є. (2025). Сучасні виклики та загрози для критичної інфраструктури України під час воєнного стану. Приватне та публічне право. № 1. 75—80. DOI: <https://doi.org/10.32782/2663-5666.2025.1.12>.
- Комплексне забезпечення економічної безпеки підприємств: [монографія] / [С. М. Лаптев, В. Г. Алькема, В. С. Сідак, М. І. Копитко]; за ред. М. І. Копитко. — К.: Університет економіки та права "КРОК", 2017. — 508 с.
- Копитко М. І. (2017). Деструктивні чинники середовища функціонування соціально-економічних систем. Вчені записки Університету "КРОК". Серія: Економіка. Вип. 46. 4—15.
- Охріменко О., Попов Р. (2022). Повоєнна відбудова України: потенціал та стратегія перетворень. Економіка та суспільство. Випуск 45. DOI: <https://doi.org/10.32782/2524-0072/2022-45-7>.
- Пазєєва Г. М. Комплексна діагностика в забезпеченні економічної безпеки підприємств (на матеріалах транспортно-експедиційних підприємств України). — К.: Університет економіки та права "КРОК", 2017. 291 с.
- Паньків Н., Чернишова А. (2023). Проблеми та перспективи відновлення України під час та після завершення російсько-української війни. Вісник Хмельницького національного університету. Економічні науки. № 1 (314). 67—79. DOI: <https://doi.org/10.31891/2307-5740-2023-314-1-9>.
- Пехник А. В., Кройтор А. В., Завгородня Ю. В. (2019). Теорія ризику: історія та сучасні підходи. Актуальні проблеми політики. Вип. 63. 33—47. DOI: <https://doi.org/10.32837/app.v63i0.5>.
- Пирога І. С., Пирога М. І. (2023). Роль місцевого самоврядування у відбудові в умовах воєнного стану. Науковий вісник Ужгородського університету: серія: Право. Т. 1. Вип. 77. 117—123. DOI: <https://doi.org/10.24144/2307-3322.2023.77.1.18>.
- Постанова КМУ "Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності" № 367 від 1 квітня 2025 року. URL: <https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text> (дата звернення: 01.10.2025).
- Риженко О., Фіщук В. (2018). Як цифрова економіка змінить Україну. Економічна правда. 16 січня. URL: <https://www.epravda.com.ua/columns/2018/01/16/633057/> (дата звернення: 01.10.2025).
- Уряднікова І. В., Заплатинський В. М. (2020). Наукові підходи до визначення терміну "критична інфраструктура". Вісті Донецького гірничого інституту. № 2 (47). URL: https://jdmi.donntu.edu.ua/wp-content/uploads/2021/02/Uriadnikova-JDMI_2_2020.pdf (дата звернення: 03.10.2025).
- Фіщук В. (2017). Цифрова економіка — це реально. Новий час. Бізнес. 18 квітня. URL: <https://biz-nv.ua/ukr/experts/fichuk/tsifrova-ekonomika-tse-rearno-1001102.html> (дата звернення: 02.10.2025).
- Шевченко С. О., Кукурудз О. М. (2024). Стратегії фінансування повоєнної відбудови: виклики та перспективи для України. Академічні візії. Випуск 28. DOI: <https://doi.org/10.5281/zenodo.10678026>.
- Шпатакова О., Іваненко Р., Погребиський М. (2022). Перспективи відновлення критичної інфраструктури на деокупованих територіях України. Економіка та суспільство. Випуск 40. DOI: <https://doi.org/10.32782/2524-0072/2022-40-5>.

21. Camillo M., Overton M. (2017, March 29). Cyber Risks and Your Supply Chain. URL: <https://www.aig.com/knowledge-andinsights/k-and-i-article-cyber-supply-chain> (дата звернення: 27.09.2025).

22. Diedrich K. (2017). Framework for Digitalized Proactive Supply Chain Risk Management. Proceedings of the Hamburg International Conference of Logistics (HICL). Digitalization in Supply Chain Management and Logistics. 381-403. URL: https://tubdok.tub.tuhh.de/bitstream/11420/1459/1/diedrich_framework_digitalized_supply_chain_hicl_2017.pdf (дата звернення: 27.09.2025).

References:

1. Biryukov, D.S., Kondratov, S.I., Nasvit, O.I. and Sukhodolia, O.M. (2015), Zelena knyha z pytan zachystu krytychnoi infrastruktury v Ukraini [Green Paper on Critical Infrastructure Protection in Ukraine], National Institute for Strategic Studies, Kyiv, Ukraine.

2. Boiko, I.V. (2017), "Definitions of "risk," "threat," and "danger" as subjects of scientific research in the field of economic security of enterprises", Pryazovskiy ekonomichnyi visnyk, vol. 5 (05), pp. 94—98, available at: http://pev.kpu.zp.ua/journals/2017/5_05_uk/20.pdf (Accessed 20 September 2025).

3. Verholias, O.O. (2020). "Reforming the protection system and improving the resilience of Ukraine's critical infrastructure in the context of current threats", Coolynews.info, available at: <https://coolynews.info/reformuvannya-sistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-infrastruktury-ukrayinii-v-rozriizii-aktual.html> (Accessed 25 September 2025).

4. Vitlinsky, V.V., & Skitsko, V.I. (2018), "Risk management of supply chains in the digital economy", Biznes Inform, vol. 4, pp. 384—392, available at: http://nbuv.gov.ua/UJRN/binf_2018_4_55 (Accessed 25 September 2025).

5. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "About critical infrastructure", available at: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (Accessed 22 September 2025).

6. The Verkhovna Rada of Ukraine (1993), The Law of Ukraine "On the status of war veterans and guarantees of their social protection", available at: <https://zakon.rada.gov.ua/laws/show/3551-12#Text> (Accessed 22 September 2025).

7. Kovalov, K. E. (2025), "Current challenges and threats to Ukraine's critical infrastructure during martial law", Pryvatne ta publichne pravo, vol. 1, pp. 75-80. <https://doi.org/10.32782/2663-5666.2025.1.12>.

8. Laptev, S.M., Alkem, V.G., Sidak, V.S. and Kopytko, M. I. (2017), Kompleksne zabezpechennia ekonomichnoi bezpeky pidpriemstv [Comprehensive provision of economic security for enterprises], KROK University of Economics and Law, Kyiv, Ukraine.

9. Kopytko, M.I. (2017), "Destructive factors in the environment of socio-economic systems", Vcheni zapysky Universytetu "KROK", serii: Ekonomika, vol. 46, pp. 4—15.

10. Okhrimenko, O. and Popov, R. (2022), "Post-war reconstruction of Ukraine: potential and strategy for transformation", Ekonomika ta suspilstvo, vol. 45. <https://doi.org/10.32782/2524-0072/2022-45-7>.

11. Pazeyeva, G.M. (2017), Kompleksna diahnostyka v zabezpechenni ekonomichnoi bezpeky pidpriemstv (na materialakh transportno-ekspedytsiinykh pidpriemstv Ukrainy) [Comprehensive diagnostics in ensuring economic security of enterprises (based on materials from transport and forwarding companies in Ukraine)], KROK University of Economics and Law, Kyiv, Ukraine.

12. Pankiv, N., & Chernyshova, A. (2023), "Problems and prospects for Ukraine's recovery during and after the Russian-Ukrainian war", Visnyk Khmelnytskoho natsionalnoho universytetu, Ekonomichni nauky, vol. 1 (314), pp. 67—79. <https://doi.org/10.31891/2307-5740-2023-314-1-9>.

13. Pehnyk, A.V., Kroitur, A.V., & Zavgorodnia, Yu.V. (2019), "Risk theory: history and contemporary approaches", Aktualni problemy polityky, vol. 63, pp. 33—47. <https://doi.org/10.32837/app.v63i0.5>.

14. Pyroha, I.S. and Pyroha, M.I. (2023), "The role of local self-government in reconstruction under martial law", Naukovyi visnyk Uzhhorodskoho universytetu, serii: Pravo, vol. 1, no. 77, pp. 117—123. <https://doi.org/10-24144/2307-3322.2023.77.1.18>.

15. Cabinet of Ministers of Ukraine (2025), Resolution "On approval of requirements for security risk management at critical infrastructure facilities of criticality category I", available at: <https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text> (Accessed 01 October 2025).

16. Ryzenko, O., & Fichuk, V. (2018), "How the digital economy will change Ukraine", Ekonomichna Pravda, available at: <https://www.epravda.com.ua/columns/2018/01/16/633057/> (Accessed 01 October 2025).

17. Ureynikova, I.V. and Zaplatynskiy, V.M. (2020), "Scientific approaches to defining the term "critical infrastructure", Visti Donetskoho hirnychoho instytutu, vol. 2 (47), available at: https://jdmi.donntu.edu.ua/wp-content/uploads/2021/02/Uriadnikova-JDMI_2_-2020.pdf (Accessed 03 October 2025).

18. Fischuk, V. (2017), "The digital economy is real", Novyi chas. Biznes, available at: <https://biz.nv.ua/ukr/experts/fichuk/tsifrova-ekonomika-tse-realno-100-1102.html> (Accessed 02 October 2025).

19. Shevchenko, S.O., & Kukuruza, O.M. (2024), "Strategies for financing post-war reconstruction: challenges and prospects for Ukraine", Akademichni vizii, vol. 28. <https://doi.org/10.5281/zenodo.10678026>.

20. Shpatakova, O., Ivanenko, R., & Pogrebitsky, M. (2022), "Prospects for the restoration of critical infrastructure in the deoccupied territories of Ukraine", Ekonomika ta suspilstvo, vol. 40. <https://doi.org/10.32782/2524-0072/2022-40-5>.

21. Camillo, M. and Overton, M. (2017), "Cyber Risks and Your Supply Chain", available at: <https://www.aig.com/knowledge-andinsights/k-and-i-article-cyber-supply-chain> (Accessed 27 September 2025).

22. Diedrich, K. (2017), "Framework for Digitalized Proactive Supply Chain Risk Management", Digitalization in Supply Chain Management and Logistics, pp. 381—403, available at: https://tubdok.tub.tuhh.de/bitstream/11420/1459/1/diedrich_framework_digitalized_supply_chain_hicl_2017.pdf (Accessed 27 September 2025).

Стаття надійшла до редакції 10.10.2025 р.