

Погребняк В. Г., доктор технічних наук, професор,
професор кафедри технології захисту навколишнього середовища
та безпеки праці
Івано-Франківського національного технічного університету
нафти і газу
ORCID: 0000-0002-7735-3408

Перкун І. В., кандидат технічних наук,
доцент, здобувач наукового ступеня доктора технічних наук
Івано-Франківського національного технічного університету
нафти і газу
ORCID: 0000-0002-6523-1606

Вишнікіна О. В., кандидат хімічних наук, доцент,
доцент кафедри міжнародного туризму
та готельно-ресторанного бізнесу
Університету митної справи та фінансів
ORCID: 0000-0002-3747-2904

Погребняк А. В., доктор технічних наук, професор,
професор кафедри міжнародного туризму
та готельно-ресторанного бізнесу
Університету митної справи та фінансів
ORCID: 0000-0003-3214-6410

ВІД ОХОРОНИ ПРАЦІ ДО КОМПЛЕКСНОЇ БЕЗПЕКИ: СТРАТЕГІЇ ІНТЕГРАЦІЇ ЦИВІЛЬНОГО ЗАХИСТУ В КОРПОРАТИВНІ СИСТЕМИ УПРАВЛІННЯ

В статті обґрунтовано нагальну науково-практичну проблему, що виникла внаслідок повномасштабної війни в Україні – фундаментальну невідповідність традиційних корпоративних систем управління безпекою новим гібридним загрозам. Доведено, що класична модель, де охорона праці (ОП) та цивільний захист (ЦЗ) функціонують як дві паралельні, слабо інтегровані системи, є застарілою та нездатною забезпечити адекватний рівень захисту персоналу та активів підприємств, які перетворилися на потенційні цілі для воєнних атак. Існуючі системи управління охороною праці, побудовані на стандартах мирного часу (напр., ISO 45001), орієнтовані на запобігання ненавмисним інцидентам і не мають інструментарію для протидії умисним зовнішнім впливам. Метою статті є розробка науково обґрунтованих стратегій інтеграції функцій цивільного захисту в корпоративні системи управління охороною праці для створення єдиної, комплексної моделі безпеки підприємства, адаптованої до умов гібридних загроз. На основі аналізу класичних концепцій (Safety-I, Safety-II, Resilience Engineering) та нормативно-правової бази України виявлено ключову прогалину – відсутність цілісної моделі управління всіма видами безпекових ризиків на корпоративному рівні. Наукова новизна роботи полягає у тому, що вперше запропоновано концептуальну модель інтегрованої системи управління комплексною безпекою (СУКБ). На відміну від існуючих підходів, дана модель синтезує ОП та ЦЗ в єдиний управлінський цикл («аналіз – превенція – реагування – відновлення»), що базується на п'яти ключових принципах: єдності управління, проактивності, тотальної ризик-орієнтованості (з урахуванням воєнних загроз), людиноцентризму та безперервності. Цей підхід дозволяє перейти від застарілої дихотомії «внутрішні/зовнішні загрози» до єдиного контуру управління всіма ідентифікованими ризиками, незалежно від їхнього походження. Практичне значення полягає у розробці чотирьох груп конкретних стратегій інтеграції: нормативно-правової (створення єдиного Положення про комплексну безпеку), організаційно-управлінської (формування єдиного центру безпеки), техніко-технологічної (інтеграція систем оповіщення та моніторингу) та соціально-психологічної (провадження комплексних навчань, психологічна підтримка). Запропоновані стратегії можуть слугувати дорожньою картою для керівників українських підприємств для реформування існуючих систем, підвищення рівня захищеності персоналу, забезпечення стійкості бізнес-процесів та збереження людських життів в умовах воєнного стану.

Ключові слова: комплексна безпека, інтеграція систем, цивільний захист, охорона праці, воєнні ризики, гібридні загрози, система управління безпекою, стійкість підприємства, ризик-орієнтований підхід.

© В. Г. Погребняк, І. В. Перкун, О. В. Вишнікіна, А. В. Погребняк, 2025

Стаття поширюється на умовах ліцензії CC BY 4.0

Pogrebnyak V. G., Perkun I. V., Vyshnikina O. V., Pogrebnyak A. V. From Occupational Safety to Comprehensive Security: Strategies for Integrating Civil Defense into Corporate Management Systems

The article substantiates an urgent scientific and practical problem that has arisen due to the full-scale war in Ukraine – the fundamental inadequacy of traditional corporate safety management systems in the face of new hybrid threats. It is proven that the classic model, where occupational safety (OS) and civil defense (CD) function as two parallel, weakly integrated systems, is outdated and incapable of providing an adequate level of protection for personnel and assets of enterprises, which have become potential targets for military attacks. Existing occupational safety management systems, built on peacetime standards (e.g., ISO 45001), are focused on preventing unintentional incidents and lack the tools to counter deliberate external impacts. The purpose of the article is to develop scientifically-backed strategies for integrating civil defense functions into corporate occupational safety management systems to create a unified, comprehensive enterprise security model adapted to the conditions of hybrid threats. Based on an analysis of classical concepts (Safety-I, Safety-II, Resilience Engineering) and the legal framework of Ukraine, a key gap has been identified – the absence of a holistic model for managing all types of security risks at the corporate level. The scientific novelty of the work lies in the proposal of a conceptual model for an integrated comprehensive security management system (CSMS) for the first time. Unlike existing approaches, this model synthesizes OS and CD into a single management cycle ("analysis – prevention – response – recovery"), based on five key principles: unity of command, proactivity, total risk orientation (including military risks), human-centricity, and continuity. This approach allows for a transition from the outdated dichotomy of "internal/external threats" to a single management loop for all identified risks, regardless of their origin. The practical significance lies in the development of four groups of specific integration strategies: legal-regulatory (creating a unified Comprehensive Security Regulation), organizational-managerial (forming a single security center), technical-technological (integrating alert and monitoring systems), and socio-psychological (conducting comprehensive training and providing psychological support). The proposed strategies can serve as a roadmap for managers of Ukrainian enterprises to reform existing systems, enhance personnel protection, ensure the resilience of business processes, and save human lives under martial law.

Key words: comprehensive security, systems integration, civil defense, occupational safety, military risks, hybrid threats, safety management system, enterprise resilience, risk-based approach.

Постановка проблеми. Війна в Україні спричинила тектонічний зсув у безпековому середовищі, перетворивши всю територію країни на зону потенційного ураження. Для українських підприємств це означало кардинальну зміну парадигми ризиків. Якщо раніше система управління безпекою фокусувалася переважно на внутрішніх загрозах – виробничому травматизмі, професійних захворюваннях, технологічних аваріях та пожежах [1–4], – то сьогодні на перший план вийшли прямі зовнішні воєнні загрози [5, 6]. Ракетні обстріли, атаки безпілотних літальних апаратів (БпЛА), артилерійські удари, кібератаки та диверсійна діяльність перетворили промислові, енергетичні, логістичні та навіть аграрні об'єкти з виробничих майданчиків на потенційні цілі.

Ця нова реальність оголила фундаментальну вразливість існуючих корпоративних систем управління. Традиційний підхід, де охорона праці (ОП) та цивільний захист (ЦЗ) існують як дві паралельні, слабо пов'язані між собою системи, виявився нездатним забезпечити адекватний рівень захисту персоналу та активів [1, 2, 6]. Безпека працівника на робочому місці більше не залежить лише від справності обладнання чи дотримання інструкцій; вона прямо залежить від наявності та стану укриття, ефективності системи оповіщення та готовності до дій в умовах бойової загрози. Таким чином, проблема виходить за межі класичної охорони праці і набуває рис комплексної проблеми виживання та стійкості бізнесу.

Постановка завдання. Існуючі корпоративні системи управління охороною праці (СУОП), здебільшого побудовані на філософії стандартів мирного часу, таких як міжнародний стандарт ISO 45001:2018, орієнтовані на ідентифікацію, оцінку та контроль ризиків *ненавмисного* характеру [1–3, 7]. Вони ефективні для запобігання нещасним випадкам, але їх інструментарій та методологія виявляються недостатніми для протидії *умисним*, спланованим зовнішнім загрозам воєнного характеру. Ризик влучання ракети неможливо «усунути» чи «замінити» інженерними засобами контролю на робочому місці [5, 6].

З іншого боку, функції цивільного захисту на підприємствах, регламентовані Кодексом цивільного захисту України [8], до 2022 року часто виконувались формально. Плани реагування, тренування та матеріально-технічне забезпечення не завжди відповідали реальним потребам. Найголовніше – ці функції існували в організаційному вакуумі, окремо від щоденних процесів управління охороною праці та виробничою діяльністю. Виник критичний функціональний розрив між системою, що відповідає за безпеку «всередині» (СУОП), і системою, що має відповідати за безпеку «ззовні» (ЦЗ).

Відтак, виникає гостра наукова та практична проблема: відсутність цілісної, теоретично обґрунтованої концепції та практичних стратегій для повної, а не часткової, інтеграції функцій цивільного захисту в корпоративні системи управління. Необхідно подолати застарілу дихотомію «ОП проти ЦЗ» [1, 8] і перейти до єдиної моделі управління комплексною безпекою.

Мета статті – розробка науково обґрунтованих стратегій інтеграції функцій цивільного захисту в корпоративні системи управління охороною праці для створення єдиної, комплексної моделі безпеки підприємства, адаптованої до умов гібридних загроз. Досягнення мети передбачає вирішення наступних завдань: аргументувати необхідність парадигмального зсуву від ізольованих систем ОП та ЦЗ до єдиного контуру

комплексної безпеки; сформулювати ключові принципи та розробити концептуальну модель інтегрованої системи управління комплексною безпекою (СУКБ); запропонувати конкретні нормативно-правові, організаційні, технічні та соціально-психологічні стратегії практичної інтеграції.

Аналіз останніх досліджень і публікацій. *Огляд класичних моделей управління охороною праці та їхньої обмеженості.* Традиційною парадигмою в управлінні безпекою є Safety-I, яка фокусується на аналізі того, що йде не так: розслідування нещасних випадків, виявлення помилок та усунення причин збоїв [9–11]. Цей реактивний підхід, хоч і є базовим, абсолютно недостатній в умовах війни, оскільки він не може запобігти подіям типу «чорний лебідь», якими є воєнні атаки.

Новітня концепція Safety-II пропонує змістити фокус на вивчення того, чому системи працюють успішно переважну більшість часу, навіть за наявності варіативності та складнощів [10, 11]. Вона акцентує на гнучкості та адаптивності персоналу. Цей підхід є більш корисним, оскільки підкреслює важливість людського фактору в адаптації до несподіваних обставин. Проте, він не надає чітких інструментів для протидії цілеспрямованим руйнівним діям.

Найбільш релевантною є концепція Resilience Engineering (Інженерія стійкості), що визначає безпеку як здатність системи адаптуватися та відновлюватися перед лицем непередбачуваних подій. Вона оперує чотирма ключовими здібностями: моніторинг, реагування, передбачення та навчання. Ця концепція є чудовою філософською основою для побудови комплексної безпеки, але її класичні моделі розроблялися для складних соціотехнічних систем (авіація, атомна енергетика) і не враховували специфіку прямого військового впливу на рядові промислові підприємства.

Аналіз нормативно-правової бази України. Аналіз ключових законодавчих актів – Кодексу цивільного захисту України [8] та Закону України «Про охорону праці» [1] – виявляє їхню паралельність. Кожен документ чітко окреслює свою сферу відповідальності, проте механізми їхньої обов'язкової інтеграції на рівні суб'єкта господарювання прописані недостатньо. Це призводить до ситуації, коли на підприємстві є інженер з охорони праці, відповідальний за СУОП, і начальник штабу ЦЗ (або інша відповідальна особа), які звітують різним керівникам, керуються різними планами та проводять окремі навчання. Відсутній єдиний нормативний документ, який би вимагав створення інтегрованої системи управління всіма видами безпекових ризиків.

Огляд сучасних публікацій (після 2022 року). З початком повномасштабного вторгнення з'явилася значна кількість публікацій, присвячених стійкості критичної інфраструктури, енергетичній безпеці та безперервності бізнесу (business continuity) [5, 6, 12–15]. Українські та закордонні автори активно досліджують досвід функціонування економіки в умовах війни. Проте, більшість цих робіт фокусується на макrorівні (держава, галузь) або на аспектах фізичного захисту об'єктів (інженерні укріплення, ППО). Праці, що пропонують комплексну модель управління безпекою саме на корпоративному рівні, поєднуючи філософію ОП та практику ЦЗ, залишаються поодинокими [16].

Виявлення невирішених раніше частин загальної проблеми. На основі проведеного аналізу можна констатувати, що ключовою невирішеною проблемою є відсутність цілісної концептуальної моделі управління комплексною безпекою на рівні підприємства. Більшість існуючих робіт та практичних підходів продовжують розглядати охорону праці та цивільний захист як паралельні, а не глибоко інтегровані системи. Не розроблено єдиної методології оцінки ризиків, яка б органічно поєднувала аналіз виробничих небезпек (напр., за методом FMEA) та воєнних загроз (напр., за методом CARVER). Відсутній системний підхід до інтеграції планів, ресурсів, навчання та управлінських структур, що відповідають за різні аспекти безпеки. Ця стаття покликана заповнити саме цю концептуальну прогалину.

Виклад основного матеріалу дослідження. *Парадигмальний зсув: Від ізольованих систем до єдиного контуру безпеки.* Традиційне розділення безпеки на «виробничу» (охорона праці) та «цивільну» (цивільний захист) є спадком індустріальної епохи мирного часу. Воно ґрунтується на хибному припущенні, що джерела загроз можна чітко розмежувати: внутрішні (технологічні) та зовнішні (природні, військові). В умовах сучасної гібридної війни це розділення не просто застаріло, а стало небезпечним.

Аргументація: Наслідки інцидентів різного походження можуть бути ідентичними. Наприклад, пожежа на підприємстві може бути спричинена як коротким замиканням (проблема ОП), так і влучанням уламків БпЛА (проблема ЦЗ). Руйнування будівлі може статися через вибух газового балону (ОП) або через влучання ракети (ЦЗ). В обох випадках персоналу потрібно знати шляхи евакуації, вміти надавати першу домедичну допомогу та діяти скоординовано. Розділені системи реагування створюють плутанину, дублювання функцій та, як наслідок, втрату дорогоцінного часу.

Тому перехід до концепції *комплексної безпеки* – це стратегічний підхід, що визначає стан захищеності персоналу, матеріальних та нематеріальних активів, а також виробничих процесів підприємства від усього спектру ідентифікованих загроз, незалежно від їхнього походження: виробничих, природних, техногенних, воєнних, соціальних, інформаційних та кібернетичних. Єдиний контур безпеки означає, що всі загрози аналізуються в рамках єдиної системи оцінки ризиків, а заходи з контролю та реагування плануються та управляються з єдиного центру.

Принципи та модель інтегрованої системи управління комплексною безпекою (СУКБ). Для побудови ефективної інтегрованої системи пропонується базуватися на наступних ключових принципах: 1. *Принцип*

єдності управління: Створення єдиного центру відповідальності та прийняття рішень з усіх питань безпеки. Запобігання дублюванню функцій та конфлікту повноважень. 2. *Принцип проактивності:* Перехід від реактивного реагування на інциденти до проактивного прогнозування та запобігання загрозам. Постійний моніторинг безпекового середовища. 3. *Принцип тотальної ризик-орієнтованості:* Інтеграція аналізу воєнних та терористичних ризиків у стандартні процедури оцінки ризиків на робочих місцях. Кожен ризик розглядається з точки зору ймовірності та потенційних наслідків для життя, здоров'я, активів та безперервності діяльності. 4. *Принцип людиноцентризму:* Визнання життя та здоров'я працівника найвищою цінністю. Це включає не лише фізичний захист (укриття, ЗІЗ), але й психологічну підтримку, навчання та формування культури безпеки. 5. *Принцип безперервності та постійного вдосконалення:* СУКБ не є статичним документом, а циклічним процесом (цикл Демінга: Plan-Do-Check-Act), який регулярно переглядається та вдосконалюється на основі отриманого досвіду, навчань та змін у зовнішньому середовищі.

Концептуальна модель СУКБ може бути візуалізована як цикл, що складається з чотирьох взаємопов'язаних підсистем: 1. *Підсистема аналізу та оцінки ризиків:* Єдиний реєстр ризиків, що включає як виробничі небезпеки (падіння, ураження струмом), так і воєнні загрози (ракетний удар, хімічна атака, окупація). Для кожного ризику проводиться оцінка ймовірності та наслідків. 2. *Підсистема превентивних заходів:* Розробка та впровадження заходів для зниження ризиків. *Інтегрований приклад:* укріплення віконних прорізів (ЦЗ) одночасно знижує ризик травмування уламками скла як від вибухової хвилі, так і від внутрішнього технологічного вибуху (ОП). 3. *Підсистема готовності та реагування на інциденти:* Розробка єдиних, комплексних планів реагування, що охоплюють різні сценарії (напр., "повітряна тривога з подальшим загорянням"). Створення універсальних рятувальних формувань, проведення інтегрованих тренувань. 4. *Підсистема відновлення та аналізу досвіду:* Дії після інциденту, спрямовані на відновлення роботи, надання допомоги постраждалим, розслідування причин (незалежно від їх природи) та внесення змін у всі попередні підсистеми для запобігання повторенню.

Стратегії практичної інтеграції цивільного захисту в корпоративне управління.

Нормативно-правова стратегія: розробка та затвердження єдиного корпоративного стандарту – *Положення про комплексну безпеку підприємства*, який замінює собою розрізнені положення про СУОП та плани ЦЗ; оновлення посадових інструкцій: введення обов'язків з ЦЗ для всіх керівників підрозділів, а не лише для окремої особи; інтеграція вимог ЦЗ (дії під час тривоги, правила перебування в укритті) в програми інструктажів з охорони праці; створення єдиної карти (матриці) ризиків підприємства;

Організаційно-управлінська стратегія: реорганізація структур: створення єдиного *Департаменту (або Центру) комплексної безпеки*, який об'єднує фахівців з ОП, пожежної безпеки, ЦЗ, екологічної та кібербезпеки; введення посади *менеджера з комплексної безпеки (Chief Security Officer)*, який підпорядковується безпосередньо першому керівнику підприємства; розробка *інтегрованих планів реагування на надзвичайні ситуації* (напр., план дій у разі хімічного викиду повинен враховувати сценарій, коли викид стався внаслідок ворожого удару, що унеможливило евакуацію за стандартними маршрутами); формування єдиних добровільних формувань (аварійно-рятувальних, пожежних, санітарних), підготовлених до дій у різних умовах.

Техніко-технологічна стратегія: створення *інтегрованої системи оповіщення та зв'язку*, що поєднує сигнали повітряної тривоги, пожежної сигналізації та оповіщення про технологічні аварії; модернізація та обладнання укриттів з урахуванням вимог як ЦЗ (захист від уламків), так і ОП (вентиляція, освітлення, наявність аптечок, запасних виходів); активне застосування цифрових інструментів – GIS-систем для моделювання зон ураження, дронів для моніторингу периметра та оцінки збитків після атак, інтегрованих систем відеоспостереження та контролю доступу.

Соціально-психологічна стратегія: проведення *комплексних, сценарних навчань*, що максимально наближені до реальних умов і поєднують елементи ОП та ЦЗ (напр., евакуація під час "повітряної тривоги" з імітацією задимлення на шляху до укриття); впровадження *програм психологічної підтримки персоналу*, навчання технік управління стресом, тренінги з підвищення стресостійкості (resilience); системне формування *корпоративної культури всеохоплюючої безпеки*, де кожен працівник усвідомлює свою відповідальність не лише за дотримання правил ОП, а й за виконання вимог ЦЗ, розглядаючи це як єдине ціле.

Висновки

1. У ході дослідження було доведено, що традиційна модель роздільного управління охороною праці та цивільним захистом на підприємствах є застарілою та нездатною забезпечити адекватний рівень захисту в умовах повномасштабної війни. Ефективна протидія сучасним гібридним загрозам вимагає фундаментального парадигмального зсуву – переходу до інтегрованої системи управління комплексною безпекою (СУКБ), яка розглядає всі загрози (виробничі, воєнні, природні тощо) в єдиному контурі аналізу, запобігання та реагування.

2. Наукова новизна роботи полягає у тому, що вперше запропоновано *цілісну концептуальну модель інтегрованої системи управління комплексною безпекою (СУКБ) на рівні підприємства*. На відміну від існуючих підходів, які розглядають ОП та ЦЗ як окремі елементи, дана модель синтезує їх в єдиний управлінський цикл (аналіз – превенція – реагування – відновлення), що базується на принципах єдності управління,

проактивності, тотальної ризик-орієнтованості, людиноцентризму та безперервності. Модель адаптована до специфіки функціонування підприємств в умовах гібридних загроз.

3. Розроблені у статті *чотири групи стратегій (нормативно-правова, організаційно-управлінська, техніко-технологічна, соціально-психологічна)* можуть бути використані керівниками та фахівцями з безпеки українських підприємств як методичні вказівки та дорожня карта для реформування існуючих систем. Впровадження запропонованих стратегій дозволить не формально, а реально підвищити рівень захищеності персоналу, мінімізувати потенційні збитки, забезпечити стійкість бізнес-процесів та, найголовніше, зберегти людські життя в умовах воєнного стану.

Перспективи подальших досліджень. Подальший розвиток цієї теми може відбуватися у кількох напрямках. Перспективним є *розробка галузевих моделей СУКБ*, які б враховували специфічні ризики для підприємств енергетики, хімічної промисловості, агросектору, транспорту та ІТ. Іншим важливим напрямком є *створення методики кількісної оцінки рівня комплексної безпеки підприємства*, що дозволить проводити аудит, порівнювати ефективність різних заходів та обґрунтовувати інвестиції в безпеку.

Список використаних джерел:

1. Про охорону праці : Закон України від 14.10.1992 р. № 2694-XII. *Відомості Верховної Ради України*. 1992. № 49. Ст. 668. URL: <https://zakon.rada.gov.ua/laws/show/2694-12>
2. Левченко О. Г., Бахрушин В. Е., Соколов М. М. Охорона праці та цивільний захист: підручник. Київ: КПІ ім. І. Сікорського. 2019. 420 с. URL: https://ela.kpi.ua/bitstream/123456789/26895/1/OP_ta_TsZ_pidruchnyk.pdf
3. Желібо Є. П., Заверуха Н. М., Зацарний В. В. Безпека життєдіяльності : підручник. Київ : Каравела, 2017. 320 с. URL: <https://xn--elajqk.kiev.ua/wp-content/uploads/2019/12/ZHelibo-Bezpeka-ZHitt-diyalnosti-2008.pdf>
4. Пащенко О. В., Перкун І. В., Погребняк В. Г. Підвищення безпеки праці при проведенні гідроструминної водополімерної перфوراції свердловин. *Системи та технології*. 2025. Vol. 69, No.1, 176–186. <https://doi.org/10.32782/2521-6643-2025-1-69.21>
5. Вплив війни на соціально-економічні системи: безпековий аспект: колективна монографія за заг. ред. д.е.н., проф. М.І. Копитко., д.ю.н., проф. З.Р. Кісіль. Львів: ЛьвДУВС, 2024. 394 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7280/1/%D0%9C%D0%BE%D0%BD%D0%B%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%92%D0%9B%D0%98%D0%92%D0%92%D0%86%D0%99%D0%9D%D0%98.pdf
6. Про організацію трудових відносин в умовах воєнного стану: Закон України від 15.03.2022 р. № 2136-IX. URL: <https://zakon.rada.gov.ua/laws/show/2136-20#Text>
7. Радецький І. І., Горобинський С. В., Костанян В. Р. і ін. Удосконалення системи управління безпеки виробництва підприємств нафтогазового комплексу. *Нафтова і газова промисловість*, 2012. № 6. С. 16–20.
8. Кодекс цивільного захисту України: Закон України від 02.10.2012 р. № 5403-VI. URL: <https://zakon.rada.gov.ua/laws/show/5403-17#Text>
9. Ібрагім Умар, Тімоті О. І., Адеремі Адехумо, Аввал М. Г. Assessing The Use of AI for Improving Safety and Performance for Building Construction Workers. *Nile Journal of Engineering and Applied Science*. 2024. No. 2(1). P. 1–10. <https://doi.org/10.5455/NJEAS.189076>
10. Badri A., Boudreau-Trudel B., Souissi A. S. Occupational Health and Safety in the Industry 4.0 Era: A Cause for Major Concern? *Safety science*. 2018. Vol. 109. P. 403–411. <https://doi.org/10.1016/j.ssci.2018.06.012>
11. Hale A., Guldenmund F. Safety 4.0: The role of new digital technologies in occupational safety. *Safety Science*. 2022. Vol. 150. Art. no. 105697.
12. Суходоля О. М., Харазішвілі Ю. М., Рябцев Г. Л. Енергетична безпека України: перспективна модель управління ризиками: монографія за ред. О. М. Суходолі. Київ: НІСД, 2023. 152 с. <https://doi.org/10.53679/NISS-book.2023.01>
13. Енергетична безпека України: стан та шляхи зміцнення: аналітична доповідь / Центр Разумкова. 2024. URL: <https://razumkov.org.ua/novyny/energetychna-bezpeka-ukrayiny-standa-shliakhy-zmitsnennya>
14. Робота під тиском війни: важливі інсайти з дослідження психічного здоров'я працівників в Україні / Robota.ua. 2025. URL: https://budni.robota.ua/hr/robota-pid-tiskom-viyni-vazhliivi-insayti-z-doslidzhennya-psihichnogo-zdorov_ya-pratsivnikiv-v-u
15. Safety and Health at Work [Electronic resource] / International Labour Organization. 2024. URL: <https://www.ilo.org/media/67566/download>
16. Погребняк В. Г., Кондрат О. Р. Перкун І. В., Погребняк А. В. Моделювання професійних і воєнних ризиків в системі безпеки праці та цивільного захисту на об'єктах нафтогазової галузі. *Прикарпатський вісник НТШ. Число*. 2025. № 20 (77). 9 с.

References:

1. Pro okhoronu pratsi [On labor protection]. (1992). *Vidomosti Verkhovnoi Rady Ukrainy*, 49, 668. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2694-12>
2. Levchenko, O. H., Bakhrushyn, V. E., & Sokolov, M. M. (2019). *Okhorona pratsi ta tsyvilnyi zakhyst: pidruchnyk* [Occupational safety and civil defense: textbook]. KPI im. I. Sikorskoho. Retrieved from: https://ela.kpi.ua/bitstream/123456789/26895/1/OP_ta_TsZ_pidruchnyk.pdf
3. Zhelibo, Ye. P., Zaverukha, N. M., & Zatsarnyi, V. V. (2017). *Bezpeka zhyttiediialnosti: pidruchnyk* [Life safety: textbook]. Karavela. Retrieved from: <https://xn--elajqk.kiev.ua/wp-content/uploads/2019/12/ZHelibo-Bezpeka-ZHitt-diyalnosti-2008.pdf>
4. Pashchenko, O. V., Perkun, I. V., & Pohrebniak, V. H. (2025). Pidvyshchennia bezpeky pratsi pry provedenni hidrostrumynnoi vodopolimernoi perforatsii sverdlolvyn [Improving occupational safety during hydro-jet water-polymer perforation of wells]. *Systemy ta tekhnolohii*, 69(1), 176–186. <https://doi.org/10.32782/2521-6643-2025-1-69.21>
5. Kopytko, M. I., & Kisil, Z. R. (Eds.). (2024). Vplyv viiny na sotsialno-ekonomichni systemy: bezpekovi aspekt: kolektyvna monohrafiia [The impact of war on socio-economic systems: the security aspect: a collective monograph]. LvDUVS. Retrieved from: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7280/1/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%92%D0%9F%D0%9B%D0%98%D0%92%20%D0%92%D0%86%D0%99%D0%9D%D0%98.pdf
6. Pro orhanizatsiiu trudovykh vidnosyn v umovakh voiennoho stanu [On the organization of labor relations under martial law] (Zakon Ukrainy No. 2136-IX). (2022, March 15). Verkhovna Rada Ukrainy. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2136-20#Text>
7. Radetskyi, I. I., Horobynskyi, S. V., Kostanian, V. R., et al. (2012). Udoskonalennia systemy upravlinnia bezpeky vyrobnytstva pidpriemstv naftohazovoho kompleksu [Improving the safety management system for production at oil and gas complex enterprises]. *Naftova i hazova promyslovist*, (6), 16–20. [in Ukrainian].
8. Kodeks tsyvilnoho zakhystu Ukrainy [Civil Protection Code of Ukraine] (Zakon Ukrainy No. 5403-VI). (2012, October 2). Verkhovna Rada Ukrainy. Retrieved from: <https://zakon.rada.gov.ua/laws/show/5403-17#Text>
9. Umar, I., O. I., T., Adehumu, A., & M. G., A. (2024). Assessing The Use of AI for Improving Safety and Performance for Building Construction Workers. *Nile Journal of Engineering and Applied Science*, 2(1), 1–10. <https://doi.org/10.5455/NJEAS.189076>
10. Badri, A., Boudreau-Trudel, B., & Souissi, A. S. (2018). Occupational Health and Safety in the Industry 4.0 Era: A Cause for Major Concern? *Safety Science*, 109, 403–411. <https://doi.org/10.1016/j.ssci.2018.06.012>
11. Hale, A., & Guldenmund, F. (2022). Safety 4.0: The role of new digital technologies in occupational safety. *Safety Science*, 150, Article 105697. <https://doi.org/10.1016/j.ssci.2022.105697>
12. Sukhodolia, O. M., Kharazishvili, Yu. M., & Riabtsev, H. L. (2023). *Enerhetychna bezpeka Ukrainy: perspektyvna model upravlinnia ryzykamy: monohrafiia* [Energy security of Ukraine: a promising risk management model: monograph] (O. M. Sukhodolia, Ed.). NISD. <https://doi.org/10.53679/NISS-book.2023.01>
13. Tsentrazumkova. (2024). Enerhetychna bezpeka Ukrainy: stan ta shliakhy zmitsnennia: analitychna dopovid [Energy security of Ukraine: state and ways to strengthen: analytical report]. Retrieved from: <https://razumkov.org.ua/novyny/energetychna-bezpeka-ukrayiny-stan-ta-shliakhy-zmitsnennia>
14. Robota.ua. (2025). Robota pid tyskom viiny: vazhlyvi insaity z doslidzhennia psykhichnoho zdorovia pratsivnykiv v Ukraini [Work under the pressure of war: important insights from a study of the mental health of workers in Ukraine]. Retrieved from: <https://budni.robota.ua/hr/robota-pid-tyskom-viyni-vazhlyvi-insayti-z-doslidzhennia-psyhichnogo-zdorov-ya-pratsivnykiv-v-u>
15. International Labour Organization. (2024). *Safety and Health at Work*. Retrieved from: <https://www.ilo.org/media/67566/download>
16. Pohrebniak, V. H., Kondrat, O. R., Perkun, I. V., & Pohrebniak, A. V. (2025). Modeliuvannia profesiinykh i voiennykh ryzykiv v systemi bezpeky pratsi ta tsyvilnoho zakhystu na ob'ektakh naftohazovoi haluzi [Modeling of professional and military risks in the system of labor safety and civil protection at oil and gas facilities]. *Prycarpatskyi visnyk NTSh. Chyslo*, 20(77), 9. [in Ukrainian].

Дата надходження статті: 03.10.2022

Дата прийняття статті: 10.11.2025

Опубліковано: 30.12.2025