№ 2(32) 2025

НАУКОВИЙ ВІСНИК
Івано-Франківського національного технічного університету нафти і газу
СЕРІЯ
Економіка та управління в нафтовій і газовій промисловості

ISSN 2409-0948 print
ISSN 2415-3311 online

https://eung.nung.edu.ua

Прийнято 04.10.2025. Прорецензовано 16.11.2025. Опубліковано 31.12.2025.

УДК 65.01(075.8): 338.4
JEL H12, H56, O14
DOI: 10.31471/2409-0948-2025-2(32)-21-38

АДАПТИВНА МОДЕЛЬ ВИРОБНИЧОЇ БЕЗПЕКИ В СИСТЕМІ СИТУАЦІЙНОГО УПРАВЛІННЯ

Полянська Алла Степанівна*
Доктор економічних наук, професор кафедри менеджменту та адміністрування
Івано-Франківський національний технічний університет нафти і газу
76019, Івано-Франківськ, вул. Карпатська, 15
e-mail: alla.polianska@nung.edu.ua
Orcid id: http://orcid.org/0000-0001-5169-1866

Микитюк Олег Романович
Аспірант кафедри менеджменту та адміністрування
Івано-Франківський національний технічний університет нафти і газу
76019, Івано-Франківськ, вул. Карпатська, 15
E-mail: oleg.mykytiuk75@gmail.com
Orcidid: https://orcid.org/0009-0008-3732-4582

Анотація. У статті розглянуто теоретично-методичні засади управління виробничою безпекою підприємства в умовах ситуаційного управління. Обґрунтовано, що сучасна модель управління виробничою безпекою є адаптивною, оскільки має враховувати вимоги внутрішнього і зовнішнього середовища. Розглянуто та представлено інтегровану систему виробничої безпеки, яку потенційно може використовувати підприємство, що охоплює стандарти та системи та визначає їх роль в управління виробничою безпекою. Розроблено концептуально-аналітичну модель ситуаційного управління виробничою безпекою (МСУВБ), яка диференціює підходи до ризик-менеджменту, стійкості та реагування у воєнний період, у фазі переходу та під час післявоєнного відновлення. Модель складається із 3-х рівнів – ситуаційного, операційного та блоку стратегічної адаптації. Інтегрована у модель адаптивна зона управління в середині операційного блоку об'єднує безпеку, безперервність і стійкість, переводячи рішення з реактивних у проактивні, закриває зворотний зв'язок контуром навчання. Методологічний каркас становлять вимоги системи управління безперервністю бізнесу на основі традиційних та сучасних міжнародних та вітчизняних стандартів управління безпекою. Запропоновано чотири етапну

Запропоноване посилання: Полянська, А. С. & Микитюк, О. Р. (2025). Адаптивна модель виробничої безпеки в системі ситуаційного управління. Науковий вісник ІФНТУНГ. Серія: економіка та управління в нафтовій і газовій промисловості, 2(32), 21-38. doi: 10.31471/2409-0948-2025-2(32)-21-38

* Відповідальний автор

процедуру управління виробничою безпекою на основі ідентифікації зовнішніх та внутрішніх чинників і слабких сигналів для трьох часових фаз; визначення критичних процесів і порогів впливу з оцінюванням ризиків; проєктування МСУВБ із виділенням етапів «дані-моделі-правила-рішення-KPI-зворотний зв'язок» з наборами дій для кожної фази; обґрунтування стилів керівництва у логіці ситуативного лідерства Херсі-Бланшара. На основі опрацювання теоретичних концепцій безпеки розглянуто схему управління виробничою безпекою за слабкими сигналами, яка складається із послідовних етапів, що дозволяють управляти виробничою безпекою на основі послідовного циклу обробки даних із урахуванням відхилень та ескалацій, що у підсумку робить процес управління прозорим, зрозумілим та керованим. Запропоновано поєднання управління за слабкими сигналами з циклом управління безперервністю бізнесу, що спирається на міжнародні стандарти якості та прив'язано із ситуаційними стилями керівництва відповідно до часових зрізів «війна-перехід-відновлення».

Ключові слова: виробнича безпека, безперервність бізнесу, слабкі сигнали, ситуаційні стилі керівництва, стандарти, адаптивність.

Вступ. Війна створює безпрецедентні виклики для промислових систем. Умови постійних ризиків – фізичних (ракетні обстріли, вибухи), логістичних (розриви поставок), кібернетичних та кадрових – формують новий контекст виробничої безпеки, у якому традиційні системи менеджменту безпеки виявляються недостатньо гнучкими. У період воєнних дій ключовим завданням є забезпечення операційної безперервності, швидкого реагування та захисту критичної інфраструктури, тоді як у післявоєнний період пріоритет зміщується до відновлення, модернізації та створення стійких виробничих систем.

Сучасні системи управління виробничою безпекою (ВБ) доцільно розглядати як адаптивні, оскільки вони працюють за циклом PDCA (Plan-Do-Check-Act), спираються на ризик-орієнтований підхід та інтегрують безперервне вдосконалення, управління змінами й урахування контексту організації – саме так структуровано вимоги ISO 45001 (в Україні – ДСТУ ISO 45001:2019). Стандарт вимагає ідентифікувати небезпеки, оцінювати ризики та можливості, визначати контрольні заходи, а далі – перевіряти результативність і коригувати дії, що і формує адаптивний контур управління безпекою. Традиційні практики доповнюються практиками динамічної оцінки ризиків та стійкості, а в умовах війни рекомендації прямо вимагають адаптації процедур, робочих місць і планів реагування. Паралельно до «класичної» безпеки дедалі ширше застосовується логіка побудови стійких процесів, здатних працювати у змінному середовищі, з фокусом на тому, як і чому речі зазвичай «йдуть добре», і як підсилити таку продуктивну варіативність. Цей підхід стимулює практики динамічної оцінки ризиків, для прикладу раннє виявлення слабких сигналів, передбачувальна аналітика, навчання з інцидентів, доповнюючи вимоги ISO 45001 і переводячи безпеку від суто реактивної до проактивної.

В українському контексті воєнний стан поставив вимогу адаптувати процедури ВБ до умов підвищених загроз у формі переміщення персоналу, укриття, зміни режимів роботи, додаткових інструктажів, особливої оцінки ризиків. Офіційні роз'яснення Держпраці [1] наголошують на оновленні інструкцій, планів реагування та організації безпечного доступу та евакуації – тобто на пристосуванні систем безпеки до ситуації та швидкому зворотному зв'язку. Це безпосередньо корелює з адаптивною логікою PDCA й сучасними підходами до управління безпекою.

Узагальнюючи, адаптивність сучасних систем управління ВБ – це результат взаємодії нормативної «рамки» ISO 45001 (PDCA, ризик-орієнтація), проактивної парадигми управління безпекою на основі передбачення, навчання, стійкість до збурень та вимог політики міжнародних організацій і національних настанов. Така конфігурація дозволяє підприємствам у реальному часі перебудовувати контроль, підтримувати безперервність і керувати ризиками навіть у високо волатильних умовах, водночас зберігаючи доказову відповідність стандартам.

Таким чином, розробка адаптивних моделей ситуаційного управління, що враховують обидва етапи – воєнний і післявоєнний, є необхідною умовою ефективного відновлення промислового потенціалу України та інтеграції у європейські безпекові та екологічні стандарти. Відтак, тема є актуальною і на часі.

Аналіз публікацій з досліджуваної проблематики. На сьогодні проблема безпекових питань, особливо у сфері виробництва займає вагоме місце у публікаціях вітчизняних і зарубіжних науковців. Комплексний огляд ризиків для економіки у воєнний час щодо макрофінансової стійкості, енергетичної безпеки, критичної інфраструктури, із системою політичних рекомендацій проведено Національним інститутом стратегічних досліджень, із розробленням Базового рамкового документу для обґрунтування пріоритетів політики та індикаторів безпеки [2]. Оновлене картування макро-, фінансові, енергетичні, інфраструктурні ризиків та сценарії їх розв'язання у 2026-2028 [3] досліджено у джерелі.

У статті Братель С. Г. [4] розглядається поняття «критичної інфраструктури» як сукупності ключових елементів, а також персоналу, який ними управляє, від справної та захищеної роботи яких залежить безперервне надання основних послуг. Їх втрата, пошкодження або компрометація здатні спричинити суттєві порушення доступності та цілісності виробничих і сервісних функцій, що, у свою чергу, може призвести до значних людських втрат, масштабних економічних чи соціальних наслідків і навіть вплинути на національну безпеку та функціонування держави. Тому безпека підприємства, яке експлуатує такі елементи, має розглядатися як інтегрована система управління ризиками, що поєднує виробничу безпеку, фізичний захист, кібербезпеку середовища, надійність та безперервність бізнесу, кадрову безпеку (захист ключових компетенцій) і управління ланцюгами постачання. У праці Гарькави В. розглядається методологія регіональної економічної безпеки, індикатори дисбалансва та ризиків [5]. Правовий аналіз повноважень і механізмів публічної влади під час воєнного стану, розуміння інституційної спроможності впроваджувати антикризові енергетичні заходи розглядається у статті Глущенко О. [6]. У праці [7] проаналізовано основні проблеми системи виробничої безпеки в Україні. Обґрунтовано, що формування системи виробничої безпеки сприяє не лише збереженню життя і здоров'я працівників, а й підвищенню продуктивності праці, зниженню витрат, покращенню репутації підприємств. У статті стан виробничої безпеки характеризується динамікою виробництва, ступенем зносу основних засобів, рентабельністю операційної діяльності й ефективністю діяльності підприємств за ключовими видами економічної діяльності [8]. Дослідження ВБ доповнено напрацюваннями Каплі О. [9], який розглядає механізми правового захисту та соціально-економічні гарантії громадян; релевантно для оцінки впливу тарифної політики та доступності енергії на добробут домогосподарств; розглядається економічна безпека громадянина, як складова забезпечення безпеки держави в умовах воєнного стану. Як висновок, представлено економічну безпеку громадян, як загальну категорію, що ні нормативно, ні теоретично не врегульована. Запропоновано теоретичну конструкцію поняття економної безпеки громадянина, як індикатору, який характеризує стан економічного розвитку країни. Козак С. у контексті дослідження сучасних проблем виробничої безпеки досліджує ситуацію з виробничим травматизмом у галузі у довоєнний період та аналізує втрати сектору та екології внаслідок бойових дій [10]. Узагальнені інструменти та процеси управління економічною безпекою на рівні підприємства проаналізовано у статті [11], зокрема ідентифікація ризиків, моніторинг, профілактика загроз; запропоновано методичний фундамент для мікрорівневих кейсів управління безпекою підприємства. Значна увага приділена оцінюванню ризиків як важливого елементу управління безпекою, що розглядається у статті [12] . Таким чином, вітчизняні науковці різнобічно та диверсифіковано розглядають питання безпеки.

У дослідження питання безпеки вагомий внесок зробили зарубіжні наковці. У контексті розвідок у питанні ВБ заслуговує на увагу напрацювання понять та харакетристик безпеки Еріком Холнаґелем, який розглядає два рівні безпеки. Зокрема Безпека-I (Safety-I) – безпека як мінімізація того, що йде не так; управління здебільшого реактивне, яке передбачає реагування на інциденти та невідповідності та пошук «помилок й відмов» й усунення їхніх причин; людина розглядається як джерело ризику, яке треба «виправити»; оцінка ризиків зосереджена на збоях і відмовах. Безпека-II (Safety-II) – безпека як максимізація того, що йде правильно щодня; управління проактивне шляхом передбачення подій, конструювання умов для надійної роботи, навчання з «успіхів»; людина – ресурс гнучкості та стійкості, який адаптує систему, а оцінка ризиків вивчає варіативність виконання і межі її контрольованості [13] .

Заслуговує на увагу праця С. Деккера «The Field Guide to Understanding Human Error» [14] для дослідження виробничої безпеки. Деккер у пропонує «новий погляд» на людську помилку, а саме помилка – не «причина», а симптом системних умов, та формулює принцип локальної раціональності, який говорить про те, що люди роблять те, що здавалося розумним у той момент, з їхніми цілями, інформацією, інструментами й обмеженнями. Замість «першої історії» у формі короткого опису з винуватцем і порушеною інструкцією він закликає будувати «другу історію» – відтворювати як робота реально виконується під тиском часу, ресурсних обмежень, суперечливих цілей і неоднозначних сигналів, та порівнювати її з тим, як керівництво уявляє процес. Ключові поняття, які виділяє науковець розглядають повільне накопичення відхилень, що стають «нормою», балансування ефективністю та ретельністю, роль організаційних бар'єрів і обмежень політики, планування та, ресурси проти операторів діяльності. Для управління безпекою пропонується культура справедливості, яка апелює до зміщення від покарання до навчання, прозорих меж відповідальності й стимулювання повідомлень про інциденти.

Таким чином, беручи до уваги визначення безпеки виробничого процесу як здатності відповідати вимогам безпеки праці під час його проведення в умовах, встановлених нормативно-технічною документацією [15], зазначимо що в сучасних умовах традиційні погляди на управління ВБ, а також регулюючі нормативи та документи не завжди враховують обставини і ситуації, у яких знаходяться підприємства. Не достатньо досліджено впровадження сучасних методик управління виробничими ризиками та визначено роль керівника відповідно до міжнародного досвіду, розроблених стандартів та нормативних актів.

Мета і завдання дослідження – розробити концептуально-аналітичну модель ситуаційного управління виробничою безпекою, яка диференціює підходи до управління ризиками, стійкістю та реагуванням у воєнний період і в період післявоєнного відновлення, з урахуванням впливу зовнішнього середовища, інституційних змін та технологічних обмежень. Для досягнення мети передбачено вирішення таких завдань: визначити ключові чинники і типи ризиків виробничої безпеки у воєнний і післявоєнний періоди; побудувати класифікацію сценаріїв управління безпекою за ступенем загроз і доступністю ресурсів; розробити адаптивну ситуаційну модель прийняття управлінських рішень у системі виробничої безпеки; запропонувати матрицю відповідності управлінських дій у фазах війна-відновлення, яка узгоджується з міжнародними стандартами BCM (Business Continuity Management) і ризик менеджментом.

Методологія дослідження. Дослідження побудовано на каркасі Системи управління безперервністю бізнесу (ISO 22301:2019) [16] із залученням ISO 31000 (ризики) [17], ISO 22317/22331 (стратегії безперервності) та ISO 22320/22361 [18] (управління інцидентами та кризами) з метою створити концептуальну модель ситуаційного управління виробничою безпекою (МСУВБ), яка розрізняє воєнну, перехідну та післявоєнну фази.

Метод включає чотири кроки:

– ідентифікація зовнішніх і внутрішніх чинників, зокрема воєнні загрози, логістика, мережеві та кадрові обмеження, зацікавлених сторін і політики безперервності, що формують карти ризиків та слабкі сигнали для трьох часових фаз;

– визначення критичних процесів, порогів впливу та проведення оцінювання ризиків за ISO 31000 з використанням інструментів аналізу ризиків; результатом є класифікація сценаріїв управління;

– проєктування МСУВБ: впроваджується цикл «дані-моделі-правила-рішення-KPI-зворотний зв'язок»; для кожного сценарію готуються описи дій: реактивні (війна), адаптивні (перехід), проактивні стратегічні (відновлення);

– обґрунтування вибору стилів керівництва для різних часових зрізів (війна, перехід, післявоєнне відновлення) у логіці ситуаційного лідерства Херсі-Бланшара.

Основний матеріал. Адаптивні моделі ВБ в системах ситуаційного управління для воєнних умов і післявоєнного відновлення доцільно розуміти як поєднання класичних контурів управління ризиками, що базуються на ідентифікації, оцінюванні, реагуванні, моніторингу ситуацій із реальним середовищем, яке постійно підживлюється даними з виробничих і мережевих систем, а також з ринкових та інфраструктурних джерел.

У табл. 1 представлено інтегровану систему ВБ, яку потенційно може використовувати підприємство.

На рівні методології така постановка спирається на міжнародні стандарти управління ризиками ISO 31000 та системи охорони праці ISO 45001, а для надзвичайних і конфліктних ситуацій – на рекомендації МОП щодо безпеки праці в умовах надзвичайних подій. Це зміщує акцент із «розробити план і виконати» на «спостерігати-передбачати-адаптуватися», коли індикатори небезпеки та ефекту контрзаходів постійно переоцінюються, а правила переходу між режимами (нормальна експлуатація, підвищена готовність, кризовий режим) формалізовані й прозорі для людини, яка приймає рішення [19, 20].

Ситуаційне управління в діяльності підприємств під час війни та відбудови додає до традиційних виробничих ризиків гібридні, зокрема цілеспрямовані пошкодження інфраструктури, тривалі збої в енергопостачанні, порушення ланцюгів поставок, а також кіберфізичні атаки. Тому адаптивна модель обов'язково включає кібербезпеку виробничої автоматизації і бізнес-безперервність, а також використовує «систему гарантованої адекватності» для планування резервів і гнучкості. Вона поєднує прогнозні моделі із урахуванням навантаження, ВДЕ, відмов, загроз з оптимізаційними через диспетчеризацію, аварійне відновлення, ізоляцію та переорієнтацію мережі та системами керування правилами та нормами від охорони праці до обмежень вибухопожежної та електробезпеки. Таким чином, у кризових сценаріях рішення ухвалюються за участі людини, коли алгоритм пропонує, експерт затверджує, система фіксує підстави на основі даних, ризик-індикаторів, нормативних посилань і запускає виконання з телеметричним підтвердженням [21].

Різновиди виробничої безпеки, які має охоплювати така адаптивна система, включають щонайменше:

– безпеку та гігієну праці (OSH) – організаційні та технічні заходи за ISO 45001/МОП-рекомендаціями;

– процесну та функціональну безпеку – запобігання аваріям технологічних процесів через бар'єри та захисні функції (IEC 61511/IEC 61508);

– вибухопожежну безпеку – вимоги ATEX до середовищ і обладнання (2014/34/EU, 1999/92/EC);

– електробезпеку й оперативну надійність – критерії N-1, резерви, планові відключення;

Таблиця 1 – Інтегрована система виробничої безпеки: стандарти, методи, сучасні платформи

Стандарт / система	Призначення	Ключові елементи	Роль у виробничій безпеці
SMS (Safety Management System)	Загальна система управління безпекою на рівні організації	Політика, ролі та відповідальність, ідентифікація небезпек, оцінка ризиків, контроль/бар'єри, навчання, аудит, постійне вдосконалення	«Парасолька» над усіма процесами безпеки; забезпечує цикл PDCA та культуру безпеки
ISO 45001:2018 (OHSMS)	Охорона праці та безпека здоров'я працівників	Контекст організації, лідерство, планування ризиків/можливостей, підтримка, операції, оцінювання результативності, удосконалення	Знижує травматизм, формалізує управління ризиками ОП, посилює участь персоналу
ISO 31000:2018	Загальні принципи та рамка управління ризиками	Принципи, процес (встановлення контексту - ідентифікація - аналіз - оцінка - обробка ризику), комунікація та моніторинг	Єдина методологія ризик-менеджменту для всіх підрозділів; узгоджує критерії ризику
IEC 61511	Функціональна безпека систем, що зменшують ризик (SIS) у хімічній/нафтохімічній галузях	Аналіз небезпек, визначення визначення рівня цілісної безпеки (SIL), проектування та валідація інструментованої системи безпеки (SIS), управління життєвим циклом, випробування	Забезпечує цільовий рівень зниження ризику (SIL) для критичних сценаріїв; мінімізує тяжкі інциденти
OSHA 29 CFR 1910.119 / CCPS RBPS	Процесна безпека на небезпечних виробництвах	14 елементів процесної безпеки (PSM) та 4 стовпи небезпечних виробництв (RBPS): зобов'язання, розуміння небезпек, керування ризиками, навчання	Запобігає вибухам та викидам; задає вимоги до процедур, змін, компетенцій
IEC 62443	Кібербезпека АСУ ТП (IACS)	Моделі зон/каналів, рівні безпеки, вимоги до компонентів і процесів	Захист операційних технологій від кібератак, що можуть спричинити інциденти безпеки
ISO 13849 / IEC 62061	Функціональна безпека машин	PL/SIL для машин, аналіз режимів відмов	Зменшує ризики травм на обладнанні
ISO 55001 (Управління активами – Asset Management)	Керування активами життєвого циклу	Політика, стратегії та плани, ризик-базоване технічне обслуговування і ремонт (тоір), показники	Знижує аварійність через зрілу стратегію тоір і капітальні рішення
ISO 50001 (Енергетичний менеджмент – Energy Management)	Енергоменеджмент і ефективність	Політика, цілі, енергетичний огляд, показники енергетичної ефективності (enpi), контроль операцій	Опосередковано знижує ризики (навантаження, перегрів, аварійні режими)

Продовження таблиці 1

Стандарт / система	Призначення	Ключові елементи	Роль у виробничій безпеці
ISO 22301 (BCMS)	Безперервність бізнесу	Аналіз впливу на бізнес, стратегії відновлення, плани реагування	Підтримує стійкість до збоїв та катастроф, враховуючи OHS та процесну безпеку
Safety-II та Інженерія стійкості – Resilience Engineering	Сучасна парадигма: фокус на здатності системи успішно працювати	Передбачення, моніторинг, реагування, навчання	Будує спроможність виявляти та гасити «слабкі сигнали», зменшує частку важких інцидентів
STAMP та STPA (стемно-теоретична модель управління безпекою та системно-теоретичний аналіз процесів)	Системно-теоретична модель причинності й аналіз небезпек	Обмеження керування, петлі зворотного зв'язку, метод аналізу безпеки (STPA)	Виявляє нелінійні/організаційні причини інцидентів
Barrier та Bow-Tie Management (управління бар'єрними захистами та управління ризиками методом «метелик»)	Керування бар'єрами та сценаріями	Загроза - подія - наслідки; запобіжні та пом'якшувальні бар'єри	Візуалізація та контроль стану бар'єрів у щоденній роботі
APM (управління ефективністю активів) та CBM (технічне обслуговування за станом) - платформи (iiot (промисловий інтернет речей), pdm (попереджувальне обслуговування), Digital Twin (цифровий двійник)	Прогнозна стан-орієнтована підтримка тоір	Віброаналіз, термографія, ML (машинне навчання) - прогнози відмов, цифрові двійники	Раннє попередження відмов, скорочення аварій і часу простою

Джерело: сформовано авторами на основі [16-28]

– кібербезпеку OT/ICS – сегментація, керування доступом, моніторинг аномалій за NIS2/IEC 62443/NIST SP 800-82;

– екологічну безпеку – контроль викидів, управління відходами, взаємодія з довкіллям у логіці систем екологічного менеджменту;

– безперервність бізнесу та відновлення – планування відновлення критичних функцій, взаємодія зі стейкхолдерами, тренування персоналу (ISO 22301).

Усі ці домени зводяться в єдину «панель рішень», де кожна подія чи відхилення автоматично прив'язане до нормативної бази, карти ризиків і сценаріїв реагування [22].

Окремого висвітлення потребує характеристика системи ВБ у сфері енергоефективності в будівництві, адже масштабні реновації та «зелене» оновлення фонду будівель підпадають під Європейську директиву з енергоефективності (EED 2023/1791) [23] та оновлену Директиву про енергетичні характеристики будівель (EPBD, 2024/1275) [24]. Технічні рішення для зниження енерговитрат (термомодернізація, BACS/автоматизація будівель, акумулювання енергії, електрифікація тепла) мають впроваджуватися із суворим дотриманням безпеки будівельних майданчиків (Директива 92/57/EEC) [25], вимог до вентиляції та мікроклімату, а також з урахуванням пожежних і електробезпекових ризиків, пов'язаних із системами зберігання енергії та новими матеріалами. Корисним орієнтиром є положення Регламенту ЄС про батареї (2023/1542) щодо безпеки, стійкості й циркулярності батарейних систем. Енергоефективність як управлінський процес повинна базуватися на ISO 50001 [26] (системи енергоменеджменту) та оцінювати енергетичну результативність будівель доцільно за сімейством стандартів з енергоефективності будівель, зокрема за стандартом ISO 52000-1. Для автоматизації й керування будівлею слід орієнтуватися на європейський стандарт EN 15232-1, який прямо показує, як рівень розвитку систем автоматизації та керування впливає на споживання енергії й комфорт користувачів. Усі зазначені норми інтегруються в «цифровий паспорт» об'єкта й у правила системи, щоб кожне рішення з реновації проходило перевірку на безпечність, придатність до експлуатації, відповідність мікрокліматичним вимогам і енергорезультативність. Зазначені технології та нормативні акти їх регулювання формують основу операційної діяльності та дозволяють генерувати дані за результатами для безперервного підтримання належного рівня безпеки. Подібно до викладеного прикладу, будь-яке підприємство вибирає стандарти, методи, сучасні платформи управління ВБ.

У воєнних умовах адаптивність забезпечує багатоканальне спостереження: крім промислових датчиків і систем диспетчерського керування та збору даних, постійно відстежуються руйнування, дефіцити пального, кіберінциденти й стан міжсистемних електричних з'єднань. У післявоєнний період головними стають показники відновлення основних фондів, пріоритети реконструкції та узгодження роботи з європейськими енергоринками. Це поєднується з цифровізацією: застосуванням прогнозних моделей, «цифрових двійників» і сценарного планування, що спирається на правила та оцінки адекватності, які готує Європейська мережа операторів систем передачі електроенергії, а також на акти ЄС щодо кіберстійкості критичної енергетичної інфраструктури. Оновлена Директива ЄС про безпеку мереж і інформаційних систем встановлює жорсткіші вимоги до кіберзахисту «суттєвих» і «важливих» операторів енергетики, тож включення її вимог до виробничих регламентів є обов'язковою умовою, а не опцією [27].

Практична архітектура систем ВБ узагальнює їх як безперервний цикл «дані-моделі-правила-рішення-KPI-зворотний зв'язок». Дані з операційних та інформаційних технологій і ринків очищуються та уніфікуються; моделі (прогноз навантаження/ВДЕ, оцінка ймовірності відмов, аналіз сценаріїв пошкоджень/каскадів, оптимізація режимів і планів відновлення) постачають оцінені ризики; «rule-engine» кодує норми ISO/IEC/EU-директив і корпоративні інструкції; рішення охоплюють диспетчерські дії, протиаварійні заходи, будівельно-монтажні операції та інвестиційні програми; KPI для охорони праці, кількісні метрики процесної безпеки, надійності, CO_2/кВт.год для екології, показники енергоефективності/EPB для будівель) «замикають» цикл і автоматично коригують моделі й правила. Завдяки цьому організація переходить від реактивного до проактивного управління, скорочує час реагування, підвищує прозорість і підзвітність рішень, а головне – поєднує цілі безпеки, надійності та енергоефективності в єдиному керованому контурі.

З позицій відбудови України така система дозволяє поєднати вимоги європейського права зі специфікою роботи в умовах підвищених загроз, коли пріоритет надається гнучкості, модульності та швидкій перевірці рішень на відповідність безпеці праці,

процесній і вибухопожежній безпеці, кіберстійкості й екологічності. У будівельному секторі – де реалізуватиметься основна частина «хвилі реновації» – це означає строго інтегрувати вимоги безпеки будмайданчиків, мікроклімату та пожежної безпеки з енергетичними цілями, а також застосовувати системи енергоменеджменту ISO 50001 для установлення цілей, контролю виконання та постійного поліпшення. Такі адаптивні моделі виробничої безпеки роблять політику та інвестиції відчутно керованішими, а ризики – вимірними й такими, що зменшуються завдяки даним, стандартам і дисципліні виконання. [28]

У статті запропонована концептуальна модель ситуаційного управління ВБ (МСУВБ) (рис. 1). Загальна ідея моделі виходить із принципу, що управління безпекою є ситуаційним процесом, який постійно адаптується до зміни контексту (війна, криза, стабілізація, відновлення). Вона об'єднує три взаємопов'язані домени:

– безпека (технічна безпека, запобігання інцидентам);
– безперервність (операційна безперервність, підтримання ключових процесів);
– стійкість (здатність адаптуватися, відновлюватися й навчатися після криз).

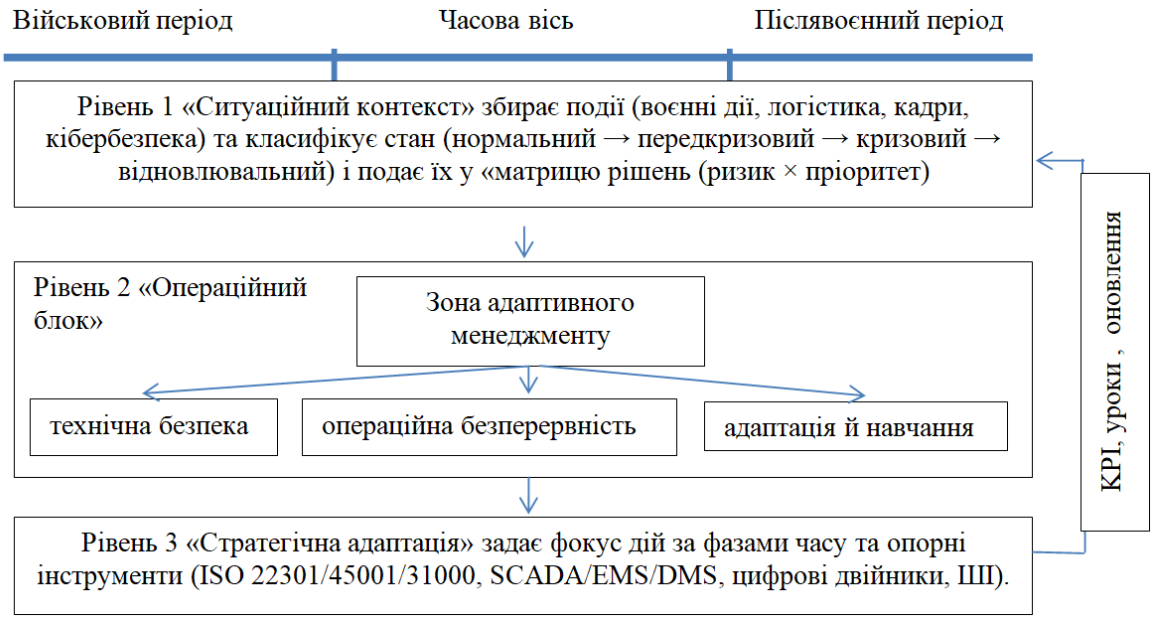


Рисунок 1 – Концептуальна модель ситуаційного управління ВБ (МСУВБ)
Джерело: сформовано авторами

Рис. 1 подає концептуальну схему МСУВБ як трирівневу архітектуру з єдиним замкненим контуром зворотного зв'язку, прив'язану до часової осі «війна-перехід-післявоєнне відновлення». Часова вісь у верхній частині слугує рамкою інтерпретації та підказує, які управлінські рішення є домінантними на кожній фазі (реактивні під час війни, комбіновані у перехідний період, проактивно-стратегічні у відновленні) і забезпечує узгодженість між оперативними діями та довгостроковими трансформаціями.

Рівень 1 («Ситуаційний контекст») акумулює події та ризики військові, технологічні, логістичні, кібернетичні, кадрові, класифікує стан системи як нормальний чи передкризовий чи кризовий чи відновлювальний і перетворює цю інформацію на вхід для матриці рішень «ризик × пріоритет». Вихід рівня 1 є стандартизованим потоком даних про контекст, який надходить до операційного блоку як підстава для вибору режимів реагування.

Рівень 2 («Операційний блок») складається з трьох взаємопов'язаних підсистем: технічна безпека процесів і обладнання, операційна безперервність і резервування, організаційна адаптація, навчання та відновлення. Ядром цього рівня виступає «зона

адаптивного менеджменту» – центр узгодження, де інтегруються сигнали контексту з рівня 1, вимоги та обмеження з рівня 3, а також операційні плани підсистем безпека-безперервність-адаптація і навчання. Функціонально «зона адаптивного менеджменту» належить до рівня 2, оскільки саме тут приймаються й запускаються узгоджені дії від аварійного реагування і планів безперервності до програм тренувань, перерозподілу ресурсів і коротких циклів удосконалення.

Рівень 3 («Стратегічна адаптація») задає політико-нормативні й технологічні рамки для всієї системи. Тут розміщено посилання на міжнародні стандарти менеджменту для безперервності, для охорони праці, для ризик-менеджменту тощо та цифрові інструменти керування. Рівень 3 визначає цілі, обмеження адекватності та надійності, а також пріоритети інвестицій і модернізації, які спускаються до «зони адаптивного менеджменту» як політики-як-код і критерії прийняття рішень.

Логіка потоків відображена простими стрілками; зворотний зв'язок реалізовано через KPI, які постачаються назад у Рівень 1 для перегляду класифікації ситуацій, правил і планів. Таким чином, рис. демонструє, як три опори – технічна безпека, операційна безперервність і організаційна стійкість – інтегруються у єдиний адаптивний контур прийняття рішень, що динамічно підлаштовується до зміни зовнішнього середовища та фазового стану системи й інституцій.

Практична реалізація концептуальної моделі можлива через перехід від концептуальної МСУВБ до моделі управління виробничою безпекою за слабкими сигналами. Зокрема «ситуаційний контекст» розширюємо до контуру раннього попередження і замість фіксації лише подій, він безперервно відстежує KPI і прекурсори як анонімні відхилення телеметрії, мікрозбої процесу, поведінкові маркери, формує слабкі сигнали та подає їх у «зону адаптивного менеджменту». У цій зоні працює поєднання правил і аналітики з принципом «людина в контурі», зокрема диспетчер підтверджує інтерпретацію, обирає ескалацію й превентивні дії (S1-S2-S3 за Херсі-Бланшаром залежно від загрози та зрілості команди, що буде розглянуто нижче). Рівень 3 задає політику та ISO 31000 для стандартизації порогів, відповідальностей і навчання. Зворотній зв'язок через KPI, а саме частота слабких сигналів, час реакції, частка проактивних втручань замикає цикл і постійно уточнює як алгоритми, так і правила ескалації – тобто переводить МСУВБ із реактивного режиму у систему Безпека II з акцентом на попередження, а не на ліквідацію наслідків.

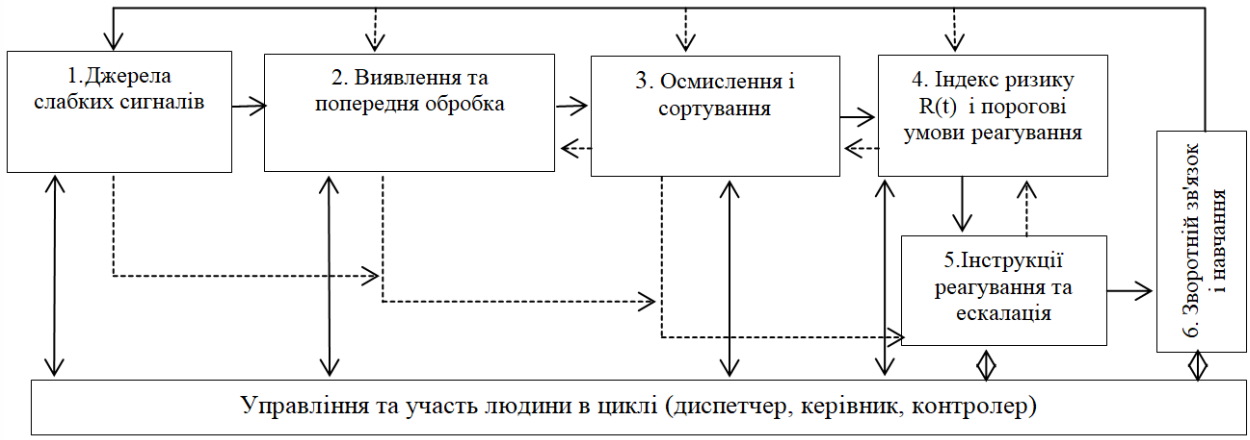
У дослідженні ситуаційного підходу в управлінні заслуговує на увагу праця І. Ансоффа [29] про «слабкі сигнали», яка закладає логіку раннього виявлення стратегічних загроз і перетворює її на керований цикл дій. Саме ці ідеї лягли в основу кожного блока на рис. 2.

1) Джерела слабких сигналів – це стратегічне сканування середовища. І. Ансофф увів поняття ранніх, нечітких ознак (weak signals) і потребу постійного сканування даних, інцидентів, скарг, погодних та логістичних відхилень.

2) Виявлення та попередня обробка – це відсів «шуму» і нарощування «сили сигналу». І. Ансофф звертав увагу на необхідність підсилювання слабкого сигналу до «сильного» через нормалізацію, тренди, класифікацію, використовуючи контрольні карти, тегування аномалій і фільтри похибок.

3) Осмислення (sensemaking) – запобігання стратегічному сюрпризу. Його мета – не чекати аварії, а тлумачити ознаки до того, як загроза матеріалізується.

4) Індекс ризику та порогові умови реагування (тригери) – це «вікно випередження». Зазвичай використовують інтегральний індекс ризику, який змінюється в часі, щоб завчасно бачити зростання загроз. Чим раніше помічено слабкий сигнал, тим більше часу організація має на підготовку й дію. Для цього задаються «вікна випередження» – час до настання події і чіткі пороги ескалації трьох рівнів: рекомендація (уважніше стежити), попередження (підготувати ресурси) і дія (негайно виконати заходи безпеки).



Примітки:
Суцільні стрілки — нормальний послідовний цикл обробки; пунктир — прискорені ескалації до дій та зворотні зв'язки
Переналаштування (навчання/корекції), які не руйнують основний цикл, а накладаються поверх нього.
Основний потік: 1 → 2 → 3 → 4 → 5 → 6 → 1;
Швидкі ескалації (пунктир):
Коли часу мало або загроза висока – минаємо проміжні кроки й одразу запускаємо дії:
1 → 5 (прямий перехід від сигналу до дій);
2 → 5 (аномалія та суворий поріг на етапі детекції → негайне реагування);
3 → 5 (осмислення відразу видає «діяти зараз»);
Петлі переналаштування (пунктир):
Щоб швидко підкрутити модель і правила після дій/уроків;
5 → 4 (результати дій уточнюють індекс і пороги);
4 → 3 (нові порогові умови реагування змінюють пріоритети в інтерпретації);
3 → 2 (уточнене розуміння → нові фільтри/метрики детекції);
6 → 4, 6 → 2, 6 → 3 (уроки можуть одразу змінювати пороги, алгоритми детекції або правила інтерпретації);
Горизонтальний блок 7 «Управління та «людина в контурі» – диспетчер, керівник зміни, контролер контролюють усі вузли 1-6 (погоджують ескалації, затверджують дії, перевіряють журнал рішень)

Рисунок 2 – Схема управління виробничою безпекою за слабкими сигналами
Джерело: сформовано авторами

5) Інструкції реагування та ескалація – це типи відповідей. Заздалегідь підготовлені покрокові інструкції, хто і що робить при різних сценаріях охоплюють три типи відповідей: оборонні (мінімізуємо шкоду), адаптивні (підлаштовуємо процеси й розподіл ресурсів) і проактивні (випереджаємо ризики через зміни в системі). У кожному сценарії розрізняємо інвестиційні дії (модернізація, резервні потужності), операційні дії (перемикання режимів, резервування, ізоляція) та організаційно-поведінкові дії (тренінги, брифінги, зміни в дисципліні безпеки). Маршрути ескалації визначають, коли питання піднімається на вищий рівень управління.

6) Зворотний зв'язок і навчання – це циклічність та спроможність. Після кожного інциденту чи тренування проводиться після дієвий структурований розбір дій, причин і висновків, оновлюються правила й інструкції та відстежуються ключові показники результативності, зокрема час реакції на слабкі сигнали та частоту тяжких подій. Підхід «культура справедливого ставлення до помилок» гарантує, що персонал може без страху повідомляти про відхилення й помилки. Це прискорює навчання організації та зменшує імовірність «стратегічних сюрпризів» у майбутньому.

Таким чином, праця І. Ансоффа дала основу управління за алгоритмом «скануй – осмислюй – запускай порогові умови реагування – дій за інструкціями – навчайся», де головна цінність – виграти час за рахунок ранніх, ще нечітких ознак і перетворити їх на керовані рішення (рис. 2).

Далі блок виявлення та попередньої обробки приводить потоки до єдиної семантики й якості шляхом нормалізації, фільтрації похибок, урахування сезонності/лагів, статистичних і контрольних карт і алгоритмів виявлення аномалій для часових рядів та текстових звітів з допомогою кластеризації повідомлень. Отримані «кандидати» переходять до осмислення (sensemaking) та сортування – кожний сигнал оцінюється в матриці «серйозність × невизначеність» [30], а сама інтерпретація спирається на принципи колективної свідомості у керуванні ризиками шляхом постійної уваги до збоїв, небажання спрощувати, чутливість до операцій, відданість відновлюваності та верховенство експертності, що зменшує ризик пропустити слабкі, але важливі ознаки HRO [31]. Сигнали зіставляються зі швейцарським сиромn Дж. Різона [30], де безпека розглядається як низка бар'єрів чи захистів із «дірками» (вразливостями), а інцидент стається, коли «дірки» тимчасово шикуються в один канал. Корисним для інтерпретації слабких сигналів як ознак деградації бар'єрів, із причинно-наслідковими схемами є системно-теоретичний підхід Н. Левесон [32], що розглядає аварії як збої керування у складних соціо-технічних системах, а не як сума ізольованих відмов. Метод «Системно-теоретичний аналіз процесів» (System-Theoretic Process Analysis) дає процедуру виявлення небезпечних керуючих дій, контекстів, у яких вони стають небезпечними, та розривів зворотного зв'язку. Такий підхід формує керувальні контури і дозволяє трактувати «слабкі сигнали» як ранні ознаки деградації бар'єрів і втрати керованості. На етапі осмислення даних розрізнені індикатори агрегуються у композитний індекс ризику $R(t)$, побудованому на провідних показниках, зокрема щільності «майже-аварій», стані технічних і організаційних бар'єрів, швидкості зростання відхилень, порушеннях контролю та зворотного зв'язку тощо. Для індексу визначаються пороги і режими ескалації (інформаційне повідомлення, попередження, негайна дія) разом із чіткими правилами переходу між ними. Така логіка узгоджується з практикою процесної безпеки, що спирається на провідні індикатори, і з підходами до оцінювання ризиків, закріпленими у стандартах Міжнародної організації зі стандартизації 45001 та документах Міжнародної електротехнічної комісії 31010. Коли $R(t)$ перевищує встановлені пороги або демонструє негативний тренд, запускаються заздалегідь підготовлені сценарії дій – інспекція та діагностика, тимчасове зниження навантаження, технічне обслуговування і ремонт або заміна вузлів, увімкнення резервування, а у разі необхідності – зупинка робіт із суворо визначеними ролями, відповідальністю та каналами комунікації. Після виконання заходів реалізується зворотний зв'язок і навчання, здійснюється короткий розбір дій «після події», оновлення правил і вагових коефіцієнтів, перегляд порогів спрацювання, а також моніторинг показників результативності (частота і тяжкість травм, частота «майже-аварій», час реагування, стан бар'єрів). Такий навчальний контур утілює перехід від підходу «Безпека-І» Еріка Холнаґеля – орієнтації на підрахунок помилок – до «Безпеки-ІІ», де фокус зміщено на розуміння того, чому система зазвичай працює добре, і на підсилення її стійкості. Увесь процес перебуває під наглядом управлінського рівня та «людини у контурі» (відповідальні за охорону праці та промислову безпеку, керівники змін, комітет з ризиків), із прозорим аудиторським слідом і культурою справедливості.

Таким чином, теоретичну основу управління виробничою безпекою за сигналами зміцнюють концепція «слабких сигналів» І. Ансоффа як механізм раннього попередження; «модель швейцарського сиру» Дж. Різона як інструмент виявлення «дір» у бар'єрах; системно-теоретичні обмеження керування й аналіз причинно-наслідкових шляхів небезпек у роботах Н. Левесон; а також настанови і вимоги міжнародних стандартів щодо формалізації провідних індикаторів та процедур реагування.

Враховуючи, що умови виробничої діяльності змінюються, залежно від впливу середовища, у табл. 2 представлено часову структуру запропонованої моделі із вказанням ключового стилю керівництва [33].

Таблиця 2 – Часова структура моделі

Фаза	Контекст	Основна мета	Ключовий стиль управління
I. Військовий час (Кризова)	Активні воєнні дії, загрози персоналу, енергосистемам і логістиці	Збереження життя, мінімізація збитків, утримання базових функцій	Реактивне, ситуаційне управління
II. Трансформаційний період (Стабілізаційна)	Часткове відновлення контролю, зменшення невизначеності	Відновлення критичних функцій, створення резервних потужностей	Комбіноване управління
III. Післявоєнна фаза (Відновлювальна)	Реконструкція, модернізація, інвестиції	Відбудова безпечної інфраструктури, інтеграція сталого розвитку	Проактивне стратегічне управління

Джерело: сформовано авторами

У часовій моделі «війна-перехід-відновлення» доречно інтерпретувати стилі управління крізь призму ситуативного лідерства Герсі-Бланшара, де вибір стилю визначається поєднанням директивності, підтримувальної взаємодії та зрілості-готовності команди (рис. 3).

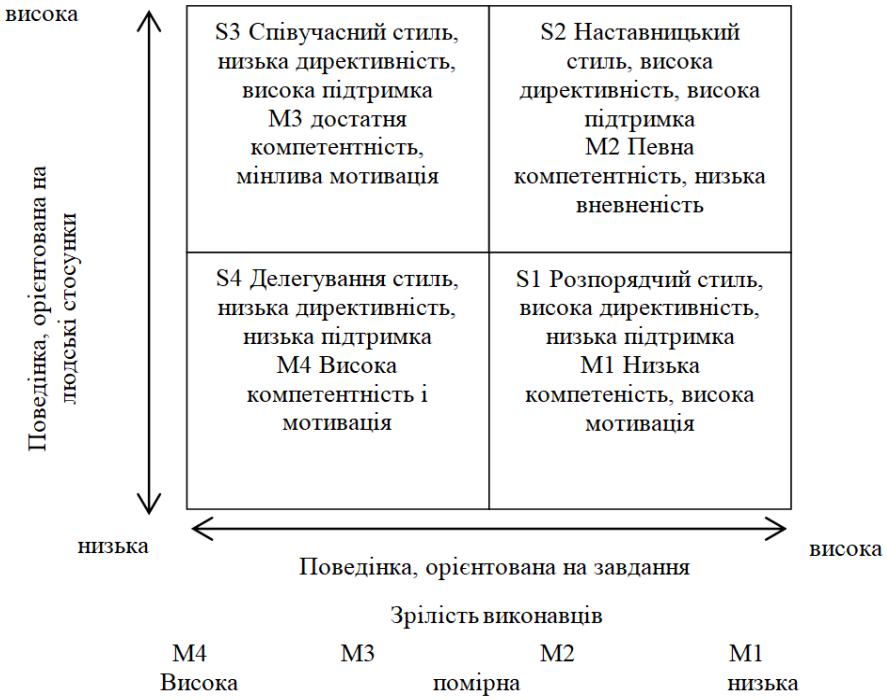


Рисунок 3 – Ситуаційна модель Херсі-Бланшара в управлінні ВБ
Джерело: сформовано авторами на основі [34]

На етапі війни домінує реактивне, ситуаційне управління, що відповідає стилям S1 та S2: за високої невизначеності й дефіциту часу керівник забезпечує чітке завдання, одномоментне прийняття рішень і коротке прийняття рішення для мобілізації залученості. Тут акцент зміщено на одноманітні, прості у виконанні інструкції та жорстке дотримання протоколів, що мінімізує помилки і дає змогу швидко стабілізувати процеси.

У перехідний період доцільним стає комбіноване управління S2 та S3: зростання компетентності персоналу дозволяє зменшити директивність і посилити співучасть, тому рішення обґрунтовуються, порівнюються за сценаріями, частина повноважень делегується крос-функціональним командам, а управлінський фокус зміщується від одноразових реакцій до збалансування жорстких стандартних процедур із варіантними планами дій.

На етапі відновлення раціональним є проактивне стратегічне управління S3 та S4: за високої зрілості команд директивність мінімізується, рішення приймаються із широкою участю та делегуванням, а головним змістом управління стає випереджальне проектування стійкості через цифрові двійники ризиків, виявлення аномалій, профілактичне обслуговування, інтеграція систем менеджменту безпеки й безперервності, що переводить безпеку з площини «реакції на інциденти» у площину стратегічної конкурентної переваги.

Отже, вибір стилю є функцією поєднання загроз і часових обмежень із поточною зрілістю команди. За високого ризику й тиску часу переважає S1 та S2; за часткового відновлення маневру – S2 та S3; за стабілізації та інституційного зміцнення – S3 та S4. Ця логіка забезпечує безперервний перехід від негайної стабілізації через збалансоване відновлення до інноваційно-орієнтованої стійкості, узгоджуючи стиль керівництва з фазою розвитку системи та її організаційною готовністю.

Висновки та перспективи подальших досліджень. Таким чином, у статті обґрунтовано зміст моделі адаптивного управління ВБ та запропоновано концептуально-аналітичну модель ситуаційного управління виробничою безпекою (МСУВБ), що інтегрує циклічну логіку управління безперервністю бізнесу, механізм роботи зі слабкими сигналами та ситуативне лідерство Херсі-Бланшара. Модель характеризує стилі керівництва і набір дій для трьох часових фаз – війна, перехід, відновлення та дозволяє узгоджувати оперативні рішення з обмеженнями й цілями діяльності організації. Ключовим елементом є ризик із визначеними сигналами ідентифікування, що дає змогу рано виявляти відхилення, керовано здійснювати реагування та узгоджувати його з процесами управління інцидентами, кризами й планами безперервності. Центральна «адаптивна зона управління» поєднує технічну безпеку, безперервність і організаційну стійкість, переводячи практику з переважно реактивних дій на проактивне попередження з чітким зворотним зв’язком і навчанням. Практична придатність моделі підтверджується впровадженням операційних інструкцій, що скорочують час реакції й втрати, підвищують прогнозованість, підзвітність і узгодженість рішень між підрозділами. Сукупно це формує основу для системного, прозорого та відтворюваного управління ВБ у змінному середовищі – від високого тиску воєнного періоду до стратегічної модернізації в післявоєнному відновленні.

До дискусійних моментів у статті відносимо відсутність даних щодо розрахунку результативності моделі. Запропоновані джерела даних наразі розглядаються як цільовий контур збору інформації для майбутнього використання. Відсутність фактичних даних у статті визначає, що робота носить концептуально-методологічний характер і формує специфікацію даних, необхідних для верифікації моделі. Аналогічно, перелік показників результативності як «рамка оцінювання» буде застосована в подальших дослідженнях для вимірювання ефектів впровадження. Відсутність доступу до оперативних даних у воєнних умовах, потенційні прогалини якості журналів інцидентів, етичні та безпекові обмеження щодо публікації операційних даних на даний момент обмежує можливості кількісної оцінки. Таким чином, запропонована методологія вирішує завдання статті на рівні теоретичної специфікації, а емпірична перевірка визначена як наступний етап дослідження.

Список використаних джерел

1. Офіційний сайт Держпраці. https://dsp.gov.ua/
2. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану» (аналітична доповідь, 31.05.2023). https://niss.gov.ua/sites/default/files/2023-05/executive-1.pdf
3. НІСД. «Економічна безпека України в умовах високих воєнних ризиків та глобальної нестабільності» (аналітична доповідь, 2025). URL. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/ekonomichna-bezpeka-ukrayiny-v-umovakh-vysokykh-voyennykh-ryzykiv
4. Братель С.Г. (2023). Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. *Південноукраїнський правничий часопис*, № 3. https://doi.org/10.31733/15-03-2024/1/35-36
5. Гарькава В.Ф. (2022). Економічна безпека регіонів України. *Економіка України*, № 2. С. 37-49. https://doi.org/10.15407/economyukr.2022.02.037
6. Глущенко О. О. (2023). Функція забезпечення безпеки держави в умовах воєнного стану. *Часопис Київського університету права*, № 1, 53-56. https://doi.org/10.36695/2219-5521.1.2023.10
7. Новик І. (2025). Гарантування виробничої безпеки як важливої умови підвищення рівня конкурентоспроможності національної економіки. *Економіка та суспільство*, № 77. https://doi.org/10.32782/2524-0072/2025-77-54
8. Вашай Ю. В., Дорошенко О. О. (2019). Методичні аспекти дослідження стану виробничої безпеки держави в умовах військово-політичної нестабільності. *Бізнес Інформ*, № 5. С. 150-156. https://doi.org/10.32983/2222-4459-2019-5-150-156
9. Капля О. (2023). Забезпечення економічної безпеки громадянина в умовах воєнного стану: правовий аспект. *Наукові праці Міжрегіональної Академії управління персоналом*. Юридичні науки, № 2 (62), 29-33. https://doi.org/10.32689/2522-4603.2022.2.5
10. Козак С. (2023). Сучасні проблеми виробничої безпеки підприємств Нафтогазового комплексу України. *Вісник Хмельницького національного університету. Економічні науки*, № 6, 291-297. https://doi.org/10.31891/2307-5740-2023-324-6-49
11. Полянська А.С., Трощенкова Т.А. (2010). Сучасні технології управління економічною безпекою підприємства. *Вісник економіки транспорту і промисловості*, № 29, С.164-168.
12. Polyanska A. (2024). Application of decision support systems (DSS): the case of energy company. Proceedings of the 44th International Business Information Management Association Conference (IBIMA): empower business and create economic development in digital future: vision 2030 : 27-28 November 2024, Granada, Spain / ed. Khalid S. Soliman. https://u.pcloud.link/publink/show?code=cLzrtalK#folder=24197.. .
13. Vanderhaegen, F., Erik Hollnagel. (2015). Safety-I and Safety-II, the past and future of safety management. *Cognition Technology & Work*, № 17(3), 461-464. https://doi.org/10.1007/s10111-015-0345-z
14. Dekker S. (2001). The Field Guide to Understanding Human Error. Cranfield University Press, https://www.leonardo-in-flight.nl/PDF/FieldGuide%20to%20Human%20Error.PDF
15. Мезенцева І. О. (2022). Безпека виробничих процесів і устаткування : навчальний посібник Частина І. Організаційні та технічні заходи безпеки трудового процесу. Харків: НТУ "ХПІ", 246 с
16. ISO 22301:2019(en). Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en
17. Міжнародний стандарт ISO 31000. https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf
18. ISO 22320:2018(en). Security and resilience — Emergency management — Guidelines for incident management. https://www.iso.org/obp/ui/en/#iso:std:iso:22320:ed-2:v1:en
19. Gexcon AS 2025. https://www.gexcon.com/resources/blog/atex-directives-an-introduction/
20. EU-OSHA 2025. An agency of the European Union. https://osha.europa.eu/en
21. Сайт Європейської Комісії. Energy, Climate change, Environment. https://environment.ec.europa.eu/topics/waste-and-recycling/batteries_en
22. Сайт Європейської Комісії. Circular economy: New law on more sustainable, circular and safe batteries enters into force. https://environment.ec.europa.eu/news/new-law-more-sustainable-circular-and-safe-batteries-enters-force-2023-08-17_en?utm_source=chatgpt.com

23. Директива (ЄС) 2023/1791 Європейського Парламенту та Ради від 13 вересня 2023 року про енергоефективність та внесення змін до Регламенту (ЄС) 2023/955. https://eur-lex.europa.eu/eli/dir/2023/1791/oj/eng

24. Directive (EU) 2024/1275 of the European Parliament and of the Council of 24 April 2024 on the energy performance of buildings (recast) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1275

25. Directive 92/57/EEC-temporary or mobile construction sites. https://osha.europa.eu/en/legislation/directives/15

26. ISO 50001: Guide to effective energy management with an EMS. https://enity.io/en/e-book-iso-50001-guide-to-effective-energy-management-with-an-ems/?gad_source=1&gad_campaignid=23011774016&gclid=Cj0KCQiAuvTJBhCwARIsAL6Demg8iSM6mj91nvmEcwC7iqeecQttxfIp46meH8HQwVJXPJWCZJsBLVoaAnzYEALw_wcB

27. European Resource Adequacy Assessment. https://www.entsoe.eu/eraa/

28. Renovation Wave: guidance for local and regional implementation. https://rise.esmap.org/sites/default/files/library/austria/Renewable%20Energy/Austria_page17_Renovation%20wave_full%20study.pdf

29. Ansoff H. I. (1975). Managing Strategic Surprise by Response to Weak Signals. *California Management Review*, № 18(2), 21-33. https://doi.org/10.2307/41164635

30. Reason J. (2000) Human Error: Models and Management. *British Medical Journal*, 320, 768-770. https://doi.org/10.1136/bmj.320.7237.768. https://pmc.ncbi.nlm.nih.gov/articles/PMC1117770/

31. Weick K. E., Sutcliffe K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). John Wiley & Sons. 224 p.

32. Leveson N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. https://my.eng.utah.edu/~cs5785/slides-f10/safer-world-draft.pdf

33. Полянська А. С. (2013). Актуальність ситуаційних теорій керівництва в управлінні розвитком підприємств нафтогазового комплексу. *Науковий вісник ІФНТУНГ*, № 1(34). С. 209-216.

34. Hersey H. Paul, Blanchard Kenneth H. (2013). Management of organizational behavior: leading human resources. Dewey E. Johnson.10th ed.

References

1. Official website of the State Labor Service. URL. https://dsp.gov.ua/

2. Current challenges and threats to the economic security of Ukraine under martial law" (analytical report, 05/31/2023). URL. https://niss.gov.ua/sites/default/files/2023-05/executive-1.pdf

3. NISD. “Economic Security of Ukraine in Conditions of High Military Risks and Global Instability” (analytical report, 2025). URL. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/ekonomichna-bezpeka-ukrayiny-v-umovakh-vysokykh-voyennykh-ryzykiv

4. Bratel S.G. (2023). Experience of foreign countries in the field of ensuring the security of critical infrastructure facilities. *South Ukrainian Law Journal*, № 3. URL.https://doi.org/ 10.31733/15-03-2024/1/35-36

5. Garkava V.F. (2022). Economic security of the regions of Ukraine. *Economy of Ukraine*, № 2. С. 37-49. URL. https://doi.org/10.15407/economyukr.2022.02.037

6. Glushchenko O. O. (2023). The function of ensuring state security in conditions of martial law. *Journal of the Kyiv University of Law*, № 1, 53-56. URL.https://doi.org/10.36695/2219-5521.1.2023.10

7. Novik I. (2025). Ensuring industrial safety as an important condition for increasing the level of competitiveness of the national economy. *Economy and Society*, № 77. URL. https://doi.org/10.32782/2524-0072/2025-77-54

8. Vashai Y. V., Doroshenko O. O. (2019). Methodological aspects of studying the state of industrial security of the state in conditions of military-political instability. *Business Inform*, № 5. С. 150-156. URL. https://doi.org/10.32983/2222-4459-2019-5-150-156

9. Kaplya O. (2023). Ensuring the economic security of a citizen in martial law: legal aspect. *Scientific works of the Interregional Academy of Personnel Management. Legal Sciences*,№ 2 (62), 29-33. URL. https://doi.org/10.32689/2522-4603.2022.2.5

10. Kozak S. (2023). Modern problems of industrial safety of enterprises of the Oil and Gas Complex of Ukraine. *Bulletin of Khmelnytsky National University. Economic Sciences,* № 6, 291-297. URL. https://doi.org/10.31891/2307-5740-2023-324-6-49

11. Polyanska A.S., Troshchenkova T.A. (2010). Modern technologies for managing the economic security of an enterprise. *Bulletin of the Economy of Transport and Industry*, № 29, С.164-168.

12. Polyanska A. (2024). Application of decision support systems (DSS): the case of energy company. Proceedings of the 44th International Business Information Management Association Conference (IBIMA): empower business and create economic development in digital future: vision 2030 : 27-28 November 2024, Granada, Spain. ed. Khalid S. Soliman. URL. https://u.pcloud.link/publink/show?code=cLzrtalK#folder=24197.

13. Vanderhaegen, F., Erik Hollnagel. (2015). Safety-I and Safety-II, the past and future of safety management. *Cognition Technology & Work,* № 17(3), 461-464. URL. https://doi.org/10.1007/s10111-015-0345-z

14. Dekker S. (2001). The Field Guide to Understanding Human Error. Cranfield University Press, URL. https://www.leonardo-in-flight.nl/PDF/FieldGuide%20to%20Human%20Error.PDF

15. Mezentseva I. O. (2022). Safety of production processes and equipment: textbook Part I. Organizational and technical measures of labor process safety. NTU "KhPI", Kharkiv, 246 c

16. ISO 22301:2019(en). Security and resilience — Business continuity management systems — Requirements. URL.https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en

17. ISO 31000. URL. https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf

18. ISO 22320:2018(en). Security and resilience — Emergency management — Guidelines for incident management. URL. https://www.iso.org/obp/ui/en/#iso:std:iso:22320:ed-2:v1:en

19. Gexcon AS 2025. URL. https://www.gexcon.com/resources/blog/atex-directives-an-introduction/

20. EU-OSHA 2025. An agency of the European Union. URL.https://osha.europa.eu/en

21. European Commission website. Energy, Climate change, Environment. URL. https://environment.ec.europa.eu/topics/waste-and-recycling/batteries_en

22. European Commission website. Circular economy: New law on more sustainable, circular and safe batteries enters into force. URL. https://environment.ec.europa.eu/news/new-law-more-sustainable-circular-and-safe-batteries-enters-force-2023-08-17_en?utm_source=chatgpt.com

23. Directive (EU) 2023/1791 of the European Parliament and of the Council 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955. URL. https://eur-lex.europa.eu/eli/dir/2023/1791/oj/eng

24. Directive (EU) 2024/1275 of the European Parliament and of the Council of 24 April 2024 on the energy performance of buildings (recast) (Text with EEA relevance). URL. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1275

25. Directive 92/57/EEC-temporary or mobile construction sites. URL. https://osha.europa.eu/en/legislation/directives/15

26. ISO 50001: Guide to effective energy management with an EMS. URL.https://enity.io/en/e-book-iso-50001-guide-to-effective-energy-management-with-an-ems/?gad_source=1&gad_campaignid=23011774016&gclid=Cj0KCQiAuvTJBhCwARIsAL6Demg8iSM6mj91nvmEcwC7iqeecQttxfIp46meH8HQwVJXPJWCZJsBLVoaAnzYEALw_wcB

27. European Resource Adequacy Assessment. https://www.entsoe.eu/eraa/

28. Renovation Wave: guidance for local and regional implementation. URL. https://rise.esmap.org/sites/default/files/library/austria/Renewable%20Energy/Austria_page17_Renovation%20wave_full%20study.pdf

29. Ansoff H. I. (1975). Managing Strategic Surprise by Response to Weak Signals. *California Management Review*, № 18(2), 21-33. URL. URL. https://doi.org/10.2307/41164635

30. Reason J. (2000) Human Error: Models and Management. *British Medical Journal*, 320, 768-770. https://doi.org/10.1136/bmj.320.7237.768. URL.https://pmc.ncbi.nlm.nih.gov/articles/PMC1117770/

31. Weick K. E., Sutcliffe K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). John Wiley & Sons. 224 p.

32. Leveson N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. https://my.eng.utah.edu/~cs5785/slides-f10/safer-world-draft.pdf

33. Polyanska A. S. (2013). The relevance of situational theories of management in managing the development of oil and gas enterprises. *Scientific Bulletin of the Institute of Oil and Gas Industry and Energy (IFNTUNG)*, № 1(34). C.209-216.

34. Hersey H. Paul, Blanchard Kenneth H. (2013). Management of organizational behavior: leading human resources. Dewey E. Johnson.10th ed.

ADAPTIVE MODEL OF INDUSTRIAL SAFETY IN THE SITUATIONAL MANAGEMENT SYSTEM

Polyanska Alla Stepanivna
Doctor of Economics, professor,
Ivano-Frankivsk National Technical University of Oil and Gas
76019, Ivano-Frankivsk, st. Karpatska, 15
e-mail: alla.polianska@nung.edu.ua
ORCID ID: http://orcid.org/0000-0001-5169-1866

Mykytiuk Oleg Romanovych
PhD student of Management and Administration Department
Ivano-Frankivsk National Technical University of Oil and Gas
76019, Ivano-Frankivsk, Karpatska St.15
e-mail: oleg.mykytiuk75@gmail.com
ORCIDID: https://orcid.org/0009-0008-3732-4582

Abstract. The article considers the theoretical and methodological principles of industrial safety management of an enterprise in the context of situational management. It is substantiated that the modern industrial safety management model is adaptive, since it must take into account the requirements of the internal and external environment. An integrated industrial safety system that can potentially be used by an enterprise is considered and presented, which covers standards and systems and defines their role in industrial safety management. A conceptual and analytical model of situational industrial safety management (SIMSM) is developed, which differentiates approaches to risk management, resilience and response in the war period, in the transition phase and during post-war recovery. The model consists of 3 levels - situational, operational and strategic adaptation block. The adaptive management zone integrated into the model in the middle of the operational block combines safety, continuity and resilience, transferring decisions from reactive to proactive, closes the feedback loop with a learning loop. The methodological framework is made up of the requirements of the business continuity management system based on traditional and modern international and domestic safety management standards. A four-stage procedure for industrial safety management is proposed based on the identification of external and internal factors and weak signals for three time phases; determination of critical processes and impact thresholds with risk assessment; design of ISMS with the allocation of the stages “data-models-rules-decisions-KPI-feedback” with sets of actions for each phase; justification of leadership styles in the logic of situational leadership of Hersey-Blanchard. Based on the development of theoretical safety concepts, a scheme for industrial safety management based on weak signals is considered, which consists of sequential stages that allow industrial safety management based on a sequential data processing cycle taking into account deviations and escalations, which ultimately makes the management process transparent, understandable and manageable. A combination of weak signal management with a business continuity management cycle based on international quality standards and linked to situational leadership styles according to the time frames "war-transition-recovery" is proposed.

Key words: industrial safety, business continuity, weak signals, situational leadership styles, standards, adaptability.