УДК 005.21:005.334:330.131.7
DOI: https://doi.org/10.37734/2409-6873-2026-3-6

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ БЕЗПЕКООРІЄНТОВАНОГО МЕНЕДЖМЕНТУ ПІДПРИЄМСТВА: БАГАТОРІВНЕВА АРХІТЕКТУРА ТА ПРОГРАМА ОПЕРАЦІОНАЛІЗАЦІЇ

Б. С. КОЛОМІЄЦЬ
доктор філософії (кандидат педагогічних наук), докторант,
Полтавський університет економіки і торгівлі
ORCID: https://orcid.org/0000-0002-7723-6666

Анотація. *У статті досліджено теоретико-методологічні засади безпекоорієнтованого менеджменту підприємства в умовах зростання складності, невизначеності та взаємопов'язаності сучасних загроз. Обґрунтовано, що традиційні підходи до забезпечення безпеки, зосереджені на окремих функціональних складових або реактивному реагуванні на ризики, не забезпечують належного рівня стійкості та адаптивності підприємств у сучасному безпековому середовищі.* ***Метою статті*** *є обґрунтування теоретико-методологічних засад і розроблення багаторівневої архітектури дослідження безпекоорієнтованого менеджменту підприємства, яка забезпечує концептуальне розмежування суміжних управлінських конструкцій, інтеграцію управлінських і безпекових підходів та формування програми подальшої операціоналізації й емпіричної валідації.* ***Методологічну основу дослідження*** *становлять системний, складнісно-адаптивний, соціотехнічний, стратегічний, ризик-орієнтований та резильєнтнісний підходи, а також методи аналізу, синтезу, систематизації, порівняння, контент-аналізу й теоретичного моделювання. Визначено місце безпекоорієнтованого менеджменту в системі сучасних управлінських концепцій та обґрунтовано його відмінність від економічної безпеки підприємства, ризик-менеджменту, кризового менеджменту, безпекового врядування та організаційної резильєнтності. Запропоновано авторське визначення безпекоорієнтованого менеджменту як інтегрованої системи врядування, стратегічного спрямування, управлінських процесів, рішень і організаційних спроможностей, у якій безпекові та резильєнтнісні критерії інтегровані в досягнення місії та розвиток підприємства. Розроблено багаторівневу методологічну архітектуру дослідження, процесний цикл безпекоорієнтованого менеджменту та програму його операціоналізації на основі послідовного змішаного дизайну дослідження. Обґрунтовано доцільність використання закладів вищої освіти як критичних інформаційно насичених кейсів для апробації запропонованого методологічного підходу.* ***Практична значущість отриманих результатів*** *полягає у можливості використання запропонованих теоретико-методологічних положень для розроблення систем оцінювання безпекоорієнтованого менеджменту, проведення емпіричних досліджень, формування профілів спроможностей, моделей зрілості та управлінських інструментів підвищення стійкості й безпеки підприємств в умовах динамічних зовнішніх викликів.*

Ключові слова: *безпекоорієнтований менеджмент, економічна безпека підприємства, ризик-менеджмент, організаційна резильєнтність, безпекове врядування, менеджмент безперервності діяльності, кризовий менеджмент, методологія дослідження, операціоналізація, заклади вищої освіти.*

Постановка проблеми в загальному вигляді та зв'язок із найважливішими науковими чи практичними завданнями. Функціонування сучасних підприємств відбувається в умовах зростання складності та взаємопов'язаності загроз. Воєнні дії, кіберінциденти, енергетичні обмеження, кадровий дефіцит, фінансові ризики, логістичні збої та репутаційні кризи дедалі частіше виникають одночасно й взаємно підсилюють один одного. За таких умов безпека перестає бути лише окремою функцією чи сферою відповідальності спеціалізованих підрозділів і перетворюється на невід'ємну складову системи менеджменту підприємства.

Сучасне розуміння безпеки пов'язане не лише із захистом ресурсів або реагуванням на загрози, а й зі здатністю організації передбачати зміни, забезпечувати безперервність діяльності, адаптуватися до нових умов, підтримувати стійкість і накопичувати організаційний досвід. У зв'язку з цим формується концепція безпекоорієнтованого менеджменту, яка інтегрує безпекові критерії в процеси стратегічного управління, організаційного розвитку та прийняття управлінських рішень.

Разом із тим розвиток цієї концепції супроводжується низкою теоретико-методологічних проблем. У науковій літературі безпеко-орієнтований менеджмент часто ототожнюється з ризик-менеджментом, кризовим управлінням, менеджментом безперервності діяльності або організаційною резильєнтністю. Крім того, нерідко змішуються різні складові методології дослідження: теоретичні підходи, принципи, методи, дослідницькі дизайни та прикладні інструменти, що ускладнює

формування цілісного наукового підходу та перехід від концептуальних моделей до їх практичного вивчення й оцінювання.

Отже, наукова проблема полягає у необхідності формування цілісного теоретико-методологічного підґрунтя дослідження безпекоорієнтованого менеджменту підприємства. Її розв'язання потребує уточнення змісту цієї категорії, розмежування її із суміжними управлінськими концепціями, розроблення багаторівневої методологічної архітектури дослідження та створення програми подальшої операціоналізації й емпіричної валідації отриманих результатів.

Аналіз останніх досліджень і публікацій. Теоретичні засади дослідження безпекоорієнтованого менеджменту сформувалися на перетині кількох наукових напрямів. Перший із них пов'язаний із проблематикою економічної безпеки підприємства. Вагомий внесок у розвиток цього напряму зробили В. Гаркуша та Н. Єршова, які систематизували наукові підходи до сутності економічної безпеки підприємства, З. Тітенко, яка досліджувала фінансову безпеку, С. Гринкевич, яка проаналізувала еволюцію відповідних теоретичних концепцій, а також Л. Яструбецька, яка вивчала вплив сучасних загроз на фінансову безпеку суб'єктів підприємництва [1–4]. Водночас цей підхід переважно зосереджений на економічних і фінансових аспектах безпеки та не повною мірою враховує організаційні, поведінкові та цифрові чинники.

Другий напрям представлений ризик-орієнтованим управлінням. О. Герасименко розробила теоретико-методологічні основи ризик-орієнтованого управління в системі економічної безпеки підприємства, а Л. Гриценко, І. Кожушко, В. Чепурко та Г. Перепелицин обґрунтували місце ризик-менеджменту в системі корпоративної безпеки [5; 6]. Перевагою цього підходу є його орієнтація на роботу з невизначеністю, однак він не охоплює повною мірою механізми відновлення, адаптації та організаційного навчання після кризових подій.

Важливе місце у сучасній управлінській науці посідає концепція організаційної резильєнтності. Дж. Гіллман і Е. Гюнтер досліджували теоретичні аспекти резильєнтності організацій, С. Раетце, С. Духек, М. Мейнард і Б. Кіркман запропонували її багаторівневу інтерпретацію, М. Багхерсад і К. Зобель розробили підходи до кількісного оцінювання резильєнтності, а Г. Акпінар і Д. Озер-Кайлан пов'язали її з концепцією складних адаптивних систем [7–10]. Цей напрям дозволяє розглядати безпеку крізь призму здатності організації адаптуватися, відновлюватися та розвиватися після криз.

Окрему групу становлять дослідження менеджменту безперервності діяльності та кризового менеджменту. С. Галайці зі співавторами здійснили порівняння менеджменту безперервності діяльності, операційної та організаційної резильєнтності, а міжнародні стандарти ISO 22301, ISO 22336 та ISO 22361 сформували практичне підґрунтя для забезпечення безперервності діяльності та управління кризовими ситуаціями [11–14].

Подальший розвиток безпекової проблематики пов'язаний із концепціями security governance та кібербезпекового врядування. Г. Мелаку запропонував адаптивну модель кібербезпекового врядування, Е. Ченг і Т. Ванг дослідили інституційні механізми кібербезпеки у закладах вищої освіти, а NIST Cybersecurity Framework 2.0 закріпив інтеграцію кібербезпеки в загальну систему управління організацією [15–17].

Безпосередньо питання безпекоорієнтованого управління та розвитку підприємств розглядаються у працях Т. Момот, О. Філонич, А. Косяка та О. Лобача, які запропонували систему показників безпекоорієнтованого управління, А. Івченка, О. Кудріної та А. Івченка, М. Галгаша, Р. Мороза й О. Загороднюк, а також Н. Гавловської, О. Кримчак і В. Подгали [18–22]. У цих дослідженнях простежується тенденція до розгляду безпеки як складової стратегічного розвитку та довгострокової стійкості підприємства.

Проведений аналіз свідчить, що сучасні дослідження поступово переходять від вузького трактування безпеки як стану захищеності до її розгляду як інтегрованої характеристики системи управління. Водночас залишаються недостатньо розробленими питання методологічного розмежування суміжних концепцій, операціоналізації безпекоорієнтованого менеджменту та його емпіричної валідації. Саме ці аспекти потребують подальшого наукового опрацювання.

Формування цілей статті (постановка завдання). Метою статті є обґрунтування теоретико-методологічних засад і розроблення багаторівневої архітектури дослідження безпекоорієнтованого менеджменту підприємства, яка забезпечує концептуальне розмежування суміжних управлінських конструкцій, упорядкування методологічних підходів за їхнім науковим статусом, інтеграцію управлінських і безпекових лінз та формування програми операціоналізації й подальшої емпіричної валідації з урахуванням специфіки закладів вищої освіти як критичного інформаційно насиченого кейсу.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. З огляду на результати аналізу, безпекоорієнтований менеджмент не може бути зведений ані до стану захищеності підприємства, ані до діяльності його служби безпеки, ані до сукупності процедур ризик-менеджменту. Він характе-

ризує спосіб організації всієї системи управління, у межах якого безпекові критерії враховуються у формуванні місії, стратегічних цілей, структур, процесів, рішень, ресурсів і взаємовідносин зі стейкхолдерами. Враховуючи це, пропонується таке визначення: безпекоорієнтований менеджмент підприємства – це інтегрована система врядування, стратегічного спрямування, управлінських процесів, рішень і організаційних спроможностей, у якій безпекові та резильєнтнісні критерії вбудовано у досягнення місії й розвиток підприємства через цикл передбачення, запобігання, підготовки, поглинання впливу, підтримання безперервності, реагування, відновлення, адаптації, трансформації та організаційного навчання.

На відміну від традиційних трактувань безпеки як стану, запропоноване визначення акцентує увагу на її управлінській процесності, адже безпека не є остаточно досягнутим результатом: вона постійно відтворюється через управлінські рішення, навчання, оновлення політик, перерозподіл ресурсів і розвиток спроможностей.

Результативність безпекоорієнтованого менеджменту також не слід оцінювати виключно за відсутністю інцидентів або збитків, адже відсутність зафіксованих подій може бути наслідком випадковості, недостатнього моніторингу або приховування проблем, натомість релевантними результатами є: захищеність критичних цінностей; прийнятний рівень безперервності критичних процесів; здатність підтримувати місію під час збурення; швидкість і якість відновлення; гнучкість перерозподілу ресурсів; здатність до адаптації та трансформації; накопичення організаційного знання; довіра внутрішніх і зовнішніх стейкхолдерів; збереження передумов сталого розвитку.

Отже, безпекоорієнтований менеджмент постає як динамічна управлінська метасистема, що інтегрує безпекове врядування, ризик-менеджмент, безперервність діяльності, кризове управління, резильєнтність, організаційну культуру і стратегічний розвиток, але не ототожнюється з жодною з цих складових.

Розроблення методології дослідження безпекоорієнтованого менеджменту потребує не лише визначення сукупності релевантних підходів, а й установлення їхнього наукового статусу, місця та функції у загальній логіці дослідження. На нашу думку, це особливо важливо з огляду на те, що у сучасних працях нерідко на одному класифікаційному рівні подаються системний підхід, процесний аналіз, превентивність, SWOT-аналіз, експертне оцінювання та управлінський dashboard. Така практика створює категоріальну невизначеність, оскільки змішує теоретичні способи інтерпретації об'єкта, принципи управління, дизайн дослідження, методи отримання наукового доказу та прикладні інструменти.

Відповідно до цього ми пропонуємо здійснювати систематизацію не за формальною назвою підходу, а за його функціональною роллю в процесі наукового пізнання, тому доцільно виокремити: теоретико-методологічні засади, управлінське ядро, контекстні лінзи, принципи, дизайн дослідження, методи та інструменти (табл. 1).

Запропонована систематизація дозволяє усунути дві типові помилки: перша полягає у формальному об'єднанні всіх названих у публікаціях категорій під загальною назвою «методологічні підходи»; друга – у спробі визначити один універсальний підхід, який нібито здатний повністю пояснити безпекоорієнтований менеджмент. Складність досліджуваного явища вимагає методологічного плюралізму, але такий плюралізм має бути впорядкованим і функціонально обґрунтованим. Результати проведеного аналізу дають підстави запропонувати багаторівневу методологічну архітектуру дослідження безпекоорієнтованого

Таблиця 1

Систематизація методологічних складових дослідження безпекоорієнтованого менеджменту підприємства

Методологічний рівень	Складові	Роль у дослідженні	Обмеження або ризик змішування
1	2	3	4
Теоретико-методологічні засади	системний, складнісно-адаптивний, соціотехнічний	визначають спосіб бачення підприємства, складність взаємозв'язків і взаємодію людей та технологій	не замінюють конкретного дизайну й методів
Управлінське ядро	процесний, стратегічний, ризик-орієнтований, резильєнтнісний, структурно-функціональний, ситуаційний, динамічних здатностей	розкривають логіку управління, процеси, механізми адаптації, відновлення та розвитку	часткове концептуальне перетинання потребує чіткого розмежування
Спеціальні управлінські контури	безпекове врядування, BCM, кризовий менеджмент	формують відповідальність, безперервність, реагування і навчання	кожен контур є вужчим за безпеко-орієнтований менеджмент

Завершення таблиці 1

1	2	3	4
Контекстні лінзи	інституційна, стейкхолдерська, екосистемна	визначають середовище, інтереси, залежності та межі застосування	можуть розмити одиницю аналізу
Принципи	превентивність, людиноцентричність, місієорієнтованість, партисипативність, пропорційність, навчання	задають нормативну орієнтацію системи	не є рівнопорядковими теоретичним підходам
Дизайн дослідження	багаторівневий sequential mixed-method, триангуляція	визначає послідовність і спосіб поєднання доказів	не є ще однією теоретичною концепцією
Методи	контент-аналіз, Delphi, опитування, EFA/CFA, SEM, case study, process tracing, сценарний аналіз, стрес-тести	забезпечують отримання й аналіз наукових доказів	окремий метод не охоплює весь конструкт
Інструменти	SWOT, PESTEL, risk matrix, FMEA, Bow-Tie, BIA, модель зрілості, dashboard	забезпечують прикладну реалізацію методів у менеджменті	не повинні трактуватися як методологія дослідження

Джерело: авторська систематизація, сформована на основі аналізу праць [2; 5; 6; 10; 14–25]

менеджменту підприємства і її призначення полягає в тому, щоб пов'язати теоретичне розуміння об'єкта із програмою емпіричного дослідження та подальшим формуванням прикладного інструментарію (рис. 1).

Архітектура включає п'ять взаємопов'язаних рівнів:

перший рівень – теоретичне бачення підприємства як відкритої соціально-економічної системи, складної адаптивна система та соціотехнічної організації, що дозволяє враховувати внутрішні та зовнішні взаємозалежності, нелінійність, поведінкові фактори, технологічні компоненти та емерджентні ефекти;

другий рівень – управлінське ядро і на ньому інтегруються: стратегічне спрямування; ризик-орієнтоване управління; резильєнтнісні спроможності; процесна організація; безпекове врядування; динамічні здатності та визначаються, як безпекові критерії вбудовуються у місію, цілі, структури, процеси, рішення та ресурсну конфігурацію;

третій рівень – контекст і межі на якому контекстні лінзи пояснюють, чому конфігурація безпекоорієнтованого менеджменту має відрізнятися залежно від інституційного середовища, галузі, стейкхолдерів, мережевих залежностей та типів загроз;

четвертий рівень – дизайн дослідження під час якого визначається послідовність отримання доказів, одиниці аналізу, джерела даних і способи триангуляції;

п'ятий рівень – методична та прикладна реалізація і він охоплює методи операціоналізації, вимірювання, перевірки валідності, моделювання та управлінські інструменти, які в подальшому можуть бути використані для оцінювання, порівняння і розвитку системи.

Принципова особливість запропонованої архітектури полягає у тому, що її рівні не є ізольованими: теоретична основа визначає вибір управлінського ядра; управлінське ядро формує домени і процеси; контекстні лінзи встановлюють межі застосування; дизайн визначає спосіб отримання доказів; методи та інструменти забезпечують операціоналізацію.

Тобто архітектура є не статичною класифікацією, а логікою переходу від абстрактного до конкретного. Методологічна архітектура має бути доповнена процесною моделлю, оскільки безпекоорієнтований менеджмент проявляється не лише у структурі системи, а й у динаміці її функціонування. Відповідно до цього ми пропонуємо використовувати адаптований інтегрований цикл який доцільно інтерпретувати як сім взаємопов'язаних управлінських фаз (рис. 2).

Передбачення охоплює аналіз середовища, виявлення слабких сигналів, нових ризиків, залежностей і потенційних каскадних ефектів і його завданням є не точне прогнозування майбутнього, а розширення поля управлінської уваги й підготовка до кількох можливих сценаріїв. На фазі запобігання та підготовки формуються політики, бар'єри, резерви, альтернативні процедури, плани, компетентності та системи раннього реагування. Запобігання зменшує ймовірність реалізації загрози, а підготовка – потенційні наслідки. Фаза поглинання впливу та підтримання безперервності характеризує здатність підприємства витримувати негативний вплив без критичного руйнування основних функцій і безпосередньо пов'язана з резервуванням, диверсифікацією,

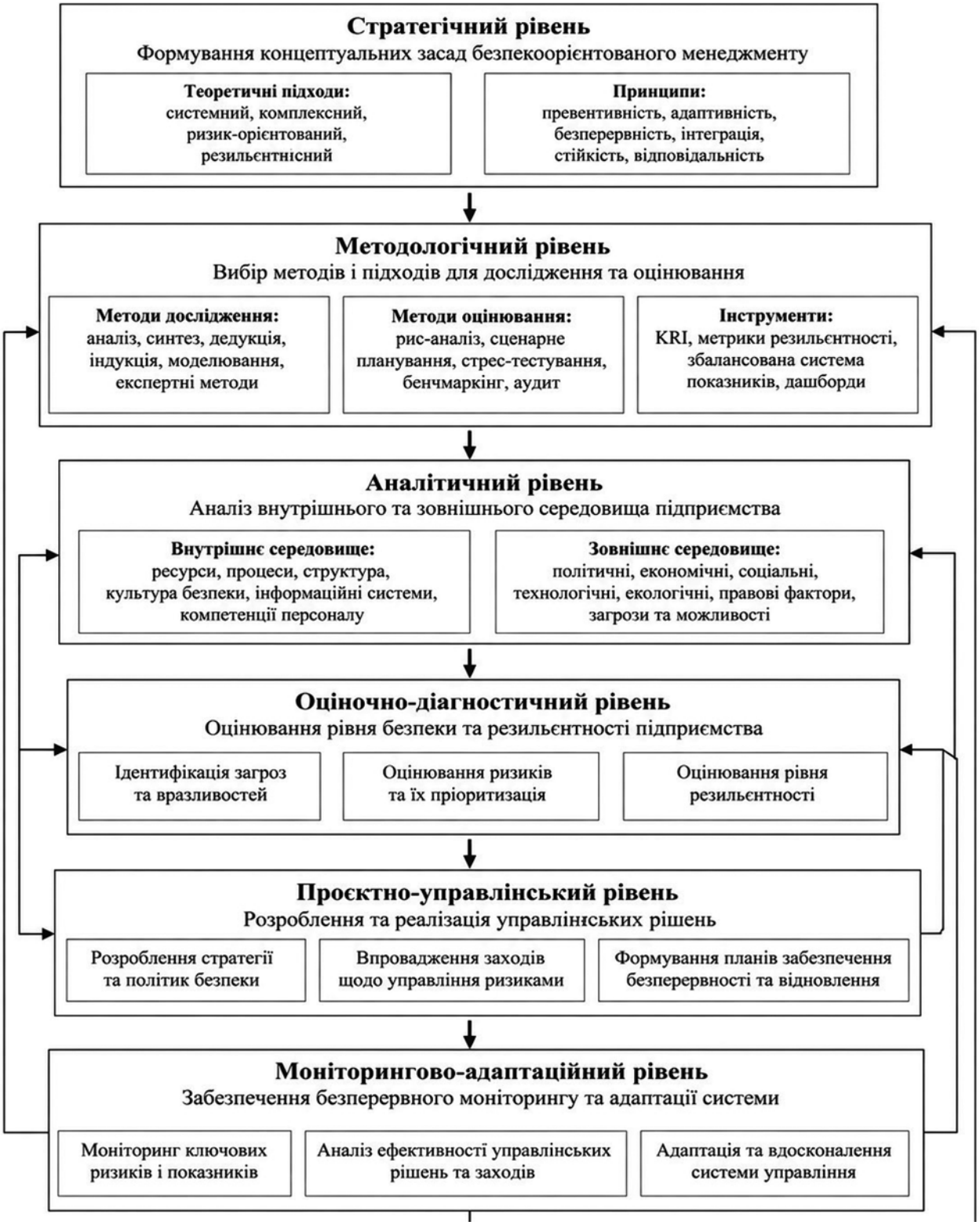

Рис. 1. Багаторівнева методологічна архітектура дослідження безпекоорієнтованого менеджменту підприємства

Джерело: авторська розробка

гнучкістю ресурсів, критичними процесами та допустимими рівнями погіршення результативності. Реагування передбачає оперативне прийняття рішень, активацію планів, комунікацію, координацію, захист людей і критичних активів, а також перерозподіл ресурсів. Відновлення означає повернення критичних процесів до прийнятного рівня, а не обов'язково до попереднього стану. В окремих випадках повернення до попередньої конфігурації може бути неефективним або

Рис. 2. Процесний цикл безпекоорієнтованого менеджменту підприємства

Джерело: авторська розробка

неможливим. На фазі адаптації та трансформації підприємство змінює процеси, структуру, технології, компетентності, партнерства або бізнес-модель відповідно до нових умов та відбувається поєднання безпекоорієнтованого менеджменту з розвитком.

Організаційне навчання забезпечує аналіз інцидентів, перегляд припущень, оновлення реєстрів ризиків, політик, сценаріїв, процедур і ресурсних рішень. Без цього процесний цикл не замикається, а система відтворює попередні вразливості. Представлений цикл не має виключно лінійного характеру, зокрема, окремі фази можуть відбуватися паралельно, повторюватися або змінювати послідовність залежно від типу загрози. Наприклад, під час тривалого воєнного збурення підприємство одночасно реагує, відновлює окремі процеси, адаптує структуру і продовжує передбачати нові ризики.

Запропонована архітектура має концептуальний характер і потребує операціоналізації, тобто переходу від теоретичних категорій до вимірюваних конструктів, показників, шкал і процедур емпіричної перевірки. Для цього, на нашу думку, доцільно застосувати послідовний змішаний дизайн, у якому кожний наступний етап спирається на результати попереднього (табл. 2).

Принциповим методологічним положенням є відмова від використання одного інтегрального індексу як єдиного доказу рівня безпекоорієнтованого менеджменту, а інтегральна оцінка має супроводжуватися профілем складових, аналізом чутливості, процесними даними та показниками результативності під реальними або змодельованими збуреннями.

Важливо зазначити, що заклади вищої освіти є специфічною емпіричною базою дослідження безпекоорієнтованого менеджменту і, на нашу

Таблиця 3

Послідовність операціоналізації методології дослідження

Етап	Метод	Основний результат	Значення для подальшого дослідження
1	систематичний огляд, контент-аналіз	кодбук понять, доменів, процесів і результатів	формування теоретичної основи
2	Delphi	уточнений перелік доменів та індикаторів	змістова валідність
3	AHP / MCDA	ваги й пріоритети критеріїв	побудова профілю та агрегування
4	опитування, EFA/CFA, SEM	вимірювальна і структурна модель	конструктна валідність
5	адміністративні та процесні дані	об'єктивні показники результативності	критеріальна валідність
6	case study, process tracing	механізми й контекстні умови	пояснення динаміки
7	сценарний аналіз, stress-testing	поведінка системи під шоками	перевірка стійкості
8	модель зрілості, dashboard	прикладний управлінський інструментарій	впровадження і моніторинг

Джерело: авторська розробка

думку, їх доцільно розглядати не як статистично репрезентативні аналоги всіх підприємств, а як критичні, інформаційно насичені кейси, у яких виразно проявляються взаємозв'язки різних безпекових доменів. До ЗВО без суттєвих змін можуть бути перенесені загальні принципи ризик-менеджменту, менеджменту безперервності, кризового лідерства, інформаційної безпеки, сценарного аналізу, stress-testing та навчання після інцидентів, проте низка характеристик потребує адаптації (табл. 3).

Таким чином, ЗВО є доцільною базою для апробації методології, оскільки дозволяє дослідити взаємодію фізичної, цифрової, кадрової, фінансової, психосоціальної, академічної та репутаційної безпеки за умов реальних екстремальних збурень але результати потребують обережної аналітичної генералізації, оскільки публічна місія, академічна свобода, колегіальність і неприбуткова логіка змінюють критерії результативності порівняно з комерційними підприємствами.

Висновки. Проведене дослідження дозволило сформувати теоретико-методологічні засади дослідження безпекоорієнтованого менеджменту підприємства та обґрунтувати логіку їх подальшої операціоналізації:

– встановлено, що сучасне наукове поле формується на перетині економічної безпеки підпри-

Таблиця 3

Напрями адаптації методології безпекоорієнтованого менеджменту до ЗВО

Домен	Специфіка ЗВО	Необхідна адаптація	Приклади індикаторів
Врядування	автономія, колегіальність, розподілена відповідальність	RACI, кризове делегування, нагляд	час рішення, виконання рішень, evidence of oversight
Освітня безперервність	календарні й акредитаційні обмеження	BIA програм, резервні LMS, alternative delivery	RTO/RPO LMS, частка відновлених курсів
Наукова безпека	дані, IP, лабораторії, міжнародні партнери	класифікація активів, резервування, access control	втрати даних, простої лабораторій
Фізична безпека	кампуси, укриття, евакуація, енергозалежність	drills, backup power, site assessment	час оповіщення, автономність, покриття укриттями
Кібербезпека	відкриті мережі, BYOD, висока ротація	ISMS, MFA, segmentation, incident response	MFA coverage, MTTD/MTTR, recovery tests
Психосоціальна безпека	війна, переміщення, вигорання	підтримка, workload management, safe reporting	wellbeing, burnout, психологічна безпека
Фінансова стійкість	публічне фінансування, демографія, гранти	scenario budgeting, liquidity buffer	liquidity days, концентрація доходів
Людський капітал	дефіцит критичних компетентностей	succession, cross-training, retention	bus factor, turnover, competence readiness
Репутація і доброчесність	залежність легітимності від довіри	integrity governance, crisis communication	порушення, time-to-disclose, trust measures

Джерело: адаптовано автором за [5–9]

ємства, ризик-менеджменту, security governance, менеджменту безперервності діяльності, кризового менеджменту, кібербезпекового врядування та організаційної резильєнтності. Жодна із зазначених концепцій не є повним еквівалентом безпекоорієнтованого менеджменту, оскільки охоплює лише окремий функціональний, процесний, governance- або спроможнісний контур;

– обґрунтовано визначення безпекоорієнтованого менеджменту підприємства як інтегрованої системи врядування, стратегічного спрямування, управлінських процесів, рішень і організаційних спроможностей, у якій безпекові та резильєнтнісні критерії вбудовано у досягнення місії й розвиток підприємства через цикл передбачення, запобігання, підготовки, поглинання впливу, підтримання безперервності, реагування, відновлення, адаптації, трансформації та організаційного навчання;

– виявлено три основні прогалини сучасних досліджень: інтеграційно-концептуальну; категоріально-методологічну; операціоналізаційно-валідаційну. Для їх подолання запропоновано багаторівневу методологічну архітектуру, що охоплює теоретико-методологічну основу, управлінське ядро, контекстні лінзи, дизайн дослідження, методи та прикладні інструменти, сформовано процесний цикл безпекоорієнтованого менеджменту та запропоновано програму операціоналізації на основі послідовного змішаного дизайну, яка включає систематичний огляд і контент-аналіз, Delphi, багатокритеріальне оцінювання, EFA/CFA, адміністративні дані, case study, process tracing, сценарний аналіз і стрес-тестування;

– обґрунтовано доцільність використання закладів вищої освіти України як критичних інформаційно насичених кейсів, адже їхня специфіка вимагає врахування академічної місії, автономії, колегіальності, освітньої та наукової безперервності, фізичної, кібернетичної, психосоціальної, фінансової, кадрової та репутаційної безпеки.

Подальші дослідження мають бути спрямовані на: визначення доменної структури безпекоорієнтованого менеджменту; формування системи критеріїв та індикаторів; розроблення вимірювальної шкали; експертну і психометричну валідацію; побудову профілю спроможностей; розроблення моделі зрілості; проведення сценарного аналізу та стрес-тестування на матеріалах закладів вищої освіти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гаркуша В. О., Єршова Н. Ю. Систематизація наукових поглядів щодо сутності поняття «економічна безпека підприємства». *Економіка та суспільство.* 2021. № 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-34

2. Тітенко З. М. Теоретичні основи фінансової безпеки підприємства. *Економіка та суспільство.* 2022. № 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-76

3. Гринкевич С. С. Еволюція теоретичних концепцій економічної безпеки підприємства. *Економіка та суспільство.* 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-70

4. Яструбецька Л. С. Концептуальні підходи до вивчення чинників фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних агресій та воєнного стану. *Економіка та суспільство.* 2023. № 54. DOI: https://doi.org/10.32782/2524-0072/2023-54-82

5. Герасименко О. М. Ризик-орієнтоване управління в системі економічної безпеки підприємства : дис. ... д-ра екон. наук : 21.04.02. Київ : Університет економіки та права «КРОК», 2021.

6. Гриценко Л. Л., Кожушко І. О., Чепурко В. О., Перепелицин Г. Б. Ризик-орієнтоване управління в системі економічної безпеки корпоративного підприємства. *Бізнес Інформ.* 2023. № 8. С. 281–288. DOI: https://doi.org/10.32983/2222-4459-2023-8-281-288

7. Hillmann J., Guenther E. Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews.* 2021. Vol. 23, No. 1. P. 7–44. DOI: https://doi.org/10.1111/ijmr.12239

8. Raetze S., Duchek S., Maynard M. T., Kirkman B. L. Resilience in Organizations: An Integrative Multilevel Review and Editorial Introduction. *Group & Organization Management.* 2021. Vol. 46, No. 4. P. 607–656. DOI: https://doi.org/10.1177/10596011211032129

9. Baghersad M., Zobel C. W. Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies. *Risk Analysis.* 2022. Vol. 42. P. 561–579. DOI: https://doi.org/10.1111/risa.13769

10. Akpinar H., Ozer-Caylan D. Achieving Organizational Resilience through Complex Adaptive Systems Approach: A Conceptual Framework. *Management Research.* 2022. Vol. 20, No. 4. P. 289–309. DOI: https://doi.org/10.1108/MRJIAM-01-2022-1265

11. Galaitsi S. E., Pinigina E., Keisler J. M., Pescaroli G., Keenan J. M., Linkov I. Business Continuity Management, Operational Resilience, and Organizational Resilience: Commonalities, Distinctions, and Synthesis. *International Journal of Disaster Risk Science.* 2023. Vol. 14. P. 713–721. DOI: https://doi.org/10.1007/s13753-023-00494-x

12. International Organization for Standardization. *ISO 22301:2019. Security and Resilience – Business Continuity Management Systems – Requirements.* Geneva : ISO, 2019.

13. International Organization for Standardization. *ISO 22336:2024. Security and Resilience – Organizational Resilience – Guidelines for Resilience Policy and Strategy.* Geneva : ISO, 2024.

14. International Organization for Standardization. *ISO 22361:2022. Security and Resilience – Crisis Management – Guidelines.* Geneva : ISO, 2022.

15. Melaku H. M. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy.* 2023. Vol. 3, No. 3. P. 327–350. DOI: https://doi.org/10.3390/jcp3030017

16. Cheng E. C. K., Wang T. Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information.* 2022. Vol. 13, No. 4. Article 192. DOI: https://doi.org/10.3390/info13040192

17. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0.* Gaithersburg, MD : NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29

18. Момот Т. В., Філонич О. М., Косяк А. П., Лобач О. О. Збалансована система показників забезпечення безпекоорієнтованого управління підприємств будівельної галузі. *Сучасний стан наукових досліджень та технологій в промисловості.* 2021. № 2(16). С. 54–62. DOI: https://doi.org/10.30837/ITSSI.2021.16.054

19. Івченко А. Г. Безпекоорієнтований розвиток підприємства: вектори, можливості та загрози. *Бізнес Інформ.* 2023. № 12. С. 368–378. DOI: https://doi.org/10.32983/2222-4459-2023-12-368-378

20. Кудріна О. Ю., Івченко А. Г. Стратегія безпекоорієнтованого розвитку підприємства: компонентний підхід. *Цифрова економіка та економічна безпека.* 2024. № 2(11). С. 95–102. DOI: https://doi.org/10.32782/dees.11-15

21. Галгаш М. Р. Проблематика формування безпекоорієнтованого управління в організаціях. *Вісник Східноукраїнського національного університету імені Володимира Даля.* 2024. № 4(284). С. 5–14. DOI: https://doi.org/10.33216/1998-7927-2024-284-4-5-14

22. Мороз Р. В., Загороднюк О. В. Постулати безпекоорієнтованого управління підприємством. *Економіка та суспільство.* 2024. № 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-116

23. Гавловська Н. І., Кримчак О. С., Подгала В. В. Формування пріоритетів безпекоорієнтованого управління підприємствами в умовах турбулентності зовнішнього середовища. *Modeling the Development of the Economic Systems.* 2024. № 11. DOI: https://doi.org/10.31891/mdes/2024-11-41

REFERENCES

1. Harkusha V. O., Yershova N. Yu. (2021). Systematization of scientific views on the essence of the concept of enterprise economic security. *Economy and Society.* No. 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-34

2. Titenko Z. M. (2022). Theoretical foundations of enterprise financial security. *Economy and Society.* No. 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-76

3. Hrynkevych S. S. (2023). Evolution of theoretical concepts of enterprise economic security. *Economy and Society.* No. 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-70

4. Yastrubetska L. S. (2023). Conceptual approaches to studying the factors of financial security of business entities in Ukraine under hybrid aggression and martial law. *Economy and Society.* No. 54. DOI: 1https://doi.org/0.32782/2524-0072/2023-54-82

5. Herasymenko O. M. (2021). *Risk-oriented management in the system of enterprise economic security. Doctoral Dissertation in Economics* (21.04.02). Kyiv: KROK University.

6. Hrytsenko L. L., Kozhushko I. O., Chepurko V. O., Perepelytsyn H. B. (2023). Risk-oriented management in the system of economic security of a corporate enterprise. *Business Inform.* No. 8. P. 281–288. DOI: https://doi.org/10.32983/2222-4459-2023-8-281-288

7. Hillmann J., Guenther E. (2021). Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews.* Vol. 23, No. 1. P. 7–44. DOI: https://doi.org/10.1111/ijmr.12239

8. Raetze S., Duchek S., Maynard M. T., Kirkman B. L. (2021). Resilience in Organizations: An Integrative Multilevel Review and Editorial Introduction. *Group & Organization Management.* Vol. 46, No. 4. P. 607–656. DOI: https://doi.org/10.1177/10596011211032129

9. Baghersad M., Zobel C. W. (2022). Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies. *Risk Analysis.* Vol. 42. P. 561–579. DOI: https://doi.org/10.1111/risa.13769

10. Akpinar H., Ozer-Caylan D. (2022). Achieving Organizational Resilience through Complex Adaptive Systems Approach: A Conceptual Framework. *Management Research.* Vol. 20, No. 4. P. 289–309. DOI: https://doi.org/10.1108/MRJIAM-01-2022-1265

11. Galaitsi S. E., Pinigina E., Keisler J. M., Pescaroli G., Keenan J. M., Linkov I. (2023). Business Continuity Management, Operational Resilience, and Organizational Resilience: Commonalities, Distinctions, and Synthesis. *International Journal of Disaster Risk Science.* Vol. 14. P. 713–721. DOI: https://doi.org/10.1007/s13753-023-00494-x

12. International Organization for Standardization. (2019). *ISO 22301:2019. Security and Resilience – Business Continuity Management Systems – Requirements*. Geneva: ISO.

13. International Organization for Standardization. (2024). *ISO 22336:2024. Security and Resilience – Organizational Resilience – Guidelines for Resilience Policy and Strategy.* Geneva: ISO.

14. International Organization for Standardization. (2022). *ISO 22361:2022. Security and Resilience – Crisis Management – Guidelines.* Geneva: ISO.

15. Melaku H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy.* Vol. 3, No. 3. P. 327–350. DOI: https://doi.org/10.3390/jcp3030017

16. Cheng E. C. K., Wang T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information.* Vol. 13, No. 4. Article 192. DOI: https://doi.org/10.3390/info13040192

17. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* Gaithersburg, MD: NIST. DOI: https://doi.org/10.6028/NIST.CSWP.29

18. Momot T. V., Filonych O. M., Kosiak A. P., Lobach O. O. (2021). Balanced scorecard for security-oriented management of construction enterprises. *Current State of Scientific Research and Technologies in Industry.* No. 2(16). P. 54–62. DOI: https://doi.org/10.30837/ITSSI.2021.16.054

19. Ivchenko A. H. (2023). Security-oriented enterprise development: vectors, opportunities and threats. *Business Inform.* No. 12. P. 368–378. DOI: https://doi.org/10.32983/2222-4459-2023-12-368-378

20. Kudrina O. Yu., Ivchenko A. H. (2024). Strategy of security-oriented enterprise development: a component approach. *Digital Economy and Economic Security.* No. 2(11). P. 95–102. DOI: https://doi.org/10.32782/dees.11-15

21. Halhash M. R. (2024). Problems of formation of security-oriented management in organizations. *Bulletin of Volodymyr Dahl East Ukrainian National University*. No. 4(284). P. 5–14. DOI: https://doi.org/10.33216/1998-7927-2024-284-4-5-14

22. Moroz R. V., Zahorodniuk O. V. (2024). Postulates of security-oriented enterprise management. *Economy and Society.* No. 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-116

23. Havlovska N. I., Krymchak O. S., Podhala V. V. (2024). Formation of priorities for security-oriented enterprise management under conditions of external environment turbulence. *Modeling the Development of the Economic Systems.* No. 11. DOI: https://doi.org/10.31891/mdes/2024-11-41

Bohdan Kolomiiets, *Poltava University of Economics and Trade.* ***Theoretical and methodological foundations of research on security-oriented enterprise management: a multilevel architecture and operationalization program.***

Annotation. *The article examines the theoretical and methodological foundations of security-oriented enterprise management under conditions of increasing complexity, uncertainty, and interdependence of contemporary threats. It is substantiated that traditional approaches to security management, focused on individual functional components or reactive risk response, do not ensure the required level of resilience and adaptability of enterprises in the modern security environment.* ***The purpose*** *of the article is to substantiate the theoretical and methodological foundations and develop a multilevel architecture for researching security-oriented enterprise management, which provides a conceptual distinction between related management constructs, integrates management and security approaches, and forms a framework for further operationalization and empirical validation.* ***The methodological framework*** *of the study comprises systemic, complex adaptive, sociotechnical, strategic, risk-oriented, and resilience-based approaches, as well as methods of analysis, synthesis, systematization, comparison, content analysis, and theoretical modeling. The place of security-oriented management within the system of contemporary management concepts is identified, and its distinction from enterprise economic security, risk management, crisis management, security governance, and organizational resilience is substantiated. The author proposes a definition of security-oriented enterprise management as an integrated system of governance, strategic direction, managerial processes, decisions, and organizational capabilities in which security and resilience criteria are embedded into the achievement of organizational mission and development objectives. A multilevel methodological architecture for research, a process cycle of security-oriented management, and an operationalization program based on a sequential mixed-method research design are developed. The expediency of using higher education institutions as critical information-rich cases for testing the proposed methodological approach is substantiated.* ***The practical significance of the obtained results*** *lies in the possibility of applying the proposed theoretical and methodological provisions for the development of assessment systems for security-oriented management, conducting empirical studies, forming capability profiles and maturity models, and designing managerial tools aimed at enhancing enterprise resilience and security under dynamic external challenges.*

Keywords: *security-oriented management, enterprise economic security, risk management, organizational resilience, security governance, business continuity management, crisis management, research methodology, operationalization, higher education institutions.*

Дата надходження статті: 17.07.2026
Дата прийняття статті до публікації: 15.08.2026
Дата публікації статті: 10.09.2026