

<https://doi.org/10.15407/econlaw.2026.01.118>
УДК 338.2

Федір НЕМИРОВСЬКИЙ, аспірант
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна
orcid.org/0009-0008-0219-8029

СТРАТЕГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІННОВАЦІЙНО-ІНФОРМАЦІЙНОЮ СКЛАДОВОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ

Ключові слова: стратегічне управління, інноваційно-інформаційна безпека, будівельні підприємства, матриця управлінських рішень, стратегічний моніторинг.

Обґрунтовано стратегічні підходи до управління інноваційно-інформаційною складовою економічної безпеки будівельних підприємств в умовах цифровізації та зростання невизначеності зовнішнього середовища. Сформовано систему принципів розроблення стратегій з урахуванням рівня економічної безпеки та причинно-наслідкових зв'язків між її складовими. На основі рівневого підходу розроблено типологію стратегій управління інноваційно-інформаційною складовою економічної безпеки будівельних підприємств, визначено їх цілі, пріоритети, ключові заходи та очікувані результати. Запропоновано інструментарій моніторингу реалізації стратегій і матрицю управлінських рішень для корекції стратегічних дій у разі відхилень від планових параметрів. Практична цінність дослідження полягає у можливості використання запропонованих підходів у системі стратегічного управління економічною безпекою будівельних підприємств.

Вступ. У сучасних умовах будівельний комплекс відіграє важливу роль у забезпеченні стійкого розвитку національної економіки, формуванні інфраструктурного потенціалу та реалізації інвестиційних проєктів. Однак будівельні підприємства функціонують в умовах підвищеної невизначеності, що зумовлена економічною нестабільністю, цифровою трансформацією та посиленням інформаційних ризиків [1].

Особливістю сучасного етапу розвитку будівельної галузі є інтенсивне впровадження цифрових технологій, інноваційних управлінських рішень і нових форматів організації бізнес-процесів [2, 3]. З одного боку, це створює передумови для підвищення ефективності та керованості проєктів, з іншого — нові ризики, пов'язані з інформаційною асиметрією, залежністю від цифрової інфраструктури та нерівномірністю інноваційного розвитку [4, 5]. За таких умов інноваційно-інформаційна складова економічної безпеки підприємства (далі ПСЕБП)

Ц и т у в а н н я: Немировський Ф. Стратегічні підходи до управління інноваційно-інформаційною складовою економічної безпеки будівельних підприємств. *Економіка та право*. 2026. № 1. С. 118—126. <https://doi.org/10.15407/econlaw.2026.01.118>

@ Видавець ВД «Академперіодика» НАН України, 2026. Стаття опублікована на умовах відкритого доступу за ліцензією CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

набуває самостійного значення та потребує цілеспрямованого стратегічного управління. Для будівельних підприємств характерний специфічний профіль загроз ПСЕБП: витік проектною документації та *VIM*-моделей, несанкціонований доступ до даних замовників і підрядників, істотна залежність від хмарних сервісів і зовнішніх ІТ-постачальників, нерівномірність цифрових компетентностей персоналу на різних рівнях організаційної ієрархії, а також низька інноваційна активність у поєднанні з недостатнім захистом об'єктів інтелектуальної власності. Ці загрози безпосередньо впливають на конкурентоспроможність і фінансову стійкість будівельних підприємств, що спричинює необхідність створення відповідних стратегічних інструментів управління.

У цьому контексті виникає потреба в розробленні стратегічних підходів до управління ПСЕБП, що враховуватимуть специфіку будівельного комплексу, диференційованість рівнів безпеки та динамічний характер загроз.

Аналіз останніх досліджень і публікацій.

Питання економічної безпеки підприємства активно досліджують українські та зарубіжні вчені. К. Зайченко та Н. Діма аналізують різні підходи до визначення економічної безпеки підприємств, розкриваючи ключові характеристики та структурні компоненти [6]. О. Заячківська зосереджується на принципах управління економічною безпекою підприємства [7]. М. Ско-

рик та співавт. систематизують наявні підходи до визначення поняття «економічна безпека підприємства» [8]. Л. Ковальська та співавт. визначають основні характеристики економічної безпеки підприємства та пропонують чотири стратегічні підходи: формування передумов безпеки, фокусування забезпечення безпеки, активізація процесів безпеки та підтримання статусу безпеки [9].

У зарубіжних дослідженнях також приділяють увагу проблемам економічної безпеки підприємств. Т. Primorac і співавт. досліджують концептуальні основи економічної безпеки підприємств, виділяючи внутрішні та зовнішні фактори загроз [10]. М. Jurgilewicz і співавт. аналізують сучасні виклики економічної безпеки підприємств, підкреслюючи посилення ролі цифровізації та інформаційних загроз у забезпеченні стійкості організацій [11].

Водночас, попри велику кількість наукових праць, недостатньо дослідженими залишаються питання формування саме стратегічних підходів до управління ПСЕБП, що охоплюють рівневу оцінку безпеки, пріоритизацію управлінських впливів та механізми стратегічного моніторингу з урахуванням ресурсних обмежень, особливо у контексті діяльності будівельних підприємств.

Метою статті є обґрунтування стратегічних підходів до управління ПСЕБП в умовах цифрової трансформації та зростання зовнішніх загроз.

Таблиця 1. Основні принципи для формування стратегій нівелювання загроз інноваційно-інформаційної складової економічної безпеки підприємства

| Принцип | Зміст |
|------------------------------------|---|
| Диференціації за рівнями ПСЕБП | Формування стратегії здійснюється з урахуванням поточного рівня ПСЕБП; кожному рівню відповідає специфічний тип стратегії з власними цілями, горизонтом планування та пріоритетами. Перехід між рівнями має поетапний характер і не допускає реалізації стратегій, невідповідних фактичному стану ПСЕБП |
| Причинно-наслідкової пріоритизації | Розподіл ресурсів між складовими ПСЕБП здійснюється з урахуванням причинно-наслідкових зв'язків, виявлених методом <i>DEMATEL</i> |
| Критичних обмежень | Стратегічні заходи зосереджуються на складовій ПСЕБП з найнижчим значенням часткового індексу, яка є «вузьким місцем» системи та лімітує можливість переходу підприємства на вищий рівень ПСЕБП |
| Мінімально життєздатної безпеки | Для підприємств з обмеженими ресурсами стратегія передбачає реалізацію мінімально необхідного набору заходів, достатнього для досягнення мінімального задовільного рівня ПСЕБП, з відтермінуванням опціональних ініціатив |
| Адаптивності горизонту планування | Горизонт стратегічного планування коригується залежно від рівня ПСЕБП: для нижчих рівнів застосовується коротко- та середньострокове планування, для вищих — середньо- та довгострокове, з урахуванням невизначеності та ресурсних обмежень |

Джерело: розроблено автором.

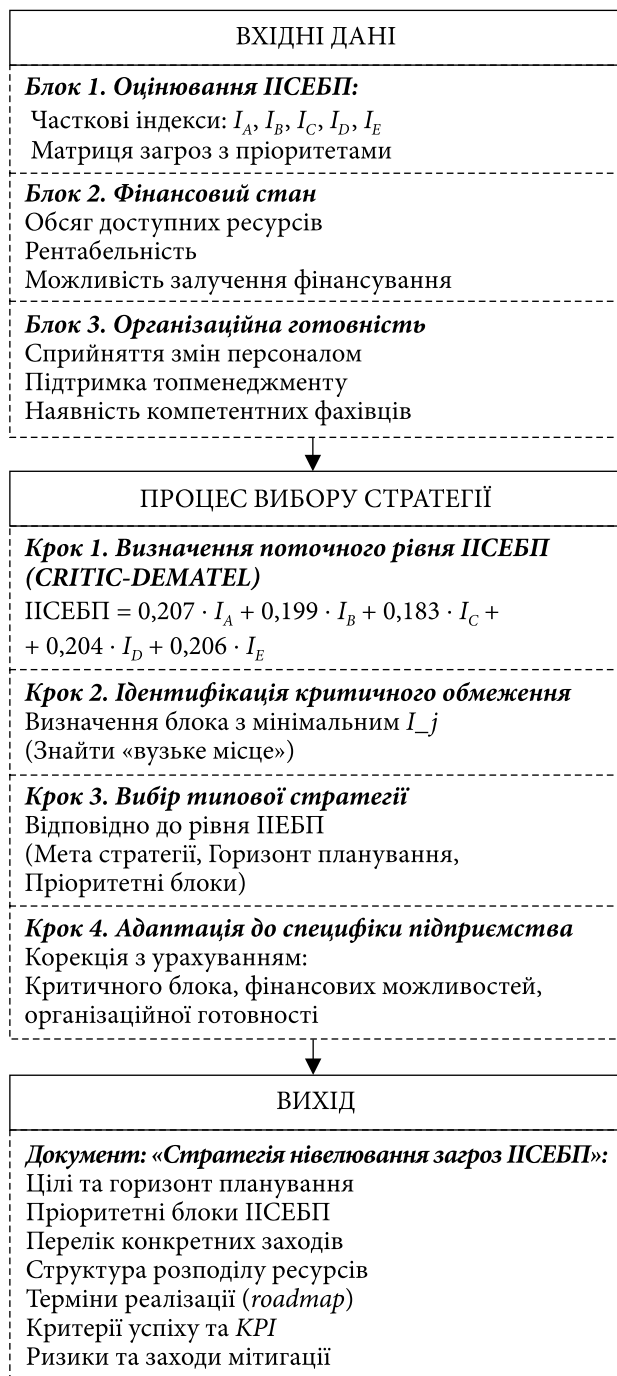


Рис. 1. Концептуальна модель вибору стратегії нівелювання загроз інноваційно-інформаційної складової економічної безпеки підприємства

Джерело: розроблено автором.

Для досягнення мети визначено такі завдання: обґрунтувати систему принципів формування стратегій забезпечення ПСЕБП; розробити типологію стратегій і концептуальну модель їх вибору залежно від рівня безпеки та ресурсних можливостей підприємства; запропонувати систему моніторингу реалізації стратегій та мат-

рицю ухвалення управлінських рішень у разі виявлення відхилень від планових показників.

Результати дослідження. Стратегічне управління ПСЕБП має ґрунтуватися на чітких концептуальних засадах, що враховують специфіку будівельного комплексу, динамічний характер загроз та обмеженість ресурсів підприємств.

ПСЕБП розглядається як інтегрована система з п'яти взаємопов'язаних блоків: *A* — інформаційного (рівень зрілості IT-інфраструктури, цифровізація бізнес-процесів, інтеграція інформаційних систем); *B* — інноваційного (частка інноваційних технологій, інноваційна активність); *C* — кадрового (цифрові компетентності, частка IT-фахівців); *D* — безпекового (кіберзахист, наявність сертифікатів безпеки); *E* — управлінського (ефективність проектного управління, ухвалення рішень на основі даних). Рівень ПСЕБП визначається через інтегральний індекс економічної безпеки (*IES*) за формулою:

$$\text{ПСЕБП} = 0,207 \cdot I_A + 0,199 \cdot I_B + 0,183 \cdot I_C + 0,204 \cdot I_D + 0,206 \cdot I_E,$$

де вагові коефіцієнти блоків визначено методом *DEMATEL* на основі аналізу причинно-наслідкових зв'язків, а часткові індекси блоків — методом *CRITIC* з урахуванням варіативності та міжкритеріальної кореляції 20 показників. Апробація методики на 10 будівельних підприємствах Київського регіону (з чисельністю персоналу від 50 до 500 осіб) засвідчила значну диференціацію рівнів безпеки: від 0,32 до 0,75, що охоплює діапазон від «низького» до «достатнього» рівня. Це актуалізує потребу в розробленні диференційованих стратегій забезпечення ПСЕБП залежно від рівня безпеки конкретного підприємства.

Логіка стратегічного управління ПСЕБП передбачає три послідовні етапи: 1) формування принципів, що визначають загальну філософію та обмеження стратегії; 2) розроблення типології стратегій і концептуальної моделі їх вибору залежно від рівня безпеки та ресурсних можливостей підприємства; 3) створення інструментарію моніторингу реалізації стратегії та ухвалення управлінських рішень. Розглянемо кожен із цих етапів детально.

Формування ефективних стратегій нівелювання загроз ПСЕБП вимагає чіткого базису, що визначатиме логіку управлінських рішень та послідовність їх реалізації. На основі узагальнення наукових підходів до стратегічного управ-

Таблиця 2. Порівняльна характеристика стратегій нівелювання загроз інноваційно-інформаційної складової економічної безпеки підприємства

| Параметр | Назва стратегії * | | | | |
|---------------------------------|---|---|--|---|--|
| | Антикризове реагування | Стабілізація | Поступовий розвиток | Акселерація | Інноваційне лідерство |
| Рівень ПСЕБП | 0,00—0,20 | 0,21—0,40 | 0,41—0,60 | 0,61—0,80 | 0,81—1,00 |
| Головна мета | Виживання | Базова захищеність | Системний розвиток | Інноваційно-технологічне лідерство | Екосистемне лідерство |
| Горизонт планування | 3—6 міс. | 1—2 роки | 2—3 роки | 3—5 років | 5—7 років і більше |
| Пріоритетні блоки (%) ** | D (50), E (30), A (20) | D (40), B (25), E (20) | A (30), C (25), B (25) | E (30), B (30), C (25) | B (45), E (25), C (20) |
| Ключовий фокус | Усунення критичних загроз безпеці | Формування базового захисту та управління | Модернізація інфраструктури та розвиток персоналу | Упровадження передових технологій | Створення R&D-центру та <i>tech</i> -продуктів |
| Основні заходи | Аварійний аудит; базові засоби захисту; <i>backup</i> ; кризовий менеджер | SIEM / SOC; політика ІБ; перший BIM-пілот; базова стратегія | Модернізація ІТ; 3—5 BIM-проектів; <i>innovation Lab</i> ; масове навчання | BIM 5D / 6D; AI-прогнозування; R&D-підрозділ; корпоративний університет | R&D-центр 20+ осіб; портфель патентів; акселератор стартапів; міжнародна експансія |
| Залучення зовнішньої експертизи | Критично (понад 90 % заходів) | Високе (60—70 %) | Середнє (40—50 %) | Низьке (20—30 %) | Партнерства (10—15 %) |
| Фокус інновацій | Відсутній (виживання) | Пілоты (1—2 проекти) | Масштабовані впровадження (3—5) | Передові технології (5—10) | Створення власних технологій (більше 10) |
| Роль персоналу | Виконавці антикризових заходів | Навчання базовим навичкам (60 %) | Активні учасники трансформації (70 %) | Драйвери інновацій (понад 80 % з <i>advanced</i> -компетенціями) | Творці знань (корпоративний університет, R&D) |
| KPI успіху *** | ПСЕБП $\geq 0,21$; без критичних інцидентів 1 міс. | ПСЕБП $\geq 0,41$; $I_D \geq 0,30$; 1—2 інновації | ПСЕБП $\geq 0,61$; усі $I_j \geq 0,60$; BIM на понад 60 % проектів | ПСЕБП $\geq 0,81$; усі $I_j \geq 0,75$; 3—5 інновацій / рік | ПСЕБП $\geq 0,90$; усі $I_j \geq 0,85$; 15—25 патентів; <i>tech</i> -виручка 60—80 млн/рік |
| Очікуваний ROI *** | Негативний (інвестиція у виживання) | 50—100 % (економія від безпеки) | 150—250 % (оптимізація процесів) | 200—300 % (конкурентні переваги) | 200—400 % (нові бізнес-моделі + капіталізація) |
| Термін окупності *** | Не застосовується | 3—4 роки | 4—5 років | 5—7 років | 7—10 років |
| Головний ризик | Недостатність фінансування | Відтік фахівців, невдача пілотів | Перевантаження персоналу змінами | Технологічне застарівання | Недостатність ROI від R&D |

* Пріоритетні блоки ПСЕБП, визначені за результатами причинно-наслідкового аналізу DEMATEL. ** Стратегії розроблено з урахуванням специфіки будівельних підприємств: проектного характеру діяльності, залежності від зовнішніх ІТ-постачальників та диференційованості цифрових компетентностей персоналу; можуть бути адаптовані до підприємств інших галузей шляхом коригування порогових значень. *** Наведено на основі апробації методики оцінювання ПСЕБП на 10 будівельних підприємствах Київського регіону; для підприємств інших галузей або регіонів рекомендується врахувати специфіку.

Джерело: розроблено автором.

ління економічною безпекою [2, 4, 7] та практики функціонування будівельних підприємств обґрунтовано систему принципів, що має забезпечити відповідність стратегії реальному стану підприємства, ефективність використання обмежених ресурсів та можливість адаптації до змін зовнішнього середовища (табл. 1).

Запропоновані принципи формування стратегій є основою для розроблення практичного інструментарію стратегічного вибору. Проте для забезпечення структурованості й відтворюваності процесу ухвалення рішень необхідна модель, що інтегруватиме вхідну інформацію про стан підприємства, логіку вибору стратегії та специфіку її адаптації до конкретних умов. Концептуальна модель вибору стратегії нівелювання загроз ПСЕБП структурує процес стратегічного вибору через три послідовні блоки: вхідні дані, процес вибору стратегії та вихід (рис. 1).

Процес вибору стратегії реалізується за чотири послідовних кроки: 1) визначення поточного рівня ПСЕБП шляхом розрахунку інтегрально-

го показника за методикою *CRITIC-DEMATEL*; 2) ідентифікація критичного обмеження системи — блок з найнижчим значенням часткового індексу, що є «вузьким місцем» та лімітує можливість переходу підприємства на вищий рівень; 3) вибір типової стратегії відповідно до рівня ПСЕБП із визначенням мети, горизонту планування та пріоритетних блоків; 4) адаптація типової стратегії до специфіки підприємства з урахуванням критичного блока, фінансових можливостей та організаційної готовності.

Застосування концептуальної моделі на практиці вимагає наявності детально розробленої типології стратегій, що відповідають різним рівням ПСЕБП, адже кожен рівень економічної безпеки характеризується специфічним набором загроз, ресурсних обмежень і можливостей для розвитку, що визначає принципово різні стратегічні пріоритети.

Для кожної стратегії запропоновано комплекс характеристик, що дають змогу підприємству обрати найкращий варіант. Порівняльну харак-

Таблиця 3. Моніторинг реалізації на підприємстві інноваційно-інформаційної складової економічної безпеки підприємства

| Рівень моніторингу | Мета | Показники | Інструменти | Критерії втручання |
|---|---|--|--|--|
| Операційний моніторинг (щотижнево / щомісячно) | Контроль виконання окремих заходів | Виконання бюджету (план / факт по кожному заходу); дотримання термінів; використання ресурсів | Система управління проектами: трекінг завдань; щотижневі зустрічі команди реалізації стратегії; щомісячні звіти відповідальних за блоки | Відставання >1 міс. для критичних заходів; перевитрата бюджету >20 % для будь-якого заходу; більше трьох заходів зі статусом «заблоковані» |
| Тактичний моніторинг (щоквартально) | Оцінювання прогресу на рівні блоків та підприємства загалом | Зміна часткових індексів I_j (порівняння з базовим значенням); досягнення проміжних цілей (<i>milestone KPI</i>); ефективність витрат (витрати / приріст I_j) | Квартальна оцінка 10—15 ключових показників ПСЕБП; квартальний аналіз діяльності засідання стратегічного комітету; порівняння з плановою траєкторією | Приріст будь-якого I_j <50 % від запланованого; відставання від планової траєкторії ПСЕБП >0,05; негативна динаміка будь-якого блока (I_j зменшується замість зростання) |
| Стратегічний моніторинг (один раз на 6—12 міс.) | Всебічне оцінювання ефективності стратегії та ухвалення рішення про продовження / корекцію / заміну | Повний перерахунок ПСЕБП за методикою <i>CRITIC-DEMATEL</i> ; повторний аналіз причинно-наслідкових зв'язків; оцінювання бізнес-ефектів; порівняння з конкурентами (<i>benchmarking</i>) | Річне оцінювання ПСЕБП; стратегічна сесія топменеджменту (2—3 дні); зовнішній аудит (залучення консультантів для незалежного оцінювання раз на 2 роки) | ПСЕБП виріс на <50 % від запланованого за рік; зміна зовнішніх умов (нова регуляція, економічна криза, поява нових технологій); зміна стратегічних пріоритетів підприємства (наприклад, вихід на нові ринки) |

Джерело: розроблено автором.

теристика стратегій нівелювання загроз ПСЕБП систематизовано у табл. 2.

Однак вибір стратегії є лише першим кроком у забезпеченні ПСЕБП. Успішність реалізації обраної стратегії критично залежить від наявності дієвої системи моніторингу (табл. 3), що дасть можливість своєчасно виявляти відхилення від планових траєкторій та ухвалювати обґрунтовані рішення для коригування.

Проте реалізація стратегій економічної безпеки може призвести до того, що підприємство зіштовхнеться з типовими проблемними ситуаціями, для кожної з яких має бути розроблений набір адекватних коригувальних заходів (табл. 4). Для кожної ситуації матриця визначає: симптоми (як виявити проблему), діагноз

(у чому причина відхилення) та корекцію (конкретні управлінські дії для усунення проблеми). Така структура забезпечує швидкість та обґрунтованість реагування на відхилення, що є критично важливим в умовах обмеженого часу для ухвалення рішень.

Узагальнюючи результати дослідження, значимо, що застосування інтегрального індексу ПСЕБП, обчисленого за методикою *CRITIC-DEMATEL*, дає змогу не лише кількісно оцінити рівень економічної безпеки, а й визначити відповідні управлінські дії, що мають бути реалізовані для забезпечення стабільності та розвитку. В умовах збільшення цифрових ризиків, посилення інформаційної вразливості та підвищення турбулентності середовища будь-які

Таблиця 4. Матриця рішень у разі відхилення від плану реалізації стратегії

| Ситуація | Симптоми | Діагноз | Корекція |
|---------------------------------------|--|---|--|
| Недофінансування | Виконано <60 % заходів через відсутність коштів | Переоцінювання фінансових можливостей під час планування | Розтягнути стратегію на більше як 30—50 % часу; зосередження на мінімальних заходах; пошук зовнішнього фінансування |
| Відсутність компетенцій | Заходи виконані формально, без бажаного ефекту | Недостатня кваліфікація виконавців або опір змінам | Посилити блок С (навчання) більше ніж на 10—15 % бюджету; залучити зовнішніх експертів; запровадити програму управління організаційними змінами |
| Зміна пріоритетів через зовнішні шоки | Виконання йде за планом, але зовнішня загроза вимагає переорієнтації | Зміна ландшафту загроз | Екстремне перенаправлення 20—30 % бюджету на критичний блок (наприклад, D у разі кібератак); тимчасова пауза некритичних заходів |
| Перевиконання плану | ПСЕБП збільшилася на >120 % від запланованого значення | Консервативне оцінювання потенціалу або сприятливі умови | Прискорити перехід на стратегію наступного рівня; збільшити амбітність цілей (наприклад, орієнтуватися одразу на високий рівень замість достатнього) |
| Асиметричний розвиток блоків | Один блок виріс значно | Неправильна пріоритизація або нереалістичні цілі для слабких блоків | Перерозподіл бюджету на наступний період: зменшити фінансування «успішного» блока, компенсувавши тому, що відстає; використати сильний блок як «локомотив» для слабких (наприклад, сильні інновації стимулюють навчання персоналу) |
| Відтік ключових фахівців | Звільнення CIO, керівника R&D або інших основних виконавців | Недостатня мотивація, перевантаження або переманювання конкурентами | Екстремне підвищення компенсації ключовим фахівцям (більше 20—30 %); розподіл відповідальності (менша залежність від 1—2 осіб); довгострокові бонуси |
| Втрата підтримки топменеджменту | Менеджмент вимагає скорочення бюджету ПСЕБП або ставить під сумнів стратегію | Відсутність видимих результатів або зміна пріоритетів власників | Демонстрація <i>quick wins</i> (швидких перемог); фінансове обґрунтування ROI (розрахунок економії); <i>benchmark</i> з конкурентами (ризик відставання); у крайньому випадку — перехід на стратегію нижчого рівня (з меншим бюджетом) |

Джерело: розроблено автором.

управлінські рішення повинні бути адаптивними та залежними від того, у якому стані перебуває система економічної безпеки підприємства на певний момент часу.

Запропонований підхід базується на тому, що підприємство може бути у різних станах, які відображають принципово різний ступінь стійкості системи — від критичного до високого. Відповідно, стратегії управління не можуть бути універсальними, а мають диференціюватися залежно від діапазону ПСЕБП, що відображає здатність підприємства протистояти загрозам.

Запропонований підхід є важливим, оскільки інтегральний показник відіграє не тільки роль індикатора, а й сигналізує як про наявність загроз, так і про те, які саме стратегічні дії доцільні. Це дає змогу перейти від статичної оцінки до динамічної моделі управління, заснованої на принципах адаптивності, випереджувального розвитку та ресурсної достатності. Отже, розроблені стратегії є цілісними управлінськими концепціями, що інтегрують організаційні, економічні, інформаційні та інноваційні рішення відповідно до п'яти структурних блоків ПСЕБП.

Висновки. Обґрунтовано стратегічні підходи до управління інноваційно-інформаційною складовою економічної безпеки будівельних підприємств, що інтегрують принципи формування стратегій, типологію стратегічних альтернатив, концептуальну модель їх вибору та інструментарій моніторингу реалізації.

Розроблено систему з п'яти принципів формування стратегій забезпечення ПСЕБП. Запропоновано типологію п'яти базових стратегій, диференційованих за рівнем ПСЕБП: антикризове реагування, стабілізацію, поступовий розвиток, акселерацію, інноваційне лідерство. Визначено тривірневу систему моніторингу реалізації стратегій, що охоплює всі п'ять блоків ПСЕБП і дає змогу відстежувати прогрес досягнення цілей. Сформульовано матрицю ухвалення управлінських рішень у разі відхилен-

нях від планових показників, яка класифікує ситуації за масштабом відхилення та критичністю показника, а також допомагає скорегувати управлінські дії.

Практична значущість результатів полягає в можливості використання розробленого інструментарію будівельними підприємствами для формування та реалізації стратегій забезпечення інноваційно-інформаційної безпеки відповідно до їх індивідуальних характеристик та ресурсних можливостей. Запропонований підхід дає підприємствам можливість уникнути типових помилок, зокрема обрання надто амбітної стратегії за недостатності ресурсів або консервативної стратегії за наявності потенціалу для інноваційного прориву. Система моніторингу та матриця ухвалення рішень забезпечують інструментарій для регулярного контролю та своєчасного коригування стратегічних дій, що підвищує ймовірність досягнення цілей забезпечення економічної безпеки.

Обмеженнями дослідження є орієнтація на будівельний комплекс, адже для інших галузей економіки може знадобитися адаптування типології стратегій і системи показників моніторингу з урахуванням галузевої специфіки. Запропоновані стратегії є базовими, вони потребують конкретизації та деталізації для кожного підприємства з урахуванням його організаційної структури, корпоративної культури та конкурентного середовища. Оцінка довгострокової ефективності стратегій потребує проведення моніторингу фінансово-економічних результатів підприємств протягом щонайменше 3—5 років після впровадження обраних стратегій.

Перспективними напрямками подальших досліджень є розроблення цифрових інструментів автоматизації процесів моніторингу ПСЕБП на основі інтеграції з інформаційними системами підприємства (*ERP, CRM, BIM*), а також застосування технологій штучного інтелекту для прогнозування реалізації загроз.

СПИСОК ЛІТЕРАТУРИ

1. Фісуненко П., Пісклов О. Роль інформаційних технологій у забезпеченні економічної безпеки проєктно-орієнтованої будівельної організації. *Цифрова економіка та економічна безпека*. 2024. № 1 (10). С. 99—102. <https://doi.org/10.32782/dees.10-18>
2. Броварний Е., Замазій О., Янковська Г. Ціннісно-орієнтоване управління підприємствами будівельної галузі в умовах економічної нестабільності: аналіз та стратегічні орієнтири. *Modern Engineering and Innovative Technologies*. 2025. № 1 (39—01). С. 104—112. <https://doi.org/10.30890/2567-5273.2025-39-01-031>
3. Осадча О., Роздопченюк В. Цифровізація бізнес-процесів підприємства як інструмент економічної безпеки. *Вісник Національного університету водного господарства та природокористування*. 2025. № 109. С. 136—148. <https://doi.org/10.31713/ve1202513>

4. Шостак Л., Помазун О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека*. 2024. № 5 (14). С. 160—165. <https://doi.org/10.32782/dees.14-25>
5. Жовтяк Г., Богданов Р. Розвиток потенціалу будівельних підприємств в умовах цифровізації. *Економіка та суспільство*. 2025. № 75. <https://doi.org/10.32782/2524-0072/2025-75-64>
6. Зайченко К.С., Діма Н.І. Економічна безпека підприємства: сутність та роль. *Ефективна економіка*. 2021. № 5. <https://doi.org/10.32702/2307-2105-2021.5.90>
7. Заячківська О.В. Управління економічною безпекою підприємства: сутність, принципи, проблеми. *Вісник Національного університету водного господарства та природокористування*. 2022. № 100. С. 15—23. <https://doi.org/10.31713/ve420222>
8. Скорик М.О., Горбань С.Ю., Скрицька О.Ю. Сутність економічної безпеки підприємства як складника національної безпеки України. *Підприємництво та інновації*. 2020. № 11—1. С. 7—11. <https://doi.org/10.37320/2415-3583/11.1>
9. Ковальська Л., Голій О., Голій В. Економічна безпека підприємства: сутність, структура та механізм забезпечення. *Економічний форум*. 2023. № 1. С. 126—137. <https://doi.org/10.36910/6775-2308-8559-2023-1-16>
10. Primorac T., Kozina T., Turčić I. Economic Security of Enterprises. *Poslovna izvrsnost — Business excellence*. 2018. Vol. 12. No. 2. P. 167—175. <https://doi.org/10.22598/pi-be/2018.12.2.167>
11. Jurgilewicz M., Kozicki B., Piwowarski J., Grabowska S. Contemporary Challenges for the Economic Security of Enterprises in Poland. *Journal of Security and Sustainability Issues*. 2022. Vol. 12. Iss. 1. P. 71—80. <https://doi.org/10.47459/jssi.2022.12.6>

Дата надходження: 09.02.2026

Дата прийняття до друку: 09.02.2026

Дата публікації: 31.03.2026

REFERENCES

1. Fisunen P., Pisklov O. Rol informatsiinykh tekhnolohii u zabezpechenni ekonomichnoi bezpeky proiektno-oriientovanoi budivelnnoi orhanizatsii. *Tsyfrova ekonomika ta ekonomichna bezpeka*. 2024. No. 1 (10). P. 99-102. <https://doi.org/10.32782/dees.10-18> [in Ukrainian].
2. Brovarnyi E., Zamazii O., Yankovska, H. Tsinnisno-oriientovane upravlinnia pidprijemstvamy budivelnnoi haluzi v umovakh ekonomichnoi nestabilnosti: analiz ta stratehichni oriientyry. *Modern Engineering and Innovative Technologies*. 2025. No. 1 (39-01). P. 104-112. <https://doi.org/10.30890/2567-5273.2025-39-01-031> [in Ukrainian].
3. Osadcha O., Rozdopcheniuk V. Tsyfrovizatsiia biznes-protseviv pidprijemstva yak instrument ekonomichnoi bezpeky. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia*. 2025. No. 109. P. 136-148. <https://doi.org/10.31713/ve1202513> [in Ukrainian].
4. Shostak L., Pomazun O. Informatsiina bezpeka v konteksti innovatsiinoho rozvytku biznes-modeli vitchyznianskykh pidprijemstv v umovakh tsyfrovoy ekonomiky. *Tsyfrova ekonomika ta ekonomichna bezpeka*. 2024. No. 5 (14). P. 160-165. <https://doi.org/10.32782/dees.14-25> [in Ukrainian].
5. Zhovtiak H., Bohdanov R. Rozvytok potentsialu budivelnnykh pidprijemstv v umovakh tsyfrovizatsii. *Ekonomika ta suspilstvo*. 2025. No. 75. <https://doi.org/10.32782/2524-0072/2025-75-64> [in Ukrainian].
6. Zaichenko K.S., Dima N.I. Ekonomichna bezpeka pidprijemstva: sutnist ta rol. *Efektivna ekonomika*. 2021. No. 5. <https://doi.org/10.32702/2307-2105-2021.5.90> [in Ukrainian].
7. Zaiachkivska O.V. Upravlinnia ekonomichnoiu bezpekoiu pidprijemstva: sutnist, pryntsyepy, problemy. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia*. 2022. No. 100. P. 15-23. <https://doi.org/10.31713/ve420222> [in Ukrainian].
8. Skoryk M.O., Horban S.Yu., Skrytska O.Yu. Sutnist ekonomichnoi bezpeky pidprijemstva yak skladnyka natsionalnoi bezpeky Ukrainy. *Pidprijemnytstvo ta innovatsii*. 2020. No. 11-1. P. 7-11. <https://doi.org/10.37320/2415-3583/11.1> [in Ukrainian].
9. Kovalska L., Holii O., Holii V. Ekonomichna bezpeka pidprijemstva: sutnist, struktura ta mekhanizm zabezpechennia. *Ekonomichnyi forum*. 2023. No. 1. P. 126-137. <https://doi.org/10.36910/6775-2308-8559-2023-1-16> [in Ukrainian].
10. Primorac T., Kozina T., Turčić I. Economic Security of Enterprises. *Poslovna izvrsnost — Business excellence*. 2018. Vol. 12. No. 2. P. 167-175. <https://doi.org/10.22598/pi-be/2018.12.2.167>
11. Jurgilewicz M., Kozicki B., Piwowarski J., Grabowska S. Contemporary Challenges for the Economic Security of Enterprises in Poland. *Journal of Security and Sustainability Issues*. 2022. Vol. 12. Iss. 1. P. 71-80. <https://doi.org/10.47459/jssi.2022.12.6>

Date of receipt: 09.02.2026

Date of acceptance for publication: 09.02.2026

Date of publication: 31.03.2026

Fedir NEMYROVSKYI,
Postgraduate
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
orcid.org/0009-0008-0219-8029

STRATEGIC APPROACHES TO THE MANAGEMENT
OF THE INNOVATION-INFORMATION COMPONENT
OF ECONOMIC SECURITY IN CONSTRUCTION ENTERPRISES

The article substantiates strategic approaches to managing the innovation-information component of economic security of construction enterprises under conditions of digitalization and growing environmental uncertainty. The relevance of the study is determined by the fact that construction enterprises operate under a dual challenge: on the one hand, the need to implement digital technologies and innovations to ensure competitiveness, and on the other hand, the growth of information risks, cyber threats, and technological lag, which creates systemic threats to economic security. A system of five principles for strategy development has been formed: differentiation by security levels, cause-and-effect prioritization, critical constraints, minimally viable security, and planning horizon adaptability. These principles take into account the enterprise's security level and cause-and-effect relationships between its components. Based on the level-based approach, a typology of five strategies for managing the innovation-information component of economic security of construction enterprises has been developed according to security levels (critical, low, satisfactory, sufficient, high): crisis response, stabilization, gradual development, acceleration, and innovation leadership. For each strategy, goals, planning horizons (from 3—6 months to 5—7 years), priority development blocks, key measures, and expected results are defined. A conceptual model for strategy selection has been developed, structuring the process through four sequential steps: determining the current security level, identifying critical constraints, selecting a typical strategy, and adapting to enterprise specifics. A three-level toolkit for monitoring strategy implementation (operational, tactical, strategic) and a matrix of managerial decisions for correcting strategic actions in case of deviations from planned parameters have been proposed. The matrix covers seven typical deviation situations and defines adequate corrective actions. The practical value of the study lies in the possibility of using the proposed approaches in the strategic management system of economic security of construction enterprises, taking into account their resource capabilities and current state.

Keywords: strategic management, threat mitigation, economic security levels, strategic monitoring, adaptive planning.