УДК 005.591.6:005.334(477)

# БЕЗПЕКООРІЄНТОВАНИЙ МЕНЕДЖМЕНТ ІННОВАЦІЙ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ В УКРАЇНІ

Моісеєнко Є.Ю.
e-mail: yelyzaveta.moiseienko@nure.ua
Науковий керівник – д.е.н., проф. Перепелюкова О.В.
Харківський національний університет радіоелектроніки, каф. ЕК
м. Харків, Україна

The full-scale war in Ukraine has transformed innovation management, making security integration a critical success factor. This paper examines security-oriented innovation management as a system combining competitiveness objectives with systematic management of war-related threats, including cyberattacks on R&D systems, intellectual property theft, and physical infrastructure destruction. The proposed model is based on three principles: diversification of innovation resources, adaptive management, and cyber security. Effective implementation requires business process transformation, investments in protection technologies, and security culture development among innovation teams.

Управління інноваціями в умовах війни супроводжується значним ускладненням ризик-ландшафту. Традиційні моделі інноваційного менеджменту, орієнтовані на максимізацію швидкості виходу на ринок та відкриту співпрацю, вимагають фундаментального переосмислення. Організації стикаються з критичними загрозами: від промислового шпигунства та кібератак на R&D-підрозділи до фізичного знищення інноваційної інфраструктури та витоку критичних технологій. Безпекоорієнтований менеджмент інновацій у цьому контексті набуває стратегічного значення як інструмент збалансування інноваційної динаміки та захисту критичних розробок, забезпечуючи не лише корпоративну стійкість, а й технологічну безпеку держави.

Інноваційний менеджмент – це система управління, у межах якої взаємодіють різні фактори, спрямовані на забезпечення необхідного рівня життєздатності та конкурентоспроможності підприємства шляхом управління інноваційними процесами [1]. Об’єктом інноваційного менеджменту можуть виступати інноваційний процес, окремо взята інновація або інноваційна діяльність у цілому.

Воєнний контекст трансформує класичну модель інноваційного менеджменту, вимагаючи інтеграції безпекової домінанти у всі управлінські процеси. Безпекоорієнтований менеджмент інновацій – це система управління, яка поєднує традиційні завдання забезпечення конкурентоспроможності із систематичним управлінням безпековими загрозами на кожному етапі життєвого циклу інновації. Основною особливістю є розширення об’єктів впливу та управління. Окрім власне

інноваційного процесу, до них належать захист інтелектуальної власності, кібербезпека R&D-систем, фізична безпека інноваційної інфраструктури, контроль доступу до критичних технологій та забезпечення безперервності інноваційної діяльності в умовах воєнних загроз.

Під час повномасштабної війни з Росією інноваційно-інвестиційна діяльність підприємств характеризується зниженням обсягів інвестицій, зростанням витрат на забезпечення безпеки, зменшення доступу до фінансування, зменшення інноваційної діяльності та зміни в регіональній економіці [2].

Одним з основних прийомів управління ризиками та фінансово-економічною безпекою є диверсифікація. В контексті безпекоорієнтованого менеджменту інновацій можуть бути застосованими такі заходи: географічне розподілення дослідницьких центрів, створення резервних лабораторій, дублювання критичних даних у безпечних локаціях.

Важливою рисою інноваційної діяльності в умовах конкурентного середовища, а надто в умовах воєнних ризиків є здатність адаптуватися. Бізнесу слід переходити від лінійних моделей інновацій до адаптивних, із вбудованими сценаріями екстреного реагування на енергетичні атаки, кібератаки та фізичні загрози. Критичною стає здатність до швидкої реконфігурації R&D-діяльності в умовах руйнування фізичної інфраструктури, міграції ключових фахівців та обмеженості ресурсів. Організації впроваджують гібридні та повністю віддалені моделі інноваційної роботи, що супроводжується необхідністю посилення контролю доступу до критичних розробок та використання шифрованих каналів комунікації.

Окремо слід згадати кібербезпеку як важливий чинник забезпечення загальної системи безпекоорієнтованого менеджменту. Ефективний захист інноваційних проєктів передбачає багаторівневу систему заходів: сегментацію мереж з ізоляцією критичних R&D-систем, впровадження моделі Zero Trust Architecture, обов'язкове шифрування даних у спокої та при передачі, регулярний аудит безпеки програмного коду (SAST/DAST), контроль цілісності розробок через систему версіонування з криптографічним підписом [3]. Особливої уваги потребує управління доступом на основі застосування принципу найменших привілеїв, багатофакторна автентифікація, відеофіксація роботи з критичними системами.

Водночас необхідним є формування культури кібергігієни серед інноваційних команд, яка реалізується на основі регулярних тренінгів з розпізнавання соціальної інженерії, симуляції кіберінцидентів, чіткі протоколи реагування на підозрілу активність. Інтеграція Security Champions у кожну R&D-команду забезпечує проактивний підхід до виявлення вразливостей на ранніх стадіях розробки.

Ефективна модель безпекоорієнтованого менеджменту інновацій базується на трьох взаємопов'язаних принципах: застосування диверсифікації, адаптивне управління, приділення уваги кібербезпеці. Диверсифікація передбачає розподіл інноваційних ресурсів для мінімізації локальних загроз. Адаптивне управління ґрунтується на гнучкості та швидкому реагуванні. Кіберстійкість формується через інтеграцію безпекових механізмів на всіх етапах життєвого циклу інновацій.

Повномасштабна війна створила принципово нові умови для інноваційної діяльності підприємств, де забезпечення безпеки стало не додатковою функцією, а критичним фактором успішності інноваційних проектів. Безпекоорієнтований менеджмент інновацій являє собою інтегровану систему управління, що поєднує традиційні завдання забезпечення конкурентоспроможності із систематичним управлінням широким спектром воєнних загроз – від кібератак на R&D-системи до фізичного знищення інноваційної інфраструктури. Запропонована модель, заснована на принципах диверсифікації, адаптивності та кіберстійкості, дозволяє організаціям підтримувати інноваційну динаміку в екстремальних умовах, одночасно захищаючи критичні розробки та інтелектуальну власність. Перспективним напрямком досліджень є вимірювання ефективності безпекоорієнтованого підходу та розробка галузевих моделей управління інноваціями в умовах війни.

## Список використаних джерел


1. Вікарчук О. І. Інноваційний менеджмент в Україні як складова загальної системи управління підприємством. *Вісник Житомирського державного технологічного університету. Економічні науки*. 2010. Вип. 1 (51). С. 156-159.
2. Михайлик О., Бірак Є. Інвестиційно-інноваційна діяльність підприємств в умовах воєнного стану. *Економіка та суспільство*. 2023. № 58. URL: https://doi.org/10.32782/2524-0072/2023-58-86.
3. Popova D., Yaremenko S. Cyber Security in the Age of Industry 5.0: New Challenges and Opportunities. *Economic Herald of the Donbas*. 2024. No. 3(77). pp. 203-216. URL: https://doi.org/10.12958/1817-3772-2024-3(77)203-216.