

**БЕЗПЕКООРІЄНТОВАНИЙ МЕНЕДЖМЕНТ ЯК ФАКТОР
СТІЙКОСТІ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ
ТРАНСФОРМАЦІЇ**

Балабуха І.О.

e-mail: ihor.balabukha@nure.ua

Науковий керівник – д.е.н., проф. Перепелюкова О.В.

Харківський національний університет радіоелектроніки, кафедра ЕК
м. Харків, Україна

The paper considers the role of security oriented management in ensuring enterprise resilience under conditions of digital transformation. The growing use of information technologies, business process automation and digital platforms creates both new opportunities and new threats for organizations. Particular attention is paid to the integration of risk management into strategic and operational management. The study emphasizes the importance of identifying internal and external threats, assessing their impact and implementing preventive measures. It is determined that digital technologies improve monitoring, analytics and decision making in the field of enterprise security. The implementation of security oriented management principles helps increase economic stability, reduce the negative impact of uncertainty and ensure sustainable development. The proposed approach can be used as a basis for improving management systems in modern organizations.

У сучасних умовах розвитку цифрової економіки підприємства функціонують у середовищі високої динамічності, невизначеності та зростання ризиків. Використання інформаційних технологій, автоматизація процесів, цифрові платформи, хмарні сервіси й аналітичні інструменти створюють нові можливості для підвищення продуктивності, оптимізації витрат і розширення ринків збуту. Разом із цим цифрова трансформація супроводжується новими викликами, зокрема кіберзагрозами, втратою даних, порушенням безперервності бізнес-процесів, інформаційною вразливістю та посиленням конкуренції. За таких умов особливого значення набуває безпекоорієнтований менеджмент як системний підхід до управління підприємством.

Сутність безпекоорієнтованого менеджменту полягає в інтеграції питань безпеки в усі основні управлінські функції. Його призначення полягає не лише в реагуванні на наявні проблеми, а й у формуванні такої системи управління, яка дозволяє завчасно виявляти загрози, оцінювати їх наслідки та розробляти превентивні рішення. У такому підході безпека виступає не окремим напрямом діяльності, а необхідною умовою стабільного функціонування, адаптації та розвитку підприємства [1, 2].

Актуальність цього підходу зумовлена впливом зовнішніх і внутрішніх факторів ризику. До зовнішніх належать макроекономічна нестабільність,

зміни ринкової кон'юнктури, трансформація нормативно-правового середовища, кібератаки, порушення логістичних ланцюгів і репутаційні ризики. Внутрішні ризики пов'язані з помилками в ухваленні управлінських рішень, недосконалістю організаційної структури, недостатнім рівнем інформаційного захисту, низькою кваліфікацією персоналу та слабкістю корпоративної культури. Сукупний вплив цих чинників знижує стійкість підприємства, ускладнює його адаптацію до змін і підвищує ймовірність кризових ситуацій.

Основним завданням безпекоорієнтованого менеджменту є забезпечення здатності підприємства протидіяти загрозам без втрати керованості, ресурсного потенціалу та стратегічних перспектив розвитку. Це передбачає формування цілісної системи, що поєднує стратегічне планування, управління ризиками, інформаційну безпеку, внутрішній контроль, аналітичне забезпечення та організаційну адаптивність. Саме комплексність робить цей підхід результативним, оскільки окремі заходи не здатні забезпечити належного рівня стійкості в умовах багатофакторних загроз.

Однією з основних складових безпекоорієнтованого менеджменту є управління ризиками, адже воно дає змогу своєчасно виявляти потенційні загрози, оцінювати їх вплив і обирати способи реагування. Такий підхід має не лише захисне, а й адаптаційне значення, оскільки дозволяє не тільки знижувати можливі втрати, а й виявляти нові можливості для вдосконалення діяльності підприємства. У сучасних умовах ефективно управління ризиками неможливе без цифрових технологій, які забезпечують оперативне отримання інформації, моніторинг відхилень і визначення критичних точок у бізнес-процесах. Завдяки цьому підвищується якість управлінських рішень і розширюються можливості прогнозування.

Особливе місце в системі безпекоорієнтованого менеджменту посідає інформаційна безпека, оскільки для сучасного підприємства інформація є стратегічним ресурсом. Її втрата, спотворення або несанкціоноване використання можуть спричинити фінансові, правові та репутаційні втрати. Тому система управління має передбачати захист інформаційних активів, контроль доступу, резервне копіювання даних і безпечне використання цифрових каналів комунікації. Разом із тим безпекоорієнтований менеджмент не обмежується лише технічними аспектами, адже важливу роль у ньому відіграє кадрова складова. Саме рівень компетентності персоналу, дотримання внутрішніх процедур і сформованість культури безпеки значною мірою визначають ефективність усієї системи [3, 4, 5].

Не менш важливою є інтеграція принципів безпекоорієнтованого менеджменту до стратегічного управління підприємством. Якщо загрози не враховуються на етапі стратегічного планування, підприємство втрачає можливість своєчасної адаптації та стикається з кризовими наслідками під час реалізації своїх цілей. Саме тому безпекоорієнтований підхід має бути

спрямований на узгодження стратегічних рішень з оцінкою ризиків, ресурсних обмежень і потенційних загроз.

Перевагою впровадження безпекоорієнтованого менеджменту є підвищення загальної стійкості підприємства, тобто його здатності підтримувати основні функції, досягати запланованих результатів і відновлюватися після негативних впливів. Така стійкість формується завдяки своєчасному виявленню критичних факторів, наявності альтернативних сценаріїв реагування, резервуванню ресурсів, налагодженій комунікації та координації між структурними підрозділами.

Отже, безпекоорієнтований менеджмент є важливим інструментом забезпечення стійкості підприємства в умовах цифрової трансформації. Його впровадження дає змогу інтегрувати управління ризиками, інформаційний захист, контроль ресурсів і стратегічне планування в єдину систему управління. Це сприяє підвищенню рівня економічної безпеки, зниженню вразливості до загроз і формуванню передумов для довгострокового розвитку підприємства.

Список використаних джерел

1. Brigham E., Ehrhardt M. Financial Management: Theory & Practice 16th Editio. Cengage Learning, 2020. 1186 p.
2. Max M. Weber¹, Burkhard Pedell, Peter G. Rötzel. Resilience-oriented management control systems: a systematic review of the relationships between organizational resilience and management control systems. *Journal of Management Control*. 2024. <https://doi.org/10.1007/s00187-024-00385-2>
3. Pilanawithana N. M., Liyanage S. Developing resilience for safety management systems in building repair and maintenance: A conceptual model. *Journal of Safety Research*. 2022. <https://doi.org/10.1016/j.ssci.2022.105768>
4. Adra I., Abu Sheikha A., Larivière R. What is safety leadership? A systematic review of definitions. *Journal of Safety Research*. 2024. <https://doi.org/10.1016/j.jsr.2024.04.001>
5. Andrew Sutton, John McAlaney. Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*. 2025. <https://doi.org/10.1016/j.cose.2024.104110>