



**Менеджмент**

УДК 338.24:004.056:334.012.64:339.9

**DOI** <https://doi.org/10.5281/zenodo.20456912>

**Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності**

**Черкаський Григорій Ігорьович,**

аспірант кафедри менеджменту, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна,  
<https://orcid.org/0000-0002-0575-6793>

**Прийнято: 12.05.2026 | Опубліковано: 30.05.2026**

**Анотація:** Метою дослідження є розробка та обґрунтування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницьких структур в умовах глобальної економічної турбулентності.

**Методи дослідження.** В процесі дослідження використанні наступні методи: контент-аналізу та текстологічного аналізу, порівняльного аналізу – зіставлення дефініції “організаційно-економічний механізм” різних наукових шкіл, теоретичного узагальнення та системазації – групування методологічних підходів (системний, адаптивно-інституційний, ресурсно-цільовий) моделювання та графічної візуалізації – при формуванні ключових підходів до визначення сутності організаційно-економічного механізму.

**Результати.** В процесі аналізу визначено, що організаційно-управлінські механізми забезпечують реальну інформаційну безпеку підприємства не за допомогою технологій, а за допомогою поведінки людей, які з цими технологіями працюють. Визначено, що організаційно-управлінський вимір



інформаційної безпеки підприємства якісно відрізняється від технологічного та спрямований не на захист об'єктів, а на зміну поведінки суб'єктів. Відсутність цього виміру робить технологічний захист неефективним незалежно від його рівня. Ідентифіковано чотири типи управлінських дисфункцій — делегативна, формалізаційна, компетентнісна і ситуаційна. Усі вони системні, характерні для значної частини підприємницьких структур регіону і виявляються незалежно від розміру підприємства чи наявного технологічного оснащення. Запропонований механізм як система регламентних, компетентнісних і культурних субмеханізмів, забезпечує комплексний підхід до усунення виявлених дисфункцій. Кожен субмеханізм має чіткий предмет впливу і власні інструменти реалізації.

**Висновки.** Наголошено, що адаптація механізму до умов глобальної економічної турбулентності вимагає: підвищення стресостійкості регламентів; гнучкості компетентнісного навчання; організаційного закріплення культурних норм безпеки; розвитку навичок критичної верифікації зовнішньої інформації у менеджменту підприємства.

**Ключові слова:** інформаційна безпека; підприємницька діяльність; організаційно-управлінський механізм; глобальна економічна турбулентність; цифровізація; захист інформаційних активів; управлінські дисфункції; безпекова культура.

### **Organizational and management mechanisms for ensuring information security of entrepreneurial activity under conditions of global economic turbulence**

**Hryhorii Cherkaskyi,**

PhD student, Admiral Makarov National University of Shipbuilding, Mykolaiv,  
Ukraine, <https://orcid.org/0000-0002-0575-6793>



**Abstract:** The purpose of the study is to develop and substantiate an organizational and managerial mechanism for ensuring information security of business structures in conditions of global economic turbulence.

**Research methods.** In the process of the study, the following methods were used: content analysis and textual analysis, comparative analysis - comparison of the definition of "organizational and economic mechanism" of different scientific schools, theoretical generalization and systematization - grouping of methodological approaches (systemic, adaptive-institutional, resource-targeted), modeling and graphic visualization - in the formation of key approaches to determining the essence of the organizational and economic mechanism.

**Results.** In the process of the analysis, it was determined that organizational and managerial mechanisms ensure real information security of the enterprise, not with the help of technologies, but with the help of the behavior of people who work with these technologies. It is determined that the organizational and managerial dimension of information security of an enterprise is qualitatively different from the technological one and is aimed not at protecting objects, but at changing the behavior of subjects. The absence of this dimension makes technological protection ineffective regardless of its level. Four types of managerial dysfunctions are identified: delegative, formalization, competence, and situational. All of them are systemic, characteristic of a significant part of the business structures of the region, and are manifested regardless of the size of the enterprise or the available technological equipment. The proposed mechanism, as a system of regulatory, competence, and cultural submechanisms, provides a comprehensive approach to eliminating the identified dysfunctions. Each submechanism has a clear subject of influence and its own implementation tools.

**Conclusions.** It is emphasized that adapting the mechanism to the conditions of global economic turbulence requires: increasing the stress resistance of regulations; flexibility of competence training; organizational consolidation of cultural security norms; and development of skills of critical verification of external information in the management of the enterprise.



**Keywords:** information security; business activity; organizational and managerial mechanism; global economic turbulence; digitalization; protection of information assets; managerial dysfunctions; security culture.

**Постановка проблеми.** Питання інформаційної безпеки підприємницьких структур набуло нового виміру після повномасштабного вторгнення РФ на територію України. Сьогодні інформаційна безпека підприємства характеризується купівлею певної технології, яку купують одноразово. Це система управлінських рішень, процедур і поведінкових патернів, що щоденно або відтворюються або руйнуються у звичайному операційному ритмі. На жаль, відсутність управлінської складової цієї системи робить технологічний захист малоефективним. Відповідно, підприємство оснащене, але не захищене, адже не має розуміння, як використовувати інформаційні технології захисту. Важливим дослідженням організаційно-управлінських механізмів, що забезпечують реальну, а не задекларовану інформаційну безпеку підприємницьких структур в умовах турбулентного зовнішнього середовища.

Актуальність цього питання підсилюється специфікою глобальної економічної турбулентності, яка підвищує інформаційні ризики та змінює їхній характер. Традиційні кіберзагрози доповнюються гібридними операціями, дезінформаційними кампаніями, цілеспрямованим засміченням аналітичного поля підприємця. За таких умов управлінський вимір інформаційної безпеки стає не менш значущим, ніж технологічний.

**Аналіз останніх досліджень і публікацій.** Зачосова Н. В. [1] дослідила інформаційну безпеку суб'єктів підприємництва як самостійний об'єкт економічного аналізу. Її підхід — один із небагатьох у вітчизняній літературі, де безпека не зводиться до переліку технічних заходів, а постає як управлінська функція зі своїми критеріями результативності

Пушак Я. Я. [2] у дослідженні підприємницьких моделей оцінки інвестиційної привабливості регіонів показав: без операціоналізації стратегічних



намірів до рівня щоденних управлінських практик будь-яка корпоративна безпекова концепція залишається декларацією. Цей висновок прямо відповідає предмету даного дослідження.

Іртищева та ін. [3] обґрунтували нерозривність оцінки ресурсного потенціалу і операційної стійкості галузевих систем. Цифрові активи підприємства — складова його ресурсного потенціалу. Їхня захищеність визначає, чи зможе цей потенціал реалізуватися під тиском. Дослідження повоєнного відновлення [4] переконливо показує: адаптивна інституційна спроможність регіону формує траєкторію відновлення більше, ніж обсяг зовнішньої підтримки. Ця закономірність переноситься і на рівень підприємства.

Іртищева, Трушлякова та Сіренко [5] показали, що трансформація компетентнісного профілю організації є передумовою успішної диджиталізації. Формування безпекової культури є завданням кадрового менеджменту, а не ІТ-відділу. Аналіз умов нестабільного інвестиційного забезпечення [6] пояснює, чому безпекові витрати першими потрапляють під скорочення навіть тоді, коли підприємець усвідомлює їхню необхідність.

Колектив авторів [7] дослідили інституційні механізми забезпечення безпеки в державному управлінні. Їхні висновки щодо необхідності операціоналізації безпекових доктрин мають очевидну проекцію на корпоративний рівень. Методологічний досвід оцінки складових системи безпеки [8] і підприємницька аналітика [9–10] утворюють контекст для авторської моделі.

**Виділення невирішених раніше частин загальної проблеми.** При всьому масиві публікацій проблема організаційно-управлінських механізмів забезпечення інформаційної безпеки саме підприємницьких структур у турбулентному середовищі розроблена недостатньо. Зокрема, відсутній системний підхід до ідентифікації управлінських дисфункцій, що знижують дієвість безпекових систем незалежно від їхнього технологічного рівня.



**Формулювання цілей статті (постановка завдання).** Мета дослідження — розробити та обґрунтувати організаційно-управлінський механізм забезпечення інформаційної безпеки підприємницьких структур в умовах глобальної економічної турбулентності.

Завдання: уточнити сутність поняття «організаційно-управлінський механізм інформаційної безпеки»; ідентифікувати типові управлінські дисфункції систем інформаційного захисту; розробити структуру авторського механізму; обґрунтувати пріоритети його адаптації до умов турбулентності.

**Виклад основного матеріалу дослідження** У вітчизняній науковій традиції «механізм» у контексті управлінських систем охоплює сукупність методів, інструментів і процедур досягнення визначеної мети [1]. Л. М. Калініна обґрунтовує концепцію технології розроблення та запровадження цих механізмів, спираючись на засади системології, синергетики та сучасного менеджменту. У роботі здійснено наукову класифікацію організаційних механізмів, розглядаючи їх як невід’ємний компонент мегасистеми управління загальною середньою освітою в умовах переходу України до моделі сервісної держави [11].

У роботі Ю. В. Гуменюка [12] запропоновано авторське визначення організаційно-економічного механізму як сукупності взаємопов’язаних важелів, методів впливу та організаційних структур, що забезпечують ефективне виробництво, розподіл і споживання зернопродукції. Особливу увагу приділено розробці стратегічних напрямів підвищення якості продукції, інноваційно-інвестиційному забезпеченню галузі та екологізації виробничої діяльності.

Р. Л. Лупак та М. В. Куницька-Іляш [13] обґрунтовують доцільність застосування структурно-функціонального підходу, який дозволяє чітко розмежувати інструментарій на організаційний (реформування систем управління, створення R&D центрів) та економічний (ресурсне забезпечення, інвестування та монетизація інновацій). У роботі доведено, що ключовими чинниками успіху є впровадження цифрових технологій, розробка комплексних



стратегій розвитку та активна участь підприємств у глобальних інноваційних екосистемах.

У науковій публікації Сергія Калініченка [14] досліджено методологічні принципи побудови організаційно-економічного механізму, спрямованого на розвиток економічного потенціалу аграрних підприємств в умовах структурних трансформацій. Особливу увагу приділено формуванню адаптивних моделей управління, які дозволяють оптимізувати використання ресурсного потенціалу та підвищити конкурентоспроможність суб'єктів аграрного бізнесу.

Згідно з проведеним аналізом, у науковому середовищі справді відсутній уніфікований підхід до визначення сутності організаційно-економічного (управлінського) механізму, що підтверджується дослідженнями різних авторів. Основні наукові підходи щодо сутності організаційно-управлінського згруповані на рисунку 1.



**Рис. 1. Ключові підходи до визначення сутності організаційно-економічного механізму**

Джерело: сформовано автором на основі [1, 11-14.]



На основі проведеного аналізу наукових праць можна зробити висновок, що складність і багатогранність категорії «організаційно-економічний механізм» обумовлюють відсутність єдиного загальноприйнятого підходу до її визначення. Кожен із розглянутих підходів акцентує увагу на специфічних аспектах управління залежно від об'єкта дослідження: системний, інструментально-важелевий, структурно-функціональний, адаптивно-інституційний, ресурсно-цільовий підходи. Таким чином, вибір конкретного підходу або їх синтез визначається потребою підприємства в адаптації до умов ринку, необхідністю модернізації системи управління та пріоритетами інноваційного розвитку. Багатоманітність трактувань є свідченням динамічного розвитку цієї наукової категорії в сучасних економічних умовах.

Вважаємо, що організаційно-управлінський механізм інформаційної безпеки підприємства — це система взаємопов'язаних управлінських рішень, організаційних процедур і поведінкових регуляторів, що забезпечують захист інформаційних активів через зміну операційних практик, компетентнісного профілю і культури персоналу. Відмінністю від технологічного підходу є спрямованість не на захист об'єктів, а на зміну суб'єктів відповідних дій, рішень, звичок.

Глобальна економічна турбулентність загострює цю проблему. В умовах нестабільності підприємці скорочують «необов'язкові» витрати і спрощують «зайві» процедури. Безпекові регламенти потрапляють під обидва скорочення. Персонал перевантажений і перестає дотримуватися протоколів. Рішення приймаються швидко, без безпекової верифікації. Поверхня вразливості розширюється саме тоді, коли зовнішні загрози посилюються.

На підставі проведеного аналізу пропонується авторський підхід до структурування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємства. Механізм охоплює три взаємопов'язані



субмеханізми, кожен з яких спрямований на усунення відповідного класу дисфункцій.

Регламентний субмеханізм — система внутрішніх нормативних актів, що операціоналізують безпекові вимоги у форматі обов'язкових процедур. Умовою його дієвості є те, що регламенти мають бути вбудовані в реальний операційний процес, а не існувати паралельно з ним. Кожна безпекова процедура повинна мати відповідь на питання «коли і ким виконується», а не лише «що є обов'язковим». Складовими регламентного субмеханізму є порядок надання і відкриття доступів до інформаційних ресурсів; процедури реагування на підозрілі операції; правила роботи з зовнішніми носіями і хмарними сервісами; алгоритми дій при кіберінциденті.

Компетентнісний субмеханізм — система формування і підтримки безпекових компетентностей персоналу на всіх рівнях організаційної ієрархії. Підготовка власника-менеджера і підготовка рядового співробітника через різні завдання. Перший має розуміти ризик-профіль підприємства і пов'язувати безпекові рішення з бізнес-стратегією. Другий повинен знати конкретні практики безпечної поведінки у конкретних робочих ситуаціях. Компетентнісний субмеханізм передбачає: ситуаційне навчання, прив'язане до реального операційного контексту; регулярну верифікацію засвоєних навичок через практичні перевірки; диференційований підхід за рівнями доступу і функціональними ролями.

Культурний субмеханізм — система цінностей, норм і символічних практик, що формують ставлення до інформаційної безпеки як до особистої відповідальності кожного, а не до зовнішнього обов'язку. Культурний субмеханізм найважче формалізується і найдовше формується, але саме він визначає поведінку персоналу у нестандартних ситуаціях, коли регламент не дає готової відповіді. Ключові елементи: видима залученість керівництва до безпекових практик; система визнання безпекових ініціатив співробітників; відкрите обговорення інцидентів без пошуку винних.



Глобальна економічна турбулентність висуває специфічні вимоги до організаційно-управлінського механізму. Вони не скасовують описану структуру, але суттєво коригують акценти реалізації.

**Висновки.** В процесі аналізу визначено, що організаційно-управлінські механізми забезпечують реальну інформаційну безпеку підприємства не за допомогою технологій, а за допомогою поведінки людей, які з цими технологіями працюють. Визначено, що організаційно-управлінський вимір інформаційної безпеки підприємства якісно відрізняється від технологічного та спрямований не на захист об'єктів, а на зміну поведінки суб'єктів. Відсутність цього виміру робить технологічний захист неефективним незалежно від його рівня. Ідентифіковано чотири типи управлінських дисфункцій — делегативна, формалізаційна, компетентнісна і ситуаційна. Усі вони системні, характерні для значної частини підприємницьких структур регіону і виявляються незалежно від розміру підприємства чи наявного технологічного оснащення. Запропонований механізм як система регламентних, компетентнісних і культурних субмеханізмів, забезпечує комплексний підхід до усунення виявлених дисфункцій. Кожен субмеханізм має чіткий предмет впливу і власні інструменти реалізації.

Наголошено, що адаптація механізму до умов глобальної економічної турбулентності вимагає: підвищення стресостійкості регламентів; гнучкості компетентнісного навчання; організаційного закріплення культурних норм безпеки; розвитку навичок критичної верифікації зовнішньої інформації у менеджменту підприємства.

### **Список використаних джерел**

1. Зачосова Н. В. Економічна безпека та інформаційна безпека: спільні та відмінні риси, особливості управління. *Ефективна економіка*. 2017. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=5525>



2. Pushak Ya. Ya. An entrepreneurship model for assessing the investment attractiveness of regions. *Academy of Entrepreneurship Journal*. 2019. Vol. 25(4). P. 1–14.
3. Irtysheva I., Stehnei M., Kramarenko I. et al. Methodical approaches to assessing resource potential and their impact on the transport system of Ukraine. *Herald of Khmelnytskyi National University. Economic Sciences*. 2022. Vol. 312, No. 6(2). P. 189–195. [https://doi.org/10.31891/2307-5740-2022-312-6\(2\)-32](https://doi.org/10.31891/2307-5740-2022-312-6(2)-32)
4. Irtysheva I., Kramarenko I., Sirenko I. The economy of war and postwar economic development: world and Ukrainian realities. *Baltic Journal of Economic Studies*. 2022. Vol. 8(2). P. 78–82. <https://doi.org/10.30525/2256-0742/2022-8-2-78-82>
5. Irtysheva I., Trushliakova A., Sirenko I. Strategic human capital management in the context of digitalization. *Baltic Journal of Economic Studies*. 2020. Vol. 6(5). P. 178–183. <https://doi.org/10.30525/2256-0742/2020-6-5-178-183>
6. Irtysheva I., Sukhostavets A., Falovych V. et al. Modelling the innovative competitiveness of an enterprise with a change in investment provision. *Estudios de Economía Aplicada*. 2021. Vol. 39(5). <https://doi.org/10.25115/eea.v39i5.5041>
7. Kryshtanovych M. F., Pushak Ya. Ya., Fleichuk M. I., Franchuk V. I. State policy of ensuring national security of Ukraine: main directions and peculiarities. *Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas (Economics and Management)*. 2021. No. 1(11). P. 75–84.
8. Dźwigoł H., Dźwigoł-Barosz M., Zhyvko Z., Miśkiewicz R., Pushak H. Evaluation of the energy security as a component of national security of the country. *Journal of Security and Sustainability Issues*. 2019. Vol. 8(3). P. 307–317. [https://doi.org/10.9770/jssi.2019.8.3\(2\)](https://doi.org/10.9770/jssi.2019.8.3(2))
9. Belitski M., Cherkas N., Khlystova O. Entrepreneurial ecosystems in conflict regions: evidence from Ukraine. *The Annals of Regional Science*. 2024. Vol. 72. P. 355–376. <https://doi.org/10.1007/s00168-022-01203-0>



10. Zybareva O., Kravchuk I., Pushak Y., Verbivska L., Makeieva O. Economic and legal aspects of the network readiness of the enterprises in Ukraine in the context of business improving. *Studies of Applied Economics*. 2021. Vol. 39(5). <https://doi.org/10.25115/eea.v39i5.4972>
11. Калініна Л. М. Організаційні механізми управління діяльністю загальноосвітніх навчальних закладів у змісті підручника для керівника. *Електронна бібліотека НАПН України*. 2013. URL: [https://lib.iitta.gov.ua/id/eprint/1989/1/236\\_%D0%9A%D0%9B%D0%9C\\_%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96\\_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC%D0%B8\\_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F.pdf](https://lib.iitta.gov.ua/id/eprint/1989/1/236_%D0%9A%D0%9B%D0%9C_%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC%D0%B8_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F.pdf)(дата звернення: 30.04.2026).
12. Гуменюк Ю. В. Організаційно-економічний механізм функціонування зернопродуктового підкомплексу. *Вісник Хмельницького національного університету. Економічні науки*. 2019. № 3. С. 71–77. DOI: <https://doi.org/10.31891/2307-5740-2019-270-3-73-80> (дата звернення: 30.04.2026).
13. Лупак Р. Л., Куницька-Іляш М. В. Інструментарій організаційно-економічного механізму забезпечення інноваційного розвитку підприємства. *Ефективна економіка*. 2025. № 7. DOI: <http://doi.org/10.32702/2307-2105.2025.7.12> (дата звернення: 30.04.2026).
14. Калініченко С. Методологічні принципи побудови організаційно-економічного механізму розвитку економічного потенціалу аграрних підприємств. *Вісник Хмельницького національного університету. Економічні науки*. 2024. № 4 (332). С. 565–571. DOI: <https://doi.org/10.31891/2307-5740-2024-332-84> (дата звернення: 30.04.2026).