

УДК 658.012:004:330.341

JEL Classification: K22, L51, D23, F15

ФОРМУВАННЯ ПРИНЦИПІВ КОРПОРАТИВНОГО КОМПЛАЄНСУ В УПРАВЛІННІ ПІДПРИЄМСТВАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

ЧОБИТОК Вікторія¹, НЕСТЕРЕНКО Роман², ГОХ Ірина³

¹ ННІ «Українська інженерно-педагогічна академія»
Харківського національного університету імені В.Н. Каразіна, м. Харків
<https://orcid.org/0000-0002-5272-388X>

² ННІ «Професійної освіти» Національної академії
Національної гвардії України, м. Харків
<https://orcid.org/0000-0001-6357-3613>

³ ННІ «Професійної освіти» Національної академії
Національної гвардії України, м. Харків
<https://orcid.org/0000-0001-8465-9774>

Актуальність дослідження зумовлена зростанням ролі підприємств критичної інфраструктури у забезпеченні стійкості соціально-економічних систем в умовах посилення безпекових викликів, цифрової трансформації та активізації євроінтеграційних процесів. Це підвищує вимоги до ефективності систем управління, зокрема щодо забезпечення відповідності нормативним вимогам, управління ризиками та підтримання безперервності діяльності. Імплементація європейських регуляторних норм у сфері стійкості критичних суб'єктів і кібербезпеки зумовлює необхідність формування сучасних комплаєнс-систем, інтегрованих у загальну систему управління підприємствами.

Аналіз наукових праць засвідчує, що проблематика корпоративного комплаєнсу, управління ризиками та внутрішнього контролю активно досліджується як зарубіжними, так і вітчизняними вченими. Водночас комплаєнс переважно розглядається як інструмент забезпечення прозорості та мінімізації ризиків, тоді як питання його системної інтеграції в управління підприємствами критичної інфраструктури залишаються недостатньо розробленими. Особливої уваги потребує формування цілісної системи принципів корпоративного комплаєнсу з урахуванням сучасних регуляторних та безпекових вимог.

Метою дослідження є обґрунтування принципів корпоративного комплаєнсу в управлінні підприємствами критичної інфраструктури в умовах європейської інтеграції та розроблення інтегрованої моделі комплаєнс-системи. У роботі узагальнено наукові підходи до трактування комплаєнсу, що дозволило виокремити його нормативний, управлінський та інституційний виміри. На цій основі запропоновано систему принципів корпоративного комплаєнсу та розроблено інтегровану модель його реалізації.

Запропонована модель поєднує зовнішні регуляторні вимоги, стратегічні орієнтири, ключові напрями реалізації, інструментарій та інформаційно-аналітичне забезпечення, а також передбачає поетапний механізм впровадження із зворотним зв'язком. Це забезпечує узгодженість управлінських процесів із європейськими стандартами, підвищує ефективність функціонування підприємств і сприяє їх адаптації до змінного регуляторного середовища. Доведено, що інтеграція комплаєнсу в систему корпоративного управління є важливою умовою підвищення стійкості підприємств критичної інфраструктури та мінімізації ризиків їх діяльності.

Ключові слова: корпоративний комплаєнс, підприємства критичної інфраструктури, комплаєнс-система, управління ризиками, європейська інтеграція, регуляторне середовище, безперервність діяльності, корпоративне управління

<https://doi.org/10.31891/mdes/2026-20-38>



This is an Open Access article distributed under the terms of the [Creative Commons CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)

Стаття надійшла до редакції / Received 05.03.2026

Прийнята до друку / Accepted 10.04.2026

Опубліковано / Published 30.04.2026

© Чобіток Вікторія, Нестеренко Роман, Гох Ірина

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Актуальність дослідження зумовлена зростанням ролі підприємств критичної інфраструктури в забезпеченні стійкості соціально-економічних систем в умовах посилення безпекових викликів, цифрової трансформації та активізації євроінтеграційних процесів. Це зумовлює зростання вимог до ефективності систем управління, зокрема у частині забезпечення відповідності, управління ризиками та підтримання безперервності діяльності.

Імплементація європейських регуляторних норм і стандартів, зокрема у сфері стійкості критичних суб'єктів і кібербезпеки, актуалізує необхідність формування сучасних комплаєнс-систем, інтегрованих у загальну систему управління підприємством. Водночас недостатня розробленість принципів корпоративного комплаєнсу та їх практичної реалізації в умовах функціонування підприємств критичної інфраструктури обумовлює потребу у подальших наукових дослідженнях у цьому напрямі.

У цих умовах особливого значення набуває забезпечення ефективного функціонування комплаєнс-систем на підприємствах критичної інфраструктури як інструменту управління ризиками та забезпечення відповідності нормативним вимогам. Водночас на практиці спостерігається фрагментарність їх впровадження, що не забезпечує повноцінної інтеграції комплаєнсу у систему

управління підприємством та обмежує ефективність управління ризиками.

Крім того, відсутність чітко структурованої системи принципів корпоративного комплаєнсу з урахуванням специфіки підприємств критичної інфраструктури та вимог європейського регуляторного середовища ускладнює формування ефективних управлінських рішень.

Це зумовлює необхідність теоретичного обґрунтування принципів корпоративного комплаєнсу та розроблення інтегрованої моделі його реалізації.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання корпоративного комплаєнсу, управління ризиками та забезпечення відповідності діяльності підприємств нормативним вимогам широко досліджуються у працях вітчизняних і зарубіжних науковців. Зокрема, теоретичні та прикладні аспекти корпоративного управління, ролі нематеріальних ресурсів і репутаційних чинників розкрито у працях Charles J. Fombrun, David J. Teece, Violina P. Rindova та інших [1-3]. У зазначених дослідженнях комплаєнс розглядається переважно як інструмент забезпечення прозорості та зниження ризиків, проте питання його інтеграції у систему управління підприємствами критичної інфраструктури залишаються недостатньо розкритими.

Значний внесок у розвиток підходів до управління ризиками та внутрішнього контролю здійснено в межах концепції COSO ERM [4], а також у працях зарубіжних дослідників, які акцентують увагу на інтеграції комплаєнсу в систему корпоративного управління. У цьому контексті комплаєнс розглядається як складова стратегічного управління, спрямована на забезпечення ефективності управлінських рішень та мінімізацію ризиків.

У вітчизняній науковій літературі питання комплаєнсу, внутрішнього контролю та адаптації підприємств до змін регуляторного середовища досліджували В. М. Гець, С. В. Кириленко, Б. І. Косович, Стеблянко- М. С. Авраменко, М. А. Дорошенко та інші [5-8]. У їхніх працях розглядаються питання розвитку підприємництва, інноваційної діяльності, екологізації економіки та впровадження сучасних управлінських підходів.

Разом із тим аналіз наукових джерел свідчить, що проблематика корпоративного комплаєнсу здебільшого розглядається або в межах загального корпоративного управління, або з позицій окремих функціональних напрямів. Недостатньо уваги приділяється формуванню системи принципів корпоративного комплаєнсу з урахуванням специфіки підприємств критичної інфраструктури, а також розробленню комплексних моделей, які б інтегрували регуляторний, управлінський та інституційний аспекти в умовах європейської інтеграції.

ВИДІЛЕННЯ НЕДОСЛІДЖЕНИХ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Незважаючи на значну кількість наукових праць, присвячених питанням корпоративного управління, комплаєнсу та управління ризиками, низка аспектів залишається недостатньо розробленою. Зокрема, у науковій літературі відсутній єдиний підхід до формування принципів корпоративного комплаєнсу, який би враховував специфіку функціонування підприємств критичної інфраструктури в умовах посилення безпекових викликів та цифрової трансформації.

Недостатньо дослідженими залишаються питання інтеграції комплаєнс-систем у загальну систему управління підприємством із урахуванням вимог європейського регуляторного середовища, зокрема у контексті імплементації сучасних стандартів щодо стійкості, кібербезпеки та управління ризиками. Обмеженою є також розробленість комплексних моделей корпоративного комплаєнсу, які б поєднували принципи, інструменти та механізми їх практичної реалізації.

Крім того, потребують подальшого наукового обґрунтування підходи до забезпечення проактивного характеру комплаєнс-систем, їх адаптивності до змін зовнішнього середовища та орієнтації на підтримання безперервності функціонування підприємств критичної інфраструктури.

Таким чином, наявні теоретичні та прикладні напрацювання не забезпечують повною мірою формування цілісного підходу до корпоративного комплаєнсу в умовах європейської інтеграції, що зумовлює необхідність подальших досліджень у цьому напрямі.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є обґрунтування принципів корпоративного комплаєнсу в управлінні підприємствами критичної інфраструктури в умовах європейської інтеграції та розроблення інтегрованої моделі комплаєнс-системи з урахуванням сучасних регуляторних вимог і безпекових викликів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сучасний етап розвитку підприємств критичної інфраструктури характеризується суттєвим ускладненням умов їх функціонування, що зумовлено синергетичним впливом низки системних факторів, серед яких ключову роль відіграють безпекові виклики, процеси цифрової трансформації економіки та активізація євроінтеграційних перетворень. Зазначені фактори не лише змінюють зовнішнє середовище діяльності підприємств, але й трансформують внутрішню логіку управління, підвищуючи вимоги до гнучкості, адаптивності та ефективності управлінських рішень.

Поглиблення безпекових ризиків, пов'язаних як із військово-політичними, так і з кібернетичними загрозами, обумовлює необхідність формування стійких механізмів захисту критичних об'єктів та забезпечення їх безперервного функціонування. Водночас цифровізація управлінських і виробничих процесів створює додаткові можливості для підвищення ефективності діяльності, проте одночасно супроводжується виникненням нових ризиків, пов'язаних з обробкою даних, кібербезпекою та залежністю від інформаційно-комунікаційних систем.

Не менш вагомим чинником виступає європейська інтеграція, яка передбачає імплементацію норм і стандартів Європейського Союзу у національне регуляторне поле. Це, у свою чергу, зумовлює необхідність приведення діяльності підприємств критичної інфраструктури у відповідність до вимог щодо прозорості, підзвітності, управління ризиками та забезпечення стійкості. Внаслідок цього значно посилюється роль внутрішніх механізмів контролю та саморегулювання.

В сучасних умовах забезпечення стійкості функціонування підприємств, їх здатності до відновлення після кризових ситуацій, а також відповідності регуляторним вимогам набуває стратегічного характеру та виходить за межі традиційних підходів до управління. Це потребує формування комплексних управлінських систем, орієнтованих не лише на досягнення економічних результатів, але й на мінімізацію ризиків, дотримання нормативних вимог і забезпечення довіри з боку стейкхолдерів [13].

Корпоративний комплаєнс зазнає суттєвої трансформації: від інструменту формального контролю за дотриманням правил він еволюціонує у системоутворюючий елемент управління підприємством. Його функціональне призначення розширюється від забезпечення нормативної відповідності до інтегрованого управління ризиками, формування комплаєнс-культури та підтримання стратегічної стійкості підприємства.

Корпоративний комплаєнс стає невід'ємною складовою сучасної системи управління підприємствами критичної інфраструктури, забезпечуючи їх адаптацію до динамічних умов зовнішнього середовища та інтеграцію у європейський економічний простір. У зв'язку з цим особливої актуальності набуває теоретичне осмислення сутності корпоративного комплаєнсу, оскільки його ефективне впровадження безпосередньо залежить від чіткого визначення концептуальних засад та методологічних підходів до його формування.

У науковій літературі сформувався багатовекторний підхід до трактування поняття «корпоративний комплаєнс», що відображає еволюцію його змісту від вузько нормативного інструменту до комплексної управлінської категорії. Аналіз існуючих наукових підходів дозволяє виокремити декілька концептуальних напрямів, кожен із яких акцентує увагу на певному аспекті функціонального призначення комплаєнсу [1-4].

Нормативний підхід інтерпретує корпоративний комплаєнс передусім як забезпечення відповідності діяльності підприємства вимогам чинного законодавства, підзаконних актів та регуляторних норм. У межах цього підходу комплаєнс розглядається як інструмент мінімізації правових ризиків та запобігання порушенням, що можуть призвести до санкцій або втрати репутації [4]. Водночас його обмеженням є орієнтація переважно на формальне дотримання встановлених правил без належного врахування внутрішніх управлінських процесів і стратегічних цілей підприємства.

Управлінський підхід розширює зміст комплаєнсу, інтегруючи його у систему корпоративного управління. У цьому контексті комплаєнс виступає інструментом забезпечення ефективності управлінських рішень, зниження агентських витрат, узгодження інтересів стейкхолдерів та формування системи внутрішнього контролю. Такий підхід дозволяє розглядати комплаєнс не лише як реакцію на зовнішні вимоги, але і як проактивний механізм управління ризиками та підвищення результативності діяльності підприємства [1-3].

Інституційний підхід, своєю чергою, акцентує увагу на ролі неформальних норм та інституційного середовища, в якому функціонує підприємство. У межах цього підходу

корпоративний комплаєнс пов'язується з дотриманням етичних стандартів, формуванням корпоративної культури, підтриманням ділової репутації та відповідністю галузевим і суспільним очікуванням. Це дозволяє розширити межі комплаєнсу за рахунок включення поведінкових та соціальних аспектів діяльності підприємства [1-3].

Узагальнення зазначених підходів дає підстави розглядати корпоративний комплаєнс підприємств критичної інфраструктури як інтегровану, багаторівневу систему організаційно-правових, управлінських та інформаційно-аналітичних заходів, спрямованих на забезпечення відповідності діяльності підприємства вимогам законодавства, міжнародних стандартів та внутрішніх регламентів, а також на системне управління ризиками з метою підтримання стійкості та безперервності його функціонування [1-4].

Специфіка застосування комплаєнсу у сфері критичної інфраструктури полягає у його тісному взаємозв'язку з питаннями безпеки, що істотно розширює функціональні межі цього інструменту. Порушення комплаєнс-вимог у даному секторі здатне спричинити не лише економічні втрати, але й масштабні соціальні, техногенні та інституційні наслідки, що впливають на функціонування суспільства в цілому. У зв'язку з цим корпоративний комплаєнс трансформується у критично важливий елемент забезпечення національної та економічної безпеки, інтегрований у загальну систему управління підприємствами критичної інфраструктури. Систематизація наукових підходів до трактування корпоративного комплаєнсу дозволяє узагальнити їх сутнісні характеристики та обмеження, що відображено на рис. 1.

Узагальнення наведених підходів дозволяє сформуванню цілісного уявлення про сутність корпоративного комплаєнсу як багатовимірної категорії, що поєднує нормативний, управлінський та інституційний аспекти. Разом із тим, сучасні умови функціонування підприємств, особливо у сфері критичної інфраструктури, потребують подальшого розвитку зазначених підходів з урахуванням трансформацій зовнішнього середовища.



Рис.1. Систематизація підходів до трактування корпоративного комплаєнсу

Джерело: узагальнено авторами на основі аналізу наукових підходів [1-4].

Визначальним фактором виступають євроінтеграційні процеси, які формують нові орієнтири розвитку систем корпоративного управління в Україні, що передбачає не лише формальну імплементацію норм і стандартів Європейського Союзу, але й глибоку трансформацію підходів до організації управлінських процесів на підприємствах, зокрема у сфері функціонування підприємств критичної інфраструктури. Особливого значення набуває гармонізація регуляторного середовища у сфері функціонування підприємств критичної інфраструктури, діяльність яких безпосередньо пов'язана із забезпеченням стійкості соціально-економічних систем.

Ключовими орієнтирами у формуванні сучасних підходів до управління виступають положення Директиви (ЄС) 2022/2557 щодо стійкості критичних суб'єктів (CER) та Директиви (ЄС)

2022/2555 щодо мережевої та інформаційної безпеки (NIS2), які закладають основу комплексного підходу до забезпечення стійкості підприємств [9, 10]. На відміну від традиційних моделей регулювання, зазначені нормативні акти орієнтовані на інтеграцію різних аспектів управління, що охоплюють як організаційні, так і технологічні складові функціонування підприємства.

У межах сучасної європейської регуляторної парадигми забезпечення стійкості підприємств передбачає системне управління ризиками, що базується на їх ідентифікації, оцінюванні та пріоритизації; розроблення та впровадження механізмів забезпечення безперервності діяльності; інтеграцію заходів кібербезпеки у загальну систему управління; формування процедур оперативного інформування про інциденти; а також посилення відповідальності вищого керівництва за дотримання встановлених вимог. Важливою характеристикою зазначеного підходу є його проактивний характер, спрямований не лише на реагування на загрози, але й на їх попередження.

Міжнародні стандарти, зокрема ISO 37301:2021, а також принципи корпоративного управління OECD, формують концептуальні засади побудови ефективних комплаєнс-систем, акцентуючи увагу на необхідності інституціоналізації комплаєнс-функції, розвитку комплаєнс-культури та інтеграції механізмів контролю у процес прийняття управлінських рішень [11- 14]. У цьому контексті комплаєнс розглядається не як ізольований інструмент контролю, а як невід’ємний елемент системи управління, що забезпечує узгодженість внутрішніх процесів підприємства із зовнішніми регуляторними вимогами.

У сучасних умовах корпоративний комплаєнс набуває системного, міжфункціонального характеру та виступає не лише механізмом забезпечення нормативної відповідності, але й інструментом стратегічної інтеграції підприємств у європейський економічний простір, підвищення їх інституційної стійкості та конкурентоспроможності.

Систематизація ключових вимог європейського регуляторного середовища та їх імплікацій для формування корпоративного комплаєнсу підприємств критичної інфраструктури представлена в табл. 1.

Таблиця 1

Вимоги ЄС до корпоративного комплаєнсу підприємств критичної інфраструктури

Вимога ЄС	Джерело (CER / NIS2 / ISO / OECD)	Зміст вимоги	Імплікації для корпоративного комплаєнсу
Управління ризиками	CER, NIS2, ISO 37301	Ідентифікація, оцінювання та управління ризиками	Формування ризик-орієнтованої комплаєнс-системи, впровадження реєстру ризиків та KRI
Забезпечення безперервності діяльності	CER	Розроблення планів безперервності (BCP) та відновлення (DRP)	Інтеграція процедур антикризового управління у систему комплаєнсу
Кібербезпека	NIS2	Захист інформаційних систем та управління кіберризиками	Включення кіберкомплаєнсу як складової загальної системи відповідності
Звітність про інциденти	NIS2	Своєчасне інформування про кіберінциденти та порушення	Формування процедур комплаєнс-моніторингу та системи внутрішньої звітності
Відповідальність керівництва	NIS2, OECD	Посилення ролі топменеджменту у забезпеченні комплаєнсу	Закріплення відповідальності керівництва за стан комплаєнсу та ризики
Прозорість діяльності	OECD	Розкриття інформації для стейкхолдерів	Розвиток системи нефінансової звітності та комплаєнс-комунікацій
Формування комплаєнс-культури	ISO 37301	Розвиток етичних стандартів і внутрішніх норм поведінки	Впровадження кодексу етики, навчання персоналу та комплаєнс-політик
Інтеграція комплаєнсу в управління	ISO 37301, OECD	Вбудованість комплаєнсу у бізнес-процеси	Перехід до моделі «compliance by design» у всіх управлінських рішеннях

Джерело: узагальнено авторами на основі [9-12].

З урахуванням вимог європейського регуляторного середовища, а також сучасних концепцій корпоративного управління, доцільним є виокремлення системи принципів корпоративного комплаєнсу, структурованої за ієрархічною логікою. Такий підхід дозволяє не

лише систематизувати комплаєнс як управлінську категорію, але й відобразити його багаторівневу природу, починаючи від базових нормативних засад і завершуючи стратегічними орієнтирами розвитку підприємства.

На першому рівні доцільно виділити фундаментальні принципи, які формують основу функціонування комплаєнс-системи та визначають її нормативно-правовий і організаційний базис. До них належить принцип законності, що передбачає безумовне дотримання вимог національного законодавства, актів Європейського Союзу та міжнародних стандартів у всіх сферах діяльності підприємства. Важливим доповненням виступає принцип підзвітності, який забезпечує чітке розмежування відповідальності між органами управління та визначає механізми контролю за виконанням комплаєнс-функцій. Принцип пропорційності, своєю чергою, орієнтує систему комплаєнсу на збалансування витрат і заходів із рівнем ризиків та масштабами діяльності підприємства, що є особливо актуальним для суб'єктів критичної інфраструктури.

Другий рівень представлений операційними принципами, які визначають практичні аспекти реалізації комплаєнс-системи у поточній діяльності підприємства. Центральне місце серед них займає принцип ризик-орієнтованості, що передбачає пріоритизацію комплаєнс-заходів відповідно до значущості та ймовірності виникнення ризиків. Не менш важливим є принцип безперервності, спрямований на забезпечення стабільного функціонування підприємства та здатності до швидкого відновлення у разі виникнення кризових ситуацій. Принцип прозорості забезпечує відкритість діяльності підприємства, формує довіру з боку стейкхолдерів та створює передумови для ефективної взаємодії з регуляторними органами.

Третій рівень складають адаптаційні принципи, які відображають стратегічний вимір розвитку комплаєнс-системи та її здатність функціонувати в умовах динамічних змін зовнішнього середовища. Принцип адаптивності передбачає гнучке реагування системи комплаєнсу на трансформації регуляторного поля, зокрема у процесі європейської інтеграції. Водночас принцип інтеграції забезпечує вбудованість комплаєнсу у всі бізнес-процеси підприємства, що дозволяє розглядати його не як окрему функцію, а як невід'ємний елемент системи управління.

Концептуалізація принципів корпоративного комплаєнсу потребує їх практичної інтеграції у систему управління підприємством, що обумовлює доцільність побудови узагальненої моделі корпоративного комплаєнсу підприємств критичної інфраструктури (рис. 2).

Запропонована ієрархічна система принципів корпоративного комплаєнсу формує методологічну основу побудови ефективної комплаєнс-системи підприємств критичної інфраструктури та визначає логіку її функціонування. Узагальнення зазначених принципів, а також врахування вимог європейського регуляторного середовища дозволили сформуувати інтегровану модель корпоративного комплаєнсу, представлену на рис. 2.

На відміну від традиційних підходів, запропонована модель має комплексний характер і поєднує структурні елементи комплаєнс-системи, принципи її функціонування та поетапний механізм впровадження. Такий підхід забезпечує узгодженість між стратегічними цілями, операційною діяльністю та інструментами реалізації комплаєнсу, що є критично важливим для підприємств, які функціонують в умовах підвищеної невизначеності та регуляторного навантаження. Змістовно модель відображає взаємозв'язок між зовнішнім середовищем, яке формує вимоги до діяльності підприємства, цільовими орієнтирами комплаєнсу, ключовими напрямками його реалізації, інструментарієм та інформаційно-аналітичним забезпеченням. Важливим елементом моделі є результативний компонент, що характеризує досягнення відповідності регуляторним вимогам, зниження рівня ризиків та забезпечення безперервності діяльності.

Особливістю моделі є наявність зворотного зв'язку, який забезпечує її адаптивність та здатність до постійного вдосконалення відповідно до змін зовнішнього середовища, що дозволяє розглядати комплаєнс не як статичну систему, а як динамічний механізм управління, інтегрований у всі бізнес-процеси підприємства. Крім того, у межах моделі відображено поетапний процес впровадження комплаєнс-системи, що охоплює діагностику поточного стану підприємства, формування нормативної бази, організаційне забезпечення, технологічну інтеграцію та подальший моніторинг і вдосконалення. Інтеграція зазначених етапів у загальну структуру моделі дозволяє забезпечити її практичну спрямованість та можливість застосування в діяльності підприємств критичної інфраструктури.

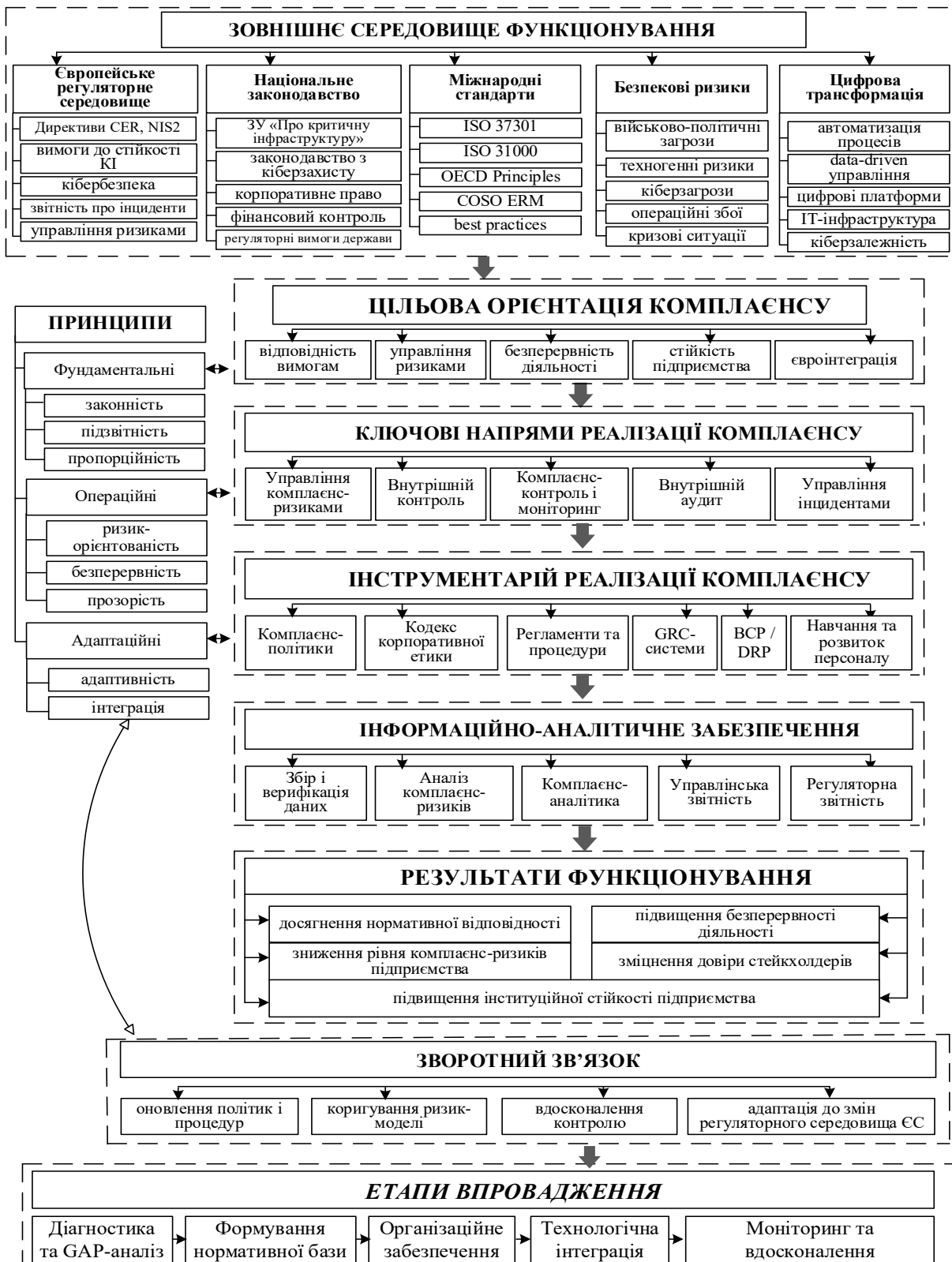


Рис.2. Модель корпоративного комплаєнсу підприємств критичної інфраструктури в умовах європейської інтеграції
 Джерело: розроблено авторами

Формування корпоративного комплаєнсу на підприємствах критичної інфраструктури зумовлюється їх системною значущістю та підвищеною чутливістю до зовнішніх ризиків, що вимагає переосмислення традиційних підходів до забезпечення відповідності. На відміну від інших суб'єктів господарювання, комплаєнс у цьому секторі виконує не лише функцію дотримання нормативних вимог, а й виступає інструментом забезпечення стійкості та безперервності виконання критично важливих функцій.

У цьому контексті комплаєнс-система набуває інтегрованого характеру, поєднуючись із системами управління безпекою, зокрема у частині фізичного захисту, кібербезпеки та інформаційної безпеки. Така інтеграція відповідає логіці побудови моделі, представленій на рис. 2, де комплаєнс розглядається як складова комплексної системи управління підприємством, що забезпечує узгодженість між внутрішніми процесами та зовнішніми вимогами.

Суттєвою характеристикою комплаєнсу в умовах функціонування критичної інфраструктури є його орієнтація на підтримання безперервності діяльності, що передбачає розроблення та впровадження механізмів реагування на інциденти, планів відновлення функціонування та інструментів управління ризиками, що узгоджується з вимогами європейського регуляторного середовища щодо підвищення стійкості критичних суб'єктів.

Зростає значення інституційної взаємодії підприємств із державними органами та регуляторами, що обумовлює необхідність забезпечення прозорості діяльності, дотримання стандартів звітності та своєчасного інформування про ризики й інциденти. У цьому аспекті комплаєнс виконує функцію координації взаємодії між підприємством і зовнішнім середовищем, сприяючи підвищенню рівня довіри та ефективності регуляторного контролю.

Таким чином, корпоративний комплаєнс підприємств критичної інфраструктури доцільно розглядати як проактивну, адаптивну та інтегровану систему управління, яка забезпечує не лише відповідність регуляторним вимогам, але й формує передумови для підвищення стійкості, безпеки та ефективності функціонування підприємства в умовах європейської інтеграції.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, встановлено, що в умовах посилення безпекових викликів, цифрової трансформації та євроінтеграційних процесів корпоративний комплаєнс набуває стратегічного значення для підприємств критичної інфраструктури та трансформується у системоутворюючий елемент управління, орієнтований на забезпечення відповідності, управління ризиками та підтримання безперервності діяльності. Узагальнення наукових підходів дозволило виокремити нормативний, управлінський та інституційний напрями трактування комплаєнсу та обґрунтувати доцільність їх інтеграції. На цій основі розроблено модель корпоративного комплаєнсу, яка поєднує принципи, ключові напрями реалізації, інструментарій та поетапний механізм впровадження з урахуванням вимог європейського регуляторного середовища.

Практичне значення отриманих результатів полягає у можливості застосування запропонованої моделі для підвищення ефективності управління комплаєнс-ризиками, забезпечення безперервності функціонування та зміцнення стійкості підприємств критичної інфраструктури в умовах європейської інтеграції.

ЛІТЕРАТУРА:

1. Fombrun C. J. *Reputation: Realizing Value from the Corporate Image*. Boston: Harvard Business School Press, 1996. 441 p.
2. Teece D. J. Intangible Resources. *The Palgrave Encyclopedia of Strategic Management*. London, 2016. P. 1–2. DOI: https://doi.org/10.1057/978-1-349-94848-2_132-1
3. Rindova V. P., Williamson I. O., Petkova A. P., Sever J. M. Being Good or Being Known: An Empirical Examination of the Dimensions, Antecedents, and Consequences of Organizational Reputation. *Academy of Management Journal*. 2005. Vol. 48, No. 6. P. 1033–1049. DOI: <https://doi.org/10.5465/amj.2005.19573108>
4. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management – Integrating with Strategy and Performance*. 2017. URL: <https://www.coso.org/Pages/erm.aspx>
5. Геєць В. М. Економіка України: ключові проблеми і перспективи. *Науковий вісник Дипломатичної академії України*. 2016. Вип. 23. С. 164–176.
6. Кириленко С. В. ІННОВАЦІЙНИЙ РОЗВИТОК БІЗНЕС-СТРУКТУР В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ. *Journal of Strategic Economic Research*. 2025. № 5. С. 43–51. URL: <https://doi.org/10.30857/2786-5398.2024.5.4>
7. Косович Б. І. ЕКОЛОГІЗАЦІЯ ЯК НАПРЯМ ІННОВАЦІЙНОГО РОЗВИТКУ ПІДПРИЄМНИЦТВА. *Підприємництво та інновації*. 2021. № 17. С. 60–65. URL: <https://doi.org/10.37320/2415-3583/17.12>

8. Стеблянко-Авраменко М. С., Дорошенко М. А. Політика управління підприємством в сучасних умовах трансформації економіки України : thesis. 2014. URL: <http://dspace.puet.edu.ua/handle/123456789/2282>
9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER). URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
11. ISO 37301:2021. *Compliance management systems - Requirements with guidance for use*. International Organization for Standardization, 2021.
12. OECD. *G20/OECD Principles of Corporate Governance*. Paris: OECD Publishing, 2015. URL: <https://www.oecd.org/corporate/principles-corporate-governance/>
13. Чобіток В., Гавриш О. Формування механізму управління ризиками в процесі розвитку критичної інфраструктури України. *Development Service Industry Management*, 4, 2025, 230-237. [https://doi.org/10.31891/dsim-2025-12\(31\)](https://doi.org/10.31891/dsim-2025-12(31))
14. Чобіток В., Чорна Т.Актуальність інформаційних ресурсів в системі управління підприємствами критичної інфраструктури на регіональному рівні. *Актуальні проблеми економіки* № 8 (290), 2025. С. 210-221.

REFERENCES:

1. Fombrun C. J. *Reputation: Realizing Value from the Corporate Image*. Boston: Harvard Business School Press, 1996. 441 p.
2. Teece D. J. Intangible Resources. *The Palgrave Encyclopedia of Strategic Management*. London, 2016. P. 1-2. DOI: https://doi.org/10.1057/978-1-349-94848-2_132-1
3. Rindova V. P., Williamson I. O., Petkova A. P., Sever J. M. Being Good or Being Known: An Empirical Examination of the Dimensions, Antecedents, and Consequences of Organizational Reputation. *Academy of Management Journal*. 2005. Vol. 48, No. 6. P. 1033-1049. DOI: <https://doi.org/10.5465/amj.2005.19573108>
4. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management – Integrating with Strategy and Performance*. 2017. URL: <https://www.coso.org/Pages/erm.aspx>
5. Heiets V. M. *Ekonomika Ukrainy: kluchovi problemy i perspektyvy*. *Naukovyi visnyk Dyplomatychnoi akademii Ukrainy*. 2016. Vyp. 23. S. 164-176.
6. Kyrylenko S. V. Innovatsiyni rozvytok biznes-struktur v umovakh tsyfrovoy ekonomiky. *Journal of Strategic Economic Research*. 2025. № 5. S. 43-51. URL: <https://doi.org/10.30857/2786-5398.2024.5.4>
7. Kosovych B. I. Ekolohizatsiia yak napriam innovatsiynoho rozvytku pidpriemnytstva. *Pidpriemnytstvo ta innovatsii*. 2021. № 17. S. 60-65. URL: <https://doi.org/10.37320/2415-3583/17.12>
8. Steblianko-Avramenko M. S., Doroshenko M. A. Polityka upravlinnia pidpriemstvom v suchasnykh umovakh transformatsii ekonomiky Ukrainy: thesis. 2014. URL: <http://dspace.puet.edu.ua/handle/123456789/2282>
9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER). URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
11. ISO 37301:2021. *Compliance management systems – Requirements with guidance for use*. International Organization for Standardization, 2021.
12. OECD. *G20/OECD Principles of Corporate Governance*. Paris: OECD Publishing, 2015. URL: <https://www.oecd.org/corporate/principles-corporate-governance/>
13. Chobitok V., Havrysh O. Formuvannya mekhanizmu upravlinnia ryzykamy v protsesi rozvytku krytychnoi infrastruktury Ukrainy. *Development Service Industry Management*, 4, 2025, 230-237. [https://doi.org/10.31891/dsim-2025-12\(31\)](https://doi.org/10.31891/dsim-2025-12(31))
14. Chobitok V., Chorna T. Aktualnist informatsiinykh resursiv v systemi upravlinnia pidpriemstvamy krytychnoi infrastruktury na rehionalnomu rivni. *Aktualni problemy ekonomiky* № 8 (290), 2025. S. 210-221.

FORMATION OF PRINCIPLES OF CORPORATE COMPLIANCE IN THE MANAGEMENT OF
CRITICAL INFRASTRUCTURE ENTERPRISES UNDER THE CONDITIONS OF EUROPEAN
INTEGRATION

CHOBITOK Viktoriia¹, NESTERENKO Roman², HOKH Iryna³

¹ National Research Institute "Ukrainian Engineering Pedagogical Academy" V.N. Karazin Kharkiv National University
<https://orcid.org/0000-0002-5272-388X>

² National Institute of Professional Education of the National Academy of the National Guard of Ukraine
<https://orcid.org/0000-0001-6357-3613>

³ National Institute of Professional Education of the National Academy of the National Guard of Ukraine
<https://orcid.org/0000-0001-8465-9774>

The relevance of the study is обусловлена the growing role of critical infrastructure enterprises in ensuring the resilience of socio-economic systems amid increasing security challenges, digital transformation, and the intensification of European integration processes. These conditions heighten the requirements for effective management systems, particularly in ensuring regulatory compliance, risk management, and business continuity. The implementation of European regulatory standards in the fields of critical entity resilience and cybersecurity necessitates the development of modern compliance systems integrated into the overall enterprise management framework.

An analysis of recent research indicates that issues of corporate compliance, risk management, and internal control are widely explored by both international and domestic scholars. However, compliance is predominantly viewed as a tool for ensuring transparency and minimizing risks, while its systemic integration into the management of critical infrastructure enterprises remains insufficiently developed. In particular, there is a need to form a comprehensive system of corporate compliance principles that considers current regulatory and security requirements.

The purpose of the study is to substantiate the principles of corporate compliance in managing critical infrastructure enterprises under European integration conditions and to develop an integrated compliance system model. The paper generalizes scientific approaches to the interpretation of compliance, allowing the identification of its regulatory, managerial, and institutional dimensions. Based on this, a system of corporate compliance principles is proposed, along with an integrated model for its implementation.

The proposed model combines external regulatory requirements, strategic objectives, key implementation directions, tools, and information-analytical support. It also prevede a phased implementation mechanism with feedback. This ensures the alignment of management processes with European standards, enhances enterprise performance, and facilitates adaptation to a dynamic regulatory environment. It is concluded that integrating compliance into corporate governance is a key factor in strengthening the resilience of critical infrastructure enterprises and mitigating operational risks.

Keywords: corporate compliance, critical infrastructure enterprises, compliance system, risk management, European integration, regulatory environment, business continuity, corporate governance