УДК 351:005.334:005.35:338.27
DOI: https://doi.org/10.32782/2311-844X/2025-2-1

**Копитко Марта Іванівна**
завідувач кафедри менеджменту та економічної безпеки
Навчально-наукового інституту управління, психології та безпеки,
Львівський державний університет внутрішніх справ
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0001-6598-3798

**Вінічук Марія Володимирівна**
професор кафедри менеджменту та економічної безпеки
Навчально-наукового інституту управління, психології та безпеки,
Львівський державний університет внутрішніх справ
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0002-6588-1254

# КОМПЛАЄНС-КОНТРОЛЬ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ ТА КОНТРОЛІНГУ БЕЗПЕКИ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

***Анотація.*** *У статті досліджено теоретико-методологічні засади та прикладні аспекти інтеграції комплаєнс-контролю у систему публічного управління та контролінгу безпеки підприємств критичної інфраструктури України. Проаналізовано сучасні підходи до забезпечення законності, етичності та ефективності управлінських рішень у сфері безпеки стратегічно важливих об'єктів, що виконують ключові функції в економіці та національній безпеці. Визначено роль комплаєнс-механізмів як інструменту управління ризиками на підприємстві, запобігання кризовим подіям, підвищення організаційної стійкості та забезпечення корпоративної відповідальності. Досліджено взаємозв'язок між державним регулюванням, корпоративними практиками та контролінговими інструментами безпеки. Встановлено зв'язок між рівнем впровадження контролінгу безпеки та здатністю підприємств протидіяти кризовим ситуаціям, що дозволяє визначити ключові фактори підвищення ефективності організаційно-правового механізму забезпечення безпеки підприємств критичної інфраструктури. На основі проведеного аналізу запропоновано концептуальні підходи до вдосконалення системи публічного управління безпекою, інтеграції комплаєнс-механізмів у корпоративну практику та формування єдиного контролінгового середовища для підприємств критичної інфраструктури. Отримані висновки можуть слугувати методологічною основою для удосконалення системи публічного управління та впровадження комплексних механізмів контролінгу безпеки на підприємствах критичної інфраструктури України. Перспективами подальших наукових досліджень виступає розробка кількісних методик оцінювання ефективності комплаєнс-контролю шляхом створення інтегрованих індексів та шкали, які дозволять вимірювати рівень впровадження комплаєнс-механізмів та їхній вплив на готовність підприємств до кризових подій.*

***Ключові слова:*** *комплаєнс-контроль, публічне управління, контролінг, критична інфраструктура, управління ризиками.*

**Kopytko Marta, Vinichuk Mariia**
Lviv State University of Internal Affairs

# COMPLIANCE CONTROL IN THE SYSTEM OF PUBLIC ADMINISTRATION AND SECURITY CONTROLLING OF CRITICAL INFRASTRUCTURE ENTERPRISES IN UKRAINE

***Abstract.*** *The article examines the theoretical and methodological foundations as well as practical aspects of integrating compliance control into the system of public administration and security controlling of critical*

*infrastructure enterprises in Ukraine. Modern approaches to ensuring legality, ethical standards, and the effectiveness of managerial decisions in the security of strategically important facilities, which perform key functions in the economy and national security, are analyzed. The study highlights the role of compliance mechanisms as tools for enterprise risk management, crisis prevention, enhancing organizational resilience, and ensuring corporate responsibility. The interrelationship between state regulation, corporate practices, and security controlling instruments is investigated. A connection between the level of security controlling implementation and the ability of enterprises to respond to crisis situations is established, allowing identification of key factors for improving the effectiveness of the organizational and legal mechanism for ensuring the security of critical infrastructure enterprises. Based on the analysis, conceptual approaches are proposed for enhancing the public administration system of security, integrating compliance mechanisms into corporate practices, and creating a unified controlling environment for critical infrastructure enterprises. The findings can serve as a methodological basis for improving public administration systems and implementing comprehensive security controlling mechanisms in critical infrastructure enterprises in Ukraine. Prospects for further research include the development of quantitative methods for assessing the effectiveness of compliance control through the creation of integrated indices and scales, which will enable measuring the level of compliance mechanism implementation and their impact on the crisis readiness of enterprises.*

***Keywords:*** *compliance control, public administration, controlling, critical infrastructure, risk management.*

**Вступ.** Сучасні виклики, зумовлені геополітичною нестабільністю, гібридними загрозами, військовою агресією проти України, масштабною цифровізацією та зростанням рівня кіберризиків, актуалізують необхідність формування нових підходів до забезпечення безпеки підприємств критичної інфраструктури (КІ). У цих умовах особливого значення набуває інтеграція інструментів комплаєнс-контролю, контролінгу безпеки та публічного управління, що дозволяє забезпечити належний рівень організаційно-правової, інформаційної та економічної стійкості стратегічно важливих суб'єктів господарювання.

Підприємства критичної інфраструктури, як основа функціонування національної економіки та суспільної стабільності, перебувають у полі постійної взаємодії з державними інституціями, регуляторними органами, місцевим самоврядуванням та громадськістю, що вимагає впровадження ефективних механізмів комплаєнс-контролю, під яким розуміється система дотримання законодавчих, нормативних, етичних і безпекових вимог, що є інструментом попередження правопорушень, зловживань, конфліктів інтересів та корупційних ризиків.

Водночас, контролінг безпеки на підприємстві виступає аналітичною та моніторинговою підсистемою управління, що забезпечує оцінювання ризиків, результативності заходів захисту, а також формування інформаційно-аналітичного підґрунтя для прийняття управлінських рішень у сфері безпеки. Його ефективне функціонування можливе лише за умови належної інституційної підтримки з боку системи публічного управління, яка визначає стратегічні пріоритети, регламентує стандарти безпеки та координує діяльність суб'єктів критичної інфраструктури. Стає очевидним, що формування інтегрованої системи «публічне управління – контролінг безпеки – комплаєнс-контроль» постає ключовою умовою підвищення ефективності організаційно-правового механізму безпеки підприємств критичної інфраструктури. Її впровадження сприяє зміцненню інституційної спроможності держави, забезпеченню прозорості управлінських процесів, підвищенню рівня довіри до державних і корпоративних структур та мінімізації ризиків порушення вимог національної і міжнародної безпеки.

Водночас, незважаючи на зростання уваги до питань корпоративного комплаєнсу та державного контролю безпеки, інтеграція цих систем у контексті публічного управління критичною інфраструктурою залишається недостатньо дослідженою. Це зумовлює потребу у формуванні цілісної концепції комплаєнс-контролю в системі публічного управління та контролінгу безпеки підприємств критичної інфраструктури України, що поєднує державні, корпоративні та соціально-етичні аспекти управління безпекою.

**Матеріали та методи.** Метою статті є дослідження теоретико-методологічних засад інтеграції комплаєнс-контролю в систему публічного управління та контролінгу безпеки підприємств критичної інфраструктури України з урахуванням сучасних викликів економічної, інформаційної та організаційно-правової безпеки.

Сучасні дослідження у сфері комплаєнсу, публічного управління та контролінгу свідчать про зростання уваги науковців до питань формування інтегрованих механізмів управління безпекою підприємств критичної інфраструктури. Зокрема, О. Ковальчук, К. Моранченко та Д. Бібік [1] наголошуюь на тому, що комплаєнс є багатовимірним інструментом управління, який поєднує правові, етичні та організаційно-контрольні механізми забезпечення відповідності діяльності підприємства нормативним вимогам і корпоративним стандартам. Автори підкреслюють, що ефективність комплаєнс-системи визначається ступенем її інтеграції з процесами внутрішнього контролю та оцінювання ризиків, що є безпосереднім предметом контролінгу безпеки.

В даному контексті, слушним є зауваження А. Мулик [2, с. 65], який розкриває специфіку правового регулювання корпоративного комплаєнсу в Україні, наголошуючи на необхідності вдосконалення законодавчого поля для забезпечення узгодженості між корпоративними стандартами та вимогами державного регулювання. Науковець зазначає, що комплаєнс має розглядатися як складова організаційно-правового механізму безпеки, який формує довіру між бізнесом і державою, а також мінімізує ризики зловживань і корупційних практик.

У свою чергу, М. Нежива, В. Мисюк та В. Негоденко [3] у власних дослідженнях окресленої проблематики акцентують увагу на практичному значенні антикорупційних процедур комплаєнсу, які забезпечують доброчесність корпоративного управління, запобігають конфлікту інтересів і сприяють підвищенню репутаційної стійкості підприємств. При цьому, М. Бліхар, Н. Лук'янова, О. Скочиляс-Павлів та М. Вінічук [4] доводять, що антикорупційний компонент є невід'ємним елементом загальної системи безпеки підприємства, особливо у сфері критичної інфраструктури, де ризики неправомірних дій можуть мати стратегічні наслідки для національної безпеки, що обумовлює необхідність належного реагування на такі виклики зі сторони органів публічного управління.

З позиції кібербезпеки цінними є результати дослідження С. Толюпа, С. Бучик, О. Кулініч та О. Бучик [5], які обґрунтували методи управління інформаційною безпекою критичної інфраструктури через ризик-орієнтований підхід, системи моніторингу загроз і контролю відповідності нормативним вимогам. Науковці підкреслюють, що технічний рівень кіберзахисту має бути безпосередньо пов'язаний із процедурним контролем комплаєнсу, який забезпечує сталість політик безпеки в межах публічного управління.

А. Волков, М. Бречка, В. Стадніченко, В. Ярощук та С. Черкашин [6] розглядають питання фізичного та організаційного захисту об'єктів критичної інфраструктури, вважаючи їх вкрай важливими в умовах сьогодення, наголошуючи на потребі комплексного публічно-приватного підходу до управління ризиками. Дослідники роблять висновок, що ефективність системи безпеки підприємств критичної інфраструктури залежить від узгодженості дій державних органів, органів місцевого самоврядування та суб'єктів господарювання, що повністю відповідає ідеї інтеграції комплаєнс-контролю в систему публічного управління.

Актуальні аспекти взаємодії комплаєнсу та державного сектору розкрито у праці П. Шпиги [7], який аналізує реалізацію принципів комплаєнсу в системі реформ публічного управління України, роблячи акцент на необхідності запровадження ефективних механізмів моніторингу виконання стратегічних документів і підзвітності державних структур. Дослідження науковця доводить, що впровадження комплаєнс-принципів у публічному секторі створює підґрунтя для підвищення ефективності управління об'єктами критичної інфраструктури.

Додатковим напрямом, який тісно пов'язаний із зазначеним, є контролінг. У статті Т. Кладницької, І. Артімонова, І. Каменяш та

Н. Свиноус [8] розкрито аналітичні та методичні підходи до оцінювання ефективності систем безпеки підприємств через призму фінансових показників, ризик-аналізу та контролю витрат. Науковці обґрунтовують, що контролінг виступає дієвим інструментом раннього попередження кризових явищ, виявлення нецільового використання ресурсів і порушень принципів комплаєнсу. Водночас, на вагомості проблематики контролінгу та ефективності його інструментів при дослідженні основних аспектів економічної безпеки підприємств ми наголошували у попередніх дослідженнях [9, с. 131; 10], де встановлено, що контролінг охоплює комплекс заходів з моніторингу, аналізу та управління процесами, які дозволяють оптимізувати ресурси, мінімізувати ризики та підвищити ефективність діяльності суб'єктів господарювання.

Узагальнення наведених наукових позицій дає змогу констатувати, що в науковому дискурсі основна увага зосереджується переважно на окремих аспектах комплаєнсу, а саме: правових, організаційних, антикорупційних або технічних, проте інтеграція цих елементів у єдину систему публічного управління та контролінгу безпеки підприємств досі залишається недостатньо розробленою. Отже, виникає наукова потреба у формуванні цілісної концепції комплаєнс-контролю як складової системи публічного управління та контролінгу безпеки підприємств критичної інфраструктури України, що й визначає напрям подальших досліджень.

У дослідженні використано комплексний підхід, що поєднує теоретичний аналіз наукових джерел у сфері комплаєнсу та безпеки критичної інфраструктури, а також емпіричні дані, отримані шляхом опитування менеджерів та спеціалістів підприємств критичної інфраструктури та аналітичного моніторингу таких підприємств. Зокрема, теоретичний аналіз та узагальнення використано для виявлення концептуальних підходів до інтеграції комплаєнс-контролю та контролінгу безпеки. Порівняльний аналіз застосовано з метою зіставлення практик державного регулювання та корпоративного впровадження контролінгу безпеки. Емпіричні методи: опитування, інтерв'ю та аналіз статистичних даних підприємств критичної інфраструктури використані в процесі дослідження елементів системи контролінгу та комплаєнсу.

**Результати.** У сучасних умовах зростання рівня техногенних, кібернетичних і воєнних загроз, а також деструктивних змін енергетичних і цифрових мереж питання ефективного функціонування системи безпеки критичної інфраструктури набуває стратегічного значення для держави і суспільства. Підприємства критичної інфраструктури є основою економічної, енергетичної та інформаційної стабільності, а отже – ключовим об'єктом публічного управління у сфері національної безпеки. Водночас досвід останніх років свідчить, що наявність нормативно-правової бази не гарантує належного рівня готовності суб'єктів господарювання до кризових подій. Це зумовлює необхідність переосмислення організаційно-правового механізму безпеки через призму сучасних управлінських інструментів, серед яких особливе місце посідає контролінг.

Контролінг у сфері безпеки критичної інфраструктури слід розглядати не лише як систему внутрішнього моніторингу, а як інтегрований механізм стратегічного управління, що поєднує аналітику ризиків, планування ресурсів, оцінювання ефективності управлінських рішень і забезпечення зворотного зв'язку між державними регуляторами та операторами інфраструктури. Впровадження контролінгових практик у публічне управління дозволяє підвищити рівень прозорості, підзвітності та скоординованості дій між державними та корпоративними суб'єктами безпеки.

З огляду на це, актуальним є комплексне дослідження взаємозв'язку між рівнем розвитку систем контролінгу та результативністю організаційно-правового забезпечення безпеки підприємств критичної інфраструктури. Емпіричне дослідження дозволить виявити ключові тенденції, аналітичні залежності та проблемні зони у формуванні ефективної системи публічного управління безпекою критичної інфраструктури України.

З метою кількісного аналізу впливу контролінгових механізмів на рівень безпеки під-

приємств критичної інфраструктури було проведено емпіричне дослідження, яке охопило 45 підприємств із різних секторів: енергетики, транспорту, фінансів, телекомунікацій, водопостачання та охорони здоров'я. Для оцінювання використано комплекс показників, що характеризують ступінь впровадження елементів контролінгу безпеки, наявність внутрішніх регламентів, систем моніторингу ризиків, інституційну зрілість служби безпеки та інтегрованість у державну систему реагування. Результати проведеного дослідження узагальнимо в табл. 1.

Дані таблиці 1 свідчать, що лише близько половини підприємств критичної інфраструктури (50,1%) реалізовують системний підхід до впровадження контролінгу безпеки. Найвищий рівень сформованості спостерігається у сфері нормативно-організаційного забезпечення (наявність політик і регламентів – 85 %) та у проведенні внутрішніх аудитів (62 %). Водночас найменше поширеними залишаються такі інструменти, як автоматизація звітності (29%) і виділення окремих посад контролера безпеки (33%), що вказує на недостатню інституціоналізацію контролінгової функції на підприємствах критичної інфраструктури. Очевидно, що узагальнені результати оцінювання рівня впровадження елементів контролінгу безпеки за секторальним розрізом відображають середні значення інтегрального показника, розрахованого за 100-бальною шкалою, що дає змогу порівняти рівень розвитку контролінгових систем між різними галузями критичної інфраструктури.

Отримані результати підтверджують, що розвиток системи контролінгу безпеки потребує інтеграції публічного управління і внутрішньокорпоративних механізмів для формування єдиних стандартів моніторингу, оцінювання та звітності у сфері критичної інфраструктури. Це дозволить забезпечити не лише формальну відповідність законодавчим вимогам, а й реальне підвищення рівня готовності підприємств до кризових подій, що підтверджується також кореляційними результатами, наведеними на рис. 1.

Результати емпіричного дослідження, проведеного на вибірці з 45 підприємств критичної інфраструктури України, які представляють енергетичний, транспортний, фінансовий, телекомунікаційний та водопостачальний сектори, відображають оцінювання двох інтегральних показників (1) рівень впровадження контролінгу (агрегований індекс, що включає частоту контролінгових аудитів, наявність внутрішніх стандартів безпеки, використання аналітичних панелей (dashboard) для моніторингу ризиків та показників ефективності) та індекс готовності до кризових подій (інтегральний

Таблиця 1

**Рівень впровадження елементів системи контролінгу безпеки на підприємствах критичної інфраструктури України**

| № за/п | Елемент системи контролінгу безпеки | Частка підприємств, що впровадили, % | Середній рівень ефективності (за 5-бальною шкалою) |
|---|---|---|---|
| 1 | Наявність внутрішньої політики безпеки та контролінгових регламентів | 85 | 4,2 |
| 2 | Регулярне проведення внутрішніх аудитів і перевірок ризиків | 62 | 3,6 |
| 3 | Використання аналітичних панелей (dashboard) для моніторингу показників безпеки | 47 | 3,2 |
| 4 | Інтеграція контролінгових даних у систему стратегічного управління | 41 | 3,0 |
| 5 | Наявність окремого підрозділу або посадової особи з контролінгу безпеки | 33 | 2,8 |
| 6 | Автоматизація процесів звітності та оцінювання ризиків | 29 | 2,6 |
| 7 | Регулярна взаємодія з державними органами у сфері кібер- та фізичної безпеки | 54 | 3,4 |

*Джерело: розраховано за [11–12]*

 ISSN 2311-844X

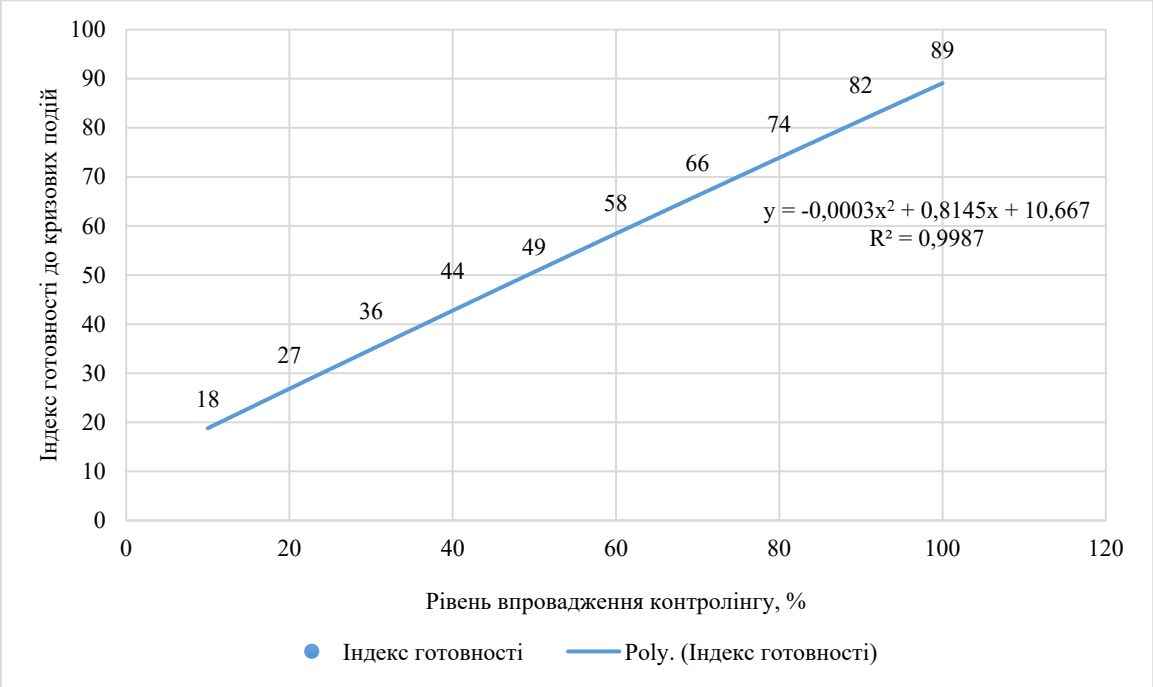


**Рис. 1. Взаємозв'язок між рівнем контролінгу та індексом готовності підприємства до кризових подій**

*Джерело: розраховано за [11–12]*

індикатор, який відображає здатність підприємства до оперативного реагування, наявність планів безперервності діяльності (Business Continuity Plans) та швидкість відновлення після інцидентів). На рисунку зображено позитивну лінійну залежність між рівнем контролінгу та кризовою готовністю підприємств. Згідно з отриманими даними, підприємства, що мають високий рівень розвитку контролінгу (70–100 %), демонструють індекс готовності на рівні 70–90 пунктів, тоді як підприємства з низьким рівнем контролінгу (менше 40 %) – лише до 40–45 пунктів. Це свідчить, що контролінг безпеки виконує роль системоутворювального механізму управління ризиками, забезпечуючи при цьому своєчасне виявлення відхилень і потенційних загроз, підвищення точності управлінських рішень у кризових умовах та інтеграцію фінансових, операційних і інформаційних потоків для комплексного моніторингу стійкості.

З позицій публічного управління, результати підкреслюють необхідність державного стимулювання впровадження контролінгових систем на підприємствах критичної інфраструктури через регуляторні стандарти безпеки, цифрові платформи обміну аналітичними даними між державними органами та операторами інфраструктури та інтеграцію контролінгових індикаторів у систему оцінювання національної стійкості (National Resilience Index).

Таким чином, рис. 1 ілюструє пряму залежність між якістю управлінського контролю та здатністю підприємства функціонувати в умовах кризових ситуацій, що підтверджує стратегічну важливість контролінгу як інструменту публічного управління безпекою критичної інфраструктури.

Результати дослідження підприємств критичної інфраструктури України (енергетика, транспорт, телекомунікації, банківська сфера, водопостачання тощо) за показником рівня впровадження елементів контролінгу безпеки підприємств критичної інфраструктури України (рис. 2) дають підстави стверджувати, що за шкалою 0–100 % найвищий рівень демонструють енергетичні підприємства (78 %) і фінансовий сектор (72 %), тоді як у водопостачанні та транспортній галузі цей показник становить лише 54–59 %.

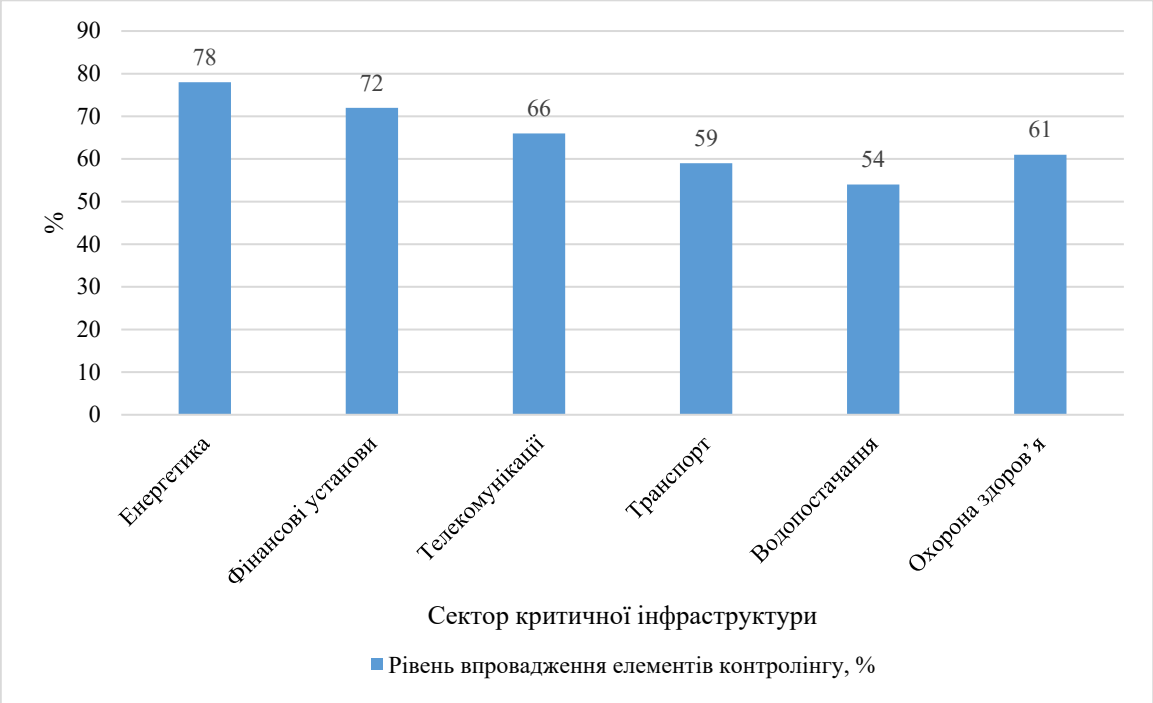


**Рис. 2. Рівень впровадження елементів контролінгу безпеки підприємств критичної інфраструктури України**

*Джерело: розраховано за [11–12]*

Отримані данні свідчать про нерівномірність розвитку контролінгових механізмів безпеки в різних секторах критичної інфраструктури. Це зумовлено різним рівнем цифровізації, вимогами регуляторів та інституційною зрілістю систем внутрішнього аудиту й ризик-менеджменту. Дані підтверджують потребу у створенні єдиної державної політики публічного управління та контролінгу у сфері безпеки критичної інфраструктури. Основними бар'єрами залишаються нормативна фрагментарність, нестача фінансування, кадрові прогалини та слабка міжвідомча координація. Тому, важливим залишається формування комплексу ефективних заходів щодо удосконалити нормативно-правової бази безпеки критичної інфраструктури з урахуванням контролінгових стандартів, запровадження обов'язкових KPI безпеки для операторів КІ та механізм державного аудиту ефективності, розроблення системи підготовки кадрів з безпекового контролінгу у сфері публічного управління, а також створення національної платформи обміну даними між державними органами та операторами критичної інфраструктури.

**Висновки.** Таким чином, проведене дослідження засвідчило, що публічне управління у поєднанні з контролінгом є ключовим інструментом підвищення ефективності організаційно-правового механізму безпеки підприємств критичної інфраструктури України. Емпіричні дані доводять нерівномірність впровадження контролінгових механізмів: найбільш поширеними є політики безпеки та внутрішні аудити, тоді як автоматизація процесів і інтеграція контролінгу у стратегічне управління залишаються недостатньо розвиненими. При цьому, статистичний аналіз підтвердив позитивний взаємозв'язок між рівнем розвитку контролінгу та індексом готовності підприємств до кризових подій ($r \approx 0{,}9987$). Це підкреслює стратегічну роль контролінгу як механізму оцінки ризиків, планування ресурсів і координації дій між державними органами та операторами критичної інфраструктури. Отже, розвиток системи контролінгу у поєднанні з ефективним публічним управлінням здатен значно підвищити стійкість і готовність підприємств до кризових ситуацій, забезпечуючи комплексну безпеку на національному рівні.

**Список використаних джерел:**

1. Ковальчук О. В., Моренченко К. Г., Бібік Д. В. Сутність і характеристика комплаєнсу: визначення, функції, цілі, етичні основи, місце в організаційній структурі підприємства. *Ефективна економіка.* 2023. № 1. DOI: https://doi.org/10.37634/efp.2023.1.4

2. Мулик А. К. Правовий режим корпоративного комплаєнсу. *Молодий вчений.* 2023. № 9 (121). С. 64–69. DOI: https://doi.org/10.32839/2304-5809/2023-9-121-13

3. Нежива М., Мисюк В., Негоденко В. Антикорупційний комплаєнс: нові правила ведення бізнесу. *Економіка, управління та адміністрування.* 2024. № 2(108). С. 92–102. DOI: https://doi.org/10.26642/ema-2024-2(108)-92-102

4. Blikhar M., Lukianova H., Skochylias-Pavliv O., Vinichuk M. Institutional Stability of Public Administration: The Economic and Legal Dimension. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu.* 2024. № 2. P. 178–184. DOI: https://doi.org/10.33271/nvngu/2024-2/178

5. Toliupa S., Buchyk S., Kulinich O., Buchyk O. Protection of State Management of Critical Infrastructure Objects under the Influence of Cyber Attacks. *Information and communication technologies, electronic engineering.* 2022. Vol. 2. No. 2. P. 33–41. P. 33–41. DOI: https://doi.org/10.23939/ictee2022.02.033

6. Volkov A., Brechka M., Stadnichenko V., Yaroshchuk V., Cherkashyn S. The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics.* 2023. № 14(4). P. 23–32. DOI: https://doi.org/10.31548/machinery/4.2023.23

7. Shpyha P., Karpenko Y. Compliance of the Public Administration Reform Strategy of Ukraine with the Requirements of the Regulations of the Cabinet of Ministers. *Public administartion aspects.* 2023. № 11 (4). P. 21–27. DOI: https://doi.org/10.15421/152348

8. Кладницька Т., Артімонова І., Кеменяш І., Свиноус Н. Роль і місце фінансового контролінгу в управлінні фінансових корпорацій. *Сталий розвиток економіки.* 2024. Вип. (2(49). С. 314–318. DOI: https://doi.org/10.32782/2308-1988/2024-49-50

9. Вінічук М. В., Нагірна О. В. Роль інвестиційного контролінгу, корпоративної культури та паблік рілейшнз у забезпеченні стратегічної стійкості, інвестиційної привабливості та соціально-економічної безпеки підприємств ІТ-сфери. *Агросвіт.* 2025. № 14. С. 131–136. DOI: https://doi.org/10.32702/2306-6792.2025.14.131

10. Вінічук М. В., Нагірна О. В. Корпоративна культура, PR-менеджмент та офіс-менеджмент як фактори ефективності інвестиційного контролінгу в системі соціально-економічної безпеки автотранспортних підприємств. *Інвестиції: практика та досвід.* 2025. № 17. С. 177–182. DOI: https://doi.org/10.32702/2306-6814.2025.17.177

11. Calibrated. Are Ukrainian businesses prepared to communicate during cyber and info crises? 2025. URL: https://calibrated.agency/survey-cyber-crisis-response-2025

12. Винниченко І. Організаційна стійкість та операційна безперервність під час кризи: дослідження України. Київ : Американський університет у Києві, 2025. 44 с. URL: https://er.auk.edu.ua/server/api/core/bitstreams/c5d4f798-1167-4b4e-9356-3747b4b871e5/content

**References:**

1. Kovalchuk O. V., Morenchenko K. H. & Bibik D. V. (2023). The essence and characteristics of compliance: Definitions, functions, goals, ethical foundations, and place in the organizational structure of an enterprise. *Effective Economy,* (1). DOI: https://doi.org/10.37634/efp.2023.1.4

2. Mulyk A. K. (2023). Legal regime of corporate compliance. *Molodyi Vchenyi*, 9(121), 64–69. DOI: https://doi.org/10.32839/2304-5809/2023-9-121-13

3. Nezhyva M., Mysiuk, V., & Nehodenko, V. (2024). Anti-corruption compliance: New rules for doing business. *Economics, Management and Administration*, 2(108), 92–102. DOI: https://doi.org/10.26642/ema-2024-2(108)-92-102

4. Blikhar M., Lukianova H., Skochylias-Pavliv O. & Vinichuk M. (2024). Institutional stability of public administration: The economic and legal dimension. *Scientific Bulletin of the National Mining University*, 2, 178–184. DOI: https://doi.org/10.33271/nvngu/2024-2/178

5. Toliupa S., Buchyk S., Kulinich O. & Buchyk O. (2022). Protection of state management of critical infrastructure objects under the influence of cyber attacks. *Information and Communication Technologies, Electronic Engineering*, 2(2), 33–41. DOI: https://doi.org/10.23939/ictee2022.02.033

6. Volkov A., Brechka M., Stadnichenko V., Yaroshchuk V. & Cherkashyn S. (2023). The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics*, 14(4), 23–32. DOI: https://doi.org/10.31548/machinery/4.2023.23

7. Shpyha P. & Karpenko Y. (2023). Compliance of the public administration reform strategy of Ukraine with the requirements of the regulations of the Cabinet of Ministers. *Public Administration Aspects*, 11(4), 21–27. DOI: https://doi.org/10.15421/152348

8. Kladnytska T., Artimonova I., Kemenyash I. & Svynous N. (2024). The role and place of financial controlling in the management of financial corporations. *Sustainable Economic Development*, 2(49), 314–318. DOI: https://doi.org/10.32782/2308-1988/2024-49-50

9. Vinichuk M. V. & Nahirna O. V. (2025). The role of investment controlling, corporate culture, and public relations in ensuring strategic resilience, investment attractiveness, and socio-economic security of IT enterprises. *Agrosvit*, 14, 131–136. DOI: https://doi.org/10.32702/2306-6792.2025.14.131

10. Vinichuk M. V. & Nahirna O. V. (2025). Corporate culture, PR management, and office management as factors of investment controlling efficiency in the system of socio-economic security of transport enterprises. *Investments: Practice and Experience*, 17, 177–182. DOI: https://doi.org/10.32702/2306-6814.2025.17.177

11. Calibrated. (2025). Are Ukrainian businesses prepared to communicate during cyber and info crises? Available at: https://calibrated.agency/survey-cyber-crisis-response-2025

12. Vynnychenko I. (2025). *Organizational resilience and operational continuity during a crisis: A study of Ukraine.* Kyiv: American University in Kyiv. Available at: https://er.auk.edu.ua/server/api/core/bitstreams/c5d4f798-1167-4b4e-9356-3747b4b871e5/content

*Стаття надійшла: 06.10.2025*
*Стаття прийнята: 14.11.2025*
*Стаття опублікована: 22.01.2026*