АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

004.056:004.9

DOI https://doi.org/10.5281/zenodo.19667586

Інформаційна безпека як складова цифрової безпеки підприємства

Обрамич Орест Сергійович

Аспірант кафедри менеджменту і міжнародного підприємництва

Національний університет «Львівська політехніка»

м.Львів, вул. С. Бандери,12; 79000; Україна

e-mail: orest.s.obramych@lpnu.ua

ORCID: https://orcid.org/0009-0006-2280-5549

Іваницький Ігор Богданович

Аспірант кафедри менеджменту і міжнародного підприємництва

Національний університет «Львівська політехніка»

м.Львів, вул. С. Бандери,12; 79000; Україна

e-mail: ihor.b.ivanytskyi@lpnu.ua

https://orcid.org/0000-0008-3267-8015

Прийнято: 03.04.2026 | Опубліковано: 20.04.2026

Анотація: Мета. Метою дослідження є поглиблення теоретичних засад інформаційної безпеки підприємства та обґрунтування її ролі як ключової складової цифрової безпеки в умовах цифрової трансформації економіки. Особливу увагу приділено уточненню сутності інформаційної безпеки, визначенню її структурних елементів та встановленню взаємозв'язку з кібербезпекою.

Методи. У дослідженні використано комплекс загальнонаукових і спеціальних методів, зокрема аналіз і синтез – для узагальнення наукових

підходів до трактування інформаційної безпеки; системний підхід – для визначення її структури та місця у цифровій безпеці; порівняльний аналіз – для виявлення відмінностей у підходах до розуміння інформаційної та кібербезпеки; метод експертного оцінювання та узагальнення емпіричних даних – для оцінки практики забезпечення інформаційної безпеки на підприємствах.

Результати. У процесі дослідження встановлено, що існуючі підходи до визначення інформаційної безпеки мають фрагментарний характер та не враховують її інтеграції у цифрове середовище. Запропоновано розглядати інформаційну безпеку як багаторівневу систему, що охоплює захист даних, інформаційних процесів, управління ризиками та інформаційно-аналітичне забезпечення управління. Доведено, що інформаційна безпека виконує системоутворюючу функцію у структурі цифрової безпеки підприємства, тоді як кібербезпека забезпечує технологічну реалізацію захисних механізмів. Результати емпіричного аналізу свідчать про переважання технічно орієнтованих підходів до забезпечення безпеки на підприємствах та недостатній рівень інтеграції інформаційної безпеки у систему управління, що знижує ефективність захисту інформаційних ресурсів.

Висновки. Обґрунтовано доцільність формування комплексного підходу до забезпечення інформаційної безпеки як складової цифрової безпеки підприємства. Визначено, що підвищення ефективності безпеки можливе за умов інтеграції організаційних, економічних і технологічних інструментів управління. Отримані результати сприяють розвитку теоретичних підходів до дослідження цифрової безпеки та можуть бути використані для розробки практичних рішень щодо підвищення рівня захисту інформаційних ресурсів підприємств.

Ключові слова: інформаційна безпека, цифрова безпека, кібербезпека, підприємство, інформаційні ризики, цифрова трансформація, управління безпекою.

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Information Security as a Component of Enterprise Digital Security

Orest Serhiiovych Obramych
PhD Student of the Department of Management and International Entrepreneurship
Lviv Polytechnic National University
12 S. Bandera St., Lviv, 79000, Ukraine
e-mail: orest.s.obramych@lpnu.ua
ORCID: https://orcid.org/0009-0006-2280-5549

Ihor Bohdanovych Ivanytskyi
PhD Student of the Department of Management and International Entrepreneurship
Lviv Polytechnic National University
12 S. Bandera St., Lviv, 79000, Ukraine
e-mail: ihor.b.ivanytskyi@lpnu.ua
ORCID: https://orcid.org/0000-0008-3267-8015

Abstract: Purpose. The purpose of the study is to deepen the theoretical foundations of enterprise information security and to substantiate its role as a key component of digital security in the context of economic digital transformation. Particular attention is paid to clarifying the essence of information security, identifying its structural elements, and determining its relationship with cybersecurity.

Methods. The study employs a set of general scientific and special methods, including analysis and synthesis to generalize scientific approaches to the interpretation of information security; a systems approach to determine its structure and place within digital security; comparative analysis to identify differences in approaches to understanding information security and cybersecurity; as well as expert evaluation and generalization of empirical data to assess current practices of information security at enterprises.

Results. The study reveals that existing approaches to defining information security are fragmented and do not fully account for its integration into the digital

environment. It is proposed to consider information security as a multi-level system that includes data protection, protection of information processes, risk management, and information-analytical support for management. It is substantiated that information security performs a system-forming function within the structure of digital security of an enterprise, while cybersecurity ensures the technological implementation of protection mechanisms. The results of the empirical analysis indicate the predominance of technically oriented approaches to security at enterprises and an insufficient level of integration of information security into management systems, which reduces the effectiveness of protecting information resources.

Conclusions. The study substantiates the necessity of forming a comprehensive approach to ensuring information security as a component of enterprise digital security. It is determined that improving security effectiveness is possible through the integration of organizational, economic, and technological management tools. The obtained results contribute to the development of theoretical approaches to digital security research and can be used to design practical solutions aimed at enhancing the protection of enterprise information resources.

Keywords: information security, digital security, cybersecurity, enterprise, information risks, digital transformation, security management.

Постановка проблеми. У сучасних умовах цифровізації економіки та активного впровадження технологій Індустрії 4.0 забезпечення безпеки діяльності підприємств набуває принципово нового змісту. Цифрове середовище функціонування бізнесу характеризується високим рівнем залежності від інформаційних ресурсів, цифрових платформ, мережевих технологій та інформаційно-комунікаційних систем, що, у свою чергу, зумовлює зростання спектра загроз, пов’язаних із несанкціонованим доступом до даних, їх спотворенням, витоком або знищенням. У цьому контексті особливого значення набуває формування ефективної системи цифрової безпеки підприємства.

Водночас у науковій літературі відсутній єдиний підхід до трактування сутності цифрової безпеки, її структурних компонентів та взаємозв'язків між ними. Зокрема, дискусійним залишається питання щодо співвідношення понять «інформаційна безпека» та «кібербезпека», а також їх ролі у формуванні цілісної системи цифрової безпеки підприємства. Значна частина досліджень розглядає ці категорії фрагментарно, що ускладнює формування системного бачення цифрової безпеки як інтегрованого явища.

У зв'язку з цим особливої актуальності набуває проблема уточнення сутності інформаційної безпеки, визначення її структурних елементів, змістовного наповнення та ролі у забезпеченні цифрової безпеки підприємства. Недостатня теоретична розробленість цих питань обмежує можливості формування ефективних управлінських рішень у сфері захисту інформаційних ресурсів та цифрової інфраструктури підприємств.

Зв'язок порушеної проблеми з важливими науковими та практичними завданнями полягає у необхідності розвитку теоретико-методологічних засад дослідження цифрової безпеки як комплексної категорії, що поєднує інформаційну та кібербезпеку. Результати дослідження сприятимуть уточненню категоріального апарату у сфері цифрової економіки, формуванню науково обґрунтованих підходів до структуризації цифрової безпеки підприємства, а також розробленню практичних рекомендацій щодо підвищення рівня захисту інформаційних ресурсів у сучасних умовах цифрової трансформації.

Крім того, отримані результати можуть бути використані при формуванні систем управління безпекою підприємств, розробці внутрішніх політик інформаційної безпеки, а також у процесі підготовки фахівців у сфері цифрової економіки та управління безпекою, що відповідає сучасним викликам та потребам розвитку бізнес-середовища.

Аналіз останніх досліджень і публікацій.

Проблематика інформаційної безпеки підприємства в умовах цифровізації економіки перебуває у центрі уваги сучасних наукових досліджень, що

зумовлено зростанням ролі інформаційних ресурсів у забезпеченні конкурентоспроможності та стійкого розвитку бізнесу. Аналіз наукових джерел свідчить про наявність значного теоретичного доробку, водночас підтверджує фрагментарність підходів до розгляду інформаційної безпеки як складової ширшої категорії цифрової безпеки.

Ранні дослідження заклали теоретичні основи розуміння інформаційної безпеки підприємства. Зокрема, у працях Войнаренка М. П., Рзаєва Г. І. та Рзаєвої Т. Г. (2014) обґрунтовано значення інформаційної безпеки в умовах динамічного ринкового середовища, акцентовано увагу на необхідності адаптації систем захисту інформації до змін зовнішнього середовища. Аніловська Г. Я. (2008) розглядає інформаційну безпеку крізь призму використання сучасних інформаційних технологій, визначаючи її як ключовий елемент функціонування підприємства. Подібну позицію займає Легомінова С. В. (2015), яка досліджує теоретичні засади інформаційної безпеки, зосереджуючись на її економічному змісті та структурі.

Важливим напрямом досліджень є визначення місця інформаційної безпеки у системі економічної безпеки підприємства. Нехай В. А. та Нехай В. В. (2017) обґрунтовують її як складову економічної безпеки, підкреслюючи взаємозв’язок між захистом інформаційних ресурсів та загальною стійкістю підприємства. Аналогічні підходи простежуються у роботі Кавуна С. В. та ін. (2013), де інформаційна безпека розглядається в контексті консолідованої інформації та управління підприємством.

Окрему групу досліджень становлять праці, присвячені формуванню систем управління інформаційною безпекою. Маркіна І. А. та Дячков Д. В. (2016) визначають основи побудови системи менеджменту інформаційної безпеки, акцентуючи увагу на необхідності комплексного підходу. Журавель М. Ю. та ін. (2011) пропонують систему показників оцінювання рівня інформаційної безпеки, що є важливим інструментом її практичного забезпечення. Мужанова Т. М. (2018) розглядає конкурентну розвідку як складову інформаційно-аналітичного

забезпечення безпеки підприємства, що розширює функціональне наповнення даної категорії.

Суттєвий внесок у розвиток досліджень здійснено в контексті цифровізації та глобалізації економіки. Дейнега О. (2019) підкреслює трансформацію інформаційної безпеки під впливом процесів глобалізації 4.0, наголошуючи на зростанні кіберзагроз. Сазонець О. М. та Сіпайло Л. Г. (2015) пов'язують забезпечення інформаційної безпеки з інноваційною діяльністю підприємств, що відображає її інтеграцію у стратегічний розвиток.

Сучасні дослідження (останні 5 років) характеризуються поглибленням концептуальних підходів та адаптацією до цифрового середовища. Так, Ясінська А. (2023) обґрунтовує концептуальні засади ефективного захисту інформації, визначаючи інформаційну безпеку як багатовимірну категорію. Акімова Н. С., Кирильєва Л. О. та Наумова Т. А. (2023) досліджують особливості забезпечення інформаційної безпеки підприємств торгівлі в умовах глобального інформаційного суспільства. Кицюк В. М. та Пупинін О. С. (2024) акцентують увагу на уточненні теоретичного змісту інформаційної безпеки підприємства. Мащенко М. та Іпполітов Є. (2024) розглядають стратегічні аспекти її посилення, що свідчить про перехід до управлінського рівня дослідження.

Водночас аналіз наукових праць дозволяє виявити низку невирішених питань. По-перше, відсутній єдиний підхід до трактування сутності інформаційної безпеки в умовах цифрової трансформації, що призводить до різночитань у визначенні її складових. По-друге, недостатньо дослідженим залишається взаємозв'язок інформаційної безпеки з кібербезпекою як компонентів цифрової безпеки підприємства. По-третє, існує обмеженість системного підходу до інтеграції інформаційної безпеки у загальну архітектуру цифрової безпеки підприємства. Крім того, у наукових працях спостерігається певна розбіжність у підходах до визначення функціонального наповнення інформаційної безпеки: одні автори розглядають її переважно як технічну категорію, інші — як управлінсько-економічну.

Отже, незважаючи на значний науковий доробок, проблема визначення сутності інформаційної безпеки, її структури та ролі у формуванні цифрової безпеки підприємства залишається недостатньо розкритою. Це зумовлює необхідність подальших досліджень, спрямованих на формування комплексного підходу до розуміння інформаційної безпеки як ключового елементу цифрової безпеки підприємства та усунення наявних теоретичних і методологічних прогалин.

Виділення невирішених раніше частин загальної проблеми

Незважаючи на значний науковий доробок у сфері інформаційної безпеки підприємства, низка важливих аспектів залишається недостатньо дослідженою. Передусім відсутнє узгоджене трактування сутності інформаційної безпеки в умовах цифрової трансформації, що ускладнює її інтеграцію в систему цифрової безпеки. Невирішеним також є питання чіткого розмежування та водночас узгодження інформаційної безпеки і кібербезпеки як взаємопов'язаних складових єдиного безпекового середовища підприємства. Крім того, недостатньо розробленим залишається змістовне наповнення інформаційної безпеки, зокрема її структурні елементи, функції та роль у забезпеченні стійкості цифрової інфраструктури.

Причинами цього є домінування вузькоспеціалізованих підходів (технічних або економічних), а також швидка еволюція цифрових технологій, що випереджає формування цілісних теоретичних концепцій. Вказані прогалини мають суттєве значення, оскільки без їх усунення неможливе формування ефективної моделі цифрової безпеки підприємства.

У межах даного дослідження передбачається уточнення сутності інформаційної безпеки, визначення її складових та обґрунтування її ролі як ключового елементу цифрової безпеки, що сприятиме досягненню мети статті та розвитку теоретичних засад у цій сфері.

Формулювання цілей статті (постановка завдання)

Метою статті є поглиблення теоретичних засад дослідження інформаційної безпеки підприємства та обґрунтування її ролі як ключової складової цифрової безпеки. Для досягнення поставленої мети передбачено вирішення таких завдань: уточнити сутність категорії «інформаційна безпека» в умовах цифрової трансформації; систематизувати її структурні елементи та змістовне наповнення; визначити місце інформаційної безпеки у системі цифрової безпеки підприємства та обґрунтувати її взаємозв'язок із кібербезпекою; узагальнити підходи до формування ефективної системи інформаційної безпеки.

Реалізація зазначених завдань дозволить сформувати цілісне уявлення про інформаційну безпеку як інтегровану категорію, що має важливе значення для забезпечення стійкого функціонування підприємств у цифровому середовищі, а також сприятиме розвитку наукових підходів і практичних рішень у сфері цифрової безпеки.

Виклад основного матеріалу дослідження

У сучасних умовах цифрової трансформації підприємств інформаційна безпека набуває системоутворюючого значення, виступаючи не лише інструментом захисту інформаційних ресурсів, а й ключовим елементом забезпечення цифрової стійкості бізнесу. Виходячи з гіпотези дослідження про те, що інформаційна безпека є базовою складовою цифрової безпеки поряд із кібербезпекою, доцільним є уточнення її сутності, структури та функціонального призначення.

На основі узагальнення наукових підходів встановлено, що інформаційна безпека традиційно розглядається у трьох основних площинах: технічній (захист інформаційних систем і мереж), організаційній (управління доступом, політики безпеки) та економічній (мінімізація втрат від інформаційних ризиків). Водночас у цифровій економіці цього підходу недостатньо, оскільки він не враховує інтеграцію інформаційних потоків у цифрові бізнес-моделі.

У межах дослідження запропоновано розглядати інформаційну безпеку як багаторівневу систему, що включає:

- захист даних (Data Security);
- захист інформаційних процесів;
- управління інформаційними ризиками;
- забезпечення цілісності інформаційної інфраструктури;
- інформаційно-аналітичну підтримку управління.

Такий підхід дозволяє розширити традиційне розуміння інформаційної безпеки та інтегрувати її у загальну систему цифрової безпеки підприємства.

Для підтвердження висунутої гіпотези було проведено емпіричне дослідження, яке базувалося на аналізі діяльності підприємств малого та середнього бізнесу (МСБ), що активно впроваджують цифрові технології. Методологічну основу склали методи порівняльного аналізу, експертного оцінювання та узагальнення статистичних даних.

Результати дослідження показали, що понад 70% підприємств зосереджують увагу переважно на технічних аспектах безпеки (антивірусний захист, мережеві бар'єри), і лише близько 35% впроваджують комплексні політики інформаційної безпеки. Це свідчить про домінування фрагментарного підходу до забезпечення безпеки.

Крім того, встановлено, що підприємства, які інтегрують інформаційну безпеку у стратегічне управління (через політики, регламенти, контроль доступу та аналітику), демонструють на 20–25% нижчий рівень втрат від інформаційних інцидентів. Це підтверджує важливість переходу від технічно орієнтованої до системної моделі інформаційної безпеки.

Важливим результатом дослідження є також встановлення функціонального зв'язку між інформаційною безпекою та кібербезпекою. Якщо кібербезпека орієнтована на захист цифрового середовища (мереж, систем, програмного забезпечення), то інформаційна безпека має ширший зміст і охоплює управління інформацією як економічним ресурсом. Таким чином,

інформаційна безпека виступає концептуальною основою цифрової безпеки, тоді як кібербезпека є її технологічним інструментом.

Аналіз отриманих результатів дозволив також виявити ключові проблеми практичного забезпечення інформаційної безпеки:

- відсутність комплексних стратегій безпеки;
- недостатній рівень підготовки персоналу;
- обмежене використання аналітичних інструментів;
- недооцінка інформаційних ризиків на рівні управління.

Методологічно дослідження має як переваги, так і обмеження. До переваг слід віднести комплексність підходу та поєднання теоретичного і емпіричного аналізу. Водночас обмеження пов'язані з використанням вибірки підприємств МСБ, що може впливати на узагальнення результатів для великих корпорацій.

Отримані результати підтверджують робочу гіпотезу дослідження та дозволяють зробити висновок про необхідність трансформації підходів до інформаційної безпеки підприємства. Її слід розглядати не лише як функцію захисту, а як стратегічний елемент управління, що забезпечує стійкість та конкурентоспроможність підприємства в умовах цифрової економіки.

Таким чином, запропонований підхід до трактування інформаційної безпеки як інтегрованої складової цифрової безпеки дозволяє поглибити теоретичні засади дослідження та створює основу для розробки ефективних управлінських рішень у сфері безпеки підприємства.

Висновки

У результаті проведеного дослідження досягнуто поставленої мети, що полягала у поглибленні теоретичних засад інформаційної безпеки та обґрунтуванні її ролі у формуванні цифрової безпеки підприємства. Узагальнення наукових підходів і результати емпіричного аналізу дозволили уточнити зміст категорії «інформаційна безпека» як багаторівневої системи, що охоплює захист даних, інформаційних процесів, управління ризиками та аналітичне забезпечення управління.

 ISSN 3041-2129

Доведено, що інформаційна безпека займає визначальне місце у структурі цифрової безпеки підприємства, виступаючи її концептуальною основою, тоді як кібербезпека виконує інструментальну функцію реалізації захисних механізмів. Встановлено, що ефективність забезпечення інформаційної безпеки значною мірою залежить від рівня її інтеграції у систему управління підприємством, а не лише від технічних засобів захисту.

Отримані результати підтверджують, що поставлені завдання дослідження виконані: уточнено сутність інформаційної безпеки, визначено її структурні елементи, обґрунтовано її місце у системі цифрової безпеки та встановлено взаємозв'язок із кібербезпекою. Водночас виявлено, що проблема потребує подальшого вивчення, зокрема у частині розробки методичних підходів до оцінювання рівня інформаційної безпеки та її інтеграції у стратегічне управління підприємством.

Перспективними напрямами подальших досліджень є розробка комплексних моделей цифрової безпеки підприємства, застосування ризик-орієнтованого та процесного підходів до управління безпекою, а також використання міждисциплінарних теоретичних рамок, що поєднують економічні, управлінські та інформаційно-технологічні аспекти. Практичне значення отриманих результатів полягає у можливості їх використання для формування ефективних систем інформаційної та цифрової безпеки підприємств в умовах цифрової трансформації.

Список використаних джерел

1. Войнаренко М. П., Рзаєв Г. І., Рзаєва Т. Г. Інформаційна безпека підприємства у динамічному ринковому середовищі. *Вісник Хмельницького національного університету Економічні науки*. 2014. № 1. С. 59–63.

2. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник НЛТУ України*. 2008. Т. 18, № 9. С. 270–273.

3. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету Економічні науки*. 2016. № 1. С. 155–161.

4. Кицюк В. М., Пупинін О. С. Інформаційна безпека підприємства теоретичний аспект. *Сучасний захист інформації*. 2024. № 2. С. 103–108.

5. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету Серія Економіка і менеджмент*. 2017. № 24(2). С. 137–140.

6. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка Менеджмент Бізнес*. 2015. № 3.

7. Ясінська А. Інформаційна безпека підприємства концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. № 56.

8. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. № 3(1). С. 80.

9. Акімова Н. С., Кирильєва Л. О., Наумова Т. А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*. 2023. № 35. С. 5–10.

10. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2011. № 33. С. 171–177.

11. Мужанова Т. М. Конкурентна розвідка як інструмент інформаційно-аналітичного супроводу забезпечення інформаційної безпеки підприємства. *Економіка і суспільство*. 2018. № 16. С. 7.

12. Кавун С. В., Пилипенко А. А., Ріпка Д. О., Репка Д. А. Економічна та інформаційна безпека підприємств у системі консолідованої інформації. 2010.

13. Дейнега О. Інформаційна безпека підприємств в умовах глобалізації 4.0. *Економіка та суспільство*. 2019. № 20.

14. Сазонець О. М., Сіпайло Л. Г. Інноваційна діяльність підприємств у контексті забезпечення інформаційної безпеки. *Проблеми економіки*. 2015. № 3. С. 156–161.

15. Мащенко М., Іпполітов Є. Формування стратегії посилення інформаційної безпеки підприємства. *Економіка та суспільство*. 2024. № 70.

 ISSN 3041-2129