

РОЗВИТОК СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

ТРУШ Ірина

Західноукраїнський національний університет

<https://orcid.org/0000-0003-4821-4449>

e-mail: iratrush22@gmail.com

В статті досліджено особливості розвитку системи економічної безпеки підприємств в умовах цифрової трансформації економіки. Проаналізовано вплив цифровізації, поширення інформаційно-комунікаційних технологій, цифрових платформ, великих даних, автоматизації бізнес-процесів на функціонування суб'єктів господарювання. Розкрито трансформацію підходів до забезпечення економічної безпеки підприємств у середовищі зростання технологічних ризиків, інформаційних витоків, залежності від цифрової інфраструктури та посилення конкуренції. Обґрунтовано необхідність формування комплексної системи економічної безпеки, що інтегрує організаційні, інформаційні, технологічні та управлінські механізми захисту. Визначено роль функціональних стратегій підприємства у протидії цифровим загрозам та окреслено інструменти зміцнення економічної безпеки в межах маркетингової, виробничої, фінансової, інноваційної та кадрової стратегій. Особливу увагу приділено розвитку цифрових компетентностей персоналу як ключового чинника мінімізації цифрових ризиків та підвищення стійкості підприємства.

Ключові слова: економічна безпека підприємства; цифрова трансформація; цифровізація; цифрові компетентності; функціональні стратегії підприємства; цифрова економіка.

<https://doi.org/10.31891/mdes/2026-21-46>



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 30.06.2026

Прийнята до друку / Accepted 20.08.2026

Опубліковано / Published 27.08.2026

© ТРУШ Ірина

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

Сучасний етап розвитку світової та національної економіки характеризується активним впровадженням цифрових технологій, що зумовлює глибокі трансформаційні зміни у функціонуванні суб'єктів господарювання, структурі ринкових відносин та механізмах управління господарською діяльністю. Зауважимо, процеси цифрової трансформації економіки супроводжуються широким використанням інформаційно-комунікаційних технологій, цифрових платформ, великих масивів даних, хмарних сервісів, систем штучного інтелекту та автоматизації бізнес-процесів. В результаті змінюються традиційні моделі ведення бізнесу, посилюється конкуренція, зростає швидкість обробки інформації та прийняття управлінських рішень, а також формуються нові умови функціонування підприємницьких структур.

Слід зазначити, що в умовах цифрової трансформації економічні системи суб'єктів господарювання функціонують у середовищі високої невизначеності, швидких технологічних змін та зростання різноманітних ризиків. Кіберзагрози, інформаційні витокі, залежність від цифрової інфраструктури та постійна необхідність адаптації до нових технологій актуалізують питання формування ефективної системи економічної безпеки підприємства. В цьому контексті особливого значення набуває використання засад стоїчного менеджменту (*Stoic Management*), який ґрунтується на ідеях стоїчної філософії, адже ще в античності було сформовано принципи раціонального управління ризиками, самоконтролю, передбачення загроз та здатності адаптуватися до зовнішніх змін. Як писав Епіктет, «Не події турбують людей, а їхнє ставлення до цих подій», яке в контексті зазначеної теми дослідження можна інтерпретувати як ефективна система економічної безпеки підприємства полягає не лише у реагуванні на цифрові загрози, а у здатності своєчасно їх передбачати, управляти ризиками та адаптуватися до змін цифрового середовища [10]. Нагадаємо, стоїки розглядали управління як процес усвідомленого прийняття рішень у складних обставинах, де ключову роль відіграють розсудливість, стратегічне мислення та здатність відокремлювати керовані процеси від неконтрольованих факторів. Саме ці ідеї сьогодні знаходять відображення у сучасному менеджменті та системах управління ризиками, що лежать в основі забезпечення економічної безпеки підприємств. Умови цифрової економіки вимагають від управлінців здатності прогнозувати загрози, ефективно використовувати інформаційні ресурси та формувати стійкі організаційні системи, здатні протистояти технологічним і економічним викликам. Таким чином, принципи стоїчної філософії можуть розглядатися як методологічна основа сучасного управління

в умовах цифрових трансформацій, оскільки вони акцентують увагу на стратегічній передбачливості, раціональному прийнятті рішень та здатності організації адаптуватися до нестабільного середовища. Це робить їх актуальними для дослідження розвитку системи економічної безпеки підприємства в умовах цифрової економіки.

Цифровізація економічних процесів не лише створює нові можливості для розвитку підприємств, але й супроводжується виникненням додаткових ризиків та загроз, що безпосередньо впливають на рівень їх економічної безпеки. Зокрема, йдеться про витік конфіденційної інформації, порушення безперервності функціонування інформаційних систем, залежність від цифрової інфраструктури, зростання технологічних ризиків та ускладнення управління цифровими активами [4]. В умовах стрімкого розвитку цифрового середовища традиційні підходи до забезпечення економічної безпеки підприємства часто виявляються недостатньо ефективними, оскільки вони здебільшого орієнтовані на реагування на класичні економічні та фінансові загрози і не враховують комплексного впливу цифрових факторів.

В зв'язку з цим особливою актуальністю набуває проблема розвитку системи економічної безпеки підприємства з урахуванням специфіки цифрової трансформації економіки, що передбачає перегляд підходів до ідентифікації загроз, удосконалення інструментарію управління ризиками, інтеграцію інформаційно-аналітичних систем безпеки та формування нових організаційно-управлінських механізмів захисту економічних інтересів суб'єктів господарювання. Вирішення зазначених питань є важливою передумовою підвищення стійкості, адаптивності та конкурентоспроможності підприємств у сучасному цифровому економічному середовищі, що зумовлює наукову та практичну значущість дослідження проблем розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Відмітимо, що в сучасній науковій літературі проблематика формування та розвитку систем економічної безпеки підприємств в умовах цифрової трансформації економіки посідає одне з провідних місць у дослідженнях вітчизняних і зарубіжних науковців. Особлива увага приділяється аналізу змін у функціонуванні підприємств, зумовлених активним розвитком цифрових технологій, зростанням рівня кіберзагроз, посиленням глобальної конкуренції, нестабільністю економічного середовища та необхідністю адаптації бізнес-процесів до нових умов господарювання. В працях науковців ґрунтовно розглядаються сучасні підходи до забезпечення економічної безпеки підприємств, модернізації управлінських механізмів, удосконалення інформаційно-аналітичної підтримки прийняття управлінських рішень, підвищення ефективності використання ресурсів та впровадження цифрових інструментів управління ризиками. Водночас значна увага приділяється формуванню адаптивних і гнучких систем економічної безпеки, здатних забезпечити стійкість підприємств до впливу внутрішніх і зовнішніх загроз у умовах динамічних трансформацій економічного середовища. Зокрема, В. Лугова із колективом авторів дослідила трансформацію економічної безпеки підприємств в цифровій економіці, а також запропонувала інтегроване управління ризиками й рекомендації для підвищення стійкості та конкурентоспроможності підприємств [5], І. Нагорна та Л. Букань довели, що цифрова трансформація створює нові ризики для економічної безпеки підприємств, водночас надаючи можливості для підвищення ефективності та захисту через організаційні, фінансові та правові інструменти, інтегроване управління ризиками та розвиток стійкості і цифрової компетентності персоналу [6], О. Правдивець показав, що впровадження цифрових технологій у діяльність підприємств є ключовим чинником забезпечення економічної стабільності, безпеки та конкурентоспроможності, особливо в кризові періоди, і дозволяє ефективно підтримувати розвиток малих і середніх підприємств [8], О. Халіна та В. Шмагалю обґрунтували доцільність інтеграції сучасних цифрових технологій, інструментів ризик-менеджменту, кібербезпеки й розвитку кадрового потенціалу у систему стратегічного управління економічною безпекою підприємств [9].

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Водночас у сучасних наукових дослідженнях недостатньо систематизованим залишається підхід до розгляду системи економічної безпеки підприємства як комплексної управлінсько-інформаційної архітектури, що формується під впливом процесів цифрової трансформації економіки. Більшість наукових праць зосереджені переважно на окремих аспектах забезпечення економічної безпеки, зокрема на управлінні ризиками, інформаційній або фінансовій безпеці, не

приділяючи достатньої уваги їх комплексній взаємодії в умовах цифровізації бізнес-процесів, посилення невизначеності економічного середовища. В зв'язку з цим актуалізується потреба у поглибленому дослідженні трансформаційних змін у системі економічної безпеки підприємств з позицій інтеграції управлінських, інформаційних та технологічних механізмів, а також обґрунтування напрямів формування адаптивної та стійкої системи економічної безпеки, здатної забезпечити ефективне функціонування підприємств в умовах цифрової трансформації економіки та зростання багатовекторних загроз.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета дослідження полягає в науковому обґрунтуванні особливостей розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки, а також визначенні ролі функціональних стратегій і цифрових компетентностей персоналу у зміцненні стійкості, адаптивності та конкурентоспроможності підприємств.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Умови стрімкого розвитку цифрових технологій та поширення процесів цифровізації зумовлюють функціонування підприємств у середовищі підвищеної невизначеності, що супроводжується появою нових ризиків, кіберзагроз і трансформацією традиційних бізнес-процесів. За таких обставин особливого значення набуває формування ефективних стратегічних та тактичних підходів до забезпечення економічної безпеки підприємств, здатних своєчасно реагувати на внутрішні та зовнішні виклики та забезпечувати їх стійкий розвиток. В зв'язку з цим актуалізується необхідність інтеграції цифрових трансформацій у систему стратегічного та тактичного управління економічною безпекою підприємств. Як зазначає О. Халіна, з огляду на ризики, що виникають унаслідок цифрових змін, а також на внутрішні та зовнішні виклики, необхідно розробити ефективну стратегію, здатну захищати активи підприємства, мінімізувати загрози та забезпечувати його стійкий розвиток. Стратегія розвитку економічної безпеки, яка інтегрує цифрові трансформації, повинна сприяти підвищенню ефективності діяльності підприємства та зміцненню його економічної безпеки в умовах цифрової економіки [9].

Зазначимо, цифровізація суттєво трансформує умови функціонування підприємств, створюючи водночас нові можливості для розвитку та додаткові ризики, пов'язані з кіберзагрозами, інформаційною безпекою і цифровою компетентністю персоналу. В таких умовах забезпечення економічної безпеки підприємств потребує формування ефективних стратегічних підходів, спрямованих на захист цифрових активів, інформаційних систем і корпоративних даних як ключових ресурсів сучасного бізнесу. Погоджуємось із думкою В. Лугової та колективу співавторів, як відзначають, що цифровізація стала ключовою тенденцією сучасної економіки, докорінно змінюючи принципи розвитку підприємств, організації виробництва та створення доданої вартості. Штучний інтелект, великі дані, хмарні сервіси, інтернет речей і блокчейн формують нові правила конкуренції та висувають підвищені вимоги до підприємницьких структур, трансформуючи всі сфери діяльності – від стратегічного планування до операційної роботи та маркетингу. Цифрове середовище відкриває широкі можливості для бізнесу, зокрема доступ до глобальних ринків, персоналізацію послуг, оптимізацію витрат і впровадження інноваційних моделей, однак одночасно породжує нові ризики: кіберзагрози, витоки інформації, технічні помилки та недостатню цифрову компетентність персоналу, що можуть призвести до фінансових втрат і втрати конкурентних переваг. В цих умовах економічна безпека підприємств виходить за межі фінансової стабільності, включаючи захист цифрових активів, інформаційних систем, корпоративних даних та інтелектуальної власності, які стають критично важливими ресурсами для розвитку. Враховуючи динамічність цифрових змін і зростання кіберризиків, дослідження стратегій зміцнення економічної безпеки в умовах цифрової трансформації є надзвичайно актуальним [5? 7].

В сучасних умовах розвитку цифрової економіки вітчизняний бізнес дедалі активніше інтегрує цифрові технології у свою діяльність, що зумовлює трансформацію традиційних бізнес-моделей, управлінських процесів та механізмів забезпечення економічної безпеки, адже процеси цифровізації суттєво змінюють конкурентне середовище, водночас створюючи нові можливості для розвитку та генеруючи додаткові ризики для функціонування суб'єктів господарювання. Як зазначає О. Кравченко та С. Бойко, швидкий розвиток цифрових технологій, поширення цифрових платформ, автоматизація бізнес-процесів та зростання значущості даних суттєво трансформують умови функціонування вітчизняних підприємств. В цифровій економіці формуються нові моделі створення вартості, управління ресурсами та взаємодії між учасниками ринку. Водночас

цифровізація породжує численні загрози економічній безпеці підприємств, зокрема зростання масштабів кібератак, ризики витоку даних, вразливість цифрової інфраструктури, посилені регуляторні вимоги та залежність від автоматизованих систем і технологій штучного інтелекту [3].

Зауважимо, за таких умов суб'єкти господарювання стикаються з безпрецедентними викликами щодо забезпечення економічної безпеки, оскільки цифровізація охоплює всі сфери їхньої діяльності – від маркетингу та виробництва до фінансів, інновацій та управління персоналом [1]. Розширення застосування цифрових технологій, включаючи хмарні сервіси, автоматизацію виробничих процесів та цифрові фінансові платформи, створює нові можливості для підвищення ефективності та конкурентоспроможності підприємств, водночас породжуючи комплексні цифрові загрози, серед яких кіберзлочини, технічні збої, витоки даних, технологічне шпигунство та помилки персоналу. В цьому контексті виникає необхідність системного підходу до управління економічною безпекою підприємств, що передбачає інтеграцію організаційних, фінансових, технологічних і правових інструментів захисту (табл. 1).

Таблиця 1.

Функціональні стратегії підприємства, цифрові загрози та роль цифрових компетентностей працівників у зміцненні економічної безпеки*

Функціональна стратегія	Цифрові загрози	Інструменти покращення / зміцнення економічної безпеки	Цифрові компетентності працівника
Маркетингова стратегія	витік клієнтських даних, цифрове шахрайство, неправомірний доступ до CRM-систем, порушення конфіденційності споживачів	захищені CRM-системи, шифрування даних, контроль доступу, аналітика поведінки клієнтів, навчання персоналу щодо безпечного використання даних	вміння працювати з CRM та аналітичними платформами, навички безпечного оброблення даних, розуміння політик конфіденційності
Виробнича стратегія	технічні збої, кібератаки на виробниче обладнання, порушення безперервності процесів	моніторинг виробничих систем, резервне копіювання, інтеграція кіберзахисту у виробничі процеси, тестування безпеки автоматизованих систем	навички роботи з автоматизованими системами, моніторинг виробничих процесів, розуміння кіберзахисту обладнання
Фінансова стратегія	кібератаки на фінансові системи, цифрове шахрайство, втрати фінансових ресурсів	моніторинг фінансових транзакцій, контроль доступу до фінансових систем, впровадження аналітичних систем для виявлення аномалій	вміння користуватися фінансовими цифровими платформами, аналітичні навички для виявлення аномалій, безпечне управління транзакціями
Інноваційна стратегія	технологічне та інтелектуальне шпигунство, порушення захисту інновацій, втрати конкурентних переваг	патентний захист, контрольований доступ до технологій, захист інтелектуальної власності, аудит безпеки інноваційних рішень	вміння працювати з інноваційними технологіями, знання стандартів захисту інтелектуальної власності, навички оцінки ризиків нових рішень
Кадрова стратегія	людські помилки, низька цифрова компетентність, ризики соціотехнічних атак (фішинг, інженерні атаки)	навчання персоналу, регулярні тренінги з кібербезпеки, розвиток цифрових компетенцій, формування культури безпеки	навички цифрової грамотності, управління HR-платформами, знання методів захисту від фішингу та соціотехнічних атак
Стратегія економічної безпеки	внутрішні та зовнішні загрози для стабільності бізнесу, цифрові атаки, витоки інформації	інтегроване управління ризиками, стандарти інформаційної безпеки, технологічні та організаційні інструменти захисту, підвищення адаптивності та стійкості підприємства	цифрова грамотність на всіх рівнях, здатність до роботи з системами управління ризиками та інформаційною безпекою, навички реагування на кіберзагрози

* побудовано автором

Слід зауважити, що цифрові загрози мають комплексний та багатовимірний характер і впливають на всі функціональні стратегії підприємства, починаючи від маркетингу та виробництва і закінчуючи фінансами, інноваціями, кадрами та економічною безпекою. Для маркетингової стратегії найбільші ризики пов'язані з витоком клієнтських даних та цифровим шахрайством, тоді як виробнича стратегія вразлива до технічних збоїв і кібератак на обладнання. Фінансова та інноваційна стратегії схильні до цифрових шахрайств, втрат фінансових ресурсів та інтелектуального шпигунства, що може підривати конкурентні переваги. Кадрова стратегія виділяється особливою роллю людського фактору: низька цифрова компетентність і соціотехнічні загрози підвищують ризики для підприємства. Стратегія економічної безпеки об'єднує всі

внутрішні та зовнішні загрози, включаючи цифрові атаки та витоки інформації, вимагаючи інтегрованого підходу до управління ризиками та підвищення стійкості організації. Водночас, ефективне зміцнення економічної безпеки можливе через поєднання технологічних, організаційних та правових інструментів захисту та розвиток цифрових компетентностей працівників, які забезпечують безпечне використання цифрових платформ, правильне управління інформацією та своєчасне реагування на кіберзагрози. Таким чином, цифрові компетентності персоналу виступають критичною ланкою у підвищенні стійкості та адаптивності підприємства, а інтеграція їх у всі функціональні стратегії дозволяє мінімізувати ризики та зміцнити економічну безпеку в умовах цифрової трансформації [2, 3].

За таких умов особливої актуальності набуває дослідження ролі цифрових компетентностей персоналу у забезпеченні економічної безпеки підприємства, оскільки сучасні організації дедалі більше залежать від цифрової інфраструктури, інформаційних систем та даних, що підвищує їхню вразливість до технічних збоїв і помилок у використанні цифрових інструментів. У зв'язку з цим рівень цифрових компетентностей працівників стає одним із ключових чинників ефективного функціонування системи економічної безпеки. На нашу думку, дослідження різних видів цифрових компетентностей персоналу дозволяє визначити їхню роль у мінімізації цифрових ризиків, підвищенні ефективності управління інформаційними ресурсами та формуванні здатності підприємства адаптуватися до швидких технологічних змін. В цьому контексті особливого значення набуває використання ідей стоїчної філософії, які акцентують увагу на раціональному мисленні, передбаченні ризиків, самоконтролі та здатності ефективно діяти в умовах невизначеності. Як зазначав Марк Аврелій: «Ти маєш владу над своїм розумом, а не над зовнішніми подіями. Усвідом це, і знайдеш силу» [10, 11]. Отже, принципи стоїцизму, що сформувалися у працях античних мислителів, сьогодні знаходять відображення у сучасних підходах до управління та формують концепцію так званого стоїчного менеджменту, спрямованого на розвиток стійкості організації, відповідальності за прийняття рішень та здатності адаптуватися до складних зовнішніх умов. Застосування таких підходів у поєднанні з розвитком інформаційно-аналітичних, технологічних, комунікаційних, кібербезпекових та стратегічних цифрових компетентностей сприяє не лише оптимізації бізнес-процесів, а й формуванню стійкої системи управління ризиками та зміцненню економічної безпеки підприємства (рис. 1).

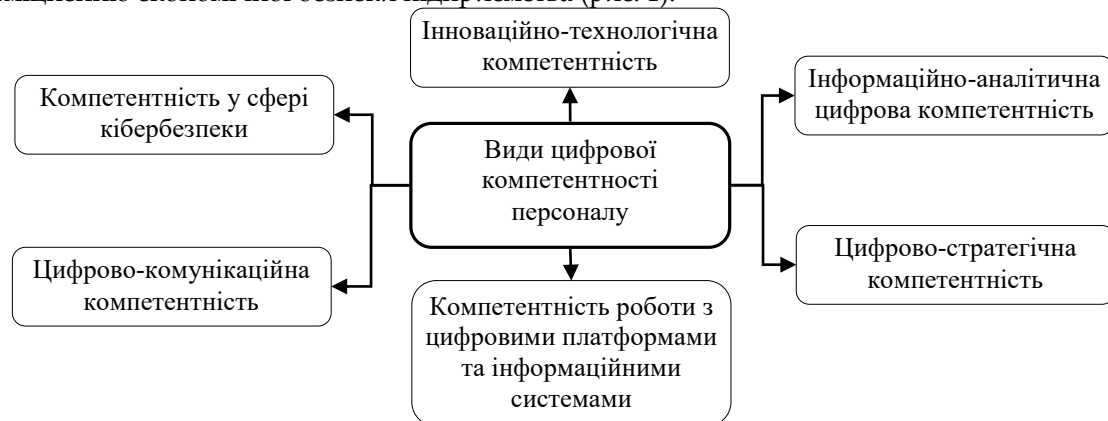


Рис. 1. Види цифрової компетентності персоналу

Джерело: побудовано автором

Узагальнення цифрових компетентностей персоналу в контексті економічної безпеки підприємства є важливим науковим і практичним завданням, оскільки дозволяє сформувати ефективні підходи до управління цифровими ризиками, підвищити адаптивність організації та забезпечити її стабільний розвиток в умовах цифрової трансформації економіки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Цифрова трансформація підприємства формує комплекс нових загроз для всіх функціональних стратегій, зокрема маркетингової, виробничої, фінансової, інноваційної, кадрової, інвестиційної та інформаційного забезпечення, які проявляються у витоку даних, кібератаках, технічних збоях, порушенні безперервності процесів, технологічному та інтелектуальному шпигунстві, а також у низькому рівні цифрової компетентності працівників та соціотехнічних ризиках. Зміцнення економічної безпеки досягається через впровадження комплексних

інструментів захисту, таких як кіберзахист, шифрування даних, контроль доступу, моніторинг систем, резервне копіювання, аудит безпеки, патентний захист, інтегроване управління ризиками та дотримання стандартів інформаційної безпеки. При цьому розвиток цифрових компетентностей працівників є критичною складовою, що дозволяє ефективно використовувати цифрові платформи, безпечно обробляти дані, управляти ризиками та запобігати кіберзагрозам на всіх рівнях організації. Інтеграція цифрових навичок у всі функціональні стратегії забезпечує підвищення стійкості, адаптивності та конкурентоспроможності підприємства в умовах сучасної цифрової економіки.

ЛІТЕРАТУРА:

1. Васильців Т. Г., Лупак Р. Л., Куницька-Іляш М. В., Наконечна Н. В. Економічна безпека суб'єктів господарювання та держави: аспект гарантування фінансово-економічної безпеки пріоритетних галузей національної економіки України. *Наукові записки Львівського університету бізнесу та права*. 2023. № 37. С. 22–30.
2. Кравченко О. О., Бойко С. О. Економічна безпека підприємства в умовах цифрової економіки: теоретичні засади та сучасні виклики. *Науковий вісник Національного транспортного університету*. 2026. № 1(55). С. 584–597.
3. Кравченко О., Гаврилюк О., Челомбітько О., Бойко С. Управління економічною безпекою підприємств в умовах цифрової економіки. *Адаптивне управління: теорія і практика. Серія Економіка*, 2024, 19 (38). URL: <https://amtp.org.ua/index.php/journal2/article/view/690>
4. Мельник С. І., Штангрет І. А. М Економічна безпека підприємства в умовах цифрової трансформації економіки: теоретичні та практичні аспекти : *монографія*. Львів : Растр-7, 2025. 256 с.
5. Лугова В. М., Кравчик Ю. В., Пушак Я. Я., Літвінов Д. О., Печка С. С. Економічна безпека підприємств в умовах цифрової економіки. *Всеукраїнський науковий журнал «Актуальні проблеми інноваційної економіки та права»*, 2025, № 4 С. 99-103.
6. Нагорна І. І., Букань Л. В. Економічна безпека підприємства в умовах цифрової трансформації: виклики та інструменти захисту. *Механізми забезпечення сталого розвитку економіки: проблеми, перспективи, міжнародний досвід: матеріали VI Міжнар. науково-практ. конференції*, 10 жовтня 2025 р. Харків: ДБТУ, 2025. С. 463-466.
7. Пілецька С. Т., Ареф'єв С. О., Петровська С. В., Колесников С. О. Стратегічне забезпечення економічної безпеки підприємств в контексті цифровізації економіки України. *Проблеми економіки*. 2024. № 2 (60), С. 181–190.
8. Правдивець О. М. Цифровізація як основа економічної стабільності та безпеки підприємницької діяльності. *Регіональна економіка*. 2022. № 4 (106). С. 81-86.
9. Халіна О., Шмагалю В. Стратегія розвитку економічної безпеки підприємств в умовах цифрових трансформацій. *Економіка та суспільство*, 2025, № 73, <https://economyandsociety.in.ua/index.php/journal/article/view/5936/5875>
10. Stead J., Sellars J. The Stoic Leader: Ancient Lessons to Succeed in Business. London: Michael O'Mara Books Ltd, 2025. 256 p.
11. Vasylytsiv T., Irtysheva I., Lupak R., Popadynets N., Shyshkova Y., Boiko Y., Ishchenko O. Economy's Innovative Technological Competitiveness: Decomposition, Methodics of Analysis and Priorities of Public Policy. *Management Science Letters*. 2020. № 10(13). Pp. 3173-3182.

REFERENCES:

1. Vasylytsiv T. H., Lupak R. L., Kuniyska-Iliash M. V., Nakonechna N. V. (2023) Ekonomichna bezpeka subiektiv hospodariuvannia ta derzhavy: aspekt harantuvannia finansovo-ekonomichnoi bezpeky priorytetnykh haluzei natsionalnoi ekonomiky Ukrainy. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava*. № 37. P. 22–30.
2. Kravchenko O. O., Boiko S. O. (2026) Ekonomichna bezpeka pidpriemstva v umovakh tsyfrovoy ekonomiky: teoretychni zasady ta suchasni vyklyky. *Naukovyi visnyk Natsionalnoho transportnoho universytetu*. № 1(55). P. 584–597.
3. Kravchenko O., Havryliuk O., Chelombitko O., Boiko S. (2024) Upravlinnia ekonomichnoiu bezpekoiu pidpriemstv v umovakh tsyfrovoy ekonomiky. *Adaptyvne upravlinnia: teoriia i praktyka. Seriya Ekonomika*, 19 (38). URL: <https://amtp.org.ua/index.php/journal2/article/view/690>.
4. Melnyk S. I., Shtanhret I. A. M (2025) Ekonomichna bezpeka pidpriemstva v umovakh tsyfrovoy transformatsii ekonomiky: teoretychni ta praktychni aspekty : *monohrafiia*. Lviv : Rastr-7., 256 p.
5. Luhova V. M., Kravchik Yu. V., Pushak Ya. Ya., Litvinov D. O., Piechka S. S. (2025) Ekonomichna bezpeka pidpriemstv v umovakh tsyfrovoy ekonomiky. *Vseukrainskyi naukovi zhurnal «Aktualni problemy innovatsiinoi ekonomiky ta prava»*, № 4 P. 99-103.
6. Nahorna I. I., Bukan L. V. (2025) Ekonomichna bezpeka pidpriemstva v umovakh tsyfrovoy transformatsii: vyklyky ta instrumenty zakhystu. *Mekhanizmy zabezpechennia staloho rozvytku ekonomiky: problemy, perspektivy, mizhnarodnyi dosvid: materialy VI Mizhnar. naukovo-prakt. konferentsii*, 10 zhovtnia 2025 r. Kharkiv: DBTU. P. 463–466.

7. Piletska S. T., Arefiev S. O., Petrovska S. V., Kolesnykov S. O. (2024) Stratehichne zabezpechennia ekonomichnoi bezpeky pidpriemstv v konteksti tsyfrovizatsii ekonomiky Ukrainy. *Problemy ekonomiky*. № 2 (60), S. 181–190.
8. Pravdyvets O. M. (2022) Tsyfrovizatsiia yak osnova ekonomichnoi stabilnosti ta bezpeky pidpriemnytskoi diialnosti. *Rehionalna ekonomika*, № 4 (106). P. 81–86.
9. Khalina O., Shmahalo V. (2025) Stratehiia rozvytku ekonomichnoi bezpeky pidpriemstv v umovakh tsyfrovyykh transformatsii. *Ekonomika ta suspilstvo*, , № 73, <https://economyandsociety.in.ua/index.php/journal/article/view/5936/5875>
10. Stead J., Sellars J. The Stoic Leader: Ancient Lessons to Succeed in Business. London: Michael O'Mara Books Ltd, 2025. 256 p.
11. Vasylytsiv T., Irtysheva I., Lupak R., Popadynets N., Shyshkova Y., Boiko Y., Ishchenko O. Economy's Innovative Technological Competitiveness: Decomposition, Methodics of Analysis and Priorities of Public Policy. *Management Science Letters*. 2020. № 10(13). Pp. 3173–3182.

DEVELOPMENT OF ENTERPRISE ECONOMIC SECURITY SYSTEM IN THE CONTEXT OF DIGITAL TRANSFORMATION OF THE ECONOMY

TRUSH Iryna
West Ukrainian National University

The article examines the development of the enterprise economic security system in the context of the digital transformation of the economy. The rapid spread of digital technologies, information and communication systems, digital platforms, big data, artificial intelligence, and the automation of business processes significantly transforms the conditions of enterprise functioning and creates new challenges for ensuring economic security. The study analyzes the impact of digitalization on business activities and highlights the emergence of new risks and threats, including cyberattacks, data leaks, technological failures, and the growing dependence of enterprises on digital infrastructure and information systems.

Particular attention is paid to the transformation of traditional approaches to economic security management under conditions of increased uncertainty and the dynamic development of the digital environment. The article substantiates the necessity of forming an integrated system of enterprise economic security that combines organizational, technological, informational, and managerial mechanisms aimed at protecting corporate resources, information assets, and business processes. The role of functional strategies of the enterprise in counteracting digital threats is also determined. In particular, the influence of marketing, production, financial, innovation, and personnel strategies on the formation of a comprehensive system of economic security is analyzed.

Special emphasis is placed on the importance of developing employees' digital competencies as a key factor in minimizing digital risks and ensuring the safe use of digital tools and platforms. The study also highlights the relevance of applying the principles of stoic management, which emphasize rational decision-making, risk anticipation, self-control, and the ability of organizations to adapt to a rapidly changing environment. The integration of these approaches contributes to strengthening the resilience, adaptability, and competitiveness of enterprises in the digital economy and ensures the effective functioning of economic security systems in the face of modern technological and economic challenges.

Keywords: enterprise economic security; digital transformation; digitalization; digital competencies; functional strategies of the enterprise; digital economy.