

ЛУГОВА Вікторія Миколаївна, к.е.н., доцент, доцент кафедри соціальної економіки, Харківський національний економічний університет імені Семена Кузнеця, <https://orcid.org/0000-0001-9584-2259>
 КРАВЧИК Юрій Васильович, к.е.н., доцент, доцент кафедри менеджменту та адміністрування, Хмельницький національний університет, <https://orcid.org/0000-0002-2780-5605>
 ПУШАК Ярослав Ярославович, д.е.н., професор, професор кафедри соціально-поведінкових, гуманітарних наук та економічної безпеки, Львівський державний університет внутрішніх справ, <https://orcid.org/0000-0003-1369-8770>
 ЛІТВІНОВ Дмитро Олександрович, PhD, кафедра торговельного підприємництва, товарознавства та управління бізнесом, Одеський національний технологічний університет, <https://orcid.org/0000-0001-8612-3834>
 ПЕЧКА Сергій Сергійович, PhD, викладач кафедри торговельного підприємництва, товарознавства та управління бізнесом, Одеський національний технологічний університет, <https://orcid.org/0000-0003-2688-2729>

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Лугова В. М., Кравчик Ю. В., Пушак Я. Я., Літвінов Д. О., Печка С. С. Економічна безпека підприємств в умовах цифрової економіки.

У статті досліджено сучасні підходи до забезпечення економічної безпеки підприємств в умовах цифрової економіки, де ключову роль відіграють цифрові технології, інформаційні ресурси та кіберзахист. Обґрунтовано, що цифровізація трансформувує усі сфери діяльності підприємства – від стратегічного управління та операційних процесів до управління даними й кадрової політики, водночас формує новий спектр ризиків, зокрема кіберінциденти, витоки інформації, технічні збої, інноваційні та інституційні загрози. На основі аналізу наукових праць визначено основні теоретичні підходи до економічної безпеки: ресурсний, функціональний, ризик-орієнтований, інституційно-правовий та соціотехнічний, що відображають багатовимірність сучасної безпеки підприємства. Показано, що цифрові активи – дані, хмарні сервіси, алгоритми, прозорі забезпечення та IT-інфраструктура – стають ключовими ресурсами, від рівня захищеності яких безпосередньо залежить економічна стійкість і конкурентоспроможність компанії. Значну увагу приділено ролі цифрової компетентності персоналу як критичного чинника зниження ймовірності кіберінцидентів, оскільки більшість порушень безпеки спричинені людськими помилками та недостатнім рівнем навичок роботи з технологіями. Розкрито важливість технологічних інструментів кіберзахисту, ефективного управління даними, впровадження стандартів інформаційної безпеки та інтегрованого управління ризиками, які взаємодіють із стратегіями організаційної стійкості. Сформульовано комплекс рекомендацій щодо підвищення економічної безпеки підприємств, включно з розвитком цифрових навичок персоналу, модернізацією IT-інфраструктури, вдосконаленням політик безпеки, регулярними аудитими й тестуванням систем, а також посиленням інституційної відповідності національним і міжнародним стандартам. Окреслено перспективи подальших досліджень, що полягають у формуванні інтелектуальних моделей оцінювання цифрових ризиків на основі штучного інтелекту, розвитку методик вимірювання цифрової компетентності співробітників, а також вивченні впливу новітніх технологій – блокчейн, квантові обчислення, автономні системи – на економічну стійкість і конкурентоспроможність підприємств у цифровому середовищі.

Ключові слова: економічна безпека підприємства, ризики, загрози, інноваційний розвиток, цифрова економіка, цифрова трансформація, інформаційна безпека, цифрова компетентність, системний підхід.

Постановка проблеми у загальному вигляді.

Цифровізація перетворилася на одну з провідних тенденцій сучасної світової економіки, докорінно змінюючи уявлення про розвиток підприємств, принципи організації виробництва та способи створення доданої вартості. Стрімке впровадження цифрових технологій – штучного інтелекту, великих даних, хмарних сервісів, інтернету речей, блокчейну – формує нові правила конкуренції та висуває нові вимоги до підприємницьких структур. Поступовий, а подекуди й різкий, перехід від традиційних економічних механізмів до цифрово керування процесів спричиняє фундаментальну трансформацію усіх сфер діяльності підприємства: від стратегічного планування до операційної діяльності, від маркетингових інструментів до логістичних моделей.

Цифрове середовище створює безпрецедентні можливості для бізнесу. Підприємства отримують доступ до глобальних ринків, можуть реалізовувати персоналізовані підходи до клієнтів, значно підвищувати швидкість обробки інформації, оптимізувати витрати та запроваджувати інноваційні бізнес-моделі. Дані перетворюються на ключовий виробничий ресурс, а автоматизація та аналітика стають фундаментальними елементами конкурентоспроможності. Проте разом із новими перспективами цифровізація формує спектр інноваційних ризиків, які принципово відрізняються від загроз, які притаманні попереднім економічним етапам.

У цифрову епоху підприємства стають залежними від інформаційних систем, технологічної інфраструктури та цифрових активів, що є надзвичайно вразливими до зовнішніх і внутрішніх дестабілізуючих чинників. Збої в роботі програмного забезпечення, кібератаки, витоки інформації, технічні помилки персоналу, недостатній рівень цифрових компетенцій працівників або невдала цифрова трансформація можуть спричинити масштабні економічні наслідки – від порушення операційних процесів до втрати конкурентних переваг та значних фінансових збитків.

У цьому контексті економічна безпека підприємств набуває якісно нового змісту. Її межі перестають обмежуватися виключно питаннями фінансової

стабільності або матеріальних ресурсів. Сучасні підприємства мають забезпечувати захист цифрових активів, інформаційних систем, корпоративних даних, програмного забезпечення, інтелектуальної власності, мережевої інфраструктури. Ці активи не мають фізичної форми, проте часто визначають основу вартості бізнесу та є ключовими драйверами розвитку в умовах цифрової економіки. Невміння їх захистити перетворюється на одну з найбільших загроз економічній стабільності та довгостроковому розвитку підприємств.

З огляду на динамічність цифрових змін, зростання складності технологічних систем і посилення кіберзагроз дослідження економічної безпеки підприємств в умовах цифрової економіки є вкрай актуальним. Саме тому стаття спрямована на аналіз сучасних викликів, ризиків та стратегічних напрямів забезпечення економічної безпеки в епоху цифрових трансформацій.

Аналіз останніх досліджень і публікацій. Аналіз наукових статей, опублікованих за останні 5 років у журналах, що індексуються у Scopus, свідчить, що дослідження економічної безпеки підприємств у цифровій економіці зосереджуються навколо кількох ключових тенденцій. Передусім простежується посилення уваги до ролі кібербезпеки як критичного економічного фактору, що визначає стійкість підприємств, їхню здатність зберігати безперервність діяльності та мінімізувати втрати від цифрових інцидентів. Водночас зростає значення управління даними (data governance), оскільки дані стають основним стратегічним ресурсом. Сучасні дослідження акцентують на потребі інтегрованих підходів, що поєднують технічні, економічні й організаційні інструменти управління ризиками. Крім того, активно розвиваються методи кількісної оцінки економічної безпеки, що враховують цифрові загрози, а також зростає інтерес до взаємозв'язку між цифровою трансформацією, інноваційністю та високоякісним розвитком підприємств.

Так, Арройабе М. Ф. зі співавторами досліджують економічний зміст кібербезпеки в діяльності малих і середніх підприємств, доводячи, що інвестиції в

безпеку слід розглядати як форму економічного блага, яка забезпечує підвищення продуктивності й зниження довгострокових ризиків [1]. Тянь Z., Хан M., Цзян С. аналізують стратегії управління безпекою даних на цифрових платформах та пропонують модель оптимізації співвідношення між витратами на безпеку та економічною вигодою від збереження даних, що є важливим для формування корпоративної політики data governance [2]. Аналогічно, у роботі Сан Л., Чжан Х., Фан Ч систематизовано глобальні практики управління безпекою даних і запропоновано набір технічних і регуляторних рішень, спрямованих на зниження економічних збитків від витоків даних [3].

Чен З. та Сінг Р. доводять, що цифровізація сприяє економічній стійкості та високоякісному розвитку підприємств, зокрема через інновації та оптимізацію бізнес-процесів [4]. Дослідження Фотіс Ф. показують, що витрати на кібербезпеку та ІТ-інвестиції слід розглядати не як суто адміністративний тягар, а як економічно обґрунтовані інвестиції, що знижують довгострокові операційні ризики і вартісні втрати від інцидентів [5].

Практичні аспекти кількісної оцінки економічної безпеки розглядають у своїй роботі Самоїленко Ю. та ін. Автори систематизували компоненти економічної безпеки в умовах цифрової трансформації та запропонували показники оцінки рівня цифрової безпеки підприємств у контексті цифровізації [6]. Пілецька С. Т., Ареф'єв С. О., Петровська С. В. та Колесников С. О. здійснили комплексний аналіз впливу цифровізації на економічну безпеку підприємств в Україні. Автори обґрунтували актуальність оцінки рівня цифрової трансформації та її впливу на економічну безпеку на регіональному, національному та глобальному рівнях [7]. Іванов М. та ін. доводять, що впровадження цифрових технологій трансформуює структуру стратегічних ризиків підприємства та вимагає нових методів управління ними [8].

Узагальнюючи проаналізовані джерела, можна стверджувати, що сучасна наукова думка сходиться на розумінні економічної безпеки підприємства як динамічної системи протидії ризикам, яка охоплює як традиційні економічні загрози, так і нові виклики цифрової трансформації. В рамках цієї системи поєднуються механізми стратегічного управління, адаптації, моніторингу та превентивного реагування на кіберризики, втрату цифрових активів, порушення інформаційної безпеки та невизначеність у регуляторному полі. Серед ключових напрямків наукових пошуків – оцінка впливу цифровізації на економічну стабільність, розробка індикаторів цифрової безпеки, а також формування комплексних стратегій управління ризиками. Водночас сучасні дослідження демонструють, що цифрові загрози створюють новий спектр проблем для підприємств, які потребують подальшого вивчення: ризики кіберінцидентів, витоків інформації, порушення цілісності даних, неузгодженості цифрових процесів та недостатньої цифрової компетентності персоналу. Їх систематизація та вироблення ефективних механізмів управління ними є ключовим напрямом подальших наукових пошуків і практичних рішень у сфері забезпечення економічної безпеки підприємств у цифровій економіці.

Формулювання цілей статті (постановка завдання). Метою статті є комплексна ідентифікація ключових ризиків функціонування системи економічної безпеки підприємства в умовах цифрової трансформації, визначення їхньої природи, взаємозв'язків і впливу на ефективність господарської діяльності.

Для досягнення поставленої мети передбачено виконання таких завдань:

- проаналізувати основні теоретичні підходи до визначення сутності та структури економічної безпеки підприємства в умовах цифрової економіки;
- систематизувати основні цифрові загрози для підприємств;

– визначити роль цифрових компетенцій персоналу та керівництва у забезпеченні економічної безпеки підприємства;

– розробити практичні рекомендації щодо підвищення економічної безпеки підприємств у цифровій економіці.

Методологія і методи. Для досягнення поставленої мети використано комплекс загальнонаукових і спеціальних методів дослідження: метод теоретичного узагальнення – для визначення сутності економічної безпеки підприємств у цифровій економіці, виділення ключових компонентів і підходів, а також формування цілісного уявлення про сучасні виклики та цифрові ризики; методи аналізу та синтезу – для дослідження наукових публікацій, звітів і статистичних даних з метою виявлення тенденцій цифровізації, кіберзагроз та впливу цифрових компетенцій на економічну безпеку; методи систематизації – для класифікації підходів до економічної безпеки, цифрових загроз, складових цифрової компетентності персоналу та стратегічних рекомендацій щодо управління ризиками; метод узагальнення – для формування комплексних висновків та практичних рекомендацій щодо підвищення економічної безпеки підприємств в умовах цифрової економіки.

Виклад основного матеріалу дослідження. Поняття економічної безпеки зазнало значної еволюції: від вузького розуміння як забезпечення фінансової стабільності до сучасного багатовимірного й міждисциплінарного підходу, що охоплює цифрові, інституційні, людські та кібернетичні аспекти. Сучасні автори підкреслюють, що в епоху цифрової трансформації економічна безпека підприємства – це складна система, яка має одночасно реагувати на старі традиційні загрози та на нові цифрові виклики.

Аналіз наукових праць дозволяє виділити такі підходи до розуміння поняття «економічна безпека» в умовах цифрової економіки: ресурсний підхід, функціональний підхід, ризик-орієнтований підхід, інституційно-правовий підхід, соціотехнічний підхід.

У межах ресурсного підходу економічна безпека розглядається як здатність підприємства акумулювати, зберігати та ефективно використовувати свої ресурси. Для сучасних підприємств важливим ресурсом стають не лише фінанси та матеріальні засоби, а й цифрові активи – дані, хмарні платформи, алгоритми й ІТ інфраструктура. Так, у роботі «Трансформація системи фінансово-економічної безпеки підприємства в умовах цифрової економіки» Шкарлет С. М. та Садчикова І. В. підкреслюють, що інформація, яка зберігається на електронних носіях, є найбільш вразливою частиною ресурсної бази сучасних компаній, і її захист повинен стати пріоритетом [9].

Функціональний підхід розглядає економічну безпеку через призму стабільного функціонування ключових бізнес функцій: фінансів, виробництва, логістики та маркетингу. У контексті цифрової економіки ці функції дедалі більше залежать від цифрових інфраструктур, аналітичних систем та ІТ рішень. Зокрема, у статті Кульчицького І. І. «Цифрова економіка та економічна безпека підприємства: стратегії управління» підкреслюється, що цифровізація створює як нові можливості (автоматизація, аналітика), так і системні загрози, які мають бути враховані у стратегічному управлінні [10].

Ризик-орієнтований підхід є провідною парадигмою в сучасних дослідженнях. У середовищі цифрової трансформації підприємства стикаються з новими уразливостями: кібератаки, витокі даних, технологічні збої, атаки на хмарні системи. Наприклад, Муравський С. та Толпежніков Р. аналізують, як цифрові ініціативи підвищують загрози кібербезпеці, водночас вимагаючи стратегічної узгодженості між цифровими процесами та бізнес-цілями [11].

Інституційно-правовий підхід акцентує увагу на ролі інститутів – законодавчих, нормативних, організаційних – у забезпеченні безпечного цифрового середовища. Воронюк Є. В. та Чепелюк М. І. у своїй праці «Інституційний підхід до формування економічної безпеки підприємницької діяльності» описують, що економічна безпека підприємств формується під впливом системи правил, норм і структур, які забезпечують стабільне функціонування бізнесу й мінімізацію ризиків, у тому числі цифрових [12]. Крім того, цифрова економіка часто потребує адаптації нормативної бази, щоб відповісти на нові загрози, пов'язані з інформаційною безпекою, захистом персональних даних та кібератаками.

Соціотехнічний підхід враховує людський фактор, організаційну культуру, компетенції співробітників і готовність персоналу до цифрової трансформації. У контексті економічної безпеки це означає, що навіть

коли є технічні рішення, без належного рівня цифрових навичок, кібергігієни та внутрішньої культури безпеки підприємство залишається вразливим. В огляді підходів забезпечення безпеки ІТ сектору, Блинков В. доводить, що ключову роль відіграє організаційна компетентність та знання, здатність працівників усвідомлювати та реагувати на цифрові загрози [13].

Серед ключових загроз, які сьогодні вважаються найбільш небезпечними для економічної безпеки підприємств у цифрову еру, можна виділити такі (табл. 1).

У сучасних умовах цифрової економіки цифрова компетентність персоналу та керівництва підприємства стає критичним чинником забезпечення його економічної безпеки. Вона визначає здатність організації адаптуватися до цифрових змін, ефективно використовувати технології, протидіяти кіберзагрозам і забезпечувати стійкість бізнес-процесів.

Таблиця 1

Класифікація цифрових загроз для економічної безпеки підприємств

Тип загрози	Характеристика	Потенційні наслідки
Кібернапади	Віруси, ransomware, фішинг, DDoS	Втрата даних, фінансові збитки, простой систем
Збої інфраструктури	Відмова хмар, перевантаження серверів	Переривання роботи бізнес-процесів, недоступність даних
Людський фактор	Низька цифрова грамотність, помилки користувачів	Неавторизований доступ, витоки інформації, внутрішні інциденти
Неправильне використання технологій	Помилки при впровадженні ІТ, неправильна конфігурація	Зниження продуктивності, зростання витрат, технічні збої
Маніпуляції з даними	Несанкціоновані зміни, підтасовки, шпайдерство	Викривлення звітності, прийняття неправильних рішень
Інноваційні ризики	Неузгодженість цифрових інновацій, невдалі проєкти	Втрата конкурентоспроможності, невиконані інвестиції

Джерело: узагальнено за [7; 9-11; 14].

Згідно з поглядами Вуорікарі Р. та ін. цифрова компетентність включає такі компоненти: інформаційна грамотність (вміння працювати з даними), комунікація та взаємодія в цифровому середовищі, створення цифрового контенту, безпека в цифровому середовищі, вирішення проблем з використанням цифрових технологій [15].

В економічній площині це означає, що працівники не лише вміють користуватися ІТ-інструментами,

а й усвідомлюють ризики, які пов'язані з цифровою діяльністю, і здатні мінімізувати їх вплив (табл. 2).

Дослідження ENISA (European Union Agency for Cybersecurity) [16] та IBM Security [17] показують, що понад 80% інцидентів у кібербезпеці виникають через людські помилки, зокрема: некоректне поводження з пароллями, фішинг, несвоєчасне оновлення ПЗ, використання незахищених хмарних сервісів.

Таблиця 2

Структура цифрової компетентності працівника в умовах цифрової економіки

Компонент	Характеристика
Цифрова грамотність	Безпечне використання цифрових інструментів та сервісів, базове розуміння ризику
Кібергігієна	Усвідомлення й практики запобігання типовим кіберзагрозам: фішинг, слабкі паролі, оновлення ПЗ
Управління даними	Розуміння принципів обробки даних, важливість їх цілісності, конфіденційності та доступності
Технологічна адаптивність	Здатність швидко освоювати нові цифрові рішення, впроваджувати інновації, адаптуватися до змін середовища
Аналітичні навички	Використання цифрової аналітики, інструментів BI, прогнозування, аналіз даних для прийняття обґрунтованих рішень

Джерело: сформовано автором.

Таким чином, високий рівень цифрової компетентності персоналу безпосередньо впливає на зниження ймовірності економічних збитків від кібератак. За висновками Вестермана Дж., Бонне Д., МакАфі Е., компанії з "digital masters" досягають на 26% вищої прибутковості, мають більш стійкі бізнес-моделі, краще реагують на зовнішні шоки. Це пов'язано з тим, що цифрово компетентне керівництво обирає безпечні ІТ-рішення, впроваджує політику кібербезпеки, проводить внутрішні аудити цифрових ризиків, оцінює вартість потенційних кіберінцидентів [18].

Згідно з дослідженням Міністерства цифрової трансформації, 93% дорослих (18–70 років) мають хоча б базовий рівень цифрових навичок. Частка тих, хто не має жодних цифрових навичок, складає 7,2%. У 2025 році Мінцифра повідомляє, що 96% українців володіють цифровими навичками, а 58% – на базовому або вищому рівні. Також із повідомлення Мінцифри: за шість років (з 2019 до 2025) частка дорослих без базових навичок знизилась з 15% до 4% [19].

Висновки та перспективи подальших досліджень. Економічна безпека підприємств у цифрову епоху постає як багаторівнева, інтегрована система, що охоплює технологічні, інформаційні, кадрові, стратегічні та інституційно-правові елементи. Її сутність

виходить далеко за межі традиційного розуміння фінансової або ресурсної стабільності та перетворюється на складну мережу взаємозалежних процесів, здатних забезпечити стійкість підприємства в умовах швидкої цифрової трансформації та постійно зростаючих кіберзагроз. Кібербезпека в сучасних умовах набуває статусу стратегічного економічного ризику, а не технічної проблеми. Будь-яка атака на цифрову інфраструктуру підприємства може спричинити фінансові втрати, втрату клієнтських даних, репутаційні збитки та переривання бізнес-процесів. Тому інвестиції в кіберзахист, оновлення ІТ-інфраструктури та впровадження стандартів кібергігієни мають розглядатися як невід'ємна частина системи економічної безпеки.

Підвищення економічної безпеки підприємств у цифровій економіці потребує формування цілісного, комплексного й стратегічно орієнтованого підходу, який поєднує технологічні, організаційні, кадрові та нормативно-правові інструменти. Насамперед підприємствам слід посилювати технологічну складову безпеки шляхом впровадження сучасних рішень, таких як системи моніторингу інцидентів безпеки, багатомірної аутентифікація, мережеве сегментування та архітектура Zero Trust. Регулярні аудити безпеки, тестування на проникнення й оновлення ІТ-інфраструктури

забезпечують стійкість до нових загроз і зменшують імовірність технологічних збоїв. Не менш важливою є побудова ефективної системи управління даними, яка передбачає чітке регламентування доступу, шифрування критично важливої інформації, застосування резервного копіювання та використання захищених хмарних сервісів. Дані стають ключовим активом підприємства, тому їхня надійність є фундаментом економічної стабільності та конкурентоспроможності.

Особливу увагу необхідно приділяти розвитку цифрових компетенцій персоналу. Практика свідчить, що більшість інцидентів безпеки виникають через людські помилки, тому системне навчання співробітників основам кібергігієни, моделювання фішингових атак, тренінги з реагування на інциденти та формування цифрової культури стають критичними умовами забезпечення економічної безпеки. Кадрова політика підприємства має враховувати рівень цифрової грамотності, а система управління персоналом – забезпечувати постійне підвищення кваліфікації співробітників у сфері цифрових технологій.

Стратегічне управління ризиками повинно бути інтегрованим елементом корпоративної стратегії. Підприємствам слід проводити ідентифікацію та оцінювання цифрових ризиків, розробляти сценарії розвитку подій, формувати плани реагування на інциденти. Важливо забезпечити відповідне ресурсне забезпечення системи безпеки – фінансове, кадрове й технічне, а також забезпечити гнучкість і адаптивність до швидких технологічних змін.

Значну роль відіграє дотримання нормативно-правових вимог і міжнародних стандартів у сфері

інформаційної безпеки, таких як ISO/IEC 27001, GDPR чи NIS2. Підприємства мають впроваджувати політики відповідності, проводити правові аудити та інтегрувати вимоги регуляторів у внутрішні процеси управління. Корисною є співпраця з державними структурами, галузевими центрами кіберзахисту та міжнародними організаціями для обміну інформацією, отримання консультацій та доступу до актуальних рекомендацій щодо протидії сучасним кіберзагрозам. Узагальнюючи, можна стверджувати, що економічна безпека підприємств у цифровій економіці формується на перетині технологічної стійкості, ефективного управління даними, цифрових компетенцій персоналу, стратегічного управління ризиками та відповідності інституційно-правовим стандартам. Лише комплексна взаємодія цих компонентів дозволяє підприємствам забезпечити стабільність, конкурентоспроможність і здатність до розвитку в умовах цифрової трансформації.

Перспективи подальших досліджень полягають у поглибленому вивченні механізмів оцінювання цифрових ризиків на основі штучного інтелекту та машинного навчання, розробці моделей прогнозування кіберзагроз, формуванні методичних підходів до вимірювання цифрової компетентності персоналу, а також дослідженні впливу інноваційних технологій – зокрема блокчейну, квантових обчислень і автономних систем – на рівень економічної безпеки підприємств. Важливим напрямом є створення адаптивних, гнучких і самооновлюваних систем безпеки, здатних реагувати на високодинамічне середовище цифрової економіки.

Література.

1. Arroyabe M. F., Arranz C. F. A., Fernandez De Arroyabe I., Fernandez de Arroyabe J. C. Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*. 2024, vol. 78, p. 102670. DOI: <https://doi.org/10.1016/j.techsoc.2024.102670>.
2. Tian Z., Han M., Jiang C. Research on platform data security governance strategy based on three-party evolutionary game. *Heliyon*. 2024, vol. 10. DOI: <https://doi.org/10.1016/j.heliyon.2024.e36391>
3. Sun L., Zhang H., Fang C. Data security governance in the era of big data: Status, challenges, and prospects. *Data Science and Management*. 2021, vol. 2, pp. 41–44. DOI: <https://doi.org/10.1016/j.dsm.2021.06.001>.
4. Chen Z., Xing R. Digital economy, green innovation and high-quality economic development. *International Review of Economics & Finance*. 2025, vol. 99, p. 104029. DOI: <https://doi.org/10.1016/j.iref.2025.104029>.
5. Fotis F. Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. *Procedia Computer Science*. 2024, Vol. 251, pp. 471–478. DOI: <https://doi.org/10.1016/j.procs.2024.11.135>.
6. Samoilenko Y., Britchenko I., Levchenko I., Lošonczy P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs*. 2022, Vol. 67, No. 04, pp. 619–629. DOI: <https://doi.org/10.46852/0424-2513.4.2022.28>.
7. Цілецька 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. DOI: <https://doi.org/10.32983/2222-0712-2024-2-181-190>.
8. Іванов М., Martseniuk L., Angelova M., Faifer, S. Strategic risk management of digital transformation in the economic security of industrial enterprises. *Economics Ecology Socium*. 2025, Vol. 9, No 2, pp. 124–141. DOI: <https://doi.org/10.61954/2616-7107/2025.9.2-9>.
9. Шкарлет С. М., Садчикова І. В. Трансформація системи фінансово-економічної безпеки підприємства в умовах цифрової економіки. *Проблеми і перспективи економіки та управління*. 2019. № 3. С. 264–276. URL: http://nbuv.gov.ua/UJRN/prpu_2019_3_29.
10. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*. 2024. № 6. DOI: <https://doi.org/10.5281/zenodo.14575016>.
11. Muravskiy S., Tolpezhnikov R. Digital transformation and its impact on enterprise economic security. *Вісник мариупольського державного університету*. Серія: Економіка. 2024. № 28. С. 62–70. DOI: <https://doi.org/10.34079/2226-2822-2024-14-28-62-70>.
12. Воронюк Є. В., Чеплюк М. І. Інституційний підхід до формування економічної безпеки підприємницької діяльності в Україні та світі. *Бізнес Інформ*. 2019. № 9. С. 86–91. DOI: <https://doi.org/10.32983/2222-4459-2019-9-86-91>.
13. Блинков В. Підходи забезпечення економічної безпеки ІТ-сектору: міжнародний огляд. *Економіка та суспільство*. 2024. № 68. DOI: <https://doi.org/10.32782/2524-0072/2024-68-5>.
14. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. Серія «Економічні науки». 2020. № 4. Т. 1. С. 32–35. DOI: <https://www.doi.org/10.31891/2307-5740-2020-284-4-5>.
15. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022. DOI: 10.2760/115376.
16. ENISA Threat Landscape 2023. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.
17. Cost of a Data Breach Report 2023. URL: <https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf>.
18. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology Into Business Transformation. Boston: Harvard Business Press, 2014. 292 p.
19. Digital State UA: 96% of Ukrainians Now Have Digital Skills. URL: <https://digitalstate.gov.ua/news/govtech/96-of-ukrainians-now-have-digital-skills?>

References.

1. Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, vol. 78, p. 102670. <https://doi.org/10.1016/j.techsoc.2024.102670>.
2. Tian, Z., Han, M., & Jiang, C. (2024). Research on platform data security governance strategy based on three-party evolutionary game. *Heliyon*, vol. 10. <https://doi.org/10.1016/j.heliyon.2024.e36391>.
3. Sun, L., Zhang, H., & Fang, C. (2021). Data security governance in the era of big data: Status, challenges, and prospects. *Data Science and Management*, vol. 2, pp. 41–44. <https://doi.org/10.1016/j.dsm.2021.06.001>.
4. Chen, Z., & Xing, R. (2025). Digital economy, green innovation and high-quality economic development. *International Review of Economics & Finance*, vol. 99, p. 104029. <https://doi.org/10.1016/j.iref.2025.104029>.

5. Fotis, F. (2024). Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. *Procedia Computer Science*, vol. 251, pp. 471–478. <https://doi.org/10.1016/j.procs.2024.11.135>.
6. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O., & Bodnar, O. (2022). Economic security of the enterprise within the conditions of digital transformation. *Economic Affairs*, vol. 67, no. 4, pp. 619–629. <https://doi.org/10.46852/0424-2513.4.2022.28>.
7. Piletska, S. T., Arefiev, S. O., Petrovska, S. V., & Kolesnykov, S. O. (2024). Stratehichne zabezpechennya ekonomichnoyi bezpeky pidpryyemstv v konteksti tsyfrovizatsiyi ekonomiky Ukrainy [Strategic provision of economic security of enterprises in the context of digitalization of Ukraine's economy]. *Problemy ekonomiky*, no. 2 (60), pp. 181–190. <https://doi.org/10.32983/2222-0712-2024-2-181-190>.
8. Ivanov, M., Martseniuk, L., Angelova, M., & Faifer, S. (2025). Strategic risk management of digital transformation in the economic security of industrial enterprises. *Economics Ecology Socium*, vol. 9, no. 2, pp. 124–141. <https://doi.org/10.61954/2616-7107/2025.9.2-9>.
9. Shkarlet, S. M., & Sadchykova, I. V. (2019). Transformatsiya systemy finansovo-ekonomichnoyi bezpeky pidpryyemstva v umovakh tsyfrovoyi ekonomiky [Transformation of the financial and economic security system of the enterprise in the conditions of the digital economy]. *Problemy i perspektivy ekonomiky ta upravlinnya*, no. 3, pp. 264–276. Available at: http://nbuv.gov.ua/UJRN/ppeu_2019_3_29.
10. Kulchytskyi, I. I. (2024). Tsyfrova ekonomika ta ekonomichna bezpeka pidpryyemstva: stratehiyi upravlinnya [Digital economy and economic security of an enterprise: management strategies]. *Aktualni pytannya ekonomichnykh nauk*, no. 6. <https://doi.org/10.5281/zenodo.14575016>.
11. Muravskiy, S., & Tolpezhnikov, R. (2024). Digital transformation and its impact on enterprise economic security. *Visnyk Mariupol'skoho derzhavnogo universytetu. Seriya: Ekonomika*, no. 28, pp. 62–70. <https://doi.org/10.34079/2226-2822-2024-14-28-62-70>.
12. Voroniuk, Ye. V., & Chepeliuk, M. I. (2019). Instytutsiinyi pidkhid do formuvannya ekonomichnoyi bezpeky pidpryyemnytskoyi diyal'nosti v Ukraini ta sviti [Institutional approach to shaping economic security of entrepreneurial activity in Ukraine and worldwide]. *Biznes Inform*, no. 9, pp. 86–91. <https://doi.org/10.32983/2222-4459-2019-9-86-91>.
13. Blyukov, V. (2024). Pidkhody zabezpechennya ekonomichnoyi bezpeky IT-sektoru: mizhnarodnyi ohlyad [Approaches to ensuring the economic security of the IT sector: international review]. *Ekonomika ta suspil'stvo*, no. 68. <https://doi.org/10.32782/2524-0072/2024-68-5>.
14. Bakai, V. Y. (2020). Zabezpechennya ekonomichnoyi bezpeky pidpryyemstva na osnovi vykorystannya tsyfrovyykh tekhnolohiy [Ensuring enterprise economic security based on the use of digital technologies]. *Visnyk Khmelnytskoho natsionalnogo universytetu. Seriya "Ekonomichni nauky"*, no. 4, vol. 1, pp. 32–35. <https://doi.org/10.31891/2307-5740-2020-284-4-5>.
15. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. <https://doi.org/10.2760/115376>.
16. ENISA Threat Landscape 2023. (2023). Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.
17. Cost of a Data Breach Report 2023. (2023). Available at: <https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf>.
18. Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology Into Business Transformation*. Harvard Business Press.
19. Digital State UA. (n.d.). 96% of Ukrainians now have digital skills. Available at: <https://digitalstate.gov.ua/news/govtech/96-of-ukrainians-now-have-digital-skills>.

Abstract.

Luhova V., Kravchuk Y., Pushak Y., Litvinov D., Piechka S. *Economic security of enterprises in the digital economy.*

The article examines modern approaches to ensuring the economic security of enterprises in the digital economy, where digital technologies, information resources, and cybersecurity are key. It is substantiated that digitalization transforms all areas of enterprise activity—from strategic management and operational processes to data governance and personnel policy—while simultaneously generating a new spectrum of risks, including cyber incidents, information leaks, technical failures, innovative threats, and institutional vulnerabilities. Based on the analysis of scientific works, the main theoretical approaches to economic security are identified: the resource-based, functional, risk-oriented, institutional-legal, and sociotechnical approaches, which reflect the multidimensional nature of modern enterprise security. It is demonstrated that digital assets – data, cloud services, algorithms, software, and IT infrastructure – have become key resources, and the level of their protection directly determines companies' economic resilience and competitiveness. Particular attention is paid to personnel's digital competence as a critical factor in reducing the likelihood of cyber incidents, as most security breaches are caused by human error and insufficient technological skills. The article highlights the importance of technological cybersecurity tools, effective data management, implementation of information security standards, and integrated risk management, all of which interact with organizational resilience strategies. A set of recommendations is formulated to enhance enterprises' economic security, including developing employees' digital skills, modernizing IT infrastructure, improving security policies, conducting regular audits and system testing, and strengthening institutional compliance with national and international standards. The prospects for further research are outlined, including the development of intelligent models for assessing digital risks based on artificial intelligence, advancement of methods for measuring employees' digital competence, and the study of the impact of emerging technologies—blockchain, quantum computing, and autonomous systems – on the economic resilience and competitiveness of enterprises in the digital environment.

Keywords: economic security of the enterprise, risks, threats, innovative development, digital economy, digital transformation, information security, digital competence, system approach.

Стаття надійшла до редакції 12.08.2025 р.

Бібліографічний опис статті:

Лугова В. М., Кравчук Ю. В., Пушак Я. Я., Літвінов Д. О., Печка С. С. Економічна безпека підприємств в умовах цифрової економіки. Актуальні проблеми інноваційної економіки та права. 2025. № 5. С. 99–103.
Luhova V., Kravchuk Y., Pushak Y., Litvinov D., Piechka S. *Economic security of enterprises in the digital economy. Actual problems of innovative economy and law*. 2025. No. 5, pp. 99–103.

УДК 339.923:330.341.1:004.9; JEL classification: F15; O33; C18; R11 DOI: <https://doi.org/10.36887/2524-0455-2025-4-24>

СЕРПІЄНКО Олена Андріанівна, д.е.н., професор, професор кафедри підприємництва, торгівлі і логістики, Національний технічний університет, «Харківський політехнічний інститут», <https://orcid.org/0000-0002-9796-9218>
СМОРОДІН Андрій Юрійович, почесний професор НТУ «ХПІ», президент Національної платформи «Ініціати́ва Трьох морів – Україна» (м. Київ)
СІЛЧОВА Тетяна Василівна, кандидат педагогічних наук, доцент кафедри економічної кібернетики та прикладної економіки Харківського національного університету ім. В. Н. Каразіна, <https://orcid.org/0000-0001-5003-2711>

ЦИФРОВА ТРАНСФОРМАЦІЯ ЯК КАТАЛІЗАТОР РОЗВИТКУ ПРОЦЕСІВ ЄВРОІНТЕГРАЦІЇ

Сергієнко О. А., Смородін А. Ю., Сілічова Т. В. *Цифрова трансформація як каталізатор розвитку процесів євроінтеграції.*

Самовідентифікація України як європейської держави підштовхує країну до активних дій на шляху до євроінтеграції з метою посісти гідне місце в спільноті країн Європейського Союзу. Встановлено, що євроінтеграційний курс, поряд із розширенням можливостей для розвитку держави, водночас висуває перед Україною низку важливих викликів. Ці виклики пов'язані з необхідністю докорінних змін в багатьох сферах життя, що стосуються питань фундаментальних змін, вдосконалення внутрішнього ринку, забезпечення конкурентоспроможності та інклюзивного зростання, дотримання вимог «зеленого» порядку денного та сталого з'єднання, покращення залучення та використання ресурсів, вдосконалення функціонування сільського господарства та дотримання політики згуртованості, поліпшення зовнішніх відносин. Важливе значення для вдосконалення цих сфер відіграє цифрова трансформація. У ході дослідження ідентифіковано ключові інституційні документи євроінтеграційного розвитку України та доведено критичну роль цифрової трансформації у забезпеченні виконання рекомендацій Європейської Комісії. Проведено детальний кількісний аналіз індикаторів цифровізації: розраховано основні статистичні характеристики для інтеграційного індексу та всіх субіндексів цифрової трансформації; сформовано та проаналізовано гістограми розподілу субіндексів, що дозволило визначити їх модальні значення, характер розподілу та інтенсивність цифрових змін у регіонах; здійснено кореляційний аналіз субіндексів, що дав змогу виявити взаємозв'язки між компонентами цифрової трансформації та визначити субіндекси з найбільшим впливом на