



Менеджмент

УДК 338.2:658

DOI <https://doi.org/10.5281/zenodo.14575016>

**Цифрова економіка та економічна безпека підприємства:
стратегії управління**

Кульчицький Іван Іванович

кандидат економічних наук, старший викладач, Львівський інститут менеджменту, м. Львів, Україна, ORCID: <https://orcid.org/0009-0000-6294-7863>

Прийнято: 19.12.2024|Опубліковано: 29.12.2024

Анотація. Метою дослідження є обґрунтування сучасних підходів до стратегічного управління економічною безпекою підприємств, встановлення впливу цифрової економіки на забезпечення безпеки суб'єктів господарювання.

Методи. Для реалізації поставленої мети дослідження було використано такі методи: критичний аналіз наукових джерел – для обґрунтування особливостей цифрової економіки в Україні; метод синтезу – для аналізу впливу цифрових трансформацій на економічну безпеку підприємства; табличний метод – для наочної візуалізації отриманих досліджень; метод наукового абстрагування – для обґрунтування і узагальнення стратегій управління економічною безпекою підприємства в умовах цифрової економіки.

Результати. Установлено, що цифрову економіку можна охарактеризувати як сучасну бізнес-модель для національної та глобальної економік, що спирається на інформаційні технології, інтелектуальний капітал, нематеріальні активи та інновації. Зазначено, що цифрова економіка відкриває нові можливості для підприємств, і створює нові виклики для їх економічної безпеки. В статті обґрунтовано, що для успішного функціонування в умовах



цифрової економіки підприємствам необхідно приділяти увагу комплексному управлінню загрозами економічної безпеки. На основі експертних досліджень наведено основні стратегії забезпечення економічної безпеки для підприємств в умовах цифрової економіки: стратегія зростання; стратегія вибіркового посилення; стратегія адаптації; стратегія трансформації; стратегія відновлення. Ці стратегії забезпечують системний підхід до управління економічною безпекою компаній в умовах інформаційних викликів.

Висновки. Дослідження доводить, що у сучасних умовах цифрової економіки економічна безпека підприємств залежить від їх здатності адаптуватися до змін і протидіяти новим загрозам. Інтеграція цифрових технологій стає невід'ємною складовою управління безпекою. Лише правильно розроблена стратегія управління економічною безпекою дозволяє підприємствам залишатися конкурентоспроможними та фінансово стабільними.

Ключові слова: цифрова економіка, економічна безпека підприємства, стратегії, загрози, управління, ризики, цифровізація.

Digital Economy and Economics of the Enterprise: Management Strategies

Kulchytsky Ivan

Lviv Institute of Management, PhD in Economics, Senior Lecturer of Department of Management and International Business, Lviv, Ukraine, ORCID: <https://orcid.org/0009-0000-6294-7863>

Abstract. The purpose of the study is to analyze modern approaches to managing the economic security of enterprises, to establish the impact of the digital economy on ensuring the security of business entities.

Methods. To achieve the stated goal of the study, the following methods were used: critical analysis of scientific sources - to substantiate the features of the digital economy in Ukraine; synthesis method - to analyze the impact of digital transformations on the economic security of the enterprise; tabular method - for visual



visualization of the obtained research; scientific abstraction method - to substantiate and generalize strategies for managing the economic security of the enterprise in the conditions of the digital economy.

Results. It was established that the digital economy can be characterized as a modern business model for the national and global economy, based on information technologies, intellectual capital, intangible assets and innovations. It is noted that the digital economy opens up new opportunities for enterprises, digitalization, and creates new challenges for the economic security of enterprises. The article substantiates that for successful functioning in the digital economy, enterprises need to pay attention to comprehensive management of economic security threats. Based on expert research, the main strategies for ensuring economic security for enterprises in the digital economy are presented: growth strategy; selective reinforcement strategy; adaptation strategy; transformation strategy; recovery strategy. These strategies provide a systematic approach to managing the economic security of companies in the context of information challenges.

Conclusions. The study proves that in modern conditions of the digital economy, the economic security of enterprises depends on their ability to adapt to changes and counteract new threats. The integration of digital technologies is becoming an integral part of security management. Only a properly developed economic security management strategy allows enterprises to remain competitive and financially stable.

Keywords: digital economy, economic security of the enterprise, strategies, threats, management, risks, digitalization.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. Сучасні українські підприємства функціонують в складних умовах, що формуються під впливом значної кількості різноспрямованих факторів. Це стосується не лише трансформаційних змін у національній економіці, що супроводжуються постійним коригуванням монетарної політики, спробами стабілізації бізнес-середовище шляхом пошуку балансу між потребою наповнення державного та місцевих бюджетів і



посиленням фіскального тиску на бізнес. Також слід враховувати зростання використання цифрових технологій на тлі кризових умов, що впливає на конкурентоспроможність українських виробників як на внутрішньому, так і на зовнішньому ринках. Додатковими викликами є значні втрати людського капіталу через активну трудову міграцію та демографічну кризу. Якщо ці фактори є характерними для більшості українських підприємств, то низка проблем має індивідуальний характер. Комплексний вплив цих чинників вимагає від кожного підприємства в умовах цифровізації побудови нових стратегій управління економічною безпекою, які б відповідали рівню агресивності зовнішнього середовища та внутрішньому потенціалу. Відсутність таких стратегій знижує шанси на виживання самого суб'єкта господарювання.

Аналіз останніх досліджень і публікацій. Сучасні наукові дослідження пропонують напрацьований теоретичний базис, який містить інформацію про сутність і особливості стратегії економічної безпеки суб'єктів господарювання. Серед таких фахівців можна визначити Дуднєва Ю., Артем'єв О., Дячков Д., Потапюк І., Капран І., Колісніченко П., Ушенко Н., Терещенко Е., Кондратенко Н., Трембач Р., Копилюк О., Гузар У., Гута С., Кравченко О., Гаврилюк О., Челомбітько О., Бойко С., Масюк Ю., Мельник С., Огренич Ю., Зайцев Є. [1-9] та інші. Також, у науковій літературі наявні ґрунтовні висновки щодо поняття «цифрова економіка» та проведені дослідження щодо основних компонентів цифровізації розвитку держави [10-14].

Виділення невирішених раніше частин загальної проблеми. Попри значний науковий доробок, залишається низка нерозв'язаних питань, зокрема потребують подальшого розгляду особливості формування стратегії управління економічною безпекою підприємства в контексті цифрової трансформації. В умовах воєнного стану та стрімкого розвитку цифрової економіки доцільно охарактеризувати загрози та їх прояви; на основі дослідження загроз сформувати основні стратегії управління економічною безпекою суб'єкта господарювання з урахуванням тренду діджиталізації.



Формулювання цілей статті. Метою цього дослідження є визначення властивостей розвитку цифрової економіки в Україні та обґрунтування напрямів стратегічного управління економічною безпекою підприємства.

Виклад основного матеріалу дослідження. Цифрова економіка являє собою нову форму підприємницької діяльності, що базується на мережевій взаємодії через Інтернет. Її можна охарактеризувати як сучасну бізнес-модель для національної та глобальної економік, що спирається на інформаційні технології, інтелектуальний капітал, нематеріальні активи та інновації. Це включає не лише використання передового обладнання та програмного забезпечення, але й фундаментальні зміни в управлінні, корпоративній культурі та зовнішніх комунікаціях. Такий підхід сприяє підвищенню продуктивності працівників, збільшенню задоволеності клієнтів та формуванню іміджу підприємств як інноваційних і сучасних організацій. У практичному аспекті це передбачає впровадження систем наскрізних бізнес-процесів.

На сьогодні не існує єдиного підходу до визначення сутності поняття «інформаційна економіка». Узагальнюючи думки науковців, можна зазначити, що рушійною силою трансформаційних процесів є інноваційні цифрові технології [11-12]. Інформаційна економіка орієнтована на використання знань у сучасному світі, приділяючи особливу увагу digital-процесам в економіці, та має тісний зв'язок з інноваційною складовою. Її основними ресурсами виступають знання та інформація, які формують основу економічного зростання та підвищення конкурентоспроможності держави [10].

Цифрова економіка, що базується на інформаційних технологіях, інноваціях і нематеріальних активах, змінює не лише форми ведення бізнесу, а й підходи до забезпечення економічної безпеки підприємств. Цей вплив має як позитивні, так і негативні аспекти, що вимагає від організацій адаптації до нових умов.

По-перше, цифрова економіка відкриває нові можливості для підприємств. Використання сучасних технологій, таких як великі дані, штучний інтелект та автоматизація, дозволяє підвищити ефективність бізнес-процесів, мінімізувати



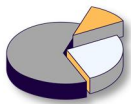
витрати та покращити якість продукції чи послуг. Наприклад, цифрові платформи дозволяють підприємствам швидше реагувати на зміни попиту, аналізувати поведінку клієнтів і впроваджувати персоналізовані пропозиції. Це позитивно впливає на конкурентоспроможність і забезпечує стійкість до економічних ризиків.

Однак, цифровізація також створює нові виклики для економічної безпеки підприємств. Найбільшу загрозу становлять кіберризики. Використання цифрових інструментів та мережевих технологій підвищує вразливість до атак хакерів, витоків даних та шахрайства. Наприклад, компрометація конфіденційної інформації чи втрата доступу до критичних систем може призвести до фінансових втрат, репутаційних ризиків та навіть зупинки діяльності підприємства.

Додатково, цифрова економіка вимагає перегляду підходів до управління внутрішніми процесами. Використання новітніх технологій потребує значних інвестицій у навчання персоналу, модернізацію інфраструктури та впровадження систем захисту даних. Відсутність таких інвестицій може поставити під загрозу не лише економічну безпеку, а й існування підприємства в умовах жорсткої конкуренції.

Крім того, цифрова економіка змінює характер регуляторного середовища. Підприємства повинні дотримуватись нових стандартів і законодавчих вимог у сфері захисту даних, прозорості бізнес-процесів та електронної торгівлі. Недотримання цих норм може призвести до штрафів, судових позовів та втрати довіри клієнтів. Для забезпечення економічної безпеки в умовах цифрової економіки та воєнного стану підприємствам необхідно приділяти увагу стратегіям, які повинні враховувати моніторинг ризиків, використання сучасних систем управління даними та розробку антикризових планів. Важливо також інвестувати в людські ресурси, щоб запобігти внутрішнім загрозам, таким як відтік людського капіталу в умовах військової агресії рф [14-16].

Отже, цифрова економіка має значний вплив на економічну безпеку підприємств. Вона надає нові можливості для розвитку, але водночас створює



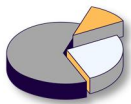
нові ризики. Лише підприємства, які здатні адаптуватись до цифрових трансформацій, зможуть забезпечити свою економічну стійкість і ефективно захищати свої ресурси в сучасному динамічному середовищі.

У цифрову епоху економічна безпека підприємств зазнає значного впливу нових типів загроз, зумовлених стрімким розвитком технологій та переходом бізнесу до цифрових моделей діяльності. Розглянемо ключові загрози та їхні прояви (табл. 1).

Таблиця 1

Основні загрози та їхні прояви

Загрози	Прояви	Ризики
Кіберзагрози	кібератаки, злам інформаційних систем, розкрадання конфіденційних даних, впровадження шкідливого програмного забезпечення, блокування доступу до даних (наприклад, атаки типу ransomware)	витік комерційної інформації, фінансові втрати, зупинка бізнес-процесів, репутаційні ризики
Ненадійність інформаційних систем	збої в роботі програмного забезпечення, апаратні несправності, втрати даних через технічні проблеми або помилки в управлінні інформаційними потоками	зупинка діяльності, втрата клієнтів, додаткові витрати на відновлення
Незахищеність даних і порушення конфіденційності	несанкціонований доступ до баз даних, зловживання персональною інформацією клієнтів чи співробітників, недотримання вимог до захисту даних (наприклад, GDPR)	штрафні санкції, судові позови, втрата довіри клієнтів
Конкурентні загрози в цифровому середовищі	зростання конкуренції через онлайн-платформи, використання конкурентами технологій для отримання переваг, недобросовісні практики (наприклад, кібершпигунство)	втрата ринкової частки, зниження прибутковості
Фінансові шахрайства та цифрові злочини	махінації з онлайн-платежами, фальсифікація фінансових транзакцій, використання фішингових схем для викрадення коштів	фінансові втрати, зниження ліквідності, послаблення довіри з боку партнерів
Залежність від зовнішніх постачальників цифрових послуг	збої у роботі хмарних сервісів, монополізація постачальників програмного забезпечення, розрив контрактів з провайдерами	втрата даних, затримки в роботі, зростання витрат на альтернативні рішення
Низький рівень цифрової компетентності персоналу	людські помилки під час роботи з інформаційними системами, невміння користуватися захисними інструментами, невідповідність вимогам цифрової економіки	зростання внутрішніх загроз, втрати часу і ресурсів на навчання або відшкодування помилок
Зміна регуляторного середовища	посилення вимог до захисту даних, нові податкові норми для цифрової економіки,	штрафи, судові розгляди, адміністративні ускладнення



	невідповідність існуючих бізнес-процесів законодавчим нормам	
Інноваційна залежність	швидке старіння технологій, необхідність постійних інвестицій у нові розробки, високі витрати на впровадження інновацій	відставання від конкурентів, зниження ефективності, додаткове фінансове навантаження
Репутаційні ризики у цифровому середовищі	поширення негативної інформації у соціальних мережах, кібератаки, що шкодять іміджу підприємства, витоки даних клієнтів	зменшення кількості клієнтів, втрати інвесторів, негативний вплив на партнерські відносини

Джерело: розроблено автором

Для успішного функціонування в умовах цифрової економіки підприємствам необхідно приділяти увагу комплексному управлінню загрозами економічної безпеки. Це включає інвестування в сучасні системи кіберзахисту, підвищення цифрової грамотності персоналу, розробку стратегій управління ризиками та дотримання вимог регуляторного середовища. Лише підприємства, які готові проактивно реагувати на нові виклики, зможуть забезпечити свою стійкість та конкурентоспроможність.

Дефініція «стратегія економічної безпеки» є багатовимірною, що зумовлено різними підходами до її трактування. Вона часто розглядається у співвідношенні або в протиставленні з такими поняттями, як «стратегія забезпечення економічної безпеки», «стратегія системи економічної безпеки підприємства» чи навіть «стратегія інноваційного розвитку системи економічної безпеки підприємства» тощо [2; 8; 15-16]. На основі проаналізованих підходів, «стратегія економічної безпеки» розглядається як додатковий, логічно інтегрований елемент загальної системи стратегій господарського суб'єкта. Вона може бути представлена у вигляді окремого плану, системи планів або складової частини іншого стратегічного документа. Метою стратегії є досягнення довгострокових цілей економічної безпеки шляхом реалізації певних заходів (дій, способів, операцій тощо), що створюють сприятливі умови для задоволення інтересів підприємства. Це стосується сталого розвитку, підтримання і посилення конкурентоспроможності, підвищення ефективності роботи, фінансово-економічної стабільності та захисту від актуальних і потенційних



загроз. Варто підкреслити, що стратегія економічної безпеки, як системна категорія, формується із врахуванням розміру, структури, рівня управління та галузевої належності господарського суб'єкта, щоб забезпечити його стабільне функціонування у довгостроковій перспективі.

Експерти виділяють п'ять основних стратегій забезпечення економічної безпеки для підприємств в умовах цифрової економік:

1. Стратегія зростання – спрямована на підтримання досягнутого рівня економічної безпеки, постійний моніторинг результатів діяльності та запобігання потенційним загрозам, які можуть вплинути на економічні інтереси підприємства.

2. Стратегія вибіркового посилення – передбачає заходи, спрямовані на укріплення окремих показників чи компонентів економічної безпеки компанії.

3. Стратегія адаптації – фокусується на адаптації елементів економічної безпеки підприємства до змін у зовнішньому середовищі.

4. Стратегія трансформації – включає внесення змін, пов'язаних із типом діяльності, ринковими умовами та коригуванням компонентів фінансово-економічної безпеки компанії.

5. Стратегія відновлення – орієнтована на реалізацію заходів, які дозволяють досягти необхідного рівня економічної безпеки підприємства.

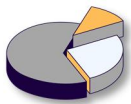
Ці стратегії забезпечують системний підхід до управління економічною безпекою компаній в умовах сучасних викликів.

В умовах цифрової економіки кожна з ключових стратегій забезпечення економічної безпеки набуває специфічних, зумовлених впливом новітніх технологій, змін у бізнес-процесах і підвищенням рівня інформаційних ризиків.

Таблиця 2

Основні загрози та їхні прояви

Назва	Специфіка	Мета
Стратегія зростання	Забезпечення економічної безпеки в цифрову епоху вимагає впровадження інструментів автоматизованого моніторингу фінансових показників, аналітичних платформ для оцінки ризиків і технологій big data для прогнозування загроз. Підприємства повинні активно	Збереження стабільного рівня економічної безпеки шляхом інтеграції



	використовувати штучний інтелект для раннього виявлення відхилень у фінансових операціях	сучасних цифрових рішень
Стратегія вибіркового посилення	Зосередження на зміцненні окремих компонентів економічної безпеки, наприклад, захисту конфіденційних даних клієнтів або впровадженні технологій кібербезпеки. Використання блокчейн-технологій для захисту фінансових транзакцій і перевірки достовірності даних є ключовим елементом цієї стратегії	Модернізація критично важливих складових безпеки відповідно до цифрових викликів
Стратегія адаптації	Передбачає адаптацію компонентів економічної безпеки до стрімких змін у цифровому середовищі. Це включає автоматизацію страхових процесів, розробку онлайн-сервісів для клієнтів та інтеграцію хмарних технологій для зберігання і обробки даних. Особливу увагу слід приділяти управлінню ризиками, пов'язаними з кібератаками та витоком даних	Гнучка адаптація до технологічних змін для збереження конкурентоспроможності
Стратегія трансформації	Фокус на використанні цифрових технологій для радикальних змін у бізнес-процесах. Це може включати впровадження інноваційних інструментів страхування, таких як телематика (у страхуванні транспорту) або аналіз IoT-даних для оцінки ризиків. Стратегія також передбачає перехід до цифрових каналів взаємодії з клієнтами і партнерами	Перебудова бізнес-моделі з урахуванням можливостей цифрової економіки
Стратегія відновлення	Реалізація цифрових рішень для відновлення рівня економічної безпеки. Це може включати впровадження антикризових систем моніторингу, інвестиції в кібербезпеку, створення резервних копій даних у хмарних сховищах та автоматизованих платформ управління ризиками	Досягнення стабільності шляхом використання технологій для відновлення фінансових і операційних процесів

Джерело: розроблено автором

Усі ці стратегії в умовах цифрової економіки потребують інтеграції сучасних цифрових технологій, таких як штучний інтелект, хмарні обчислення, блокчейн і великі дані. Крім того, ключову роль відіграє формування цифрової культури в компанії, навчання персоналу та впровадження політик кібербезпеки для захисту від нових ризиків цифрового середовища.

Висновки.

1. Цифрова економіка трансформує підходи до управління економічною безпекою підприємств, створюючи як нові можливості, так і загрози. Інноваційні технології, такі як штучний інтелект, великі дані, блокчейн



і хмарні обчислення, сприяють підвищенню ефективності, адаптивності та конкурентоспроможності підприємств. Проте, паралельно посилюється вразливість до кіберзагроз, витоків даних і шахрайства.

2. Умови цифрової економіки вимагають системних знань та напрацювань до розробки стратегій економічної безпеки. Ключові стратегії – зростання, вибіркове посилення, адаптація, трансформація та відновлення – набувають нового змісту через інтеграцію цифрових технологій. Ефективне застосування цих стратегій дозволяє підприємствам адаптуватися до змін зовнішнього середовища, зміцнювати вразливі компоненти безпеки, впроваджувати інновації та відновлювати стабільність у разі кризових ситуацій.

3. Інформаційні технології стають основою забезпечення економічної безпеки підприємств. Використання автоматизованих систем моніторингу, аналітичних платформ і інструментів кіберзахисту дозволяє своєчасно виявляти ризики, мінімізувати фінансові втрати і забезпечувати стійкість до зовнішніх та внутрішніх загроз.

4. Ефективне впровадження стратегій економічної безпеки в умовах цифрової економіки залежить від рівня цифрової компетентності персоналу. Інвестиції в навчання працівників і формування культури цифрової безпеки є ключовими для запобігання людським помилкам, які можуть стати причиною значних збитків.

5. Стратегія економічної безпеки має бути інтегрованою складовою загальної стратегії підприємства, враховуючи його розмір, галузь, рівень цифровізації та особливості конкурентного середовища. Такий підхід забезпечує не лише захист від загроз, але й створює умови для довгострокового розвитку, підвищення конкурентоспроможності та фінансової стабільності.

6. Розвиток нормативно-правового середовища. Цифрова економіка потребує постійного вдосконалення регуляторної бази для забезпечення прозорості, захисту даних та мінімізації цифрових ризиків. Відповідність нормативним вимогам стає обов'язковою складовою стратегії економічної безпеки підприємств.



У цифрову епоху економічна безпека підприємства як підґрунтя повоєнного відновлення держави є багатогранною категорією, що вимагає адаптивного підходу. Лише ті підприємства, які здатні інтегрувати цифрові технології, забезпечити ефективний захист даних і гармонізувати стратегії безпеки з цілями сталого розвитку, зможуть залишатися конкурентоспроможними, фінансово стабільними та захищеними від загроз у сучасному динамічному середовищі.

Список використаних джерел

1. Дуднєва Ю., Артем'єв О. Економічна безпека суб'єктів господарювання в умовах перманентної кризи. *Адаптивне управління: теорія і практика. Серія Економіка*. 2023. №17(34). URL: <https://amtp.org.ua/index.php/journal2/article/view/607/515> (дата звернення 10.12.2024)
2. Дячков Д., Потапюк І., Капран І. Економічна безпека в системі стратегічного управління підприємством. *Економіка та суспільство*. 2021. № (24). URL: <https://economyandsociety.in.ua/index.php/journal/article/view/173> (дата звернення 10.12.2024)
3. Колісніченко П. Т., Ушенко Н. В., Терещенко Е. Ю. Методичні засади аналізу ефективності механізму управління фінансово-економічною безпекою підприємства. *Часопис економічних реформ*. 2023. № 3. С. 42-53
4. Кондратенко Н. О., Трембач Р. П. Теоретико-методичні основи управління фінансово-економічною безпекою суб'єктів підприємницької діяльності. *Наукові записки Національного університету «Острозька академія»*. Серія: Економіка. 2024. № 34. С. 56-61.
5. Копилук О. І., Гузар У. Є., Гута С. В. Сучасні підходи до організації системи фінансово-економічної безпеки підприємства. *Бізнес Інформ*. 2019. № 3. С. 229-234.
6. 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).

[https://doi.org/10.33296/2707-0654-19\(38\)-12](https://doi.org/10.33296/2707-0654-19(38)-12)

7. Масюк Ю. В. Організація наукових досліджень в системі фінансово-економічної безпеки: сутність, завдання та методичні підходи. *Агросвіт*. 2023. № 22. С. 56-61.
8. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика: монографія. Львів: «Растр-7», 2020. 384 с.
9. Огренич Ю. О., Зайцев Є. А. Стан та забезпечення фінансово-економічної безпеки промислових підприємств в умовах цифровізації економіки. *Економічний простір*. 2024. № 189. С. 12-18.
10. Романовська Ю. Прогнозування та сценарування розвитку міст в умовах інформаційної економіки. *Економіка та суспільство*. 2024. №67. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4826> (дата звернення 11.12.2024)
11. Зінченко О. А., Даріюш П., Зінченко Д. С. Інформаційна економіка: концепція, сутність та розвиток. *Економічний вісник НТУУ «КПІ»*. 2019. № 16. С. 3–12
12. Котелевець Д. О. Проблема наукового визначення поняття цифрової економіки. *Актуальні проблеми розвитку економіки регіону*. 2022. Вип. 18. Т. 2. С. 239–247.
13. Шаповал Н., Федосєнко М., Грибановський О., Терещенко О. Повоєнне відновлення України. Нові ринки та цифрові рішення / Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH; Київська школа економіки. 2022. URL: <https://kse.ua/wp-content/uploads/2022/09/Digital-instruments-in-Ukrainian-recovery.pdf> (дата звернення 09.12.2024)
14. Фінагіна О. В., Бітюк І. М., Матвієнко О. Д., Гудима Д. М. Принципи розвитку українського освітнього простору в умовах інформаційної економіки: креативні підходи та європейський досвід. Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. 2022. Випуск 65. С. 16–24.



15. European Economic Security: Current practices and further development. URL: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO_IDA(2024)754449_EN.pdf (дата звернення 10.12.2024)

16. Information Economy Report (Series) // United nations conference on trade and development. URL: <https://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx> (дата звернення 12.12.2024)