

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 5.

DOI: <http://doi.org/10.32702/2307-2105.2025.5.118>

УДК 330.1:658

Г. Г. Тигач,

аспірант кафедри безпеки та правоохоронної діяльності,

Західноукраїнський національний університет

ORCID ID: <https://orcid.org/0009-0009-7989-6738>

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Н. Tyhach,

Postgraduate student of the Department of Security and Law Enforcement,

West Ukrainian National University

ENSURING ENTERPRISE ECONOMIC SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION

У статті досліджено особливості забезпечення економічної безпеки підприємства в умовах цифрової трансформації. Розглянуто вплив процесів цифровізації на формування нових ризиків та загроз для бізнесу. Проаналізовано системні, структурні, галузеві, підприємницькі та особистісні загрози економічній безпеці, що виникають у цифровому середовищі. Обґрунтовано трансформацію складових економічної безпеки підприємства під впливом цифрових технологій, зокрема фінансової, інтелектуально-кадрової, техніко-технологічної, інформаційної, ринкової та репутаційної. Досліджено європейський досвід оцінки ризиків цифрової безпеки.

Запропоновано комплексний підхід до забезпечення економічної безпеки, що враховує сучасні виклики цифровізації та воєнного стану. Визначено етапи впровадження системи забезпечення економічної безпеки в умовах цифрової трансформації та окреслено перспективні напрями подальших досліджень у сфері розробки методик кількісної оцінки впливу цифровізації на безпеку підприємств.

This paper investigates the specifics of ensuring economic security of enterprises under digital transformation conditions. The research reveals that rapid digitalization of the economic environment creates significant advantages for businesses while simultaneously generating unprecedented risks and threats that require revolutionary rethinking of security strategies.

The study systematizes digital threats to economic security into five categories: systemic threats (technological dependence on foreign digital solutions, lack of domestic electronic component production base); structural threats (labor market transformation and technological unemployment); industry-specific threats (absence of domestic digital solutions in critical economic sectors); entrepreneurial threats (unauthorized access to corporate data and various forms of cyberattacks); and personal threats (confidentiality breaches and information manipulation).

Analysis of European experience demonstrates significant differences in approaches to digital risk assessment depending on company size and digital maturity levels of national economies. Data shows assessment rates ranging from 14% in Hungary to 60% in Finland, with risk transfer through insurance mechanisms varying from 4% in Lithuania to over 56% in Denmark.

The paper proposes a comprehensive approach to economic security that incorporates financial, intellectual-personnel, technical-technological, political-legal, informational, environmental, force, market, and reputational components, each acquiring new characteristics in the digital environment. Of particular importance is the information component, as information becomes one of the most crucial security resources for enterprises in the digital era.

A methodological framework for implementing economic security systems under digital transformation is presented, including diagnostic stages of digital maturity, risk assessment, security strategy development, organizational structure formation, technological solution implementation, personnel digital competence development, and effectiveness monitoring.

The research outlines promising directions for further investigations, including development of quantitative assessment methodologies for measuring the impact of digital transformations on economic security levels across different industries, formation of industry-specific digital security standards, and study of adaptive security mechanisms that allow businesses to respond effectively to rapidly changing conditions in the digital environment, particularly during hybrid warfare.

Ключові слова: *економічна безпека підприємства, цифрова трансформація, цифровізація, кібербезпека, цифрові загрози, діджиталізація, інформаційна безпека, цифрові ризики, стратегія цифрової безпеки, цифрова економіка.*

Keywords: *economic security of enterprise, digital transformation, digitalization, cybersecurity, digital threats, digital security, information security, digital risks, digital security strategy, digital economy.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. *Сьогодні проблематика економічної безпеки підприємств постає надзвичайно гостро через блискавичну цифровізацію економічного простору. Хоча підприємства отримують значні переваги від діджиталізації, одночасно виникають непередбачувані ризики та загрози.*

Трансформація цифрового середовища невпинно руйнує усталені механізми ведення бізнесу. Інтеграція таких технологічних новацій як AI, big data, IoT і блокчейн змушує бізнес докорінно переглядати підходи до безпеки. З'явилися принципово нові кіберзагрози, зросли ризики витоку конфіденційної

інформації та промислового шпигунства у віртуальному просторі, що вимагає революційного переосмислення безпекових стратегій.

Воєнні дії в Україні спричинили шоковий вплив на умови функціонування підприємств, породивши безпрецедентні виклики для їхньої економічної безпеки. Зруйновані ланцюги постачання, відрізані ринки збуту, загрози знищення майна, відтік фахівців та енергетична криза – ці чинники спонукають до розробки кардинально нових механізмів забезпечення стійкості бізнесу.

За таких обставин критично важливим стає дослідження інтегрованих підходів до економічної безпеки, що враховують як класичні, так і новітні загрози, пов'язані з цифровізацією, пандемічними наслідками та бойовими діями. Надзвичайної ваги набуває пошук методів впровадження цифрових рішень у системи безпеки, максимальне використання можливостей технологічних трансформацій для зміцнення стійкості та зменшення впливу нових ризиків.

Аналіз останніх досліджень і публікацій. Питання забезпечення економічної безпеки є предметом дослідження значної кількості вчених. Разом з тим новітні умови інтенсивних цифрових трансформацій зумовлюють появу нових загроз економічній безпеці та їх ідентифікаторів. Окремі питання врахування аспектів цифрової трансформації в контексті забезпечення економічної безпеки розглядали у своїх працях такі вчені, як О. Боднар [1], А. Колесніков [2], В. Бакай [3], С. Тульчинська, О. Солосіч, В. Чорний [4], О. Литовченко [5], О. Ляхович, І. Оплачко [6], В. Проскура, Т. Черничко, Д. Верецький [7] та інші.

Мета статті. Дослідження особливостей та вироблення окремих пропозицій щодо забезпечення економічної безпеки підприємства в умовах цифрової трансформації.

Викладення основного матеріалу дослідження. Однією з ключових рис цифрової економіки є переорієнтація з матеріальних активів на інформаційні (відомості, дані, знання). Останні, своєю чергою, не втрачаються при споживанні, допускають багаторазове застосування незалежно від місця, часу

та автора, що зумовлює легкість тиражування інформаційних ресурсів. Це, як наслідок, спричиняє те, що великі та малі компанії стають більш уразливими до загроз у цифровому просторі, що негативно відбивається на їхній економічній безпеці [3, с. 33].

Збільшення числа порушень в умовах цифровізації господарства зумовлене безперервним ускладненням та розширенням сфер використання цифрових технологій. Більшість загроз для інформаційної, а відтак, і економічної безпеки, криються власне у цифрових технологіях [5, с. 77].

О. Ляхович та І. Оплачко структурують цифрові загрози економічній безпеці підприємства відповідно п'яти напрямків.

1. Системні загрози охоплюють вразливості всієї економіки або її значних сегментів, як-от технологічна залежність від закордонних цифрових рішень, брак власної виробничої бази електронних компонентів та поглиблення цифрового розриву між різними соціальними групами.

2. Структурні загрози виникають унаслідок масштабного впровадження цифрових технологій, що призводить до фундаментальних змін економічного ландшафту, зокрема трансформації ринку праці та зростання технологічного безробіття.

3. Галузеві загрози стосуються відсутності вітчизняних цифрових рішень у критичних секторах економіки, наприклад, брак національної платіжної системи, що створює ризики для економічного суверенітету.

4. Підприємницькі загрози формуються як ззовні, так і всередині бізнес-структур, включаючи несанкціонований доступ до корпоративних даних та різноманітні форми кібератак на інформаційну інфраструктуру компаній.

5. Особистісні загрози зачіпають індивідуальний рівень і стосуються порушення конфіденційності персональних даних громадян, їх несанкціонованого використання та інформаційних маніпуляцій [6, с. 103]

Цифрова трансформація змістовно відрізняється від автоматизації та інформатизації. Вона вимагає комплексних змін у всіх сферах: від бізнес-процесів та моделей до економічних відносин. Ці зміни мають відбутися як у внутрішній структурі підприємства, так і в його взаємодії з зовнішнім

середовищем. Для успішного здійснення цифрової трансформації на підприємствах традиційних галузей необхідно створити сприятливе середовище, що включає в себе проведення спеціалізованих технологічних та бізнес-консультацій, які можуть бути забезпечені відповідними центрами компетенції [1, с. 240].

Особливості оцінки ризиків цифрової безпеки підприємств ЄС подано у таблиці 1.

Таблиця 1. Особливості оцінки ризиків цифрової безпеки підприємств ЄС [1, с. 243]

Індикатор	Держава
Частка компаній, які проводять оцінку ризиків цифрової безпеки	Від 14 % в Угорщині до 60 % у Фінляндії. Показник зростає зі збільшенням розміру компанії (менше 1/3 серед малих компаній, наближається до 3/4 серед великих)
Передача ризику (страхування)	Від 4 % у Литві до понад 56 % у Данії. В усіх країнах ЄС, крім двох, схильність до передачі ризику зростає з розміром підприємств. У Данії він значно вищий серед малих підприємств (57 %) порівняно з середніми підприємствами (5 %) і великими підприємствами (40 %). Це також виявлено в Словенії, хоча й у значно меншій мірі
Частка підприємств, на яких працюють люди, які знають про свої зобов'язання щодо безпеки ІКТ	Він коливається від 1/3 у Греції до понад 3/4 в Ірландії, де також спостерігається висока концентрація бізнесу в секторі ІКТ. Ця частка також зростає з розміром підприємств: менше 60% серед малих підприємств, але більше 90% серед великих

Наведені в таблиці дані свідчать про суттєві відмінності в підходах до оцінки ризиків цифрової безпеки серед європейських підприємств. Прослідковується чітка залежність між розміром компанії та її увагою до питань цифрової безпеки, що підтверджує гіпотезу про прямий зв'язок між масштабом діяльності та рівнем усвідомлення кіберзагроз. Особливо показовим є приклад Фінляндії, де 60% компаній регулярно проводять оцінку ризиків, що корелює з високим рівнем цифрової зрілості фінського бізнесу та державної політики у сфері кіберзахисту.

Водночас, низькі показники в окремих країнах ЄС (зокрема, в Угорщині та Литві) свідчать про наявність значного потенціалу для вдосконалення систем

економічної безпеки. Важливим аспектом є також передача ризиків через механізми страхування, що відображає стратегічний підхід до управління цифровими загрозами. Данський досвід, де понад половина підприємств використовує страхові інструменти, демонструє перспективний напрямок розвитку для українського бізнесу в контексті посилення захисту від кіберзагроз.

Економічна безпека підприємства в цифровому просторі – це динамічний стан захищеності економічних інтересів суб'єкта господарювання в умовах цифрової трансформації, що забезпечує стійкість до зовнішніх і внутрішніх загроз, ефективне використання ресурсів та реалізацію бізнес-потенціалу через інтегровану систему фізичного та цифрового захисту його активів, процесів, інформації та репутації.

Змістовне наповнення даного визначення передбачає дослідження складових забезпечення економічної безпеки підприємства через призму розвитку цифрових технологій [4].

Фінансова складова в цифровому середовищі передбачає зниження непродуктивних витрат завдяки автоматизації, спрощення банківських операцій та розвиток фінтех-послуг. Водночас збільшуються витрати на інформаційний захист і виникають нові ризики, пов'язані з криптовалютами та цифровими фінансовими ринками.

Інтелектуально-кадрова складова трансформується через впровадження електронних систем управління персоналом, зміни у структурі ринку праці та перехід до гібридних форм зайнятості. Зростає цінність інтелектуального потенціалу працівників та актуалізуються питання захисту інтелектуальної власності.

Техніко-технологічна складова охоплює автоматизацію виробничих процесів, розширення можливостей контролю над виробництвом та створення нових цифрових продуктів. Ця сфера демонструє найбільш помітні позитивні зміни від впровадження цифрових технологій.

Політико-правова складова відображає цифровізацію відносин між підприємством і державою, посилення правових аспектів у сфері

інтелектуальної власності та вплив транснаціональних ІТ-корпорацій на інформаційне середовище.

Інформаційна складова є ключовою в цифрову епоху і включає захист даних, розвиток аналітичного інструментарію та управління інформаційними потоками. Інформація стає одним із найважливіших безпекових ресурсів підприємства.

Екологічна складова в цифровому контексті проявляється через скорочення паперового документообігу, застосування цифрових технологій для моніторингу впливу на навколишнє середовище та підвищення екологічної відповідальності бізнесу.

Силова складова в епоху діджиталізації протидіє новим формам цифрового рейдерства, шантажу з використанням персональних даних, промислового шпівонажу та PR-атак через соціальні мережі.

Ринкова складова безпеки адаптується до розвитку електронної комерції, підвищення конкуренції в онлайн-середовищі, зростання значущості цифрового маркетингу та ризиків монополізації ІТ-ринку.

Додатково варто відзначити репутаційну складову, що набуває особливого значення в цифровому просторі, де інформація поширюється миттєво, а репутаційні ризики суттєво зростають через соціальні мережі та інші онлайн-канали комунікації.

Один із підходів щодо вироблення системи показників дослідження економічної безпеки підприємства в умовах цифровізації описана у праці [7]. Модель включає п'ять взаємопов'язаних складових: кадрову, виробничо-технологічну, фінансову, екологічну та цифрову безпеку. Ключовою особливістю підходу є введення нової цифрової складової, що охоплює використання віддаленої роботи, наскрізних технологій, електронного документообігу та цифрового маркетингу.

Методологічно підхід базується на перетворенні різнорідних показників до єдиної безрозмірної шкали з урахуванням їхніх порогових значень. Далі розраховуються інтегральні індекси для кожної функціональної складової з використанням вагових коефіцієнтів, що визначаються експертним шляхом.

Загальний рівень економічної безпеки встановлюється на основі підсумкового інтегрального індексу, який дозволяє класифікувати стан підприємства від критично низького до дуже високого.

Впровадження комплексної системи забезпечення економічної безпеки в умовах цифрової трансформації вимагає послідовного підходу, що охоплює кілька ключових етапів:

1. Діагностика цифрової зрілості підприємства з використанням спеціалізованих індексів та показників, що дозволяє визначити поточний рівень цифровізації та виявити проблемні зони.

2. Оцінка цифрових ризиків і загроз із застосуванням сучасних методик моделювання кіберінцидентів, включаючи сценарний аналіз та стрес-тестування інформаційних систем.

3. Розробка стратегії цифрової безпеки, інтегрованої в загальну стратегію розвитку підприємства, з чітким визначенням пріоритетів, ресурсів та часових горизонтів.

4. Формування організаційної структури з визначеними центрами відповідальності за різні аспекти цифрової безпеки, включаючи створення спеціалізованих підрозділів або залучення зовнішніх експертів.

5. Впровадження технологічних рішень, що забезпечують захист даних, систем і процесів, з особливою увагою до критичної інфраструктури підприємства.

6. Розвиток цифрових компетенцій персоналу через системні навчальні програми, тренінги та симуляції кібератак для підвищення пильності співробітників.

7. Моніторинг ефективності системи економічної безпеки з використанням ключових показників ефективності (KPI) та регулярне оновлення безпекових протоколів відповідно до еволюції загроз.

Таким чином, забезпечення економічної безпеки в умовах цифрової трансформації стає не одноразовим проєктом, а безперервним процесом адаптації до динамічних змін технологічного середовища.

Процес цифрової трансформації у цьому контексті повинен бути зосереджений на створенні мережевих платформ взаємодії, щоб забезпечити необхідний рівень економічної безпеки – важливий спосіб зберегти бізнес в умовах швидкої зміни технологічного ландшафту. Такий підхід передбачає не лише впровадження сучасного обладнання або програмного забезпечення, але й суттєві зміни в підходах до управління, корпоративної культури та зовнішніх комунікацій.

Висновки та перспективи подальших розвідок у даному напрямі. Дослідження підтверджує, що забезпечення економічної безпеки підприємств в умовах цифрової трансформації вимагає комплексного підходу. Встановлено, що основними викликами є системні, структурні, галузеві, підприємницькі та особистісні загрози, особливо щодо захисту інформаційних активів.

Європейський досвід демонструє залежність підходів до управління цифровими ризиками від розміру підприємств та цифрової зрілості економік. Перспективним напрямком є розвиток механізмів страхування від кіберзагроз.

Запропоновано багатокомпонентний підхід до забезпечення безпеки, що враховує фінансову, інтелектуально-кадрову, техніко-технологічну, інформаційну та інші складові, які трансформуються в цифровому середовищі.

Перспективними напрямками подальших досліджень є розробка методики оцінки впливу цифровізації на рівень економічної безпеки, формування галузевих стандартів та вивчення адаптивних механізмів протидії кіберзагрозам в умовах гібридної війни.

Література

1. Боднар О.А. Модернізація фінансово-економічної безпеки підприємства в умовах цифровізації. Наукові перспективи. 2023. № 2 (32). С. 234-246.
2. Колесніков А. Практичний інструментарій формування економічної безпеки підприємств мережевих структур: інформаційно-аналітичний аспект. Вісник Хмельницького національного університету. Економічні науки. 2024. № 1. С. 71-76.

3. Бакай В.Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету. Економічні науки*. 2020. №4, Том 1. С. 32-35.

4. Тульчинська С., Солосіч О., Чорній В. Вплив діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства. *Інвестиції: практика та досвід*. 2021. № 9. С. 54-58.

5. Литовченко О. Ю. Забезпечення економічної безпеки підприємств в умовах цифрових трансформації. *Інтеграція освіти, науки та бізнесу в сучасному середовищі: зимові диспути: тези доповідей II Міжнародної науково-практичної інтернет-конференції (м. Дніпро, 4-5 лютого 2021 р.)*. С. 76-78.

6. Ляхович О., Оплачко І. Економічна безпека та транспарентність підприємств в умовах цифровізації. *Вісник НУБГП. Серія Економічні науки*. 2021. № 2 (94). С. 100-111.

7. Проскура В., Черничко Т., Верецький Д. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. № 4 (13). С. 61-67.

References

1. Bodnar, O.A. (2023), "Modernization of financial and economic security of the enterprise in the conditions of digitalization", *Naukovi perspektyvy*, vol. 2(32), pp. 234-246.

2. Kolesnikov, A. (2024), "Practical tools for forming economic security of network structure enterprises: information-analytical aspect", *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky*, vol. 1, pp. 71-76.

3. Bakai, V.Y. (2020), "Ensuring economic security of the enterprise based on the use of digital technologies", *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky*, vol. 4, part 1, pp. 32-35.

4. Tulchynska, S., Solosich, O. and Chornii, V. (2021), "The impact of digitalization of management processes on the system of ensuring economic security of the enterprise", *Investytsii: praktyka ta dosvid*, vol. 9, pp. 54-58.

5. Lytovchenko, O.Yu. (2021), "Ensuring economic security of enterprises in the conditions of digital transformations", *Intehratsiia osvity, nauky ta biznesu v suchasnomu seredovyshchi: zymovi dysputy: tezy dopovidei II Mizhnarodnoi naukovo-praktychnoi internet-konferentsii* [Integration of education, science and business in the modern environment: winter disputes: abstracts of the II International scientific-practical Internet conference], Dnipro, Ukraine, pp. 76-78.

6. Liakhovych, O. and Oplachko, I. (2021), "Economic security and transparency of enterprises in the conditions of digitalization", *Visnyk NUVHP. Seriia Ekonomichni nauky*, vol. 2(94), pp. 100-111.

7. Proskura, V., Chernychko, T. and Veretskyi, D. (2024), "Modern approaches to determining the level of economic security of the enterprise in the conditions of digitalization", *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 4(13), pp. 61-67.

Стаття надійшла до редакції 28.04.2025 р.