

УДК 323.321

DOI: https://doi.org/10.31521/modecon.V58(2026)-02

Бойко С. О., здобувач третього (освітньо-наукового) рівня вищої освіти, Національний транспортний університет, м. Київ, Україна

ORCID: 0009-0009-6736-9500

e-mail: boiko_asp@gsuite.duit.edu.ua

Роль цифрових технологій у забезпеченні економічної безпеки сучасного підприємства

Анотація. У статті досліджено вплив цифрової економіки на формування та зміцнення економічної безпеки підприємств. Обґрунтовано, що розвиток цифрових технологій, зокрема хмарних обчислень, великих даних, штучного інтелекту, блокчейну та Інтернету речей, створює нові можливості для підвищення ефективності управління, оптимізації витрат і посилення конкурентних переваг підприємств. Водночас цифровізація зумовлює появу нових загроз, серед яких кібератаки, витоки конфіденційної інформації, цифрове шахрайство, порушення функціонування інформаційних систем і зростання залежності від ІТ-інфраструктури.

Доведено, що більшість підприємств активно впроваджують цифрові технології, однак рівень готовності до протидії цифровим ризикам залишається недостатнім. Традиційні підходи до управління економічною безпекою не повною мірою враховують особливості функціонування бізнесу в цифровому середовищі, що ускладнює своєчасне виявлення, оцінювання та нейтралізацію ризиків.

Розкрито сутність економічної безпеки підприємства як інтегрованого стану захищеності від внутрішніх і зовнішніх загроз, що забезпечує стабільність діяльності та довгострокову конкурентоспроможність. Визначено роль цифрових технологій у підвищенні рівня економічної безпеки через автоматизацію процесів, удосконалення системи контролю, прогнозування ризиків, підтримку управлінських рішень і підвищення прозорості діяльності.

На основі статистичних даних встановлено, що у 2025 році понад 53% підприємств ЄС використовують цифрові бізнес-системи, рівень впровадження хмарних технологій сягає 90%, близько 78% компаній перебувають на етапі цифрової трансформації, а в Україні лише 6% підприємств є повністю цифровізованими.

Систематизовано основні цифрові інструменти забезпечення економічної безпеки підприємства, зокрема ERP-системи, BI-аналітику, технології кіберзахисту та платформи управління ризиками. Запропоновано практичні заходи підвищення рівня економічної безпеки, серед яких формування стратегії цифрової безпеки, аудит ризиків, підвищення цифрової грамотності персоналу, впровадження багаторівневого кіберзахисту, резервування даних, постійний моніторинг операцій у режимі реального часу та вдосконалення системи управління цифровими ризиками підприємств.

Ключові слова: цифрові технології, економічна безпека, Україна, загрози, інструменти, методи, управління.

Boyko Svyatoslav, applicant for the third (educational and scientific) level of higher education, National Transport University, Kyiv, Ukraine

The Role of Digital Technologies in Ensuring the Economic Security of Modern Enterprises

Abstract. Introduction. This article examines the transformative impact of the digital economy on the development and strengthening of enterprises' economic security. The rapid advancement of digital technologies, including cloud computing, big data, artificial intelligence, blockchain, and the Internet of Things, creates significant opportunities for improving management efficiency, optimizing costs, and enhancing business competitiveness. At the same time, digitalization generates new threats, such as cyberattacks, confidential data breaches, information system failures, digital fraud, and increasing dependence on IT infrastructure, requiring enterprises to reconsider existing approaches to economic security management.

Purpose. The purpose of the study is to investigate the impact of digital transformation on enterprises' economic security, identify the main digital risks and opportunities, and determine effective digital tools and management approaches for strengthening enterprise resilience in the digital environment.

Results. The study demonstrates that although most enterprises actively implement digital technologies, their readiness to manage digital risks remains insufficient. Traditional economic security management approaches do not adequately address the specific features of digital business processes, creating a gap between the pace of digital transformation and the development of security management mechanisms. The essence of enterprise economic security is defined as an integrated state of protection against internal and external threats that ensures operational stability and long-term competitiveness. It is established that digital technologies contribute to strengthening economic security by automating business processes, improving management transparency, enhancing control systems, forecasting risks, and supporting informed managerial decision-making. Statistical evidence indicates that by 2025 more than 53% of EU enterprises use digital business systems (ERP, CRM, BI), approximately 90% have adopted cloud technologies, and between 40% and 78% employ artificial intelligence solutions, while about 78% of companies worldwide are actively undergoing digital transformation. In Ukraine, digitalization remains uneven, with only 6% of enterprises reaching a high level of digital maturity. The research systematizes the principal digital tools for ensuring economic security, including ERP systems, business intelligence analytics, cybersecurity technologies, and digital risk management platforms,

¹Стаття надійшла до редакції: 02.07.2026

Received: 2 July 2026

and substantiates their role in ensuring business continuity, reducing financial losses, increasing operational transparency, and preventing crisis situations.

Conclusions. The study concludes that ensuring enterprise economic security under conditions of digital transformation requires an integrated management approach combining technological innovation with comprehensive risk management. The implementation of digital security strategies, continuous risk assessment, improvement of employees' digital competencies, deployment of multi-layered cybersecurity systems, reliable data backup, and real-time monitoring are identified as the key priorities for enhancing enterprise resilience, sustainable development, and long-term competitiveness in the digital economy.

Keywords: digital technologies, economic security, Ukraine, threats, tools, methods, management.

JEL Classification: D81, L25, O33, M15.

Постановка проблеми. Умови цифрової економіки кардинально змінюють підходи до формування та підтримання економічної безпеки підприємств. Швидкий розвиток цифрових технологій - таких як хмарні обчислення, великі дані, штучний інтелект, блокчейн та інтернет речей - створює для бізнесу нові можливості підвищення ефективності, оптимізації витрат і посилення конкурентних позицій. Проте саме цифровізація стає джерелом принципово нових загроз, пов'язаних із кібератаками, витоками даних, порушенням роботи інформаційних систем, шахрайством у цифрових каналах та зростанням залежності підприємства від цифрової інфраструктури.

Більшість підприємств активно впроваджують цифрові рішення, проте рівень готовності до протидії цифровим ризикам залишається недостатнім. У практиці управління економічною безпекою все ще домінують традиційні методи, які не враховують зміненої логіки функціонування бізнес-процесів у цифровому середовищі. Виникає суперечність між швидким темпом цифрової трансформації та відставанням механізмів забезпечення економічної безпеки, що ускладнює своєчасне виявлення загроз, оцінку цифрових ризиків і розробку адекватних методів захисту.

Отже, проблема полягає у недостатній науково обґрунтованій оцінці ролі цифрових технологій у забезпеченні економічної безпеки сучасного підприємства та необхідності формування комплексного підходу, який би поєднував можливості цифровізації з ефективними механізмами запобігання загрозам і мінімізації їхніх наслідків.

Аналіз останніх досліджень і публікацій. У науковій літературі накопичено значний теоретичний доробок, присвячений сутності, структурі, управлінню та механізмам забезпечення економічної безпеки, а також специфіці формування їх стратегії. Вагомий внесок у розвиток цієї тематики зробили такі дослідники, як Левченко О., Вовк М., Юрченко Н. Гаврилюк А. [1], Дуднев Ю., Артем'єв О., Дячков Д., Потапюк І., Капран І., Колісниченко П., Ушенко Н., Ліпкан В., Васильців Т., Ілляшенко О., Онищенко В., Мельник С., Рибальченко Л., Терещенко Е., Кондратенко Н., Трембач Р., Копилюк О., Гузар У., Гута С., Кравченко О., Гаврилюк О., Челомбітько О., Бойко С., Масюк Ю., Огренич Ю., Зайцев Є, Шило Ж. [2] та інші. Окремий напрям сучасних наукових досліджень пов'язаний із вивченням впливу цифровізації на забезпечення економічної безпеки

підприємств, зокрема використання цифрових технологій, цифрових платформ, інформаційно-аналітичних систем і цифрових інструментів управління ризиками, що знайшло відображення у працях Проскури В. Ф., Черничко Т. В., Верецького Д. З. [3], Бакая В. Й. [4], Поліни В. Пузирьової [5], Халіни О., Шмагало В. [6] та інших дослідників.

Зарубіжні вчені, серед яких А. Барні, Р. Каплан, М. Портер, Д. Норт, розглядають економічну безпеку через призму стратегічних переваг, конкурентоспроможності та ефективності управління, акцентуючи увагу на інструментах раннього виявлення ризиків і формуванні довгострокової стійкості підприємства.

Сучасні дослідження, наприклад, С. Мельника та І. Штангрета [7] та інших, інтегрують у традиційні підходи аспекти цифрової трансформації, підкреслюючи зростання цифрових ризиків, зміну ринку праці, необхідність підвищення цифрової зрілості та впровадження інноваційних технологій у систему забезпечення економічної безпеки. Однак, недостатньо дослідженими залишаються питання практичної інтеграції цифрових технологій у систему економічної безпеки підприємства, зокрема у контексті зростання кіберзагроз, ускладнення бізнес-процесів та появи нових форм цифрових ризиків. Бракує комплексних підходів, що поєднують традиційні інструменти забезпечення безпеки з сучасними цифровими рішеннями та дозволяють оперативно реагувати на зміни зовнішнього середовища.

Формулювання цілей дослідження. Метою дослідження є визначення ролі цифрових технологій у формуванні та зміцненні економічної безпеки підприємства, а також обґрунтування напрямів їх ефективного використання для мінімізації цифрових ризиків і підвищення конкурентоспроможності бізнесу.

Виклад основного матеріалу дослідження. Цифрові технології є ключовим фактором підвищення стійкості підприємства. Вони забезпечують швидкість обробки інформації, точність управлінських рішень, зниження людського фактору, автоматизований контроль за ресурсами, підвищення ефективності бізнес-процесів. У сучасних умовах без цифрових технологій неможливо забезпечити фінансову, інформаційну, операційну та стратегічну складові економічної безпеки.

Економічна безпека підприємства розуміється як інтегрований стан його захищеності від внутрішніх і зовнішніх ризиків, який гарантує стабільність роботи та ефективність розвитку. Її сутність полягає у зменшенні фінансових, операційних та стратегічних загроз, що можуть завдати шкоди діяльності підприємства [1; 3]. У межах економічної безпеки здійснюється контроль за ресурсами, активами та рухом капіталу з метою їхнього збереження та раціонального використання. Вона передбачає функціонування дієвої системи управління ризиками й ухвалення своєчасних та обґрунтованих управлінських рішень.

При цьому економічна безпека враховує вплив зовнішнього середовища - ринкові флуктуації, зміни у правовому полі та конкурентний тиск. Вона виступає ключовою умовою підтримання стійкості та довгострокової конкурентоспроможності підприємства [2]. Таким чином, економічна безпека є базисом для сталого розвитку й результативного функціонування підприємства в сучасних економічних умовах.

Цифрова трансформація суттєво змінює підходи до формування та зміцнення економічної безпеки, забезпечуючи оперативний контроль за фінансовими потоками й ресурсами. Вона дає змогу автоматизувати процеси оцінювання ризиків, своєчасно виявляти загрози та реагувати на них на ранніх етапах. Використання аналітичних платформ та технологій Big Data підвищує обґрунтованість управлінських рішень.

Цифрові технології покращують точність внутрішнього аудиту, посилюють контроль за операційними процесами та сприяють інтеграції структурних підрозділів у єдиний інформаційний простір, що пришвидшує реагування на будь-які види загроз [4; 5].

Окрім цього, цифрова трансформація знижує ризики шахрайства та нецільового використання ресурсів, створює інструментарій для прогнозування можливих криз та розроблення антикризових рішень. Її впровадження покращує взаємодію між персоналом і технологічними системами, підвищуючи загальну стійкість підприємства та його конкурентні позиції на ринку [5].

У підсумку цифрова трансформація виступає одним із визначальних чинників розвитку економічної безпеки підприємства.

Як інструмент забезпечення економічної безпеки, цифровізація охоплює сукупність заходів і технологічних рішень, спрямованих на автоматизацію управління, підвищення прозорості фінансових та операційних процесів, а також на своєчасне виявлення й мінімізацію ризиків. Це включає застосування сучасних інформаційних систем, аналітичних платформ, великих даних і засобів кіберзахисту для контролю за ресурсами підприємства.

Цифровізація забезпечує інтеграцію окремих підрозділів у єдину інформаційну систему, що дає змогу оперативно отримувати дані та приймати

ефективні управлінські рішення. Вона підвищує швидкість реагування на зовнішні та внутрішні загрози, зменшує ймовірність фінансових втрат і шахрайських дій. Крім того, цифрові інструменти сприяють прогнозуванню кризових явищ і формуванню антикризових стратегій, а також забезпечують постійний моніторинг та контроль за виконанням планових показників і нормативів [3,8].

Вплив цифровізації на формування та зміцнення економічної безпеки підприємства можна описати за такими основними напрямками [3-5], що показано на рис.1. Даний вплив проявляється через формування нових можливостей для управління ризиками, підвищення ефективності використання ресурсів та забезпечення адаптивності до змін зовнішнього середовища. Впровадження цифрових технологій забезпечує оперативний збір, обробку та аналіз інформації, що дозволяє своєчасно ідентифікувати потенційні загрози та приймати обґрунтовані управлінські рішення. Використання інформаційно-аналітичних систем сприяє підвищенню прозорості бізнес-процесів, автоматизація операцій – оптимізації витрат і зниженню операційних ризиків, а цифрові інструменти кіберзахисту – мінімізації інформаційних загроз.

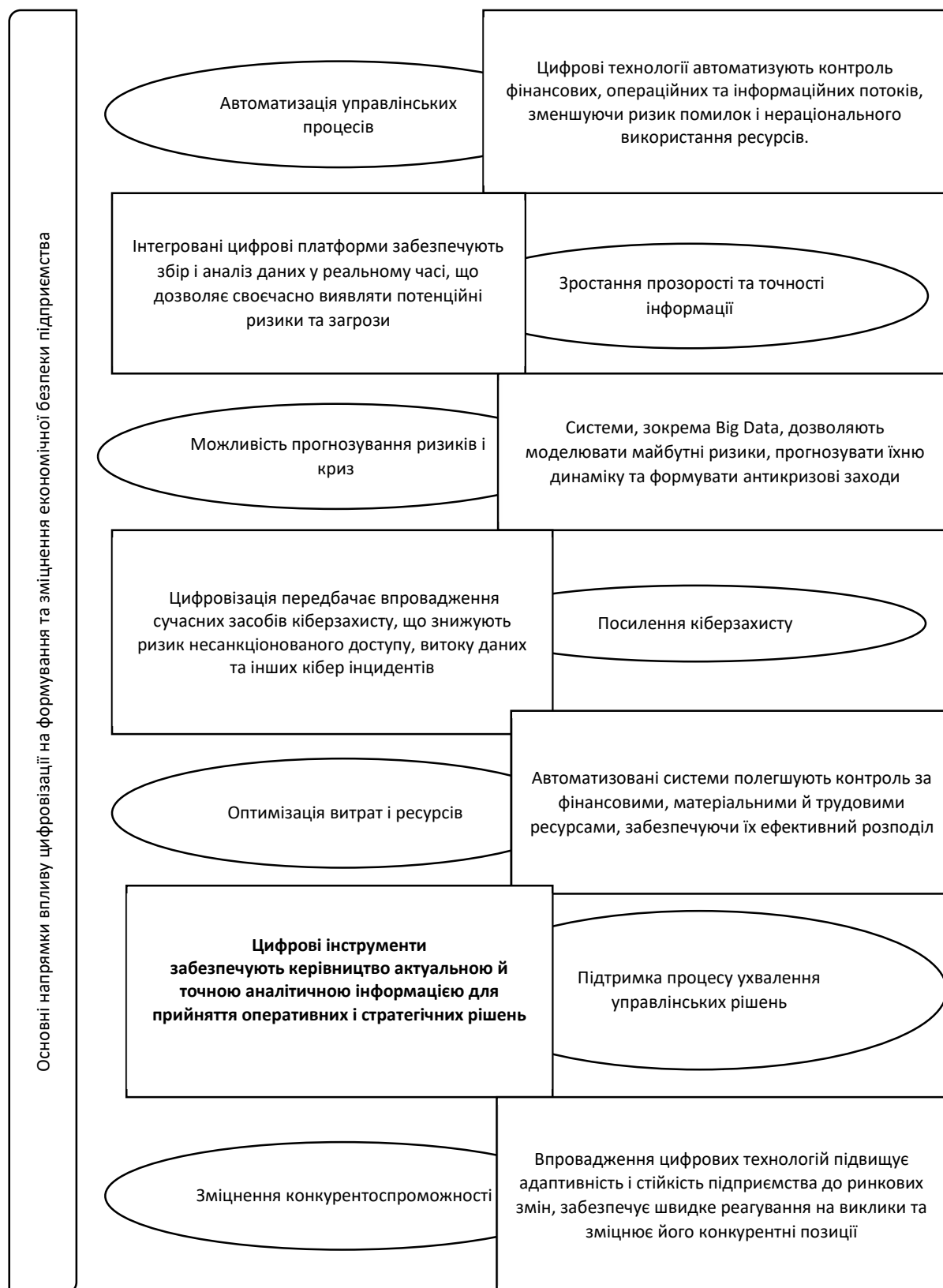


Рисунок 1 - Основні напрямки впливу цифровізації на формування та зміцнення економічної безпеки підприємства
 Джерело: [3-5].

Таким чином, цифровізація виступає не лише фактором технологічного розвитку підприємства, а й важливим інструментом посилення його економічної безпеки через підвищення стійкості, конкурентоспроможності та здатності адаптуватися до трансформаційних змін.

Статистично встановлено, що станом на 2024 р. світовий ринок цифрової трансформації оцінювався приблизно у 1,07 трлн USD, а до 2030 р. прогнозується його збільшення до 4,62 трлн USD при середньорічному темпі зростання близько 28,5 %. Це свідчить про суттєве зростання інвестицій підприємств у цифрові технології з метою підвищення ефективності, прозорості бізнес-процесів та рівня економічної безпеки.

У 2025 р. понад 53% підприємств ЄС використовують цифрові бізнес-системи (ERP/CRM/BI), 46,5% підприємств використовують ERP - системи, 28,5% - CRM, 16,3% - BI-аналітику, а 90% організацій впровадили хмарні технології. Світові витрати на цифрову трансформацію досягли \$5,7 трлн у 2025 р. [9,10].

Близько 78% компаній у світі перебувають у фазі активної цифрової трансформації, а частка підприємств, що застосовують штучний інтелект, сягає 40-78%. Понад 75% підприємств використовують хмарні сервіси, Big Data або AI як основу цифровізації (ціль ЄС до 2030 р.) [10,11].

ЄС планує, щоб до 2030 р.: 90% МСП мали базовий рівень цифровізації, а 75% компаній використовували AI/Big Data/Cloud.

Очікується, що цифрова трансформація стане основним фактором конкурентоспроможності підприємств у найближчі 5-10 років. Прогнози для українських малих і середніх підприємств також демонструють поступове зростання цифрової зрілості. Аналітичні оцінки передбачають, що до 2030 р. рівень впровадження базових цифрових технологій (хмарні рішення, автоматизація) може зрости до 81 %, використання аналітики на основі AI - до 35 %, а частка МСП, залучених до цифрових проєктів, збільшиться до 48 % порівняно із приблизно 21 % у 2025 р. Водночас прогнозується покращення ключових результатів діяльності підприємств: зростання доходів на 8 %, продуктивності - на 8 %, скорочення витрат - на 6 %, а частка цифрових інвестицій у загальному бюджеті може сягнути 30 % [11,12].

Окремо слід відзначити швидке зростання ринку штучного інтелекту: за оцінками, до 2030 р. його обсяг може перевищити 4,2 трлн USD, з яких близько 1,9 трлн USD формуватиметься за рахунок корпоративного використання AI у бізнес-процесах. Це свідчить про стратегічну роль AI у формуванні конкурентоспроможності та підвищенні рівня економічної безпеки підприємств [11, 13].

В Україні рівень цифровізації залишається нижчим: лише 6% підприємств є повністю цифровізованими, тоді як 51% перебувають на частковому рівні цифрової

трансформації, а 31% - на початковому його рівні [14,15].

У результаті впровадження цифрових технологій зростає адаптивність та стійкість підприємства до змін ринкового середовища. Компанії, які активно використовують інноваційні рішення, демонструють вищу конкурентоспроможність, швидше реагують на зовнішні виклики та здатні ефективніше протистояти загрозам. Прикладами таких технологій є ERP-системи, системи BI-аналітики, модулі кіберзахисту, автоматизовані платформи управління ризиками тощо. Наприклад, ERP-системи забезпечують комплексне управління фінансовими, виробничими, логістичними та кадровими процесами підприємства. Завдяки інтеграції всіх підсистем в єдиний інформаційний простір, ERP-рішення дають змогу не лише контролювати рух ресурсів у реальному часі, а й оперативно виявляти відхилення від планових показників. Це мінімізує ризики фінансових втрат і сприяє підвищенню прозорості операційної діяльності.

Важливу роль відіграють і системи BI-аналітики, які дозволяють формувати глибокі аналітичні звіти, візуалізувати дані та здійснювати оперативне моделювання різних сценаріїв розвитку подій. Завдяки використанню алгоритмів машинного навчання такі системи здатні прогнозувати можливі загрози - наприклад, порушення ланцюгів постачання, зростання дебіторської заборгованості чи зміни в ринковому середовищі. Це дає підприємству змогу впроваджувати превентивні заходи та підвищувати стійкість до кризових ситуацій [16].

Практичним підтвердженням впливу цифрових технологій на зміцнення економічної безпеки є досвід провідних міжнародних компаній. Так, наприклад, BMW Group використовує ERP-рішення на базі SAP S/4HANA, що забезпечує інтеграцію виробничих, фінансових і логістичних процесів в єдину інформаційну систему. Використання цифрової платформи дозволило компанії підвищити прозорість ланцюгів постачання, стандартизувати операційні процеси, швидше реагувати на зміни попиту та ризики у виробничо-логістичній діяльності [17].

Аналогічно, використання хмарних технологій та аналітичних платформ у BMW Group забезпечує обробку великих обсягів даних у режимі реального часу, що сприяє прогнозуванню можливих відхилень, оптимізації ресурсів та прийняттю управлінських рішень на основі даних. Досвід таких компаній демонструє, що цифровізація виступає не лише фактором технологічної модернізації, а й інструментом зниження операційних, фінансових та інформаційних ризиків, що безпосередньо впливає на зміцнення економічної безпеки підприємства [18].

Не менш важливими є модулі кіберзахисту, що включають системи виявлення вторгнень, засоби шифрування, інструменти багатофакторної автентифікації та автоматизовані системи моніторингу інформаційних інцидентів. Їх використання забезпечує

захист конфіденційних даних від кібератак, несанкціонованого доступу та внутрішніх загроз. У сучасних умовах кіберризиків ці модулі формують основу інформаційної безпеки підприємства та значною мірою впливають на загальний рівень економічної безпеки.

Окреме значення мають автоматизовані платформи управління ризиками (Risk Management Platforms), що забезпечують системний підхід до ідентифікації, оцінювання, моніторингу та нейтралізації ризиків. Їх функціонал дозволяє формувати реєстри ризиків, визначати пріоритетність

загроз, контролювати ефективність впроваджених заходів і моделювати наслідки можливих відхилень. Використання таких платформ посилює антикризове управління та сприяє підвищенню надійності бізнес-процесів.

У сукупності ці цифрові інструменти забезпечують створення комплексної системи економічної безпеки, що працює на основі даних, автоматизації та проактивного управління ризиками [19].

Найбільш поширені загрози, що впливають на економічну безпеку підприємства наведені на рис. 2.

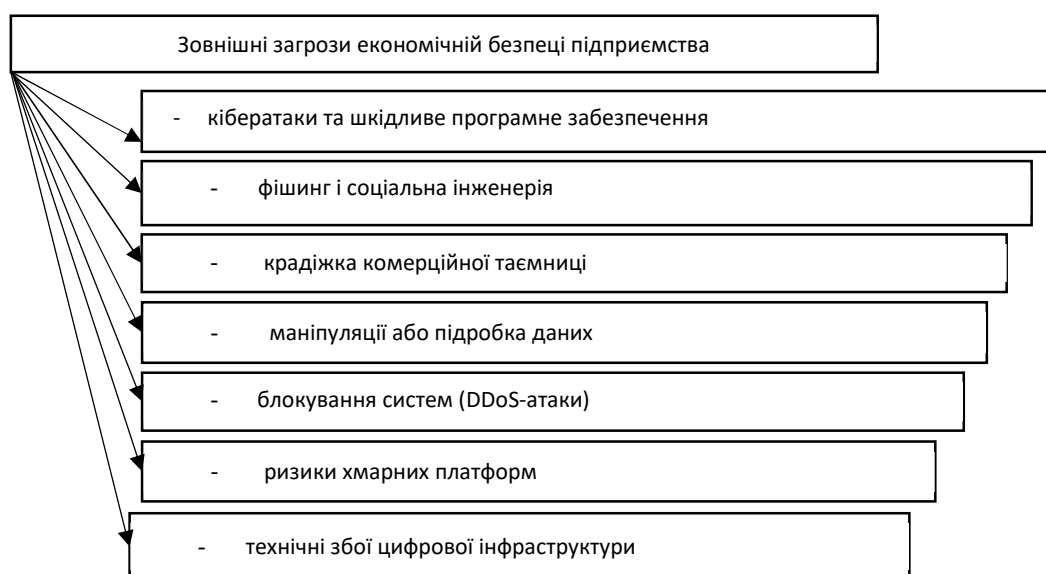


Рисунок 2 - Ключові зовнішні загрози, що впливають на економічну безпеку підприємства

Джерело: [19].

Дані загрози здатні спричиняти суттєві фінансові втрати, що проявляються у прямих витратах на відновлення інформаційних систем, простої виробничих і управлінських процесів, штрафних санкціях та втраті прибутку через зниження операційної ефективності. Окрім того, вони можуть призводити до порушення безперервності діяльності підприємства, збоїв у ланцюгах постачання, втрати доступу до критично важливих даних і блокування ключових бізнес-процесів, що в окремих випадках паралізує роботу організації. Не менш важливим наслідком є руйнування ділової репутації

підприємства, зниження рівня довіри з боку клієнтів, партнерів та інвесторів, а також погіршення його позицій на ринку, що в довгостроковій перспективі може призвести до втрати конкурентоспроможності та скорочення ринкової частки. Для зниження цифрових ризиків підприємства впроваджують інструменти цифрового забезпечення економічної безпеки, що наведені на рис. 3. Для підвищення економічної безпеки підприємства у цифровому середовищі доцільно реалізовувати комплекс заходів, спрямованих на зниження цифрових ризиків та посилення стійкості бізнес-процесів [6,19], а саме:

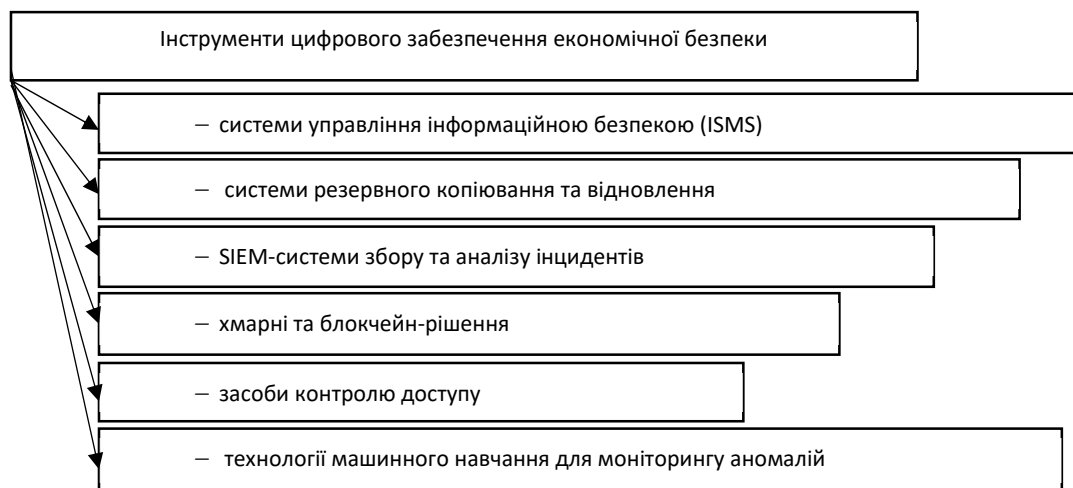


Рисунок 3 - Інструменти цифрового забезпечення економічної безпеки

Джерело: [6, 19].

1. Формувати стратегію цифрової безпеки. Підприємству необхідно розробляти довгострокову стратегію, що визначає ключові цифрові ризики, пріоритети їх мінімізації та механізми реагування на інциденти. Така стратегія має включати політики доступу, правила поведінки з інформаційними ресурсами, а також стандарти безпечної роботи з даними.

2. Регулярно проводити аудит цифрових ризиків. Систематична оцінка цифрових загроз дає змогу визначити вразливі місця, оцінити рівень ймовірних збитків та розробити ефективні заходи контролю. Аудит включає аналіз IT-інфраструктури, бізнес-процесів, політик безпеки та інцидентів, що вже мали місце.

3. Навчати персонал основам кібергігієни. Людський фактор залишається одним із найбільших джерел ризиків, тому важливо підвищувати цифрову грамотність працівників. Навчання має охоплювати правила безпечного використання корпоративних ресурсів, виявлення фішингових атак, управління пароллями та реагування на підозрілі дії в системах.

4. Впроваджувати багаторівневі системи кіберзахисту, тобто доцільно використовувати комплекс рішень, що включають міжмережеві екрани, системи виявлення вторгнень, шифрування даних, багатофакторну автентифікацію та автоматизований моніторинг подій безпеки. Такий підхід мінімізує ризики кібератак і витоку інформації.

5. Забезпечувати резервування даних. Регулярне створення резервних копій дає змогу захистити критичні дані від втрати внаслідок технічних збоїв, кібератак або людських помилок. Доцільно

використовувати географічно розподілені сховища, а також тестувати працездатність резервних копій для гарантування їх відновлення.

6. Моніторити операції в режимі реального часу. Застосування цифрових систем моніторингу дозволяє відстежувати транзакції, операційні процеси та стан IT-інфраструктури в реальному часі. Це забезпечує своєчасне виявлення аномалій, спроб несанкціонованого доступу та інших подій, що становлять загрозу економічній безпеці.

Висновки та перспективи подальших досліджень. Дослідження підтверджують, що цифрові технології стають ключовим фактором формування та зміцнення економічної безпеки підприємства. Цифрові інструменти - ERP-системи, BI-аналітика, модулі кіберзахисту, платформи управління ризиками - підвищують точність управління, забезпечують контроль ресурсів у реальному часі, зменшують ризики фінансових втрат і шахрайства, а також дають змогу прогнозувати можливі загрози. Вони формують основу проактивного управління ризиками та зміцнюють загальну стійкість підприємства.

Цифровізація створює нову модель економічної безпеки, у якій провідну роль відіграють аналітика, автоматизація та захист інформаційних активів. Підприємства, що інтегрують цифрові технології в систему економічної безпеки, підвищують свою адаптивність до ринкових змін і довгострокову конкурентоспроможність. Таким чином, цифрова трансформація стає необхідною умовою сталого розвитку та ефективного функціонування бізнесу в сучасному середовищі.

Література:

1. Левченко О.М., Вовк М.О., Юрченко Н.І. Гаврилюк А.Р. Діагностика системи управління фінансово-економічною безпекою конкурентоспроможних підприємств агропродовольчої сфери в умовах цифровізації. *Агросвіт*. 2024. Вип. 4. С. 22-30.. URL: <https://doi.org/10.32702/2306-6792.2024.4.22>.
2. Шило Ж. С. Методи оцінки рівня економічної безпеки підприємства: підходи до оцінювання та забезпечення економічної безпеки. *Вісник НУВГП. Серія «Економічні науки»*. 2022. Вип. 2(98), С. 278-288. URL: <https://ep3.nuwm.edu.ua/24406/1/Ve9824%20%281%29.pdf>.
3. Проскура В. Ф., Черничко Т. В., Веретський Д.З. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024, Вип. 4(13), С. 61–67. URL: <https://doi.org/10.32782/dees.13-9>.
4. Бакай В.Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. 2020. Вип. 4. Т. 1, С. 32-35. URL: <https://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/7-19.pdf>.
5. Поліна В. Пузырьова. Механізм забезпечення економічної безпеки у сфері сталого розвитку фінансової системи держави в умовах цифрової економіки та глобалізаційних змін. *Публічне управління та адміністрування*. 2025. Вип. 1(283). С. 189-204. URL: https://eco-science.net/wp-content/uploads/2025/01/1.25._topic_Polina-V.-Puzyrova-189-204-1.pdf.
6. Халіна О., Шмагало В. Стратегія розвитку економічної безпеки підприємств в умовах цифрових трансформацій. *Економіка та суспільство*. (73). 2025. URL: <https://doi.org/10.32782/2524-0072/2025-73-138>.
7. Мельник С. Ірина Штангрет. Економічна безпека підприємства в умовах цифрової трансформації економіки: теоретичні та практичні аспекти: Львів, Растр-7, 2025. с. 256. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/8735>.
8. Білоус С. П., Супрун Д. А., Перепелиця Є. В. Інтеграція цифрових технологій у маркетингові процеси: виклики та перспективи. *Економічний простір*. 2024. Вип. 195, С. 154-158. URL: <https://economicspace.pgasa.dp.ua/article/view/317855>.
9. Digital economy and society statistics – enterprises. *Statistics Explained*. 2026. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises.
10. Цифрова трансформація - статистика та факти. *Statista*. 2025. URL: https://www.statista.com/topics/6778/digital-transformation/?utm_source=chatgpt.com&srltid=AfmBOooi4Otn4K08_hCAHWaXiSCNVc5EDb_jsYuL5HIJ4Pb8J_xjiuGT
11. Цифровізація в Європі – видання 2025 року. *Eurostat*. 2025. URL: <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025>.
12. Підвищення стійкості шляхом стимулювання цифрової трансформації бізнесу в Україні, *OECD Publishing*, Париж, 2024. URL: <https://doi.org/10.1787/4b13b0bb-en>.
13. Europe's Digital Decade: digital targets for 2030 – Documents. *European Commission*. 2023. URL: https://commission.europa.eu/europes-digital-decade-digital-targets-2030-documents_en?utm_source=chatgpt.com.
14. Цифрова трансформація прискорюється в багатьох галузях. *PSglobal*. 2025. URL: https://psglobals.com/insights/news/digital-transformation-acceleration/?utm_source=chatgpt.com.
15. Каленюк І., Цимбал Л., Челіка М. (2025). Цифрова трансформація бізнесу: тенденції та можливості в Україні. *Балтійський журнал економічних досліджень*. 11(5). URL: <http://baltijapublishing.lv/index.php/issue/article/view/3076>.
16. ERP та BI: ключові відмінності та як вони функціонують разом. *SelectHub*: URL: https://www.selecthub.com/enterprise-resource-planning/erp-bi/?utm_source=chatgpt.com.
17. BMW Group and SAP SE. Successful go-live of new production IT at BMW Group in cooperation with SAP SE. *BMW Group*. 2023. URL: <https://www.press.bmwgroup.com/global/article/detail/T0436900EN/successful-go-live-of-new-production-it-at-bmw-group-in-cooperation-with-sap-se>.
18. BMW Group chooses RISE with SAP to drive business transformation. *BMW Group*. 2023. URL: <https://news.sap.com/2023/01/bmw-group-chooses-rise-with-sap-to-drive-business-transformation/>
19. Пані Рупеш. Рішення та практики кібербезпеки: брандмауери, виявлення/запобігання втручень, шифрування, багатофакторська автентифікація. *Академічний журнал з інновацій та сталого розвитку в бізнес-адмініструванні*. 2024. 4(3) С.37-52.

References:

1. Levchenko, O. M., Vovk, M. O., Yurchenko, N.I. & Havrylyuk, A. R. (2024). Diagnostics of the financial and economic security management system of competitive agri-food enterprises in the context of digitalization, *Agrosvit*, 4, 22-30. <https://doi.org/10.32702/2306-6792.2024.4.22>.
2. Shylo, ZH. S. (2022). Methods for assessing the level of economic security of an enterprise: approaches to assessing and ensuring economic security. *Bulletin of the National University of Economics and Business. Series "Economic Sciences"*, 2(98), 278–288. <https://ep3.nuwm.edu.ua/24406/1/Ve9824%20%281%29.pdf>.
3. Proskura, V. F., Chernychko, T. V., Verets'kyi, D. Z. (2024). Modern approaches to determining the level of economic security of an enterprise in the context of digitalization. *Digital Economy and Economic Security*, 4(13), 61-67. <https://doi.org/10.32782/dees.13-9>.
4. Bakay, V. Y. (2020). Ensuring the economic security of an enterprise based on the use of digital technologies. *Bulletin of the Khmelnytsky National University*, 4, 1, 32-35. <https://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/7-19.pdf>.
5. Polina, V. Puzyr'ova. (2025). Mechanism for ensuring economic security in the sphere of sustainable development of the state financial system in the context of the digital economy and globalization changes. *Public Management and Administration*, 1(283), 189-204. https://eco-science.net/wp-content/uploads/2025/01/1.25._topic_Polina-V.-Puzyrova-189-204-1.pdf.
6. Khalina, O., Shmahalo, V. (2025). Strategy for the development of economic security of enterprises in the context of digital transformations. *Economy and Society*, (73). <https://doi.org/10.32782/2524-0072/2025-73-138>.
7. Mel'nyk, S. Iryna, Shtanhret. (2025). Ekonomichna bezpeka pidpryyemstva v umovakh tsyfrovoyi transformatsiyi ekonomiky: teoretychni ta praktychni aspekty. L'viv, Rastr-7. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/8735>.

8. Bilous, S. P., Suprun, D. A., Perepelytsya, YE. V. (2024). Integration of digital technologies into marketing processes: challenges and prospects. *Economic Space*, 195, 154-158. <https://economicspace.pgasa.dp.ua/article/view/317855>.
9. Statistics Explained. (2026, february). Digital economy and society statistics – enterprises. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises.
10. Statista. (2025, december 17). Digital Transformation: Facts and Figures. https://www.statista.com/topics/6778/digital-transformation/?utm_source=chatgpt.com&srsId=AfmBOooi4Otn4K08_hCAHWaXiSCNVc5EDb_jsYuL5HiJ4Pb8J_xjiuGT.
11. Eurostat. (2025). Digitalisation in Europe – 2025 edition. <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025>.
12. OECD Publishing, Paris. (2024). Enhancing Resilience by Stimulating Digital Business Transformation in Ukraine. <https://doi.org/10.1787/4b13b0bb-en>.
13. European Commission. (2023). Europe's Digital Decade: digital targets for 2030 – Documents. https://commission.europa.eu/europes-digital-decade-digital-targets-2030-documents_en?utm_source=chatgpt.com.
14. PSglobal. (2025, May, 19). Digital transformation is accelerating in many industries. 2025. https://psglobals.com/insights/news/digital-transformation-acceleration/?utm_source=chatgpt.com.
15. Kalenyuk, I., Tsymbal, L., Chelika M. (2025). Digital Business Transformation: Trends and Opportunities in Ukraine. *Baltic Journal of Economic Research*, 11(5). <http://baltijapublishing.lv/index.php/issue/article/view/3076>.
16. SelectHub. (2026, march). ERP and BI: Key Differences and How They Work Together. https://www.selecthub.com/enterprise-resource-planning/erp-bi/?utm_source=chatgpt.com.
17. BMW Group. (2023, September, 8). BMW Group and SAP SE. Successful go-live of new production IT at BMW Group in cooperation with SAP SE. <https://www.press.bmwgroup.com/global/article/detail/T0436900EN/successful-go-live-of-new-production-it-at-bmw-group-in-cooperation-with-sap-se>.
18. BMW Group. (2023, january, 30). BMW Group chooses RISE with SAP to drive business transformation. URL: <https://news.sap.com/2023/01/bmw-group-chooses-rise-with-sap-to-drive-business-transformation/>
19. Rupesh, Pani (2024). Cybersecurity Solutions and Practices: Firewalls, Intrusion Detection/Prevention, Encryption, Multi-Factor Authentication. *Academic Journal of Innovation and Sustainability in Business Administration*, 4(3), 37-52.



Ця робота ліцензована Creative Commons Attribution 4.0 International License