

DOI: <https://doi.org/10.32782/2524-0072/2026-89-16>

УДК 338.2:004.9:658.14/.17

ЦИФРОВІЗАЦІЯ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

DIGITALIZATION AS A MEANS OF ENSURING THE ECONOMIC SECURITY OF ENTERPRISES

Ровінський Олександр Олександрович

аспірант,

Запорізький національний університет

ORCID: <https://orcid.org/0009-0008-5854-0364>**Rovinskyi Oleksandr**

Zaporizhzhia National University

У статті комплексно досліджено цифровізацію як провідний інструмент захисту сучасних підприємств від внутрішніх та зовнішніх загроз. Оцінено її безпосередній вплив в умовах високої мінливості ринку, воєнних ризиків та суттєвої активізації кіберзагроз. Доведено підвищення безпеки бізнесу через побудову прозорого автоматизованого контролю фінансових потоків. Охарактеризовано ключові процеси управління матеріальними ресурсами, взаємодії з контрагентами та моніторингу персоналу. Систематизовано безпековий вплив впровадження ERP та CRM-платформ на стабільність бізнес-моделі компанії. Визначено роль сучасних систем BI-аналітики, хмарних технологій та електронного документообігу. Сформовано поетапну модель інтеграції цифрових технологій в загальну архітектуру безпеки суб'єкта господарювання. Вона включає аудит ризиків, побудову карти загроз, вибір рішень та навчання працівників. Запропоновано прикладні метрики оцінювання ефективності впроваджених трансформацій з метою забезпечення довгострокової конкурентоспроможності бізнесу в умовах нестабільного середовища.

Ключові слова: цифровізація, економічна безпека, підприємство, кібербезпека, цифрові технології, управління ризиками, інформаційна безпека, конкурентоспроможність.

The article examines the strategic and operational role of digitalization in building a resilient economic security system for modern commercial enterprises. The relevance of this academic study is determined by extreme market volatility, systemic wartime risks, structural disruptions in supply chains, and the rapid growth of sophisticated cyber threats. Under such conditions, traditional security and internal control procedures lack the necessary speed, flexibility, and depth. Modern digital instruments transform information into a core asset for risk prevention and tactical decision-making. The main purpose of this research is to justify the multifaceted impact of advanced digital technologies on mitigating corporate threats and to present a structured model for integrating digital solutions into the enterprise protective infrastructure. The methodological foundation of the study includes systematic analysis, comparative synthesis, logical modeling, and the interpretation of actual economic indicators from official international databases. The research results indicate that digitalization deeply transforms and reinforces key functional components of economic security, including financial stability, informational integrity, human resources safety, operational efficiency, and legal protection. Special attention is dedicated to the impact of complex ERP platforms, CRM systems, business intelligence architectures, cloud storage models, automated document management, and artificial intelligence instruments. The dual nature of digital transformation is evaluated because technological open-ness generates specific vulnerabilities, such as data leakages, software dependencies, and human errors. The practical value of the article is represented by a customized six-stage implementation framework that guides management from initial vulnerability audits to continuous performance monitoring through specific digital indicators. Implementation of these stages allows creating an adaptive mechanism that responds quickly to external fluctuations and builds a proactive shield for corporate asset management.

Keywords: digitalization, economic security, enterprise, cybersecurity, digital technologies, risk management, information security, competitiveness.

Постановка проблеми. Цифровізація виступає базовим вектором розвитку для сучасних суб'єктів господарювання. Поточні

умови в Україні характеризуються суттєвими воєнними викликами, нестабільністю ринків, руйнуванням логістичних ланцюгів та дефі-



© Ровінський О. О., 2026

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

цитом ресурсів. Паралельно спостерігається стрімке зростання кількості кібератак, що змушує менеджмент переосмислювати класичні підходи до безпеки. Якщо раніше ключова увага приділялася фізичній охороні активів та юридичному супроводу, то сьогодні першочергове значення мають корпоративні дані та цифрова інфраструктура підприємств.

У загальному розумінні економічна безпека компанії відображає рівень захищеності її ресурсів та спроможність протидіяти внутрішнім і зовнішнім небезпекам. В умовах розгортання цифрової економіки до класичних фінансових ризиків додаються нові технологічні загрози: несанкціонований доступ до комерційних даних, кібершахрайство та критична залежність від стабільності програмного забезпечення. Практична значущість цієї проблеми має двосторонній характер, оскільки технології одночасно виступають джерелом вразливостей та найефективнішим інструментом їх мінімізації. Через це актуальним завданням є побудова цілісної системи цифрового забезпечення економічної безпеки підприємств.

Аналіз останніх досліджень і публікацій. теоретичні засади формування систем захисту бізнесу закладені у фундаментальних працях багатьох науковців. Зокрема, у дослідженнях. Які викладені у монографії Череп А.В. та інших [1] досліджено досвід розвинених країн щодо використання цифрових технологій та визначено кращі практики для українських підприємств; досліджено особливості адаптації європейського досвіду цифрової трансформації економіки України задля забезпечення соціально економічної безпеки та сталого розвитку; сформовані теоретичні, методичні і практичні засади впровадження інноваційних цифрових технологій забезпечення економічної безпеки та розвитку конкурентоспроможності економіки України. Череп О., Щєбликіна І. [3] відмітили, що за період військового стану в Україні виріс обсяг ринку штучного інтелекту та експорту технологій, з є позитивними показниками поглиблення цифровізації української економіки та дослідили рівень цифровізації українських регіонів. Як перспективний напрямок розвитку цифровізації в Україні та збільшення кількості робочих місць було запропоновано створити цифрову платформу, яка має на меті залучити іноземні компанії в український бізнес. Авторка Андріїв Н. М. своїй роботі [3] присвятила дослідженню економічної безпеки підприємства в умовах масштабної цифровізації ринку праці.

Сучасний етап наукових дискусій зміщується в бік оцінювання цифрових трансформацій. У тематичному звіті Організації економічного співробітництва та розвитку (OECD) [9] проаналізовано роль цифрових інструментів як драйвера відновлення та адаптації українського бізнесу до умов глибокої невизначеності. Попри значну кількість напрацювань, безпековий вплив конкретних програмних продуктів (ERP, CRM, BI) на фінансову, кадрову та інформаційну складові захисту підприємства залишається вивченим фрагментарно, що вимагає розробки комплексного методологічного підходу.

Формулювання цілей статті (постановка завдання). Метою статті є наукове обґрунтування цифровізації як ефективного засобу забезпечення економічної безпеки підприємств, а також визначення ключових напрямів використання сучасних інформаційних технологій для попередження та мінімізації комерційних загроз.

Виклад основного матеріалу дослідження. Цифровізація підприємства є складним процесом інтеграції інноваційних рішень у всі рівні його операційної діяльності. На відміну від звичайної автоматизації окремих операцій, діджиталізація змінює архітектуру управління, забезпечуючи тотальну прозорість бізнес-процесів та раннє виявлення фінансових або кадрових відхилень. Корпоративні дані перетворюються на ключовий захищений актив, що мінімізує вплив людського фактора.

На думку авторів [3], основні проблеми які негативно впливають на цифровізацію економіки в Україні, можна виділити такі як, відсутність належного державного фінансування та застаріле обладнання яке не тільки не допомагає, а заважає працювати та розвиватися. Звичайно, в умовах воєнного стану всі бюджетні кошти спрямовані на підтримку армії, саме тому, після відновлення пропонується створити інноваційні платформи для співпраці з іноземними партнерами, які будуть зацікавлені в інвестуванні та розвитку бізнесу та технологій в Україні.

Проблема забезпечення економічної безпеки підприємств (ЕБП) в Україні є надзвичайно гострою через трансформацію економіки, політичну нестабільність, демографічну кризу та руйнівні наслідки воєнних дій [4]. На цьому тлі стрімка цифровізація економіки та ринку праці створює не лише нові можливості, але й серйозні виклики. Підприємства змушені здійснювати глибоку цифрову

трансформацію, щоб не втратити конкурентні позиції. Проте цей процес гальмується високими витратами, нестачею кваліфікованих кадрів, внутрішньо корпоративним спротивом та зростанням кількості кібератак. Водночас глибоко трансформується сам ринок праці: поширюється віддалена робота та фріланс, змінюється структура зайнятості, зростає технологічне безробіття, поглиблюється цифрова нерівність населення. Крім того, критичною проблемою є масштабна трудова міграція та відтік кращих фахівців за кордон. Усе це призводить до втрати людського капіталу, провокує соціальну нестабільність і прямо загрожує економічній безпеці як окремого підприємства, так і держави загалом. Для подолання цих проблем пропонується декілька як теоретичних так і практичних рішень: системний підхід до безпеки. Доведено, що економічну безпеку підприємства не можна розглядати відокремлено. Існує чітка ієрархія: економічна безпека держави та підприємства безпосередньо залежить від стану соціальної безпеки, ключовим елементом якої є ринок праці та пріоритетність захисту людського капіталу, тобто центральною ланкою економічної безпеки визнається людський капітал. Тому, необхідно постійно інвестувати в його розвиток, оновлювати цифрові компетентності працівників та протидіяти загрозі «старіння знань». Цифрова трансформація систем безпеки (СЕБП). Система безпеки підприємства повинна не лише реагувати на загрози, а й адаптуватися до умов цифрової економіки – це вимагає відмови від застарілих методів та залучення не тільки фінансових, а й організаційних, техніко-технологічних та інтелектуальних ресурсів для нейтралізації загроз. Втілення та впровадження або модернізація механізмів мотивації, для утримання талантів в умовах цифровізації необхідно впроваджувати нові мотиваційні механізми (як матеріальні, так і нематеріальні, наприклад, гнучкий графік чи віддалене робоче місце). Це має стимулювати працівників до розвитку цифрових навичок та узгоджувати їхні інтереси з безпековими цілями підприємства. І ще один підхід це ідентифікація найвпливовіших загроз. Завдяки математичному моделюванню встановлено, що (якщо абстрагуватися від руйнівного впливу війни) найбільший деструктивний вплив на трансформацію ринку праці мають саме фактори, пов'язані з цифровізацією та структурними перекосами: недостатній рівень цифрових компетенцій у населення, інноваційна пасивність бізнесу,

розрив між системою освіти та реальними потребами роботодавців, а також виготовлення продукції з низькою доданою вартістю.

Є визначення авторів [6], що цифровізація економіки має «двоїстий вплив», з одного боку, цифровізація є ключовим інструментом для зміцнення економічної безпеки держави, оскільки вона робить економічні процеси прозорішими, покращує управління та знижує рівень корупції. З іншого боку, вона генерує нові загрози: зростання кіберзлочинності, ризики витоку конфіденційних даних, технологічну залежність від інших країн та соціально-економічні дисбаланси, спричинені цифровою нерівністю.

В дослідженнях автора [6] визначено, як цифровізація одночасно створює нові можливості для розвитку підприємств та генерує серйозні кіберзагрози для їхньої діяльності. Виокремлюється в окремі категорії – по перше, інформація як головний ресурс. В умовах цифрової економіки акцент зміщується з матеріальних на інформаційні ресурси. Дані стають головною цінністю, що вимагає для їх обробки впровадження сучасних технологій, таких як Big Data та штучний інтелект. По друге, критична необхідність адаптації. Цифровізація підвищує продуктивність і конкурентоспроможність. Підприємства, які не усвідомлюють необхідності цифрової трансформації бізнесу, ризикують втратити всі переваги і найближчим часом взагалі піти з ринку. Далі, кіберзагрози виходять на перший план тобто, разом із технологіями зростає кількість інформаційних загроз. Головними небезпеками є крадіжка корпоративних даних, промислове шпигунство та хакерські атаки, які призводять до колосальних фінансових втрат і знищення репутації (як показують приклади компаній Sony Pictures та Equifax). Кадрова проблема у службах безпеки, окрім зовнішніх кіберзлочинців, внутрішньою загрозою є самі працівники та недостатня компетенція служб безпеки підприємства. Традиційна вимога наймати в такі служби людей виключно з досвідом у правоохоронних органах вже не дозволяє ефективно боротися з новітніми цифровими викликами. Як висновок, кібербезпека стала ключовим елементом економічної безпеки підприємства. Тому, успішний захист та розвиток вимагають не просто закупівлі нових комп'ютерів чи програм, а фундаментальних змін у корпоративній культурі та підходах до управління. Відповідно, збереження та захист цифрових даних має бути абсолютним пріоритетом для будь-якого сучасного бізнесу.

Системне впровадження технологій базується на принципах стратегічної доцільності, комплексності, захищеності даних та безперервного моніторингу. Згідно зі світовою статистикою Eurostat [11], у 2024 році близько 92,76% європейських компаній використовували принаймні один захід ІКТ-безпеки. В тому числі, більше ніж кожне третя компанія, близько 35,5% має в наявності документи, що запроваджують заходи, практики або процедури щодо безпеки ІКТ. Також 21,82% компаній переглянули ці документи протягом останніх 12 місяців. 59,97% компаній ЄС повідомили своїх працівників про їхні зобов'язання щодо питань безпеки ІКТ. Зрештою, кожна п'ята компанія – 21,54% зазнала наслідків через інциденти безпеки, пов'язані з ІКТ, у 2023 році. Надійна автентифікація була налаштована у 83,69% фірм, а резервне копіювання – у 79,23% суб'єктів. Це підтверджує, що цифровий захист став невіддільною передумовою стабільного функціонування бізнесу, представлено в Таблиці 1.

Важливу роль відіграють хмарні обчислення та системи штучного інтелекту. За аналітичними даними Eurostat [12; 13], частка компаній ЄС, які застосовують платні хмарні послуги, досягла 52,74% у 2025 році, а інструменти ШІ інтегрували понад 19,95% підприємств. Такі рішення дозволяють автоматизувати прогнозу аналітику та вчасно блокувати потенційні загрози. Разом з тим, вартість кіберінцидентів залишається критичною. Звіт компанії IBM [17] свідчить, що середня світова вартість витоку комерційних даних у 2024 році склала 4,88 млн дол. США, при цьому дослідження Verizon [18] доводить, що 68% інцидентів пов'язані з помил-

ками персоналу. Це підкреслює необхідність виконання вимог Закону України «Про основні засади забезпечення кібербезпеки України» [19] та впровадження засобів електронної ідентифікації згідно із законодавством [20]. З метою усунення фрагментарності автоматизації автором структуровано вплив основних засобів діджиталізації на функціональні компоненти безпеки підприємства. Комплексні ERP-системи забезпечують наскрізний фінансовий та матеріальний облік, виключаючи зловживання та нецільове використання ресурсів. CRM-платформи гарантують надійне збереження клієнтських баз та захищають комерційну таємницю від несанкціонованого копіювання звільненими працівниками. BI-інструменти дозволяють візуалізувати відхилення індикаторів фінансової стійкості в режимі реального часу, представлено в Таблиці 2.

Все більше авторів за результатами їх досліджень [8] сходяться на думці, щодо захисту бізнесу в сучасному середовищі. Визначають, що цифрові активи як основа стійкості – дані, алгоритми, хмарні сервіси, програмне забезпечення та IT-інфраструктура стали ключовими ресурсами підприємств. Від рівня їхньої захищеності безпосередньо залежить конкурентоспроможність компанії, оскільки цифровізація генерує нові серйозні загрози: витоки інформації, кіберінциденти, інституційні ризики та технічні збої. Саме, більшість порушень безпеки спричинені людськими помилками та недостатнім рівнем навичок при роботі з технологіями, тому цифрова компетентність співробітників визнається найважливішим чинником для зниження ймовірності кібератак. Задля підвищення

Таблиця 1

Статистичні показники цифровізації та цифрової безпеки підприємств

Показник	Значення	Рік	Безпекове значення для підприємства
Застосування заходів ІКТ-безпеки в ЄС	92,76%	2024	Базова умова стабільної діяльності бізнесу
Сильна парольна автентифікація	83,69%	2024	Контроль доступу до корпоративних систем
Резервне копіювання даних в ЄС	79,23%	2024	Забезпечення відновлення критичної інформації
Негативні наслідки безпекових інцидентів	21,54%	2023	Доводить реальність ризиків втрати активів
Використання платних хмарних сервісів	52,74%	2025	Перехід до гнучкої та віддаленої інфраструктури
Інтеграція штучного інтелекту	19,95%	2025	Зростання ролі швидкої прогнозової аналітики

Джерело: сформовано автором на основі [11]

Таблиця 2

Специфікація впливу цифрових інструментів на безпекове середовище підприємства

Цифровий інструмент	Складова безпеки	Очікуваний безпековий результат
ERP-системи	Фінансова, виробнича	Жорсткий контроль витрат, мінімізація крадіжок та оптимізація складських запасів.
CRM-платформи	Інформаційна, ринкова	Захист баз даних клієнтів від витоку інформації, прозорість комерційних угод.
BI-аналітика	Управлінська, фінансова	Швидке моделювання загроз, прогнозування ліквідності та виявлення аномальних операцій.
Хмарна інфраструктура	Операційна, технічна	Безперервність бізнесу в умовах фізичного руйнування офісів або серверних станцій.

Джерело: сформовано автором на основі [10]

рівня економічної безпеки підприємствам необхідно модернізувати IT-інфраструктуру, вдосконалювати внутрішні політики безпеки, а також проводити регулярні аудити й тестування систем. Важливим є посилення відповідності національним і міжнародним стандартам інформаційної безпеки. У перспективі для забезпечення економічної стійкості підприємствам доведеться впроваджувати інтелектуальні моделі оцінювання ризиків на базі штучного інтелекту, а також вивчати та адаптувати під свої потреби автономні системи, блокчейн і квантові обчислення.

Європейський бізнес та інфраструктура активно трансформуються завдяки хмарним сервісам та ШІ. Проте, щоб виконати амбітний план цифровізації до 2030 року, ключовим пріоритетом має стати інвестування в людський капітал: масове навчання населення цифровим навичкам, підготовка нових ІКТ-спеціалістів, подолання гендерного дисбалансу в IT-галузі, а також цілеспрямована підтримка цифровізації малого та середнього бізнесу, якому нині бракує ресурсів і кадрів.

Задля ефективного забезпечення економічної безпеки в умовах стрімкої цифровізації, необхідно реалізувати комплексний підхід, який охоплює дії як на рівні окремих підприємств, так і на рівні держави.

Здійснити глибинну цифрову трансформацію бізнесу. Перейти від простого оцифрування до зміни бізнес-моделей. Інтегрувати новітні технології, активно впроваджувати інструменти аналітики великих даних (Big Data), штучний інтелект (AI), хмарні обчислення та Інтернет речей (IoT) для оптимізації процесів, кращого розуміння клієнтів та підвищення конкурентоспроможності.

Інвестувати у розвиток та захист людського капіталу. Підвищувати цифрові компетентності, оскільки роль фізичної праці

зменшується, підприємства та держава повинні масово інвестувати у перенавчання працівників та розвиток їхніх цифрових навичок, щоб уникнути технологічного безробіття та дефіциту кадрів. Впровадити нові механізми мотивації, для утримання талантів (особливо молоді «покоління Z») необхідно відходити від застарілих методів управління. Слід пропонувати гнучкий графік, віддалені робочі місця, прив'язувати оплату праці до конкретних здобутих компетенцій та результатів, а також створювати умови для саморозвитку та творчості. Адаптуватися до нових форм зайнятості: Підприємствам необхідно навчитися ефективно та безпечно інтегрувати у свою діяльність фрилансерів та IT-аутсорсинг.

Модернізувати системи безпеки та кіберзахисту. Система економічної безпеки підприємства (СЕБП) має перейти від реактивного реагування на загрози до проактивного прогнозування. Необхідно постійно моніторити як внутрішні процеси, так і зовнішнє інформаційне середовище (зокрема, зміни на ринку праці, дії конкурентів та нові технологічні тренди). Посилити захист даних як головного активу, тому кібербезпека є пріоритетом. Необхідно впроваджувати постійний моніторинг вразливостей, системи управління обліковими записами, а також процеси автоматичного резервного копіювання та відновлення даних в ізольованих середовищах. Контролювати ризики у ланцюгах постачання, вимоги щодо безпеки повинні бути пріоритетними на етапі планування та прописуватися у контрактах із третіми сторонами. Працівники служб безпеки повинні володіти не лише традиційними навичками, але й високим рівнем цифрової грамотності для протидії кібератакам, промислового шпигунству та інформаційним витокам.

Реалізувати кроки на рівні держави. Створити єдину цифрову екосистему, держава має



Рис. 1. Поетапна модель інтеграції цифрових рішень в систему безпеки компанії

Джерело: сформовано автором

автоматизувати процеси фінансового моніторингу та управління бюджетними коштами, використовуючи алгоритми машинного навчання та смарт-контракти для зниження рівня корупції та виявлення фінансових злочинів. Вдосконалити нормативно-правову базу та інфраструктуру, розробляти національні стандарти кібербезпеки, захищати критичну цифрову інфраструктуру та гармонізувати освітні програми з реальними потребами цифрового бізнесу.

Для успішного впровадження інновацій пропонується ввести поетапну модель інтеграції рішень представлено на Рисунку 1. Вона складається з шести послідовних кроків: первинний експрес-аудит інформаційної інфраструктури, побудова деталізованої карти ризиків, вибір та ліцензування програмних засобів, технічне розгортання та інтеграція баз даних, комплексне навчання персоналу правилам кібергігієни, а також постійний моніторинг захищеності через розроблений набір KPI (наприклад, швидкість реагування на атаки, відсоток успішного відновлення бекапів, зниження рівня про-

термінованої дебіторської заборгованості контрагентів).

Висновки. Проведене дослідження підтверджує, що цифровізація виступає дієвим засобом забезпечення безпеки сучасного бізнесу. Вона безпосередньо посилює фінансову, кадрову, правову та виробничу складові захисного контуру. Встановлено дуалістичний характер діджиталізації: оптимізуючи операційні процеси, вона одночасно генерує нові технологічні вразливості, що вимагає переходу від хаотичного використання програм до побудови системного кіберзахисту.

Запропонована автором шестиетапна модель забезпечує послідовну трансформацію цифрового середовища компанії, мінімізуючи вплив людського фактора завдяки чітким регламентам та безперервному моніторингу KPI. Перспективами подальших наукових розробок у цьому напрямі є формування прикладних методик кількісного оцінювання окупності інвестицій в інформаційну безпеку, а також побудова галузевих моделей захисту для підприємств логістичного та промислового секторів економіки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Андріїв Н. М. Економічна безпека підприємства в умовах цифровізації ринку праці: теоретичні та практичні аспекти : монографія. Львів : Растр-7, 2023. 320 с.
2. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. 2020. № 4, Т. 1. С. 32–35. DOI: <https://doi.org/10.31891/2307-5740-2020-284-4-5>
3. Гнатенко І. А., Хорошко Д. Р. Трансформація системи економічної безпеки країни в контексті цифровізації. *Актуальні проблеми економіки*. 2025. № 3 (285). С. 195–207. DOI: <https://doi.org/10.32752/1993-6788-2025-1-285-195-207>
4. Державна служба статистики України. Використання інформаційно-комунікаційних технологій на підприємствах. URL: <https://stat.gov.ua/en/datasets/use-information-and-communication-technologies-enterprises> (дата звернення: 06.06.2026).
5. Коляденко С., Дзісь О., Гайдей В. Перспективні напрями цифровізації аграрних підприємств у контексті економічної безпеки. *Економіка та суспільство*. 2024. Вип. 59. DOI: <https://doi.org/10.32782/2524-0072/2024-59-84>
6. Лугова В. М., Кравчик Ю., Пушак Я. Я., Літвінов Д. О., Печка С. С. Економічна безпека підприємств в умовах цифрової економіки. *Актуальні проблеми інноваційної економіки та права*. 2025. № 4. С. 99–103. DOI: <https://doi.org/10.36887/2524-0455-2025-4-23>
7. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19>
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
9. Череп А., Щєбликіна І., Щєбликіна З., Гуль Я. Технологічне безробіття в умовах цифрової економіки України: міф чи реальність?. *Фінансові стратегії інноваційного розвитку економіки*. 2025. № 3 (67). С. 84–92. DOI: <https://doi.org/10.26661/2414-0287-2025-3-67-16>
10. Череп О., Щєбликіна І., Гуль Я. Цифровізація України у повоєнний період та її вплив на робочі місця. *Фінансові стратегії інноваційного розвитку економіки*. 2025. № 1 (65). С. 109–115. DOI: <https://doi.org/10.26661/2414-0287-2025-1-65-18>
11. Eurostat. Cloud computing - statistics on the use by enterprises. Statistics Explained. 2026. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
12. Eurostat. ICT security in enterprises. Statistics Explained. 2024. URL: <https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf>
13. Eurostat. Towards Digital Decade targets for Europe. Statistics Explained. 2026. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe
14. Eurostat. Use of artificial intelligence in enterprises. Statistics Explained. 2025. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
15. IBM. Surging data breach disruption drives costs to record highs. 2024. URL: <https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report>
16. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems — Requirements. Geneva : International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/27001>
17. IT Ukraine Association. Ukraine's IT Exports Declined by Over 4% in 2024. URL: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/>
18. NIST. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
19. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris : OECD Publishing, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf
20. Porter M. E., Heppelmann J. E. How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*. 2014. Vol. 92, No. 11. P. 64–88.

21. Socio-economic security in the context of war: innovative approaches and strategic guidelines for the postwar period : collective monograph / ed. by A. V. Cherep, I. M. Dashko, Yu. O. Ohrenych, O. H. Cherep. Riga, Latvia : Baltija Publishing, 2025. 218 p. DOI: <https://doi.org/10.30525/978-9934-26-585-3>
22. Verizon. 2024 Data Breach Investigations Report. 2024. URL: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>

REFERENCES:

1. Socio-economic security in the context of war: innovative approaches and strategic guidelines for the postwar period : collective monograph / ed. by A. V. Cherep, I. M. Dashko, Yu. O. Ohrenych, O. H. Cherep. Riga, Latvia : Baltija Publishing, 2025. 218 p. DOI: <https://doi.org/10.30525/978-9934-26-585-3>
2. Cherep, A., Shcheblykina, I., Shcheblykina, Z., & Hul, Ya. (2025). Tekhnologichne bezrobittia v umovakh tsyfrovoy ekonomiky Ukrainy: mif chy realist? [Technological unemployment in the conditions of the digital economy of Ukraine: myth or reality?]. *Finansovi stratehii innovatsiinoho rozvytku ekonomiky*, (3 (67)), 84–92. DOI: <https://doi.org/10.26661/2414-0287-2025-3-67-16> [in Ukrainian].
3. Cherep, O., Shcheblykina, I., & Hul, Ya. (2025). Tsyfrovizatsiia Ukrainy u povoiennyi period ta yii vplyv na robochi mistia [Digitalization of Ukraine in the post-war period and its impact on jobs]. *Finansovi stratehii innovatsiinoho rozvytku ekonomiky*, (1 (65)), 109–115. DOI: <https://doi.org/10.26661/2414-0287-2025-1-65-18> [in Ukrainian].
4. Andriiv, N. M. (2023). *Ekonomichna bezpeka pidpriemstva v umovakh tsyfrovizatsii rynku pratsi: teoretychni ta praktychni aspekty* [Economic security of the enterprise in the conditions of digitalization of the labor market: theoretical and practical aspects] (Monograph). Lviv : Rastr-7. 320 p. [in Ukrainian].
5. Bakai, V. I. (2020). Zabezpechennia ekonomichnoi bezpeky pidpriemstva na osnovi vykorystannia tsyfrovoykh tekhnologii [Ensuring the economic security of the enterprise based on the use of digital technologies]. *Visnyk Khmelnytskoho natsionalnoho universytetu*, (4, Vol. 1), 32–35. DOI: <https://doi.org/10.31891/2307-5740-2020-284-4-5> [in Ukrainian].
6. Hnatenko, I. A., & Khoroshko, D. R. (2025). Transformatsiia systemy ekonomichnoi bezpeky krainy v konteksti tsyfrovizatsii [Transformation of the country's economic security system in the context of digitalization]. *Aktualni problemy ekonomiky*, (3 (285)), 195–207. DOI: <https://doi.org/10.32752/1993-6788-2025-1-285-195-207> [in Ukrainian].
7. Koliadenko, S., Dzis, O., & Haidei, V. (2024). Perspektyvni napriamy tsyfrovizatsii ahrarykh pidpriemstv u konteksti ekonomichnoi bezpeky [Perspective directions of digitalization of agricultural enterprises in the context of economic security]. *Ekonomika ta suspilstvo*, (59). DOI: <https://doi.org/10.32782/2524-0072/2024-59-84> [in Ukrainian].
8. Luhova, V. M., Kravchyk, Yu., Pushak, Ya. Ya., Litvinov, D. O., & Piechka, S. S. (2025). Ekonomichna bezpeka pidpriemstv v umovakh tsyfrovoy ekonomiky [Economic security of enterprises in the conditions of the digital economy]. *Aktualni problemy innovatsiinoy ekonomiky ma prava*, (4), 99–103. DOI: <https://doi.org/10.36887/2524-0455-2025-4-23> [in Ukrainian].
9. OECD. (2024). *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*. Paris : OECD Publishing. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf
10. State Statistics Service of Ukraine. (2026). *Vykorystannia informatsiino-komunikatsiinykh tekhnologii na pidpriemstvakh* [Use of information and communication technologies in enterprises]. URL: <https://stat.gov.ua/en/datasets/use-information-and-communication-technologies-enterprises> [in Ukrainian].
11. Eurostat. (2024). *ICT security in enterprises*. Statistics Explained. URL: <https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf>
12. Eurostat. (2026). *Cloud computing – statistics on the use by enterprises*. Statistics Explained. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
13. Eurostat. (2025). *Use of artificial intelligence in enterprises*. Statistics Explained. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
14. Eurostat. (2026). *Towards Digital Decade targets for Europe*. Statistics Explained. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe
15. NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg : National Institute of Standards and Technology. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
16. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva : International Organization for Standardization. URL: <https://www.iso.org/standard/27001>

17. IBM. (2024). *Surging data breach disruption drives costs to record highs*. URL: <https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report>
18. Verizon. (2024). *2024 Data Breach Investigations Report*. URL: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>
19. Verkhovna Rada of Ukraine. (2017). *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"* [Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine"] (No. 2163-VIII). URL: <https://zakon.rada.gov.ua/laws/show/2163-19> [in Ukrainian].
20. Verkhovna Rada of Ukraine. (2017). *Zakon Ukrainy "Pro elektronni dovirchi posluhy"* [Law of Ukraine "On electronic trust services"] (No. 2155-VIII). URL: <https://zakon.rada.gov.ua/laws/show/2155-19> [in Ukrainian].
21. IT Ukraine Association. (2025). *Ukraine's IT Exports Declined by Over 4% in 2024. What's Next?* URL: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/>
22. Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*, 92(11), 64–88.

Дата надходження статті: 01.07.2026

Дата прийняття статті до публікації: 17.08.2026

Дата публікації статті: 15.09.2026