

УДК 005.35:004.9

DOI: <https://doi.org/10.30838/EP.216.68-75>**Богач К.С.**

кандидат економічних наук

Національний технічний університет «Дніпровська політехніка»

Bohach Kyrylo

PhD in Economic Sc.

Dnipro University of Technology

<https://orcid.org/0000-0002-7359-7747>**Бардась А.В.**

доктор економічних наук

Національний технічний університет «Дніпровська політехніка»

Bardas Artem

Dr. of Economic Sc.

Dnipro University of Technology

<https://orcid.org/0000-0002-8309-3796>

ПРОБЛЕМИ СОЦІАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ У ПИТАННЯХ ДІДЖИТАЛІЗАЦІЇ БІЗНЕСУ

Стаття присвячена систематизації проблемних напрямів соціальної відповідальності бізнесу в умовах його діджиталізації. Розглянуто трансформацію корпоративної соціальної відповідальності у концепцію корпоративної цифрової відповідальності, яка охоплює захист даних, цифрове благополуччя, цифрову інклюзію та етичне використання технологій. Виокремлено п'ять ключових проблемних напрямів: захист персональних даних, алгоритмічна упередженість штучного інтелекту, цифровий розрив, права платформних працівників та відповідальність бізнесу за автоматизацію ринку праці. Проаналізовано специфіку прояву цих проблем в українському бізнес-середовищі в умовах війни й європейської інтеграції. Обґрунтовано напрями інституціоналізації цифрової соціальної відповідальності бізнесу на рівні підприємства з урахуванням і галузевих зв'язків та інтересів держави.

Ключові слова: соціальна відповідальність бізнесу, діджиталізація, корпоративна цифрова відповідальність, штучний інтелект, захист персональних даних, цифровий розрив, платформна зайнятість, ESG, цифрова трансформація, бізнес-етика.

PROBLEMS OF SOCIAL RESPONSIBILITY IN THE ISSUES OF BUSINESS DIGITALIZATION

The purpose of this article is to systematize the key problem areas of business social responsibility under conditions of digitalization and to substantiate directions for institutionalizing digital social responsibility of enterprises, with particular attention to the specifics of the Ukrainian business environment. The relevance of the topic is determined by the accelerating digital transformation of business under wartime conditions, the harmonization of Ukrainian legislation with European Union data protection and artificial intelligence regulation, and the recent adoption of a binding international treaty on platform work.

The study applies methods of theoretical generalization, systemic and comparative analysis, induction and deduction, abstract-logical reasoning, and scientific classification to synthesize findings from Ukrainian and international scholarly literature, reports of international organizations, and legal acts of Ukraine and the European Union. As a result, the article demonstrates that traditional corporate social responsibility, historically built around economic, legal, ethical, and philanthropic dimensions, requires extension through the concept of corporate digital responsibility, which additionally covers data protection, digital well-being, digital inclusion, and the ethical use of technology. Five key problem areas of business social responsibility under digitalization are identified and characterized: personal data protection and digital privacy; algorithmic bias and artificial intelligence ethics; the digital divide and digital inclusiveness; the rights of platform workers and transparency of algorithmic management; and business responsibility for the social consequences of labor market automation.

The analysis of these problems in the Ukrainian business environment reveals an adaptive, crisis-driven character of

ISSN друкованої версії: 2224-6282

ISSN електронної версії: 2224-6290

© Богач К.С., Бардась А.В., 2026

digital transformation during wartime, a dual regulatory pressure arising from outdated national legislation combined with the need for anticipatory alignment with European standards, and a close interconnection between digital responsibility and the ESG agenda as a factor of international competitiveness.

The practical value of the obtained results lies in the substantiation of a multilevel framework for institutionalizing digital social responsibility, encompassing corporate-level digital responsibility policies and artificial intelligence ethics committees, industry-level codes of digital conduct, and state-level acceleration of legislative harmonization with European data protection and artificial intelligence regulation, as well as consideration of ratifying the International Labour Organization convention on decent work in the platform economy. The proposed framework can be used by enterprise management to design digital responsibility strategies and by public authorities to shape digitalization policy.

Keywords: social responsibility of business, digitalization, corporate digital responsibility, artificial intelligence, personal data protection, digital divide, platform employment, ESG, digital transformation, business ethics.

JEL classification: M14, M15, O33.

Постановка проблеми. Глобальна діджиталізація бізнесу, що прискорилося під впливом пандемійних обмежень, воєнних викликів та стрімкого поширення технологій штучного інтелекту, кардинально змінює не лише операційні моделі підприємств, а й характер їхньої взаємодії із суспільством. Традиційна концепція корпоративної соціальної відповідальності (КСВ), що формувалася протягом другої половини ХХ ст. навколо питань охорони праці, екологічної безпеки та благодійності [7; 9], виявляється недостатньою для врегулювання нового кола викликів, породжених цифровою трансформацією: обробки величезних масивів персональних даних, використання алгоритмів прийняття рішень, автоматизації робочих місць, поширення платформної зайнятості та формування цифрової нерівності. У відповідь на ці виклики в іноземній англійській науковій літературі з 2019–2021 рр. активно розвивається концепція корпоративної цифрової відповідальності (Corporate Digital Responsibility, CDR), яка розглядається як логічне розширення КСВ на цифрову сферу діяльності підприємства [16].

Актуальність теми для українського бізнесу має додаткове обґрунтування. *По-перше*, повномасштабна війна пришвидшила цифрову трансформацію українських підприємств, змусивши бізнес переносити операції в цифрове середовище, впроваджувати дистанційні формати роботи та цифрові платформи для збереження операційної спроможності в умовах логістичних і виробничих розривів [1]. *По-друге*, курс України на європейську інтеграцію вимагає гармонізації національного законодавства у сфері захисту персональних даних та регулювання штучного інтелекту із Регламентом (ЄС) 2016/679 (GDPR) [11] з Актом ЄС про штучний інтелект [12], що прямо стосується соціальної відповідальності бізнесу, який працює з цифровими технологіями. По-третє, на глобальному рівні щойно, у червні 2026 р., Міжнародна організація праці ухвалила Конвенцію № 193 про гідну працю в платформній економіці [14] – перший обов'язковий міжнародний договір, що регулює права працівників цифрових платформ та додатково підтверджує: проблема соціальної відповідальності бізнесу за цифровізацію із суто теоретичної перетворюється на практично-регуляторну.

Зазначена проблема полягає в тому, що діджиталізація бізнесу організації створює специфічне поле соціальної відповідальності, яке не покривається традиційними інструментами КСВ (кодекси поведінки, звітність зі сталого розвитку, благодійні програми) і

водночас не має усталеного, загальновизнаного теоретико-методологічного апарату аналізу. Підприємства, зокрема українські, стикаються з необхідністю одночасно впроваджувати цифрові технології для підвищення конкурентоспроможності та нести відповідальність за етичні, соціальні й правові наслідки цього впровадження – часто без чіткого розуміння меж такої відповідальності, релевантного інструментарію та законодавчого підґрунтя. Це зумовлює потребу в систематизації проблемних напрямів соціальної відповідальності бізнесу в умовах діджиталізації та визначенні шляхів їх інституціоналізації, що і формує наукову проблему цього дослідження.

Аналіз останніх досліджень та публікацій. Теоретичні засади класичної корпоративної соціальної відповідальності закладені у працях Г. Боуена, який ще у 1953 р. визначив соціальну відповідальність бізнесмена як зобов'язання дотримуватися такої політики та приймати такі рішення, що відповідають цілям і цінностям суспільства [7], та розвинуті А. Керроллом, який запропонував багаторівневу модель КСВ, що охоплює економічну, правову, етичну та філантропічну відповідальність [9]. Ці концепції залишаються методологічним фундаментом для сучасних досліджень, однак потребують адаптації до цифрового контексту.

Проблематику взаємозв'язку соціальної відповідальності та цифровізації бізнесу активно досліджують українські науковці. Ю. Магиляс аналізує особливості становлення соціально відповідального бізнесу в Україні в умовах цифрової трансформації суспільства, наголошуючи на уповільненості цього процесу через усталеність негативних соціальних очікувань населення щодо держави та недостатню сформованість суспільного запиту на соціально відповідальні практики бізнесу [4]. Н. Євтушенко та Д. Стеценко досліджують цифрову трансформацію українського бізнесу в умовах війни, підкреслюючи, що воєнні виклики одночасно посилюють потребу в цифровізації та ускладнюють її реалізацію через порушення виробничих і логістичних ланцюгів [1]. О. Серікова розглядає трансформацію моделей корпоративної соціальної відповідальності бізнесу в умовах війни, виділяючи нові напрями КСВ – від IT-підтримки та безкоштовного доступу до інформаційних ресурсів до цифрового супроводу релокації бізнесу [5]. Г. Лучко досліджує розвиток соціальної відповідальності бізнесу в Україні крізь призму ESG-показників і ESG-рейтингів, обґрунтовуючи, що регулярна ESG-звітність підвищує ділову репутацію та

конкурентоспроможність підприємств на міжнародному ринку [3].

У міжнародній літературі концепція корпоративної цифрової відповідальності (CDR) розроблена Л. Лобшат та співавторами, які визначають її як сукупність спільних цінностей і норм, що визначають діяльність організації щодо створення, впровадження, оцінювання та вдосконалення цифрових технологій і роботи з даними [16]. М. Каміллері досліджує етичні виміри врядування штучним інтелектом (AI governance) та його імплікації для соціальної відповідальності, наголошуючи на необхідності поєднання формальних регуляторних вимог із добровільними етичними принципами розробників технологій [8]. З. Чень у своєму огляді алгоритмічної дискримінації в підборі персоналу за допомогою ШІ виявляє, що упередженість алгоритмів найму часто походить із обмежених або незбалансованих навчальних даних та упереджень розробників, пропонуючи поєднання технічних (аудит датасетів, підвищення прозорості алгоритмів) і управлінських (внутрішнє етичне врядування, зовнішній нагляд) заходів для її подолання [10].

Незважаючи на значний масив досліджень, не вирішеною залишається частина проблеми, пов'язана із системним об'єднанням розрізнених напрямів соціальної відповідальності бізнесу в умовах діджиталізації (захист даних, алгоритмічна етика, цифровий розрив, платформна зайнятість) у єдину аналітичну рамку, застосовну до умов українського бізнес-середовища, що перебуває одночасно під тиском воєнних викликів, євроінтеграційних регуляторних вимог та потреби прискореної цифрової трансформації. Саме це визначає напрям цього дослідження.

Метою статті є систематизація ключових проблемних напрямів соціальної відповідальності бізнесу організації в умовах її діджиталізації та обґрунтування напрямів інституціоналізації цифрової соціальної відповідальності підприємств з урахуванням специфіки українського бізнес-середовища.

Досягнення поставленої мети передбачає вирішення таких завдань:

- ✓ визначення концептуальних відмінностей між традиційною корпоративною соціальною відповідальністю та корпоративною цифровою відповідальністю;
- ✓ систематизація основних проблемних напрямів соціальної відповідальності бізнесу, породжених процесами діджиталізації;
- ✓ аналізування специфіки прояву цих проблем в українському бізнес-середовищі в умовах воєнного стану та європейської інтеграції;
- ✓ обґрунтування напрямів інституціоналізації соціально відповідальних практик цифровізації бізнесу.

Методи дослідження. Для досягнення мети дослідження застосовано комплекс загальнонаукових методів. Метод теоретичного узагальнення та системного аналізу використано для систематизації наукових підходів до визначення сутності соціальної відповідальності бізнесу в умовах діджиталізації та виокремлення її структурних елементів. Порівняльний аналіз застосовано для зіставлення традиційної моделі КСВ та

концепції корпоративної цифрової відповідальності, а також для порівняння регуляторних підходів України та Європейського Союзу до захисту персональних даних і врегулювання штучного інтелекту. Методи індукції та дедукції використано для виведення узагальнених характеристик проблемних напрямів соціальної відповідальності на основі окремих випадків і практик, наведених у проаналізованих джерелах. Абстрактно-логічний метод застосовано для формулювання авторського бачення структури проблемного поля цифрової соціальної відповідальності бізнесу. Метод наукової класифікації використано для групування виявлених проблем за напрямками (захист даних, алгоритмічна етика, цифровий розрив, платформна зайнятість, автоматизація ринку праці).

Виклад основних результатів дослідження. Традиційна концепція КСВ ґрунтується на моделі, у якій підприємство добровільно бере на себе зобов'язання щодо суспільства, працівників, довкілля та споживачів понад законодавчо встановлений мінімум [9]. Однак цифрова трансформація бізнесу породжує принципово нові об'єкти відповідальності – дані, алгоритми та автоматизовані системи прийняття рішень, – які не вписуються у традиційну структуру КСВ ні за суб'єктом впливу (не лише люди, а й алгоритмічні системи), ні за характером наслідків (часто відкладені, важко передбачувані, системні). Виокремлення даних та алгоритмів та систем прийняття рішень пояснюється їхнім значенням для збереження конфіденційної інформації та забезпечення конкурентних переваг організації.

У відповідь на це в науковій літературі сформувався концепція корпоративної цифрової відповідальності (Corporate Digital Responsibility, CDR), яку Л. Лобшат і співавтори визначають як сукупність спільних цінностей і норм, що скеровують діяльність організації щодо створення технологій і збору даних, їх експлуатації та прийняття рішень на їх основі, оцінювання наслідків впровадження та вдосконалення технологій [16]. На відміну від КСВ, яка історично формувалася навколо трьох вимірів сталого розвитку (економічного, соціального, екологічного), CDR охоплює щонайменше п'ять специфічних вимірів: захист і конфіденційність даних, цифрове благополуччя користувачів і працівників, екологічну сталість цифрової інфраструктури, цифрову інклюзію та доступність, а також етичне використання технологій.

Важливо підкреслити, що CDR не заперечує і не замінює КСВ, а є її логічним розширенням на цифрову сферу діяльності підприємства: цифрові технології стають не окремим об'єктом відповідальності, а наскрізним виміром, що пронизує всі традиційні напрями КСВ – від відповідальності перед працівниками (цифровий моніторинг, автоматизація робочих місць) до відповідальності перед споживачами (персоналізація на основі даних, алгоритмічна дискримінація) і суспільством загалом (цифровий розрив, вплив на зайнятість). М. Каміллері наголошує, що ефективне врядування штучним інтелектом вимагає поєднання формальних регуляторних вимог (законодавчих актів і обов'язкових регламентів) із добровільними етичними принципами, що скеровують розробників і користувачів технологій

у досягненні довгострокових цілей за одночасного забезпечення інтересів усіх заінтересованих сторін [8].

Дослідники також зазначають, що вивчення CDR перебуває на ранній стадії розвитку: не існує усталеного консенсусу щодо визначення, концептуалізації та інструментів оцінювання цифрової відповідальності бізнесу, що створює як науковий виклик, так і практичну прогалину для підприємств, які потребують операційних орієнтирів. Для українського бізнесу, що перебуває у стані пришвидшеної, часто вимушеної цифровізації [1], відсутність усталеної методології CDR є особливо відчутною проблемою, оскільки унеможливає системну оцінку соціальних наслідків власних цифрових ініціатив і ускладнює приведення внутрішніх практик у відповідність до вимог, що постають перед українськими компаніями в межах європейської інтеграції.

Обробка персональних даних є, ймовірно, найбільш розробленим у регуляторному сенсі напрямом цифрової соціальної відповідальності бізнесу. Регламент (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних (GDPR) встановив глобальний орієнтир для корпоративних практик у цій сфері, вимагаючи від бізнесу прозорості обробки даних, отримання явної згоди суб'єктів даних, права на видалення й перенесення даних та призначення відповідальних за захист даних [11]. Українське законодавство у цій сфері досі спирається на Закон України «Про захист персональних даних» від 2010 р. № 2297-VI [2], який, за оцінками правозахисних організацій, більше не відповідає сучасним міжнародним стандартам захисту даних [6]. Розроблений законопроект, спрямований на гармонізацію національного регулювання з GDPR, викликає неоднозначні оцінки експертного середовища: з одного боку, його ухвалення є політично й економічно важливим кроком в умовах перетворення України на привабливу локацію для розміщення бек-офісів і центрів підтримки європейських та американських компаній, з іншого – критики зазначають, що запропонований варіант не повною мірою відтворює усталені практики, що діють у системах захисту персональних даних європейських країн, зокрема щодо створення незалежного наглядового органу [6].

Для бізнесу, що активно впроваджує цифрові інструменти – CRM-системи, аналітику поведінки клієнтів, програми лояльності на основі персональних даних, – ця регуляторна невизначеність створює подвійний виклик соціальної відповідальності. *По-перше*, підприємства змушені самостійно визначати рівень захисту даних клієнтів і працівників за відсутності повністю гармонізованого з європейськими стандартами національного регулювання, що підвищує ризики або надмірної, або недостатньої обережності в роботі з даними. *По-друге*, соціально відповідальна поведінка у сфері захисту даних дедалі частіше є не просто питанням дотримання законодавства, а фактором довіри споживачів і конкурентоспроможності на міжнародному ринку, оскільки партнерство з європейськими контрагентами вимагає застосування стандартів, еквівалентних GDPR, незалежно від стану національного регулювання.

Стрімке впровадження систем штучного інтелекту в бізнес-процеси – від автоматизованого відбору кандидатів на вакансії до кредитного скорингу та персоналізованого ціноутворення – породжує проблему алгоритмічної упередженості (algorithmic bias), яка полягає в тому, що системи штучного інтелекту можуть відтворювати й посилювати упередження своїх розробників або упередження, закладені в навчальних даних, стосовно статі, віку, етнічного походження чи інших демографічних характеристик. З. Чень у своєму дослідженні алгоритмічної дискримінації в процесах підбору персоналу з використанням ШІ показує, що, попри здатність підвищувати якість і швидкість рекрутингу, такі системи часто відтворюють дискримінаційні патерни, які походять з обмежених або незбалансованих масивів даних і упереджень розробників алгоритмів [10]. Дослідник пропонує поєднання технічних заходів (використання неупереджених фреймворків для формування наборів даних, підвищення прозорості й пояснюваності алгоритмів) з управлінськими інструментами – внутрішнім етичним врядуванням і зовнішнім наглядом – як найбільш ефективний шлях мінімізації алгоритмічної упередженості [10].

На регуляторному рівні Європейський Союз відповів на ці виклики ухваленням Акту про штучний інтелект (Регламент (ЄС) 2024/1689), який запроваджує ризик-орієнтований підхід до регулювання систем ШІ: найсуворіші вимоги – щодо прозорості, документування та постійного моніторингу – застосовуються до систем «високого ризику», до яких віднесено, зокрема, системи, що використовуються у сфері зайнятості, освіти та доступу до основних послуг [12]. Перехідний період дії Акту завершується у серпні 2026 р., після чого повною мірою набувають чинності вимоги щодо високоризикових систем ШІ, управління та прозорості, а санкції за найсерйозніші порушення можуть сягати 35 млн євро або 7% глобального річного обороту компанії [12]. Для бізнесу, який використовує алгоритмічні системи в кадровій роботі, маркетингу чи обслуговуванні клієнтів, це означає перехід від добровільної етики штучного інтелекту до обов'язкового комплаєнсу, що потребує завчасного інвентаризування систем ШІ, їх класифікації за рівнем ризику та розробки внутрішніх процедур етичного врядування – елементів, які відповідно до концепції CDR становлять частину виміру «етичне використання технологій» [8; 16].

Третім проблемним напрямом соціальної відповідальності бізнесу в умовах діджиталізації є цифровий розрив (digital divide) – нерівний доступ до цифрових технологій та нерівні можливості їх ефективного використання, що виявляється у розрізі міської й сільської місцевості, вікових груп, рівня доходів, а також між розвиненими і такими, що розвиваються, економіками. Цифрова інклюзія дедалі частіше визнається одним із визначальних пріоритетів ESG-порядку денного XXI ст., оскільки довгострокова конкурентоспроможність бізнесу залежить від рівня цифрової залученості суспільства, у якому він оперує: чим глибший цифровий розрив, тим вужчим є потенційний ринок цифрових продуктів і послуг та тим гострішою – соціальна напруга навколо цифровізації.

Для українського бізнесу проблема цифрового розриву має виражений регіональний і безпековий вимір: воєнні дії спричиняють внутрішню міграцію, руйнування інфраструктури зв'язку та електропостачання, що поглиблює нерівність доступу до цифрових сервісів між регіонами [1]. Соціально відповідальна поведінка бізнесу в цьому контексті виходить за межі традиційної благодійності і включає інвестиції у відновлення цифрової інфраструктури, забезпечення доступності цифрових сервісів для вразливих груп населення (людей похилого віку, внутрішньо переміщених осіб, осіб з інвалідністю) та розроблення цифрових продуктів з урахуванням принципів універсального дизайну. Г. Лучко у дослідженні розвитку соціальної відповідальності бізнесу в Україні наголошує, що впровадження регулярної звітності зі сталого розвитку за ESG-показниками, яка дедалі частіше включає цифровий вимір, дозволяє підприємствам підвищувати ділову репутацію та конкурентоспроможність на міжнародному ринку [3], що опосередковано стимулює бізнес враховувати проблематику цифрової інклюзії у власних стратегіях.

Четвертий напрям пов'язаний зі стрімким зростанням платформної (gig) зайнятості – роботи, опосередкованої цифровими платформами, від таксі та доставки їжі до догляду за особами й виконання мікрозавдань онлайн. За оцінками Міжнародної організації праці, обсяги платформної зайнятості практично подвоїлися в період 2016–2021 рр., а за оцінками Світового банку, дохід через цифрові трудові платформи отримують до 435 млн осіб у світі [13; 14]. Специфіка цієї форми зайнятості полягає в тому, що ключові аспекти роботи – розподіл завдань, оплата, оцінювання якості виконання, навіть відключення від платформи – визначаються алгоритмічними системами управління (algorithmic management), часто без прозорості для самих працівників і без механізмів оскарження автоматизованих рішень [13].

Ця ситуація тривалий час залишалася поза межами традиційного трудового законодавства, оскільки більшість платформ класифікують працівників як самозайнятих, а не найманих працівників, що звільняє компанії від обов'язків щодо мінімальної заробітної плати, охорони праці та соціального страхування [13]. Переломним моментом стало ухвалення 12 червня 2026 р. на 114-й сесії Міжнародної конференції праці Конвенції МОП № 193 про гідну працю в платформній економіці – першого обов'язкового міжнародного договору, що встановлює стандарти праці для гіг-працівників [14]. Конвенція вимагає від урядів забезпечити коректну класифікацію статусу платформних працівників, гарантує право на своєчасну оплату та повну інформацію про її нарахування, право працівника на отримання письмового пояснення й перегляду автоматизованих рішень, що негативно впливають на його роботу (включно з невилплатою, призупиненням чи відключенням від платформи за участю людини), а також захист приватності й персональних даних працівників [14].

Для бізнесу, що використовує платформні моделі організації праці або алгоритмічні системи управління персоналом загалом, ухвалення цієї конвенції означає перехід від суто добровільних ініціатив соціальної

відповідальності до окресленого міжнародного стандарту, який, найімовірніше, поступово транспонуватиметься в національні законодавства держав-членів МОП, включно з Україною в перспективі євроінтеграційного зближення регуляторних систем. Соціально відповідальна платформна бізнес-модель, таким чином, повинна включати прозорість алгоритмічного управління, механізми людського перегляду автоматизованих рішень і гарантії базового соціального захисту незалежно від формального статусу зайнятості виконавця.

П'ятий проблемний напрям – це ширше питання відповідальності бізнесу за наслідки автоматизації робочих місць для ринку праці загалом. Впровадження технологій, що замінюють людську працю (від систем автоматизованої обробки документів до генеративного штучного інтелекту, здатного виконувати частину інтелектуальних завдань), ставить перед підприємствами питання, що виходить за межі внутрішньої кадрової політики: якою мірою бізнес несе відповідальність за перекваліфікацію працівників, чиї функції автоматизуються, і за пом'якшення соціальних наслідків структурного безробіття, спричиненого технологічними змінами.

У межах концепції CDR цей вимір частково охоплюється категорією «цифрове благополуччя» (digital well-being), яка передбачає врахування впливу цифрових технологій не лише на клієнтів, а й на власних працівників підприємства [16]. Соціально відповідальний підхід до автоматизації передбачає завчасне інформування працівників про плановані технологічні зміни, інвестиції в програми перекваліфікації та підвищення кваліфікації, а також поступове, а не одномоментне впровадження технологій, що замінюють людську працю, з урахуванням соціальних наслідків для трудового колективу й місцевої громади. Для українського бізнесу це питання набуває особливої гостроти в контексті післявоєнного відновлення, коли, з одного боку, дефіцит робочої сили внаслідок мобілізації та міграції населення стимулює прискорену автоматизацію, а з іншого – відновлення зайнятості й повернення внутрішньо переміщених осіб до продуктивної праці є критично важливим завданням соціально-економічної стабільності.

Узагальнення розглянутих проблемних напрямів засвідчує, що прояв цифрової соціальної відповідальності бізнесу в Україні має принаймні три специфічні риси порівняно із загальносвітовим контекстом.

По-перше, воєнний стан виступає одночасно каталізатором і бар'єром цифрової трансформації: з одного боку, бізнес змушений пришвидшено переходити у цифровий формат для збереження операційної спроможності в умовах релокації, порушення логістичних ланцюгів і обстрілів інфраструктури [1], з іншого – ці ж чинники ускладнюють рівномірний, соціально відповідальний розподіл переваг цифровізації між регіонами та групами населення. О. Серікова слушно зазначає, що воєнні виклики трансформували самі критерії корпоративної соціальної відповідальності: до традиційних напрямів додалися фінансова й гуманітарна допомога, IT-підтримка (безкоштовний доступ до цифрових

ресурсів), цифровий супровід релокації бізнесу та збереження зайнятості персоналу, який часто перейшов у режим цілодобової роботи [5]. Це означає, що цифрова соціальна відповідальність українського бізнесу під час війни набула виразного адаптивного, кризового характеру, на відміну від переважно проактивного, стратегічного характеру CDR-ініціатив західних компаній.

По-друге, курс на європейську інтеграцію формує для українського бізнесу подвійний регуляторний тиск: необхідність одночасно відповідати вимогам національного законодавства, яке в частині захисту даних усе ще спирається на застарілий закон 2010 р. [2], і випереджувально готуватися до стандартів GDPR та Акту ЄС про штучний інтелект, оскільки саме відповідність цим стандартам визначає спроможність українських компаній інтегруватися в європейські ланцюги постачання цифрових послуг [6; 11; 12]. Ю. Магиляс слушно зауважує, що концепція соціально відповідального бізнесу в Україні все ще недостатньо узгоджується з процесами цифровізації й глобалізації та не виступає джерелом об'єднання представників усіх рівнів українського бізнесу [4], що додатково ускладнює вироблення єдиних галузевих стандартів цифрової відповідальності.

По-третє, для українського бізнесу питання цифрової соціальної відповідальності дедалі тісніше пов'язується з ESG-порядком денним: Г. Лучко демонструє, що компанії – лідери запровадження КСВ в Україні дедалі активніше включають цифрові аспекти (кібербезпеку, цифрову інклюзію, прозорість використання даних) до власних ESG-стратегій, оскільки це безпосередньо впливає на присутність компанії в міжнародних ESG-рейтингах і, відповідно, на доступ до міжнародного капіталу [3].

На основі проведеного аналізу можна виокремити комплекс взаємопов'язаних напрямів інституціоналізації соціально відповідальних практик цифровізації бізнесу.

На рівні окремого підприємства доцільним є формування внутрішньої політики цифрової відповідальності (Corporate Digital Responsibility Policy), яка інтегрувала б усі виокремлені проблемні напрями – захист даних, етику алгоритмів, цифрову інклюзію, права платформних працівників і відповідальність за автоматизацію – в єдиний документ, що визначає цінності та процедури компанії щодо цифрових технологій, за аналогією з тим, як CDR розглядається в науковій літературі як логічне продовження КСВ [16]. Практичним інструментом реалізації такої політики може бути створення внутрішніх комітетів або відповідальних осіб з етики штучного інтелекту, що здійснюють попередню оцінку впливу нових алгоритмічних систем до їх впровадження – підхід, що узгоджується з вимогами ризик-орієнтованого регулювання, закладеними в Акті ЄС про штучний інтелект [12]. Разом з тим, оскільки підприємство є частиною цифрової екосистеми національної економіки, то необхідно розглянути пріоритетні напрямки регулювання штучного інтелекту та автоматизованих систем керування на галузевому та державному рівнях.

На галузевому рівні доцільним є розроблення

секторальних стандартів і кодексів цифрової відповідальності, які враховували б специфіку окремих видів економічної діяльності (фінансовий сектор, IT, роздрібна торгівля, платформна економіка), а також поширення практики включення цифрового виміру до ESG-звітності підприємств, що вже демонструє позитивний вплив на конкурентоспроможність українських компаній [3].

На державному рівні пріоритетними напрямами є пришвидшення ухвалення законодавства про захист персональних даних, гармонізованого з GDPR, з обов'язковим створенням незалежного наглядового органу [6; 11], підготовка національної імплементаційної рамки для поступового приведення регулювання штучного інтелекту у відповідність до підходів ЄС [12], а також вивчення можливостей ратифікації Конвенції МОП № 193 про гідну працю в платформній економіці з адаптацією її вимог до національного трудового законодавства [14]. Держава також може відігравати роль катализатора цифрової інклюзії через програми відновлення цифрової інфраструктури в постраждалих від бойових дій регіонах у партнерстві з бізнесом.

Нарешті, на рівні суспільного діалогу необхідним є формування майданчиків взаємодії бізнесу, держави та громадянського суспільства для вироблення консенсусних підходів до цифрової відповідальності – напрям, важливість якого підкреслюють українські дослідники, наголошуючи на потребі синергетичної взаємодії бізнесу з державною владою, що враховує вітчизняну специфіку соціально-економічного середовища [4].

Висновки. Проведене дослідження дало змогу систематизувати ключові проблемні напрями соціальної відповідальності бізнесу в умовах його діджиталізації та обґрунтувати шляхи їх інституціоналізації. Встановлено, що традиційна концепція корпоративної соціальної відповідальності, сформована навколо економічного, правового, етичного та філантропічного вимірів, потребує розширення за рахунок концепції корпоративної цифрової відповідальності (CDR), яка охоплює специфічні для цифрового середовища виміри – захист даних, цифрове благополуччя, цифрову інклюзію та етичне використання технологій.

Систематизація проблемних напрямів дала змогу виокремити п'ять ключових сфер, у яких соціальна відповідальність бізнесу стикається з новими викликами внаслідок діджиталізації: захист персональних даних і цифрова приватність; алгоритмічна упередженість та етика штучного інтелекту; цифровий розрив і цифрова інклюзивність; права працівників цифрових платформ і прозорість алгоритмічного менеджменту; відповідальність бізнесу за соціальні наслідки автоматизації ринку праці. Кожен із цих напрямів має власну динаміку регуляторного розвитку – від Регламенту GDPR і Акту ЄС про штучний інтелект до щойно ухвалені Конвенції МОП № 193 про гідну працю в платформній економіці, – що свідчить про поступовий перехід цифрової соціальної відповідальності від суто добровільних корпоративних ініціатив до обов'язкових регуляторних вимог.

Для українського бізнесу доведено наявність трьох специфічних рис прояву цих проблем: адаптивно-

кризовий характер цифрової трансформації в умовах війни; подвійний регуляторний тиск, зумовлений необхідністю одночасного дотримання застарілого національного законодавства й випереджувальної підготовки до європейських стандартів; тісний взаємозв'язок цифрової відповідальності з ESG-порядком денним як чинником міжнародної конкурентоспроможності.

Практична цінність одержаних результатів полягає в обґрунтуванні багаторівневого комплексу напрямів інституціоналізації цифрової соціальної відповідальності – від впровадження внутрішньокорпоративних політик і комітетів з етики ШІ до пришвидшення гармонізації національного законодавства з європейськими стандартами захисту даних і регулювання штучного інтелекту. Ці напрями можуть бути використані менеджментом підприємств для розроблення власних стратегій цифрової відповідальності, а органами державної влади – для формування регуляторної політики у сфері цифровізації бізнесу.

Перспективи подальших досліджень пов'язані з

розробленням кількісного інструментарію оцінювання рівня цифрової соціальної відповідальності підприємств, зокрема системи індикаторів для інтеграції цифрового виміру до ESG-звітності українських компаній, а також з емпіричним дослідженням готовності українського бізнесу до впровадження принципів корпоративної цифрової відповідальності в умовах післявоєнного відновлення.

Декларація про використання ШІ. У процесі підготовки статті автори використовували інструмент штучного інтелекту Claude (модель Claude Sonnet 5, розробник Anthropic) для пошуку та попередньої систематизації наукових джерел за темою дослідження, а також для структурування тексту статті й підготовки його чорнового варіанта. Усі статистичні дані та бібліографічні джерела, використані в статті, перевірені авторами на відповідність першоджерелам. Наукове узагальнення, формулювання висновків, а також відповідальність за зміст і достовірність статті повністю належать авторам.

Список використаних джерел:

1. Євтушенко Н., Стеценко Д. Цифрова трансформація бізнесу в умовах війни в Україні: виклики та можливості. *Економічний простір*. 2024. № 191. С. 211–216. DOI: <https://doi.org/10.32782/2224-6282/191-34>
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 29.07.2026).
3. Лучко Г. Соціальна відповідальність бізнесу в Україні. *Економіка та суспільство*. 2024. № 67. DOI: <https://doi.org/10.32782/2524-0072/2024-67-130>
4. Магиляс Ю. Соціально відповідальний бізнес в умовах цифрової трансформації суспільства. *Аспекти публічного управління*. 2022. Т. 10, № 6. С. 55–60. DOI: <https://doi.org/10.15421/152244>
5. Серікова О. М. Корпоративна соціальна відповідальність бізнесу в умовах війни в Україні: національний і глобальний виміри. *Бізнес Інформ*. 2022. № 6. С. 94–100. DOI: <https://doi.org/10.32983/2222-4459-2022-6-94-100>
6. Слободянюк Д. Захист персональних даних (GDPR / Директива ЄС): що змінюють нові законопроекти в Україні. *Юридична газета*. (13 квіт. 2025). URL: <https://yur-gazeta.com/dumka-eksperta/zahist-personalnih-danih-gdpr--direktiva-es-shcho-zminyuyut-novi-zakonoproekti-v-ukrayini.html> (дата звернення: 29.07.2026).
7. Bowen H. R. *Social Responsibilities of the Businessman*. New York : Harper & Row, 1953. 276 p. URL: <https://ia601509.us.archive.org/20/items/in.ernet.dli.2015.126534/2015.126534.Social-Responsibilities-Of-The-Businessman.pdf> (дата звернення: 29.07.2026).
8. Camilleri M. A. Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems*. 2024. Vol. 41, No. 7. Art. e13406. DOI: <https://doi.org/10.1111/exsy.13406>
9. Carroll A. B. Corporate social responsibility: Evolution of a definitional construct. *Business & Society*. 1999. Vol. 38, Iss. 3. Pp. 268–295. DOI: <https://doi.org/10.1177/000765039903800303>
10. Chen Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*. 2023. Vol. 10. Art. 567. DOI: <https://doi.org/10.1057/s41599-023-02079-x>
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*. L 119. Pp. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата звернення: 29.07.2026).
12. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата звернення: 29.07.2026).
13. Human Rights Watch. ILO Adopts Landmark Treaty on Gig Work. 2026. URL: <https://www.hrw.org/news/2026/06/12/ilo-adopts-landmark-treaty-on-gig-work> (дата звернення: 29.07.2026).
14. Convention concerning decent work in the platform economy, 2026 (No. 193). *International Labour Conference*, 114th Session. Geneva : International Labour Organization, 2026. URL: <https://www.ilo.org/resource/record-decisions/convention-concerning-decent-work-platform-economy-2026> (дата звернення: 29.07.2026).
15. ISO 26000:2010. Guidance on social responsibility. URL: <https://www.iso.org/standard/42546.html> (дата звернення: 29.07.2026).
16. Lobschat L., Mueller B., Eggers F., Brandimarte L., Diefenbach S., Kroschke M., Wirtz J. *Corporate digital*

responsibility. Journal of Business Research. 2021. Vol. 122. Pp. 875–888.
DOI: <https://doi.org/10.1016/j.jbusres.2019.10.006>

References:

1. Yevtushenko, N., & Stetsenko, D. (2024). Tsyfrova transformatsiia biznesu v umovakh viiny v Ukraini: vyklyky ta mozhlyvosti [Digital transformation of business in the context of war in Ukraine: challenges and opportunities]. *Ekonomichnyi prostir*, (191), 211–216. <https://doi.org/10.32782/2224-6282/191-34>
2. Pro zakhyst personalnykh danykh [On personal data protection]. (2010). *Zakon Ukrainy № 2297-VI* [Law of Ukraine No. 2297-VI]. <https://zakon.rada.gov.ua/laws/show/2297-17>
3. Luchko, H. (2024). Sotsialna vidpovidalnist biznesu v Ukraini [Social responsibility of business in Ukraine]. *Ekonomika ta suspilstvo*, (67). <https://doi.org/10.32782/2524-0072/2024-67-130>
4. Mahylias, Yu. (2022). Sotsialno vidpovidalnyi biznes v umovakh tsyfrovoy transformatsii suspilstva [Socially responsible business in the conditions of digital transformation of society]. *Aspekty Publichnoho Upravlinnia*, 10(6), 55–60. <https://doi.org/10.15421/152244>
5. Serikova, O. M. (2022). Korporatyvna sotsialna vidpovidalnist biznesu v umovakh viiny v Ukraini: natsionalnyi i hlobalnyi vymiry [Corporate social responsibility of business in the conditions of war in Ukraine: national and global dimensions]. *Biznes Inform*, (6), 94–100. <https://doi.org/10.32983/2222-4459-2022-6-94-100>
6. Slobodianiuk D. (13 kvit. 2025). Zakhyst personalnykh danykh (GDPR / Dyrektyva YeS): shcho zminiuiut novi zakonoproekty v Ukraini [Personal data protection (GDPR/EU Directive): what the new bills change in Ukraine]. *Yurydychna Hazeta*. <https://yur-gazeta.com/dumka-eksperta/zahist-personalnih-danih-gdpr--direktiva-es-shcho-zminyuyut-novi-zakonoproekti-v-ukrayini.html>
7. Bowen, H. R. (1953). Social responsibilities of the businessman. Harper & Brothers. <https://ia601509.us.archive.org/20/items/in.ernet.dli.2015.126534/2015.126534.Social-Responsibilities-Of-The-Businessman.pdf>
8. Camilleri, M. A. (2024). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems*, 41(7), e13406. <https://doi.org/10.1111/exsy.13406>
9. Carroll, A. B. (1999). Corporate social responsibility: Evolution of a definitional construct. *Business & Society*, 38(3), 268–295. <https://doi.org/10.1177/000765039903800303>
10. Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, (10), Art. 567. <https://doi.org/10.1057/s41599-023-02079-x>
11. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
12. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
13. Human Rights Watch. (2026, June 12). ILO adopts landmark treaty on gig work. <https://www.hrw.org/news/2026/06/12/ilo-adopts-landmark-treaty-on-gig-work>
14. International Labour Organization. (2026). Convention concerning decent work in the platform economy, 2026 (No. 193). International Labour Conference, 114th Session. <https://www.ilo.org/resource/record-decisions/convention-concerning-decent-work-platform-economy-2026>
15. International Organization for Standardization. (2010). ISO 26000:2010 Guidance on social responsibility. <https://www.iso.org/standard/42546.html>
16. Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, (122), 875–888. <https://doi.org/10.1016/j.jbusres.2019.10.006>

Дата надходження статті: 25.06.2026 р.

Дата прийняття статті до друку: 07.08.2026 р.

Дата публікації (оприлюднення) статті: 01.09.2026 р.

Стаття поширюється на умовах ліцензії Creative Commons Attribution License International CC-BY.