О.А. МАСЛІЙ, А.О. КУДІНОВА,
А.А. БУРЯК, А.С. ЯНКО, С.С. БІЛЬКО

ДЕТЕРМІНАНТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В ПАРАДИГМІ ЦИФРОВОГО РОЗВИТКУ

МОНОГРАФІЯ

О.А. МАСЛІЙ, А.О. КУДІНОВА,
А.А. БУРЯК, А.С. ЯНКО, С.С. БІЛЬКО

ДЕТЕРМІНАНТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В ПАРАДИГМІ ЦИФРОВОГО РОЗВИТКУ

Монографія

Івано-Франківськ 2025

ЗМІСТ

ПЕРЕДМОВА

Трансформаційні зміни глобальної економічної системи, пов'язані з цифровізацією соціально-економічних відносин, формують визначальний вектор суспільного прогресу XXI століття. Інформація та цифрові технології перетворюються з допоміжних інструментів у драйвери економічного розвитку. Внаслідок впровадження інформаційних технологій в усі сфери господарської діяльності відбуваються структурні зрушення в економіці, формуються принципово нові ринкові сегменти та форми взаємодії економічних суб'єктів, що вимагає переосмислення концептуальних засад забезпечення економічної безпеки держави.

Становлення Індустрії 4.0 й прискорена цифровізація національної економіки України виступаючи драйверами економічних перетворень під час широкомасштабної війни зумовлюють появу специфічних деструктивних феноменів (мілітаризації кіберпростору, інформаційних війн, інформаційного тероризму, масштабних відкритих та прихованих кібератак для ведення бойових дій і розвідувально-підривної діяльності), що актуалізує проблему забезпечення економічної безпеки держави на засадах інформаційної захищеності. Економічна безпека держави в парадигмі цифрового розвитку набуває якісно нового змісту, трансформуючись від захисту традиційних національних економічних інтересів до забезпечення цифрового суверенітету, технологічної незалежності та стійкості до кіберзагроз.

Головною метою монографії є теоретичне обґрунтування детермінант економічної безпеки держави та розробка концептуальних засад формування безпекоорієнтованого інформаційного середовища й стратегічних пріоритетів забезпечення економічної безпеки України в умовах цифрового розвитку. Саме цій меті підпорядкована загальна логіка і структура монографії, яка складається із п'яти взаємопов'язаних частин (розділів).

У першому розділі «Структурно-цільовий аналіз впливу цифровізації на забезпечення економічної безпеки держави» надано сутнісно-змістовні характеристики цифровізації, обґрунтовано її дуальний вплив на економічну безпеку держави та визначено домінантні тенденції цифрової трансформації. Проаналізовано передумови розвитку воєнної та повоєнної економіки України в умовах цифрової трансформації, визначено специфіку формування безпекоорієнтованої моделі господарювання. Досліджено особливості використання можливостей штучного інтелекту та віртуальної мобільності для забезпечення економічної безпеки національної економіки в парадигмі Індустрії 5.0. Здійснено формалізацію ризиків і загроз економічній безпеці держави, детермінованих процесами цифровізації, та виокремлено їх типологічні характеристики. На основі таксономічного аналізу ідентифіковано ключові драйвери підвищення економічної безпеки держави в умовах Індустрії 4.0 та

встановлено їх ієрархію за ступенем впливу на забезпечення економічної безпеки держави.

Другий розділ «Інформаційна складова економічної безпеки України у воєнний та повоєнний періоди» присвячено дослідженню інформаційної безпеки як фундаментальної складової економічної безпеки держави в умовах цифровізації. У ньому розкрито сутність та місце інформаційної безпеки в системі національної безпеки, розроблено методичні підходи до оцінювання її рівня та здійснено комплексне оцінювання інформаційної безпеки економіки України. Ідентифіковано тригерні точки впливу інформаційної безпеки на економічну безпеку держави в умовах загроз воєнного стану, що дозволило виявити критичні зони вразливості інформаційного простору.

У третьому розділі «Теоретичні засади формування безпеко-орієнтованого інформаційного середовища» сформовано понятійно-категоріальний базис безпекоорієнтованого інформаційного середовища та визначено орієнтири його розвитку для підвищення економічної безпеки держави в парадигмі цифрового розвитку. Ідентифіковано детермінанти забезпечення економічної безпеки держави в умовах Індустрії 4.0 та здійснено систематизацію загроз в інформаційній сфері, з характеристикою механізмів їх впливу на економічну безпеку, що створює теоретичне підґрунтя для розробки практичних інструментів протидії інформаційним загрозам національній економіці.

У четвертому розділі «Концептуальні засади безпекоорієнтованого інформаційного середовища» розроблено систему кластерів інформаційного середовища за критеріями доступності й пріоритетності захисту інформації, що дозволяє диференціювати підходи до забезпечення інформаційної безпеки відповідно до рівня критичності інформаційних ресурсів. На основі інтерпретаційного структурного моделювання з урахуванням безпекових параметрів розроблено концептуальну модель формування безпекоорієнтованого інформаційного середовища в Україні, що інтегрує організаційні, технологічні та нормативно-правові механізми захисту інформаційного простору держави й спрямована на захист національних економічних інтересів. Обґрунтовано концепцію розвитку високонадійних систем захисту інформації для забезпечення економічної безпеки держави в умовах війни та повоєнний період, яка передбачає створення багаторівневої системи кібербезпеки з елементами резервування та швидкого відновлення критичної інфраструктури.

Завершальну частину монографії – п’ятий розділ «Управлінський інструментарій підвищення рівня економічної безпеки України у воєнний та повоєнний періоди» − присвячено обґрунтуванню сукупності управлінських інструментів, придатних для використання у публічному управлінні для забезпечення економічної безпеки держави в умовах цифрової трансформації. Проведено моделювання взаємозв’язку рівня економічної безпеки з ключовими параметрами кіберстійкості, що є базисом для обґрунтування стратегічних

пріоритетів захисту національних економічних інтересів в умовах зростаючих кіберзагроз. Узагальнено європейський досвід зміцнення економічної безпеки на засадах кіберстійкості, розроблено дорожню карту інтеграції України до Єдиного цифрового ринку ЄС на засадах мінімізації цифрових ризиків і загроз та обґрунтовано стратегічні пріоритети підвищення економічної безпеки держави на засадах проактивного управління з використанням інформаційних технологій. Сформульовано практичні рекомендації щодо мінімізації деструктивного впливу кіберзагроз на економічну безпеку в умовах війни та в повоєнний період.

Важливість проведеного дослідження визначається упорядкуванням та систематизацією наявних знань щодо об'єктивної природи впливу цифровізації на систему економічної безпеки держави, виявлення детермінант і загроз економічній безпеці в умовах цифрової трансформації (у тому числі представлених у численних публікаціях з цієї проблематики) і на цій основі – подальшим поглибленням, уточненням та розвитком цих знань з позицій дуального впливу цифровізації. Це дозволяє сформувати концептуальні засади формування безпекоорієнтованого інформаційного середовища як фундаментальної основи забезпечення економічної безпеки держави в умовах Індустрії 4.0 та переходу до Індустрії 5.0. Саме інтеграція теоретичного осмислення детермінант економічної безпеки в парадигмі цифрового розвитку, концептуалізація механізмів формування безпекоорієнтованого інформаційного середовища та розробка практичного управлінського інструментарію підвищення економічної безпеки у воєнний та повоєнний періоди на основі ефективних систем захисту інформації відрізняє це дослідження від попередніх наукових розвідок і визначає вагомість його результатів для теорії та практики забезпечення економічної безпеки держави в парадигмі цифрового розвитку.

Монографія розраховано на науковців, викладачів, студентів, державних службовців і широке коло читачів, які цікавляться актуальними проблемами забезпечення економічної безпеки України в умовах цифровізації.

Автори висловлюють щиру вдячність рецензентам: докторам економічних наук, професорам З.С. Варналію, В.П. Мартинюку та Г.В. Назаровій за високу оцінку монографії, змістовні поради при її написанні та приділений час.

Змістовне та грунтовне дослідження стало можливим за фінансової підтримки Міністерства освіти і науки України у рамках виконання НДР молодих вчених (державний реєстраційний номер 0124U000615).

Р о з д і л 1

СТРУКТУРНО-ЦІЛЬОВИЙ АНАЛІЗ ВПЛИВУ ЦИФРОВІЗАЦІЇ НА ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Сутність, значення, домінантні тенденції та дуальний вплив цифровізації

Цифрова трансформація соціально-економічних відносин за характером поширення та впливу на економічну систему набула ознак домінантної парадигми сучасного етапу глобального розвитку. На відміну від попередніх технологічних укладів, Індустрія 4.0 характеризується нелінійністю, стрімким розвитком інновацій, автоматизацією процесів прийняття рішень через алгоритми штучного інтелекту та формуванням цифрової ідентичності як невід'ємного атрибуту економічної активності.

За таких умов відбувається фундаментальне переосмислення природи конкурентних переваг, механізмів створення доданої вартості та ролі держави в регулюванні економічних процесів. Тому концептуалізація феномену цифровізації та його впливу на економічну безпеку держави потребує комплексного аналізу сутнісних характеристик і дуальної природи цифрової трансформації економічних відносин.

Згідно з найбільш розповсюдженим та досить широким визначенням експертів Світового банку, цифровізація вважається новою парадигмою прискореного економічного розвитку, що базується на обміні даними в режимі реального часу [1]. До основних технологічних драйверів економічного розвитку в умовах цифровізації варто віднести аналіз великих даних, Інтернет речей (IoT), хмарні технології, 3D-друк та, особливо, штучний інтелект (ШІ) [2, 3]. Саме ці технології змінюють господарську діяльність, перетворюючи дані у цифровому вигляді на ключовий чинник економічного розвитку.

Еволюцію цифровізації економічних процесів доцільно структурувати через призму інтенсивності проникнення технологій в економічні процеси. Перша хвиля (1990-2000 рр.) характеризувалася становленням цифрової інфраструктури та появою перших електронних продуктів. Друга фаза (2000-2010 рр.) ознаменувалася розгортанням електронної торгівлі та формуванням онлайн-екосистем. Третій період (2010-2020 рр.) відзначився трансформацією бізнес-моделей через цифрові канали взаємодії [4]. Наразі спостерігається четверта стадія, яка розпочалася умовно на початку 2020-х років і характеризується функціонуванням і використанням алгоритмів машинного навчання та систем штучного інтелекту [5].

Для комплексного розуміння сутності цифровізації як незворотного обєктивного процесу новітнього етапу суспільного розвитку науковці виділяють її прояви, якими є цифрові технології, рішення та послуги [6–9]. Цифрові технології являють собою сукупність методологічних прийомів та інструментів оперування цифровими даними і передачі інформації. Цифрові рішення репрезентують інтегровані програмно-апаратні комплекси, що застосовують цифрові технології для розв'язання операційних завдань. Цифрові послуги являють собою форму надання комерційних та публічних сервісів через цифрові канали та телекомунікаційні мережі [10]. Для поглиблення розуміння змісту цифрових процесів доцільно структурувати систему взаємозв'язків між проявами та наслідками цифровізації (рис. 1.1).

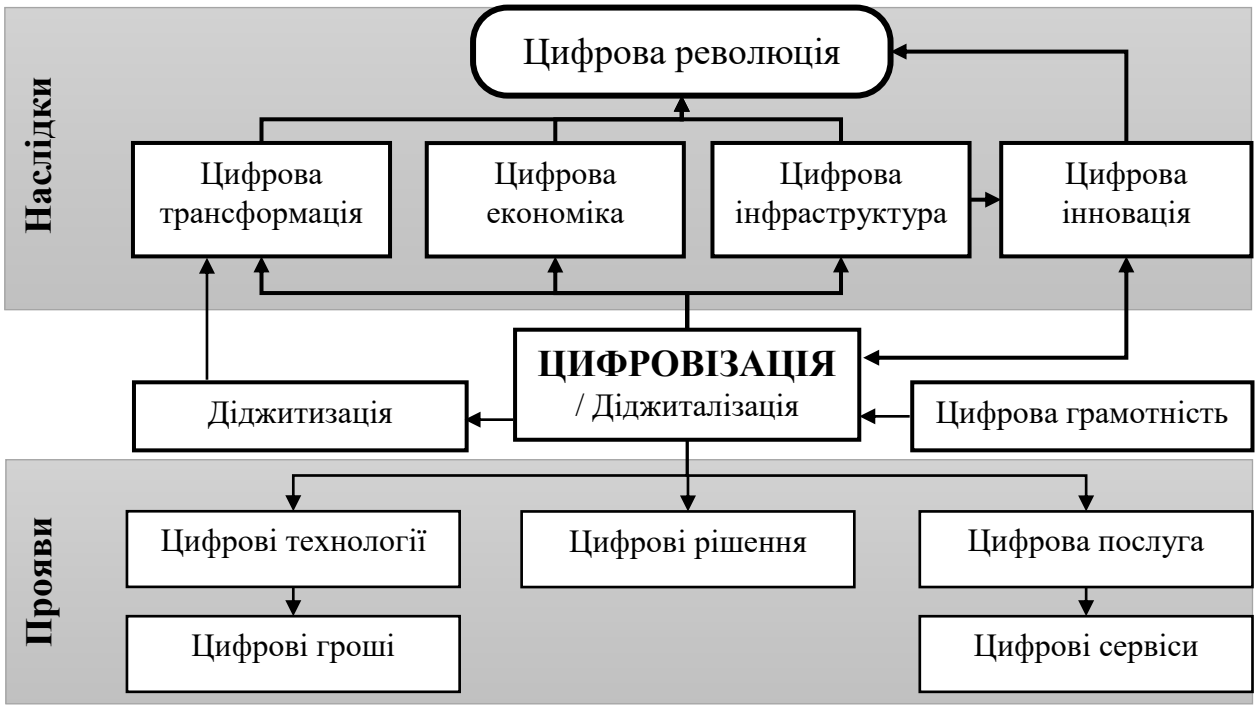

Рис. 1.1. Взаємозв'язок наслідків та проявів цифровізації
** за матеріалами [10]*

Цифрові технології активно проникають в ключові сектори економіки, фундаментально змінюючи бізнес-моделі та операційні процеси. Тому цифровізація є не просто модернізацією, а повним переосмисленням способів ведення господарської діяльності, що зрештою підвищує стійкість та гнучкість економіки в цілому.

У парадигмі цифрового розвитку однією із основних глобальних проблем є нерівномірний розподіл благ від цифровізації. Загальносвітова статистика свідчить, що значна частина населення досі не має доступу до Інтернету, що створює так звані «цифрові розриви». Дана проблема є небезпечною для країн, що розвиваються, оскільки може призвести до ще більшого відставання [11].

Значення цифровізації для суспільного прогресу визначено у основних законодавчих актах більшості країн через розробку низки стратегічних ініціатив цифрового розвитку. В Україні однією з найважливіших є Стратегія цифрового розвитку інновацій України до 2030 року [11], де визначено бачення України як лідера у сфері технологій та інновацій, пріоритезуючи такі галузі, як DefenseTech, MedTech, AI та Agritech.

Значення цифровізації для розвитку національної економіки проявляється через її стимулюючий вплив у секторальному розрізі. Так, найактивніше та еволюційно першочергово цифрові технології проникають у фінансовий сектор. Банківські та небанківські фінансові установи переглянули традиційні бізнес-моделі, що базуються на фізичних філіях та офісах, на користь більш гнучких та цифрових підходів. Автоматизація багатьох банківських процесів, таких як кредитний скоринг та обробка документів, значно підвищила їх ефективність і знизила операційні витрати. Перехід до електронного документообігу, використання чат-ботів для взаємодії з клієнтами та впровадження автоматизованих процесів на основі ШІ оптимізує роботу та прискорює надання послуг [12].

Для великого, середнього та малого бізнесу впровадження сучасних цифрових технологій, включаючи хмарні послуги, аналіз великих даних, ШІ та електронну комерцію, дозволяє оптимізувати бізнес-процеси, розширити ринок збуту та знизити витрати. Онлайн-платформи та цифрові інструменти маркетингу дозволяють охопити ширшу, навіть глобальну аудиторію, тоді як автоматизація управління запасами та прогнозування попиту роблять бізнес-моделі більш адаптивними до ринкових змін [13]. Завдяки цьому відбувається зростання ділової активності бізнесу [14], продуктивності праці, що безпосередньо впливає на його економічне зростання.

За результатами досліджень Європейського центрального банку встановлено, що підприємства, які істотно нарощують інвестиції в цифрові технології, протягом п’яти років після їх упровадження демонструють зростання як продуктивності праці, так і сукупної факторної продуктивності, причому відповідний приріст коливається в межах від 20 % до 300 % [15].

Показовим також є значення цифровізації для розвитку аграрного сектору, що формує вагому частку ВВП України. Використання дронів, датчиків, систем Інтернету речей та аналізу великих даних сприяє оптимізації управління ресурсами аграрних підприємств, зокрема зменшенню витрат на добрива та пестициди [16]. Комплексне управління технікою, системний облік палива, точне та розумне землеробство забезпечують безперервний збір і аналіз даних й дозволяють сільськогосподарським підприємствам приймати ефективні рішення, підвищувати точність планування, оптимізувати витрати, підвищувати рентабельність та продуктивність.

Разом із цим розвиток електронних сервісів, що забезпечують можливість дистанційної взаємодії громадян з органами публічної влади та доступу до інформаційних ресурсів у цифровому середовищі суттєво прискорює всі

соціально-економічні процеси. Інтеграція принципів інклюзивності в архітектуру онлайн-послуг зумовила перетворення цифровізації на загальносуспільний процес, розширивши її межі за рамки суто комерційної діяльності та закріпивши її значення на рівні державного управління.

Цифровізація характеризується циклічністю розвитку, адже кожна наступна фаза цифрового розвитку акумулює досягнення попередніх періодів і водночас формує передумови для появи та масштабування нових цифрових технологій, рішень і сервісів (рис. 1.2). У результаті технологічні інновації, що раніше розглядалися як передові, поступово набувають статусу базових, що сприяє поглибленню проникнення цифрових рішень у більш традиційні та інерційні сектори національної економіки.

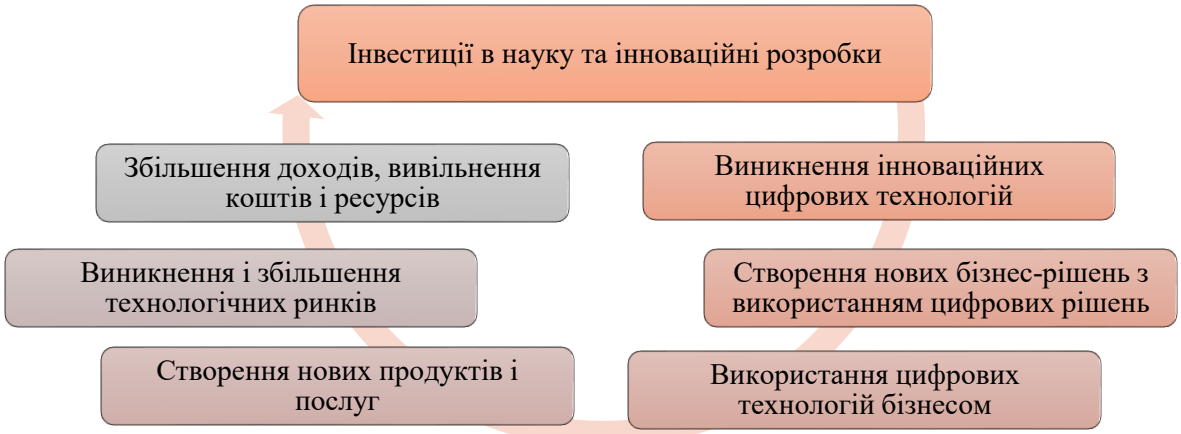

Рис. 1.2. Циклічність цифрового розвитку
* *розроблено авторами*

Причини циклічного характеру розвитку цифровізації значною мірою зумовлені безперервним зростанням обчислювальних можливостей інформаційних систем, яке концептуально відображається у відомому «законі Мура». Підвищення продуктивності напівпровідникових технологій забезпечує можливість оброблення дедалі складніших алгоритмів, що, у свою чергу, стимулює створення високофункціонального програмного забезпечення та відкриває простір для впровадження нових технічних і організаційних рішень. Аналогічні трансформаційні процеси спостерігаються і в економічній площині, де автоматизація та зростання ефективності діяльності сприяють вивільненню ресурсів, які можуть бути реінвестовані у подальший цифровий розвиток [10].

Циклічний характер розвитку цифровізації зумовлює прискорене формування та масштабування нових цифрових ринків, зокрема електронної комерції, фрилансу, криптовалют і блокчейн-технологій, хмарних сервісів, онлайн-платформ, віртуальної реальності та цифрового контенту. За оцінками UNCTAD [19], обсяг ІКТ-сектору нині становить від 4,5 % до 15,5 % світового ВВП, що еквівалентно 3,4–12,7 трлн дол. США, та свідчить про значний потенціал подальшого розвитку цієї сфери в національних економіках.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ
(до розділу 5)

1. Буряк А.А. Безпекове середовище України в контексті євроінтеграційних процесів. *Економічна безпека: держава, регіон, підприємство:* матеріали VIII Міжнародної науково-практичної конференції, 16 травня 2024 р. Полтава: НУПП, 2024. С. 209 – 212.
2. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu.
3. Buriak A.A. Institutional provision of economic, information and ecological security. *The 23rd International Conference on Information Technologies and Management 2024*. April 25-26, 2024, ISMA University of Applied Science. Riga, Latvia. Pp. 47 – 49. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/500/13309/27856-1?inline=1.
4. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/
5. NIS2 Directive (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union – NIS 2. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/ojnis-2-directive.com
6. Digital Operational Resilience Act (DORA) (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector. URL: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en
7. General Data Protection Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
8. Eurostat (2025). Digital Economy and Society Statistics. URL: https://ec.europa.eu/eurostat/web/digital-economy-and-society/database.
9. CERT-UA Annual Report (2024–2025). State Service of Special Communications of Ukraine. URL: https://cert.gov.ua.
10. The Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU). URL: https://cert.europa.eu/
11. European Cybersecurity Competence Centre (ECCC) (2025). European Cybersecurity Competence Centre. URL: https://cybersecurity-centre.europa.eu/home-0_en?page=2&prefLang=el
12. European Commission. URL: https://commission.europa.eu/index_en
13. Угода про асоціацію між Україною та ЄС (2014). Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part.

URL: https://www.kmu.gov.ua/storage/app/sites/1/ugoda-pro-asociaciyu/00ukraine-euassociationagreementbody.pdf

14. Міністерство цифрової трансформації України (2020). Дорожня карта інтеграції України до Єдиного цифрового ринку ЄС (оновлена). URL: https://thedigital.gov.ua/news/technologies/mintsifra-predstavila-onovlenu-dorozhnyu-kartu-integratsii-do-edinogo-tsifrovogo-rinku-es

15. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України. *Кабінет Міністрів України*. URL: https://zakon.rada.gov.ua/go/204-2025-%D1%80

16. ISO/IEC 27001 (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001

17. Best Practices for Cyber Crisis Management. *ENISA.* 2024. URL: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

18. Cybersecurity Guidelines for SMEs. *ENISA.* 2022. URL: https://www.enisa.europa.eu/publications/cybersecurity-guidelines-for-smes

19. Artificial Intelligence Cybersecurity Recommendations. *ENISA*. 2023. URL: https://www.enisa.europa.eu/publications/ai-cybersecurity-recommendations

20. EU Cyber Resilience Act (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

21. 2024 Report on the State of Cybersecurity in the Union. *ENISA.* URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

22. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/2297-17

23. Buriak A.A. Main areas of activity in the sphere of providing information security of the state. *Міжнародна та національна безпека: теоретичні і прикладні аспекти*: матеріали VIII Міжнар. наук.- практ. конф. (м. Дніпро, 15 бер. 2024 р.); у 2-х ч. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2024. Ч. II. С. 305 – 307. DOI: https://doi.org/10.31733/15-03-2024/2/305-307.

24. Буряк А.А. Роль міжнародних організацій у формуванні та реалізації стратегій міжнародної інформаційної безпеки. *Пріоритети розвитку національної економіки в умовах глобалізації*: матеріали III Всеукраїнської науково-практичної Інтернет-конференції, 27 березня 2024 р. Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка». 2024. С. 32 – 33.

25. Ministry of Digital Transformation of Ukraine (2025). *Annual Report on Digital Resilience and Cybersecurity*. URL: https://thedigital.gov.ua

26. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association.* 2023. 29(5). pp. 818–835.

27. Стратегія забезпечення державної безпеки. *Указ Президента України* від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

28. Про Стратегію економічної безпеки України на період до 2025 року. *Указ Президента України* від 11 серпня 2021 року № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#n2

29. Varnaliy Z., Onishchenko S., Masliy A. Preventing threats as a precondition to increase the level of Economic Security of the State. Scientific Journal «ScienceRise». 2016. № 7/1 (24). С. 41-46. DOI: https://doi.org/10.15587/2313-8416.2016.74409

30. Hang, Y., & Chen, Z. (2022). How to realize the full potentials of artificial intelligence in digital economy? Journal of Digital Economy, 1(3), 180–191. https://doi.org/10.1016/j.jdec.2022.11.003

31. Maslii O., Buriak A., Chaikina A., Cherviak A. Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies*. 2025. Vol 133. Issue 13. Pp. 35-45. DOI: https://doi.org/10.15587/1729-4061.2025.319256

32. Griffioen, P., Krogh, B. H., & Sinopoli, B. (2024). Ensuring resilience against stealthy attacks on cyber-physical systems. IEEE Transactions on Automatic Control, 69(12), 8234–8246. https://doi.org/10.1109/TAC.2024.3401013

33. Birthriya, S. K., Ahlawat, P., Jain, A. K. (2024). A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies. Journal of Applied Security Research, 20(2), 244–292. https://doi.org/10.1080/19361610.2024.2372986

34. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. *Economic and Cyber Security*, 30–58. https://doi.org/10.15587/978-617-7319-98-5.ch2

35. Parkin, S., Kuhn, K., & Shaikh, S. A. (2023). Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. Journal of Cybersecurity, 9(1), Article tyad018. https://doi.org/10.1093/cybsec/tyad018

36. Ho, H., Ko, R., Mazerolle, L., Gilmour, J., & Miao, C. (2024). Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes. Journal of Cybersecurity, 10(1), Article tyae020. https://doi.org/10.1093/cybsec/tyae020

37. Khan, K., Khurshid, A., & Cifuentes-Faura, J. (2024). Is artificial intelligence a new battleground for cybersecurity? Research Policy, 53(1), 101804. https://doi.org/10.1016/j.respol.2023.101804

38. Onyshchenko, S. V., Masliy, O. A., Buriak, A. A. (2023). Threats and Risks of Ecological and Economic Security of Ukraine in the Conditions of War. 17th International Conference Monitoring of Geological Processes and Ecological Condition of the Environment, 1–5. https://doi.org/10.3997/2214-4609.2023520072

39. Portulans Institute. (2024). The Network Readiness Index 2024. Available at: https://networkreadinessindex.org/

40. Kyiv School of Economics. (2024). Report on direct damages to infrastructure due to Russia's military aggression against Ukraine as of early 2024. Available at: https://kse.ua/wp-content/uploads/2024/04/01.01.24_Damages_Report.pdf

41. Ministry for Communities, Territories and Infrastructure Development of Ukraine. (2024). Digital Restoration Ecosystem for Accountable Management (DREAM). Available at: https://dream.gov.ua

42. Ministry of Digital Transformation of Ukraine. (2024). Digital Transformation Index of Ukraine 2024. Analytical Report. Available at: https://thedigital.gov.ua

43. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E. (2018). Influence of diagnostics errors on safety: Indicators and requirements. Proceedings of the 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 24–27, 53–57. https://doi.org/10.1109/DESSERT.2018.8409098

44. Artificial Intelligence Act (AI Act) (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council on harmonised rules on Artificial Intelligence. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

45. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC. URL: https://op.europa.eu/en/publication-detail/-/publication/3ff67256-55c4-11ed-92ed-01aa75ed71a1/language-en

46. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150

47. Digital Markets Act (DMA) (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector. URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj

48. Data Act (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854

49. Data Governance Act (DGA) (2022). Regulation (EU) on European data governance. URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

50. Maslii, O., Maksymenko, A. (2025). Digital transformation and economic deindustrialisation: Impact on state financial security. Financial and Credit Activity: Problems of Theory and Practice, 1(60), 401-414. https://doi.org/10.55643/fcaptp.1.60.2025.4599

51. United Nations, Department of Economic and Social Affairs. (2024). E-Government Development Index 2024. Available at: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/185-Ukraine

52. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A. (2023). Systematization of threats to financial security of individual, society, business, and the state in terms of the pandemic. Lecture Notes in Civil Engineering, 299, 749–760. https://doi.org/10.1007/978-3-031-17385-1_63

53. Krasnobayev, V., Yanko A., Kovalchuk, D. (2023). Control, Diagnostics and Error Correction in the Modular Number System. Proceedings of The Sixth International Workshop on Computer Modeling and Intelligent Systems (CMIS 2023), Zaporizhzhia, Ukraine, May 3, 199–213. https://doi.org/10.32782/cmis/3392-17

54. E-Governance Academy. The National Cyber Security Index. Available at: https://ncsi.ega.ee

55. International Telecommunication Union. (2024). The ICT Development Index 2024. Available at: https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/

56. United Nations. (2024). E-Government Development Index. Overview. Available at: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

57. Buriak A., Maslii O. Minimization of digital risks and threats to the economic security of the state through the use of generative artificial intelligence. *Eastern-European Journal of Enterprise Technologies*. 2025. Vol 4. Issue 13 (136). Pp. 17-25. DOI: https://doi.org/10.15587/1729-4061.2025.336640

58. Creemers, R. China's emerging data protection framework. Journal of Cybersecurity, 8(1), 2022, Article tyac011, https://doi.org/10.1093/cybsec/tyac011

59. Kravets, I. V., Mykhalchenko, H. H., Buriak, A. A., Davidyuk, L. P., Dubych, C. V. (2020). Long-term consequences of capital outflows for transition countries. International Journal of Management, 11, 5, 1017–1026. Available at: https://ssrn.com/abstract=3631765. https://doi.org/10.34218/IJM.11.5.2020.093

60. Kadam, S., Agrawal, A., Bajaj, A., Agarwal, R., Kalra, R., & Shah, J. (2023). Predicting crude oil future price using traditional and artificial intelligence-based model: Comparative analysis. Journal of International Commerce, Economics and Policy, 14(3), 1–15. https://doi.org/10.1142/S1793993323500217

61. Гбур З.В. (2018). Інструменти державного управління економічною безпекою держави. *Інвестиції: практика та досвід*, (1), 93-97.

62. Балабаниць А., Мацука В. (2022). Сучасна парадигма механізму управління фінансово-економічною безпекою держави. *Економіка та суспільство*, (39).

63. Риков В.В. (2020). Вплив глобалізаційних процесів на економічну безпеку України. *Право та державне управління*, *2*, 204-210.

64. Маслій О. А., Ківшик О. П., Котелевець М. М. Загрози економічній безпеці держави в умовах глобальних перетворень. *Економічний простір*. 2023. № 183. С. 25-30.

65. Proactive Public Services – the new standard for digital governments (2022). *ResearchGate*. URL: https://www.researchgate.net/publication/371856269_Proactive_Public_Services_-_the_new_standard_for_digital_governments

66. Proactivity in digital public services: A conceptual analysis (2023). *Government Information Quarterly*. URL: https://www.sciencedirect.com/science/article/abs/pii/S0740624X23000321

67. Kearney. Proactive Governance: Policy and Strategy Design in the Context of Accelerating Change (2021). Kearney Report. URL: https://www.kearney.com/documents/3677458/3679850/Policy%2Band%2BStrategy%2BDesign%2Bin%2Bthe%2BContext%2Bof%2BAccelerating_EN.pdf

68. Bali, A. (2021). Procedural policy tools in theory and practice. Policy and Society, 40(3), 295–311. URL: https://academic.oup.com/policyandsociety/article/40/3/295/6509331

69. Carmona, M. (2017). The formal and informal tools of design governance. Journal of Urban Design, 22(1), 1–28. URL: https://www.tandfonline.com/doi/full/10.1080/13574809.2016.1234338

70. Максименко А.П. Вплив цифровізації на загрози економічній безпеці держави. : дис. … д-ра філос. : 051; Нац. ун-т «Полтавська політехніка імені Юрія Кондратюка». Полтава, 2025. 267 с. URL: https://nupp.edu.ua/uploads/files/0/main/page/razovi-svr/44.052.016/DisMaksymenko.pdf

71. Enhancing E-Government Proactive Services Through Big Data and Digital Twin (2024). *European Scientific Journal*, 20(3), 112–129. URL: https://eujournal.org/index.php/esj/article/view/18926/18681

72. Andrews, M., & Pritchett, L. (2020). State Capabilities for Problem-Oriented Governance. Harvard University, Center for International Development. URL: https://dash.harvard.edu/bitstreams/b18fd3dc-d020-4ee0-8ef5-eeabdb2a25fb/download

73. Державна служба статистики України. URL: https://www.ukrstat.gov.ua/

74. Національний банк України. URL: https://bank.gov.ua/

75. Дослідження Digital Tiger показує основні напрямки українського IT-експорту. Expert.com.ua. URL: https://expert.com.ua/197189-doslidzhennya-digital-tiger-pokazue-osnovni-napryamky-ukrainskoho-it-eksportu.html

76. Аналітичний центр Industry4Ukraine. Про Індустрію 5.0 – чому це стає актуальним для України. Industry4Ukraine.net. URL: https://www.industry4ukraine.net/publications/pro-industriyu-5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/

77. Cybersecurity Framework. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov/cyberframework

78. ISO/IEC 27001 – Information Security Management Systems / International Organization for Standardization (ISO). URL: https://www.iso.org/isoiec-27001-information-security.html

79. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 р. про заходи для забезпечення високого спільного рівня кібербезпеки в усьому Союзі (Директива NIS2) // Офіційний журнал Європейського Союзу. L 333/80. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

80. Звіти та аналітика щодо кіберзахисту. Міністерство цифрової трансформації України. Офіційний вебсайт. URL: https://thedigital.gov.ua

81. Огляд інцидентів та кіберзагроз в Україні. CERT-UA. Офіційний вебсайт. URL: https://cert.gov.ua

82. Publications and Reports / Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov

83. Кіберзагрози та економічна безпека: сценарії для України : аналітична доповідь. Український інститут майбутнього. Київ, 2023.

84. Research Publications / NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org

85. За останні 8 років ринок кібербезпеки в Україні зріс у 8 разів. Skilky-Skilky.info. URL: https://skilky-skilky.info/za-ostanni-8-rokiv-rynok-kiberbezpeky-v-ukraini-zris-u-8-raziv/

86. Дослідження Digital Tiger показує основні напрямки українського IT-експорту. Expert.com.ua. URL: https://expert.com.ua/197189-doslidzhennya-digital-tiger-pokazue-osnovni-napryamky-ukrainskoho-it-eksportu.html

87. Про Індустрію 5.0 – чому це стає актуальним для України / Аналітичний центр Industry4Ukraine. Industry4Ukraine.net. URL: https://www.industry4ukraine.net/publications/pro-industriyu-5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/

88. Барченко Н., Лубчак В., Лаврик Т. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки країн світу. *Cybersecurity: education, science, technology*. 2022. Вип. 18. С. 73–85.

89. Блинда Я., Кіркач О. Вплив цифрових технологій на ефективність державного управління: досвід розвинених країн. *Successes and Achievements in Science*. 2024. Т. 4, вип. 4.

90. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : Постанова Кабінету Міністрів України від 23 груд. 2020 р. № 1295. Київ : Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF

91. Карімов Н. Г. та ін. Цифрова трансформація економіки як новий виклик економічній безпеці. Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS ’21). ACM, 2022. С. 348–355.

92. Койбічук В., Куровська Я. Вплив інтегральних показників цифровізації соціально-економічних перетворень на рівень цифрового розвитку країни. *Вісник економіки.* 2022. Вип. 1. С. 83–96.

93. Круп’яник А. Цифрова економіка України: ключові фактори розвитку. *VoxUkraine*. URL: https://voxukraine.org/en/digital-economy-of-ukraine-key-development-factors

94. Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082. Microsoft. Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

95. Захист критичної інфраструктури. *Національний координаційний центр кібербезпеки України*. URL: https://cip.gov.ua/ua

ПІСЛЯМОВА

Широкомасштабна війна, розв'язана російською федерацією проти України, в поєднанні з інтенсивною цифровізацією всіх сфер суспільного життя, створила безпрецедентні виклики для національної економічної системи, що вимагає переосмислення концептуальних засад забезпечення економічної безпеки держави.

У монографії здійснено систематизацію наукових знань щодо детермінант економічної безпеки держави в парадигмі цифрового розвитку. За результатами дослідження поглиблені положення економічної безпекології щодо природи впливу цифровізації на економічну безпеку держави в умовах становлення Індустрії 4.0 та переходу до Індустрії 5.0. Ідентифіковано передумови розвитку воєнної економіки України в умовах Індустрії 4.0 з урахуванням принципів та цінностей Індустрії 5.0, досліджено можливості використання штучного інтелекту та віртуальної мобільності як домінантних цифрових технологій для безпекоорієнтованого розвитку національної економіки.

Проведено моделювання ефектів впливу цифровізації на досягнення таргетів захисту національних економічних інтересів, адаптивності і стійкості національної економіки до загроз воєнного стану та забезпечення економічної безпеки, що передбачає ідентифікацію й раннє виявлення явищ, подій та процесів у кіберпросторі, які перешкоджають чи унеможливлюють реалізацію національних економічних інтересів. Формалізовані ризики, загрози та ключові драйвери підвищення економічної безпеки держави в Індустрії 4.0, що дозволило ідентифікувати детермінанти забезпечення економічної безпеки держави та визначити пріоритетність заходів протидії загрозам.

Доведено, що система забезпечення економічної безпеки держави в умовах цифровізації має ґрунтуватися на формуванні безпекоорієнтованого інформаційного середовища, яке базується на використанні надійних систем захисту інформації, регуляторній ефективності важелів та інструментів державного управління процесами запобігання ризиків і загроз інформаційній та економічній системам, а також дієвому інституційному забезпеченні інформаційної та кібербезпеки.

Авторами сформовано понятійно-категоріальний базис безпекоорієнтованого інформаційного середовища, визначено його структуру, таксономію термінології, зміст, вектори й орієнтири розвитку з урахуванням особливостей воєнного та повоєнного періодів, що дозволило удосконалити наукові підходи до забезпечення економічної безпеки держави в парадигмі цифрового розвитку.

Запропоновано систему кластерів інформаційного середовища за доступністю й пріоритетністю захисту інформації, що дозволяє диференціювати підходи до забезпечення інформаційної безпеки відповідно

до рівня критичності інформаційних ресурсів та розробити індивідуальну концепцію захисту інформації для різних суб'єктів економічної інформаційної інфраструктури.

Розроблена методика комплексного оцінювання рівня інформаційної безпеки держави з використанням методів групи Data Mining, економетричного аналітичного інструментарію, методів GSOM та PCA на основі стратегічних таргетів і тактичних індикаторів. Запропонований методичний підхід до оцінювання інформаційної безпеки базується на формуванні системи валідних індикаторів надійності сучасних комп'ютерних систем обробки даних, що є найпридатнішим для моніторингу стану захищеності національної економіки. Сформована система індикаторів не є вичерпною, її можна змінювати з урахуванням динаміки розвитку цифрових технологій.

За результатами дослідження здійснено комплексне оцінювання інформаційної безпеки економіки України та ідентифіковано тригерні точки впливу інформаційної безпеки на рівень економічної безпеки держави в умовах загроз воєнного стану. Визначено силу і напрямок їх взаємозв'язку за допомогою тесту Ґрейнджера. Встановлено, що зі зростанням рівня інформаційної безпеки на 1% відбувається зростання економічної безпеки України на 0,2%.

Розроблено концептуальну модель формування безпекоорієнтованого інформаційного середовища на основі інтерпретаційного структурного моделювання та адаптованої багатокритеріальної моделі прийняття рішень, спрямованої на захист національних економічних інтересів та забезпечення безпеки національної економіки у воєнний та повоєнний періоди, яка включає конкретні методи підвищення кіберстійкості, інструменти та важелі державного регулювання процесу запобігання кіберзагрозам, призначенням якого є створення безпечних умов функціонування національної економіки в умовах інформаційних війн та масштабних кібератак.

Розроблено концепцію розвитку високонадійних систем захисту інформації на основі формалізації оптимальних конфігурацій функціональних елементів безпекоорієнтованого інформаційного середовища для забезпечення економічної безпеки держави в умовах війни та повоєнний період з використанням нетрадиційної машинної арифметики в системі залишкових класів, що дозволяє підвищити продуктивність та надійність комп'ютерних систем обробки економічних даних та забезпечити їх стійкість до кіберзагроз.

Запропоновано когнітивну модель підвищення рівня економічної безпеки за критеріями кіберстійкості на засадах проактивного управління з використанням відповідного інструментарію й кіберінформаційних технологій їх реалізації з урахуванням Стратегії забезпечення державної безпеки та Стратегії економічної безпеки України на період до 2025 року в умовах війни та повоєнного відновлення, що визначає стратегічні напрями та

алгоритм забезпечення економічної безпеки на різних рівнях суспільної ієрархії з реалізації комплексу заходів превентивного характеру та визначення стратегічних пріоритетів захисту національних економічних інтересів від кіберзагроз в умовах посилення дуального впливу цифровізації.

Побудовано дорожню карту інтеграції України до Єдиного цифрового ринку ЄС з покроковим описом дій, спрямованих на мінімізацію цифрових ризиків та загроз із використанням можливостей штучного інтелекту, віртуальної мобільності безпекоорієнтованого розвитку Індустрії 4.0 та врахуванням принципів Індустрії 5.0.

Такий підхід, на відміну від ситуативного реагування, дає можливість запобігати реалізації потенційних кіберзагроз шляхом протидії їм на початковому етапі зародження та формувати пріоритетні напрями мінімізації реальних загроз інформаційній безпеці, що особливо актуально та має практичну цінність в умовах війни та численних загроз, пов'язаних з мілітаризацією кіберпростору.

На основі дослідження європейського досвіду зміцнення економічної безпеки держави на засадах кіберстійкості, розроблено стратегічні пріоритети підвищення економічної безпеки України та напрями державної політики щодо формування безпекоорієнтованого інформаційного середовища у воєнний та повоєнний періоди, а також практичні рекомендації щодо мінімізації деструктивного впливу кіберзагроз на економічну безпеку в умовах війни та в повоєнний період шляхом впровадження комплексу заходів превентивного характеру на основі проактивного управління.

Закцентовано увагу на дуальному впливі цифровізації в умовах війни. Цифрова трансформація є не лише інструментом реалізації національних економічних інтересів, що створює нові можливості для зміцнення економічної безпеки держави, але й джерелом нових ризиків і загроз безпеці національної економіки (мілітаризація кіберпростору, інформаційні війни, інформаційний тероризм, масштабні кібератаки). Ця теза покладена в основу розробки концептуальної моделі формування безпекоорієнтованого інформаційного середовища, заходів мінімізації впливу кіберзагроз та стратегічних пріоритетів забезпечення економічної безпеки держави в парадигмі цифрового розвитку.

Наукове видання

МАСЛІЙ ОЛЕКСАНДРА АНАТОЛІЇВНА
КУДІНОВА АЛІНА ОЛЕКСАНДРІВНА
БУРЯК АЛЬОНА АНАТОЛІЇВНА
ЯНКО АЛІНА СЕРГІЇВНА
БІЛЬКО СТАНІСЛАВ СЕРГІЙОВИЧ

ДЕТЕРМІНАНТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В ПАРАДИГМІ ЦИФРОВОГО РОЗВИТКУ

Монографія

Компютерна верстка О.А. Маслій

Матеріали друкуються мовами оригіналів.

Підп. до друку 03.12.2025 р. Формат 60х84 1/16.
Папір офсет. Друк цифровий.
Гарнітура Times New Roman.
Ум. друк. арк. – 13,5. Обл.-вид.арк. 17,33
Тираж 100 прим. Замовл № 018/12/25

Видавництво «НАІР»
м. Івано-Франківськ, вул. Височана, 18
Тел. (050) 433-67-93
email: fedorynrr@ukr.net
Свідоцтво суб'єкта видавничої справи
№4191 від 12.11.2011р.