

DOI [10.28925/2663-4023.2022.18.7385](https://doi.org/10.28925/2663-4023.2022.18.7385)

УДК 004.051

Барченко Наталя Леонідівна

кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук

Сумський державний університет, Суми, Україна

ORCID ID: 0000-0002-5439-8750

n.barchenko@cs.sumdu.edu.ua**Любчак Володимир Олександрович**

кандидат фізико-математичних наук, доцент, завідувач кафедри кібербезпеки

Сумський державний університет, Суми, Україна

ORCID ID: 0000-0002-7335-6716

v.liubchak@dcs.sumdu.edu.ua**Лаврик Тетяна Володимирівна**

кандидат педагогічних наук, доцент, старший викладач кафедри кібербезпеки

Сумський державний університет, Суми, Україна

ORCID ID: 0000-0002-7144-7059

t.lavryk@dcs.sumdu.edu.ua

МОДЕЛЬ ІНДИКАТОРІВ ОЦІНКИ НАЦІОНАЛЬНОГО РІВНЯ ЦИФРОВІЗАЦІЇ ТА КІБЕРБЕЗПЕКИ ДЕРЖАВ СВІТУ

Анотація. Цифровізація є одним із головних трендів розвитку сучасного суспільства та факторів зростання світової економіки в найближчі роки. Але прогрес технологій та нові можливості цифровізації призводять до стрімкого зростання кіберзагроз та кіберінцидентів. Досягнення відповідного рівня цифровізації успішності економіки та суспільства є взаємозалежними від рівнів розвитку інформаційно-комунікаційних технологій та їх захищеності від можливих кібератак. Метою даної роботи є розробка з позицій системного аналізу формальних математичних моделей для опису визначення національного рівня цифрового розвитку країн з урахуванням національного рівня кібербезпеки та кіберзахисту. Для реалізації мети дослідження проведено збір та систематизацію даних за чотирма групами показників: загальний рівень розвитку, рівень цифрового розвитку країни, рівень технічної інфраструктури, рівень спроможності протидіяти кіберзагрозам. Проведений інформаційний аналіз дозволив визначити номенклатуру індикаторів прогресу цифровізації та рівня кібербезпеки й кіберзахисту. На його основі сформовано структуру компонентних моделей, які описують необхідні елементи предметної області завдання визначення індикаторів національного рівня цифровізації з узгодженням показників рівня кібербезпеки й кіберзахисту. Результати дослідження дозволяють стверджувати, що розвиток цифрової економіки неможливий без посилення кібербезпеки як на рівні держави, так і на рівні окремих суб'єктів. Подальше дослідження спрямовуватиметься на розробку математичних моделей для інтегральної оцінки стану цифрової трансформації країни з урахуванням спроможності країни протидіяти сучасним кіберзагрозам.

Ключові слова: цифровізація економіки; індексні рейтинги; індекси кібербезпеки; індекси цифровізації.

ВСТУП

Розвиток цифрових технологій обумовив виникнення принципово нового укладу життя суспільства – «цифрової економіки» [1], дозволив підвищити ефективність створення суспільного продукту, збалансування і стійке використання виробничих, технологічних, інтелектуальних, фінансових та природних ресурсів, фізичної та інноваційної інфраструктури.



Цифровізація є одним із головних трендів розвитку сучасного суспільства та факторів зростання світової економіки в найближчі роки. В Україні значна увага приділяється розвитку цифрової економіки та суспільства на державному рівні. Цифровізація визначена механізмом економічного зростання завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість і якість економічної, громадської та особистої діяльності. З 2018 року схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 рр. [2], у 2021 р. набув чинності закон України "Про стимулювання розвитку цифрової економіки в Україні" [3], завдання розвитку цифрової економіки в Україні визначено в Економічній стратегії України до 2030 р. [4].

Європейським Союзом прийнято стратегічний документ – Цифровий компас 2030 року [5], у якому представлено бачення та шлях до орієнтованого на людину, сталого та більш процвітаючого цифрового майбутнього. Виокремлено чотири напрями із конкретними цілями для кожного: кваліфікованого населення та висококваліфікованих фахівців у галузі цифрових технологій, безпечної та ефективної сталої цифрової інфраструктури, цифрової трансформації бізнесу, оцифрування державних послуг.

Однак, на фоні масштабної цифровізації усіх сфер життя, слід враховувати й інший бік таких процесів, а саме стрімке зростання кіберзагроз.

Використання інформаційно-комунікаційних технологій для несанкціонованого доступу до даних та систем може вивести з ладу системи управління компаній, незаконно позбавити їх майна і коштів, заблокувати виробничий процес, паралізувати економіку загалом. Зростаюча кіберзалежність і масштабний розвиток інформаційно-комунікаційних технологій розширили сферу потенційних уразливостей, які можна використати в кіберінцидентах.

Найнебезпечнішими для економіки та громадян вважаються кібератаки на критичну інфраструктуру (енергозабезпечення, транспортне управління, банківський та телекомунікаційний сектори, медичне обслуговування, водопостачання тощо). Також слід враховувати, що більш сучасні та складніші цифрові технології спричиняють появу та розповсюдження нових форм кібератак, так званих вразливостей «нульового дня».

Нагальною потребою є спрямування зусиль держав світу на розробку й впровадження дієвих систем кібербезпеки державного і корпоративного управління, на проведення досліджень з розроблення засобів кіберзахисту в правовому, організаційному і технічному аспектах.

Постановка проблеми. Показники розвитку країн щодо їх рівня цифровізації в подальшому будуть тісно корелювати з показниками, пов'язаними з рівнем розвитку їх систем кібербезпеки та кіберзахисту. Таким чином, постає завдання щодо розроблення такої узагальненої моделі показників (індикаторів) національного рівня цифровізації та кібербезпеки країн світу, метою якої є системна та цілісна оцінка двох взаємопов'язаних між собою процесів, визначення взаємозв'язку між кібербезпекою та рівнем розвитку цифрової економіки для формулювання рекомендацій щодо політики цифровізації.

Аналіз останніх досліджень і публікацій. Значна частина профільних впливових міжнародних організацій, інституцій та різних аналітичних агентств займаються питаннями розробки систем показників для моніторингу цифровізації економіки та соціальних відносин. Серед найбільш поширених методів оцінки стану розвитку цифрової економіки є формування рейтингових індексів. До основних рейтингових індексів цифровізації можна віднести:

- індекс прийняття цифровізації (Digital Adoption Index, DAI);
- індекс цифрової еволюції (Digital Evolution Index, DEI);
- глобальний інноваційний індекс (Global Innovation Index, GII);



— індекс цифрової економіки та суспільства (Digital Economy and Society Index, DESI);

— індекс світової цифрової конкурентоспроможності (IMD World Digital Competitiveness Index, WDCI);

— індекс цифровізації економіки (Boston Consulting Group, e-Intensity).

Згідно досліджень Світового банку [6], інфраструктура цифрової економіки не обмежується лише цифровою інфраструктурою, необхідні ефективно взаємодіючі компоненти: інформаційні та телекомунікаційні технології, людський капітал; сприятливий бізнес-клімат; ефективне управління.

Аналізу досліджень з питань цифрової трансформації бізнесу для досягнення цілей сталого розвитку з системним оглядом літератури та інформаційних джерел присвячена публікація [7].

Значну частину робіт присвячено аналізу систем індикаторів цифровізації. Наприклад, опис методології індексу розвитку інформаційно-комунікаційних технологій (ICT Development Index) та аналіз баз результатів наведено в роботі [8]. Автори у роботі [9] здійснили дослідження, присвячене глобальним питанням впровадження цифрових технологій на основі моделювання даних 183 країн з індексами глобалізації, цифрового впровадження (DAI) та інших.

Найбільш важливі показники, на яких слід зосередитися, щоб покращити статус індексу мережевої готовності (NRI) країн на різних етапах економічного розвитку, а також аналіз даних на прикладі 117 країн наведено у роботі [10].

Аналітичне дослідження та опис індексів цифрової трансформації бізнесу проведено в дисертаційній роботі [11].

У роботі [12] проаналізовано позиції України за такими глобальними індексами цифрової економіки: глобальний інноваційний індекс (GII), індекс прийняття цифровізації (DAI), індекс цифрової еволюції (DEI), індекс цифрової економіки та суспільства (DESI), індекс розвитку інформаційно-комунікаційних технологій (IDI).

Досягнення відповідного рівня цифровізації успішності економіки та суспільства не можна розглядати окремо від рівнів розвитку інформаційно-комунікаційних технологій та їх захищеності від можливих кібератак. За останні декілька десятиліть професійні міжнародні організації запропонували різні підходи до вимірювання рівнів розвитку цифрових технологій країни та національних систем кібербезпеки. Виокремимо такі основні показники:

— індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index, IDI);

— індекс мережевої готовності (Networked Readiness Index, NRI);

— глобальний індекс кібербезпеки (Global Cyber Security Index, GCI);

— національний індекс кібербезпеки (National Cyber Security Index, NCSI);

— національний індекс кіберпотужності (National Cyber Power Index, NCPI);

— національний індекс кіберготовності (Cyber Readiness Index, CRI).

У дослідженні [13] науковці провели порівняння рейтингу десяти провідних країн світу у галузі кібербезпеки за такими окремими показниками: національний індекс кіберпотужності (National Cyber Power Index, NCPI), глобальний індекс кібербезпеки (Global Cyber Security Index, GCI), індекс кіберпотужності (Cyber Power Index, CPI). Результати порівняння наведено у таблиці 1.

Наведені результати свідчать про те, що за різними показниками одні й ті ж країни займають різні позиції. Це призводить до неоднозначних висновків та уявлень про реальні оцінки кіберможливості та кіберпотужності країн. Автори дослідження пропонують новий, більш повний підхід до вимірювання кіберпотужності країни –

Національний індекс кіберпотужності Центру Белфера (National Cyber Power Index, NCPI). Індекс NCPI є поєднанням двох індексів: індекс кібернаміру (Cyber Intent Index, CII) та індекс кіберздатності (Cyber Capability Index, CCI).

Таблиця 1

**Рейтинг провідних країн світу у галузі кібербезпеки
за трьома показниками [13, с. 17]**

№	Індекс кіберпотужності (Cyber Power Index)	Глобальний індекс кібербезпеки (Global Cyber Security Index)	Національний індекс кіберпотужності (National Cyber Power Index)
1	США	Великобританія	Великобританія
2	Китай	США	США
3	Великобританія	Франція	Австралія
4	Росія	Литва	Німеччина
5	Нідерланди	Естонія	Канада
6	Франція	Сінгапур	Франція
7	Німеччина	Іспанія	Південна Корея
8	Канада	Малайзія	Японія
9	Японія	Канада	Італія
10	Австралія	Норвегія	Бразилія

У роботі [14] автори розглядають групу індексів, що вимірюють інформаційну безпеку, а саме, глобальний індекс кібербезпеки, національний індекс кібербезпеки, індекс розвитку ІКТ, індекс мережевої готовності, рівень цифрового розвитку країни. На основі цієї групи індексів дослідники пропонують визначити показники цифрової спроможності та кібербезпеки країни, констатуючи при цьому, що в цілому загальний стан національної системи кібербезпеки повністю відповідає рівню економічного розвитку країни, тобто підтверджують факт існування прямого впливу рівня розвитку країни на стан її інформаційної безпеки.

Наукова публікація [15] присвячена розгляду та моделюванню соціально-економічного розвитку країн з урахуванням рівня їх кібербезпеки. Дослідження проводилося на основі статистичних даних більше 100 країн світу за 2019 рік. Національний індекс кібербезпеки було обрано як індикатор, що характеризує рівень країн протидіяти різного роду кіберзагрозам. У якості показників соціально-економічного розвитку було обрано макроекономічні індекси, які характеризують ВВП на душу населення, рівень інфляції, легкість ведення бізнесу, рівень безробіття тощо. Здійснено кластеризацію даних країн в залежності від рівня їх кібербезпеки та соціально-економічного розвитку, що корисно для подальшого аналізу та висновків.

Аналіз показників кібербезпеки у контексті цифрової трансформації економіки та суспільства проведено у дослідженні [16]. Розглянуто рейтингові показники розвитку цифрових економік та кіберстійкості країн світу. Надано приклади відповідності рівня розвитку галузі кібербезпеки рівню розвитку цифрових технологій країни. Також зроблено висновок: якщо цифрове суспільство більш розвинуто ніж сфера національної кібербезпеки, то це є проблемним з точки зору готовності до захисту цифрових сервісів від кіберінцидентів.

У науковій роботі [17] вивчено питання взаємозв'язку характеристик національного рівня цифровізації та кібербезпеки країн світу. Проведено кореляційно-регресійне моделювання зв'язку між національним індексом кібербезпеки та



комплексним показником рівня цифрового розвитку за даними 70 країн у 2019 р. За результатами дослідження, якщо згрупувати країни за рівнем розвитку, то виявляється, що в розвинених країнах рівень кібербезпеки і рівень цифрового розвитку вище, ніж в країнах, що розвиваються. Водночас, останні демонструють, що підвищення рівня кібербезпеки позитивно впливає на розвиток цифрової економіки, тоді як у відносно розвинутих країн такий взаємозв'язок дещо слабший. Результати дослідження підтверджують висновок, що забезпечення безпеки в кіберпросторі сприятиме підвищенню рівня цифрового розвитку в країнах.

У дослідженні [18] розглядаються питання: які вимоги до кібербезпеки мають розглянути країни з обмеженими економічними ресурсами для цифровізації, щоб покращити інформаційні послуги та створити умови для подальшого економічного зростання, як виглядає економічно ефективна та життєздатна національна кібербезпека? Рейтинги різних індексів кібербезпеки країн сильно відрізняються, що свідчить про неможливість на сьогодні виміряти кібершкоду, а наявні рейтингові оцінки не дають відповідь – як виглядає «еталонна» кібербезпека. У цій роботі аналізуються підходи до національної кібербезпеки, засновані на оцінці ризику, що важливо для країн із низьким і середнім рівнем доходу, які працюють в умовах обмежених ресурсів для економічного розвитку та цифровізації. Результати представлено у формі п'яти пунктів/тестів, які можна використовувати для аналізу надійності кібербезпеки, а також для визначення шляхів, який можуть обрати країни для вирішення економічних викликів, потреб цифровізації та найважливіших викликів, кібербезпеки:

- надійна та реалістична оцінка кібероперацій ворожої держави та ймовірних намірів;
- боротьба з постійною загрозою кібершпигунства;
- визначення критичної інфраструктури та оцінка її кіберстійкості;
- оцінка ризику для даних особистого та приватного секторів;
- пошук технології та маневрування навколо конкуренції великих держав з контролю глобального управління кібербезпекою та Інтернетом.

Проведений аналіз дозволяє констатувати, що кожен з окремих показників і рівня цифровізації, і рівня національної системи кібербезпеки, не дозволяють урахувати комплексний характер цих суміжних між собою та залежних один від одного факторів, для адекватної та цілісної оцінки національного рівня цифровізації та кібербезпеки.

Мета статті. Метою даної роботи є розробка комплексу формальних математичних моделей, які забезпечують опис завдання визначення національного рівня цифрового розвитку країн з урахуванням національного рівня кібербезпеки та кіберзахисту з позицій системного аналізу.

Для досягнення поставленої мети необхідно вирішити завдання:

- Провести літературний огляд та визначити номенклатуру індикаторів прогресу цифровізації та забезпечення рівня кібербезпеки та кіберзахисту в досягненні цілей сталого розвитку.
- Сформувати структуру комплексу моделей системного аналізу предметної області індикаторів прогресу цифровізації та рівня кібербезпеки й кіберзахисту.
- Розробити компонентні моделі, які описують необхідні сутності предметної області завдання визначення індикаторів національного рівня цифровізації з узгодженням показників рівня кібербезпеки й кіберзахисту.

Спираючись на системні моделі можливо провести комплексний аналіз стану та визначити взаємозв'язок між рівнями безпеки кіберпростору та цифрового розвитку, показати необхідність підвищення рівня кібербезпеки для більш активного використання



інформаційно-комунікаційних технологій та прискорення темпів розвитку цифрової економіки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для реалізації поставленої мети наукового дослідження проведено збір та систематизацію даних за чотирма групами показників: загальний рівень розвитку, рівень цифрового розвитку країни, рівень технічної інфраструктури, рівень спроможності протидіяти кіберзагрозам.

Проведений інформаційний аналіз дозволив сформуванати комплекс описових моделей досліджуваної предметної області, який можна відобразити схемою (рис.1) та описати формулою:

$$GlobalIndex = \langle G, D, T, S \rangle,$$

де G – глобальні індекси, які відображають загальний рівень розвитку країни,

$$G = \langle GCI(WEF), GII \rangle,$$

D – глобальні індекси, які відображають рівень цифрового розвитку країни,

$$D = \langle WDC, DESI \rangle,$$

T – глобальні індекси, які відображають рівень технічної інфраструктури для ефективного розвитку бізнесу та країни,

$$T = \langle NRI, GBI \rangle,$$

S – глобальні індекси, які відображають рівень спроможності країни протидіяти кіберзагрозам,

$$S = \langle GCI, NCSI \rangle.$$

У роботі авторів [19] детально вже описано модель індикаторів прогресу цифрової трансформації країни, зокрема, наведено опис структурних формул для індексів, які відображають загальний рівень розвитку країни ($GCI(WEF)$, GII) та рівень цифрового розвитку країни (WDC , $DESI$). Ці компоненти також розглядаємо складовими для множини індикаторів оцінки рівня цифровізації та кібербезпеки. Щодо індексів, які відображають рівень технічної інфраструктури для ефективного розвитку бізнесу та країни, опис структурних формул індексу $NRI(WEF)$ детально наведено у [19]. Індекси, які відображають рівень спроможності країни протидіяти кіберзагрозам (GCI , $NCSI$) та індекс GBI рівня технічної інфраструктури опишемо у вигляді структурних формул вперше.

Глобальні індекси, які відображають загальний рівень розвитку країни.

Індекс глобальної конкурентоспроможності ($GCI(WEF)$) відображає конкурентоспроможність країн світу:

$$GCI = \langle \{S_i, W_i\} | i \in \{1, 2, \dots, m\} \rangle,$$

де S_i – субіндекси відповідно до трьох основних етапів розвитку: основні вимоги, S_1 підсилювачі ефективності, фактори інновації та складності; W_i – ваги в розрахунку загального індексу, залежно від стадії розвитку кожної економіки.

Глобальний інноваційний індекс (GII) складається з 80 індикаторів і ґрунтується на двох субіндексах:

$$GII = \langle Input\ Sub-Index, Output\ Sub-Index \rangle,$$

де $Input\ Sub-Index$ – індекси інноваційного вкладу, $Output\ Sub-Index$ – в індекси інноваційного випуску.

Глобальні індекси, які відображають рівень цифрового розвитку країни.

Індекс цифрової конкурентоспроможності (*WDC*) оцінює міру того, як країна досліджує та імплементує цифрові технології, що ведуть до трансформацій в практиці уряду, бізнесу та суспільства в цілому.

$WDC = \langle KNW, TCH, FUR \rangle$,

де *KNW* - knowledge, *TCH* - technology, *FUR* – future readiness.

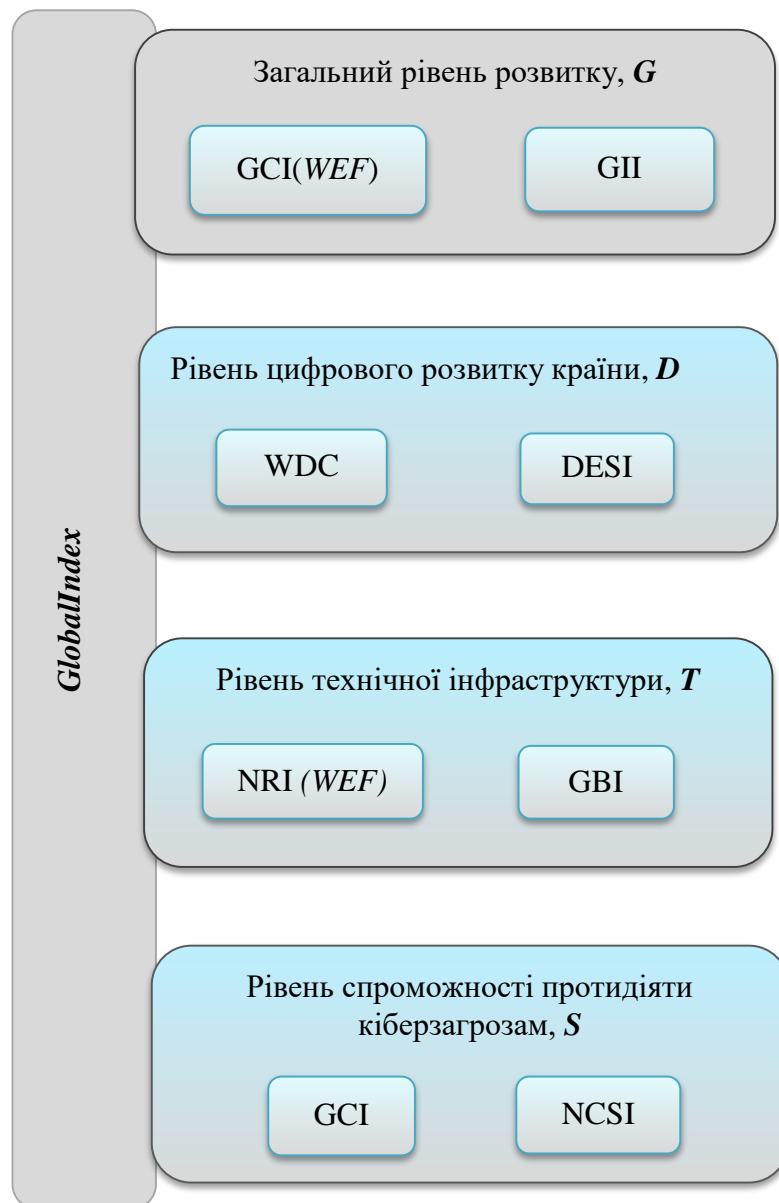


Рис. 1. Структура індикаторів оцінки рівня цифровізації та кібербезпеки



Індекс цифрової економіки та інформаційного суспільства (*DESI*) структуровано за 5 основними факторами, які розділені на субфактори з індивідуальними показниками:

$$DESI = \langle \{F_i, W_i\} | i \in \{1, 2, \dots, m\} \rangle,$$

де F_i – фактори (підключення, людський капітал, використання Інтернет-послуг, інтеграція цифрових технологій, цифрові громадські послуги), W_i – ваги індикаторів основних факторів.

Глобальні індекси, які відображають рівень технічної інфраструктури для ефективного розвитку бізнесу та країни.

Індекс мережевої готовності (*NRI (WEF)*) дозволяє оцінювати рушійні чинники і ступінь впливу мережевої готовності та можливостей ІКТ у країні.

$$NRI = \langle TECH, PPL, GOV, IMP \rangle,$$

де *TECH* – Technology, *PPL* – People, *GOV* – Governance, *IMP* – Impact.

Індекс широкопasmового доступу до Інтернету (*Global Broadband Index (OECD), GBI*). Цей показник визначається такими основними індикаторами, як: 1) швидкість (*Speed*); 2) цінова політика на послуги і доступні тарифні пакети (*Prices and rates*), 3) географічне покриття послуг широкопasmового зв'язку (*Coverage and geography*); 4) використання ІКТ у домогосподарствах та бізнесі (*Household and business usage*); 5) підписки на широкопasmовий зв'язок (*Penetration*) [20].

$$GBI = \langle SP, PR, CG, HB, PT \rangle,$$

де *SP* – Speed, *PR* – Prices and rates, *CG* – Coverage and geography, *HB* – Household and business usage, *PT* – Penetration.

Глобальні індекси, які відображають рівень спроможності країни протидіяти кіберзагрозам.

Глобальний індекс кібербезпеки (*Global Cybersecurity Index, GCI*) є зведеним індексом, що об'єднує різні індикатори в один показник для моніторингу та порівняння рівня зобов'язань країн у сфері кібербезпеки щодо п'яти основних принципів Глобальної програми кібербезпеки (*Global Cybersecurity Agenda, GCA*). Ці принципи утворюють п'ять субіндексів *GCI*.

Глобальний індекс кібербезпеки *GCI* складається з 20 індикаторів, які оцінюють 193 країни. Він ґрунтується на п'яти субіндексах [21]:

$$GCI = \langle Legal, Technical, Organizational, Capacity Building, Cooperation \rangle,$$

де *Legal* – індекси правового забезпечення, *Technical* – індекси технічного забезпечення, *Organizational* – індекси організаційного забезпечення, *Capacity Building* – індекси ресурсного забезпечення, *Cooperation* – індекси партнерського забезпечення.

Субіндекс правового забезпечення спрямовано на оцінювання наявності правової бази щодо кібербезпеки та кіберзлочинності. Правовий субіндекс структуровано таким чином

$$Legal = \langle legal_i \{Indlegal_{ij}\} | i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\} \rangle,$$

де $legal_i$ – групи індикаторів, $Indlegal_{ij}$ – j -й індикатор i -ї групи ($legal_1$ – cybercrime substantive law, $legal_2$ – cybersecurity regulation).

Субіндекси технічного забезпечення дозволяють оцінити наявність розгалуженої структури державних інститутів та установ, національної системи спостереження, попередження та реагування на інциденти. Технічний субіндекс структуровано таким чином

$$Technical = \langle technical_i \{Indtechnical_{ij}\} | i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\} \rangle,$$



де $technical_i$ – групи індикаторів, $Indtechnical_{ij}$ – j -й індикатор i -ї групи ($technical_1$ – National/Government CERT/CIRT/CSIRT, $technical_2$ – Sectorial CERT/CIRT/CSIRT, $technical_3$ – National framework for implementation of cybersecurity standards, $technical_4$ – COP).

Субіндекси організаційного забезпечення зорієнтовано на оцінювання координаційних інститутів, політик та стратегій розвитку кібербезпеки на національному рівні. Організаційний субіндекс структуровано таким чином:

$Organizational = \langle organizational_i \{Indorganizational_{ij} \mid i \in \{1, 2 \dots n\}, j \in \{1, 2 \dots m\}\} \rangle$,

де $organizational_i$ – групи індикаторів, $Indorganizational_{ij}$ – j -й індикатор i -ї групи ($organizational_1$ – National Cybersecurity Strategy, $organizational_2$ – Responsible Agency, $organizational_3$ – Cybersecurity metrics).

Субіндекси ресурсного забезпечення оцінюють наявний рівень кваліфікованого людського потенціалу, наявність програм досліджень та розробок, освітніх та навчальних програм, сертифікованих фахівців та агентств державного сектору, що сприяють нарощуванню потенціалу. Ресурсний субіндекс має таку структуру:

$Capacity\ Building = \langle capacity_building_i \{Indcapacity_building_{ij} \mid i \in \{1, 2 \dots n\}, j \in \{1, 2 \dots m\}\} \rangle$,

де $capacity_building_i$ – групи індикаторів, $Indcapacity_building_{ij}$ – j -й індикатор i -ї групи ($capacity_building_1$ – public cybersecurity awareness campaigns, $capacity_building_2$ – training for cybersecurity professionals, $capacity_building_3$ – educational programmes and academic curricula on cybersecurity, $capacity_building_4$ – research and development programmes, $capacity_building_5$ – national cybersecurity industry, $capacity_building_6$ – incentive mechanisms).

Субіндекс партнерського забезпечення враховує наявність партнерських програм, механізмів співробітництва та мереж обміну інформацією. Партнерський індекс структуровано таким чином:

$Cooperation = \langle cooperation_i \{Indcooperation_{ij} \mid i \in \{1, 2 \dots n\}, j \in \{1, 2 \dots m\}\} \rangle$,

де $cooperation_i$ – групи індикаторів, $Indcooperation_{ij}$ – j -й індикатор i -ї групи ($cooperation_1$ – bilateral agreements, $cooperation_2$ – Government participation in international mechanisms, $cooperation_3$ – multilateral agreements, $cooperation_4$ – partnerships with the private sector, $cooperation_5$ – inter-agency partnerships).

Національний індекс кібербезпеки (*National Cyber Security Index, NCSI*) є глобальним оперативним індексом, що оцінює готовність країн запобігати кіберзагрозам та керувати кіберінцидентами. NCSI також є базою даних із загальнодоступними доказовими матеріалами та інструментом для нарощування національного потенціалу кібербезпеки.

Національний індекс кібербезпеки структуровано за 3 категоріями, 12 субіндексами і 46 індикаторами. Він ґрунтується на таких субіндексах [22]:

$NCSI = \langle CSPD, CTAI, EPD, CGCS, PDS, PES, EITS, PPD, CIR, CCM, FC, MCO \rangle$,

де *CSPD* – Cyber security policy development, *CTAI* – Cyber threat analysis and information, *EPD* – Education and professional development, *CGCS* – Contribution to global cyber security, *PDS* – Protection of digital services, *PES* – Protection of essential services, *EITS* – E-identification and trust services, *PPD* – Protection of personal data, *CIR* – Cyber incidents response, *CCM* – Cyber crisis management, *FC* – Fight against cybercrime, *MCO* – Military cyber operations.



ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У дослідженні проведено літературний огляд та визначено номенклатуру індикаторів прогресу цифрової трансформації країни з урахуванням рівня її спроможності протидіяти кіберзагрозам в досягненні цілей сталого розвитку. На його основі сформовано комплекс формальних математичних моделей, які визначають національний рівень цифрового розвитку країн з урахуванням національного рівня спроможності протидіяти кіберзагрозам з позицій системного аналізу.

Розроблено компонентні моделі, які описують необхідні елементи предметної області завдання визначення індикаторів національного рівня цифровізації з узгодженням показників рівня кібербезпеки й кіберзахисту.

Попередні результати дослідження дозволяють стверджувати, що розвиток цифрової економіки неможливий без посилення кібербезпеки як на рівні держави, так і на рівні окремих суб'єктів. Зв'язок між рівнями кібербезпеки та цифрового розвитку призводить до наступного: підвищення першої веде до прискорення другого і до зростання рівня стабільності та добробуту суспільства. Тому кібербезпека повинна посісти чільне місце у загальній стратегії розвитку держави і кожної окремої компанії.

Подальші дослідження будуть спрямовані на розробку математичних моделей, які дозволять проводити інтегральне оцінювання стану цифрової трансформації країн світу та України з урахуванням спроможності країн протидіяти сучасним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1 The new digital economy. (2011). *How it will transform business (White paper)*. Oxford: Oxford Economics <https://www.pwc.com/cl/es/publicaciones/assets/the-new-digital-economy.pdf>
- 2 *Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*. (2020). Офіційний вебпортал парламенту України. <https://zakon.rada.gov.ua/laws/show/67-2018-p#Text>
- 3 Про стимулювання розвитку цифрової економіки в Україні. (2021). Офіційний вебпортал парламенту України. <https://zakon.rada.gov.ua/laws/show/1667-20#Text>
- 4 *Україна 2030E – країна з розвинутою цифровою економікою*. Економічна стратегія України 2030. <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>
- 5 *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions 2030*. (2021). Digital Compass: The European way for the Digital. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118>
- 6 *Digital Dividends*. (2016). International Bank for Reconstruction and Development / The World Bank. <https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>
- 7 Gomez-Trujillo, A. M., Gonzalez-Perez, M. A. (2021). Digital transformation as a strategy to reach sustainability. *Smart and Sustainable Built Environment, ahead-of-print* (ahead-of-print). <https://doi.org/10.1108/sasbe-01-2021-0011>
- 8 Ayanso, A., Cho, D. I., Lertwachara, K. (2011). ICT Development Index and the Digital Divide. *CONF-IRM 2011 Proceedings*. <https://aisel.aisnet.org/confirm2011/3>
- 9 Skare, M., Riberio Soriano, D. (2021). How globalization is changing digital technology adoption: An international perspective. *Journal of Innovation & Knowledge*. <https://doi.org/10.1016/j.jik.2021.04.001>
- 10 Pratipatti, S., Goma, A. (2019). A Longitudinal Analysis of the Impact of the Indicators in the Networked Readiness Index (NRI). *Journal of International Technology and Information Management*, 28(2). <https://scholarworks.lib.csusb.edu/jitim/vol28/iss2/2>
- 11 Струтинська, І.В. (2020). Цифрова трансформація як імператив інноваційного розвитку бізнес-структур [Дис. док. екон. наук, Тернопільський національний технічний; Запорізький національний університет]. http://phd.znu.edu.ua/page/dis/08_2020/Strutynska_dis.pdf
- 12 Руденко, М. В. (2021). Аналіз позицій України в глобальних індексах цифрової економіки. *Економіка та держава*. (2), 11–18. <https://doi.org/10.32702/2306-6806.2021.2.11>



- 13 Voo, Ju., Irfan H., Simon J., DeSombre, W., Cassidy, D., Schwarzenbach, A. (2020). *National Cyber Power Index 2020. Methodology and Analytical Considerations*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- 14 Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., LERNYK, S. (2022). The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of Information Technology Management*, 14 (Special Issue: Digitalization of Socio-Economic Processes), 25-58. <https://doi.org/10.22059/jitm.2022.88868>
- 15 Яровенко, Г. М., Кочережченко, Р. Д. (2022). Аналіз та моделювання соціально-економічного розвитку країн з урахуванням рівня їх кібербезпеки. *Вісник Сумського державного університету. Серія Економіка*, (1), 53–62. <https://essuir.sumdu.edu.ua/handle/123456789/87295>
- 16 Yerina, A., Honchar, I., Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*, 17(3), 3–13. <https://doi.org/10.15407/scine17.03.003>
- 17 Кіндзерський, Ю. В. (2020). Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки*, 3(71), 18-26. <https://doi.org/10.33271/ebdut/71.018>
- 18 Martin, C. Shafik Fouad, N. (2022). Five tests for risk-based approaches to national cybersecurity in resource-constrained environments. *Digital Pathways at Oxford Paper Series*, 19. https://doi.org/10.35489/BSG-DP-WP_2022/05
- 19 Барченко, Н. Л., Любчак, В. О., Карінцева, О. І., Ковальов, Б. Л., Пономаренко, І. О. (2022). Моделі опису індикаторів прогресу цифрової трансформації економіки. *Вісник Сумського державного університету. Серія Економіка*, (3), 42–50. DOI: 10.21272/1817-9215.2022.3-4
- 20 Broadband Portal - OECD. Home page - OECD. <https://www.oecd.org/digital/broadband/broadband-statistics/>
- 21 Global cybersecurity index 2020. (2022). ITU. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>
- 22 NCSI: Ranking. <https://ncsi.ega.ee/ncsi-index/>

**Natalia L. Barchenko**

PhD, Associate Professor, Associate Professor at the Department of Computer Science
Sumy State University, Sumy, Ukraine
ORCID ID: 0000-0002-5439-8750
n.barchenko@cs.sumdu.edu.ua

Volodymyr O. Lubchak

PhD, Associate Professor, Chair of the Department of Cybersecurity
Sumy State University, Sumy, Ukraine
ORCID ID: 0000-0002-7335-6716
v.liubchak@dcs.sumdu.edu.ua

Tetiana V. Lavryk

PhD, Associate Professor, Senior Lecturer at the Cybersecurity Department
Sumy State University, Sumy, Ukraine
ORCID ID: 0000-0002-7144-7059
t.lavryk@dcs.sumdu.edu.ua

MODEL OF INDICATORS FOR THE ASSESSMENT OF THE NATIONAL LEVEL OF DIGITALIZATION AND CYBER SECURITY OF THE COUNTRIES OF THE WORLD

Abstract. Digitalization is one of the main trends in the development of modern society and the growth factors of the global economy in the coming years. But the progress of technology and the new opportunities of digitalization lead to a rapid growth of cyber threats and cyber incidents. Achieving an appropriate level of digitization of the success of the economy and society is interdependent on the levels of development of information and communication technologies and their protection against possible cyber attacks. The purpose of this work is to develop, from the standpoint of system analysis, formal mathematical models for describing the determination of the national level of digital development of countries, taking into account the national level of cyber security and cyber protection. In order to realize the purpose of the study, data was collected and systematized according to four groups of indicators: the general level of development, the level of digital development of the country, the level of technical infrastructure, and the level of the ability to counter cyber threats. The conducted information analysis made it possible to determine the nomenclature of indicators of digitalization progress and the level of cyber security and cyber protection. Based on it, a structure of component models was formed that describe the necessary elements of the subject area of the task of determining the indicators of the national level of digitalization with the coordination of the indicators of the level of cyber security and cyber protection. The results of the study allow us to assert that the development of the digital economy is impossible without strengthening cyber security both at the state level and at the level of individual entities. Further research will focus on the development of mathematical models for an integral assessment of the state of the country's digital transformation, taking into account the country's ability to counter modern cyber threats.

Keywords: digitization of the economy; index rankings; indices of cyber security; indices of digitalization.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. The new digital economy. (2011). *How it will transform business (White paper)*. Oxford: Oxford Economics <https://www.pwc.com/cl/es/publicaciones/assets/the-new-digital-economy.pdf>
2. *Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii*. (2020). Ofitsiyni vebportal parlamentu Ukrainy. <https://zakon.rada.gov.ua/laws/show/67-2018-p#Text>
3. *Pro stymuliuvannia rozvytku tsyfrovoi ekonomiky v Ukraini*. (2021). Ofitsiyni vebportal parlamentu Ukrainy. <https://zakon.rada.gov.ua/laws/show/1667-20#Text>



4. *Ukraina 2030E – kraina z rozvynutoiu tsyfrovoiu ekonomikoiu. Ekonomichna stratehiia Ukrainy 2030.* <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>
5. *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions 2030.* (2021). Digital Compass: The European way for the Digital. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118>
6. *Digital Dividends.* (2016). International Bank for Reconstruction and Development / The World Bank. <https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>
7. Gomez-Trujillo, A. M., Gonzalez-Perez, M. A. (2021). Digital transformation as a strategy to reach sustainability. *Smart and Sustainable Built Environment, ahead-of-print* (ahead-of-print). <https://doi.org/10.1108/sasbe-01-2021-0011>
8. Ayanso, A., Cho, D. I., Lertwachara, K. (2011). ICT Development Index and the Digital Divide. *CONF-IRM 2011 Proceedings.* <https://aisel.aisnet.org/confirm2011/3>
9. Skare, M., Riberio Soriano, D. (2021). How globalization is changing digital technology adoption: An international perspective. *Journal of Innovation & Knowledge.* <https://doi.org/10.1016/j.jik.2021.04.001>
10. Pratipatti, S., Gomaa, A. (2019). A Longitudinal Analysis of the Impact of the Indicators in the Networked Readiness Index (NRI). *Journal of International Technology and Information Management, 28*(2). <https://scholarworks.lib.csusb.edu/jitim/vol28/iss2/2>
11. Strutynska, I.V. (2020). Tsyfrova transformatsiia yak imperatyv innovatsiinoho rozvytku biznes-struktur [Dys. dok. ekon. nauk, Ternopil'skyi natsionalnyi tekhnichnyi; Zaporizkyi natsionalnyi universytet]. http://phd.znu.edu.ua/page/dis/08_2020/Strutynska_dis.pdf
12. Rudenko, M. V. (2021). Analiz pozytsii Ukrainy v hlobalnykh indeksakh tsyfrovoi ekonomiky. *Ekonomika ta derzhava, 2*, 11–18. <https://doi.org/10.32702/2306-6806.2021.2.11>
13. Voo, Ju., Irfan H., Simon J., DeSombre, W., Cassidy, D., Schwarzenbach, A. (2020). *National Cyber Power Index 2020. Methodology and Analytical Considerations.* Belfer Center for Science and International Affairs, Harvard Kennedy School.
14. Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., Lerynk, S. (2022). The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of Information Technology Management, 14* (Special Issue: Digitalization of Socio-Economic Processes), 25-58. <https://doi.org/10.22059/jitm.2022.88868>
15. Yarovenko, H. M., Kocherezhchenko, R. D. (2022). Analiz ta modeliuvannia sotsialno-ekonomichnoho rozvytku krain z urakhuvanniam rivnia yikh kiberbezpeky. *Visnyk Sum'skoho derzhavnogo universytetu. Seriiia Ekonomika, 1*, 53–62. <https://essuir.sumdu.edu.ua/handle/123456789/87295>
16. Yerina, A., Honchar, I., Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17*(3), 3–13. <https://doi.org/10.15407/scine17.03.003>
17. Kindzerskyi, Yu. V. (2020). Kiberbezpeka ta stanovlennia tsyfrovoi ekonomiky: problemy vzaïmozv'iazku. *Ekonomichnyi visnyk Dniprovskoi politekhniki, 3*(71), 18-26. <https://doi.org/10.33271/ebdut/71.018>
18. Martin, C. Shafik Fouad, N. (2022). Five tests for risk-based approaches to national cybersecurity in resource-constrained environments. *Digital Pathways at Oxford Paper Series, 19.* https://doi.org/10.35489/BSG-DP-WP_2022/05
19. Barchenko, N. L., Liubchak, V. O., Karintseva, O. I., Kovalov, B. L., Ponomarenko, I. O. (2022). Modeli opysu indyikatoriv prohresu tsyfrovoi transformatsii ekonomiky. *Visnyk Sum'skoho derzhavnogo universytetu. Seriiia Ekonomika, 3*, 42–50. DOI: 10.21272/1817-9215.2022.3-4
20. Broadband Portal - OECD. Home page - OECD. <https://www.oecd.org/digital/broadband/broadband-statistics/>
21. Global cybersecurity index 2020. (2022). ITU. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>
22. NCSI: Ranking. <https://ncsi.ega.ee/ncsi-index/>

