UDC 004.051 336.051+338.1

JEL classification: C13, C38, C65, G20, M20

DOI: https://doi.org/10.35774/visnyk2022.03.008

Віталія КОЙБІЧУК,
кандидатка економічних наук, доцентка,
доцентка кафедри економічної кібернетики,
Сумський державний університет,
вул. Римського-Корсакова, 2, Суми, Україна, 40007,
e-mail: v.koibichuk@biem.sumdu.edu.ua
ORCID ID: orcid.org/0000-0002-3540-7922

Валерія ГЕРАСИМЕНКО,
студентка спеціальності «Економіка»,
Сумський державний університет,
вул. Римського-Корсакова, 2, Суми, Україна, 40007,
e-mail: ek81.v_herasymenko@uabs.sumdu.edu.ua
ORCID ID: orcid.org/0000-0003-1772-8017

ЕФЕКТИВНІСТЬ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ: DEA-АНАЛІТИКА

Койбічук В., Герасименко В. Ефективність національної кібербезпеки: DEA-аналітика. *Вісник економіки*. 2022. Вип. 3. С. 8–21. DOI: https://doi.org/10.35774/visnyk2022.03.008

Koibichuk, V., Gerasymenko, V. (2022). Efektyvnist natsionalnoi kiberbezpeky: DEA-analityka [Effectiveness of National Cyber Security: DEA analytics]. *Visnyk ekonomiky – Herald of Economics*, 3, 8–21. DOI: https://doi.org/10.35774/visnyk2022.03.008

Анотація

Вступ. *Ключовою детермінантою цифрової ери є кібербезпека, яка надзвичайно важлива як для індивідуальних осіб, так і для компаній, підприємств, банків, великих та малих бізнесів. Високий рівень національної кібербезпеки, ефектисть систем кіберзахисту – це запорука стабільності економіки держави. Тому актуальним та нагальним питанням сьогодення є комплексне та всебічне оцінювання якості національних систем кібербезпеки, які гарантовано підтримали би фінансову діяльність держави.*

Мета дослідження *полягає у визначенні максимального, найбільш ефективного значення індексу національної кібербезпеки країн світу, розподілених на 8 кластерів, враховуючи як рейтингове значення індексу національної кібербезпеки, так і особливості систем та процедур організації кіберзахисту, легкості ведення бізнесу, рівня цифрового розвитку.*

Методи дослідження: *бібліометричний аналіз застосування інструментів DEA-аналізу з використанням програмного забезпечення VOSviewer, лінійна оптимізація з використанням прямої моделі Банкера-Чарнеса-Купера та програмного забезпечення Frontier Analyst, кластерний аналіз з використанням метода Уорда та програмного забезпечення Statgraphics.*

Результати. *Визначено ефективність національної кібербезпеки 97 країн світу у 2021 р., виявлено еталонні країни, які мають високоякісну систему національної кібербезпеки, а також визначено потенційні резерви для збільшення таргетованого значення індексу національної кібербезпеки.*

Перспективи. *Подальші дослідження будуть спрямовані на розроблення багатоваріантних адаптивних сплайнів регресії, MARS-моделей для посилення фінансової кібербезпеки країни та розроблення дорожньої карти розвитку інноваційної системи протидії легалізації кримінальних доходів та фінансового кіберзахисту.*

Ключові слова: *національна кібербезпека; рівень цифрового розвитку; аналіз охоплення даних, багатокритеріальне лінійне програмування, ефективність.*

Vitaliia KOIBICHUK,
Ph. D. (Economics), Associate Professor
Associate Professor of the Economic Cybernetics Department,
Sumy State University,
2, Rymskogo-Korsakova st., 40007,
e-mail: v.koibichuk@biem.sumdu.edu.ua
ORCID ID: https://orcid.org/0000-0002-3540-7922

Valery GERASYMENKO,
Student, speciality “Economics”
Sumy State University,
2, Rymskogo-Korsakova st., 40007,
e-mail: ek81.v_herasymenko@uabs.sumdu.edu.ua
ORCID ID: orcid.org/0000-0003-1772-8017

EFFECTIVENESS OF NATIONAL CYBER SECURITY: DEA ANALYTICS

Abstract

Introduction. *Cyber security is a crucial determinant of the digital age, which is extremely important for both individuals and companies, enterprises, banks, and large and small businesses. A high level of national cyber security and the effectiveness of cyber protection systems guarantee the stability of the state’s economy. Therefore, a relevant and urgent issue today is a comprehensive assessment of the quality of national cyber security systems, which would guarantee the support of the state’s financial activities.*

Purpose. *The purpose of the study is to determine the maximum, most effective value of the national cyber security index of the countries of the world, divided into 8 clusters, taking into account both the rating value of the national cyber security index, as well as the*

features of cyber protection organization systems and procedures, ease of doing business, and the level of digital development.

Research methods: *a bibliometric analysis of the application of DEA analysis tools using VOSviewer software, linear optimization using the Banker-Charnes-Cooper direct model and Frontier Analyst software, cluster analysis using Ward's method and Statgraphics software.*

Results. *The effectiveness of the national cyber security of 97 countries of the world in 2021 was determined, reference countries with a high-quality national cyber security system were identified, and potential reserves for increasing the targeted value of the national cyber security index were identified.*

Prospects. *Further research will be aimed at the development of multivariate adaptive regression splines, MARS models to strengthen the financial cyber security of the country, and the creation of a road map for the development of an innovative system for countering the legalization of criminal proceeds and financial cyber protection.*

Keywords: *national cyber security; digital development level; data envelopment analysis, multicriteria linear programming, efficiency analysis.*

Formulas: 6, fig.: 5, tab.: 6, bibl.: 12.

JEL classification: C13, C38, C65, G20, M20.

Постановка проблеми. Стан та рівень сучасного цифрового світу прямопропорційно залежить від несанкціанового доступу до інформації, впровадження шахрайських кіберзлочинних, кібершпигунських схем та ступеня захисту інформаційних систем. Для кожної держави надзвичайно важливим питанням є посилення систем кіберзахисту інформації, визначення ефективності національної системи кібербезпеки та поглиблення міжнародної співпраці у цій сфері. На міжнародному рівні національний індекс кібербезпеки визначається Академією електронного урядування (e-Governance Academy) як інтегральний показник, що охоплює складові політики кібербезпеки, аналітику кіберзагроз, захист цифрової інформації, електронної аутентифікації, ідентифікації даних та користувачів, швидкість реагування на кібератаки, програми кіберкризового управління, військові кібероперації. Рівень цифрового розвитку держави Академія електронного урядування визначає як середнє арифметичне значень індексів розвитку інформаційно-телекомунікаційних технологій та мережевої готовності. Якщо різниця між оцінками національної кібербезпеки та цифровим розвитком позитивна, то розвиток кібербезпеки країни відповідає або випереджає її цифровий розвиток. Негативний результат показує, що цифрове суспільство країни більш розвинене, ніж національна сфера кібербезпеки. Тому виникає питання щодо можливості визначення найбільш ефективних країн за організацією якісної системи кіберзахисту інформації, організацією високого рівня кібербезпеки, виявленням «еталонних» країн та визначенням потенційних можливостей для кожної країни щодо посилення політики кібербезпеки, особливо в сфері фінансово-грошових операцій.

Аналіз останніх досліджень і публікацій. Методологію DEA-аналізу застосовують дуже широко в різних галузях для ґрунтовного дослідження середовища функціонування певного об'єкта та дослідження ефективності окремих процесів, що характеризують діяльність цього об'єкта. Бібліометричний аналіз лише 2000 наукових

ISSN 2786-4537 (print). Вісник економіки № 3, 2022 р.
ISSN 2786-4545 (online). Herald of Economics № 3, 2022

публікацій зі знайдених 3729, що були проіндексовані наукометричною базою даних Скопус у період з 2018 по 2022 р., за допомогою програмного забезпечення VOSviewer 1.6.15 відображено у вигляді графа (рис. 1). Вузли графа – це кластери, що сформовані з 11167 ключових слів та містять 5 та більше ключових слів, що автори спільно використовували в своїх публікаціях про застосування DEA-аналізу, а ребра – взаємозв'язки документів. Кількість вузлів становить 700 одиниць, ребер – 22806, кластерів – 9.

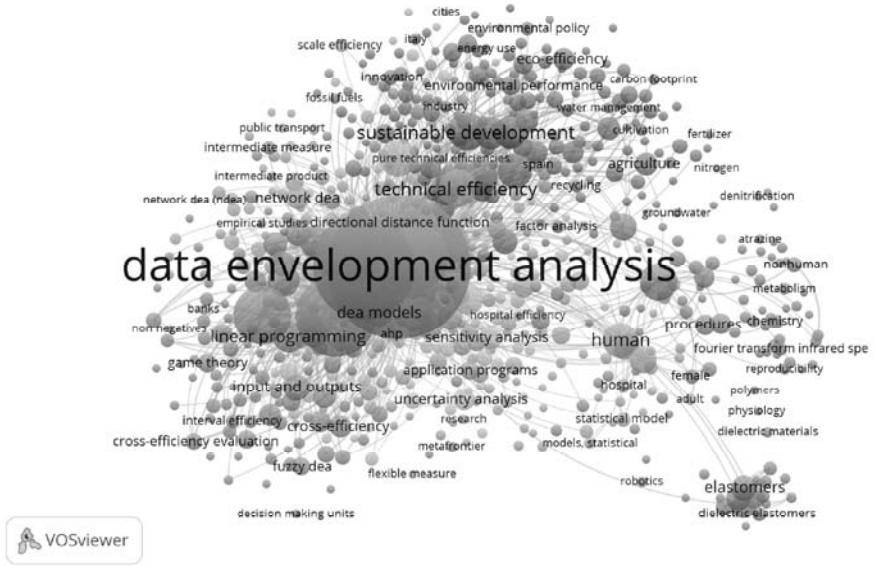

Рис. 1. Бібліографічний аналіз сфер застосовування та методології інструментарію охоплення даних методом DEA-аналізу

Джерело: розроблено авторами за результатами бази даних Скопус та програмного інструментарію VOSviewer 1.6.15.

Отже, граф (рис. 1) узагальнює перелік наукових публікацій, що присвячені найкращим практикам застосування DEA-аналізу в різних країнах світу в сфері енергетики, сільського господарства, автомобільної індустрії, підприємництва, банківської діяльності, фінансової аналітики із можливостями залучення відділів прийняття рішень та застосування як систем прийняття рішень, так і безпосередньо різноманітних моделей лінійного програмування, теорії ігор, нечіткої логіки, методів захисту інформації, дискримінантного аналізу, економічного аналізу, бенчмаркінгу для визначення ефективності банківської системи, екологічної, технічної, перехресної та відносної ефективності, стабільності розвитку об'єкта дослідження та загальної продуктивності.

Велику зацікавленість також викликає праця науковців [1], де автори для мінімізації випадків порушень кібербезпеки досліджують поведінку людей з використанням гібридної методології DEA-аналізу та MARS-аналізу, що становить метод непараметричної регресії та реалізується за допомогою сплайнів багатовимірної

адаптивної регресії (Multivariate Adaptive Regression Splines). У дослідженні наведено приклади відносин, які описують вплив внутрішніх змінних на ефективність відповідності вимогам безпеки.

Мета статті полягає у визначенні ефективності національної кібербезпеки країн світу за допомогою аналізу охоплення індексу цифрового розвитку, легкості ведення бізнесу, Базельського індексу протидії відмиванню коштів з використанням прямої оптимізаційної BCC-моделі лінійного програмування.

Виклад основного матеріалу. Вимірювання ефективності процедур фінансового моніторингу та посилення заходів щодо продуктивної кібербезпеки соціально-економічних бізнес-одиниць в умовах експоненціально зростаючої трансформації цифрового середовища вимагає застосування потужного аналітичного інструментарію. Для порівняння індексів та показників результативності досліджуваного об'єкта запропонуємо використати метод аналізу оболонки (охоплення) даних (Data Envelopment Analysis, DAE), що ґрунтується на методах багатокритеріального оптимізаційного моделювання [2]. DAE-аналіз дає змогу визначити відносну ефективність досліджуваних об'єктів на основі значень необхідних факторів та показників порівняно з еталонними показниками, що становлять найкращі практики, а також визначити рейтинг та граничне оптимальне значення для потенційного удосконалення кожного об'єкта дослідження. Так, наприклад, відносна ефективність підприємства (банка, фірми, фінансової установи) визначається як частка від зваженої суми всіх вихідних параметрів на зважену суму всіх вхідних параметрів [3]:

$$Ef = \frac{\sum_{r=1}^{s} u_r y_{jr}}{\sum_{i=1}^{n} v_i x_{ji}}, \quad (1)$$

де Ef – ефективність досліджуваного об'єкта, y_j – вихідні параметри, s – кількість вихідних параметрів, x_j – вхідні параметри, n – кількість вхідних параметрів, u_r, v_i – вагові коефіцієнти вихідних та вхідних параметрів відповідно, при цьому $\sum_{r=1}^{s} u_r = 1, u \geq 0$; $\sum_{i=1}^{n} v_i = 1, v \geq 0$.·

Основними припущеннями того, що підприємство 100% ефективне, є такі критерії: 1) жоден з вихідних параметрів (факторів) не може бути збільшений без підвищення одного або декількох вхідних параметрів, або ж зниження інших вихідних параметрів; 2) жоден з вхідних факторів не може бути зменшений без зниження одного чи більше вихідних параметрів, або ж підвищення інших вхідних факторів.

Базовими моделями DAE-аналізу є пряма та двоїста input-орієнтована CCR-модель (2) (модель Чарнеса-Купера-Родеса) [3, 4], пряма та двоїста input-орієнтована BCC-модель (3) (модель Банкера-Чарнеса-Купера) [5], двоїста сумарна VarMulti-модель (4) (табл. 1).

Таблиця 1

Базові моделі DAE-аналізу

Функціональне представлення моделі	№
$\sum_{j=1}^{s} u_j y_{j0} \rightarrow max$ при $\sum_{i=1}^{r} v_i x_i = 1$, $u_j, v_i \geq 0$	(2)

ISSN 2786-4537 (print). Вісник економіки № 3, 2022 р.
ISSN 2786-4545 (online). Herald of Economics № 3, 2022

продовження таблиці 1

$\sum_{j=1}^{s} \quad u_j y_{j0} + a_0 \to max \quad$ при $\quad \sum_{i=1}^{r} \quad v_i x_i = 1, u_j, v_i \geq 0$	(3)
$\sum_{j=1}^{s} \quad u_j log(y_{j0}) - \sum_{i=1}^{r} \quad v_i log(x_{i0}) \to max \quad$ при $\quad \sum_{i=1}^{r} \quad v_i x_i = 1\ ,\ u_j, v_i \geq 0$	(4)

Джерело: розроблено авторами на основі [3; 4; 5].

У формулах (2-4) – вхідні показники, загальна кількість яких r; y_j – вихідні показники, загальна кількість яких s; v_i, u_j – вагові коефіцієнти вхідних та вихідних показників відповідно, a_0 – константа (стала величина, без обмежень).

Пряма модель дає змогу визначити зміну вхідних показників лише щодо одного вихідного показника. Двоїста модель визначає зміну вхідних показників щодо будь-якого набору вихідних показників.

Формула (2) дає змогу визначити максимальний ефект за умови мінімізації зважених вхідних параметрів щодо будь-якого нормованого виходу. Двоїста input-орієнтована BBC DEA-модель (3) дозволяє визначити максимальний ефект за умови мінімізації зважених вхідних параметрів до будь-якого виходу ефекту масштабу a зміни вхідних параметрів x відносно вихідних y. Двоїста сумарна VarMulti-модель (4) застосовується для інтерпретації виробничих функцій.

Отже, запропоновану методологію DAE-аналізу використаємо для дослідження відносної ефективності вихідного параметра – національний індекс кібербезпеки (NCSI) для 97 країн дослідження [6]. Вхідними параметрами, що впливають на формування значення національного індексу кібербезпеки, використано такі показники, як: Базельський індекс AML [7], рівень цифрового розвитку [6], легкість ведення бізнесу [8].

Кожен із наведених показників є агрегованим за відповідною методологією інституцій, які офіційно визначають та публікують статистичну звітність щодо значень даних показників. Значення показників рівня цифрового розвитку (DDL) та національного індексу кібербезпеки (NCSI) визначаються згідно з методологією Академії електронного урядування (e-Governance Academy, EGA [4]), яка займається формуванням бази знань передового досвіду в галузі електронного врядування. Значення рівня цифрового розвитку (DDL) розраховуються як середнє арифметичне індексу розвитку інформаційно-телекомунікаційних технологій (IDI), що визначається Міжнародною спілкою електрозв'язку, та індексу мережевої готовності (NRI) [9]. Базельський індекс AML (Basel AML Index [7, 10]) визначає Базельський інститут управління за 10-бальною шкалою бо та описує ризики використання фінансових установ країн для легалізації кримінальних доходів та фінансуванню тероризму: 0 – мінімальне значення ризику (найкраща позиція, ризики виникнення та розвитку корупції, легалізації кримінальних коштів відсутні), 10 – максимальне значення ризику (найгірше значення, країна належить до високоризикованих за залученням її до відмивання грошових коштів).

Детальний опис визначення та отримання бальних рейтингових значень агрегованих показників наведено в роботі [11].

Концептуальну схему визначення відносної ефективності значення національного індексу кібербезпеки наведено на рис. 2.

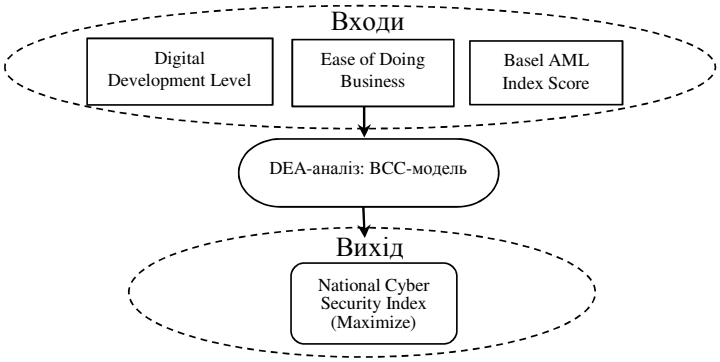

Рис. 2. Концептуальна схема визначення ефективності національної кібербезпеки країни

Джерело: розроблено авторами.

Визначення відносної ефективності проведено для 97 країн, згрупованих у 8 кластерів, що містять 12 країн за рейтинговим значенням національного індексу кібербезпеки [6]. Розподіл країн на 8 кластерів аргументовано застосуванням формули Стерджеса (5), та протоколом агломерації кластерного аналізу, що проведений у програмному забезпеченні Statgraphics 19 (рис. 3):

$$k=1+3{,}322(N), \tag{5}$$

де k – кількість кластерів, N – обсяг загальної кількості країн (дорівнює 97). За результатами обчислення k = 8, що визначає оптимальну кількість розподілу країн на кластери.

Відсутність різких розривів між точками графіка (рис. 3), що відображають кроки агломерації методом Уорда (формула (6)), за методологію якого в якості відстані між кластерами використовується приростання суми квадратів відстаней об'єктів до центра кластера, що отримуються в результаті їх об'єднання), дає можливість стверджувати, що обрана кількість кластерів для набору даних є правильною та аргументованою методами дисперсійного аналізу: чим менше буде значення внутрішньогрупової дисперсії та більше значення міжгрупової дисперсії, тим краще ознака характеризує приналежність країни до певного кластера і тим більш якісні будуть результати проведеної кластеризації [12].

$$V_I = \sum_i \sum_j (x_j - \bar{x}_J)^2, \tag{6}$$

де I – номер кластера, i – номер об'єкта (i = 1, 2, …, n_I), n_I – кількість об'єктів в I-му кластері, j – номер ознаки (j = 1, 2, …, k), k – кількість ознак, що характеризують кожний об'єкт.

ISSN 2786-4537 (print). Вісник економіки № 3, 2022 р.
ISSN 2786-4545 (online). Herald of Economics № 3, 2022

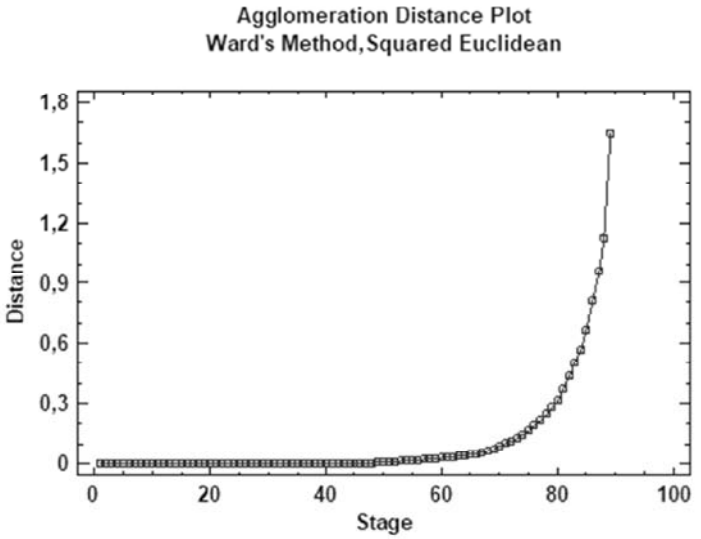

Рис. 3. Схема агломерації за методом Уорда

Джерело: розроблено авторами засобами програмного забезпечення Statgraphics 19.

Таким чином, серед країн 1-го кластера найбільш ефективними в розрізі організації національної кібербезпеки є Естонія та Греція (табл. 2). Визнання країни ефективною (еталонною) досягається за умови досягнення нею 100% значення цільового параметра, середній рівень ефективності мають країни, які отримали від 90 до 99,99 балів. В іншому випадку – неефективними.

Таблиця 2

Розподіл країн за рівнем ефективності національної кібербезпеки для кластера 1

Країна	Кількість балів, %	Країна	Кількість балів, %	Країна	Кількість балів, %	Країна	Кількість балів, %
Бельгія	97,3	Данія	88,9	Фінляндія	92,3	Німеччина	94,6
Чехія	96,0	Естонія	100,0	Франція	87,8	Греція	100,0
Литва	98,2	Польща	90,5	Португалія	93,2	Іспанія	92,3

Джерело: розроблено авторами.

Країни, які знаходяться на вертикальній або горизонтальній границі фронтір-графіка є «еталонними» за вихідним та вхідними параметрами дослідження (рис. 4)

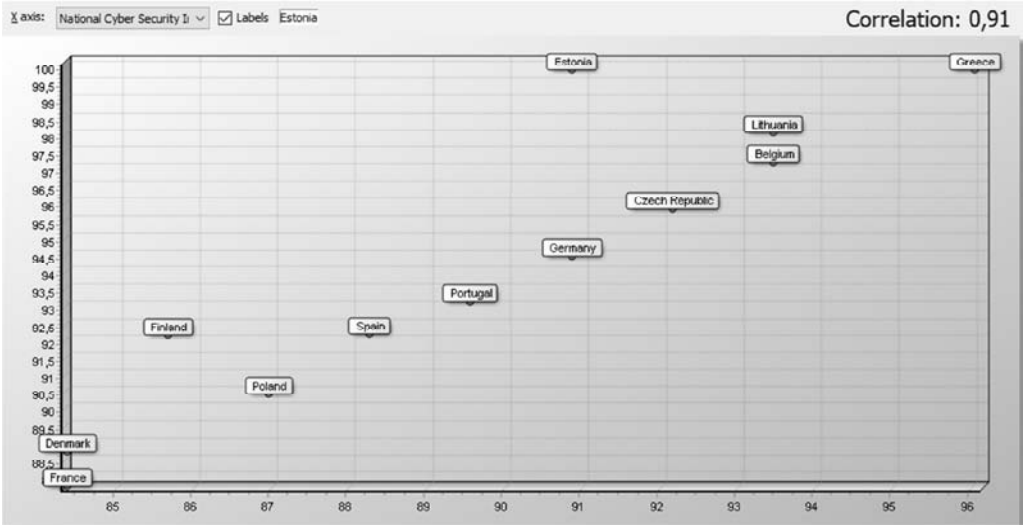

Рис. 4. Графік Ефективності країн за рівнем національної кібербезпеки

Джерело: розроблено авторами засобами програмного забезпечення Frontier Analyst.

Аналогічні розрахунки були проведені для всіх інших країн, розподілених за кластерами. Узагальнений розподіл ефективності рівня національної кібербезпеки наведено в табл. 3–4.

Таблиця 3

Розподіл країн за рівнем ефективності національної кібербезпеки для кластерів 2-4

Країна	Кількість балів, %	Країна	Кількість балів, %	Країна	Кількість балів, %
Кластер 2		Кластер 3		Кластер 4	
Хорватія	100	Австралія	89,5	Бенін	100,0
Італія	95,1	Австрія	93,0	Чилі	98,1
Латвія	90,3	Бангладеш	100,0	Єгипет	100,0
Малайзія	96,4	Болгарія	100,0	Індія	100,0
Нідерланди	97,8	Канада	89,5	Ірландія	100,0
Саудівська Аравія	100,0	Кіпр	89,5	Японія	100,0
Сербія	98,2	Угорщина	87,7	Люксембург	99,8
Словакія	99,8	Ізраїль	91,2	Нігерія	95,3
Швеція	100,0	Республіка Корея	93,0	Парагвай	94,6
Україна	100,0	Румунія	97,0	Філіппіни	100,0
Велика Британія	92,4	Сінгапур	96,5	Словенія	100,0
Сполучені штати	93,9	Тайланд	89,4	Замбія	100,0

Джерело: розроблено авторами засобами програмного забезпечення Frontier Analyst.

ISSN 2786-4537 (print). Вісник економіки № 3, 2022 р.
ISSN 2786-4545 (online). Herald of Economics № 3, 2022

Таблиця 4

Розподіл країн за рівнем ефективності національної кібербезпеки для кластерів 5-8

Країна	Кількість балів, %	Країна	Кількість балів, %	Країна	Кількість балів, %	Країна	Кількість балів, %
Кластер 5		Кластер 6		Кластер 7		Кластер 8	
Албанія	88,8	Азербайджа	73,7	Вірменія	99,4	Бахрейн	100,0
Аргентина	100,0	Бразилія	100,0	Болівія	100,0	Ботсвана	100,0
Коста Ріка	100,0	Колумбія	100,0	Боснія і Герцеговина	80,8	Камбоджа	100,0
Домініканська Республіка	100,0	Індонезія	87,9	Китай	96,8	Ель-Сальвадор	72,3
Грузія	97,3	Казахстан	79,4	Еквадор	100,0	Гватемала	100,0
Кенія	90,5	Мексика	77,3	Гана	95,1	Киргизстан	90,5
Мальта	93,9	Пакистан	100,0	Йорданія	81,1	Лаоська НДР	100,0
Маврикій	88,1	Панама	97,7	Чорногорія	100,0	Малаві	100,0
Республіка Молдова	94,5	Перу	91,1	Нікарагуа	100,0	Малі	100,0
Нова Зеландія	95,2	Шрі-Ланка	94,4	Трінідад і Тобаго	100,0	Монголія	66,7
Туреччина	100,0	Об'єднані Арабські Емірати	67,9	Узбекистан	88,5	Таджикистан	52,4
Уганда	100,0	Уругвай	100,0	В'єтнам	100,0		

Джерело: побудовано авторами засобами програмного забезпечення Frontier Analyst.

Для порівняння ефективностей еталонного набору країн доцільно використати опцію «Reference set frequencies». Така процедура програмного забезпечення Frontier Analyst дає змогу виявити, скільки разів ефективна одиниця з'являється в еталонному наборі неефективної одиниці (табл. 5, 6).

Таблиця 5

Порівння значень ефективності еталонних країн за показником «національний індекс кібербезпеки»

Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору
Кластер 1		Кластер 2		Кластер 3		Кластер 4	
Греція	11	Саудівська Аравія	9	Болгарія	11	Філіппіни	6
Естонія	5	Швеція	7	Бангладеш	3	Бенін	3
		Хорватія	3			Словенія	3
		Україна	3			Ірландія	3

продовження таблиці 5

						Індія	2
						Замбія	1
						Єгипет	1

Джерело: розроблено авторами засобами програмного забезпечення Frontier Analyst.

Таблиця 6

Порівняння значень ефективності еталонних країн за показником «національний індекс кібербезпеки»

Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору	Країна	Частота ефективності еталонного набору
Кластер 5		Кластер 6		Кластер 7		Кластер 8	
Туреччина	7	Пакистан	9	Чорногорія	7	Малаві	5
Домініканська Республіка	6	Колумбія	7	В'єтнам	7	Бахрейн	2
Уганда	6	Уругвай	5	Нікарагуа	5	Камбоджа	1
Аргентина	1	Бразилія	3	Еквадор	4	Лаоська НДР	1
				Болівія	1	Малі	1
				Трінідад і Тобаго	1	Ботсвана	1
						Гватемала	1

Джерело: розроблено авторами засобами програмного забезпечення Frontier Analyst.

Отже, серед країн першого кластера найбільш високе значення ефективності NSCI серед «еталонних» країн має Греція, оскільки вона має найбільш високе значення частоти. Серед країн другого кластера найбільш високе значення ефективності має Саудівська Аравія. В третьому кластері найбільш ефективною країною за рівнем національної кібербезпеки є Болгарія, у четвертому – Філіппіни, у п'ятому – Туреччина, у шостому – Пакистан, у сьомому – Чорногорія, у восьмому – Малаві.

Для неефективних країн доцільно вжити заходи щодо підвищення їхніх значень індексу національної кібербезпеки та можливості його підвищення. Так, наприклад у першому кластері значення ефективності національної кібербезпеки для Франції становить 87,8%. Реальне значення індексу національної кібербезпеки у 2021 р. становило 84,42, а потенційне його значення (порівняно з «еталонною» країною Грецією) може бути покращеним до 96,10, тобто зростати на 13,84% (рис. 5).

ISSN 2786-4537 (print). Вісник економіки № 3, 2022 р.
ISSN 2786-4545 (online). Herald of Economics № 3, 2022

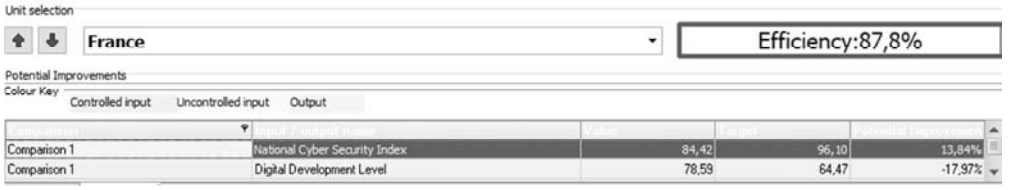

Рис. 5. Графік ефективності країн за рівнем національної кібербезпеки

Джерело: розроблено авторами засобами програмного забезпечення Frontier Analyst.

Висновки. Застосування багатокритеріального лінійного програмування з використанням методології охоплення даних, DEA-аналізу та програмного забезпечення Frontier Analyst, дали змогу виявити найбільш ефективні країни за організацією національної системи кіберзахисту. З метою врахування особливостей економік та соціально-політичного становища досліджуваних країн здійснено процедуру кластеризації, в результаті якої було отримано 7 кластерів, що охоплюють 12 країн та 1 кластер, що охоплює 11 країн. Процедуру розподілу саме на 8 кластерів підтверджено протоколом агломерації методом Уорда із застосуванням програмного забезпечення Statgraphics, застосування формули Стерджесса та рейтингових значень індексу національної кібербезпеки. Еталонними країнами у першому кластері є дві країни – Естонія та Греція, у другому кластері – Саудівська Аравія, Швеція, Хорватія, Україна, у третьому – Болгарія та Бангладеш, у четвертому – Філіппіни, Бенін, Словенія, Ірландія, Індія, Замбія, Єгипет, у п'ятому – Туреччина, Домініканська Республіка, Уганда, Аргентина, у шостому – Пакистан, Колумбія, Уругвай, Бразилія, у сьомому – Чорногорія, В'єтнам, Нікарагуа, Еквадор, Болівія, Трінідад і Тобаго, у восьмому – Малаві, Бахрейн, Камбоджа, Лаоська НДР, Малі, Ботсвана, Гватемала. Критерії щодо визначення країни відносно ефективною використано максимально жорсткі: країна вважається ефективною в разі досягнення нею 100% значення ефективності системи національної кібербезпеки за умови охоплення рівня цифрового розвитку, легкості ведення бізнесу та Базельського індексу протидії відмиванню коштів та фінансуванню тероризму. Отримані результати можуть використати Ради національних безпек країн, які мають низький рівень національної кібербезпеки, відділи кіберполіції з метою вивчення передового досвіду еталонних країн та посилити власну стратегію кіберзахисту й глобальне значення цифрового розвитку.

Перспективи подальших досліджень. Подальші дослідження будуть спрямовані на розроблення багатоваріантних адаптивних сплайнів регресії, MARS-моделей для посилення фінансової кібербезпеки країни та розроблення дорожньої карти розвитку інноваційної системи протидії легалізації кримінальних доходів та фінансового кіберзахисту.

Література

1. Donalds, Ch., Osei-Bryson, Kweku-Muata, Samoilenko, S. (2019). Exploring the impacts of intrinsic variables on security compliance efficiency using DEA and MARS. *IFIP Advances in Information and Communication Technology*, 551. P. 751–762. http://doi.org/10.1007/978-3-030-18400-1_61

2. Emmerich, M., Deutz, A. (2015). Multicriteria Optimization and Decision Making: Principles, Algorithms and Case Studies. URL : https://liacs.leidenuniv.nl/~emmerichmtm/modapage/MCOReaderEmmeirchDeutz2017.pdf
3. CCR Model (DEA): Scholarly Community Encyclopedia. URL: https://encyclopedia.pub/entry/7787#:~:text=Efficiency%20Frontier%20under%20Constant%20Returns%20to%20Scale%20(CCR%20Model)
4. Charnes, A., Cooper, W., Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research*, 2. P. 429–444. http://doi.org/10.1016/0377-2217(78)90138-8.
5. Banker, R., Charnes, A., and Cooper, W. (1984). Some models for estimating technical and scale inefficiencies in data envelopment analysis, Management Science, 30 (9). P. 1078–1092.
6. National Cyber Security Index: URL : https://ncsi.ega.ee/ncsi-index/
7. Basel AML Index 2021: 10th Public Edition Ranking money laundering and terrorist financing risks around the world. URL: https://baselgovernance.org/sites/default/files/2021-09/Basel_AML_Index_2021_10th%20Edition.pdf
8. Doing Business: The World Bank. URL: https://www.doingbusiness.org/en/data
9. Network Readiness Index 2021. Benchmarking the Future of the Network Economy. URL: https://networkreadinessindex.org/
10. Methodology What's behind the Basel AML Index? URL: https://index.baselgovernance.org/methodology
11. Койбічук В., Куровська Ю. Вплив інтегральних показників цифровізації суспільно-економічних трансформацій на рівень цифрового розвитку країни. Вісник економіки. 2022. № 1. С. 83–96. https://doi.org/10.35774/visnyk2022.01.083
12. Бізнес-аналітика багатовимірних процесів : навч. посібник / Т. С. Клебанова, Л. С. Гур'янова, Л. О. Чаговець та ін. Харків : ХНЕУ ім. С. Кузнеця, 2018. 272 с.

References

1. Donalds, Ch., Osei-Bryson, Kweku-Muata, Samoilenko, S. (2019). Exploring the impacts of intrinsic variables on security compliance efficiency using DEA and MARS. IFIP Advances in Information and Communication Technology, 551. P. 751-762. DOI: http://doi.org/10.1007/978-3-030-18400-1_61 [in English].
2. Emmerich, M., Deutz, A. (2015). Multicriteria Optimization and Decision Making: Principles, Algorithms and Case Studies. Retrieved from: https://liacs.leidenuniv.nl/~emmerichmtm/modapage/MCOReaderEmmeirchDeutz2017.pdf [in English].
3. CCR Model (DEA): Scholarly Community Encyclopedia. Retrieved from: https://encyclopedia.pub/entry/7787#:~:text=Efficiency%20Frontier%20under%20Constant%20Returns%20to%20Scale%20(CCR%20Model) [in English].
4. Charnes, A., Cooper, W., Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research*, 2, 429-444. DOI: http://doi.org/10.1016/0377-2217(78)90138-8. [in English].
5. Banker, R., Charnes, A., and Cooper, W. (1984). Some models for estimating technical and scale inefficiencies in data envelopment analysis, Management Science, 30 (9), 1078- 1092 [in English].

6. National Cyber Security Index. Retrieved from: https://ncsi.ega.ee/ncsi-index/ [in English].
7. Basel AML Index 2021: 10th Public Edition Ranking money laundering and terrorist financing risks around the world. Retrieved from: https://baselgovernance.org/sites/default/files/2021-09/Basel_AML_Index_2021_10th%20Edition.pdf [in English].
8. Doing Business: The World Bank. Retrieved from: https://www.doingbusiness.org/en/data [in English].
9. Network Readiness Index 2021. Benchmarking the Future of the Network Economy. Retrieved from: https://networkreadinessindex.org/ [in English].
10. Methodology What's behind the Basel AML Index? Retrieved from: https://index.baselgovernance.org/methodology [in English].
11. Kojbichuk, V., Kurovsjka, Ju. (2022). Vplyv integhraljnykh pokaznykiv cyfrovizaciji suspiljno-ekonomichnykh transformacij na rivenj cyfrovogho rozvytku krajiny. *Visnyk ekonomiky*, 1, 83-96. Retrieved from: https://doi.org/10.35774/visnyk2022.01.083 [in Ukrainian].
12. Biznes-analityka baghatovymirnykh procesiv: navch. posib; T. S. Klebanova, L. S. Ghur'janova, L. O. Chaghovecj ta in. Kharkiv: KhNEU im. S. Kuznecja, 2018. 272 p. [in Ukrainian].

Статтю отримано 16 липня 2022 р.
Article received July 16, 2022