DOI: https://doi.org/10.32782/2524-0072/2021-32-37

УДК 330.43:004.056:336.1.07

ПОПЕРЕДНІЙ АНАЛІЗ ПРОЦЕСУ КОНВЕРГЕНЦІЇ СИСТЕМ КІБЕРБЕЗПЕКИ ТА ФІНАНСОВОГО МОНІТОРИНГУ КРАЇН[1]

PRELIMINARY ANALYSIS OF THE CONVERGENCE PROCESS OF CYBER SECURITY SYSTEMS AND FINANCIAL MONITORING OF COUNTRIES

Кузьменко Ольга Віталіївна
докторка економічних наук, професорка,
Сумський державний університет
ORCID: https://orcid.org/0000-0001-8520-2266

Яровенко Ганна Миколаївна
докторка економічних наук, доцентка,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-8760-6835

Радько Вікторія Вікторівна
магістрантка,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-7183-6687

Kuzmenko Olha, Yarovenko Hanna, Radko Viktoria
Sumy State University

Стаття присвячена актуальній проблемі конвергенції систем кібербезпеки та фінансового моніторингу країни, що сприятиме формуванню більш ефективної системи протидії фінансовим та кібер-злочинам. Авторами проведено попередній аналіз груп показників, які ідентифікують рівень розвитку кібербезпеки в країні та її спроможність протидіяти процесам легалізації кримінальних доходів та фінансових злочинів. Дані було сформовано для 76 країн світу за 2018 рік. На першому етапі проведено статистичний аналіз відібраних показників, що дозволило виявити неоднорідність даних. На другому кроці проведено канонічний аналіз, в результаті якого встановлено тісний зв'язок між показниками кібербезпеки та фінансового моніторингу та виявлено їх причинно-наслідковість. На третьому етапі за результатами кореляційного аналізу оптимізовано дані шляхом виключення індексів розвитку інформаційно-комунікаційних технологій та сприйняття корупції.

Ключові слова: конвергенція, кібербезпека, фінансовий моніторинг, статистичний аналіз, канонічний аналіз, кореляційний аналіз.

Статья посвящена актуальной проблеме конвергенции систем кибербезопасности и финансового мониторинга страны для формирования более эффективной системы противодействия финансовым и киберпреступлениям. Авторами проведен предварительный анализ показателей, которые идентифицируют уровень развития кибербезопасности в стране и ее способность противодействовать процессам легализации криминальных доходов, финансовых преступлений. Данные были сформированы для 76 стран за 2018 год. На первом этапе проведен статистический анализ показателей, что позволило выявить неоднородность данных. На втором шаге проведен канонический анализ, в результате которого установлена тесная связь между показателями кибербезопасности и финансового мониторинга, выявлена их причинно-следственность. На третьем этапе по результатам корреляционного анализа оптимизи-

[1] Робота виконана в рамках держбюджетних науково-дослідних робіт: 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку»; 0121U100467 «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України».

рованы данные путем исключения индексов развития информационно-коммуникационных технологий и восприятия коррупции.
Ключевые слова: конвергенция, кибербезопасность, финансовый мониторинг, статистический анализ, канонический анализ, корреляционный анализ.

The article is devoted to the current problem of convergence of cybersecurity systems and financial monitoring of the countries, which will contribute to the formation of a more effective system for combating financial and cybercrime. The need for this study is due to the growing level of cyberattacks in the financial sector, which increases the risks of national security vulnerability. The authors conducted a preliminary analysis of groups of indicators that identify the level of cybersecurity development in the country and its ability to counteract the processes of legalization of criminal proceeds and financial crimes. Global Index Cybersecurity, ICT Development Index, Networked Readiness Index, National Index Cybersecurity, Digital Development Level. The second group includes the Political Stability Index, Government Effectiveness Index, Ease of Doing Business, Crime Index, Corruption Perceptions Index, Global Terrorism Index, and Financial Secrecy Index formed the first group. Statistical data on the analysed indicators were selected for 76 countries in 2018. At the first stage, a statistical analysis of the selected indicators was performed, which consisted of calculating basic statistics: mean, median, modal value, minimum and maximum levels, standard deviation and coefficient of variation. As a result, the heterogeneity of data caused by different levels of economic development of selected countries was revealed. In the second stage, a canonical analysis was conducted. As a result, it was established that there is a close relationship between cybersecurity and financial monitoring at 0.91. Causality between the groups of indices was also established. Thus the level of development of cybersecurity is a consequence indicator, and the level of countries' ability to counteract the legalization of criminal proceeds and financial crimes is the cause of cybersecurity. At the third stage, the results of correlation analysis revealed the most collinear indicators. This allowed excluding indices of information and communication technologies development and perception of corruption and optimizing data. The obtained results of the analyses are planned to be further used to calculate phase portraits and determine the levels of "maturity", "equilibrium", and "relaxation fluctuations of stability loss" for countries in the process of convergence of their cybersecurity systems and financial monitoring.
Keywords: convergence, cybersecurity, financial monitoring, statistical analysis, canonical analysis, correlation analysis.

Постановка проблеми. Забезпечення надійної та потужної системи національної безпеки є одним з пріоритетних завдань для будь-якої країни світу, особливо це є актуальним в умовах зростання рівня цифровізації різних сфер діяльності суспільства та її впливу на економічні, соціальні, політичні та інші процеси. Досягнення відповідного рівня безпеки можливо за рахунок системної взаємодії різних напрямів, одним з яких є формування оптимальної моделі системи державного фінансового моніторингу, що можливо за рахунок посилення її функцій у контексті її конвергенції із системою кібербезпеки. Даний процес є необхідним в умовах зростання інформаційних та кібер-ризиків, які є наслідками інформатизації та цифровізації, а особливо ця потреба відчувається у фінансовій сфері, що є одним з гарантів забезпечення умов надійності фінансово-економічної безпеки країни.

Здійснення конвергенції системи фінансового моніторингу та кібербезпеки повинно відбуватися на всіх рівнях управління економікою, тобто на рівні економічного об'єкта – суб'єкта внутрішнього фінансового моніторингу, так й на рівні держави – суб'єкта обов'язкового фінансового моніторингу. Даний процес повинен передбачати інформаційну, програмну, технічну, організаційну, правову, методичну інтеграції функцій моніторингу та кібербезпеки, результатом чого повинна бути потужна система протидії фінансовим та кібер-злочинам.

У даному контексті виникає потреба оцінити рівень існуючих передумов, сформованих суб'єктами моніторингу та кібербезпеки, до початку імплементації процесів інтеграції у практичну їх діяльність. Першим кроком є визначення факторів, які ідентифікують рівень країн протидіяти фінансовим та кіберзагрозам. На наступному кроці необхідно провести попередній аналіз процесу конвергенції систем фінансового моніторингу і кібербезпеки, який полягатиме у здійсненні: статистичного аналізу обраних факторів для оцінки однорідності вибірки емпіричних даних; канонічного аналізу для визначення рівня взаємовпливів системи кібербезпеки та фінансового моніторингу; кореляційного аналізу для оптимізації даних. Це сприятиме визначенню факторів, найбільш релевантних для забезпечення означеного процесу.

Аналіз останніх досліджень і публікацій. За останнє десятиріччя зросла кількість наукових праць, присвячених актуальним питанням кібербезпеки та її реалізації у фінансово-економічній сфері. Зацікавленість

даною тематикою обумовлена потребами практики щодо посилення захисту інформації та знань фінансового характеру. В цьому контексті слід виділити вектор публікацій, які вирішують проблеми, пов'язані із управлінням кібер-ризиками в банківській сфері, що розглядалися такими науковцями, як Скотт Б.Ф. [1], Ан Дж., Дуань Т., Хоу В., Лю Х. [2], Чен Дж., Чжу К., Башар Т. [3] та іншими.

Наступним актуальним напрямом досліджень є вивчення загроз та вразливостей систем кіберзахисту, що можуть виступити слабкими місцями для кіберзлочинців та кібершахраїв. В цій сфері можна виділити праці таких фахівців, як Бердибаєв Р., ГнатюкС., Євченко Ю., Кіщенко В. [4], Комаров М., Давидюк А., Онискова А., Ткаченко В., Гончар С. [5], Уддін М.Х., Алі М.Х., Хасан М.К. [6] та інші. Застосування сучасних технологій, таких як штучний інтелект та блокчейни, є значним блоком наукових досліджень, спрямованих на вирішення проблеми протидії фінансових та кібер-шахрайств. Цей напрям досліджують Коучоро М.К., Содокін К., Коріко М. [7], Карпуніна Є.К., Михайлов А.М., Бондарева Н.А., Любименко О.А., Федотова Є.В. [8], Мхланга Д. [9], Сміт К.Дж., Діллон Г. [10], Картер Д. [11] та інші.

Правові та організаційні аспекти, пов'язані із здійсненням процесів кібербезпеки та фінансового моніторингу, є також напрямом наукових досліджень, де розкриваються питання: забезпечення конфіденційності фінансової інформації в праці К. Атта Уль Хак [12]; правових аспектів технологічної нейтральності в статті Г. Гальяні [13]; системного поєднання сфери освіти, технологій та політики для підвищення ефективності системи кібербезпеки в роботі М. Доусон [14]; вимог до організації та функціонування відповідних підрозділів кібербезпеки у фінансовій сфері Т.П. Августінос [15] тощо. Не дивлячись на широко коло проблем, які вирішуються науковцями – фахівцями в сфері кібербезпеки та фінансового моніторингу, питання конвергенції цих двох систем є ще не розкритим, що потребує подальших досліджень.

Мета статті полягає у проведенні попереднього аналізу процесу конвергенції систем кібербезпеки та фінансового моніторингу країн для виявлення найбільш релевантних факторів для їх інтеграції.

Виклад основного матеріалу дослідження. Для реалізації поставленої мети даного наукового дослідження було проведено збір та систематизацію статистичних даних в розрізі 76 країн світу за 2018 рік за двома групами показників. Перша група характеризує спроможність країн протидіяти кіберзагрозам за рахунок створення відповідних умов розвитку інформаційних, комп'ютерних та мережевих технологій, а також умов організації ефективної системи кібербезпеки. Дані було узято з офіційного джерела компанії «e-Governance Academy Foundation». Сюди увійшли п'ять індексів: глобальний індекс кібербезпеки (Global Index Cybersecurity); індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index); індекс мережевої готовності (Networked Readiness Index); національний індекс кібербезпеки (National Index Cybersecurity); рівень цифрового розвитку (Digital Development Level).

Другу групу показників було сформовано з урахуванням існуючих можливостей країн світу щодо формування системи фінансового моніторингу, спроможної протидіяти процесам легалізації кримінальних доходів та фінансування тероризму. Дані було узято з офіційного джерела Світового банку. Сюди увійшли 7 індексів: індекс політичної стабільності (Political Stability Index); індекс ефективності уряду (Government Effectiveness Index); легкість ведення бізнесу (Ease of Doing Business); індекс злочинності (Crime Index); індекс сприйняття корупції (Corruption Perceptions Index); глобальний індекс тероризму (Global Terrorism Index); індекс фінансової таємниці (Financial Secrece Index).

Проведемо за допомогою аналітичного пакету "STATISTICA" статистичний аналіз обраних груп показників, який полягає у визначенні базових статистичних характеристик: середнього значення, медіани, модального значення, мінімального та максимального рівнів, стандартного відхилення та коефіцієнта варіації. Так, його результати в розрізі показників, що ідентифікують систему кібербезпеки, представлені на рисунку 1.

Отримані результати дозволяють констатувати, що серед показників кібербезпеки однорідну вибірку мають лише індекс розвитку інформаційно-комунікаційних технологій, індекс мережевої готовності та рівень цифрового розвитку, оскільки значення їх коефіцієнту варіації не перевищує гранично допустимого рівня 33%. В той же час, за показниками глобального індексу кібербезпеки та національного індексу кібербезпеки спостерігається нерівномірність розподілу значень в межах розглянутих 76 країн світу.

Переходячи до аналізу модального значення в розрізі показників (див. рис. 1), можна

Variable	Descriptive Statistics (Spreadsheet1.sta)						
	Mean	Median	Mode	Minimum	Maximum	Std.Dev.	Coef.Var.
Global Cybersecurity Index	66,07895	75,00000	89,00000	2,00000	93,00000	24,28979	36,75874
ICT Development Index	65,07895	69,50000	72,00000	0,00000	90,00000	18,07153	27,76863
Networked Readiness Index	61,89474	63,50000	63,00000	0,00000	86,00000	19,90483	32,15916
National Cyber Security Index	54,25500	57,14000	57,14000	3,90000	96,10000	23,19572	42,75316
Digital Development Level	65,57618	66,81500	58,00000	28,10000	85,13000	13,97311	21,30821

Рис. 1. Описові статистики групи показників кібербезпеки

Джерело: розраховано авторами самостійно

стверджувати, що найбільш поширене значення, яке є найбільшим і незначним чином відрізняється від максимуму, сягає рівня 89 і належить глобальному індексу кібербезпеки. Це свідчить про досить високий рівень даного показника для більшості країн світу. В розрізі інших чотирьох показників кібербезпеки модальне значення приймає значення від 57 до 72 і в усіх випадках перевищує відповідні середні рівні.

Аналогічно, як і для модального значення, глобальний індекс кібербезпеки вирізняється найбільшим середнім рівнем, набуваючи значення 66,08. Найменше значення серед медіанних рівнів, тобто рівнів, що ділять множину розглянутих країн світу навпіл, набуває значення 57 в розрізі національного індексу кібербезпеки.

Проведемо аналіз базових статистик в розрізі показників, які ідентифікують спроможність країн протидіяти процесам легалізації кримінальних доходів. Його результати представлені на рисунку 2.

Отримані результати середнього значення, медіани, модального значення, мінімального та максимального рівнів, стандартного відхилення та коефіцієнта варіації дозволяють констатувати, що серед досліджуваних показників тільки в розрізі одного – легкість ведення бізнесу, спостерігається однорідність вибірки для 76 країн світу. Для всіх інших показників виявлено сильно виражену нерівномірність, оскільки коефіцієнт варіації приймає значення від 33,87% (за показником індекс злочинності) до 241,37% (за показником індекс політичної стабільності).

Отримані модальні значення (див. рис. 2) свідчать, що найпоширене значення спостерігається лише за індексом політичної стабільності та глобальним індексом тероризму. В розрізі інших п’яти показників виявлено досить різнорідні значення характеристик спроможності країн протидіяти фінансовим злочинам.

Для виявлення причинно-наслідкових зв’язків між групами показників кібербезпеки та спроможності країн протидіяти процесам легалізації кримінальних доходів проведено канонічний аналіз із використанням аналітичного пакету “STATISTICA”. Його результати представлені на рисунку 3.

Так, виявлено, що варіативність у множині показників кібербезпеки пояснюється на 65,51% множиною показників спроможності країн протидіяти процесам легалізації кримінальних доходів. В той же час, варіативність у множині показників спроможності країн протидіяти фінансовим загрозам лише на 49,39% пояснюється множиною показників кібербезпеки. Таким чином, результати виявлення

Variable	Descriptive Statistics (Spreadsheet1.sta)						
	Mean	Median	Mode	Minimum	Maximum	Std.Dev.	Coef.Var.
Political stability index	0,3228	0,4650	,7500000	-1,86000	1,540	0,7791	241,3742
Government effectiveness index	0,6337	0,4950	Multiple	-1,58000	2,230	0,8488	133,9547
Ease of doing business	70,1993	71,8250	Multiple	30,85000	86,590	10,2343	14,5789
Crime Index	42,0550	40,1700	Multiple	13,10000	83,600	14,3604	34,1466
Corruption Perceptions Index	55,3421	55,0000	Multiple	18,00000	88,000	18,7457	33,8724
Global Terrorism Index	2,1433	1,0115	0,000000	0,00000	7,568	2,3170	108,1075
Financial Secrece Index	284,6963	208,2552	Multiple	27,86072	1589,574	279,0323	98,0105

Рис. 2. Описові статистики показників, які ідентифікують спроможність країн протидіяти процесам легалізації кримінальних доходів

Джерело: розраховано авторами самостійно

N=76	Canonical Analysis Summary (Spreadsheet1.sta) Canonical R: ,91259 Chi?(35)=196,50 p=0,0000 Left Set	Right Set
No. of variables	5	7
Variance extracted	100,000%	86,6707%
Total redundancy	65,5082%	49,3947%
Variables: 1	Global Cybersecurity Index	Political stability index
2	ICT Development Index	Government effectiveness index
3	Networked Readiness Index	Ease of doing business
4	National Cyber Security Index	Crime Index
5	Digital Development Level	Corruption Perceptions Index
6		Global Terrorism Index
7		Financial Secrece Index

Рис. 3. Результати канонічного аналізу причинно-наслідкових зв'язків між групами показників кібербезпеки та спроможності країн протидіяти фінансовим злочинам

Джерело: розраховано авторами самостійно

причинно-наслідкових зв'язків за допомогою канонічного аналізу дозволяють констатувати, що показники спроможності країн протидіяти процесам легалізації кримінальних доходів виступають причиною, а множина показників кібербезпеки, відповідно, наслідком.

Крім того, аналіз рисунку 3 свідчить також про те, що частка дисперсії (варіативності), яка пояснюється множиною показників кібербезпеки складає 100%, а частка дисперсії (варіативності), яка пояснюється множиною показників спроможності країн протидіяти фінансовим загрозам приймає значення 86,67%. Це говорить про те, що у першому випадку 100% дисперсії будуть пояснювати усі вилучені корені, у другому випадку – на 86,67%.

Канонічна кореляція R=0,91 (див. рис. 3), яка відповідає кореляції між першими канонічними змінними, дорівнює максимальному канонічному кореню. Її значення свідчить про наявність сильної лінійної залежності між групами змінних. Статистична значущість коефіцієнта канонічної кореляції підтверджується високим значеннями Хі-квадрату (196,5) та рівнем ймовірності менше ніж 0,05 (p=0,00).

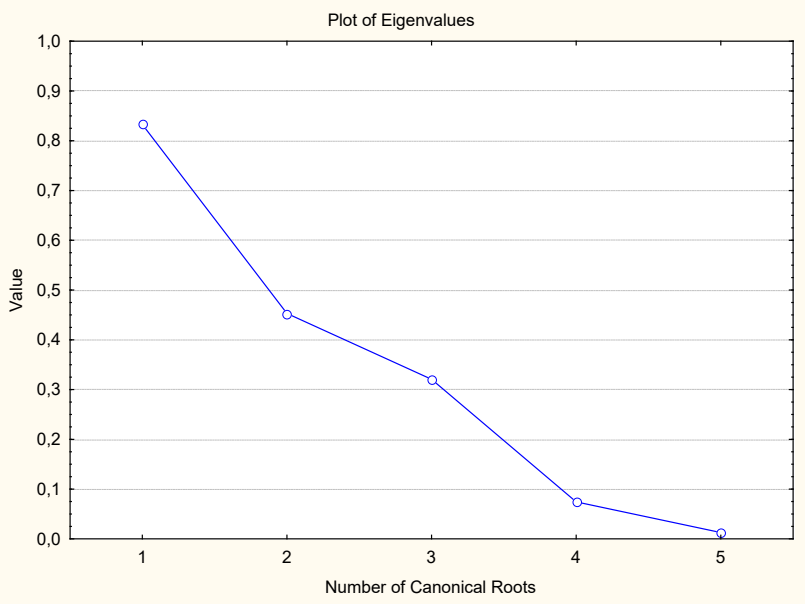

Рис. 4. Шматково-лінійний графік спадаючих власних значень, що відповідають канонічним кореням

Джерело: розраховано авторами самостійно

	Chi-Square Tests with Successive Roots Removed (Spreadsheet1					
Root Removed	Canonicl R	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0,912589	0,832818	196,4981	35	0,000000	0,056779
1	0,673046	0,452991	73,9741	24	0,000001	0,339625
2	0,566215	0,320599	32,6488	15	0,005264	0,620876
3	0,272715	0,074373	6,1705	8	0,628141	0,913858
4	0,112760	0,012715	0,8765	3	0,831083	0,987285

Рис. 5. Тести Хі-квадрат для статистичної значущості канонічних коренів

Джерело: розраховано авторами самостійно

Візуалізацію шматково-лінійного графіку спадаючих власних значень, що відповідають канонічним кореням, представимо на рисунку 4, а результати тестів Хі-квадрату для статистичної значущості канонічних коренів – на рисунку 5.

Отже, на основі рисунків 4 і 5 можна зробити висновок, що статистично значущими є перші три канонічні корені, оскільки p-значення для них не перевищують гранично допустимого рівня 0,05. Саме зазначені канонічні корені пропонується розглядати на наступному етапі при оптимізації вхідного масиву даних.

З метою оптимізації масиву вхідних даних проведемо із використанням аналітичного пакету “STATISTICA” кореляційний аналіз двох груп показників кібербезпеки та спроможності країн протидіяти фінансовим загрозам. Розглянемо спочатку кореляційну матрицю лівої множини – множини показників кібербезпеки (рисунок 6). За результатами аналізу можна зробити висновок про наявність значної кореляційної залежності між такими показниками як індекс розвитку інформаційно-комунікаційних технологій та рівень цифрового розвитку. Підтвердженням даного факту виступає високе значення коефіцієнту кореляції, що дорівнює 0,96. Для оптимізації множини вхідних показників кібербезпеки рекомендується один із колінеарних індикаторів видалити з подальших обчислень.

Для прийняття рішення щодо показника, який варто залишити в масиві вхідних даних, а який треба видалити, розглянемо отриману в результаті проведення канонічного аналізу факторну структуру за першими трьома статистично значущими канонічними коренями (рисунок 7).

	Correlations, left set (Spreadsheet1.sta)				
Root Removed	Global Cybersecurity Index	ICT Development Index	Networked Readiness Index	National Cyber Security Index	Digital Development Level
Global Cybersecurity Index	1,000000	0,535836	0,711354	0,709438	0,579198
ICT Development Index	0,535836	1,000000	0,583418	0,642989	0,960733
Networked Readiness Index	0,711354	0,583418	1,000000	0,681275	0,646743
National Cyber Security Index	0,709438	0,642989	0,681275	1,000000	0,654703
Digital Development Level	0,579198	0,960733	0,646743	0,654703	1,000000

Рис. 6. Кореляційна матриця лівої множини – множини показників кібербезпеки

Джерело: розраховано авторами самостійно

	Factor Structure, left set (Spreadsheet1.sta)				
Variable	Root 1	Root 2	Root 3	Root 4	Root 5
Global Cybersecurity Index	0,793546	-0,573776	0,032460	-0,196203	-0,038945
ICT Development Index	0,871213	0,172113	-0,390995	0,235508	-0,054996
Networked Readiness Index	0,802578	-0,240821	0,379359	0,353759	0,169749
National Cyber Security Index	0,725708	-0,296197	-0,218899	0,034132	0,580115
Digital Development Level	0,942847	0,257388	-0,197662	0,075622	0,001483

Рис. 7. Факторна структура лівої множини – множини показників кібербезпеки

Джерело: розраховано авторами самостійно

Root Removed	Correlations, right set (Spreadsheet1.sta)						
	Political stability index	Government effectiveness index	Ease of doing business	Crime Index	Corruption Perceptions Index	Global Terrorism Index	Financial Secrece Index
Political stability index	1,000000	0,657513	0,455746	-0,495251	0,750314	-0,648904	0,135375
Government effectiveness index	0,657513	1,000000	0,802933	-0,621574	0,903724	-0,047663	0,435225
Ease of doing business	0,455746	0,802933	1,000000	-0,582606	0,646477	0,002313	0,268673
Crime Index	-0,495251	-0,621574	-0,582606	1,000000	-0,557071	0,173214	-0,227253
Corruption Perceptions Index	0,750314	0,903724	0,646477	-0,557071	1,000000	-0,180892	0,344927
Global Terrorism Index	-0,648904	-0,047663	0,002313	0,173214	-0,180892	1,000000	0,214337
Financial Secrece Index	0,135375	0,435225	0,268673	-0,227253	0,344927	0,214337	1,000000

Рис. 8. Кореляційна матриця правої множини – множини показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам

Джерело: розраховано авторами самостійно

Аналіз рисунку 7 дозволяє констатувати, що більш значущий вплив здійснює показник рівень цифрового розвитку (0,9428, 0,2573, -0,1977), а ніж індекс розвитку інформаційно-комунікаційних технологій (0,8712, 0,1721, -0,3901). Відповідно, пропонується залишити індекс рівня цифрового розвитку для проведення подальших досліджень щодо конвергенції систем фінансового моніторингу та кібербезпеки.

Перейдемо до розгляду кореляційної матриці правої множини –показників спроможності країн протидіяти фінансовим злочинам (рисунок 8). За отриманими результатами аналізу можна зробити висновок про наявність значної кореляційної залежності між такими двома показниками, як індекс ефективності уряду та індекс сприйняття корупції. Підтвердженням даного факту виступає високе значення коефіцієнту кореляції, що дорівнює 0,904. Для оптимізації вхідних показників в розрізі спроможності країн протидіяти процесам легалізації кримінальних доходів рекомендується один із колінеарних індикаторів видалити для подальших досліджень.

Для прийняття рішення щодо показника, який варто залишити в масиві вхідних даних, а який треба видалити, розглянемо факторну структуру за статистично значущими канонічними коренями, отриманими в результаті проведення канонічного аналізу (рисунок 9).

Результати аналізу, представленого на рисунку 9, показують, що більш значущий вплив здійснює показник індекс ефективності уряду (0,9545 за першим канонічним коренем), ніж індекс сприйняття корупції (0,8162 за першим канонічним коренем), який і пропонується залишити для проведення подальших досліджень.

Висновки. Процес конвергенції систем фінансового моніторингу та кібербезпеки є одним з напрямів формування ефективної системи протидії фінансовим та кібер-злочинам в країні. Його реалізація потребує зваженого підходу, оскільки передбачається складна та системна інтеграція багатьох процесів, функцій та механізмів. Тому необхідно оцінити умови, сформовані в країні, які характеризують поточний рівень її кібербезпеки та фінансового моніторингу. Відповідно в даному дослідженні було сформовано дві групи показників, які характеризують для 76 країн світу рівень розвитку окреслених систем за 2018 рік. Сформована база статистичних даних дозволила провести попередній аналіз процесу конвергенції систем фінансового моніторингу і кібербезпеки. В результаті статистичного ана-

Variable	Factor Structure, right set (Spreadsheet1.sta)				
	Root 1	Root 2	Root 3	Root 4	Root 5
Political stability index	0,431400	0,613095	-0,531891	0,117958	0,025365
Government effectiveness index	0,954471	0,191497	-0,180077	0,040551	-0,102695
Ease of doing business	0,854172	-0,217032	-0,246307	0,101444	0,266008
Crime Index	-0,556918	0,012999	0,672392	-0,119773	-0,187796
Corruption Perceptions Index	0,816167	0,504821	-0,221053	-0,124591	-0,001933
Global Terrorism Index	0,149483	-0,620973	0,320721	-0,602566	-0,274481
Financial Secrece Index	0,505484	0,089914	0,322668	-0,319966	0,282863

Рис. 9. Факторна структура правої множини – множини показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам

Джерело: розраховано авторами самостійно

лізу проведено оцінку однорідності вибірки емпіричних даних, що дозволило виявити їх неоднорідність для ряду показників. Це обумовлюється нерівномірністю розвитку країн в напрямку забезпечення ефективної системи кіберзахисту та фінансового моніторингу. Проведення канонічного аналізу дозволило встановити, що між групами обраних показників існує тісний зв'язок, при цьому рівень кібербезпеки виступає наслідком, а рівень фінансового моніторингу – причиною. На основі кореляційного аналізу проведено оптимізацію даних, в результаті чого такі показники, як індекс розвитку інформаційно-комунікаційних технологій та індекс сприйняття корупції, слід виключити для проведення подальших досліджень як нерелевантних для розглянутих наборів даних.

В подальшому отримані результати планується використати для проведення біфуркаційного аналізу зрілості діючої системи протидії фінансовим та кібершахрайствам, а також побудови фазових портретів їх «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Scott B.F. Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*. 2021. № 28(1). P. 98–111. DOI: https://doi.org/10.1108/JFC-06-2020-0118

2. An J., Duan T., Hou W., Liu X. Cyber risks and initial coin offerings: Evidence from the world. *Finance Research Letters.* 2021. № 41. Article number 101858. DOI: https://doi.org/10.1016/j.frl.2020.101858

3. Chen J., Zhu Q., Başar T. Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks. *Dynamic Games and Applications*. 2021. № 11(2). P. 294–325. DOI: https://doi.org/10.1007/s13235-020-00363-y

4. Berdibayev R., Gnatyuk S.,Yevchenko Y., Kishchenko V. A concept of the architecture and creation for siem system in critical infrastructure. *Studies in Systems, Decision and Control*. 2021. № 346. P. 221–242. DOI: https://doi.org/10.1007/978-3-030-69189-9_13

5. Komarov M., Davydiuk A., Onyskova A., Tkachenko V., Honchar S. Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches. *Studies in Systems, Decision and Control*. 2021. № 346. P. 189–205. DOI: https://doi.org/10.1007/978-3-030-69189-9_11

6. Uddin M.H., Ali M.H., Hassan M.K. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*. 2020. № 22(4). P. 239–309. DOI: https://doi.org/10.1057/s41283-020-00063-2

7. Couchoro M.K., Sodokin K., Koriko M. Information and communication technologies, artificial intelligence, and the fight against money laundering in Africa. *Strategic Change*. 2021. № 30(3). P. 281–291. DOI: https://doi.org/10.1002/jsc.2410

8. Karpunina E.K., Mikhailov A.M., Bondareva N.A., Lyubimenko O.A., Fedotova E.V. Blockchain Technologies as a Reflection of Modern Reality: Diversity of Opportunities Versus Security Risks. *Studies in Systems, Decision and Control.* 2021. № 314. P. 3–14. DOI: https://doi.org/10.1007/978-3-030-56433-9_1

9. Mhlanga D. Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies*. 2020. № 8(3). 45. P. 1–14. DOI: https://doi.org/10.3390/ijfs8030045

10. Smith K.J., Dhillon G. Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*. 2020. № 46(6). P. 833–848. DOI: https://doi.org/10.1108/MF-06-2019-0314

11. Carter D. How real is the impact of artificial intelligence? The business information survey 2018. *Business Information Review*. 2018. № 35(3). P. 99–115. DOI: https://doi.org/10.1177/0266382118790150

12. Atta U.l., Haq Q. Cyber Crime and Their Restriction Through Laws and Techniques for Protecting Security Issues and Privacy Threats. *Studies in Systems, Decision and Control*. 2021. № 341. P. 31–63. DOI: https://doi.org/10.1007/978-981-33-4996-4_3

13. Gagliani G. Cybersecurity, Technological Neutrality, and International Trade Law. *Journal of International Economic Law*. 2020. № 23(3). P. 723–745. DOI: https://doi.org/10.1093/jiel/jgaa006

14. Dawson M. Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*. 2018. № 35(2). P. 60–67. DOI: https://doi.org/10.1177/0266382118773624

15. Augustinos T.P. Developing cybersecurity requirements in banking (and other financial services). *Banking Law Journal*. 2018. № 135(3). P. 155–159.

REFERENCES:

1. Scott B.F. (2021) Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*, 28(1), pp. 98–111. DOI: https://doi.org/10.1108/JFC-06-2020-0118

2. An J., Duan T., Hou W., Liu X. (2021) Cyber risks and initial coin offerings: Evidence from the world. *Finance Research Letters*, 41, article number 101858. DOI: https://doi.org/10.1016/j.frl.2020.101858

3. Chen J., Zhu Q., Başar T. (2021) Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks. *Dynamic Games and Applications*, 11(2), pp. 294–325. DOI: https://doi.org/10.1007/s13235-020-00363-y

4. Berdibayev R., Gnatyuk S.,Yevchenko Y., Kishchenko V. (2021) A concept of the architecture and creation for siem system in critical infrastructure. *Studies in Systems, Decision and Control*, 346, pp. 221–242. DOI: https://doi.org/10.1007/978-3-030-69189-9_13

5. Komarov M., Davydiuk A., Onyskova A., Tkachenko V., Honchar S. (2021) Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches. *Studies in Systems, Decision and Control*, 346, pp. 189–205. DOI: https://doi.org/10.1007/978-3-030-69189-9_11

6. Uddin, M.H., Ali, M.H., Hassan, M.K. (2020) Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, 22(4), pp. 239–309. DOI: https://doi.org/10.1057/s41283-020-00063-2

7. Couchoro M.K., Sodokin K., Koriko M. (2021) Information and communication technologies, artificial intelligence, and the fight against money laundering in Africa. *Strategic Change*, 30(3), pp. 281–291. DOI: https://doi.org/10.1002/jsc.2410

8. Karpunina E.K., Mikhailov A.M., Bondareva N.A., Lyubimenko O.A., Fedotova E.V. (2021) Blockchain Technologies as a Reflection of Modern Reality: Diversity of Opportunities Versus Security Risks. *Studies in Systems, Decision and Control*, 314, pp. 3–14. DOI: https://doi.org/10.1007/978-3-030-56433-9_1

9. Mhlanga D. (2020) Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies*, 8(3), 45, pp. 1–14. DOI: https://doi.org/10.3390/ijfs8030045

10. Smith K.J., Dhillon G. (2020) Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, 46(6), pp. 833–848. DOI: https://doi.org/10.1108/MF-06-2019-0314

11. Carter D. (2018) How real is the impact of artificial intelligence? The business information survey 2018. *Business Information Review*, 35(3), pp. 99–115. DOI: https://doi.org/10.1177/0266382118790150

12. Atta U.l., Haq Q. (2021) Cyber Crime and Their Restriction Through Laws and Techniques for Protecting Security Issues and Privacy Threats. *Studies in Systems, Decision and Control*, 341, pp. 31–63. DOI: https://doi.org/10.1007/978-981-33-4996-4_3

13. Gagliani G. (2020) Cybersecurity, Technological Neutrality, and International Trade Law. *Journal of International Economic Law*, 23(3), pp. 723–745. DOI: https://doi.org/10.1093/jiel/jgaa006

14. Dawson M. (2018) Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, 35(2), pp. 60–67. DOI: https://doi.org/10.1177/0266382118773624

15. Augustinos T.P. (2018) Developing cybersecurity requirements in banking (and other financial services). *Banking Law Journal*, 135(3), pp. 155–159.