DOI: https://doi.org/10.32782/2524-0072/2022-45-84

УДК 330.43:336.71.078.3:004.056

ОЦІНЮВАННЯ РИЗИКУ КОНВЕРГЕНЦІЇ СИСТЕМ ПРОТИДІЇ ВІДМИВАННЯ ГРОШЕЙ ТА КІБЕРБЕЗПЕКИ[1]

RISK ASSESSMENT OF THE ANTI-MONEY LAUNDERING AND CYBER SECURITY SYSTEMS' CONVERGENCE

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

Рожкова Марина Сергіївна
аспірантка,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-5444-9095

Yarovenko Hanna
Sumy State University;
University Carlos III of Madrid

Rogkova Marina
Sumy State University

Дана стаття присвячена актуальному питанню визначення ризику конвергенції систем протидії відмиванню грошей та кібербезпеки. У дослідженні запропоновано науково-методичний підхід до його оцінювання, який передбачає реалізацію чотирьох етапів. Базу емпіричних даних сформували Національний індекс кібербезпеки та Індекс протидії відмиванню коштів для 114 країн світу за 2022 рік. На першому етапі було проведено кластеризацію країн за ризиком відмивання коштів, що було виконано за допомогою «Silhouette analysis» та кластеризації «k-means». На другому етапі аналогічна процедура була проведена для отримання сегментів країн щодо рівня їх кібербезпеки. На третьому етапі було запропоновано інтегральний індекс конвергенції, який було розраховано із використанням методів нормалізації та середньогеометричного. За результатами кластерного аналізу було визначено 9 груп ризику конвергенції систем протидії фінансовим та кіберризикам для різних країн світу. Четвертий етап було присвячено розробці прогнозної моделі ризику конвергенції на основі класифікаційного дерева рішень.

Ключові слова: відмивання грошей, дерево рішень, кібербезпека, кластерний аналіз, конвергенція, ризик.

The growth of financial and cyber threats leads to the most significant losses in the financial sector. Only complex approaches can be the most effective to counteract them, which require processes of systems' convergence of financial monitoring and cyber security. Therefore, this article is devoted to determining the convergence risk for different countries. The study proposes a scientific and methodological approach to its evaluation, which involves implementing four stages. The empirical database was formed by the National Cyber Security Index and the Anti-Money Laundering Index for 114 countries in 2022. The first index characterizes the level of development of the country's cyber security system. The second indicator reflects the degree of criminal proceeds legalization risk. Calculations were made using the Python programming language. In the first stage, countries were clustered according to the money laundering risk performed using such methods as "Silhouette analysis" and "K-means" clustering. As a result, seven clusters were obtained, which make it possible to identify countries by the possibilities

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».

of criminal income legalization. In the second stage, a similar procedure was carried out to obtain countries' segments regarding the level of their cyber security. As a result, six clusters were obtained, which allowed identifying the level of development of the cyber threat countermeasure system. An integral convergence index was proposed and calculated in the third stage using normalization and geometric mean methods. Based on the cluster analysis results, nine risk groups of the systems' convergence for countering financial and cyber risks were determined for different countries. The fourth stage was devoted to developing a predictive model of convergence risk based on a classification decision tree. The quality of the model turned out to be high, although, for the second classification group, the model will not be able to make the correct prediction. The proposed approach is of practical importance for improving countries' strategies for combating financial and cybercrimes.

Keywords: money laundering, decision tree, cyber security, cluster analysis, convergence, risk.

Постановка проблеми. За останні роки рівень та масштаби кіберзлочинів невпинно зростають, а втрати від них значно переважають збитки від торгівлі наркотиками та зброєю, чого не спостерігалося ще п'ять років тому. Фінансові установи останнім часом найбільше потерпають саме від кіберзлочинців, ніж, наприклад, від змін на фондових біржах чи боргових криз. Це все зумовлює потребу в удосконаленні системи боротьби проти різного виду кібернетичних загроз.

З іншого боку, процеси відмивання коштів, отриманих незаконним шляхом або в результаті фінансування тероризму, та подальша їх легалізація також є значною проблемою для багатьох країн світу, в тому числі й для України. Розвиток технологій та вдосконалення кібернетичних інструментів дозволило злочинцям знаходити також нові методи й у відмиванні коштів, пов'язані із залученням криптовалюти та інших видів електронних грошей. Це значно підвищує потенційні ризики та можливі збитки від їх настання. Тому формування комплексу сучасних методів протидії відмиванню коштів є важливою складовою фінансової безпеки.

Кіберзагрози та небезпека щодо легалізації коштів мають багато спільних характеристик, що уможливлює конвергенцію обох систем для розробки комплексних та системних підходів щодо їх протидії. Ризики такого типу здатні модифікуватись та адаптуватися до змін системи ще задовго до виникнення можливості їх передбачення та усунення. А методи, що діють для одного виду загрози, можуть бути зовсім недієвими для іншого, тому навіть найменший ризик може спричинити значні втрати і призвести до краху цілої системи. Проведення аналітики щодо їх виявлення та усунення є надзвичайно складним завданням. Тому розробка підходу щодо оцінки ризиків, пов'язаних з фінансовими та кіберзагрозами, може потребувати схожих підходів, які будуть базуватися на конвергенційних засадах системи фінансового моніторингу та кіберзахисту.

Аналіз останніх досліджень і публікацій. В сучасному світі темі вивчення інтегрованій системі протидії кібернетичним злочинам та фінансовим махінаціям присвячено не досить багато праць, як вітчизняних, так і закордонних вчених. Більшість з них розкриває тільки окремий аспект цієї проблеми. Однією із найбільш ґрунтовних праць вважається робота Еллінга М. та Шнелла В, які досліджували сферу страхування кіберризиків [1]. Айзенбах Т. М., Ковнер А. та Лі М. Дж. розглядали дану проблему в контексті впливу кіберзагроз на фінансову систему країни [2]. Гатцерт Н. та Шуберт М. приділяли увагу процесам управління кіберризиками у фінансових установах [3]. Слід відмітити важливість дослідження документаційного забезпечення галузі кібербезпеки, розглянуте Ю. Кожедубом [4]. Фабріс Н. вивчав вплив пандемії на фінансову систему та кіберризики, які виникають через зростання обсягів цифровізації бізнеса [5]. Вучиніч М. та Лубурич Р. досліджували сферу фінансових технологій та відповідних їй кіберзагроз, які становлять потенційну небезпеку для фінансової системи країни [6]. Уддін М. Х., Алі М. Х., Хассан М. К. синтезували статті та політичні документи, які розкривають ризики кібербезпеки, які завдають шкоди банківській системі країні [7]. Гроді А. Д. наголошував на інвестиційній складовій для запобігання кіберзагрозам фінансовій системі країни [8]. Значний внесок у дослідження кіберризиків мають приватні консалтингові компанії, які мають на меті практичне застосування теоретичних напрацювань. Серед них варто виділити діяльність Deloitte, AON, IBM, тощо [9]. Саме ці компанії в останні роки сформували велику базу знань, що допомагає не лише науковцям, але й підприємствам та урядам у діяльності фінансової та кібербезпеки. Не дивлячись на значний науковий доробок теоретиків та практиків, існує ряд ще невирішених проблем, таких як визначення ризиків інтеграції систем боротьби із фінансовими та кіберзагрозами, що буде досліджено у даній роботі.

Формулювання цілей статті. Метою даного дослідження є розробка методики оцінки ризику конвергенції системи протидії відмивання грошей та кібербезпеки різних країн світу.

Виклад основного матеріалу дослідження. Методика оцінки ризику конвергенції системи протидії відмивання грошей та кібербезпеки різних країн світу, яка пропонується, здійснюється в декілька етапів.

На *першому етапі* проведемо оцінку ризиків легалізації кримінальних доходів, що характеризує систему фінансових шахрайств. Основним індексом для цього є індекс протидії відмиванню коштів (Anti-Money Laundering Index – AML) [10]. Вперше він був розрахований та застосований на базі Базельського інституту управління у 2012 році, який діє під керівництвом Програми Організації Об'єднаних Націй в сфері попередження злочинності та кримінального правосуддя. Даний індекс враховує не рівень корупції та кримінальної діяльності, що пов'язана з відмиванням коштів та фінансуванням тероризму, а більше ризики їх виникнення та розвитку в різних країнах. Він включає в себе показники різної спрямованості та значимості, що дозволяє отримати всебічну картину щодо станів системи протидії відмиванню коштів. Для оцінки ризиків було узято дані AML-індексу за 2022 рік для 114 країн світу.

Застосуємо метод кластеризації, оскільки саме такі методи дозволяють отримати групи країн з подібними характеристиками. Кластеризацію буде виконано за допомогою методу «K-means» та «Silhouette analysis». «Silhouette analysis» використовується для визначення відстані поділу між отриманими кластерами. Він відображає, наскільки близько розташована кожна точка в одному кластері відповідно до інших кластерів. Його результати дозволяють оцінити кількість кластерів, які доцільно буде використати в процесі K-середніх [11].

Результати «Silhouette» оцінки для індексу AML представлені на рисунку 1, з якого можна зробити висновок, що найбільш оптимальною кількістю кластерів є вісім, оскільки оцінка в даному випадку є найвищою. Для проведення кластеризації методом «K-means» необхідно використати саме таку кількість кластерів.

На рисунку 2 представлений результат проведеної кластеризації країн за індексом AML.

Розподіл на кластери дозволив отримати досить показові групи, які надають змогу зробити певні оцінки. Як можна побачити, країни, які є достатньо розвиненими та мають високі показники в забезпеченні фінансової безпеки, віднесені до однієї групи. Так, найкращі показники мають такі країни, як Австралія, Велика Британія, Данія, Норвегія, Фінляндія, Нова Зеландія Греція, Ізраїль, Франція, Литва, Словенія, Ісландія та Швеція. Вони мають

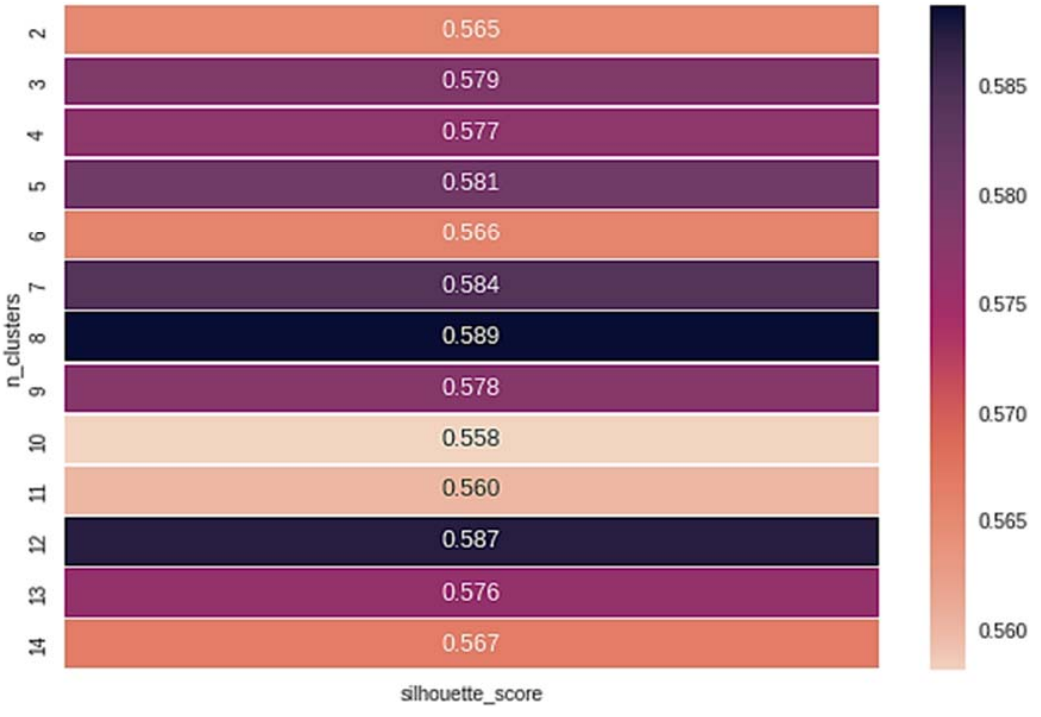

Рис. 1. Результати «Silhouette analysis» щодо оптимального вибору кластерів країн за індексом AML

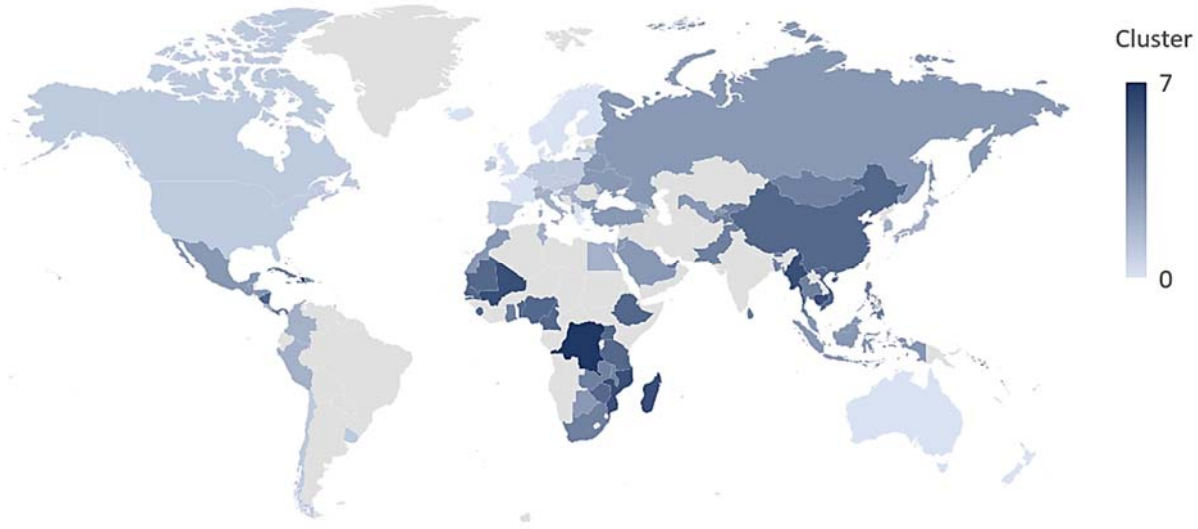

Рис. 2. Карта кластерів країн за індексом AML

високий рівень протидії відмиванню коштів і фінансування тероризму та впроваджують ефективні рішення у боротьбі з легалізацією кримінальних доходів. Вони не є привабливими для злочинців, оскільки мають потужні системи захисту у фінансових установах.

Україна входить до третьої групи за показником ризиковості щодо відмивання кримінальних доходів. Це обумовлено тим, що наша країна має досить високий рівень тінізації та корумпізації економіки, що в сукупності з військовими діями створює сприятливе підґрунтя для зменшення ризиків для легалізації нелегальних коштів. Ці процеси гальмують розвиток в економіці та соціальній сфері. До даної групи увійшли ще 21 країна, серед яких слід зазначити Гондурас, Туреччину, Сейшельські острови, Барбадос, Ямайку та інші. Країни, які є сприятливими для легалізації кримінальних доходів є країни 6 та 7 кластерів. Сюди відносяться Малі, Камбоджі, Мадагаскар, Мозамбік, М'янма, Гаїті та Демократична республіка Конго. Перелічені країни відносяться до найменш розвинених. Реформи, що проводяться в них, спрямовані на внутрішні сфери і не приносять відповідних позитивних результатів для їх розвитку. Режими цих країн є досить обмежувальними, а рівень розвитку економіки нестабільним.

На *другому етапі* проведемо оцінку ризиків, пов'язаних із системою протидії кіберзагрозам, яку характеризує Національний індекс кібербезпеки (National Cyber Security Index – NCSI) [12]. Для його розрахунку використовується значна кількість показників, найважливішим серед яких є стан законодавства, пов'язаний з охороною даних та кібербезпекою, оскільки саме юридичне забезпечення дозволяє підготувати основу для реалізації стабільних заходів щодо протидії злочинам. Враховується також частота виникнення кіберінцидентів, рівень освіти громадян в сфері кібербезпеки, види та ефективність заходів щодо захисту персональних даних громадян, щодо реагування на кібератаки та можливості зниження кіберризиків, результативність та кількісне виявлення загального рівня боротьби з кіберзлочинністю. Саме цей індекс є відображенням стабільності та надійності системи кіберзахисту країн. Для оцінки було узято дані NCSI-індексу за 2022 рік для 114 країн світу.

Проведемо кластеризацію, результати якої представлені на рисунку 3. Найвище значення оцінки відповідає кількості кластерів, яка дорівнює двом. Але дана кількість кластерів не дозволяє виявити більш детальні групи країн, тому для проведення Silhouette analysis було обрано кластери з найвищою оцінкою – 6. Кластеризація країн із використанням 6 кластерів дозволить отримати групи з однорідними даними, тому для подальших розрахунків обираємо саме дану кількість.

На рисунку 4 представлена карта кластерів країн за індексом NSCI після проведеного «Silhouette analysis».

Як можна побачити, до групи з найбільш високо розвиненим рівнем кібербезпеки відносяться країни нульового кластеру: Греція, Бельгія, Нідерланди, Німеччина, Іспанія, Малайзія, Саудівська Аравія, Сербія, Хорватія, Італія, Польща, Словаччина, Португа-

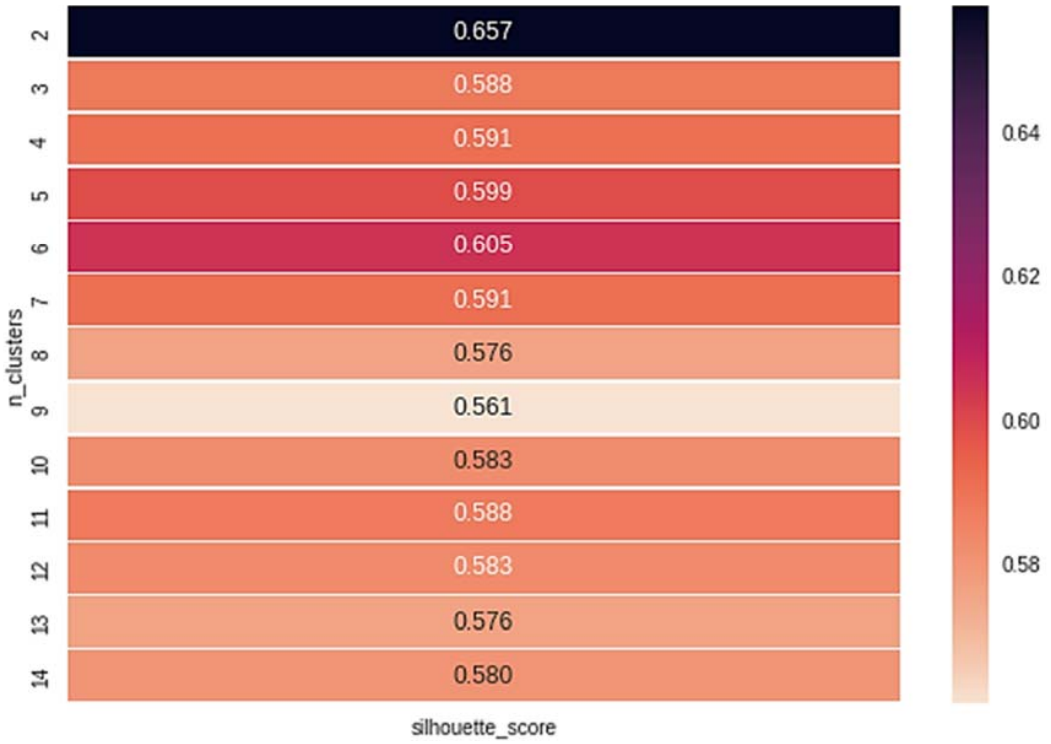

Рис. 3. Результати «Silhouette analysis» щодо оптимального вибору кластерів країн за індексом NSCI

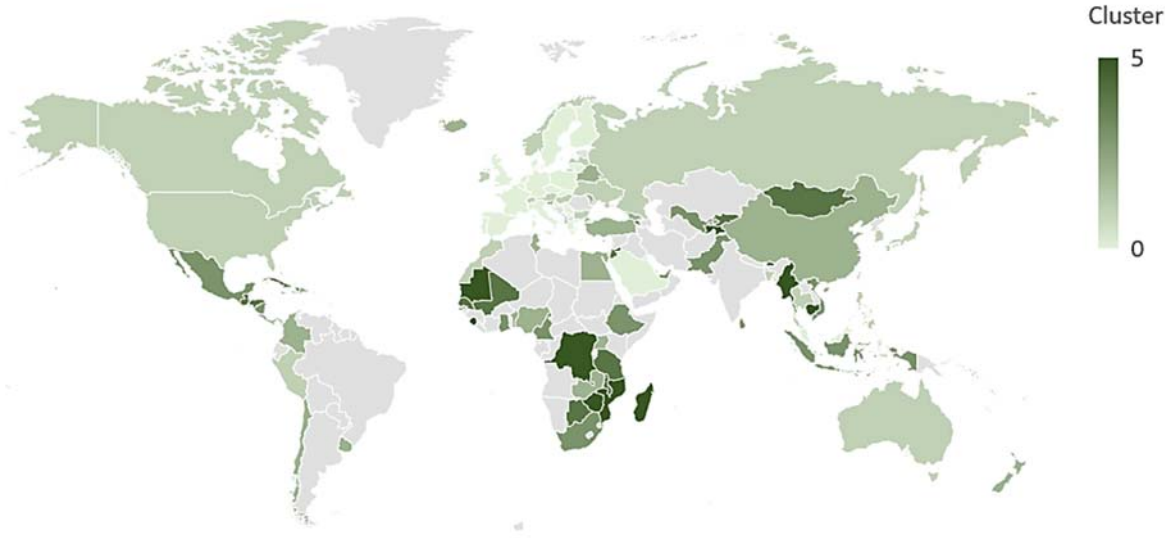

Рис. 4. Карта кластерів країн за індексом NSCI

лія, Чехія, Велика Британія, Данія, Франція, Литва, Швеція та Фінляндія. Такі результати свідчать, що ці країни мають високий рівень національної кібербезпеки, який передбачає організацію потужного комплексу інформаційного, програмного, технічного та організаційного забезпечення з питань кіберзахисту. Так само, можна побачити, що найнижчі показники мають Конго, Мадагаскар, Мозамбік, Гаїті, Камбоджі, Зімбабве, Таджикистан, Вануату, тощо. Тобто ці країни є менш розвиненими і потребують вкладень і модифікації не лише окремої системи кіберзахисту, але прогресивних державних заходів в цілому щодо розвитку її політичної та соціально-економічної сфер.

На *третьому етапі* проведемо оцінку ризиків, пов'язаних із конвергенційними процесами систем протидії фінансовим та кіберзлочинам. З цією метою доцільно впровадити

комплексну оцінку, яка в собі поєднувала б можливості країн щодо кіберзахисту від різного роду загроз та їх потенціал щодо зниження ризиків відмивання кримінальних доходів та фінансування тероризму. Пропонуємо визначити інтегральний індекс конвергенції наступним чином:

здійснюється нормалізація AML–індексу за критерієм Севіджа, як дестимулятора (формула 1):

$$x_{ij}^{*} = \frac{x_j^{max} - x_{ij}}{x_j^{max} - x_j^{min}}, \quad (1)$$

– здійснюється нормалізація NSCI за природньою нормалізацією як стимулятора (формула 2):

$$x_{ij}^{*} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}}, \quad (2)$$

– інтегральний індекс конвергенції утворюється як середньогеометричне (формула 3):

$$G_m = \left(\prod_{i=1}^{n} \widetilde{x}_{ik} \right)^{1/n}. \quad (3)$$

Розглянемо результати кластеризації щодо «Інтегрального показника конвергенції» (рис. 5). Найвище значення оцінки відповідає кількості кластерів, яке дорівнює двом. Але така кількість кластерів не дозволить отримати уявлення про ризик конвергенції. Тому для проведення «Silhouette analysis» було обрано кластер з найвищою оцінкою – 9. Використання 9 кластерів країн дозволить отримати групи з однорідними даними, що дозволяє провести кластерний аналіз за методом «K-means».

На рисунку 6 представлений результат проведеної кластеризації країн за «Інтегральним індексом конвергенції» після проведеного «Silhouette analysis».

Проведення кластеризації на основі інтегрального індексу конвергенції систем показує розподіл країн за можливостями протидіяти кіберзагрозам та фінансовим злочинам. Чим ближче його значення до 1, тим нижчий рівень ризику конвергенції, тобто в країнах створені сприятливі умови, які дозволяють інтегрувати систему кіберзахисту та систему фінансового моніторингу. Якщо значення даного показника наближається до 0, то це свідчить про неготовність країни до конвергенції двох систем, що може бути викликано сформованими сприятливими умовами для розвитку фінансової та кіберзлочинності.

Виходячи з отриманих даних сформуємо критерії ризику в залежності від отриманих кластерів для індексу конвергенції. Результати представлені в таблиці 1. Таблиця містить усереднені значення AML та NSCI для відповідного кластеру. Країни, що відносяться до 0-го кластеру генерують найнижчий ризик конвергенції. Відповідно, країни 8-го кластеру генерують найвищий ризик. Застосування

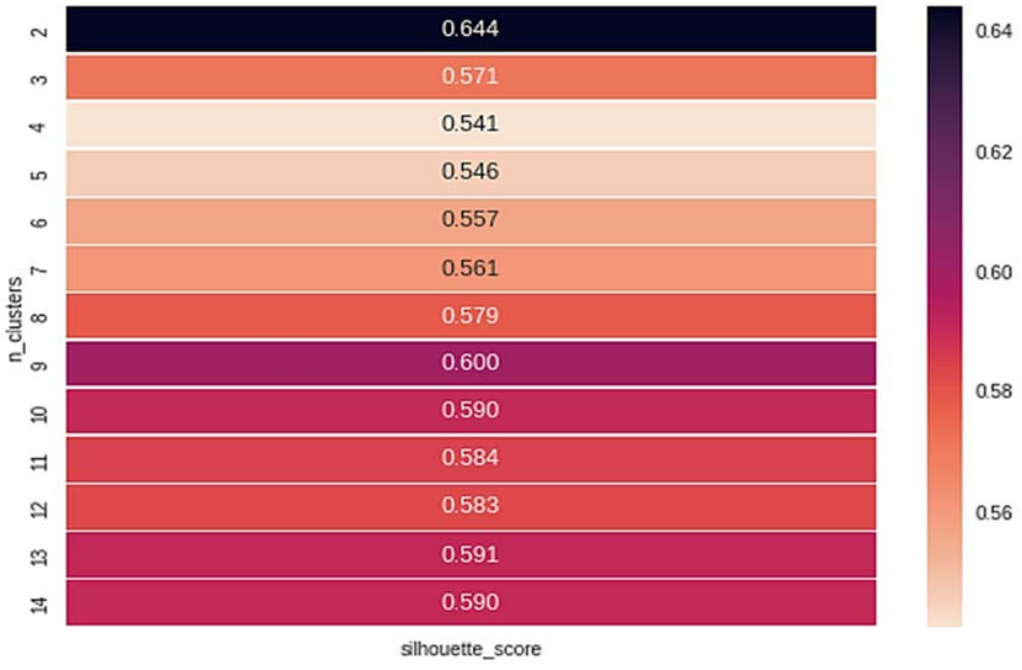

Рис. 5. Результати «Silhouette analysis» щодо оптимального вибору кластерів країн за умови конвергенції систем

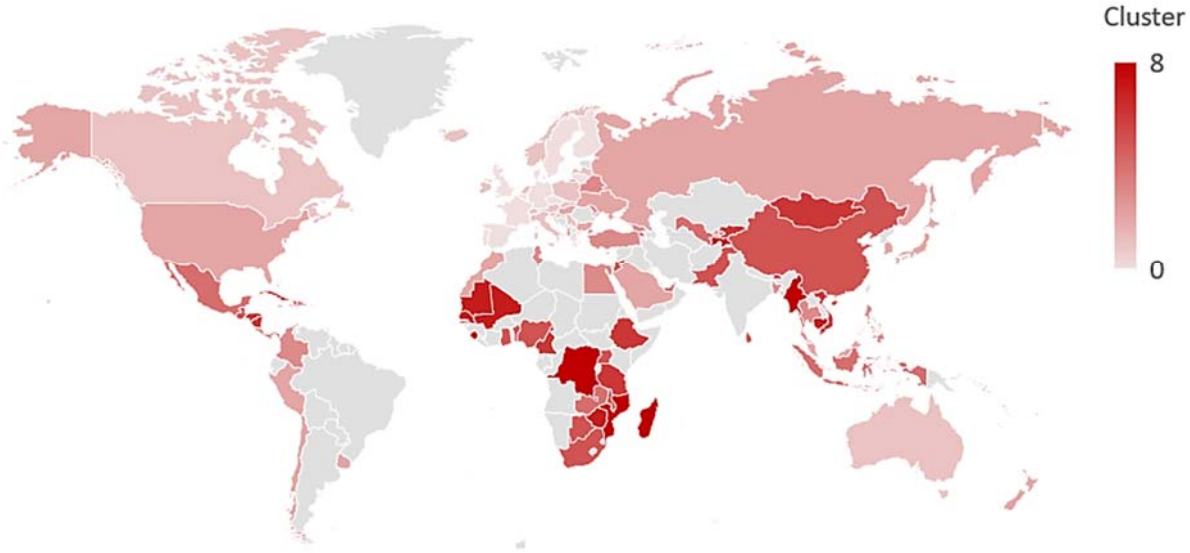

Рис. 6. Карта кластерів країн за рівнем конвергенції систем протидії відмиванню кримінальних доходів та кібербезпеки

даних карти 6 та таблиці 1 дозволить сформувати висновки щодо потенційних ризиків конвергенції систем протидії фінансовим та кіберзлочинам.

Карта кластерів 6 показує, що найбільш сприятливі умови для конвергенції сформовані в 12 країнах, таких як Німеччина, Бельгія, Португалія, Іспанія, Чехія, Греція, Велика Британія, Данія, Франція, Литва, Швеція, Фінляндія. Ці країни генерують найнижчий ризик. Що стосується України, то її було віднесено до 2-го кластеру. У даному випадку вона має високий ризик легалізації кримінальних доходів, що компенсується розвиненим рівнем кібербезпеки. Це дозволяє зменшувати ризики відмивання коштів за рахунок можливостей системи кіберзахисту. Тобто Україна має значний потенціал для створення взаємодії фінансової та інформаційної систем та підтримки їх безпеки. Рівень її системи відмивання коштів та легалізації доходів значно може скорочуватися за рахунок безпекового потенціалу. В країнах, що віднесені до 6–8 кластерів, сформовані найбільш несприятливі умови, оскільки вони знаходяться на нижчій стадії економічного і соціального розвитку. Сюди відносять найменш розвинені країни Африки, Азії та острівні держави.

На *четвертому етапі* побудуємо прогнозну модель ризику конвергенції, яка дозволить визначити відповідний його рівень за рахунок зміни умов конвергенції системи кібербезпеки та фінансового моніторингу. Для побудови класифікаційного дерева рішень було використано мову програмування Python. Модель було визначено на основі коефіцієнту Джині. Результат класифікаційної моделі представлений на рисунку 7.

Оцінка якості побудованого дерева представлена на рисунку 8.

В цілому загальна точність моделі є високою і відповідає приблизно 81%. Хоча даний показник не є гарним для моделей такого рівня, але це пов'язано із тим, що вона передбачає класифікацію значної кількості груп. Наприклад, для другого кластеру модель не зможе зробити жодного передбачення, хоча інші рівні ризику вона передбачатиме на рівні вище середнього.

Таблиця 1

Ідентифікація ризику в залежності від кластерів індексу конвергенції

Низький ризик		Помірний ризик		Високий ризик	
Кластери	**AML / NSCI**	**Кластери**	**AML / NSCI**	**Кластери**	**AML / NSCI**
0	3,65 / 88,42	3	5,09 / 55,95	6	6,07 / 22,94
1	4,09 / 72,96	4	5,30 / 41,43	7	6,30 / 12,51
2	4,72 / 67,61	5	5,83 / 37,29	8	7,75 / 9,31

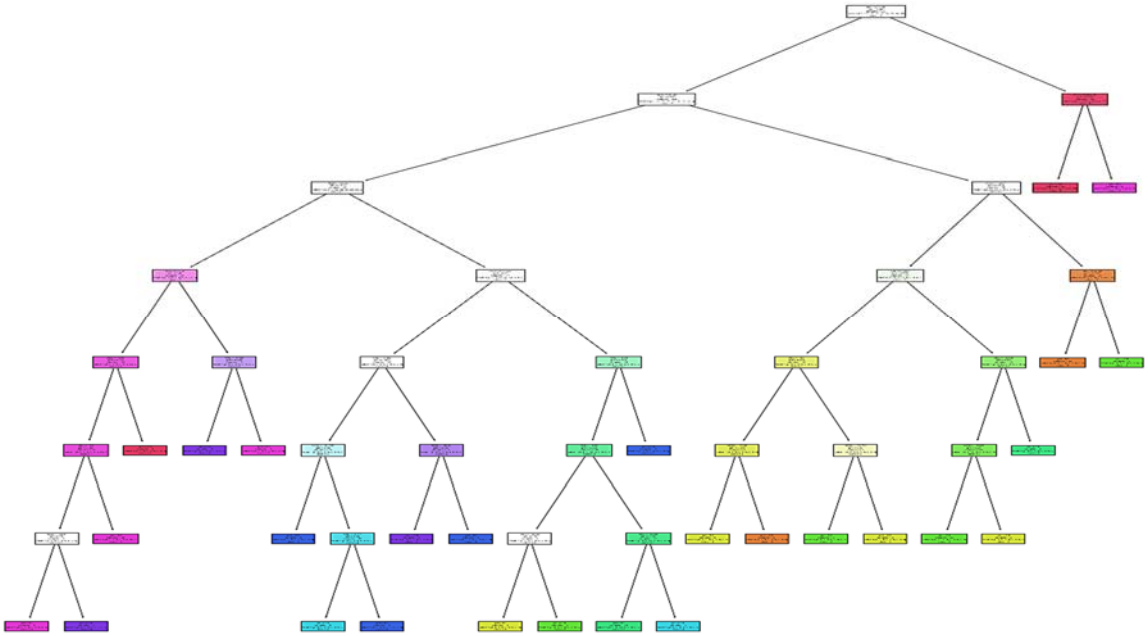

Рис. 7. Класифікаційна модель прогнозування ризиків конвергенції системи протидії фінансовим та кіберзлочинам

```
Confusion Matrix:
[[4 0 0 0 0 0 0 0 0]
 [2 3 0 0 0 0 0 0 0]
 [0 2 0 0 0 0 0 0 0]
 [0 0 0 2 0 0 0 0 0]
 [0 0 0 0 7 0 0 0 0]
 [0 0 0 0 0 3 0 0 0]
 [0 0 0 0 0 1 3 0 0]
 [0 0 0 0 0 0 0 2 1]
 [0 0 0 0 0 0 0 0 1]]
Classification Report:
              precision    recall  f1-score   support

           0       0.67      1.00      0.80         4
           1       0.60      0.60      0.60         5
           2       0.00      0.00      0.00         2
           3       1.00      1.00      1.00         2
           4       1.00      1.00      1.00         7
           5       0.75      1.00      0.86         3
           6       1.00      0.75      0.86         4
           7       1.00      0.67      0.80         3
           8       0.50      1.00      0.67         1

    accuracy                           0.81        31
   macro avg       0.72      0.78      0.73        31
weighted avg       0.79      0.81      0.78        31

Accuracy: 0.8064516129032258
```

Рис. 8. Оцінка якості класифікаційної моделі прогнозування ризиків конвергенції системи протидії фінансовим та кіберзлочинам

Висновки. Стабільність систем захисту як проти кіберризиків, так і проти процесів відмивання фінансових коштів, в першу чергу залежить від рівня розвитку країни та комплексу заходів щодо мінімізації та попередження можливих загроз. Неможливо створити єдину модель, яка б задовольняла усі потреби, оскільки, не дивлячись на можливі загальні тенденції, кожна система має власні вразливі місця, до яких можуть адаптуватися

різні види загроз. Тому для підвищення рівня кібербезпеки та зниження рівня відмивання коштів необхідно застосовувати комплексні заходи, які базуються на конвергенційних процесах системи фінансового моніторингу та кібербезпеки.

Виходячи з необхідності вирішення проблеми попередження ризиків фінансових і кіберзагроз, було запропоновано науково-методичний підхід до оцінювання ризиків конвергенції системи протидії фінансовим і кібершахрайствам на основі проведення сегментації країн із використанням кластерного аналізу за рівнем їх кібербезпеки, ризиком відмивання кримінальних доходів. В роботі запропоновано розрахунок інтегрального показника, визначення якого дозволить оцінити ризик конвергенції систем протидії фінансовим і кібершахрайствам. В результаті було встановлено кластери країн, для яких було означено 9 груп ризику, що дозволяє оцінити можливості країн щодо спроможності та готовності систем їх фінансового моніторингу та кібербезпеки інтегруватися в єдину та комплексну систему фінансового кіберзахисту. Запропонована методика передбачає побудову класифікаційної моделі дерева рішень оцінки ризиків конвергенції, яка дозволить спрогнозувати рівень ризику для будь-якої країни за сформованих умов існування і розвитку системи боротьби із легалізацією кримінальних доходів і фінансуванням тероризму, а також системи кіберзахисту. Запропонований підхід доцільно застосовувати в процесі розробки стратегії країни для боротьби із фінансовими і кіберзлочинами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Eling M., Schnell W. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*. 2016, vol. 17(5). P. 474–491. DOI: https://doi.org/10.1108/JRF-09-2016-0122.

2. Eisenbach T. M., Kovner A., Lee M. J. Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*. 2022, vol. 145(3). P. 802–826. DOI: https://doi.org/10.1016/j.jfineco.2021.10.007.

3. Gatzert N., Schubert M. Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*. 2022, vol. 89(3). P. 725–763. DOI: https://doi.org/10.1111/jori.12381.

4. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. *Information Technology and Security*. 2017, vol. 5(1). P. 82–95.

5. Fabris N. Impact of Covid-19 Pandemic on Financial Innovation, Cashless Society, and Cyber Risk. *ECONOMICS*. 2022, vol. 10(1). P. 73–86. DOI: https://doi.org/10.2478/eoik-2022-0002.

6. Vučinić M., Luburić R. Fintech, Risk-Based Thinking and Cyber Risk. *Journal of Central Banking Theory and Practice*. 2022, vol. 11(2). P. 27–53. DOI: https://doi.org/10.2478/jcbtp-2022-0012.

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

8. Grody A. D. Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*. 2020, vol. 13(2). P. 155–162.

9. Institute of Risk Management – expert Risk Predictions 2018 and the Risk Agenda 2025. *Institute of Risk Management*. URL: https://www.theirm.org/news/institute-of-risk-management-expert-risk-predictions-2018-and-the-risk-agenda-2025/ (дата звернення: 20.12.2022).

10. Basel AML. Index Assessing Money Laundering Risks Around The World. *Basel ALM Index* URL: https://index.baselgovernance.org/ (дата звернення: 20.12.2022).

11. Haro G. Shape from silhouette consensus and photo-consistency. URL: https://repositori.upf.edu/bitstream/handle/10230/35708/haro_icip14_shape.pdf;jsessionid=21B7F0CD85AB9435B87CD7AB8D338316?sequence=1/ (дата звернення: 20.12.2022)

12. National Cybersecurity Index. *E-Governance Academy*. URL: https://ncsi.ega.ee/ (дата звернення: 20.12.2022).

REFERENCES:

1. Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. DOI: https://doi.org/10.1108/JRF-09-2016-0122.

2. Eisenbach, T. M., Kovner, A. & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802–826. DOI: https://doi.org/10.1016/j.jfineco.2021.10.007.

3. Gatzert, N. & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725–763. DOI: https://doi.org/10.1111/jori.12381.

4. Kozhedub, Yu. (2017). Analiz dokumentiv z keruvannia ryzykom kiberbezpeky [Analysis of cybersecurity risk management documents]. *Information Technology and Security*, *5*(1), 82–95. [in Ukrainian]

5. Fabris, N. (2022). Impact of Covid-19 Pandemic on Financial Innovation, Cashless Society, and Cyber Risk. *ECONOMICS*, *10*(1), 73–86. DOI: https://doi.org/10.2478/eoik-2022-0002.

6. Vučinić, M. & Luburić, R. (2022). Fintech, Risk-Based Thinking and Cyber Risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27–53. DOI: https://doi.org/10.2478/jcbtp-2022-0012.

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

8. Grody, A. D. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*, *13*(2), 155–162.

9. Institute of Risk Management (2022). *Institute of Risk Management – expert Risk Predictions 2018 and the Risk Agenda 2025*. Retrieved from: https://www.theirm.org/news/institute-of-risk-management-expert-risk-predictions-2018-and-the-risk-agenda-2025.

10. Basel AML Index (2022). *Basel AML Index. Assessing Money Laundering Risks Around The World*. Retrieved from: https://index.baselgovernance.org.

11. Haro G. *Shape from silhouette consensus and photo-consistency*. Retrieved from: https://repositori.upf.edu/bitstream/handle/10230/35708/haro_ icip14_shape.pdf;jsessionid=21B7F0CD85AB9435B87CD7AB8D338316?sequence=1.

12. E-Governance Academy (2022). *National Cybersecurity Index*. Retrieved from: URL: https://ncsi.ega.ee.