DOI: 10.26565/2310-9513-2021-14-12 ISSN 2310-9513
УДК 330.43 : 004.056 : 336.1.07

ОЦІНКА РІВНЯ КОНВЕРГЕНЦІЇ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ КРИМІНАЛЬНИХ ДОХОДІВ*

Яровенко Ганна Миколаївна
докт. екон. наук, доцентка
кафедра економічної кібернетики
Сумський державний університет
вул. Римського-Корсакова, 2, м. Суми, Україна
e-mail: h.yarovenko@biem.sumdu.edu.ua
ORCID: https://orcid.org/0000-0002-8760-683
Колотіліна Олена Василівна
асистентка
кафедра економічної кібернетики
Сумський державний університет
вул. Римського-Корсакова, 2, м. Суми, Україна
e-mail: o.kolotilina@biem.sumdu.edu.ua
ORCID: https://orcid.org/0000-0002-8928-0859
Світлична Альона Олексіївна
студентка
кафедра економічної кібернетики
Сумський державний університет
вул. Римського-Корсакова, 2, м. Суми, Україна
e-mail: aliona.svitlychna@student.sumdu.edu.ua
ORCID: https://orcid.org/0000-0002-8981-7986

Зростання обсягів фінансових і кібершахрайств призводять до дестабілізації фінансового сектору країни та негативно впливають на розвиток їх економіки, що потребує розробки та впровадження дієвих інструментів та заходів на рівні державного управління. Конвергенція системи кібербезпеки та протидії легалізації кримінальних доходів і фінансування тероризму є перспективним напрямком у боротьбі із фінансовими шахрайствами. Предметом дослідження в статті є науково-методичний підхід до формування інтегральних показників оцінювання станів різних систем, який базується на функції Харрінгтона – Менчера. Мета полягає у проведенні оцінювання рівня потенційної конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів і фінансуванню тероризму на основі визначення їх інтегральних показників та застосування функції Харрінгтона – Менчера. Завдання: сформувати базу факторів для здійснення оцінювання; здійснити їх нормалізацію шляхом застосування нелінійної нормалізації; трансформувати нормалізовані значення обраних показників бази дослідження до безрозмірної шкали бажаності Харрінгтона; ідентифікувати вид функції залежності проміжного значення показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії фінансовим шахрайствам, від їх фактичних значень; розрахувати показники для формалізації перетворення Харрінгтона-Менчера; за допомогою канонічного аналізу визначити вагові показники; розрахувати інтегральні показники, що характеризують рівень розвитку системи кібербезпеки та протидії легалізації кримінальних доходів, а також визначити рівень конвергенції систем. В статті використовуються загальнонаукові методи: системний аналіз – для визначення факторів, що характеризуються системи кібербезпеки та протидії фінансовим шахрайствам; метод переваг та функція Харрінгтона – Менчера – під час інтегрального оцінювання. Отримано наступні результати: за рівнем кібербезпеки найвищі оцінки мають економічно розвинені країни – країни Європи, США, Канада, Австралія, Нова Зеландія, Японія. Інші країни мають низку проблем в цій сфері про що свідчить отримані ними оцінки «дуже погано», «погано» та «задовільно». За рівнем протидії легалізації кримінальних доходів виявилося, що ця сфера є критичної для країн із високим рівнем злочинності, тероризму, наявними військовими конфліктами та високим рівнем фінансової таємниці, що робить їх потенційними суб'єктами процесів відмивання незаконних коштів. Також встановлено, що

* ***Cite as:*** Yarovenko, H., Kolotilina, O., Svitlychna, A. (2021). Assessment Of The Convergence Level Of The Cyber Security System And Counteraction Of Money Laundering *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism.* 14, 119-130. (in Ukrainian). https://doi.org/10.26565/2310-9513-2021-14-12

за рахунок конвергенції двох систем рівень розвитку країни підвищиться. Висновки: отримані результати дослідження слід врахувати в процесі розробки стратегії конвергенції системи кібербезпеки та протидії фінансовим шахрайствам на макрорівні.

Ключові слова: конвергенція, кібербезпека, фінансові шахрайства, легалізація кримінальних доходів, функція Харрінгтона – Менчера.

Постановка проблеми. На сьогодні проблема боротьби із відмиванням кримінальних доходів та фінансування тероризму є вкрай актуальною для країн світу. Це пов'язано із тим, що за рахунок процесу легалізації коштів, джерела походження яких мають незаконний характер, значні грошові суми уникають оподаткування, сприяють розвитку тіньового сектору, стимулюють підвищення рівня злочинності та, врешті-решт, можуть вплинути на дестабілізацію економіки країни, створення конфліктів у суспільстві, зниження довіри до країни з боку міжнародних партнерів. За результатами опитування, проведеного консалтинговою компанією "PwC" за 2018 рік, обсяг операцій з відмивання кримінальних доходів та фінансування тероризму становив 1 трлн. дол., що склало приблизно від 2% до 5% світового ВВП [1]. Саме тому світова спільнота схвильована існуванням даної проблеми, оскільки з'являються загрози міжнародній фінансовій системі. Профільна міжнародна організація FATF пропонує необхідні заходи щодо здійснення боротьби та протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, в рамках яких розроблено спеціальні стандарти та інструменти, які періодично оновлюються у відповідності до реалій функціонування фінансової системи.

З іншого боку, наслідки промислової революції 4.0 викликали стрімкий розвиток інформаційних технологій та впровадження їх в усі сфери життєдіяльності людини. Процеси автоматизації та діджиталізації призвели до зростання рівня кіберзлочинів, особливо у фінансовій сфері, яка входить у п'ятірку найбільш атакованих сфер світу [2]. Також рівень збитків від кіберзлочинності зростає у геометричній прогресії та за прогнозованими оцінками експертів він дорівнюватиме за 2021 рік 6 трлн. дол. [2]. Тому проблема забезпечення відповідного рівня кіберзахисту фінансової системи країни та інших її систем є критично важливою та практично значущою.

Вирішення окреслених проблем є можливим за рахунок конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, оскільки синергетичний ефект від їх взаємодії буде значно більшим ніж від їх окремого функціонування. Це можливо за рахунок їх системного поєднання на технологічному, програмному, інформаційному, правовому та організаційному рівнях. Процес інтеграції є досить складним і потребує застосування зважених рішень, оскільки наслідки від неправильних заходів можуть бути катастрофічними. Тому попередньо необхідно здійснити оцінку фактичного стану системи кібербезпеки та протидії фінансовим шахрайствам для визначення потенційного рівня їх конвергенції для різних країн.

Аналіз останніх досліджень і публікацій. Питання конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів є досить новим для сучасної наукової спільноти. Тому можна виділити тільки ряд тих наукових досліджень, які проводилися у близькому до даного питання напрямку.

Найбільш актуальним серед практиків та науковців є напрям дослідження проблеми протидії шахрайству із кредитними картками. Це відбувається завдяки зростання обсягу шахрайств по відношенню до фізичних осіб – клієнтів банків за рахунок появи низки методів, таких як соціальна інженерія. Дану тематику досліджували Діліп М.Р., Наванет А.В., Абхішек М. [3], Ванг Р., Лью Дж. [4], Мішра С.П., Кумарі П. [5], Мектерович І., Каран М., Пінтар Д., Брккіч Л. [6], та інші.

Також вивчаються інструменти протидії фінансовим та кібершахрайствам. Особливо популярними є засоби машинного навчання та штучного інтелекту, які використовуються в процесі виявлення операцій, що носять ознаки шахрайських. Так, Чен З., Ван Хоа Л.Д., Тео Е.Н. , Назір А., Каруппія Е.К., Лам К.С. дослідили можливості застосування засобів машинного навчання для виявлення операцій з легалізації кримінальних доходів [7]. Чжоу Ю., Сонг Кс., Чжоу М. запропонували метод бустінгу для прогнозування шахрайських операцій [8]. Мультиагентна система для виявлення операцій з відмивання коштів, отриманих злочинним шляхом, яку можна інтегрувати в банківську інформаційну систему, була розроблена Гао С., Сю Д., Ванг Х., Грін П. [9]. Карпуніна Є.К., Михайлов А.М., Бондарева Н.А., Любименко О.А., Федотова Є.В. досліджували можливості застосування блокчейн-технологій для протидії фінансовим та кібершахрайствам [10-15].

Важливими є питання організаційного, технологічного, правового та інформаційного забезпечення системи кібербезпеки та протидії легалізації кримінальних доходів. Так, в напрямку інтеграції політичної, освітньої та технологічної сфери для забезпечення ефективності функціонування системи кібербезпеки та протидії фінансовим шахрайствам проведено дослідження М. Доусоном [11]. Діонісій С. Деметіс розглядав технології виявлення операцій з легалізації

незаконних коштів, серед яких виділяв ризикологію та методи оцінювання ризиків [14]. Гальяні Г. досліджував поняття «технологічної нейтральності» по відношенню до кібербезпеки у контексті формування та забезпечення міжнародного правового поля з даного питання [16].

Не зважаючи на широке коло наукових публікацій, які охоплюють напрямок дослідження проблеми боротьби і протидії фінансовим та кібершахрайствам, досить багато питань є мало вивченими і потребують уточнення, удосконалення та подальшого дослідження. Особливо це стосується можливості конвергенції системи кібербезпеки та протидії фінансовим шахрайствам й легалізації кримінальним доходам.

Метою статті є здійснення оцінки рівня потенційної конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів і фінансуванню тероризму на основі визначення їх інтегральних показників та застосування функції Харрінгтона – Менчера.

Виклад основного матеріалу. Для здійснення оцінки рівня конвергенції скористаємося підходом, запропонованим Яровенко Г.М. у роботі [17] для оцінювання рівня загрози інформаційної безпеки, суть якого полягає у визначенні інтегрального показника. Але для нашого дослідження необхідно розрахувати два композитних індикатори, один з яких характеризуватиме рівень кібербезпеки в країні, а інший – рівень протидії легалізації кримінальних доходів.

На першому етапі оберемо вхідні дані, які будуть використовуватися для здійснення розрахунків. Першу групу сформували світові індекси, що застосовуються для вимірювання окремих сфер кібербезпеки країни, узяті з офіційного сайту організації «e-Governance Academy Foundation» за 2018 рік: Глобальний індекс кібербезпеки (Global Cybersecurity Index) оцінює можливості країн світу протидіяти кіберзагрозам у світі, а також визначає їх слабкі сторони та потенційні можливості; Національний індекс кібербезпеки (National Cyber Security Index) визначає стан готовності окремої країни протидіяти кіберзагрозам та керувати кіберінцидентами; Індекс мережевої готовності (Networked Readiness Index) дозволяє оцінити рівень технологічної готовності країни для впровадження сучасних інформаційних систем та технологій для автоматизації різних процесів життєдіяльності суспільства; Рівень цифрового розвитку (Digital Development Level) показує ступінь цифровізації країни. Кожен з цих обраних показників характеризує стан кібербезпеки країни з огляду на різні її аспекти, тому їх аналіз у сукупності дозволить сформувати комплексне бачення на її розвиток та можливості інтеграції.

Другу групу індикаторів сформували індекси, які дозволяють оцінити стан системи протидії легалізації кримінальних доходів та фінансування тероризму. Сюди увійшли: Індекс політичної стабільності (Political Stability Index), який дозволяє оцінити ймовірність дестабілізації уряду країни із використанням неконституційних та насильницьких заходів, що є сприятливим або несприятливим в залежності від значення фактором для процесів легалізації незаконних коштів; Індекс ефективності уряду (Government Effectiveness Index), який вимірює його якість, що полягає у його незалежності від політичного тиску, ефективності роботи державних служб, рівня довіри до його діяльності; Легкість ведення бізнесу (Ease of Doing Business) характеризує умови для ведення бізнесу в країні, що впливає на ризики зростання тіньового сектору та відмивання коштів; Індекс злочинності (Crime Index) характеризує рівень злочинності в країні, який впливає на нестабільність соціальної, політичної та економічної сфер; Глобальний індекс тероризму (Global Terrorism Index) свідчить про рівень терористичної активності, що впливає на ризики легалізації кримінальних доходів та фінансування тероризму; Індекс фінансової таємниці (Financial Secrece Index) свідчить про ступінь захисту фінансових операцій, що багатьма країнами використовується для формування сприятливих умов для приховування незаконних доходів та здійснення фінансових операцій, джерела коштів яких є кримінальними. Дані обраних показників було узято з офіційного джерела Світового банку. Емпіричні дані обох груп відповідають 76 країнам світу за 2018 рік, оскільки саме цей період характеризується найбільш повним набором значень.

В роботі [18] авторами Кузьменко О.В., Яровенко Г.М., Радько В.В. проведено попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу, що дозволило довести релевантність саме цих показників для подальшого дослідження.

На другому етапі проведемо нормалізацію вхідних даних для їх приведення до співставного вигляду. Для цього використаємо нелінійну нормалізацію, яка згладжує різні за знаками та значеннями дані більш ефективно, ніж інші методи (формула (1)):

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \quad (1)$$

де Z_{ij}– нормалізоване значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни;

$\overline{y_j}$– середнє значення j-го показника в межах досліджуваного переліку країн;

y_{ij} – фактичне значення j-го показника в розрізі і-ої країни;

$\sigma(y_j)$ – середнє квадратичне відхилення j-го показника в межах досліджуваного переліку країн.

Всі обрані показники за своїм впливом на стан системи є стимуляторами, окрім двох – індексу злочинності та фінансової таємниці, які є дестимуляторами. Тому для того, щоб правильно врахувати їх значення при формуванні інтегрального індексу, необхідно їх розраховане нормалізоване значення відняти від одиниці.

На третьому етапі проведемо трансформацію нормалізованих значень обраних показників бази дослідження до безрозмірної шкали бажаності Харрінгтона за допомогою формули (2):

$$d_{ij} = \exp(-\exp(-Z_{ij})), \quad (2)$$

де d_{ij} - проміжне значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона;

Z_{ij} – нормалізоване значення j-го показника, в розрізі і-ої країни.

Для подальшої побудови інтегрального показника оцінки рівня конвергенції системи кібербезпеки та протидії фінансовим шахрайствам необхідно дослідити характер поведінки кривої перетворення Харрінгтона-Менчера, яка характеризує залежність d_{ij} від фактичних значень кожного вхідного показника. З цією метою проведемо візуалізацію залежностей на четвертому етапі. В результаті було виявлено, що для більшості показників є характерним перший тип кривої – S-подібна, зростаюча, симетрична. Індексу злочинності та фінансової таємниці відповідає четвертий тип – S-подібна, спадаюча, симетрична крива. Приклади отриманих графіків кривої першого та другого типів представлені на рисунках 1 та 2.

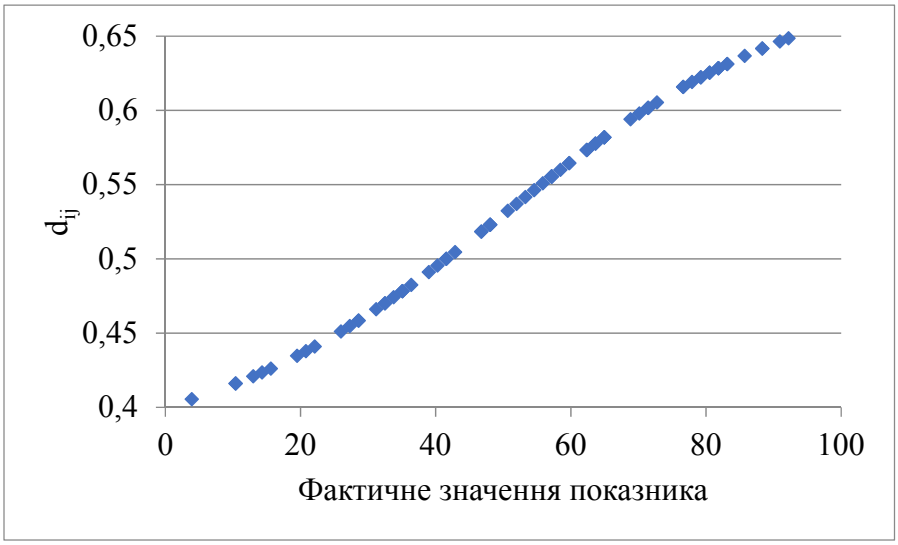

Рис. 1. Графік кривої першого типу для «Національного індексу кібербезпеки»

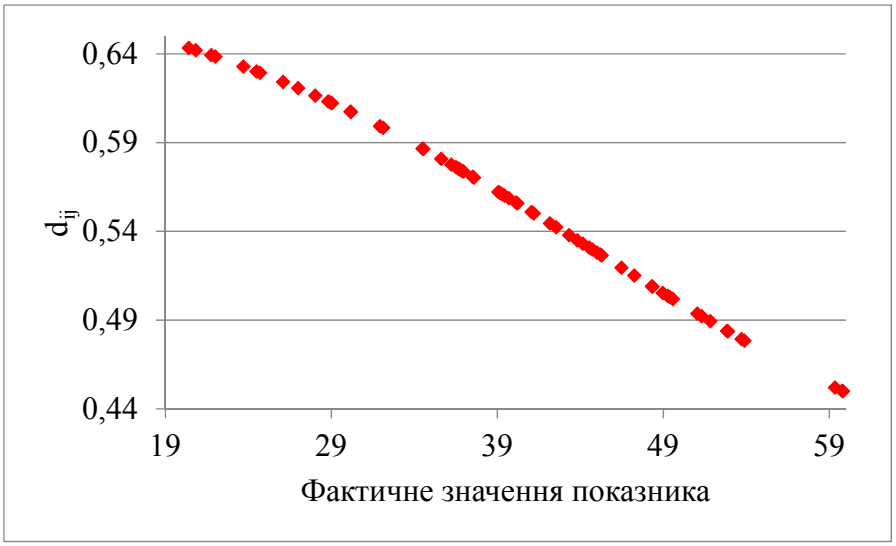

Рис. 2. Графік кривої четвертого типу для «Індексу злочинності»

На п'ятому етапі проведемо формалізацію перетворення Харрінгтона-Менчера в межах обраної на попередньому кроці залежності d_{ij} від фактичних значень в розрізі кожного вхідного показника. Тобто розрахуємо проміжні значення показників для оцінки рівня конвергенції системи кібербезпеки та протидії фінансовим шахрайствам з урахуванням їх приведення до безрозмірної шкали бажаності Харрінгтона-Менчера у відповідності із визначеним типом кривої.

Для показників, залежності для яких описуються кривою першого типу, використаємо формулу (3):

$$d_{ij}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{Z_{ij}-\min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right), \qquad (3)$$

де d_{ij}^{*} - проміжне значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера;

$\min\limits_{i} Z_{ij}$ – мінімальне значення нормалізованого j-го показника в розрізі і-ої країни;

$\max\limits_{i} Z_{ij}$ – максимальне значення нормалізованого j-го показника в розрізі і-ої країни.

Для показників, залежності для яких описуються кривою четвертого типу, використаємо формулу (4):

$$d_{ij}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_{i} Z_{ij}-Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right). \qquad (4)$$

На шостому етапі необхідно визначити ваги показників для того, щоб розрахувати узагальнену функцію. З цією метою проведемо канонічний аналіз, який дозволить визначити ступінь залежності між двома множинами показників, а також розрахувати їх канонічні ваги, які буде використано для інтегральної оцінки. Аналіз виконано із використанням модуля канонічного аналізу аналітичного пакету "STATISTICA", результати якого представлені на рисунку 3.

Canonical Analysis Summary (Konvergentcia2.sta)
Canonical R: .93762
Chi²(24)=200.41 p=0.0000

N=76		Left Set	Right Set
No. of variables		4	6
Variance extracted		100.000%	83.8201%
Total redundancy		70.3694%	47.9580%
Variables:	1	Global Cybersecurity Index	Political stability index
	2	Networked Readiness Index	Government effectiveness index
	3	National Cyber Security Index	Ease of doing business
	4	Digital Development Level	Crime Index
	5		Global Terrorism Index
	6		Financial Secrece Index

Рис. 3. Підсумки канонічного аналізу

З рисунку 3 можна побачити, що значення канонічної кореляції R = 0,93762, що свідчить про наявність дуже сильного кореляційного зв'язку між множиною факторів, які характеризують рівень розвитку системи кібербезпеки та протидії фінансовим шахрайствам [19]. Статистичну значимість коефіцієнта кореляції підтверджує високе значення критерію Пірсона (χ^2 = 200,00), рівень значущості якого не перевищує 0,05 (p = 0,0000). Значення надмірності для лівої множини, яку сформували індекси кібербезпеки, дорівнює 70,3694%. Це свідчить про те, що фактори правої множини, які відповідають показникам рівня протидії фінансовим шахрайствам країни, на 70,3694% пояснюють мінливість індикаторів кібербезпеки, що свідчить про високе значення впливу. Розвиток системи протидії процесам відмивання коштів в країні в певній мірі залежить від стану її кібербезпеки, оскільки фактори кібербезпеки на 47,9580% пояснюють мінливість факторів, які характеризують рівень протидії фінансовим шахрайствам. Хоча отримане значення є помірним, але воно є достатнім для обґрунтування впливу таких показників, як кібербезпека, на економічні процеси в країні.

Визначені значення канонічних коренів, а також отримані статистичні характеристики, дозволили зробити висновок, що значущими є 3 канонічні корені. Але для того, щоб одержати достовірні оцінки їх навантажень для трьох пар канонічних змінних, необхідно мати вибірку, яка буде перевищувати в 40-60 раз кількість початкових даних [20, с. 190]. Тому прийнято рішення, що для визначення вагів доцільно використати значення тільки першого канонічного кореня, для якого канонічний R^2

буде мати найбільше значення 0,8791. Виходячи з даних міркувань для подальшого розгляду використаємо канонічні ваги, визначені для першого кореня (рисунки 4-5).

Variable	Canonical Weights, left set (Konvergentcia2.sta)			
	Root 1	Root 2	Root 3	**Root 4**
Global Cybersecurity Index	0,313261	-0,781709	0,63400	1,14199
Networked Readiness Index	0,264381	-0,713150	-1,56282	-0,64848
National Cyber Security Index	-0,021339	0,026080	0,91519	-1,29626
Digital Development Level	0,557799	1,355225	0,21392	0,67528

Рис. 4. Канонічні ваги для показників кібербезпеки

Variable	Canonical Weights, right set (Konvergentcia2.sta)			
	Root 1	Root 2	Root 3	Root 4
Political stability index	-0,269140	0,923250	1,32088	0,990101
Government effectiveness index	0,780788	0,200480	-1,68893	0,203985
Ease of doing business	0,341713	-0,672184	0,64477	-0,816572
Crime Index	0,050110	0,111717	0,73583	-0,231753
Global Terrorism Index	0,009265	-0,080100	1,17396	1,219424
Financial Secrece Index	-0,091481	0,070369	0,35190	-0,048788

Рис. 5.– Канонічні ваги для показників, що характеризують рівень протидії легалізації кримінальних доходів

Виявилося, що отримані канонічні ваги є як додатними, так і від'ємними, що свідчить про позитивний та негативний внесок показників у значення кореня. Але для визначення узагальненої функції необхідно, щоб їх значення варіювалися від 0 до 1, тому відповідні від'ємні ваги будуть узяті по їх модулю.

На сьомому етапі обчислюються два інтегральні індекси для оцінювання рівня розвитку системи кібербезпеки та протидії легалізації кримінальних доходів. Для цього необхідно використати формули (5)-(6):

$$IC_i = \sqrt[\sum_{j=1}^{n} a_j]{\prod_{j=1}^{n} \left(d_{ij}^*\right)^{a_j}}, \qquad (5)$$

$$IP_i = \sqrt[\sum_{j=1}^{m} a_j]{\prod_{j=1}^{m} \left(d_{ij}^*\right)^{a_j}}, \qquad (6)$$

де IC_i – інтегральний індекс, що характеризує рівень розвитку системи кібербезпеки для і-тої країни;

IP_i – інтегральний індекс, що характеризує рівень розвитку системи протидії легалізації кримінальних доходів для і-тої країни;

n – кількість показників кібербезпеки країни (n = 4);

m – кількість показників, що характеризують рівень розвитку системи протидії легалізації кримінальних доходів (m = 6);

a_j – ваги відповідного j-го вхідного показника кібербезпеки або протидії легалізації кримінальних доходів;

d_{ij}^* - проміжне значення j-го показника кібербезпеки або протидії легалізації кримінальних доходів в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера.

Розраховані значення інтегральних показників інтерпретуємо із використанням якісної оцінки, а саме: якщо отримане значення знаходиться в межах 0,80 – 1,00, то стан розвитку країни відповідає оцінці «дуже добре»; від 0,63 до 0,80 – «добре»; від 0,37 до 0,63 – «задовільно»; від 0,20 до 0,37 – «погано»; від 0,00 до 0,20 – «дуже погано».

Візуалізуємо отримані значення із використанням діаграм з картами, які можна побудувати за допомогою програмного продукту MS Excel. Результати представлено на рисунках 6-7.

За інтегральним рівнем кібербезпеки виявилося, що оцінку «дуже добре» мають 38 країн, таких як: Австрія, Австралія, Канада, Данія, Естонія, Фінляндія, Німеччина, Великобританія, США та інші (див. рис. 6), тобто переважна більшість цих країн є розвиненими. Болгарія, Греція, Маврикій, Чорногорія, Північна Македонія, Туреччина та Румунія мають рівень кібербезпеки, який відповідає оцінці «добре». Задовільний рівень характерний для таких країн, як Україна, Бразилія, Чилі, Китай, Ісландія, Мальта та Тайланд. Оцінку

«погано» та «дуже погано» отримали 24 країни: Барбадос, Болівія, Ботсвана, Домініканська республіка, Гана, Гватемала, Індія, Індонезія, Кенія, Ліберія та інші країни, що розвиваються або є найменш розвиненими.

В цілому, рівень кібербезпеки відповідає рівню економічного розвитку країни. Ті, що є розвиненими, відповідно, мають потужні можливості для створення умов кіберзахисту різних об'єктів. Країни, що розвиваються та є найменш розвиненими, мають проблеми в сфері кібербезпеки, викликані відсутністю висококваліфікованих фахівців в цій галузі, недостатнім рівнем інвестування, слабким рівнем правового забезпечення цієї сфери, тощо.

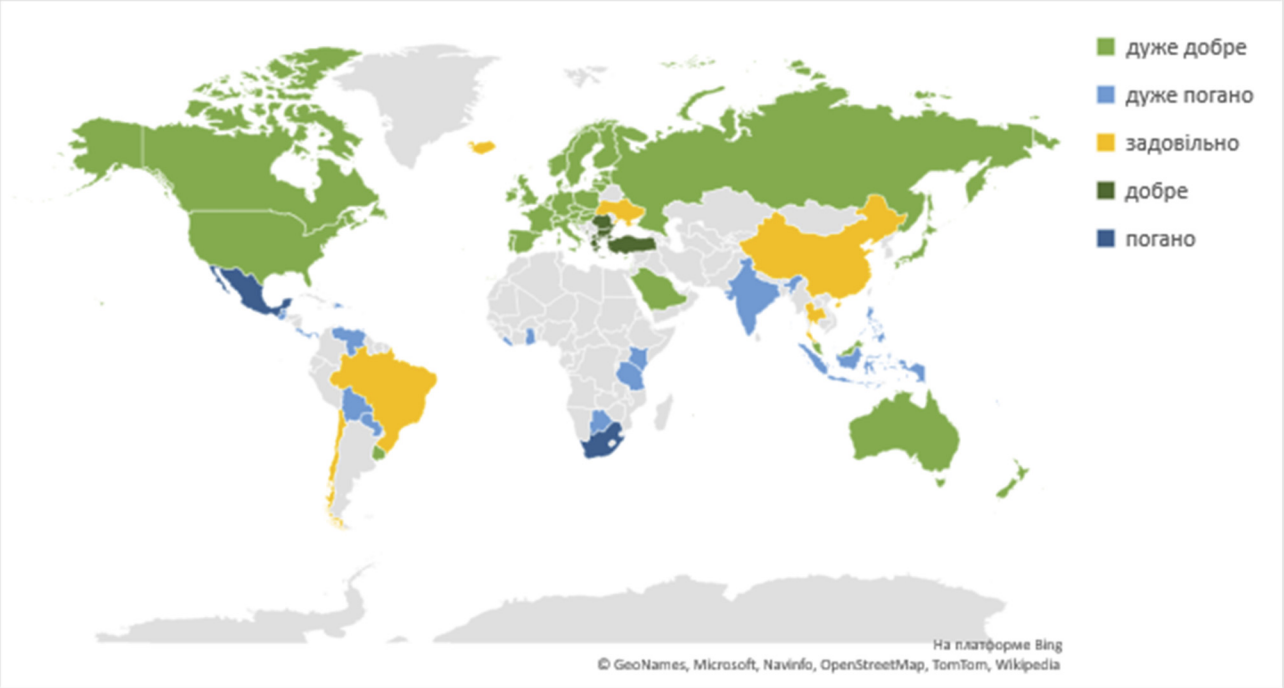

Рис. 6. Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку їх системи кібербезпеки

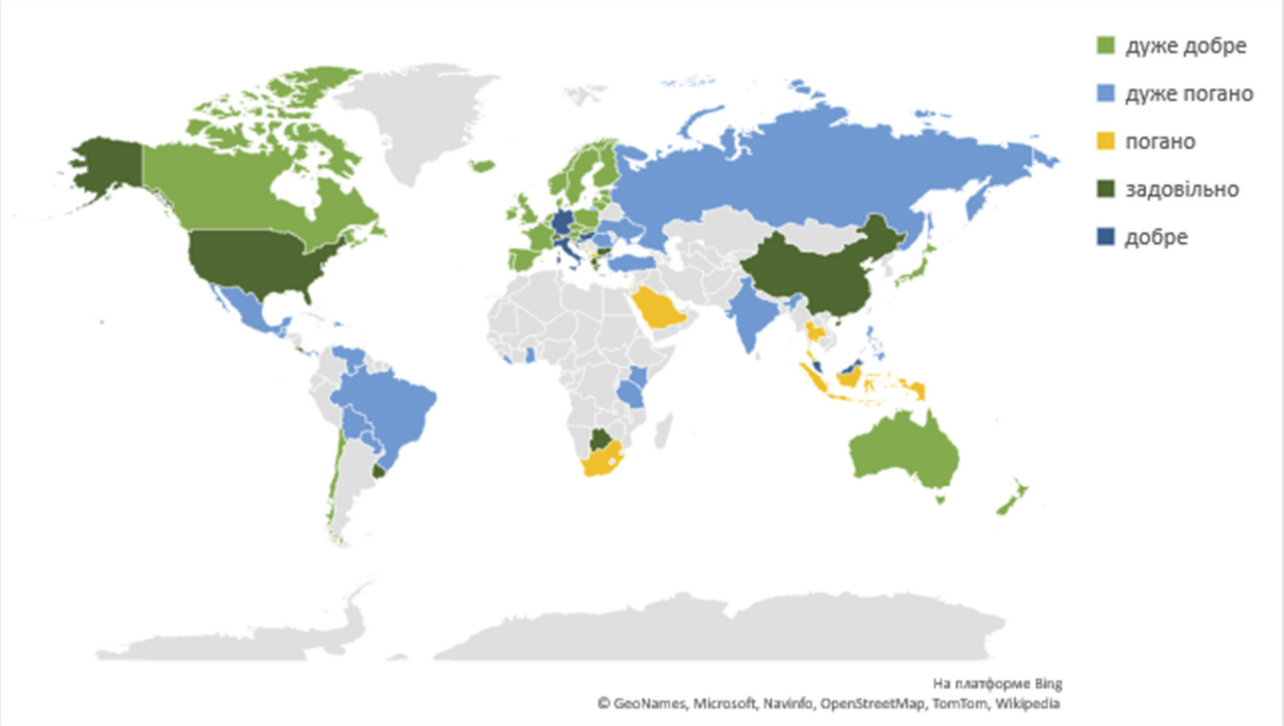

Рис. 7. Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку системи протидії легалізації кримінальних доходів

За інтегральним рівнем протидії фінансовим шахрайствам оцінку «дуже добре» отримали 28 країн (див. рис. 7): Австралія, Австрія, Бельгія, Канада, Ірландія, Нідерланди, Норвегія, Великобританія, Швеція, Чехія, та інші. Такі країни, як Хорватія, Німеччина, Угорщина, Італія, Малайзія, Мальта та Сингапур, мають рівень протидії легалізації кримінальних доходів на рівні «добре». Оцінку «задовільно» отримали Ботсвана, Болгарія, Китай, Коста Ріка, Греція, Люксембург, Сейшельські острови, Швейцарія, США та Уругвай. 9 країн отримали рівень «погано», а 22 країни – «дуже погано». До них відносяться: Болівія, Бразилія, Індія, Україна, Російська Федерація, Мексика, Південна Африка, Таїланд, Індонезія та інші. Тобто, ряд країн, які мають високий рівень злочинності та тероризму, озброєні конфлікти, низький економічний розвиток є досить привабливими для легалізації кримінальних доходів та фінансування тероризму. Тому система протидії таким операціям є досить слабкою й не розвиненою. Також країни, які мають високий рівень фінансової таємниці створюють сприятливі умови для відмивання коштів, отриманих злочинним шляхом. На сьогодні такими є Швейцарія, Люксембург та США.

Для визначення рівня конвергенції систем кібербезпеки та протидії фінансовим шахрайствам знайдемо середньоарифметичне значення двох інтегральних індексів. Результати розрахунків представимо у вигляді карти розподілу країн за рівнем конвергенції систем кібербезпеки та протидії фінансовим шахрайствам (див. рис. 8).

За умови конвергенції системи кібербезпеки та протидії фінансовим шахрайствам для тих країн, які мають низький рівень протидії, відбудеться посилення їх потенційних можливостей за рахунок системи кіберзахисту. Так, порівнюючи результати, представлені на рисунках 6-8, можна побачити, що такі країни, як Бахрейн, Ботсвана, Бразилія, Бруней, Болгарія, Чилі, Коста Рика, Ісландія, Ізраїль, Люксембург, Мальта, Чорногорія, Північна Македонія, Румунія, Російська Федерація, Саудівська Аравія, Сейшельські острови, Сінгапур, Швейцарія, Таїланд, Туреччина, Україна, США та Уругвай, матимуть позитивний ефект від процесу конвергенції.

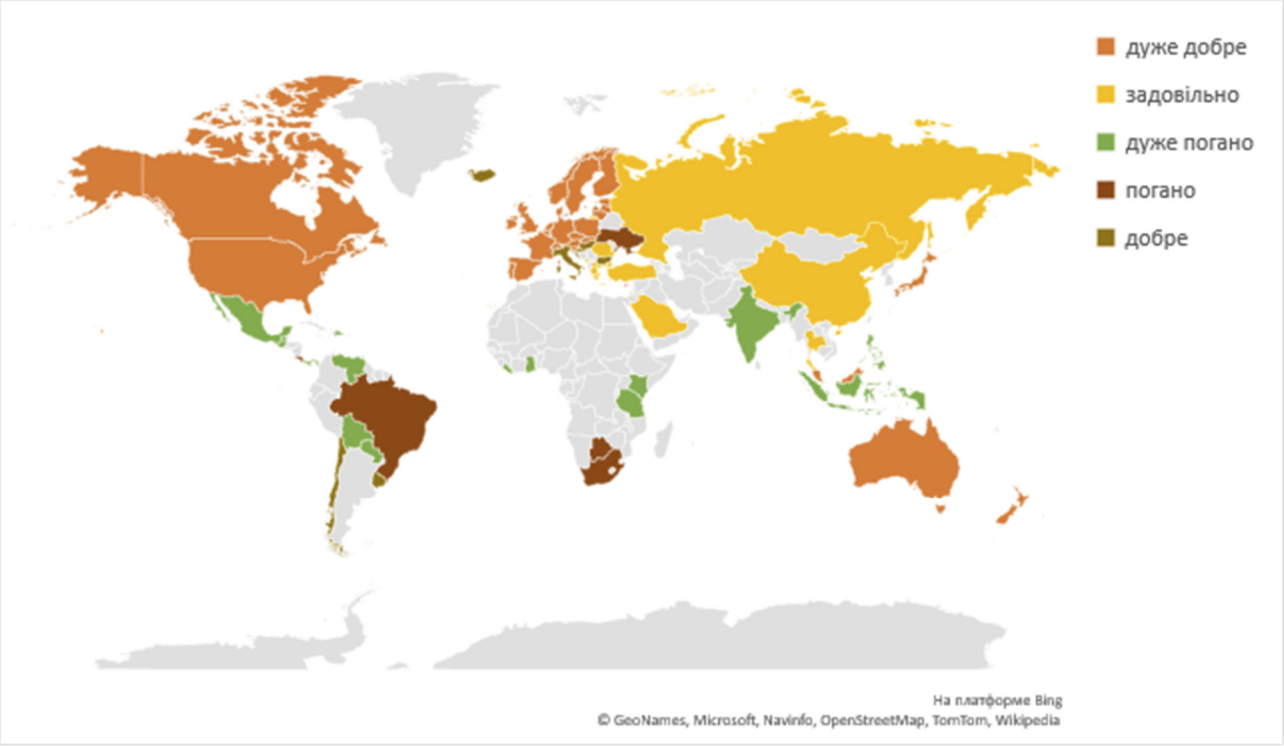

Рис. 8. Карта розподілу країн за рівнем конвергенції систем кібербезпеки та протидії легалізації кримінальних доходів

Висновки. Сучасні тенденції зростання обсягів кібершахрайств та легалізації кримінальних доходів вимагають застосування нових методів і технологій в процесі боротьби з даним явищем. Це можливо тільки за рахунок системної взаємодії програмних, технічних, інформаційних, організаційних, правових та технологічних заходів, тобто конвергенції системи кібербезпеки та протидії фінансовим шахрайствам. Цей процес є доволі складним, тому потребує зваженого підходу до його здійснення. Тому здійснення попередньої оцінки рівня потенційної конвергенції цих двох систем є необхідним заходом на шляху удосконалення та підвищення ефективності боротьби із шахрайствами на світовому рівні.

В статті розглянуто індикатори, які характеризують рівень розвитку кібербезпеки

країни та протидії легалізації кримінальних доходів і фінансування тероризму. Використаний підхід Харрінгтона – Менчера дозволив сформувати два інтегральні показники. Оцінювання рівня кібербезпеки дозволило виявити, що розвинені країни мають високий рівень кіберзахисту. Найнижчі оцінки отримали країни, що є найменш розвиненими або розвиваються та мають низький рівень розвитку. За інтегральним оцінюванням рівня протидії легалізації кримінальних доходів встановлено, що суттєві проблеми в цій сфері мають країни із високим рівнем злочинності, тероризму, низькою якістю державного управління, а також ті, де здійснюються озброєні конфлікти та є високий рівень фінансової секретності. Це сприяє можливостям відмивання кримінальних доходів та знижує спроможності системи протидіяти таким операціям.

Визначений загальний рівень конвергенції системи кібербезпеки та протидії відмиванню кримінальних доходів дозволив зробити висновок, що цей процес матиме позитивний ефект для 32% країн з досліджуваного набору. Тобто можна говорити про те, що інтеграційні процеси є сприятливими для посилення можливостей країн у боротьбі з фінансовими та кібершахрайствами. В подальшому, планується оцінити потенційний ефект від здійснення даних процесів для визначених груп країн.

Фінансування: Робота виконана в рамках держбюджетних науково-дослідних робіт: № 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».

ASSESSMENT OF THE CONVERGENCE LEVEL OF THE CYBER SECURITY SYSTEM AND COUNTERACTION OF MONEY LAUNDERING

Hanna Yarovenko, Doctor of Science, Associate Professor, Economic Cybernetics Department, Sumy State University, street Rimsky-Korsakov, 2, Sumy, Ukraine, e-mail: h.yarovenko@biem.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8760-683

Olena Kolotilina, Assistant, Economic Cybernetics Department, Sumy State University, street Rimsky-Korsakov, 2, Sumy, Ukraine, e-mail: o.kolotilina@biem.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8928-0859

Alona Svitlychna, Student, Economic Cybernetics Department, Sumy State University, street Rimsky-Korsakov, 2, Sumy, Ukraine, e-mail: aliona.svitlychna@student.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8981-7986

The growth of financial and cyber fraud leads to the destabilization of the country's financial sector and negatively affects the development of their economy, which requires the development and implementation of effective tools and measures at the level of public administration. The convergence of the cybersecurity system and counteraction of money laundering and terrorist financing is a promising area in the fight against financial fraud. The subject of research in the article is a scientific and methodological approach to forming integrated indicators for assessing the state of various systems, which is based on the Harrington - Mencher function. The aim is to determine the level of potential convergence of the cybersecurity system and counteraction of money laundering and terrorist financing based on the definition of their integrated indicators and the application of the Harrington-Mencher function. Objectives: to form a base of factors for evaluation; to carry out their normalization by applying nonlinear normalization; to transform the normalized values of the selected indicators of the research base to the dimensionless scale of Harrington's desirability; identify the function type of the dependence of the intermediate indicator value to assess the level of convergence of the cybersecurity system and combating financial fraud, from their actual values; calculate indicators to formalize the Harrington-Mencher transformation; to determine weight indicators using canonical analysis; to calculate integrated indicators that characterize the level of development of the cybersecurity system and counteraction to money laundering, as well as to determine the level of systems convergence. The article uses general scientific methods: system analysis - to determine the factors that characterize cybersecurity systems and combat financial fraud; Harrington-Mencher method of preference and function during integrated evaluation. The following results were obtained: in terms of cybersecurity, the highest scores are given to economically developed countries - European countries, the United States, Canada, Australia, New Zealand, Japan. Other countries have many problems in this area, as evidenced by their assessments of "very poor", "poor" and "satisfactory". The level of opposition to money laundering has shown that this area is critical for countries with high levels of crime, terrorism, military conflicts and high levels of financial secrecy, making them potential actors in money laundering. It is also established that due to the convergence of the two systems, the country's level of development will increase. Conclusions: the results of the study should be taken into account in the process of developing a strategy for the convergence of the cybersecurity system and combating financial fraud at the macro level.

Key words: convergence, cybersecurity, financial fraud, money laundering, Harrington - Mencher function.

ОЦЕНКА УРОВНЯ КОНВЕРГЕНЦИИ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ КРИМИНАЛЬНЫХ ДОХОДОВ

Яровенко Анна Николаевна, докт. экон. наук, доцент, кафедра экономической кибернетики, Сумский государственный университет, ул. Римского-Корсакова, 2, Сумы, Украина, e-mail: h.yarovenko@biem.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8760-683
Колотилина Елена Васильевна, ассистент, кафедра экономической кибернетики, Сумский государственный университет, ул. Римского-Корсакова, 2, Сумы, Украина, e-mail: o.kolotilina@biem.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8928-0859
Светличная Алена Алексеевна, студент, кафедра экономической кибернетики, Сумский государственный университет, ул. Римского-Корсакова, 2, Сумы, Украина, e-mail: aliona.svitlychna@student.sumdu.edu.ua, ORCID: https://orcid.org/0000-0002-8981-7986

Рост объемов финансовых и кибермошенничеств приводит к дестабилизации финансового сектора страны и негативно влияет на развитие их экономики, что требует разработки и внедрения действенных инструментов и мер на уровне государственного управления. Конвергенция системы кибербезопасности и противодействия легализации криминальных доходов и финансирования терроризма является перспективным направлением в борьбе с финансовыми мошенничествами. Предметом исследования в статье является научно-методический подход к формированию интегральных показателей оценки состояний разных систем, основанный на функции Харрингтона – Менчера. Цель состоит в проведении оценки уровня потенциальной конвергенции системы кибербезопасности и противодействия легализации криминальных доходов и финансированию терроризма на основе определения их интегральных показателей и применения функции Харрингтона – Менчера. Задание: сформировать базу факторов для осуществления оценки; выполнить их нормализацию методом внедрения нелинейной нормализации; трансформировать нормализованные значения выбранных показателей базы исследования в безразмерную шкалу желательности Харрингтона; идентифицировать вид функции зависимости промежуточного значения показателя, выбранного для осуществления оценки уровня конвергенции системы кибербезопасности и противодействия финансовым мошенничествам, от их фактических значений; рассчитать показатели для формализации преобразования Харрингтона-Менчера; с помощью канонического анализа определить весовые показатели; рассчитать интегральные показатели, характеризующие уровень развития системы кибербезопасности и противодействия легализации криминальных доходов, а также определить уровень конвергенции систем. В статье используются общенаучные методы: системный анализ – для определения факторов, которые характеризуют систему кибербезопасности и противодействия финансовым мошенничествам; метод преимуществ и функция Харрингтона – Менчера – при интегральной оценке. Получены следующие результаты: по уровню кибербезопасности наиболее высокие оценки имеют экономически развитые страны – страны Европы, США, Канада, Австралия, Новая Зеландия, Япония. Другие страны имеют ряд проблем в этой сфере, о чем свидетельствуют полученные ими оценки «очень плохо», «плохо» и «удовлетворительно». По уровню противодействия легализации незаконных доходов оказалось, что эта сфера является критической для стран с высоким уровнем преступности, терроризма, военными конфликтами и высоким уровнем финансовой тайны, что делает их потенциальными субъектами процессов отмывания незаконных средств. Также установлено, что за счет конвергенции двух систем уровень развития страны повысится. Выводы: полученные результаты исследования следует учесть в процессе разработки стратегии конвергенции системы кибербезопасности и противодействия финансовым мошенничествам на макроуровне.

Ключевые слова: конвергенция, кибербезопасность, финансовые мошенничества, легализация криминальных доходов, функция Харрингтона – Менчера.

Література

1. Відмивання грошей. *Anti-corruption walks Kyiv* : веб-сайт. URL: https://acwalks.com.ua/knowledgebase/vidmyvannia-hroshey/ (дата звернення: 01.12.2021).

2. Morgan S. *Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/ (дата звернення: 01.12.2021).

3. Dileep M.R., Navaneeth A.V., Abhishek M. A novel approach for credit card fraud detection using decision tree and random forest algorithms. In *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021.* 2021. P. 1025–10284. DOI: https://doi.org/10.1109/ICICV50876.2021.9388431.

4. Wang R., Liu G. Ensemble Method for Credit Card Fraud Detection. In *Proceedings - 2021 4th International Conference on Intelligent Autonomous Systems, ICoIAS 2021*. 2021. P. 246–252. DOI: https://doi.org/10.1109/ICoIAS53694.2021.00051.

5. Mishra S.P., Kumari P. Analysis of techniques for credit card fraud detection: A data mining perspective. *Advances in Intelligent Systems and Computing*. 2020, №1030. P. 89–98. DOI: https://doi.org/10.1007/978-981-13-9330-3_9.

6. Mekterović I., Karan M., Pintar D., Brkić L. Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences (Switzerland)*. 2021, №11(151). Article number 6766. DOI: https://doi.org/10.3390/app11156766.

7. Chen Z., Van Khoa L.D., Teoh E.N., Nazir A., Karuppiah E.K., Lam K.S. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*. 2018, №57(2). P. 245–285. DOI: https://doi.org/10.1007/s10115-017-1144-z.

8. Zhou Y., Song X., Zhou M. Supply Chain Fraud Prediction Based on XGBoost Method. In *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2021*. 2021. P. 539–542. DOI: https://doi.org/10.1109/ICBAIE52039.2021.9389949.

9. Gao S., Xu D., Wang H., Green, P. Knowledge-based anti-money laundering: a software agent bank application. *Journal of Knowledge Management.* 2009, №13(2). P. 63-75. DOI: https://doi.org/10.1108/13673270910942709.

10. 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.

11. 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.

12. Babenko, V. Gas supply security model to EU consumers. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, 2020, № 12, 78-87. DOI: https://doi.org/10.26565/2310-9513-2020-12-07

13. Shumilo, O., Babenko, V., Liubokhynets, L., Volovelska, I., Arefieva, O. Method of Enterprise Economic Security Evaluation. *Estudios de Economía Aplicada*, 2021, 39 (7). DOI: https://doi.org/10.25115/eea.v39i7.4998

14. Dionysios S. Demetis. *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach*. Edward Elgar Publishing, Incorporated, 2010. P. 188.

15. Starychenko, Ye., Skrypnyk, A., Babenko, V., Klymenko, N., Tuzhyk, K. Food Security Indices in Ukraine: Forecast Methods and Trends. *Estudios de Economía Aplicada*, 2021, Vol. 38-3(1), pp. 1-8. DOI: http://dx.doi.org/10.25115/eea.v38i4.4000

16. 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.

17. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Managemen.* 2020, № 18(3), P. 195–210. DOI: https://doi.org/10.21511/ppm.18(3).2020.17.

18. Кузьменко О.В., Яровенко Г.М., Радько В.В. Попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу країн. *Економіка та суспільство*. 2021, № 32. DOI: https://doi.org/10.32782/2524-0072/2021-32-37.

19. Gontareva, I., Babenko, V., Kuchmacz, B., Arefiev, S. Valuation of Information Resources in the Analysis of Cybersecurity Entrepreneurship. *Estudios de Economía Aplicada*, 2021, Vol. 38-3(1), pp. 1-11. DOI: http://dx.doi.org/10.25115/eea.v38i4.3984

20. Халафян А.А. *STATISTICA 6. Статистический анализ данных*. М. : ООО «Бином-Пресс», 2007. 512 с.

References

1. Vidmyvannia hroshei [Money laundering]. *Anti-corruption walks Kyiv.* Available at: https://acwalks.com.ua/knowledgebase/vidmyvannia-hroshey/ (accessed 01 December 2021).

2. Morgan S. (2019). *Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. Available at: https://cybersecurityventures.com/cybersecurity-almanac-2019/ (accessed 01 December 2021).

3. Dileep M.R., Navaneeth A.V., Abhishek M. (2021). A novel approach for credit card fraud detection using decision tree and random forest algorithms. In *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021.* P. 1025–10284. https://doi.org/10.1109/ICICV50876.2021.9388431.

4. Wang R., Liu G. (2021). Ensemble Method for Credit Card Fraud Detection. In *Proceedings - 2021 4th International Conference on Intelligent Autonomous Systems, ICoIAS 2021*. P. 246–252. https://doi.org/10.1109/ICoIAS53694.2021.00051.

5. Mishra S.P., Kumari P. (2020). Analysis of techniques for credit card fraud detection: A data mining perspective. *Advances in Intelligent Systems and Computing*, 1030, pp. 89–98. https://doi.org/10.1007/978-981-13-9330-3_9.

6. Mekterović I., Karan M., Pintar D., Brkić L. (2021). Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences (Switzerland)*, 11(151), article number 6766. https://doi.org/10.3390/app11156766.

7. Chen Z., Van Khoa L.D., Teoh E.N., Nazir A., Karuppiah E.K., Lam K.S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, 57(2), pp. 245–285. https://doi.org/10.1007/s10115-017-1144-z.

8. Zhou Y., Song X., Zhou M. (2021). Supply Chain Fraud Prediction Based on XGBoost Method. In *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2021*. P. 539–542. https://doi.org/10.1109/ICBAIE52039.2021.9389949.

9. Gao S., Xu D., Wang H., Green, P. (2009). Knowledge-based anti-money laundering: a software agent bank application. *Journal of Knowledge Management,* 13(2), pp. 63-75. https://doi.org/10.1108/13673270910942709.

10. 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. https://doi.org/10.1007/978-3-030-56433-9_1.

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

12. Babenko, V. (2020). Gas supply security model to EU consumers. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, 12, 78-87. https://doi.org/10.26565/2310-9513-2020-12-07

13. Shumilo, O., Babenko, V., Liubokhynets, L., Volovelska, I., Arefieva, O. (2021). Method of Enterprise Economic Security Evaluation. *Estudios de Economía Aplicada*, 39 (7). https://doi.org/10.25115/eea.v39i7.4998

14. Dionysios S. Demetis. (2010). *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach.* Edward Elgar Publishing, Incorporated. P. 188.

15. Starychenko, Ye., Skrypnyk, A., Babenko, V., Klymenko, N., Tuzhyk, K. (2021). Food Security Indices in Ukraine: Forecast Methods and Trends. *Estudios de Economía Aplicada*, Vol. 38-3(1), pp. 1-8. http://dx.doi.org/10.25115/eea.v38i4.4000

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

17. Yarovenko H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management,* 18(3), pp. 195–210. https://doi.org/10.21511/ppm.18(3).2020.17.

18. Kuzmenko O.V., Yarovenko H.M., Radko V.V. (2021). Poperednii analiz protsesu konverhentsii system kiberbezpeky ta finansovoho monitorynhu krain [Preliminary analysis of the convergence process of cyber security systems and financial monitoring of countries]. *Economy and society*, 32. https://doi.org/10.32782/2524-0072/2021-32-37 (in Ukrainian).

19. Gontareva, I., Babenko, V., Kuchmacz, B., Arefiev, S. (2021). Valuation of Information Resources in the Analysis of Cybersecurity Entrepreneurship. *Estudios de Economía Aplicada*, Vol. 38-3(1), pp. 1-11. http://dx.doi.org/10.25115/eea.v38i4.3984

20. Halafyan A.A. (2007) *STATISTICA 6. Statisticheskiy analiz dannyih* [STATISTICA 6. Statistical data analysis]. M. : LLC «Binom-Press» (in Russian).

Стаття надійшла до редакції 18 жовтня 2021 р.
Стаття рекомендована до друку 19 листопада 2021 р.