ЦИФРОВІ ІНСТРУМЕНТИ В БОРОТЬБІ З ВІДМИВАННЯМ КОШТІВ ТА ФІНАНСУВАННЯМ МІЖНАРОДНОГО ТЕРОРИЗМУ: МОЖЛИВОСТІ ТА ЗАГРОЗИ

DIGITAL TOOLS IN COMBATING MONEY LAUNDERING AND THE FINANCING OF INTERNATIONAL TERRORISM: OPPORTUNITIES AND THREATS

В статті систематизовано підходи науковців до встановлення взаємозв'язку між рівнем цифрового розвитку країни та ризиком легалізації кримінальних коштів. На основі критичного аналізу наукових праць підтверджено даний зв'язок та вказано на проблемності використання рейтингових індексів цифровізації для кількісної оцінки даного зв'язку. Неоднозначність висновків та складність реальної оцінки пов'язана з різними позиціями країн для різних показників. Систематизовано переваги, які створюють цифрові технології в сфері боротьбі з відмиванням коштів та фінансуванням тероризму, в розрізі компонент KYC та TM, що використовуються більшістю банків для оцінки, аналізу та вимірювання ризику фінансових злочинів. Узагальнено ситуації, які сигналізують про потенційну підозрілу діяльність та потребують додаткової уваги з боку банків. На прикладі криптовалюти здійснено оцінку характерних рис цифрових технологій щодо можливості їх використання для відмивання коштів та фінансування тероризму.

Ключові слова: *фінансування тероризму, відмивання коштів, цифрові технології, цифровізація, Базельський індекс AML.*

At the current stage, the consequences of the use of digital technologies cannot be fully predicted. Their role in combating money laundering and terrorist financing is defined in two ways: 1) facilitate the transfer and accumulation of illegally obtained funds in offshore accounts; 2) act as a source of empowerment, can be used in investigations, detection and termination of illegal money transfers. The purpose of the article is a critical analysis of approaches to assessing the relationship between the level of risk of money laundering and terrorist financing and the implementation of digital technologies in countries, as well as the identification of opportunities and threats from their application in the researched field. To achieve the goal, the following methods were used: analysis and synthesis, logical generalization, comparison. The article systematizes the approaches of scientists to establishing the relationship between the level of digital development of the country and the risk of legalization of criminal funds. Based on a critical analysis of scientific works, this connection was confirmed, taking into account the value of the Basel AML Index. The problems of using rating indices of digitization for the quantitative assessment of this connection are identified. The ambiguity of the conclusions and the complexity of the real assessment are related to the different positions of the countries for different indicators. The benefits created by digital technologies in the field of combating money laundering and terrorist financing are systematized, in terms of KYC and TM components. They are used by most banks to assess, analyze and measure the risk of financial crimes. Situations that signal potential suspicious activity and require additional attention from banks are summarized. On the example of cryptocurrency, an assessment of the characteristic features of digital technologies (the underlying blockchain technology; anonymity; regulation and taxation of transactions with cryptocurrency) was carried out regarding the possibility of their use for money laundering and terrorist financing.

Key words: *terrorist financing, money laundering, digital technologies, digitalization, Basel AML index.*

УДК 339.7:336.74:004.8

DOI: https://doi.org/10.32782/bses.80-3

Грабчук І.Л.[1]
к.е.н., доцент,
доцент кафедри інформаційних систем в управлінні та обліку,
Державний університет «Житомирська політехніка»
Березний О.В.
здобувач ступеня доктор філософії,
Державний університет «Житомирська політехніка»

Hrabchuk Iryna
Zhytomyr Polytechnic State University
Bereznyi Oleksandr
Zhytomyr Polytechnic State University

Постановка пробелеми. Цифрові технології, які супроводжують сучасний бізнес, та цифрова економіка в цілому сприяють переказу та накопиченню на офшорних рахунках коштів, отриманих незаконним шляхом. Крім того, модернізуються способи відмивання коштів, адже збільшується кількість можливостей їх приховування. Так, можливим є переказування грошових коштів без участі банку з використанням, наприклад, платіжних сервісів Paypal або Venmo.

В той же час цифрові технології можна розглядати і як інструмент для вирішення проблеми відмивання доходів, одержаних злочинним шляхом, та фінансування тероризму. Вони можуть виступати джерелом розширення можливостей і прозорості, і можуть використовуватися в розслідуваннях, виявленні та припиненні незаконних грошових переказів. На даному етапі активного розвитку цифрових процесів важливим є проведення досліджень в напрямі виявлення потенційних загроз та ризиків, які можуть продукуватися цифровими інструментами. Це дозволить оперативно виявляти використання та зловживання ними для забезпечення ефективної протидії відмиванню коштів та фінансуванню тероризму.

Аналіз основних досліджень і публікацій. Питання цифровізації протягом останніх років є досить актуальними та піднімаються в значній кількості праць. Вплив цифрових інструментів на різні сфери економіки та на діяльність суб'єктів господарювання різних організаційно-правових форм досліджували Вишневський В., Камишанський В., Пантєлєєва Н., Лакутін Д., Сорока Б., Шевченко О., Рудич Л.

Окремі аспекти взаємозв'язку між рівнем цифровізації країни та рівнем ризику відмивання коштів та фінансування тероризму розкривали такі вітчизняні та зарубіжні дослідники, як Барченко Н.,

[1] ORCID: https://orcid.org/0000-0003-3664-7765

Любчак В., Лаврик Т., Койбічук В., Куровська Ю., Мордань Є., Бухтіарова А., Кравченко Я., Піжук О., Бодеску К.Н., Ачімб М.В., Даніела Рус А.І. Проте наведені питання потребують комплексного дослідження для визначення специфіка застосування цифрових інструментів в сфері боротьби з відмиванням коштів та фінансуванням тероризму, що в наукових працях майже не здійснювалося.

Постановка завдання. Метою статті є критичний аналіз підходів до оцінки взаємозв'язку між рівнем ризику відмивання коштів та фінансування тероризму та впровадження цифрових технологій в країнах, а також визначення можливостей та загроз від їх застосування в досліджуваній сфері.

Виклад основного матеріалу дослідження. Встановлення взаємозв'язку між рівнем цифрового розвитку країни та ризиком легалізації кримінальних коштів (на основі Базельського індексу AML) все частіше стає об'єктом дослідження в наукових працях. Базельський індекс AML є незалежним рейтингом країн і інструментом оцінки ризиків відмивання грошей і фінансування тероризму. Його значення представлене за 10 бальною шкалою, де 0 – мінімальне значення ризику, а 10 – максимальне.

Значення даного індексу для країн Східної Європи представлено на рис. 1. Рівень ризику відмивання коштів та фінансування тероризму в досліджуваних країнах (обрано з регіону розташування України) є різним, оскільки між країнами існують великі відмінності, особливо щодо ефективності заходів в боротьбі з вказаними явищами.

Проведені емпіричні дослідження науковців Бодеску К. Н., Ачімб М. В., Даніела Рус А. І. надають чіткі докази, що збільшення цифрових технологій призводить до зниження ризику відмивання грошей. Причому такі висновки підтверджуються як в країнах з високим рівнем доходу, так і в країнах з низьким рівнем доходу [11]. Саме для останніх характерний нижчий відсоток користувачів Інтернету та значно нижчий рівень впровадження технологій. Крім того, науковці, проводячи дослідження 162 країн, встановили докази ролі освіти, інновацій та кібербезпеки в Базельському індексі AML, тобто їх впливу на ризик відмивання коштів та фінансування тероризму.

Підтверджують даний взаємозв'язок і українські дослідники. Так, за результатами розробки та апробації багатофакторної регресійної моделі опису впливу ключових детермінант на загальний рівень цифрового розвитку країн світу встановлено обернену пропорційну залежність між рівнем цифрового розвитку та Базельським індексом AML, «що і є логічно обґрунтованим, адже чим нижче значення Basel AML Index, тим менше країна має ризик до залучення її соціально-економічних об'єктів (особливо банків, необанків, фінансових установ, підприємств, бізнесів) в шахрайські схеми з використанням цифрових технологій, інноваційних фінансових технологій для легалізації кримінальних доходів» [2, с. 94].

З наведеними твердженням не можемо не погодитися, проте до обраної авторами методики є ряд питань, зокрема, щодо вибору індикаторів. Так, серед запропонованих є рівень цифрового розвитку (DDL), який розраховується відповідно до індексу розвитку інформаційно-комунікаційних технологій (IDI) та індексу готовності до мережі (NRI). Проте звіт щодо індексу IDI публікувався з 2009 по 2017 рік та був припинений у 2018 році через проблеми з доступом та якістю даних. Цілком зрозуміло, що «ці результати значною

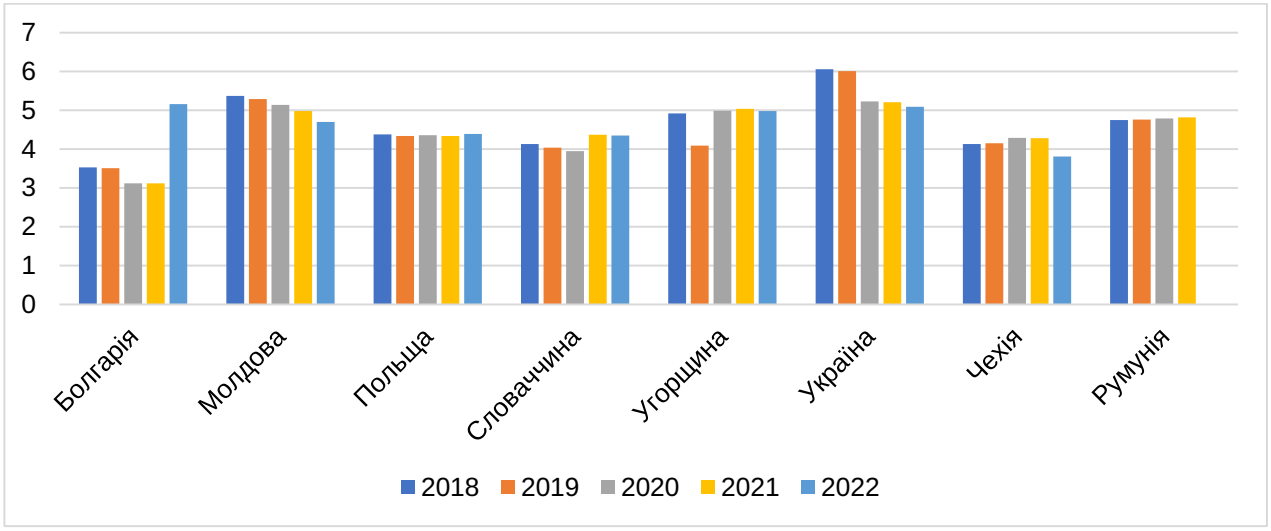

Рис. 1. Значення Базельського індексу AML для країн Східної Європи за 2018–2022 рр.*

*Примітка. За 2022 р. представлено значення лише щодо тих юрисдикції, які мають достатньо даних для розрахунку надійного показника ризику відмивання коштів та фінансування тероризму і пройшли оцінку за методологією 4-го раунду FAFT

Джерело: узагальнено на підставі звітів Basel AML Index 2018, 2019, 2020, 2021, 2022 [5]

мірою застаріли, враховуючи швидку еволюцію ІКТ-ландшафту. Тому користувачі повинні бути дуже обережними, використовуючи результати та роблячи висновки щодо поточного стану цифрового розвитку країни» [9]. Наразі ведуться роботи щодо розробка та запуск індексу IDI в 2023 р.

Проте навіть наразі перелік основних рейтингових індексів цифровізації є досить значним: глобальний індекс кібербезпеки (Global Cyber Security Index, GCI); індекс мережевої готовності (Networked Readiness Index, NRI); індекс прийняття цифровізації (Digital Adoption Index, DAI); індекс світової цифрової конкурентоспроможності (IMD World Digital Competitiveness Index, WDCI); індекс цифровізації економіки (Boston Consulting Group, e-Intensity); індекс цифрової еволюції (Digital Evolution Index, DEI); індекс цифрової економіки та суспільства (Digital Economy and Society Index, DESI) [1; 4].

В той же час «за різними показниками одні й ті ж країни займають різні позиції. Це призводить до неоднозначних висновків та уявлень про реальні оцінки кіберможливості та кіберпотужності країн» [1, с. 75], про що і свідчить порівняння ряду індексів оцінки цифровізації (DESI, NRI) та Базельського індексу AML (рис. 2).

Таким чином, однозначно можна стверджувати про вплив цифровізації як на рівень ризику відмивання коштів та фінансування тероризму, так і на заходи боротьби в цій сфері, проте чітко визначити напрям цього впливу вцілому за всіма країнами неможливо. Виходячи з положення, що використання сучасних цифрових технологій, їх активне впровадження в різноманітні сфери господарської діяльності несе як позитивні наслідки, так і ряд загроз, опишемо їх для сфери протидії відмивання коштів та фінансування тероризму.

Цифрова трансформація висуває нові вимоги та вносить суттєві зміни щодо обміну інформацією між фінансовими установами. Це призводить до того, що роль цифрових технологій у боротьбі з відмиванням коштів та фінансуванням тероризму стає ключовою.

Так, роботизована автоматизація процесів, розширена аналітика та штучний інтелект показують високі результати, допомагаючи компаніям отримувати та збирати дані, а також аналізувати поведінку клієнтів.

Нові цифрові рішення, побудовані на основі технологій штучного інтелекту та розширеної аналітики, забезпечують банкам і фінансовим установам: прозорість транзакцій; збір та перевірку клієнтських даних; допомогу у належній перевірці нових клієнтів; відстеження глобальних транзакцій; отримання в режимі реального часу інформації для ефективного управління ризиками відмивання коштів та фінансування тероризму; спрощення процесу скринінгу та зниження витрат; забезпечення захисту та конфіденційності даних.

Цифрові рішення в сфері боротьбі з відмиванням коштів та фінансуванням тероризму можна охарактеризувати в розрізі компонент, які використовуються більшістю банків для оцінки, аналізу та вимірювання ризику фінансових злочинів, зокрема «знай свого клієнта» (KYC) і «моніторинг транзакцій» (TM).

Процедура KYC описує процес перевірки клієнтів. Вона виконується для запобігання незаконним діям, зокрема відмиванню грошей, фінансуванню тероризму або шахрайству, при цьому захищаючи як компанію, так і клієнта. Цифрові рішення в межах даної процедури охоплюють процеси моніторингу та перевірки клієнтів, забезпечують єдиний доступ до різних внутрішніх і зовнішніх джерел інформації, включаючи CRM системи.

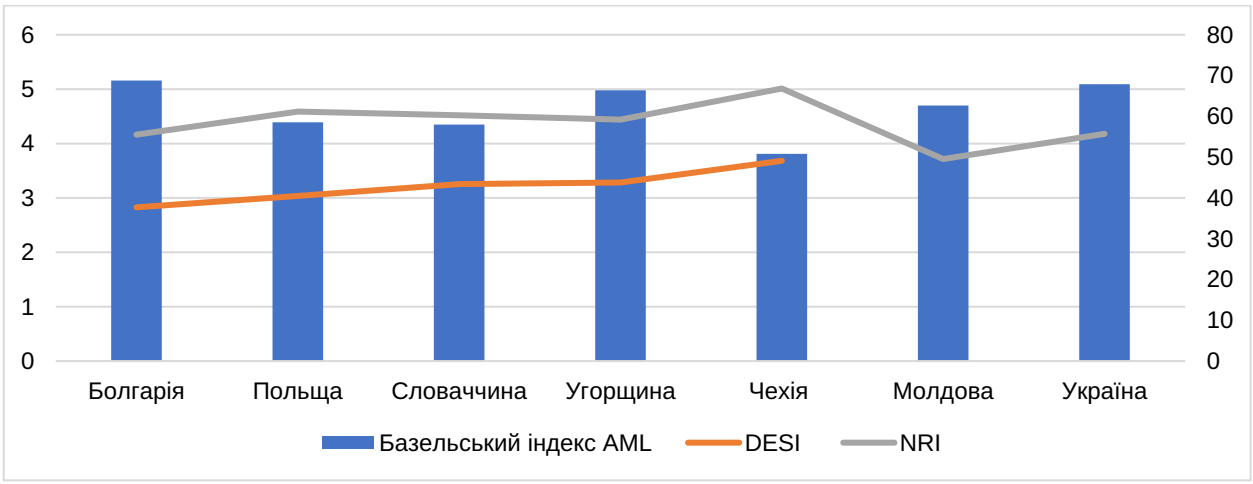

Рис. 2. Порівняння країн Східної Європи за Базельським індексом AML, DESI та NRI в 2022 р.

*Примітка. Індекс DESI розраховується для держав-членів ЄС

Джерело: побудовано на підставі даних [5; 7; 8]

Автоматизована перевірка порушень санкцій, негативних згадувань у засобах масової інформації, а також інформації про власність з усіх джерел значно підвищує ефективність перевірки клієнтів.

Окремі рішення пропонують перевірку якості даних, що дозволяє банкам стандартизувати формати даних, виправляти помилки в іменах, а також видаляти дублікати записів клієнтів у різних джерелах.

Інструменти візуалізації забезпечують фахівцям з комплаєнс-контролю легкий обмін складною структурою відносин між різними зацікавленими сторонами.

Усі системи ТМ базуються на наборі правил, призначених для виявлення підозрілої активності, використовуються для виявлення та припинення операцій з відмивання грошей та фінансування тероризму. Рішення ТМ широко використовують розширену аналітику та штучний інтелект для моніторингу, визначення рейтингів ризику, надання попереджень, а також звітування про підозрілі транзакції.

Банки можуть здійснювати автоматизований моніторинг у режимі реального часу або у режимі пакетної обробки. Більшість рішень постачається з попередньо визначеними алгоритмами та сценаріями виявлення, а також пропонують можливості налаштування для зміни перевірки на основі оцінки ризику клієнта або транзакції. Це важлива характеристика, яка може допомогти традиційному управлінню транзакціями усунути недолік затримки створення сценарію для нових пошуків.

Рішення, що використовують технологію машинного навчання, пропонують алгоритми самонавчання та дозволяють виявляти підозрілі транзакції на більш складному рівні. Цифрові інструменти візуалізації та аудиту забезпечують ефективне управління сповіщеннями, звітами та журналами аудиту.

Застосування цифрових інструментів повинно базуватися на дослідженні типових схем відмивання коштів та фінансування тероризму, що дозволить підвищити ймовірність їх виявлення та запобігання. Крім того, слід враховувати, що і самі банки можуть виступати не тільки в якості суб'єктів моніторингу, але й можуть бути задіяні в тіньових економічних схемах, як добровільно (здійснюючи нелегальні дії або знаючи про їх здійснення через банківські установи), так і виступаючи посередником між суб'єктами нелегальних схем, не знаючи про свою участь в незаконних операціях та махінаціях [3]. Саме тому для банку так важливо ідентифікувати ситуації, які потребують особливої уваги:

– наявність облікового запису, у якому кілька людей мають право підпису, проте не мають сімейних чи ділових відносин;

– здійснення частих банківських переказів в невеликих сумах (до порогових значень), щоб уникнути ідентифікації;

– використання готівки для відкриття великих депозитів або зняття з рахунків для операцій, які зазвичай не пов'язані з готівковими розрахунками;

– наявність депозитів для суб'єкта підприємницької діяльності, які характеризуються комбінація грошових інструментів, що не відповідають звичайній діяльності;

– використання декількох особистих і бізнес-рахунків або рахунків некомерційних організацій для збору та подальшого спрямування коштів негайно або через короткий час до іноземних бенефіціарів.

Однак, володіючи цифровими технологіями, банки можуть посилити перевірку, враховуючи наведені ситуації, які сигналізують про потенційну підозрілу діяльність, у свої стратегії ТМ. Такі сценарії повинні викликати попередження для подальшої перевірки.

Наразі одним з найбільш суперечливих інструментів, які можуть використовуватися для відмивання коштів, є криптовалюта. Практично одні й ті самі її характеристики науковці та дослідники наводять і як аргументи щодо можливостей її використання для відмивання коштів, і як аргументи щодо відсутності небезпеки зі сторони цієї валюти для вказаних операцій (таблиця 1).

Така неоднозначна позиція зумовлена недостатнім рівнем дослідження даного інструменту, відсутністю чіткої позиції щодо його визнання в кожній країні. В будь-якому випадку на сучасному етапі основний метод боротьби з відмиванням коштів, що здійснюється з використанням технологій анонімності (VPN, криптовалюти) полягає у послідовному відстеженні. Звичайно, що за умови придбання криптовалюти за готівку або через P2P-сервіси ці процедури значно ускладнені.

Таким чином, аналізуючи технологію блокчейн, не можемо стверджувати, що їй притаманні характеристики, які б робили її більш ефективною для злочинців в порівнянні з іншими технологіями. Цифрові валюти можуть допомогти правоохоронним органам, надаючи їм інформацію про підозрілу активність. Адже спочатку злочинці мають опублікувати всі свої транзакції у блокчейні, а тому правоохоронним органам простіше відстежити платежі через криптовалюту, ніж через готівку.

Висновки з проведеного дослідження. Цифрові технології в поєднанні з передовим комп'ютерним забезпеченням є важливими інструментами в боротьбі з відмиванням грошей та фінансуванням тероризму в міжнародній площині. Використання окремих цифрових технологій в протидії з відмиванням коштів та фінансуванням тероризму дозволяє фінансовим установам значно підвищити ефективність щодо виявлення спроб

Таблиця 1

Оцінка характерних рис криптовалют щодо можливості їх використання для відмивання коштів

Характеристика	Можливості використання для відмивання коштів	Перешкоди для використання для відмивання коштів
Технологія блокчейн, яка лежить в основі	Незворотність угоди. Застосування технології блокчейн передбачає, що після відправки коштів їх неможливо повернути без участі нового власника	Незмінно прозора природа блокчейну не підходить для відмивання коштів, оскільки вона дозволяє правоохоронним органам більш легко виявляти та відстежувати такі операції в порівнянні якби вони відбувалися з готівкою
Анонімність	Окремі види криптовалют віддають пріоритет конфіденційності транзакцій, існують також сервіси, які пропускають криптовалюту через різні гаманці для ускладнення її відстеження	Частину транзакції можна відстежити. Більшість так званих анонімних криптовалют набагато прозоріше і легше відстежувати, ніж готівку
Регулювання та оподаткування операцій з криптовалютою	Незважаючи на ряд заходів, які вживаються багатьма країнами світу щодо регулювання операцій з даним активом, залишається значна частина питань, яка чітко не визначена на законодавчому рівні, що створює сприятливі умови для використання в злочинних діях	Процес верифікації у цій сфері дуже суворий. Набагато простіше використати більш традиційні схеми, зокрема відкрити банківський рахунок із підробленими документами у невеликому місцевому чи регіональному банку

вчинення вказаних злочинів. Завдяки роботизованій автоматизації процесів та технології блокчейн багато процесів протидії відмиванню коштів та фінансуванню тероризму потребують менше часу та відбуваються з меншою кількістю помилок, що тим самим зменшує потребу втручання людей та одночасно дозволяє співробітникам зосередитися на більш важливих аспектах своїх завдань.

Інноваційні рішення на основі цифрових технологій можуть усунути прогалини в банківських операціях і полегшити процес для галузі, яка намагається скоротити зростаючі витрати та ще більше розвантажити ресурси. Аналітика та штучний інтелект – це тільки основні з цифрових технологій, які трансформують і підвищують ефективність заходів протидії відмиванню коштів та фінансуванню тероризму.

Систематизація та критичний аналіз підходів науковців до встановлення взаємозв'язку між рівнем цифровізації та рівнем відмивання коштів та фінансування тероризму показали складність в оцінці даних процесів. Саме тому незважаючи на можливості, які надають цифрові інструменти для здійснення операцій банками в ході фінансового моніторингу, необхідна чітка ідентифікація загроз, які вони провокують, та організація послідовного відстеження за операціями з їх використанням.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Барченко Н. Л., Любчак В. О., Лаврик Т. В. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2022. № 2(18). С. 73–85. DOI: https://doi.org/10.28925/2663-4023.2022.18.7385.

2. Койбічук В., Куровська Ю. Вплив інтегральних показників цифровізації суспільноекономічних трансформацій на рівень цифрового розвитку країни. *Вісник економіки*. 2022. Вип. 1. С. 83–96. DOI: https://doi.org/10.35774/visnyk2022.01.083.

3. Мордань Є. Ю., Бухтіарова А. Г., Кравченко Я. І. Оцінка ризику участі банків у нелегальних схемах. *Ефективна економіка*. 2021. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=9058. DOI: 10.32702/2307-2105-2021.7.80.

4. Піжук О. І. Сучасні методологічні підходи до оцінювання рівня цифрової трансформації економіки. *Бізнес Інформ*. 2019. № 7. С. 39–47. DOI: https://doi.org/10.32983/2222-4459-2019-7-39-47.

5. Basel AML Index. URL: https://index.baselgovernance.org/download.

6. Bodescu C. N., Achimb M. V., Daniela Rus A. I. The influence of digital technology in combating money laundering: 24th RSEP International Conference on Economics, Finance & Business – Virtual/Online 24–25 February 2022, Holiday Inn Vienna City, Vienna, Austria. P. 8. URL: https://rsepconferences.com/wp-content/uploads/2022/03/Vienna-Book-Abstract-Completed.pdf.

7. Network Readiness Index 2022. URL: https://networkreadinessindex.org.

8. The Digital Economy and Society Index (DESI). URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

9. The ICT Development Index – Background. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/Background.aspx.

REFERENCES:

1. Barchenko N. L., Liubchak V. O., Lavryk T. V. (2022) Model indykatoriv otsinky natsionalnoho rivnia tsyfrovizatsii ta kiberbezpeky derzhav svitu [A model of indicators for assessing the national level of digitalization and cyber security of the countries of the world]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»* [Cybersecurity: education,

science, technology], vol. 2, no. 18, pp. 73–85. DOI: https://doi.org/10.28925/2663-4023.2022.18.7385.

2. Koibichuk V., Kurovska Yu. (2022) Vplyv intehralnykh pokaznykiv tsyfrovizatsii suspilnoekonomichnykh transformatsii na riven tsyfrovoho rozvytku krainy [The impact of integral indicators of digitalization of socio-economic transformations on the level of digital development of the country]. *Visnyk ekonomiky* [Bulletin of the economy], vol. 1, pp. 83–96. DOI: https://doi.org/10.35774/visnyk2022.01.083.

3. Mordan Ye. Yu., Bukhtiarova A. H., Kravchenko Ya. I. (2021) Otsinka ryzyku uchasti bankiv u nelehalnykh skhemakh [Risk assessment of banks' participation in illegal schemes]. *Efektyvna ekonomika* [Efficient economy], vol. 7. Available at: http://www.economy.nayka.com.ua/op=1&z=9058 (accessed 28 March 2023). DOI: 10.32702/2307-2105-2021.7.80.

4. Pizhuk O. I. (2019) Suchasni metodolohichni pidkhody do otsiniuvannia rivnia tsyfrovoi transformatsii ekonomiky [Modern methodological approaches to assessing the level of digital transformation of the economy]. *Biznes Inform* [Business Inform], vol. 7, pp. 39–47. DOI: https://doi.org/10.32983/2222-4459-2019-7-39-47.

5. Basel AML Index. Available at: https://index.baselgovernance.org/download (accessed 22 April 2023).

6. Bodescu C.N., Achimb M.V., Daniela Rus A.I. (2022) The influence of digital technology in combating money laundering]. Proceedings of the *24th RSEP International Conference on Economics, Finance & Business – Virtual/Online* (Austria, Vienna, February 24-25, 2022), p. 8. Available at: https://rsepconferences.com/wp-content/uploads/2022/03/Vienna-Book-Abstract-Completed.pdf (accessed 28 March 2023).

7. Network Readiness Index 2022. Available at: https://networkreadinessindex.org/ (accessed 22 April 2023).

8. The Digital Economy and Society Index (DESI). Available at: https://digital-strategy.ec.europa.eu/en/policies/desi.

9. The ICT Development Index – Background. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/Background.aspx (accessed 22 April 2023).