УДК 004.6: 004.021: 336.7
КП
№ Державної реєстрації 0121U109559
Інв. №

Міністерство освіти і науки України
Сумський державний університет (СумДУ)
40007, м. Суми, вул. Р.-Корсакова, 2, тел. (0542) 66-51-10, факс (0542) 33-40-49

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
д-р. фіз.-мат. наук, професор
_____А.М. Чорноус

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку

ОБҐРУНТУВАННЯ КОНЦЕПЦІЇ КОНВЕРГЕНЦІЇ СИСТЕМИ ФІНАНСОВОГО МОНІТОРИНГУ ТА КІБЕРШАХРАЙСТВ

(проміжний)

Керівниця НДР
доцентка кафедри економічної кібернетики
д-р. екон. наук, доцентка Г.М. Яровенко

2021

Рукопис закінчений 23 грудня 2021 р.
Результати цієї роботи розглянуті науковою радою СумДУ,
протокол від 2021.12.23 № 7

СПИСОК АВТОРІВ

Доцентка кафедри економічної кібернетики, д-р. екон. наук, доцентка (керівниця)	23.12.2021	Г.М. Яровенко (вступ, підрозділи 1.2, 1.3, 2.1, 2.2, 3.1, 3.2, розділ 4, висновки)
Зав. кафедри економічної кібернетики, д-р екон. наук, професорка (відповідальна виконавиця)	23.12.2021	О.В. Кузьменко (підрозділи 1.1, 1.2, 1.3)
Професор кафедри економічної кібернетики, д-р екон. наук, професор	23.12.2021	С.В. Лєонов (підрозділ 1.3)
Аспірант кафедри економічної кібернетики	23.12.2021	О.В. Колотіліна (підрозділ 3.2)
Магістрантка кафедри економічної кібернетики	23.12.2021	Радько В.В. (підрозділ 2.2)
Бакалаврантка кафедри економічної кібернетики	23.12.2021	Світлична А.О. (підрозділ 3.2)

РЕФЕРАТ

Звіт про НДР: 199 с., 74 рис., 9 табл., 46 формул, 135 джерел, 1 додаток.

КІБЕРБЕЗПЕКА, КОНВЕРГЕНЦІЯ, НАЦІОНАЛЬНА БЕЗПЕКА, ФІНАНСОВИЙ МОНІТОРИНГ, ІНТЕЛЕКТУАЛЬНЕ МОДЕЛЮВАННЯ.

Об’єкт дослідження – система економічних відносин, що виникають між суб’єктами господарювання та регуляторами фінансового ринку, що виникають в процесі комплексного застосування засобів фінансового моніторингу та боротьби із кіберзлочинністю. Мета роботи – розвиток методології та міждисциплінарного методичного інструментарію пошуку оптимальної моделі інтеграції систем фінансового моніторингу та кібербезпеки, що дозволить напрацювати принципово нові, засновані на концептах поведінкової економіки та відокремлені від людського фактору, інтелектуальні алгоритмізовані регуляторні механізми, які уможливлять комплексне забезпечення економічної, фінансової та інформаційної складових національної безпеки держави, а також захисту прав споживачів фінансових послуг.

Методи дослідження: фундаментальні положення економічної теорії, макро- і мікроекономіки, теорії стратегічного управління, державного регулювання економіки, економіко-математичного моделювання. Інформаційно-фактологічна база: законодавчі та нормативні документи Національного банку України, інструкції банків, наукові праці вітчизняних та зарубіжних фахівців.

Досліджено поняття, цілі й задачі, напрями, моделі конвергенції систем фінансового моніторингу і кібербезпеки, здійснено попередній аналіз процесу їх конвергенції; побудовано фазові портрети «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» системи протидії фінансовим та кібершахрайствам; змодельовано ключові алгоритми конвергенції системи кібербезпеки та фінансового моніторингу; розроблено математичне забезпечення алгоритмів виявлення кібершахрайських операцій з кредитними картками; розроблено барицентричні моделі збалансованого розвитку національної економіки, що інтегрують композитні індикатори економічного, соціального й політичного розвитку країни, а також рівня її протидії фінансовим шахрайствам та кібербезпеки; розроблено сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку; оцінено синергетичний ефект від конвергенції моделей фінансового моніторингу та кібербезпеки.

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційних технологій, який спостерігається в останнє десятиліття, сприяв їх упровадженню в діяльність економічних агентів для вирішення різних економічних задач. І якщо раніше достатньо було мати інформаційну систему обліку, яка на сто відсотків вирішувала потреби суб'єктів в автоматизації їх діяльності, то на сьогодні коло задач є значно широким та не обмежується бухгалтерським обліком. З іншого боку, автоматизація та діджиталізація процесів призвела до зростання рівня кібершахрайств, особливо у фінансовій сфері. Це пов'язано із збільшенням доступності пересічному користувачу програмних та технічних інструментів для здійснення кіберзлочинів та кібершахрайств, а також зростання рівня інформаційної грамотності населення. Тому діяльність фінансових установ сьогодні спрямована на те, щоб забезпечити необхідний рівень кіберзахисту в умовах розповсюдження можливостей для реалізації кіберзлочинів.

Також фінансові установи є суб'єктами фінансового моніторингу, що зобов'язує їх здійснювати перевірку операцій, які потенційно можуть бути легалізованими кримінальними доходами чи результатом фінансування тероризму. Хоча сьогодні й зростають вимоги до системи протидії відмиванню коштів, дотримання яких має на увазі проведення постійного моніторингу для виявлення підозрілих операцій, але зростають обсяги операцій, метою яких є легалізація кримінальних доходів та фінансування тероризму, що здійснюють за рахунок втручання хакерів та інших кіберзлочинців. Тобто відбувається поєднання кібер- та фінансової злочинності, результатом чого є зростання втрат фінансових інституцій та зниження до них довіри з боку населення та суб'єктів господарювання. На цьому тлі також зростання потоків інформації, стрімка зміна навколишнього середовища, удосконалення програмних та технічних інструментів призводить до того, що фінансові установи не встигають ефективно протидіяти кібер- та фінансовим злочинам. Саме тому ідея конвергенції двох

систем – кібербезпеки та фінансового моніторингу, є досить актуальною та практично значущою для фінансових установ, оскільки це призведе до спрощення здійснення процесів управління, які стосуються виявлення та попередження кібершахрайських операцій та операцій з легалізації кримінальних доходів.

Головною передумовою конвергенції системи фінансового моніторингу та кібербезпеки є саме зростання обсягів інформаційних потоків. Їх об'єднання на інформаційному рівні, по-перше, збільшить кількість критеріїв для перевірки та пошуку злочинних операцій та дій, а по-друге, дозволить охопити різні бази вхідних даних. На організаційному рівні конвергенція дозволить відповідним підрозділам фінансової установи здійснювати обмін інформацією, що сприятиме більш ефективному моніторингу операцій не тільки на предмет їх відповідності законодавству, але й на предмет потенційного здійснення кібершахрайства. Також на технологічному рівні із зростанням можливостей використання інтелектуальних методів моделювання з'являються перспективи модернізації технологій та інструментів, які застосовуються для виявлення злочинних схем та операцій. Це сприятиме їх розвитку такими темпами, які не відстають від темпів розвитку інструментарію кібер- та фінансових злочинців.

Конвергенція систем кібербезпеки та фінансового моніторингу сприятиме отриманню ряду переваг. По-перше, зниження витрат, пов'язаних із організацією двох систем, особливо в частині залучення персоналу та використання програмно-технологічного забезпечення. По-друге, підвищення якості аналітичної інформації за рахунок реалізації саме інформаційного забезпечення, що охоплює як критерії та вимоги щодо протидії легалізації коштів, так й кібершахрайству. По-третє, синергетичний ефект від інтегральної взаємодії двох систем, який полягатиме у підвищенні ефективності перевірок за рахунок впровадження комплексу різних методів та інструментів.

Таким чином, сучасні реалії зростання обсягів кібершахрайств та легалізації кримінальних доходів, потребують не тільки збільшення вимог до операцій, але впровадження більш дієвих заходів, реалізація яких можлива на

інформаційному, програмно-технологічному та організаційному рівнях управління фінансовою установою. Відповідно забезпечення цих процесів можливо тільки за рахунок конвергенції двох систем – кібербезпеки та фінансового моніторингу.

Окреслена проблема дозволила обрати об’єкт та предмет дослідження. Об’єкт дослідження – система економічних відносин, що виникають між суб’єктами господарювання та регуляторами фінансового ринку, що виникають в процесі комплексного застосування засобів фінансового моніторингу та боротьби із кіберзлочинністю.

Предмет дослідження – методологічні засади та методичний формування комплексних, упереджувальних інтелектуальних механізмів регулювання фінансового ринку, що сприятимуть підвищенню національної безпеки в умовах цифровізації фінансового простору.

Відповідно до об’єкта та предмета дослідження було сформовано мету. Так, метою дослідження є розвиток методології та міждисциплінарного методичного інструментарію пошуку оптимальної моделі інтеграції систем фінансового моніторингу та кібербезпеки, що дозволить напрацювати принципово нові, засновані на концептах поведінкової економіки та відокремлені від людського фактору, інтелектуальні алгоритмізовані регуляторні механізми, які уможливлять комплексне забезпечення економічної, фінансової та інформаційної складових національної безпеки держави, а також захисту прав споживачів фінансових послуг.

Для реалізації поставленої мети необхідно було вирішити наступні завдання:

- охарактеризувати поняття, цілі й задачі, напрями, моделі конвергенції систем фінансового моніторингу і кібербезпеки;
- здійснити попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу країн;

- побудувати фазові портрети «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» системи протидії фінансовим та кібершахрайствам;
- здійснити моделювання ключових алгоритмів конвергенції системи кібербезпеки та фінансового моніторингу у банках;
- розробити математичне забезпечення алгоритмів виявлення кібершахрайських операцій з кредитними картками;
- розробити чотириполюсні барицентричні моделі збалансованого розвитку національної економіки, що інтегрують композитні індикатори економічного, соціального й політичного розвитку країни, а також рівня її протидії фінансовим шахрайствам та кібербезпеки;
- розробити сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку;
- оцінити синергетичний ефект від конвергенції моделей фінансового моніторингу та кібербезпеки.

Методи дослідження – фундаментальні положення економічної теорії, макро- і мікроекономіки, теорії стратегічного управління, державного регулювання економіки, економіко-математичного моделювання (теорія біфуркації динамічних систем; канонічний аналіз; сучасні концепції моделювання бізнес-процесів; методи інтелектуального аналізу даних: логіт-регресія, дерево рішень, нейронні мережі; метод переваг та функція Харрінгтона – Менчера; метод визначення центра мас; DEA-аналіз).

Інформаційно-фактологічну базу дослідження сформували законодавчі та нормативні документи Національного банку України, інструкції банків, наукові праці вітчизняних та зарубіжних фахівців.

Отримані у роботі результати впроваджені у навчальний процес, а саме при викладанні дисциплін «Введення до бізнес-аналітики», «Інформаційні системи і технології в управлінні», «Ефективність інформаційних систем», «Моделювання бізнес-процесів».

За результатами НДР опубліковано: 8 статей у журналах, що індексується у БД Scopus та WoS; 10 фахових статей у виданнях України категорії Б; 1 – монографія та розділи у монографіях у закордонних виданнях англійською мовою; 1 - монографія та розділи монографій українською мовою; захищено 2 докторські дисертації та 1 кандидатську дисертацію; отримано 8 свідоцтв про реєстрацію авторського права на твір; диплом ІІ та ІІІ ступеня за напрямком «Економічна аналітика і статистика» у Всеукраїнському конкурсі студентських наукових робіт.

Звіт виконано на основі публікацій виконавців, перелік яких надано у списку літератури.

1 ОЦІНЮВАННЯ ЗРІЛОСТІ ДІЮЧОЇ СИСТЕМИ ПРОТИДІЇ ФІНАНСОВИМ ТА КІБЕР-ШАХРАЙСТВАМ ТА ПОБУДОВА ФАЗОВИХ ПОРТРЕТІВ ЇХ «ЗРІЛОСТІ», «СТАНІВ РІВНОВАГИ» ТА «РЕЛАКСАЦІЙНИХ КОЛИВАНЬ ВТРАТИ СТІЙКОСТІ»

1.1 Конвергенція систем фінансового моніторингу і кібербезпеки: поняття, цілі й задачі, напрями, моделі

Стрімкий розвиток, зростання та накопичення сучасних технологій, інформаційного забезпечення, цифрових даних, створюють передумови застосування інформаційних технологій у різних сферах та напрямах діяльності. В Україні та світі наразі створено комфортні умови вільної роботи з новітніми технологіями фінансово-економічної галузі в online режимі. Так, фізичні особи та суб’єкти господарювання отримали майже необмежені можливості дистанційно користуватись фінансовими послугами, підключатись до online банкінгу, валютних бірж, фондового ринку, інших фінансово-кредитних установ та організацій. Наряду з цим, кожен інноваційний процес супроводжується певним загрозами. Так, в інформаційному, віртуальному кіберпросторі з’являться загроза зростання злочинів через його доступність як легальним учасникам, так і злочинцям. Але застосування в економічній сфері таких сучасних можливостей, формує потребу у забезпеченні належної економічної безпеки фінансових операцій, що проходять через відповідні системи.

За останні десять років в Україні було сформовано систему боротьби з відмиванням незаконних коштів, фінансуванням тероризму, розповсюдження зброї масового знищення, в тому числі з кіберзагрозами, у вигляді комплексу заходів з фінансового моніторингу та системи кібербезпеки, що передбачає перевірку клієнтів та їх фінансових транзакцій, з метою контролю за економічною чистотою та прозорістю фінансових транзакцій.

Тому, в сучасних ринкових умовах, питання конвергенції систем фінансового моніторингу та кібербезпеки є особливо актуальним та потребує детального вивчення та аналізу.

Загальні питання з фінансового моніторингу теоретичного характеру та його специфічні практичні особливості у своїх трактатах розкривають як вітчизняні, так і зарубіжні вчені, серед яких: Морс Дж. К. [1], який висвітлює глобальний режим боротьби з фінансуванням тероризму під впливом транснаціонального ринку; Радигін В. Ю., Купріянов Д. Ю., Бессонов Р. А., Іванов М. Н., Ослякова І. В. [2], які пропонують шляхи вирішення завдань первинного фінансового моніторингу; Яшина Н. І., Кашина О. І., Прончатова-Рубцова Н. Н., Яшин С. Н., Кузнєцов В. П. [3], які висвітлюють окремі аспекти фінансового моніторингу, фінансової стабільності та цифровізації; Грабчук О., Супрунова І. [4], які розкривають поняття, складові, етапи розвитку фінансового моніторингу як умови забезпечення державної безпеки країни; Першин В. Г. [5], який розглядає проблематику, визначає роль фінансового моніторингу в межах протидії легалізації доходів, одержаних злочинним шляхом, пропонує шляхи удосконалення системи фінансового моніторингу; Рисін В. В., Степанова А. В. [6], які описують інструменти протидії фінансуванню тероризму з використанням фінансових установ; та ін.

Питання вивчення, дослідження, використання, удосконалення поняття кібербезпека у сучасній науковій економічній літературі розглядаються такими вченими як: Шекелфорд С., Докері Р., Прабхакар Б., і Реймонд А. [7] досліджують кібербезпеку в умовах кризи; Ученду Б., Медсестра Дж. Р. К., Бада М. і Фернелл С. [8] узагальнюють розвиток культури кібербезпеки; Хан К. [9] пропонує використовувати напівкількісну оцінку ризиків кібербезпеки шляхом аналізу рівня блокування та захисту; Мохор В., Гончар С., Онискова А. [10] запроваджують оцінку ризиків кібербезпеки інформаційних систем; Гіменес-Агілар М., де Фуентес Ж. М., Гонсалес-Манцано Л., та Арройо Д. [11] висвітлюють практичні досягнення кібербезпеки в системах на основі блокчейну; Репетто М., Стрікколі Д., Піро Г., Каррега А., Боггіа Г., і Болла Р. [12]

аналізують автономну систему кібербезпеки для ланцюгів цифрових послуг нового покоління; та ін.

Результати впливу конвергенції на ефективність досліджуваних процесів у своїх працях розкривають наступні науковці: Мадейра П. М., Вале М., Мора-Алиседа Дж. [13] пропонують комбінування стратегії розумної спеціалізації та регіональної конвергенція в економіці; Ібрагім А. Е. А., Еламер А. А., і Езат А. Н. [14] описують конвергенцію великих даних та бухгалтерського обліку при прогнозування; Донг Ф., Лі Ю., Цінь К. і Сан Дж. [15] досліджують вплив промислової конвергенція на ефективність екологічного розвитку; Гілбо Д., Барончеллі А., і Чентола Д. [16] висвітлюють експериментальні докази конвергенції аналізованих категорій; та ін.

Отже, питаннями пошуку методів та шляхів упередження, протидії та боротьби з фінансовими злочинами, при здійснені яких застосовуються інформаційні, технологічні, комунікаційні, технічні системи, опікуються і національні державні органи, і міжнародне світове співтовариство.

Розглядаючи особливості фінансового моніторингу, в першу чергу необхідно розглянути його визначення. Так згідно Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» «фінансовий моніторинг - сукупність заходів, що вживаються суб’єктами фінансового моніторингу у сфері запобігання та протидії, що включають проведення державного фінансового моніторингу та первинного фінансового моніторингу» [**Ошибка! Источник ссылки не найден.**]. У загальному трактуванні, фінансовий моніторинг представляє собою комплексну систему принципів, заходів, методів, методик, які проводяться суб’єктами та учасниками фінансового моніторингу для виявлення, протидії, запобігання використання фінансової та банківської системи для легалізації доходів, отриманих незаконним шляхом, фінансування терористично діяльності, розповсюдження зброї масового знищення; сукупність дій по виявленню операцій, що можуть бути пов’язані з відмиванням коштів, їх досконале

вивчення та вчинення відповідних дій; це система контролю за фінансовими транзакціями для недопущення легалізації та відмивання шахрайських коштів. А легалізація доходів, здобутих незаконним шляхом – це такі дії, заходи, операції коштами, що мають відношення до незаконної діяльності, мають нелегальні джерела походження, приховують незаконне володіння коштами, передбачають незаконне їх переміщення, використання, зміну форми.

Враховуючи вищезазначене, формується трактування поняття системи фінансового моніторингу – сукупності заходів (державного та первинного рівнів), що вчиняються суб'єктами первинного фінансового моніторингу та Спеціально уповноваженим органом з питань фінансового моніторингу в частині ідентифікації, вивчення та аналізу фінансових транзакцій, додаткової інформації про них, про клієнтів, на предмет виявлення відношення до незаконної діяльності, фінансування тероризму, здійснення обліку таких фінансових операцій, оцінювання ризиків від подібних транзакцій. Визначальна роль в системі фінансового моніторингу відводиться суб'єктам перинного фінансового моніторингу, до яких належать [**Ошибка! Источник ссылки не найден.**]: банківські установи, страхові компанії, перестрахові організації, організації – надавачі фінансових послуг, платіжні установи, організації, що виступають членами платіжних систем, ломбарди, кредитні спілки, учасники ринку цінних паперів, товарні біржі, оператори поштових переказів, установи, що проводять валютні транзакції, аудиторські компанії, організації – надавачі бухгалтерських послуг, нотаріуси, адвокати, надавачі юридичних послуг, надавачі послуг по утворенню та управлінню суб'єктів господарювання, агентства нерухомості, суб'єкти господарювання - продавці лотерей, організатори азартних ігор, продавці віртуальних активів, інші надавачі фінансових послуг. Провідна роль належить суб'єктам державного фінансового моніторингу [**Ошибка! Источник ссылки не найден.**]: Національний банк України, Міністерство юстиції України, Національна комісія з цінних паперів та фондового ринку, Міністерство цифрової трансформації України, Спеціально уповноважений орган.

Організація ефективного фінансового моніторингу передбачає визначення та досягнення стратегічних пріоритетних цілей, тобто: протидія легалізації доході, отриманих незаконним шляхом; боротьба з фінансуванням терористичної діяльності; протидія фінансування розповсюдження зброї масового знищення; належна організація, реалізація та контроль внутрішньобанківської системи боротьби з відмиванням нелегальних коштів, фінансуванням терористичної активності; функціонування належної системи управління системою ризиків у сфері фінансового моніторингу; захист державних, суспільних, громадянських інтересів від збитків процесу легалізації незаконних доходів, фінансування тероризму; дотримання ризик-орієнтовного підходу при здійсненні фінансового моніторингу; забезпечення координованості співпраці учасників системи фінансового моніторингу; вжиття каральних заходів до порушників законодавства у сфері фінансового моніторингу.

Із зазначених цілей фінансового моніторингу формуються задачі фінансового моніторингу, які поставлені для виконання для досягнення ефективності фінансового моніторингу: розробляти та виконувати вимоги законодавчих актів, інших правових документів та внутрішньої нормативної бази згідно фінансового моніторингу; організовувати відповідні структурні органи та підрозділи з фінансового моніторингу на державному рівні, на рівні суб'єктів первинного фінансового моніторингу, на рівні суб'єктів господарювання; організовувати внутрішньобанківську систему фінансового моніторингу; забезпечувати достатність ресурсної бази для належної роботи системи фінансового моніторингу; забезпечувати ефективне функціонування системи заходів управління ризиками відмивання коштів та фінансування тероризму; забезпечувати достатню інформованість, обізнаність, компетентість фізичних осіб, суб'єктів господарювання, працівників суб'єктів первинного фінансового моніторингу та державних органів щодо ризиків відмивання коштів; організовувати та на постійній основі вдосконалювати внутрішній та зовнішній контроль за протидією легалізації злочинних ресурсів; розробляти та реалізовувати комплекс заходів з належної перевірки клієнтів - проводити

поточні та додаткові перевірки клієнта, здійснювати перевірки фінансових операцій клієнта, виявляти невідповідності між фінансовими транзакціями клієнтів та інформацією, що є у банка про таких клієнтів, про специфіку їх бізнесу, суть діяльності клієнта, цілі та очікувань від ділової співпраці клієнтом, досліджувати джерела походження коштів, визначати статки клієнтів, визначати та встановлювати кінцевих бенефіціарів клієнтів, оцінювати економічну та фінансову доцільність транзакцій клієнта; виявляти незвичність дій та операцій клієнта; запобігати використанню банківських послуг для відмивання нелегальних коштів; виявляти порогові фінансові транзакції; ідентифікувати підозрілі фінансові операції; заморожувати активи неблагонадійних клієнтів, шахраїв, терористів; оперативно та своєчасно повідомляти про ризикові та підозрілі фінансові операції Спеціально уповноваженому органу; проводити належний обмін відповідними даними між суб'єктами первинного фінансового моніторингу та Спеціально уповноваженим органом; забезпечувати роботу дієвої системи ескалації певних підозр та загрозливих питань у сфері запобігання відмивання незаконних коштів; своєчасно розглядати підозри та факти порушень сфері боротьби з легалізацію шахрайських коштів; повідомляти про злочинні дії клієнтів правоохоронним органам; своєчасно надавати потрібні дані, роз'яснення, документи, інформацію на запити Національного банку України в частині дотримання фінансового моніторингу; розробляти, використовувати та постійно удосконалювати автоматизовані системи учасників фінансового моніторингу; проводити замороження активів особам, пов'язаним терористичною діяльністю; здійснювати захист даних, відомостей, інформації у сфері фінансового моніторингу; забезпечувати необхідний доступ суб'єктам фінансового моніторингу до потрібної інформації для проведення фінансового моніторингу; організовувати своєчасний обмін інформацією між учасниками системи фінансового моніторингу; організовувати та забезпечувати міжнародне співробітництво з питань протидії відмивання незаконних коштів а фінансування терористичної діяльності; та ін.

В свою чергу, при формуванні належної системи фінансового моніторингу, виділяються ключові напрями фінансового моніторингу:

- належна перевірка клієнтів (проводиться при встановленні з клієнтом дідових відносин, у разі появи підозр та сумнівів у правдивості поданих клієнтом даних, достовірності інформації щодо суті діяльності та фінансових транзакцій клієнта, у разі проведення разової фінансової транзакції без заключення з клієнтом ділових стосунків, проведенні переказу без відкриття рахунку у сумі 30тис.грн. та більше, здійснення транзакцій по віртуальним активам у сумі 30тис.грн. та більше): ідентифікація (заходи та дії, що проводяться банком для визначення особи клієнта через ідентифікаційні клієнтські дані, до встановлення з потенційним клієнтом ділових відносин), верифікація (заходи та дії банку щодо клієнта для підтвердження відповідності наявних у банку відомостей про клієнта такому клієнту, а також для визначення кінцевих бенефіціарів клієнта, до та під час встановлення з потенційним клієнтом ділових відносин) та відеоверифікація клієнта (верифікація клієнтів шляхом відеотрансляції) – при ідентифікації, верифікації, відеоверифікації клієнтів встановлюються ідентифікаційні дані щодо його найменування паспортних даних, ідентифікаційних кодів, установчих даних, місця реєстрації та знаходження, банківських реквізитів; визначення кінцевих бенефіціарів клієнта (тобто осіб, які мають пріоритетний, вирішальний контроль та вплив на функціонування клієнта та його фінансові транзакції у вигляді прямого володіння часткою 25 та більше відсотків у статутному капіталі, чи у правах голосу, або непрямого впливу володіння менше 25 відсотків у статутному капіталі, чи у правах голосу, але зберігаючи при цьому вирішальну силу голосу); визначення мети та особливостей ділової співпраці з клієнтом (визначити вид банківських послуг, які цікавлять клієнта, особливі умови заключення угод, тарифи, масштаби транзакцій, репутацію клієнта); посилена перевірка клієнта (це заходи з мінімізації рівня ризику, що може бути притаманний клієнту, діловим відносинам з ним; застосовуються до клієнтів з високим ризиком, клієнтів з підозрами проведення операцій з метою відмивання коштів чи фінансування тероризму; проводиться наступними способами:

збільшення ряду дій по перевірці клієнта, актуалізації інформації про нього, та частоти таких дій; затребування у клієнта додаткових даних, роз'яснень, підтверджуючих документів щодо структури власності клієнта, джерел походження коштів, доходів, про наявність ліцензій та дозволів на певну діяльність; пошук додаткових даних про клієнта у відкритих офіційних інформаційних джерелах, тому числі про його господарську діяльність, його кінцевих бенефіціарних власників, про порушені кримінальні провадження, про наявні фінансово-економічні та господарські зв'язки з іншими особами та суб'єктами господарювання; виїзди на місце реєстрації та ведення діяльності клієнта, та ін.); спрощена перевірка клієнта (це заходи з мінімізації рівня ризику, що може бути притаманний клієнту, діловим відносинам з ним; застосовуються до клієнтів з низьким ризиком, до яких належать фізичні особи, які проводять оплату житлово-комунальних послуг на маленькі розміри сум; фізичні особи, у яких відкрито рахунки з виплати соціальних виплат, пенсійних виплат, виплат з оплати праці, стипендій; які проводять раціонально обґрунтовані, звичайні, типові фінансові транзакції у невеликих обсягах; підприємства – надавачі житлово-комунальних послуг, послуг телебачення, інтернет послуг, з якими заключено угоду про приймання платежів; об'єднання співвласників багатоквартирних будинків; юридичні особи та фізичні особи-підприємці при сплаті обов'язкових податкових платежів; державні органи влади; органи місцевого самоврядування; фонди соціального страхування; органи ЄС, дипломатичні представництва членів Організації економічного співробітництва та розвитку; до таких заходів належать: скорочення ряду дій по перевірці клієнта, актуалізації інформації про нього, та частоти таких дій; застосування спрощених методик верифікації клієнтів; скорочення затребування у клієнта додаткових даних, роз'яснень, підтверджуючих документів; застосування відомостей Єдиного державного реєстру юридичних осіб та фізичних осіб підприємців); актуалізація клієнтських даних (тобто актуалізація попередньо одержаних даних, документації, відомостей, а також теперішньої інформації та документів; актуалізація проводиться з різною періодичністю для різних типів ризику

клієнтів – один раз на рік для високого ризику, один раз на три роки для середнього ризику, один раз на п’ять років для низького ризику, або за потребою в певних випадках; актуалізація відбувається у такий спосіб – шляхом заповнення клієнтом при відвіданні банківської установи анкети-опитувальника; шляхом відправки клієнту поштового листа про актуалізацію інформації та документів з анкетою-опитувальником; шляхом відправки клієнту електронного листа про актуалізацію інформації та документів з анкетою-опитувальником; актуалізовані відомості фіксуються у автоматизованій системі баку картці клієнта, а документи підшиваються в особову справу клієнта); відмова банком клієнт від встановлення чи продовження з ним ділової взаємодії, відмова від проведення фінансових транзакцій клієнта (банківській установі необхідно відмовити клієнту у встановленні чи підтриманні ділової співпраці у наступних випадках: якщо клієнт не надав необхідні для ідентифікації, верифікації чи належної перевірки даних; надання клієнтом неправдивих даних; подання клієнтом інформації, яка заплутує банк, вводить його в оману; коли неможливо визначити кінцевих бенефіціарів клієнта; якщо у банківської установи з’являються сумніви стосовно проведення фінансових операцій клієнтом не від власного імені; визначення по клієнту неприйнятно високого рівня ризику; якщо учасник фінансової транзакції банк-оболонка; якщо клієнт підтримує певні відносини з банком-оболонкою; банківській установі заборонено заключати ділову співпрацю з наступними клієнтами: клієнти з Переліку осіб, до яких застосовані спеціальні санкції Міністерства економічного розвитку та торгівлі України; клієнти, які проводять фінансові транзакції, кінцевими вигодоодержувачами яких є особи з Переліку осіб, до яких застосовані спеціальні санкції Міністерства економічного розвитку та торгівлі України; банки-оболонки; особи, які підтримують певні відносини з банками-оболонками; клієнтами, що розташовані чи належать до держав, які не виконують FATF рекомендацій; клієнти, банки яких знаходяться у країнах, які не виконують FATF рекомендацій);

- управління ризиками фінансового моніторингу: визначення ризиків легалізації незаконних коштів та фінансування тероризму (оцінювання та переоцінювання ризик-портфелю банківської установи (ідентифікація та оцінка ризиків відмивання кошті та фінансування тероризму, що характерні роботі банківської установи шляхом визначення для кожної банківської послуги наявних по ним ризикам в залежності від специфіки, направленості, масштабу функціонування банку в часині направленості на обслуговування фізичних осіб роздрібного бізнесу, суб'єктів господарювання мікро, малого, середнього бізнесу, великих корпоративних клієнтів, послуг, що надаються банком, типів клієнтів, їх ризик-портфелів, географічного признаку банку, способів надання банківських послуг, цільового використання банківських послуг, специфічних можливостей використання певних послуг банку при відмиванні коштів, цільового сегменту для різних послуг, можливих обсягів обігу коштів, інших факторів, важливих для банку; аналіз наявних у банківської установи заходів та методик управління ризиками для їх мінімізації); оцінювання та переоцінювання ризик-портфелю клієнтів (визначення критеріїв ризику; ідентифікація первинного ризику встановлення ділових відносин з клієнтом; застосування скорингової ризик-моделі для оцінювання рівня ризику по клієнту; аналіз наявних у банківської установи заходів та методик управління ризиками для їх мінімізації; оцінювання залишкового ризику від встановлення з клієнтом ділових відносин); розрахунок ризик-апетиту банківської установи (визначення ризиків, що банк може прийняти; ризики, що банк готовий прийняти тільки після їх мінімізації; ризики, що банк прийняти не може – клієнти з неприйнятно високим рівнем ризику, злочинна діяльність, клієнти із санкційних та заборонених списків, клієнти з індикаторами підозрілості, визначеними банком)); заходи по мінімізації ризиків легалізації незаконних коштів та фінансування тероризму (дослідження та аналіз нових послуг на наявність ризиків; введення лімітів та обмежень по послугах; надання дозволу на взаємовідносини з публічними та пов'язаними з ними особами; надання дозволу на певні ризикові фінансові операції; використання автоматизованих систем для визначення ризиків по

клієнтам та їх фінансовим транзакціям згідно критеріїв ризиків; проведення належної перевірки клієнтів для усвідомлення та розуміння суті та особливостей господарської діяльності клієнтів; здійснення постійного вивчення та аналізу інформації про клієнта; постійне дослідження відповідності фінансових транзакцій клієнта суті його роботи; дослідження джерел походження фінансових ресурсів клієнта; особливе вивчення та моніторинг клієнті високого рівня ризику; окреме вивчення неприбуткових та благодійних організацій на предмет можливості їх використання в незаконних цілях для відмивання коштів); належне управління ризиками (проведення комплексної оцінки ризиків відмивання незаконних коштів та фінансування тероризму, та його періодичної переоцінки; здійснення належної перевірки клієнтів; організація належної оцінки та переоцінки ризиків, які можуть виникнути при встановленні чи підтриманні ділових відносин з клієнтами; відповідне усвідомлення банком ризиків легалізації незаконних коштів клієнтів; вжиття диференційованих заходів для клієнтів з різним рівнем ризику; проведення певних дій по приведенню ризиків до прийнятного для банку рівня; розробка та використання дієвих інструментів для перешкоджанню систематичному та великомаштабному проведенню підозрілих фінансових транзакцій; налагодження дієвого внутрішньобанківського контролю, аудиту, ревізій з питань фінансового моніторингу; наявність прозорої системи своєчасного виявлення політично значущих, та пов’язаних з ними осіб; наявність ефективної системи ідентифікації та вивчення кінцевих бенефіціарних власників клієнтів).

- міжнародне співробітництво (передбачає співпрацю за принципом взаємності між різними країнами у сфері попередження, перешкоджання, боротьби з відмиванням незаконних коштів, фінансування тероризму, розповсюдженням зброї масового знищення, в тому числі по питанням: надання пропозицій щодо внесення фізичних осіб та суб’єктів господарювання, та повної інформації про них, до санкційних списків іноземних держав; надання пропозицій щодо виключення фізичних осіб та суб’єктів господарювання із санкційних списків іноземних держав; приведення виконання рішень судів

стосовно конфіскації незаконних доходів; зарахування конфіскованих коштів до державного бюджету; дотримання принципу конфіденційності та таємності інформації; забезпечення дозволу спеціалізованим органам іноземних країн до розкриття певної інформації, та ін.);

- організація та забезпечення відповідальності за порушення нормативно-правових та законодавчих актів з питань фінансового моніторингу в частині протидії легалізації незаконних коштів, фінансуванню тероризму, розповсюдженню зброї масового знищення (визначення відповідальності по певним видам правопорушень, такі як письмові застереження та попередження, відкликання та анулювання ліцензій, відсторонення від робіт, штрафні санкції, ліквідація; врахування певних обставин вчинених порушень щодо характеру порушень, їх тривалості, фінансового стану банківської установи чи іншого суб'єкта первинного фінансового моніторингу, характеру та обсягів вигід від протиправних дій, розмірів отриманих збитків третіх осіб, повторності вчинення однотипного порушення, ступеня відповідальності осіб, готовності співпраці з питань фінансового моніторингу).

Ефективність фінансового моніторингу досягається шляхом застосування дієвих моделей, розроблених сучасними науковими діячами та фахівцями досліджуваного напрямку. Такими моделями є наступні:

- скорингова ризик-модель - бальна модель оцінки ризик-портфелю клієнтів, що використовується банківськими установами з застосуванням на базі наявних програмних модулів; реалізовується шляхом проведення оцінки клієнта банку за визначеними критеріями ризиків. Банком визначаються критерії ризику (визначаються відповідальними працівниками банку згідно вимог законодавства та внутрішньої нормативної бази банку; вносяться або вилучаються з відповідної вкладки критеріїв ризику автоматизованої системи банку та кожному з них присвоюється відповідний код); кожному з критеріїв ризику присвоюються відповідні бали від 0 до 101 одиниці; визначається рівень ризику для кожного з критеріїв ризику (0 балів - низький рівень ризику, коли клієнт не співпав ні з одним з критеріїв ризику; від 1 до 50 балів - середній рівень ризику; від 51 до 100

балів - високий рівень ризику; від 101 - неприйнятно високий рівень ризику); згідно результатів проведеної оцінки, бали по кожному критерію ризику, що притаманний клієнту, сумуються в автоматичному режимі; визначається сумарна кількість балів для кожного клієнта банку; сумарна кількість балів по клієнту співставляється зі шкалою визначених рівнів ризиків та клієнту присвоюється автоматично рівень відповідного ризик-портфелю клієнта, тобто рівень ризику ділових відносин з клієнтом. Відповідальні працівники банку вносять зміни у картку клієнта інформацію по критеріям ризиків в день появи обставин, які визначають рівень ризика клієнта, або в день одержання відповідної інформації від підрозділу фінансового моніторингу банку, а також один а на квартал за допомогою відповідних програмних комплексів проводять процедури виявлення притаманних клієнтам критеріїв ризиків;

- автоматизована модель фінансового моніторингу - модель автоматизації процесів фінансового моніторингу, таких як: автоматизація ідентифікації, верифікація, відеоверифікація осіб, які здійснюють фінансові транзакції, що підлягають під фінансовий моніторинг; автоматизація бізнес-процесів інтеграції результатів проведення перевірок внутрішнього моніторингу банків із системою держфінмоніторингу; автоматизація бізнес-процесу внутрішніх перевірок фінансових транзакцій, що підлягають під фінансовий моніторинг; автоматизована розробка структури шаблонів вхідної та вихідної документації, пов’язаної із ідентифікацією, верифікацією та відеоверифікацією осіб, які проводять фінансові транзакції, що підлягають фінансовому моніторингу; автоматизована розробка структури баз даних для внутрішнього фінансового моніторингу банків як схему даних з урахуванням ключових елементів та взаємозв’язків, структури нормативно-довідкової інформації, що є необхідною для проведення основних процедур фінансового моніторингу; автоматизоване розроблення структури шаблонів вхідних та вихідних документів, повідомлень, пов’язаних із початком перевірок та отриманими результатами моніторингу; та ін.

- бізнес-моделі процесів проведення фінансового моніторингу банків та інших економічних агентів – комплексна модель, що включає ряд етапі, на кожному з яких використовується певне моделювання: модель бізнес-процесу автоматизованого внутрішнього моніторингу, що реалізуються безпосередньо самими економічними агентами; модель бізнес-процесу автоматизованого здійснення моніторингу платежів, що проводить фільтрацію фінансових операцій без наявного фінансового підтвердження джерела коштів через систему Інтернет-Клієнт-Банк; бізнес-модель автоматизованого проведення внутрішньобанківського фінансового моніторингу операцій для визначення ризику, що пов'язаний із використанням послуг банку для відмивання коштів;
- та ін.

В загальному розумінні категорія кібербезпека представляє собою комплекс оптимальних заходів, стратегій попередження, захисту, мінімізації загроз, ризиків, втрат від впливу та скоєння кіберзлочинів, кібератак, цифрових нападів на фінансову систему та суспільний добробут, нівелювання шкідливих, несприятливих, небезпечних наслідків для громадян, суб’єктів господарювання, економічної системи, ефективного керівництва, розвитку потенціалу правоохоронних та кримінальних органів, інформаційно-просвітницької суспільної діяльності, національного та міжнародного співробітництва.

Основними стратегічними цілями кібербезпеки виділяють: забезпечення безпечності кіберпростору, дієвості кібероборони, ефективної протидії кіберзлочинам, розробка інструментів кібербезпеки, підтримання кіберстійкості, забезпечення надійного кіберзахисту, підтримання кіберготовності до кібератак, забезпечення безпеки цифрового фінансового ринку, забезпечення інтеграції, координації та співробітництва щодо кібербезпеки.

Поставлені вище цілі визначають важливі до виконання задачі кібербезпеки, такі як: удосконалення законодавчої бази щодо збереження електронної інформації, відомостей про рух електронних даних, збирання, перехоплення, акумулювання даних, надання та розкриття відомостей відповідним органам, стосовно арешту комп’ютерної інформації; захист від

несанкціонованого втручання у функціонування автоматизованих систем, комп'ютерної техніки, інформаційних та комп'ютерних мереж, мереж зв'язку; захист від розробки, використання, купівлі-продажу, розповсюдження шкідливих програмних комплексів та технічних винаходів; захист від несанкціонованої купівлі-продажу, поширення таємної інформації та даних з обмеженим правом доступу; захист від несанкціонованих, протиправних дій посадових осіб з відповідною інформацією; захист від неправильної експлуатації автоматизованих систем, комп'ютерної техніки, інформаційних та комп'ютерних мереж, мереж зв'язку; захист від неправильного користування інформаційними ресурсами; захист від порушення та перешкоджання функціонування автоматизованих систем, комп'ютерної техніки, інформаційних та комп'ютерних мереж, мереж зв'язку; боротьба з незаконними, протиправними діями з фінансовими документами, електронними платіжними засобами, електронними коштами, спеціалізованою технікою для їх виготовлення; прозоре, компетентне та результативне розслідування фінансових online-злочинів, шахрайств електронного, дистанційного банкінгу; криміналізація нападів на інформаційні, комп'ютерні системи, дані, бази, нелегального доступу до них, незаконного втручання у їх функціонування, зловживань ними; криміналізація правопорушень авторських прав; криміналізація комп'ютерних підробок; криміналізація правопорушень незаконного змістовного характеру; розвиток, підтримка та розширення міжнародної інтеграції, співробітництва, партнерства шляхом взаємної допомоги, обміну інформацією, розкриття певних даних, підтримки цілодобових інформаційних мереж, видачі злочинців, надання юридичної та правової допомоги, взаємовизнання судових рішень, неофіційно співпраці органів правопорядку країн світу, згоди на спеціалізовані слідчі дії; ін.

Далі слід зазначити основні напрями кібербезпеки, які розподіляються на певні групи в залежності від категорій спрямованості їх дій: згідно кіберзлочинів – боротьба з посяганнями на конфіденційність, тайну, цілісність, недоступність комп'ютерної інформації, систем, мереж (боротьба з незаконним доступом, зломом, перехопленням інформації; боротьба зі злочинним втручанням у

комп’ютерну систему, створенням перепон її функціонуванню; боротьба з протиправним втручанням у відомості, приховуванням, пошкодженням, погіршенням, порушенням, зміною, видаленням, знищенням даних; боротьба із злочинним використанням комп’ютерних систем, технологій); боротьба з незаконним застосуванням комп’ютерної техніки; боротьба з незаконним змістом даних та відомостей; боротьба з посяганнями на авторські та суміжні права на програмне забезпечення, інформаційні ресурси, бази даних, цифрові продукти та послуги; згідно кримінальних кіберзлочинних правопорушень – боротьба з використанням автоматизованих систем, комп’ютерної техніки, інформаційних та комп’ютерних мереж, мереж зв’язку для підготовки, скоєння, приховування кіберзлочинів; боротьба з передачею даних незаконного характеру шляхом використання автоматизованих систем, комп’ютерної техніки, інформаційних та комп’ютерних мереж, мереж зв’язку; боротьба з незаконною господарською діяльністю, нелегальними фінансовими транзакціями, що проводяться з використанням комп’ютерних мереж; згідно мотивації кібершахраїв – боротьба з кібершахрайством, метою якого є привласнення коштів; боротьба з кібершахрайством, метою якого є привласнення інформації; боротьба з кібершахрайством, метою якого є отримання доступу до автоматизованої системи для нанесення збитків, пошкодження, дезорганізації; згідно кіберзлочинів у банківському секторі – боротьба з банкоматним шахрайством (боротьба зі скімингом, тобто встановленням на банкоматах зчитувальних та копіювальних механізмів для отримання пін-кодів, а також інформації з магнітної смуги чи чіпу; боротьба з «білим пластиком», тобто використанням пустого неідентифікованого пластику для дублювання клієнтських карт; боротьба з шахрайством при відміні транзакції, тобто нібито з технічних причин кошти зараховуються назад на карту, але фізично встигають бути вилученими з банкомату; боротьба з кеш-трепінгом, тобто крадіжкою готівки за допомогою додатково встановлених шахраями спеціальних пристроїв вилучення готівки); боротьба з кібершахрайством торгівельно-сервісних мереж (боротьба з використанням викрадених, підроблених електронних платіжних

засобів, в тому числі пластикових карт; боротьба з привласненням шахраями реквізитів платіжних карт; боротьба з умисним дробленням фінансових операцій і проведенням фінансових транзакцій та суми, менші за граничні з уникненням авторизації та ідентифікації; боротьба фіктивними еквайринговими угодами, метою яких є здійснення операцій з використанням викрадених, підроблених платіжних карт); боротьба з інтернет шахрайством (боротьба з привласненням шахраями через інтернет ресурси реквізитів електронних платіжних засобів та проведенням з їх використанням фінансових транзакцій; боротьба з розробкою, створенням програмного забезпечення, призначеного для викрадення реквізитів електронних платіжних засобів); боротьба з шахрайством у системах банківського дистанційного обслуговування (боротьба з відкриттям рахунків для проведення нелегальних безготівкових та готівкових фінансових транзакцій за допомогою web-банкінгу, mobile-банкінгу, інших систем дистанційного обслуговування; боротьба з розробкою та створенням комп'ютерних вірусів з метою заволодіння системою управління комп'ютером інших осіб для здійснення від їх імені несанкціонованих фінансових транзакцій; боротьба із втручанням в роботу систем міжнародних грошових переказів та міжнародних платіжних систем для отримання несанкціонованих переказів із-за кордону); згідно нормативно-правового забезпечення – забезпечення змін у законодавстві щодо посилення відповідальності осіб за скоєння кіберзлочинів; затвердження законодавчим порядком визнання законної сили електронних доказів по кіберзлочинам; визначення чіткої схеми відносин та відповідальності клієнт-банк, відправник отримувач, у разі протиправного списання клієнтських коштів; законодавчо регламентувати ідентифікацію користувачів мережі Інтернет; законодавчо затвердити необхідність відбирати ідентифікаційні дані надавачем Інтернет послуг при заключенні угод на такі послуги; закріплення інтернет-магазинів за конкретними платниками податків; затвердити необхідність забезпечення захисту систем дистанційного обслуговування декількома рівнями захисту – логіни, паролі, смс-повідомлення та ін.; закріпити як обов'язкову безкоштовну послугу – надання надавачами фінансових послуг обов'язкового

онлайн інформування про всі фінансові транзакції та спроби їх провести не залежно від сум та видів транзакцій; зобов'язання банківським установам здійснювати вихідні платежі лише у межах залишку на рахунку; затвердження незмінного ліміту на зняття готівкових коштів з банкоматі в післяопераційний час; обов'язкова сертифікація усіх електронних платіжних засобів; обладнання банкоматної мережі банків антискімінговими засобами.

Моделі кібербезпеки – це комплексні організаційні, технічні, правлінські, контрольні заходи з забезпечення кібербезпеки, а саме: затвердження певних типових правил та схем для ідентифікації типових, нетипових, підозрілих, сумнівних операцій в системі дистанційного обслуговування; затвердження лімітів операцій в системі дистанційного обслуговування та в мережі інтернет; ведення бази підозрілих та сумнівних клієнтів; ведення бази клієнтів «чорного списку»; оформлення клієнтам пластикових карт чіпом, що має вищий рівень захисту; двоканальна аутентифікація; додаткове підтвердження дистанційних платежі через фінансовий номер телефону; використання захищених спеціальних токенів для електронних цифрових підписів співробітників та клієнтів; забезпечення можливості здійснення генерації електронного ключа особисто клієнтом без участі співробітників банківської установи; забезпечення повідомлення клієнтів про всі фінансові операції та спроби їх проведення; прив'язка електронного цифрового підпису до конкретного переліку серійних номерів комп'ютерної техніки; періодичний аналіз трафіку; систематичний огляд банкоматної мережі з метою ідентифікації сторонніх приладів.

Також зазначимо, що розглядаючи одночасно різні об'єкти та системи, варто виділити вагомість поняття конвергенція, яке означає процес знаходження компромісів, поєднання, зближення відмінних понять. А конвергенція систем передбачає злиття систем у єдине нероздільне ціле; процес їх універсалізації, шляхом поєднання спільних елементів, а в результаті збільшення кількості функцій таких систем, їх можливостей та переваг; виконання елементами систем різних, але подібних задач за єдиними принципами для отримання додаткового ефекту. Так, результатами конвергенції визначають формування компромісних

рішень, досягнення рівноважної позиції, спільний розвиток, загальна стійкість та стабілізація.

При чому конвергенція систем може реалізовуватись на основі різних моделей, таких як: ситуаційно-імітаційно-експертне моделювання (заснована на використання декількох типів підмоделей, передбачає мультиаспектний розгляд досліджуваного питання, дозволяє моделювати як реальну ситуацію, так і штучно створену); модель абсолютної конвергенції (зближення та збільшення рівнів розвитку однорідних об’єктів дослідження без введення додаткових умов); модель умовної конвергенції (передбачає від’ємну залежність між середніми темпами зростання за появи контролюючих факторів); модель прямої конвергенції (процес зближення та компромісів на основі наявних традицій, під впливом визначених факторів); модель непрямої конвергенції (процес зближення на основі нових запозичених понять, інтеграцію об’єктів); та ін.

В свою чергу, конвергенція систем фінансового моніторингу і кібербезпеки передбачає розбудову системи фінансового моніторингу для кібернетичних фінансових операцій; забезпечення кіберзахисту фінансових транзакцій банківської системи; підвищення кіберстійкості фінансової системи до відмивання незаконних коштів та фінансування тероризму. Завдяки конвергенції систем фінансового моніторингу і кібербезпеки формуються наступні новітні заходи, що допомагають у профілактиці, боротьбі та прогнозуванні сучасних фінансових та кіберзлочинів: затвердження на законодавчому рівні правил, інструкцій, протоколів, нормативів, вимог, стандартів, важелів, відповідальності, цінової політики, державних компенсаційних програм з питань фінансової кібербезпеки; затвердження обов’язковості проведення самооцінки стану фінансового кіберзахисту банківським установами; заборона чи обмеження використання іноземних програмних комплексів та систем захисту в національній фінансовій системі; цифрова трансформація, а також перехід на сучасну хмарову середу; впровадження засобів інформаційної безпеки даних в банківському секторі; запровадження інструментів зі штучним інтелектом; використання

багаторівневої системи захисту та боротьби з фінансовими кіберзагрозами; використання новітніх програмних комплексів для захисту операційних систем банків; запровадження міжмережевих екранів; впровадження систем виявлення сторонніх вторгнень в автоматизовану банківську систему; забезпечення посиленого захисту в'язку з віддаленими структурними елементами банківських установ; забезпечення посиленої прозорості, ідентифікації та авторизації при роботі дистанційних онлайн сервісів банків; впровадження новітніх розробок автоматизованих систем реагування на інциденти інформаційної, фінансової та кібербезпеки банків; запровадження роботизації виконання чергових банківських процедур у режимі реального часу; протидія соціальній інженерії, психологічному маніпулюванню людьми щодо здійснення неусвідомлених чи протиправних дій; використання послуг антифрода, послуги для боротьби з фінансовим шахрайством; використання способу збагачення заголовку онлайн запитів користувачів web-ресурсів; а ін.

Питання боротьби з відмиванням нелегальних коштів, протидії фінансування тероризму, розповсюдження зброї масового знищення для України та світу буде гострим ще протягом тривалого часу. Поряд з цим не менш актуальною є проблема кібернебезпеки, коли виникає потреба забезпечувати в цьому напрямку конфіденційність, захищеність, цілісність, доступність та автентичність інформаційних ресурсів. Поглиблені дослідження цих двох векторів передбачають узагальнення, структурування теоретичних надбань світової та вітчизняної літератури в частині визначення основних понять, цілей, задач, напрямів та моделей досліджуваних питань, а також розробки авторами власних висновків по зазначеним аспектам. При чому основний акцент дослідження робиться на те, що обидва комплекси заходів, як фінансовий моніторинг, так і кібербезпека, стають одними з головних завдань світового співтовариства, керівництва країн, державних органів, суспільства.

В загальному підсумку, запропонована в роботі конвергенція систем фінансового моніторингу та кібербезпеки, може бути взята за основу, адаптована та пристосована для розв'язання широкого кола питань як економічної та

фінансової безпеки, боротьби з відмивання нелегальних коштів, так і інших проблемних питань фінансового ринку.

1.2 Попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу країн

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

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

У даному контексті виникає потреба оцінити рівень існуючих передумов, сформованих суб’єктами моніторингу та кібербезпеки, до початку імплементації

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

За останнє десятиріччя зросла кількість наукових праць, присвячених актуальним питанням кібербезпеки та її реалізації у фінансово-економічній сфері. Зацікавленість даною тематикою обумовлена потребами практики щодо посилення захисту інформації та знань фінансового характеру. В цьому контексті слід виділити вектор публікацій, які вирішують проблеми, пов’язані із управлінням кібер-ризиками в банківській сфері, що розглядалися такими науковцями, як Скотт Б.Ф. [18], Ан Дж., Дуань Т., Хоу В., Лю Х. [19], Чен Дж., Чжу К., Башар Т. [20] та іншими.

Наступним актуальним напрямом досліджень є вивчення загроз та вразливостей систем кіберзахисту, що можуть виступити слабкими місцями для кіберзлочинців та кібершахраїв. В цій сфері можна виділити праці таких фахівців, як Бердибаєв Р., Гнатюк С., Євченко Ю., Кіщенко В. [21], Комаров М., Давидюк А., Онискова А., Ткаченко В., Гончар С. [22], Уддін М.Х., Алі М.Х., Хасан М.К. [23] та інші. Застосування сучасних технологій, таких як штучний інтелект та блокчейни, є значним блоком наукових досліджень, спрямованих на вирішення проблеми протидії фінансових та кібер-шахрайств. Цей напрям досліджують Коучоро М.К., Содокін К., Коріко М. [24], Карпуніна Є.К., Михайлов А.М., Бондарева Н.А., Любименко О.А., Федотова Є.В. [25], Мхланга Д. [26], Сміт К.Дж., Діллон Г. [27], Картер Д. [28] та інші.

Правові та організаційні аспекти, пов’язані із здійсненням процесів кібербезпеки та фінансового моніторингу, є також напрямом наукових

досліджень, де розкриваються питання: забезпечення конфіденційності фінансової інформації в праці К. Атта Уль Хак [29]; правових аспектів технологічної нейтральності в статті Г. Гальяні [30]; системного поєднання сфери освіти, технологій та політики для підвищення ефективності системи кібербезпеки в роботі М. Доусон [31]; вимог до організації та функціонування відповідних підрозділів кібербезпеки у фінансовій сфері Т.П. Августінос [32]; тощо. Не дивлячись на широко коло проблем, які вирішуються науковцями – фахівцями в сфері кібербезпеки та фінансового моніторингу, питання конвергенції цих двох систем є ще не розкритим, що потребує подальших досліджень.

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

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

Другу групу показників було сформовано з урахуванням існуючих можливостей країн світу щодо формування системи фінансового моніторингу, спроможної протидіяти процесам легалізації кримінальних доходів та фінансування тероризму. Дані було узято з офіційного джерела Світового банку. Сюди увійшли 7 індексів: індекс політичної стабільності (Political Stability

Index); індекс ефективності уряду (Government Effectiveness Index); легкість ведення бізнесу (Ease of Doing Business); індекс злочинності (Crime Index); індекс сприйняття корупції (Corruption Perceptions Index); глобальний індекс тероризму (Global Terrorism Index); індекс фінансової таємниці (Financial Secrece Index).

Проведемо за допомогою аналітичного пакету "STATISTICA" статистичний аналіз обраних груп показників, який полягає у визначенні базових статистичних характеристик: середнього значення, медіани, модального значення, мінімального та максимального рівнів, стандартного відхилення та коефіцієнта варіації. Так, його результати в розрізі показників, що ідентифікують систему кібербезпеки, представлені на рисунку 1.1.

	Descriptive Statistics (Spreadsheet1.sta)						
Variable	Mean	Median	Mode	Minimum	Maximum	Std.Dev.	Coef.Var.
Global Cybersecurity Index	66,0789	75,0000	89,0000	2,0000	93,0000	24,2897	36,7587
ICT Development Index	65,0789	69,5000	72,0000	0,0000	90,0000	18,0715	27,7686
Networked Readiness Index	61,8947	63,5000	63,0000	0,0000	86,0000	19,9048	32,1591
National Cyber Security Index	54,2550	57,1400	57,1400	3,9000	96,1000	23,1957	42,7531
Digital Development Level	65,5761	66,8150	58,0000	28,1000	85,1300	13,9731	21,3082

Рисунок 1.1 – Описові статистики групи показників кібербезпеки

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

Переходячи до аналізу модального значення в розрізі показників (див. рис. 1.1), можна стверджувати, що найбільш поширене значення, яке є найбільшим і незначним чином відрізняється від максимуму, сягає рівня 89 і належить глобальному індексу кібербезпеки. Це свідчить про досить високий рівень даного показника для більшості країн світу. В розрізі інших чотирьох показників кібербезпеки модальне значення приймає значення від 57 до 72 і в усіх випадках перевищує відповідні середні рівні.

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

Проведемо аналіз базових статистик в розрізі показників, які ідентифікують спроможність країн протидіяти процесам легалізації кримінальних доходів. Його результати представлені на рисунку 1.2.

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

Рисунок 1.2 – Описові статистики показників, які ідентифікують спроможність країн протидіяти процесам легалізації кримінальних доходів

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

Отримані модальні значення (див. рис. 1.2) свідчать, що найпоширене значення спостерігається лише за індексом політичної стабільності та глобальним індексом тероризму. В розрізі інших п’яти показників виявлено досить різнорідні значення характеристик спроможності країн протидіяти фінансовим злочинам.

Для виявлення причинно-наслідкових зв’язків між групами показників кібербезпеки та спроможності країн протидіяти процесам легалізації кримінальних доходів проведено канонічний аналіз із використанням аналітичного пакету “STATISTICA”. Його результати представлені на рисунку 1.3.

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

Рисунок 1.3 – Результати канонічного аналізу причинно-наслідкових зв’язків між групами показників кібербезпеки та спроможності країн протидіяти фінансовим злочинам

Так, виявлено, що варіативність у множині показників кібербезпеки пояснюється на 65,51% множиною показників спроможності країн протидіяти процесам легалізації кримінальних доходів. В той же час, варіативність у множині показників спроможності країн протидіяти фінансовим загрозам лише на 49,39% пояснюється множиною показників кібербезпеки. Таким чином, результати виявлення причинно-наслідкових зв’язків за допомогою канонічного аналізу дозволяють констатувати, що показники спроможності країн протидіяти процесам легалізації кримінальних доходів виступають причиною, а множина показників кібербезпеки, відповідно, наслідком.

Крім того, аналіз рисунку 1.3 свідчить також про те, що частка дисперсії (варіативності), яка пояснюється множиною показників кібербезпеки складає 100%, а частка дисперсії (варіативності), яка пояснюється множиною показників спроможності країн протидіяти фінансовим загрозам приймає значення 86,67%.

Це говорить про те, що у першому випадку 100% дисперсії будуть пояснювати усі вилучені корені, у другому випадку – на 86,67%.

Канонічна кореляція R=0,91 (див. рис. 1.3), яка відповідає кореляції між першими канонічними змінними, дорівнює максимальному канонічному кореню. Її значення свідчить про наявність сильної лінійної залежності між групами змінних. Статистична значущість коефіцієнта канонічної кореляції підтверджується високим значеннями Хі-квадрату (196,5) та рівнем ймовірності менше ніж 0,05 (p=0,00).

Візуалізацію шматково-лінійного графіку спадаючих власних значень, що відповідають канонічним кореням, представимо на рисунку 1.4, а результати тестів Хі-квадрату для статистичної значущості канонічних коренів –на рисунку 1.5.

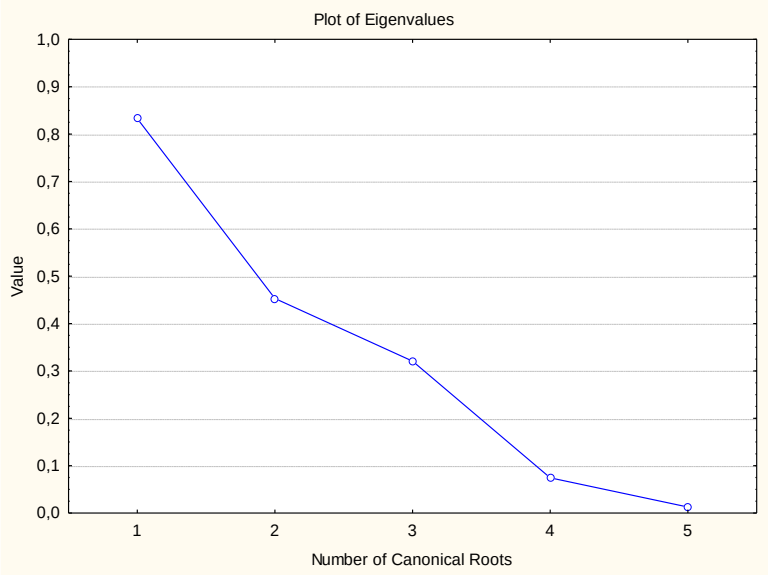

Рисунок 1.4 – Шматково-лінійний графік спадаючих власних значень, що відповідають канонічним кореням

Отже, на основі рисунків 1.4 і 1.5 можна зробити висновок, що статистично значущими є перші три канонічні корені, оскільки p-значення для них не перевищують гранично допустимого рівня 0,05. Саме зазначені канонічні корені пропонується розглядати на наступному етапі при оптимізації вхідного масиву даних.

	Chi-Square Tests with Successive Roots Removed (Spreadshee					
Root Removed	Canonicl R	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0,91258	0,832818	196,4981	35	0,00000(	0,05677
1	0,67304	0,452991	73,9741	24	0,000001	0,33962
2	0,56621	0,32059	32,648	15	0,00526	0,62087
3	0,27271	0,07437	6,1705	8	0,628141	0,91385
4	0,11276(	0,01271	0,8765	3	0,83108	0,98728

Рисунок 1.5 – Тести Хі-квадрат для статистичної значущості канонічних коренів

З метою оптимізації масиву вхідних даних проведемо із використанням аналітичного пакету “STATISTICA” кореляційний аналіз двох груп показників кібербезпеки та спроможності країн протидіяти фінансовим загрозам. Розглянемо спочатку кореляційну матрицю лівої множини – множини показників кібербезпеки (рисунок 1.6). За результатами аналізу можна зробити висновок про наявність значної кореляційної залежності між такими показниками як індекс розвитку інформаційно-комунікаційних технологій та рівень цифрового розвитку. Підтвердженням даного факту виступає високе значення коефіцієнту кореляції, що дорівнює 0,96. Для оптимізації множини вхідних показників кібербезпеки рекомендується один із колінеарних індикаторів видалити з подальших обчислень.

	Correlations, left set (Spreadsheet1.sta)				
Root Removed	Global Cybersecurity Index	ICT Development Index	Networked Readiness Index	National Cyber Security Index	Digital Development Level
Global Cybersecurity Index	1,00000(	0,53583	0,71135	0,70943	0,57919
ICT Development Index	0,53583	1,00000(	0,58341	0,64298	0,96073
Networked Readiness Index	0,71135	0,58341	1,00000(	0,68127	0,64674
National Cyber Security Index	0,70943	0,64298	0,68127	1,00000(	0,65470
Digital Development Level	0,57919	0,96073	0,64674	0,65470	1,00000(

Рисунок 1.6 – Кореляційна матриця лівої множини – множини показників кібербезпеки

Для прийняття рішення щодо показника, який варто залишити в масиві вхідних даних, а який треба видалити, розглянемо отриману в результаті

проведення канонічного аналізу факторну структуру за першими трьома статистично значущими канонічними коренями (рисунок 1.7).

Variable	Factor Structure, left set (Spreadsheet1.sta)				
	Root 1	Root 2	Root 3	Root 4	Root 5
Global Cybersecurity Index	0,79354	-0,57377	0,03246	-0,19620	-0,03894
ICT Development Index	0,87121	0,17211	-0,39099	0,23550	-0,05499
Networked Readiness Index	0,80257	-0,24082	0,37935	0,35375	0,16974
National Cyber Security Index	0,72570	-0,29619	-0,21889	0,03413	0,58011
Digital Development Level	0,94284	0,25738	-0,19766	0,07562	0,00148

Рисунок 1.7 – Факторна структура лівої множини – множини показників кібербезпеки

Аналіз рисунку 1.7 дозволяє констатувати, що більш значущий вплив здійснює показник рівень цифрового розвитку (0,9428, 0,2573, -0,1977), а ніж індекс розвитку інформаційно-комунікаційних технологій (0,8712, 0,1721, -0,3901) . Відповідно, пропонується залишити індекс рівня цифрового розвитку для проведення подальших досліджень щодо конвергенції систем фінансового моніторингу та кібербезпеки.

Перейдемо до розгляду кореляційної матриці правої множини –показників спроможності країн протидіяти фінансовим злочинам (рисунок 1.8).

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

Рисунок 1.8 – Кореляційна матриця правої множини – множини показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам

За отриманими результатами аналізу можна зробити висновок про наявність значної кореляційної залежності між такими двома показниками, як індекс ефективності уряду та індекс сприйняття корупції. Підтвердженням

даного факту виступає високе значення коефіцієнту кореляції, що дорівнює 0,904. Для оптимізації вхідних показників в розрізі спроможності країн протидіяти процесам легалізації кримінальних доходів рекомендується один із колінеарних індикаторів видалити для подальших досліджень.

Для прийняття рішення щодо показника, який варто залишити в масиві вхідних даних, а який треба видалити, розглянемо факторну структуру за статистично значущими канонічними коренями, отриманими в результаті проведення канонічного аналізу (рисунок 1.9).

	Factor Structure, right set (Spreadsheet1.sta)				
Variable	Root 1	Root 2	Root 3	Root 4	Root 5
Political stability index	0,43140(	0,61309[	-0,53189[	0,11795[	0,02536[
Government effectiveness index	0,95447[	0,19149[	-0,18007[	0,04055[	-0,10269[
Ease of doing business	0,85417[	-0,21703[	-0,24630[	0,10144[	0,26600[
Crime Index	-0,55691[	0,01299[	0,67239[	-0,11977[	-0,18779[
Corruption Perceptions Index	0,81616[	0,50482[	-0,22105[	-0,12459[	-0,00193[
Global Terrorism Index	0,14948[	-0,62097[	0,32072[	-0,60256[	-0,27448[
Financial Secrece Index	0,50548[	0,08991[	0,32266[	-0,31996[	0,28286[

Рисунок 1.9 – Факторна структура правої множини – множини показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам

Результати аналізу, представленого на рисунку 1.9, показують, що більш значущий вплив здійснює показник індекс ефективності уряду (0,9545 за першим канонічним коренем), ніж індекс сприйняття корупції (0,8162 за першим канонічним коренем), який і пропонується залишити для проведення подальших досліджень.

Процес конвергенції систем фінансового моніторингу та кібербезпеки є одним з напрямів формування ефективної системи протидії фінансовим та кіберзлочинам в країні. Його реалізація потребує зваженого підходу, оскільки передбачається складна та системна інтеграція багатьох процесів, функцій та механізмів. Тому необхідно оцінити умови, сформовані в країні, які характеризують поточний рівень її кібербезпеки та фінансового моніторингу. Відповідно в даному дослідженні було сформовано дві групи показників, які характеризують для 76 країн світу рівень розвитку окреслених систем за 2018

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

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

Пункт 1.2 було виконано із використанням матеріалів публікацій виконавців [33].

1.3 Побудова фазових портретів «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» системи протидії фінансовим та кібер-шахрайствам

Для оцінювання зрілості діючої системи протидії фінансовим та кібер-шахрайствам та побудова фазових портретів їх «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» побудуємо інтегральний індекс кібербезпеки на основі застосування методу згортки Сундаровського. Зведення

індикативних показників до єдиного інтегрального індексу кібербезпеки за допомогою методики Сундаровського передбачає застосування наступної формули (1.1):

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - a_i^*\right]^{\alpha} \tag{1.1}$$

де IS_j – інтегральний індекс кібербезпеки для j-ої країни;

a_{ij} – фактичне значення і-го показника кібербезпеки для j-ої країни;

a_i^*- рівноважне значення і-го показника кібербезпеки для розглянутої множини країн;

α – константа, показник ступеня.

З метою практичного застосування формули (1.1) для обчислення інтегрального індексу кібербезпеки введемо наступні припущення:

1) в якості рівноважних рівнів складових індикаторів оберемо абсолютне значення різниці середньоквадратичного відхилення та мінімально допустимого рівня:

$$a_i^* = \left|\min_j a_{ij} - \sigma_i\right| = \left|\min_j a_{ij} - \sqrt{\frac{\sum_{j=1}^{m}\left(a_{ij} - \overline{a_\iota}\right)}{n-1}}\right| \tag{1.2}$$

де σ_i – середньоквадратичне відхилення і-го показника кібербезпеки;

$\overline{a_\iota}$ – середнє арифметичне значення і-го показника кібербезпеки;

2) в якості постійного значення показника ступеня функціональної залежності (1.1) оберемо співвідношення одиничного значення та кількості релевантних показників характеристики кібербезпеки. Враховуючи зазначені припущення, формула (1.1) набуває вигляду (1.3):

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - \left| \min_j a_{ij} - \sqrt{\frac{\sum_{j=1}^{m} (a_{ij} - \bar{a}_\iota)}{n-1}} \right| \right]^{1/n} \quad (1.3)$$

де n - кількість релевантних показників характеристики кібербезпеки.

Проведемо обчислення за допомогою формули (1.3), представивши поетапно проведені розрахунки в таблиці 1.1: рядок «Рівноважні значення» в розрізі 4 показників кібербезпеки – абсолютні значення $\left| \min_j a_{ij} - \sigma_i \right|$; значення на перетині рядків (країн) та граф (показників кібербезпеки) – значення $\left[a_{ij} - a_i^* \right]$; значення граф IS – результативні величини інтегрального індексу кібербезпеки, визначені методом Сундаровського, в розрізі кожної країни із розглянутої множини 76 країн світу.

Таблиця 1.1 – Проміжні та кінцеві розрахунки інтегрального індексу кібербезпеки, визначені методом Сундаровського, за 76 країнами світу

Country	Global Cybersecurity Index	Networked Readiness Index	National Cyber Security Index	Digital Development Level	IS	Country	Global Cybersecurity Index	Networked Readiness Index	National Cyber Security Index	Digital Development Level	IS
Рівноважні значення	22,29	19,90	19,30	14,13							
Australia	2,86	2,77	2,52	2,85	57,03	Liberia	1,07	2,12	0,66	2,26	3,33
Austria	2,79	2,75	2,65	2,83	57,70	Lithuania	2,88	2,66	2,88	2,75	60,61
Bahrain	2,46	2,70	1,61	2,79	29,76	Luxembourg	2,86	2,80	2,56	2,88	58,97
Barbados	1,52	2,11	1,39	2,77	12,32	Malaysia	2,86	2,66	2,70	2,70	55,41
Belgium	2,77	2,75	2,85	2,82	61,32	Malta	2,25	2,65	2,37	2,78	39,17
Bolivia	1,70	2,28	1,75	2,36	15,94	Mauritius	2,85	2,56	2,32	2,61	44,16
Botswana	2,16	2,34	1,29	2,41	15,75	Mexico	2,53	2,47	2,03	2,52	31,91
Brazil	2,44	2,47	2,29	2,59	35,78	Montenegro	2,54	2,53	1,95	2,64	33,17
Brunei Darussalam	2,51	2,11	1,99	2,70	28,56	Netherlands	2,86	2,82	2,81	2,89	65,46
Bulgaria	2,66	2,50	2,39	2,65	42,09	New Zealand	2,74	2,77	2,46	2,86	53,48
Canada	2,86	2,78	2,48	2,84	55,98	North Macedonia	2,76	2,56	2,14	2,62	39,64
Chile	2,16	2,61	2,48	2,68	37,39	Norway	2,86	2,82	2,56	2,89	59,60
China	2,79	2,52	1,99	2,57	36,02	Panama	1,96	2,53	2,32	2,53	29,08
Costa Rica	0,73	2,58	2,41	2,66	12,15	Paraguay	2,48	2,32	2,48	2,36	33,70
Croatia	2,80	2,53	2,83	2,70	54,06	Philippines	2,54	2,47	1,91	2,48	29,63
Cyprus	2,56	2,61	2,17	2,75	39,86	Poland	2,78	2,58	2,67	2,69	51,48
Czech Republic	2,43	2,62	2,92	2,73	50,66	Portugal	2,71	2,66	2,69	2,74	53,06
Denmark	2,81	2,78	2,81	2,89	63,60	Romania	2,43	2,50	2,69	2,63	42,83

Продовження таблиці 1.1

Country	Global Cybersecurity	Networked Readiness Index	National Cyber Security Index	Digital Development Level	IS	Country	Global Cybersecurity	Networked Readiness Index	National Cyber Security Index	Digital Development Level	IS
Dominica	2,12	2,11	1,98	2,56	22,71	Russian Federation	2,80	2,58	2,60	2,70	50,74
Dominican Republic	2,13	2,36	2,17	2,42	26,45	Saudi Arabia	2,85	2,65	2,50	2,70	50,99
Estonia	2,88	2,75	2,91	2,84	65,41	Seychelles	1,39	2,47	1,73	2,51	14,84
Finland	2,83	2,85	2,81	2,87	65,08	Singapore	2,87	2,85	2,80	2,88	65,94
France	2,89	2,74	2,83	2,84	63,45	Slovakia	2,67	2,56	2,78	2,69	51,23
Germany	2,81	2,78	2,80	2,87	62,90	Slovenia	2,63	2,62	2,48	2,74	46,79
Ghana	2,16	2,34	1,86	2,36	22,17	South Africa	2,56	2,52	1,68	2,53	27,30
Greece	2,35	2,50	2,96	2,68	46,64	Spain	2,87	2,65	2,88	2,77	60,68
Grenada	1,70	2,11	1,50	2,57	13,80	Sweden	2,77	2,82	2,48	2,89	55,84
Guatemala	1,28	2,34	1,75	2,29	12,02	Switzerland	2,74	2,82	2,75	2,90	61,78
Hungary	2,77	2,56	2,60	2,68	49,49	Tanzania	2,54	2,14	1,58	1,99	17,16
Iceland	2,18	2,77	2,29	2,89	40,08	Thailand	2,76	2,52	2,20	2,58	39,41
India	2,66	2,42	2,52	2,30	37,28	Trinidad and Tobago	1,35	2,50	1,10	2,60	9,65
Indonesia	2,73	2,47	2,11	2,45	34,80	Turkey	2,81	2,56	2,44	2,63	46,17
Ireland	2,73	2,74	2,58	2,83	54,54	Ukraine	2,57	2,52	2,58	2,58	43,00
Israel	2,73	2,75	2,60	2,83	55,18	United Kingdom	2,90	2,80	2,77	2,89	64,85
Italy	2,80	2,56	2,75	2,69	53,19	United States	2,90	2,82	2,78	2,87	65,35
Japan	2,85	2,78	2,56	2,87	58,31	Uruguay	2,60	2,58	2,32	2,71	42,02
Kenya	2,69	2,42	1,99	2,29	29,73	Vanuatu	1,87	2,11	1,73	1,93	13,21
Latvia	2,69	2,65	2,69	2,74	52,54	Venezuela	1,89	2,32	1,91	2,45	20,47

Визначення релевантних показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам за допомогою методу сигма-обмеженої параметризації та Парето-оптимізації. Для реалізації даного етапу використовується інструментарій Statistics, Advanced Linear/Nonlinear Models, GRM Results. В якості результативної ознаки пропонується обрати інтегральний індекс кібербезпеки, визначений методом Сундаровського, в якості факторів впливу – відповідно, показники характеристики спроможності країн протидіяти фінансовим і кіберзагрозам. Представимо отримані результати на рисунку 1.10.

На основі даних рисунку 1.10, в якій приведені одномірні результати для оцінки ступеня та характеру взаємозв’язку відгука та впливів, можна стверджувати, що статистично значущими виступають лише два впливи: індекс ефективності уряду та легкість ведення бізнесу, оскільки рівні значущості p критерія Фішера для них менше 0,05.

Effect	Univariate Tests of Significance foIS (Spreadsheet1.sta) Sigma-restricted parameterization Effective hypothesis decomposition SS	Degr. of Freedom	MS	F	p
Intercept	15,932	1	15,932	0,19911	0,656838
Political stability index	60,262	1	60,262	0,75310	0,388504
Government effectiveness index	651,476	1	651,476	8,14157	0,005706
Ease of doing business	1068,591	1	1068,591	13,3543(	0,000499
Crime Index	197,796	1	197,796	2,47187	0,120474
Global Terrorism Index	185,399	1	185,399	2,31695	0,132540
Financial Secrece Index	63,668	1	63,668	0,79566	0,375494
Error	5521,278	69	80,019		

Рисунок 1.10 - Одномірний тест значущості впливу показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам на інтегральний індекс кібербезпеки, визначений методом Сундаровського

Найбільший вклад в загальну модель вносить показник легкість ведення бізнесу, оскільки сума квадратів відхилень SS, яка приймає значення 1068,59, має найбільше значення, а p-значення приймає найменше значення 0,000499. Наступним статистично значущим впливом виступає індекс ефективності уряду, для якого SS=651.48, а p-рівень 0,0057. Наступним за пріоритетністю показником характеристики спроможності країн протидіяти фінансовим і кіберзагрозам виступає індекс злочинності, хоча для даного показника p-рівень приймає значення 0,12. Візуальним підтвердженням значущості розглянутих факторів виступає діаграма Парето t-значень значущості впливу показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам на інтегральний індекс кібербезпеки, визначений методом Сундаровського (рисунок 1.11).

Представлена на рисунку 1.11 діаграма Парето дозволяє не просто визначити статистично значущі впливи (регресори) інтегрального індексу кібербезпеки, визначеного методом Сундаровського, але й впорядкувати їх від найбільшого на найменшого впливу.

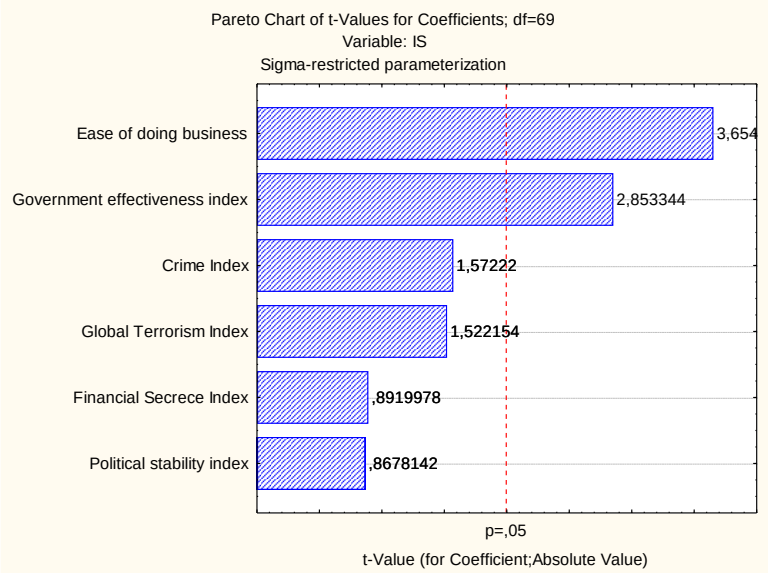

Рисунок 1.11 - Діаграма Парето t-значень значущості впливу показників характеристики спроможності країн протидіяти фінансовим і кіберзагрозам на інтегральний індекс кібербезпеки, визначений методом Сундаровського

Даний статистичний інструментарій дозволяє графічно проінтерпретувати правило 80 на 20, виділяючи 80% впливових факторів зовнішнього середовища, зокрема: індекс ефективності уряду; легкість ведення бізнесу; індекс злочинності, які і виступають релевантними і пропонується обрати для проведення подальшого дослідження.

Побудова нелінійної регресії з покроковим виключенням залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності на основі комбінації логарифмічної та квадратичної функцій, та мультиплікативної залежності трьох показників з метою подальшого проведення біфуркаційного аналізу зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазових портретів їх «зрілості» та «релаксаційних коливань втрати стійкості».

Для реалізації даного етапу пропонується скористатись можливостями програмних пакетів Statistica (Statistics/Advanced Linear/Nonlinear Models/Fixed Nonlinear Regression) та MS Excel (Аналіз даних/Регресія).

Для реалізації даного етапу виникає необхідність визначення специфікації нелінійної регресійної залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, для чого скористаємось можливостями програмного пакетіву Statistica, зокрема інструментарію Fixed Nonlinear Regression, який за допомогою методу покрокового включення дозволяє констатувати наявність статистично значущої залежності у вигляді квадратного кореня для індексу ефективності уряду, логарифмічної залежності для показника легкість ведення бізнесу, квадратичної залежності для показника індекс злочинності (рисунок 1.12). В розрізі індексу ефективності уряду, у зв'язку із наявністю від'ємних значень вхідної статистичної бази, пропонується розглянути залежність інтегрального індексу кібербезпеки від даного показника лише у складі мультиплікативної залежності.

	Regression Summary for Dependent VariableS (Spreadsheet1.sta) R= ,80929115 R?= ,65495216 Adjusted R?= ,62891081 F(4,53)=25,150 p<,00000 Std.Error of estimate: 9,2027					
N=58	Beta	Std.Err. of Beta	B	Std.Err. of B	t(53)	p-level
Intercept			-229,789	67,41833	-3,4084(	0,001255
LN-V9	0,421814	0,111687	61,729	16,34451	3,77675	0,000404
SQRV8	0,401105	0,126867	17,088	5,40484	3,16163	0,002595
V10**2	-0,187681	0,08862(	-0,003	0,00128	-2,11782	0,03889(
1/V8	0,150132	0,093801	0,172	0,10727	1,60054	0,115423

Рисунок 1.12 – Результати регресійної статистики залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності

Враховуючи результати специфікації залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності як логарифмічної, квадратичної функцій та мультиплікативної залежності трьох показників, на наступному другому кроці даного етапу проведемо формалізацію зазначеної нелінійної залежності. Так, скористаємось можливостями MS Excel (Аналіз даних/Регресія), обираючи в

якості змінних ln(EDI), CI^2, GEI*EDI*CI. Представимо отримані результати у вигляді таблиці 1.2.

Таблиця 1.2 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності

Показники	Коефіцієнти	Стандартна похибка	t-статистика	P-Значення	Нижні 95%	Верхні 95%
Y-перетин	-108,69291	56,58893	-1,92074	0,05872	-221,50089	4,11507
ln(EDI)	35,37739	13,25911	2,66816	0,00942	8,94585	61,80893
CI^2	-0,00188	0,00117	-1,60802	0,11221	-0,00420	0,00045
GEI*EDI*CI	0,00277	0,00077	3,58477	0,00061	0,00123	0,00432

На основі даних таблиці 1.2, побудуємо регресійну модель у вигляді формули (1.4):

$$IS = -108.69 + 35.3774 \cdot \ln(EDI) - 0.00188 \cdot CI^2 + 0.00277 \cdot GEI \cdot EDI \cdot CI \qquad (1.4)$$

де IS – інтегральний індекс кібербезпеки;

GEI - індекс ефективності уряду,

EDI – легкість ведення бізнесу,

CI - індекс злочинності.

Статистичну значущість показників ln(EDI) та GEI*EDI*CI підтверджено з рівнем p менше рівня 0,05 та показника CI^2 з рівнем p=0,11. Коефіцієнт детермінації для даної моделі складає 62,73%, фактичне значення критерію Фішера на рівні 40,40 перевищує критично допустимий рівень.

Проведення біфуркаційного аналізу зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазових портретів їх «зрілості» та «релаксаційних коливань втрати стійкості».

Для реалізації даного етапу виникає необхідність попереднього здійснення проміжних обчислень за допомогою застосування апарату диференціального

числення, що включає визначення часткових похідних функції залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, формування системи диференційних рівнянь, які виступають основою подальшого дослідження динамічної стійкості розглянутої системи (формули 1.5-1.8). Для реалізації даного етапу пропонується застосування пакету прикладних програм MathCAD.

Основою подальшого дослідження динамічної стійкості системи протидії фінансовим та кібершахрайствам та побудові фазових портретів їх «зрілості» та «релаксаційних коливань втрати стійкості» виступає нелінійна функція (1.5):

$$f(gei, edi, ci) := -108.693 + 35.37739\ln(edi) - 0.00188ci^2 + 0.002774gei \cdot edi \cdot ci \tag{1.5}$$

На основі розглянутої функції (1.5), змоделюємо систему диференціальні рівнянь, які характеризують поводження динамічної системи протидії фінансовим та кібершахрайствам:

$$\frac{d}{dgei} f(gei, edi, ci) \rightarrow 0.002774ci \cdot edi \tag{1.6}$$

$$\frac{d}{dedi} f(gei, edi, ci) \rightarrow \frac{35.37739}{edi} + 0.002774ci \cdot gei$$

$$\frac{d}{dci} f(gei, edi, ci) \rightarrow -0.00376ci + 0.002774edi \cdot gei$$

Представлені три диференційні рівняння (1.6) дозволяють встановити взаємозв'язки між змінними GEI (індекс ефективності уряду), EDI (легкість ведення бізнесу), CI (індекс злочинності) та їх першими частковими похідними $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci)$.

Ґрунтуючись на нелінійному підході, який лежить в основі теорії біфуркації, побудуємо «фазові портрети» показника інтегральний індекс кібербезпеки у вигляді відображення фазових траєкторій як проекцій на попарно

розглянуті площини: індекс ефективності уряду - легкість ведення бізнесу, легкість ведення бізнесу - індекс злочинності, індекс ефективності уряду - індекс злочинності. Побудуємо фазові портрети «зрілості» та «релаксаційних коливань втрати стійкості» системи протидії фінансовим та кібершахрайствам на базі системи диференційних рівнянь (1.6) на основі застосування математичного пакету програмного забезпечення математичного аналізу MathCad:

$$\begin{aligned}
&Faza(gei0, edi0, ci0, dt, N) := \\
&\left|\begin{array}{l}
\left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
\text{for } k \in 0..N \\
\quad \left|\begin{array}{l}
fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
gei_{k+1} \leftarrow \left[gei_k + dt\cdot\left(0.002774ci_k\cdot edi_k\right)\right] \\
edi_{k+1} \leftarrow \left[edi_k + dt\cdot\left(\frac{35.37739}{edi_k} + 0.002774ci_k\cdot gei_k\right)\right] \\
ci_{k+1} \leftarrow \left[ci_k + dt\cdot\left(-0.00376ci_k + 0.002774edi_k\cdot gei_k\right)\right]
\end{array}\right. \\
(gei \quad edi \quad ci)
\end{array}\right.
\end{aligned} \tag{1.7}$$

З метою надання візуалізації представленого за допомогою формули (1.7) фазового портрету системи протидії фінансовим та кібершахрайствам та подальшої ідентифікації його типу як однієї із можливих альтернатив – різновидів у вигляді сідла, вузла чи фокуса, розглянемо різні варіанти можливих значень як факторів (індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності), так і значення функції, яка описує інтегральний індекс кібербезпеки із заданим рівнем точності на основі зазначеній кількості точок реалізації:

$$\begin{aligned}
(gei1 \quad edi1 \quad ci1) &:= Faza(1.6, 80, 42, 0.01, 100) \\
(gei2 \quad edi2 \quad ci2) &:= Faza(1.45, 78, 20, 0.01, 100) \\
(gei3 \quad edi3 \quad ci3) &:= Faza(0.18, 68, 36, 0.01, 100) \\
(gei4 \quad edi4 \quad ci4) &:= Faza(0.43, 56, 51, 0.01, 100) \\
(gei5 \quad edi5 \quad ci5) &:= Faza(-0.32, 50, 52, 0.01, 100) \\
(gei6 \quad edi6 \quad ci6) &:= Faza(-0.45, 57, 70, 0.01, 100)
\end{aligned} \tag{1.8}$$

Таким чином, підставляючи фактичні значення вхідних даних (формули 1.8) у співвідношення, які дозволяють формалізувати фазові портрети (1.7), зобразимо для прикладу (перше співвідношення формул (1.8)) нелінійну залежність інтегрального індексу кібербезпеки від релеванитиних факторів у площинах «індекс ефективності уряду - легкість ведення бізнесу» (лівий фрагмент рисунку 1.13) та «легкість ведення бізнесу - індекс злочинності» (правий фрагмент рисунку 1.13).

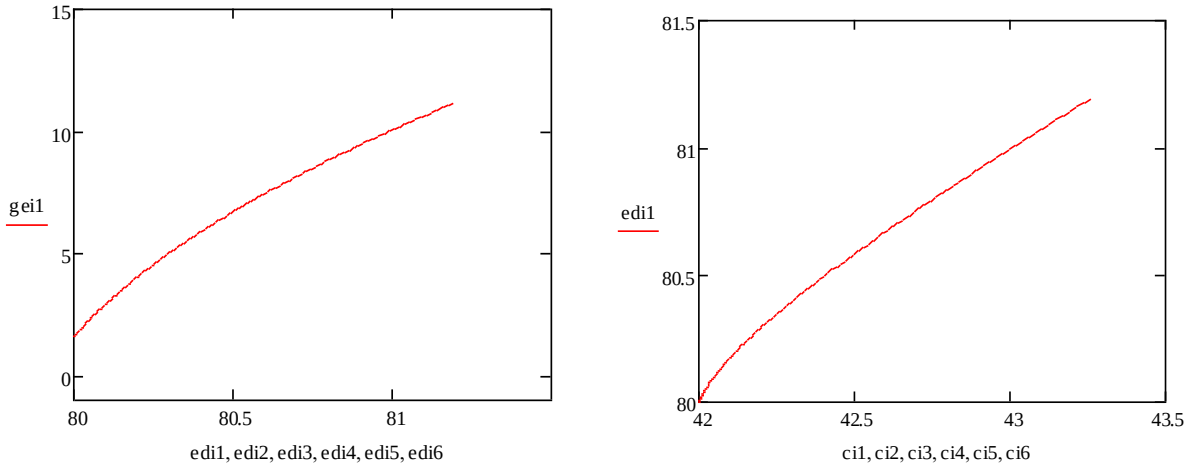

Рисунок 1.13 – Криві нелінійної залежності інтегрального індексу кібербезпеки від релеванитиних факторів у площинах «індекс ефективності уряду - легкість ведення бізнесу» (лівий фрагмент) та «легкість ведення бізнесу - індекс злочинності» (правий фрагмент)

Проведемо дослідження фазового портрету динамічної системи протидії фінансовим та кібершахрайствам на всій множині значень вхідних показників (формули (1.8)). Розглянемо спочатку фрагмент фазового портрету даної системи протидії фінансовим та кібершахрайствам в розрізі площини «індекс ефективності уряду - легкість ведення бізнесу» (рисунок 1.14). Даний «фазовий портрет» демонструє тип біфуркації «нестійкий фокус». Даний тип біфуркації свідчить про нестійкий стан системи, тобто при суттєвій зміні одного параметра і фіксованому значенні іншого параметра розглянута система знаходиться в нерівноважному стані.

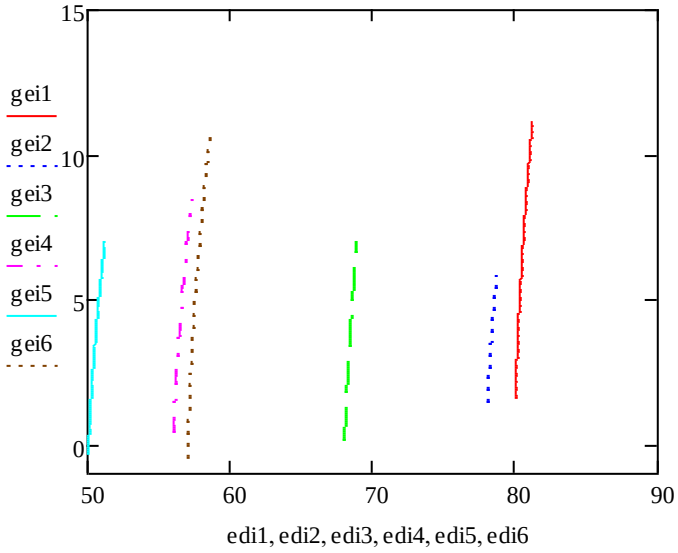

Рисунок 1.14 – Фазовий портрет «нестійкий фокус» системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «(індекс ефективності уряду - легкість ведення бізнесу»

Переходячи до розгляду фрагменту фазового портрету динамічної системи протидії фінансовим та кібершахрайствам, в розрізі площини «легкість ведення бізнесу - індекс злочинності» (рисунок 1.15) спостерігаємо, що вона знаходиться в нерівноважному стані, який характеризується як «нестійкий фокус».

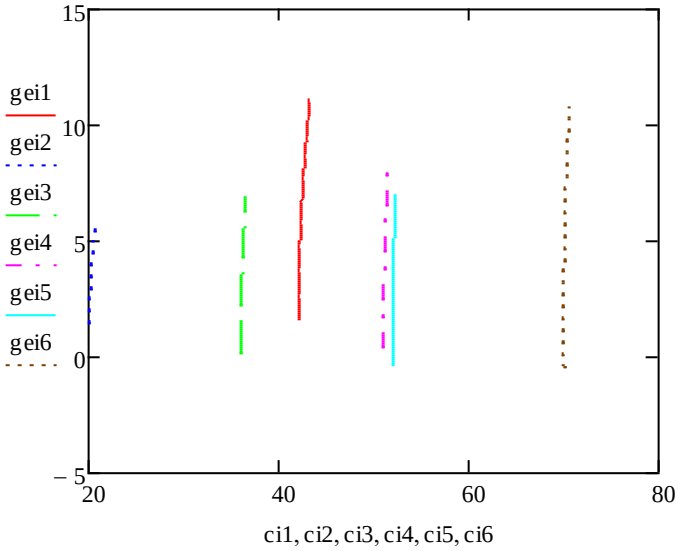

Рисунок 1.15 – Фазовий портрет «нестійкий фокус» системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «легкість ведення бізнесу - індекс злочинності»

Нерівноважний стан динамічної системи протидії фінансовим та кібершахрайствам у вигляді фазового портрету «нестійкий вузол» спостерігається і в розрізі площини «індекс ефективності уряду - індекс злочинності», що представлено на рисунку 1.16.

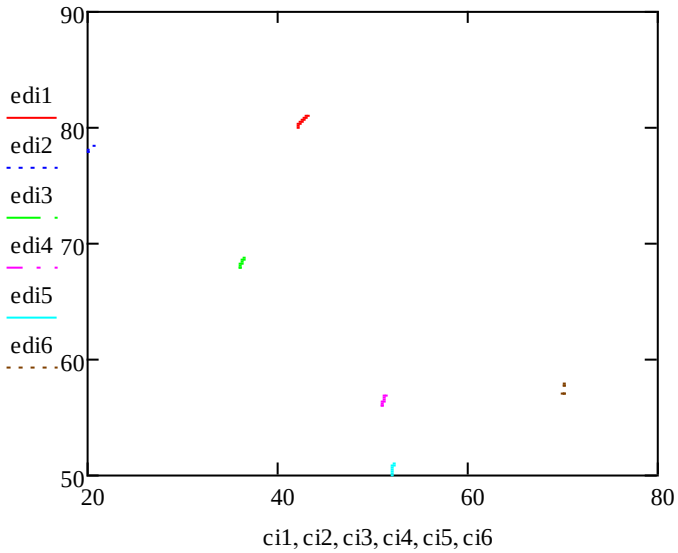

Рисунок 1.16 – Фазовий портрет «нестійкий вузол» системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «індекс ефективності уряду - індекс злочинності»

Таким чином, на основі аналізу рисунків 1.14-1.16, які дозволяють провести біфуркаційний аналіз зрілості діючої системи протидії фінансовим та кібершахрайствам та побудувати фазові портрети їх «зрілості» та «релаксаційних коливань втрати стійкості» за допомогою портретів типу «нестійкий фокус» та «нестійкий вузол» в залежності від розглянутої проекції, що свідчать про нерівноважний стан розглянутої системи.

Побудова нелінійної регресії залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності на основі комбінації степеневої, тригономеричної, та мультиплікативної залежності трьох показників з метою подальшого проведення біфуркаційного аналізу зрілості діючої системи протидії

фінансовим та кібершахрайствам та побудовані фазових портретів їх «станів рівноваги».

Для реалізації даного етапу пропонується скористатись можливостями програмних пакетів Statistica (Statistics/Advanced Linear/Nonlinear Models/Fixed Nonlinear Regression) та MS Excel (Аналіз даних/Регресія).

Для реалізації даного етапу виникає необхідність визначення специфікації нелінійної регресійної залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, для чого скористаємось можливостями програмного пакетіву MS Excel, зокрема інструментарію Аналіз даних/Регресія.

Визначимо специфікацію нелінійної залежності інтегрального індексу кібербезпеки від першої релевантної ознаки індексу ефективності уряду. Для цього розглянемо в якості результативної ознаки інтегральний індекс кібербезпеки, визначений методом Сундаровського, а в якості факторних: поліноміальну (другого і третього ступеня), обернену, тригонометричну залежності індексу ефективності уряду. Застосувавши інструментарій регресійного аналізу отримаємо результат, представлений в таблиці 1.3.

Таблиця 1.3 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від індексу ефективності уряду

Показники	Коефіцієнти	Стандартна похибка	t-статистика	P-Значення	Нижні 95%	Верхні 95%
Y-перетин	47,85679	43,45225	1,10137	0,27456	-38,82807	134,54166
GEI*EDI* CI	0,00035	0,00145	0,24021	0,81088	-0,00255	0,00325
gei2	-5,11919	18,25602	-0,28041	0,78000	-41,53895	31,30057
gei3	1,76326	2,04495	0,86225	0,39154	-2,31630	5,84282
1/gei	0,08037	0,09631	0,83447	0,40690	-0,11177	0,27250
Singei	14,12290	6,36372	2,21929	0,02976	1,42763	26,81816
Cosgei	-16,85691	43,99535	-0,38315	0,70278	-104,62523	70,91140

На основі даних таблиці 1.3 (графи p-значення) можна стверджувати, що статистично значущою є змінна sin(GEI), оскільки p-рівнеь приймає значення 0,0298, що менше ніж гранично допустимий рівень 0,05. Саме тому в якості

специфікації залежності інтегрального індексу кібербезпеки від індексу ефективності уряду пропонується в подальших обчисленнях обрати синусоїду.

Визначимо специфікацію нелінійної залежності інтегрального індексу кібербезпеки від другої релевантної ознаки легкості ведення бізнесу. Для цього, як і в попередньому випадку, розглянемо в якості результативної ознаки інтегральний індекс кібербезпеки, визначений методом Сундаровського, а в якості факторних: поліноміальну (другого і третього ступеня), обернену, логарифмічну, квадратний корінь, тригонометричну залежності легкості ведення бізнесу. Застосувавши інструментарій регресійного аналізу отримаємо результат, представлений в таблиці 1.4.

Таблиця 1.4 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від легкості ведення бізнесу

Показники	Коефіцієнти	Стандартна похибка	t-статистика	P-значення	Нижні 95%	Верхні 95%
Y-перетин	-215579,91	167427,76	-1,28760	0,20225	-549676,79	118516,97
edi2	5,40	4,03	1,33864	0,18515	-2,64699	13,44
edi3	-0,02	0,01	-1,36340	0,17725	-0,04614	0,01
1/edi	890050,46	692798,38	1,28472	0,20325	-492407,17	2272508,1
ln(edi)	99794,06	77102,97	1,29430	0,19994	-54062,512	253650,63
edi^0,5	-28814,34	22124,27	-1,30239	0,19718	-72962,638	15333,95
sinedi	0,24	1,78	0,13587	0,89233	-3,31319	3,80
cosedi	0,86	1,62	0,53233	0,59623	-2,36443	4,08

На основі даних таблиці 1.4 (графи p-значення) можна стверджувати, що відсутня жодна статистично значуща змінна з рівнем не більше 0,05, але p-рівень приймає найменше 0,1773 значення для кубічної залежності результативної ознаки від змінної легкість ведення бізнесу. Саме тому в якості специфікації залежності інтегрального індексу кібербезпеки від легкості ведення бізнесу пропонується в подальших обчисленнях обрати кубічну залежність.

Визначимо специфікацію нелінійної залежності інтегрального індексу кібербезпеки від третьої релевантної ознаки індексу злочинності. Для цього розглянемо в якості результативної ознаки інтегральний індекс кібербезпеки, визначений методом Сундаровського, а в якості факторних: поліноміальну

(другого і третього ступеня), обернену, тригонометричну залежності індексу злочинності. Застосувавши інструментарій регресійного аналізу отримаємо результат, представлений в таблиці 1.5.

Таблиця 1.5 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від індексу злочинності

Показники	Коефіцієнти	Стандартна похибка	t-статистика	P-Значення	Нижні 95%	Верхні 95%
Y-перетин	7828,56244	5651,85	1,38513	0,17054	-3449,52	19106,65
ci2	-0,56852	0,40	-1,41177	0,16258	-1,37	0,24
ci3	0,00268	0,00	1,39037	0,16895	-0,00	0,01
1/ci	-24362,11353	18011,51	-1,35259	0,18067	-60303,52	11579,30
ln(ci)	-4624,84426	3329,88	-1,38889	0,16940	-11269,52	2019,83
ci^0,5	1679,55972	1203,49	1,39558	0,16738	-721,97	4081,09
sinci	-3,24185	2,36	-1,37646	0,17320	-7,94	1,46
cosci	5,72062	2,37	2,41124	0,01861	0,99	10,46

На основі даних таблиці 1.5 (графи p-значення) можна стверджувати, що статистично значущою є змінна cos(CI), оскільки p-рівнеь приймає значення 0,0186, що менше ніж гранично допустимий рівень 0,05. Саме тому в якості специфікації залежності інтегрального індексу кібербезпеки від індексу злочинності пропонується в подальших обчисленнях обрати косинусоїду.

Таким чином, визначивши специфікацію залежності інтегрального індексу кібербезпеки від релевантних предикторів (індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності) у вигляді синусоїди, кубічної залежності, косинусоїди відповідно, а також ввівши додатково змінну мультиплікативного впливу на результативну ознаку усіх трьох релевантних факторів, побудуємо відповідну регресійну залежність. Представимо отримані результати в табличному вигляді (таблиця 1.6).

Таблиця 1.6 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності

Показники	Коефіцієнти	Стандартна похибка	t-статистика	P-значення	Нижні 95%	Верхні 95%
Y-перетин	10,89788	4,12827	2,63982	0,01019	2,66634	19,12942
singei	9,97709	5,09017	1,96007	0,05391	-0,17241	20,12659
edi3	0,00008	0,00001	5,63831	0,00000	0,00005	0,00010
cosci	3,40130	1,60508	2,11909	0,03758	0,20087	6,60174
GEI*EDI* CI	-0,00057	0,00121	-0,47375	0,63713	-0,00299	0,00184

На основі даних графи «Коефіцієнти» таблиці 1.6 побудуємо регресійну залежність інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності у вигляді наступного співвідношення (1.9):

$$IS = 10{,}8989 + 9{,}9771 \cdot \sin(GEI) + 0.00008 \cdot EDI^3 + 3.4013 \cdot \cos(CI) - 0.00057 \cdot GEI \cdot EDI \cdot CI \quad (1.9)$$

Достовірність та точність рівняння (9) підтверджено на основі наступних критеріїв. Статистично значущими є значеннями коефіцієнтів перед змінними за допомогою значень p-рівня менше 0,05, окрім коефіцієнту перед змінною мультиплікативного впливу трьох факторів. Але дану змінну пропонується залишити в моделі з метою подальшого проведення біфуркаційного аналізу зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазових портретів їх «станів рівноваги», оскільки наявність даної змінною мультиплікативного впливу трьох факторів є необхідною умовою проведення якісного біфуркаційного аналізу. Коефіцієнт детермінації приймає значення 70,59%, це свідчить про те, що варіація результативної ознаки інтегрального індексу кібербезпеки на 70,59% пояснюється варіацією обраних факторних ознак.

Проведення біфуркаційного аналізу зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазових портретів їх «станів рівноваги».

Для реалізації даного етапу виникає необхідність попереднього здійснення проміжних обчислень за допомогою застосування апарату диференціального числення, що включає визначення часткових похідних функції залежності інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, формування системи диференційних рівнянь, які виступають основою подальшого дослідження динамічної стійкості розглянутої системи (формули 1.10-1.13). Для реалізації даного етапу пропонується застосування пакету прикладних програм MathCAD.

Основою подальшого дослідження динамічної стійкості системи протидії фінансовим та кібершахрайствам та побудові фазових портретів їх «зрілості» та «релаксаційних коливань втрати стійкості» виступає нелінійна функція:

$$f(gei, edi, ci) \coloneqq 10.8978783 + 9.977087\sin(gei) + 7.643510 \cdot 10^{-5} \cdot (edi^3) + 3.40130281\cos(ci) - 0.00057478 gei \cdot edi \cdot ci \tag{1.10}$$

На основі розглянутої функції (10), змоделюємо систему диференціальні рівнянь, які характеризують поводження динамічної системи протидії фінансовим та кібершахрайствам з метою подальшої побудови фазових портретів «станів рівноваги»:

$$\frac{d}{dgei} f(gei, edi, ci) \rightarrow 9.97708769\cos(gei) + -0.00057478 ci \cdot edi \tag{1.11}$$

$$\frac{d}{dedi} f(gei, edi, ci) \rightarrow 0.000229305 edi^2 + -0.00057478 ci \cdot gei$$

$$\frac{d}{dci} f(gei, edi, ci) \rightarrow -3.40130281 \cdot \sin(ci) + -0.0005747 \cdot 8 \cdot edi \cdot gei$$

Представлені три диференційні рівняння (1.11) дозволяють встановити взаємозв'язки між змінними GEI (індекс ефективності уряду), EDI (легкість ведення бізнесу), CI (індекс злочинності) та їх першими частковими похідними $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci).$

Грунтуючись на нелінійному підході, який лежить в основі теорії біфуркації, побудуємо фазові портрети «станів рівноваги» показника інтегральний індекс кібербезпеки у вигляді відображення фазових траєкторій як проекцій на попарно розглянуті площини: індекс ефективності уряду - легкість ведення бізнесу, легкість ведення бізнесу - індекс злочинності, індекс ефективності уряду - індекс злочинності. Побудуємо фазові портрети «станів рівноваги» системи протидії фінансовим та кібершахрайствам на базі системи диференційних рівнянь (1.12) на основі застосування математичного пакету програмного забезпечення математичного аналізу MathCad:

$$\begin{aligned}
&Faza(gei0, edi0, ci0, dt, N) := \left| \begin{array}{l}
\left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
\text{for } k \in 0..N \\
\quad \left| \begin{array}{l}
fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
gei_{k+1} \leftarrow \left[gei_k + dt \cdot \left(9.97708769 \cdot \cos\left(gei_k\right) + -0.0005747 \cdot 8 \cdot ci_k \cdot edi_k\right)\right] \\
edi_{k+1} \leftarrow \left[edi_k + dt \cdot \left[0.000229305 \cdot \left(edi_k\right)^2 + -0.0005747 \cdot 8 \cdot ci_k \cdot gei_k\right]\right] \\
ci_{k+1} \leftarrow \left[ci_k + dt \cdot \left(-3.40130281 \cdot \sin\left(ci_k\right) + -0.0005747 \cdot 8 \cdot edi_k \cdot gei_k\right)\right]
\end{array} \right. \\
(gei \quad edi \quad ci)
\end{array} \right.
\end{aligned} \tag{1.12}$$

З метою надання візуалізації представленого за допомогою формули (1.12) фазового портрету «станів рівноваги» системи протидії фінансовим та кібершахрайствам та подальшої ідентифікації його типу як однієї із можливих альтернатив – різновидів у вигляді сідла, вузла чи фокуса, розглянемо різні варіанти можливих значень як факторів (індекс ефективності уряду, легкість

ведення бізнесу, індекс злочинності), так і значення функції, яка описує інтегральний індекс кібербезпеки із заданим рівнем точності на основі зазначеній кількості точок реалізації:

$$(gei1\ \ edi1\ \ ci1) := Faza(1.6, 80, 42, 0.01, 100) \tag{1.13}$$

$$(gei2\ \ edi2\ \ ci2) := Faza(1.45, 78, 20, 0.01, 100)$$

$$(gei3\ \ edi3\ \ ci3) := Faza(0.18, 68, 36, 0.01, 100)$$

$$(gei4\ \ edi4\ \ ci4) := Faza(0.43, 56, 51, 0.01, 100)$$

$$(gei5\ \ edi5\ \ ci5) := Faza(-0.32, 50, 52, 0.01, 100)$$

$$(gei6\ \ edi6\ \ ci6) := Faza(-0.45, 57, 70, 0.01, 100)$$

Таким чином, підставляючи фактичні значення вхідних даних (формули 1.13) у співвідношення, які дозволяють формалізувати фазові портрети (1.12), визначимо рівноважні точки, представлені у площині «індекс ефективності уряду - легкість ведення бізнесу» рисунку 1.17 для різних значень вхідних даних. Отже, рівноважному стану системи протидії фінансовим та кібершахрайствам відповідають наступні значення її параметрів (точки перетину графіків, зображені на рисунку 1.17): індекс ефективності уряду – 1,4838, легкість ведення бізнесу –80,183.

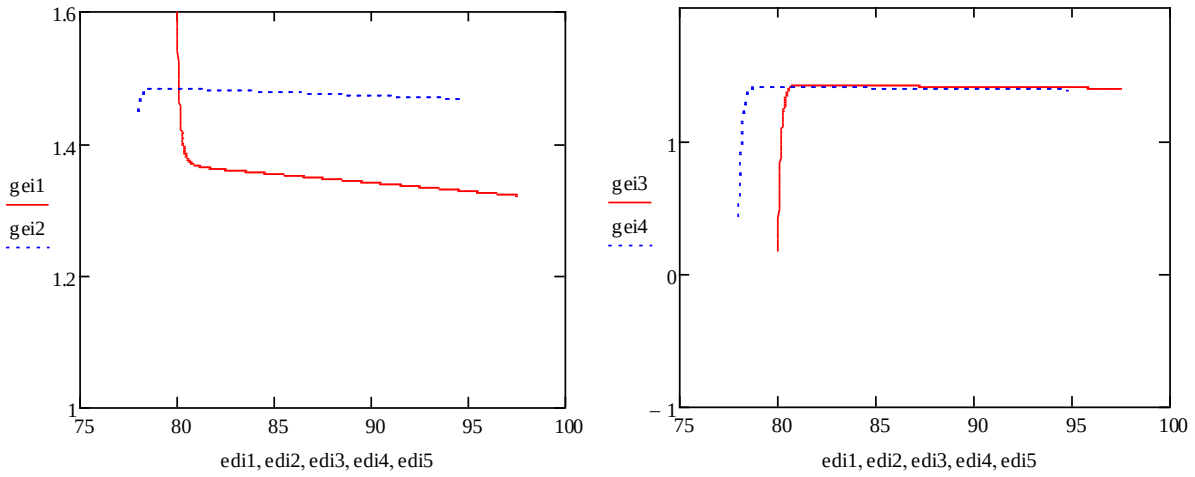

Рисунок 1.17 – Зображення рівноважних точок системи протидії фінансовим та кібершахрайствам у площині «індекс ефективності уряду - легкість ведення бізнесу»

Проведемо дослідження фазового портрету динамічної системи протидії фінансовим та кібершахрайствам на всій множині значень вхідних показників (формули (1.13)). Розглянемо спочатку фрагмент фазового портрету даної системи протидії фінансовим та кібершахрайствам в розрізі площини «індекс ефективності уряду - легкість ведення бізнесу» (рисунок 1.18). Даний «фазовий портрет» демонструє наявність рівноважної точки.

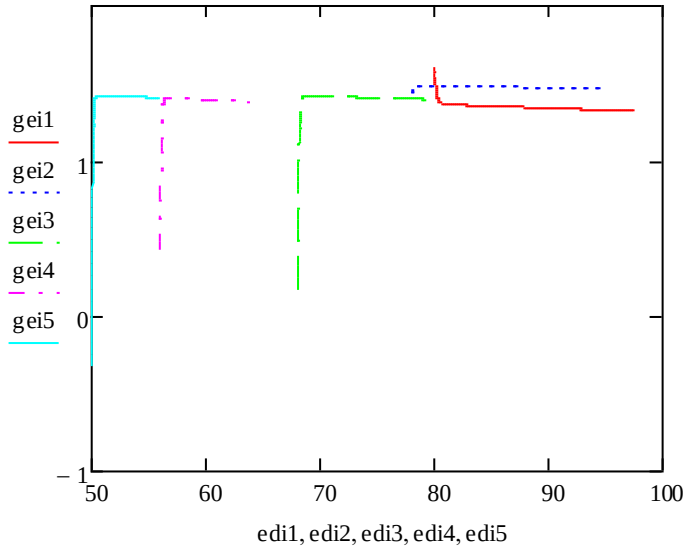

Рисунок 1.18 – Фрагмент фазового портрету «стан рівноваги» динамічної системи протидії фінансовим та кібершахрайствам в розрізі площини «індекс ефективності уряду - легкість ведення бізнесу»

Переходячи до розгляду фрагменту фазового портрету динамічної системи протидії фінансовим та кібершахрайствам, в розрізі площини «легкість ведення бізнесу - індекс злочинності» (рисунок 1.19) спостерігаємо, що вона знаходиться в нерівноважному стані, який характеризується як «сідло». Даний тип біфуркації свідчить про нестійкий стан системи, тобто при суттєвій зміні одного параметра і фіксованому значенні іншого параметра розглянута система знаходиться в нерівноважному стані.

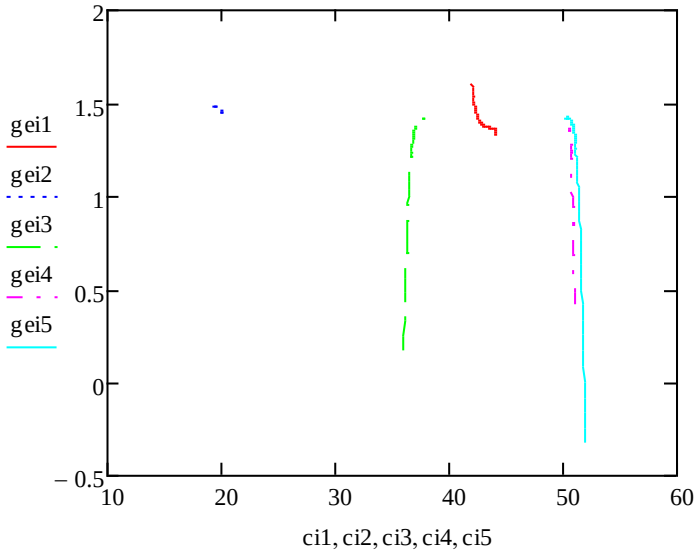

Рисунок 1.19 – Фрагмент фазового портрету «сідло» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «легкість ведення бізнесу - індекс злочинності»

Нерівноважний стан динамічної системи протидії фінансовим та кібершахрайствам у вигляді фазового портрету «сідло» спостерігається і в розрізі площини «індекс ефективності уряду - індекс злочинності», що представлено на рисунку 1.20.

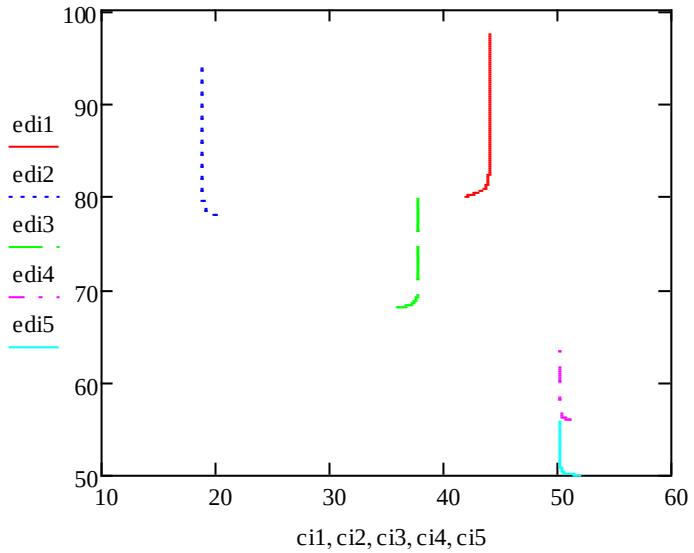

Рисунок 1.20 – Фрагмент фазового портрету «сідло» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «індекс ефективності уряду - індекс злочинності»

Таким чином, на основі аналізу рисунків 1.18-1.20, які дозволяють провести біфуркаційний аналіз зрілості діючої системи протидії фінансовим та кібершахрайствам визначено фазовий портрет «станів рівноваги» у площині «індекс ефективності уряду - легкість ведення бізнесу» та нерівноважні фазові портрети типу «сідло» в розрізі інших проекцій.

2 ВИЗНАЧЕННЯ КЛЮЧОВИХ АЛГОРИТМІВ СИСТЕМ ФІНАНСОВОГО МОНІТОРИНГУ ТА КІБЕРБЕЗПЕКИ

2.1 Моделювання ключових алгоритмів конвергенції системи кібербезпеки та фінансового моніторингу у банках

За оцінками експертів серед галузей, які найбільше потерпають від кіберзлочинців, перше місце займає банківський сектор, друге – енергетичний та добувний сектор, третє – телекомунікаційний. Так, у 2017 році від фішингових атак найбільшої шкоди зазнали 51,7% банків в порівнянні з електронною комерцією та платіжними системами – представниками фінансового сектору [34].

Тому для банків одним з важливіших та актуальних питань є вирішення проблеми, пов’язаної із виявленням та попередженням шахрайських, незаконних дій з його фінансовими ресурсами. Шахрайства, об’єктами яких частіше всього стають клієнти банків, сприяють зниженню довіри до фінансових інститутів та пошуку альтернативних способів для зберігання коштів. Удосконалення методів шахрайств та збільшення частоти кібератак призводять до збільшення втрат банків та їх клієнтів. Банківська система безпеки часто не встигає за швидкими темпами модернізації способів та інструментів шахраїв. Відповідно рівень протидії загрозам поступається рівню зростаючих загроз.

За статистичними даними ЕМА (Української міжбанківської асоціації членів платіжних систем), сума збитків громадян внаслідок дій шахраїв із платіжними картками у 2017 році досягла 670 млн.грн., що значно перевищує збитки за попередні роки – 339,13 млн.грн. (2016 р.), 181,00 млн.грн. (2015 р.), 90,00 млн.грн. (2014 р.). Збільшилася також і середня сума втрат від одного шахрайства із використанням методів соціальної інженерії. Так, у 2017 році ця сума склала 2543,00 грн. проти 1403,00 грн. у 2016 році та 834,00 грн. у 2015 році [35].

Боротьба із шахрайством – це глобальна проблема. Для її вирішення створюються спеціальні підрозділи, її намагаються регулювати на законодавчому рівні. На боротьбу із шахрайством впливають: розвиток нових способів шахрайства; збільшення обсягу інформації, обробка якої потребує нових методів, наприклад, Data Mining; обмеження в інформаційних системах, які не дозволяють своєчасно адаптувати їх до ефективної протидії новим за формою і рівнем новизни загрозам; проблеми, пов'язані з управлінням даними на фізичному та організаційному рівнях; банківські ризики; психологія взаємовідносин «клієнт – шахрай – банк», яка дозволяє клієнту у випадках спілкування із шахраєм надавати конфіденційну інформацію.

Одним із головних напрямків боротьби із шахрайством, зазначеним у Постанові НБУ №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року, є впровадження банками основних технічних систем [36]: виявлення атак; моніторингу події управління інцидентами; контролю доступу до мережі; захисту електронної пошти; запобігання атак, спрямованих на відмову в обслуговуванні; антивірусного захисту; двофакторної автентифікації. Але роз'яснення щодо їх створення, впровадження, фінансування, тощо, відсутні. Тобто перед банками поставлена задача, а її виконання – це вже прерогатива власників, при цьому спостерігається нехватка спеціалістів в галузі кібербезпеки, що ускладнює виконання задачі.

До вирішення такої складної проблеми треба підходити системно, та ключем її рішення має бути розвиток та комплексне удосконалення автоматизованих інформаційних технологій та систем у поєднанні із математичними методами. Так, в сфері інтеграції автоматизованих та математичних методів для банківської сфери багато зроблено працівниками американської компанії в галузі бізнес-аналітики "SAS Institute", результатом чого стають програмні розробки для банківського сектору [37].

Також можна виділити роботу в цьому напрямку компанії "Kaspersky Lab", яка багато років розробляє програмні рішення для антивірусного захисту та

інтернет-безпеки, а також здійснює статистичні дослідження видів, способів, типів шахрайств для різних сфер економіки [38].

В умовах зростання кількості та різновидів інформаційних та кіберзагроз для забезпечення функціонування ефективної системи інформаційної безпеки будь-якого суб'єкту економіки є потреба у конвергенції систем. Так, можливим напрямом є інтеграція системи фінансового моніторингу та кібербезпеки, що може здійснюватися на алгоритмічному, програмно-технічному, інформаційному та організаційному рівнях функціонування інформаційної системи банківської установи. Тільки системне поєднання кібербезпеки та фінансового моніторингу дозволить сформувати надійну систему захисту, яка буде не тільки виявляти наслідки, але й попереджувати загрози. Тому вкрай важливим є розуміння сутності та структури процесів забезпечення безпеки інформації, особливо тих, що стосуються заходів перевірок стосовно виявлення порушень цілісності, конфіденційності даних або наслідків кібершахрайств та кіберзагроз.

Пропонуємо розробку трирівневої системи попередження фінансових кіберзагроз, яку буде реалізовано для банківських установ та яка буде охоплювати організаційний, інформаційний та алгоритмічний рівні, заходи кожного з яких будуть спрямовані на виявлення ознак кіберзагроз на етапі, що передує здійсненню зовнішніх та внутрішніх загроз. Концептуальна модель даної системи представлено на рисунку 2.1.

Концепція моделі полягає в тому, що операції, які відбуваються у фронт-офісі банку (безпосередньо у банку, за допомогою програмних та мобільних додатків) проходять перевірку на предмет наявності ознак кіберзагроз. Тому доцільно, що така система буде мати модуль моніторингу, побудований за принципами застосування методів інтелектуального аналізу "Data Mining", де буде реалізовано два рівні – інформаційний (створення бази знань із статистикою шахрайств) та алгоритмічний (створення бази правил (критеріїв) для відслідковування ознак шахрайств) (рисунок 2.1).

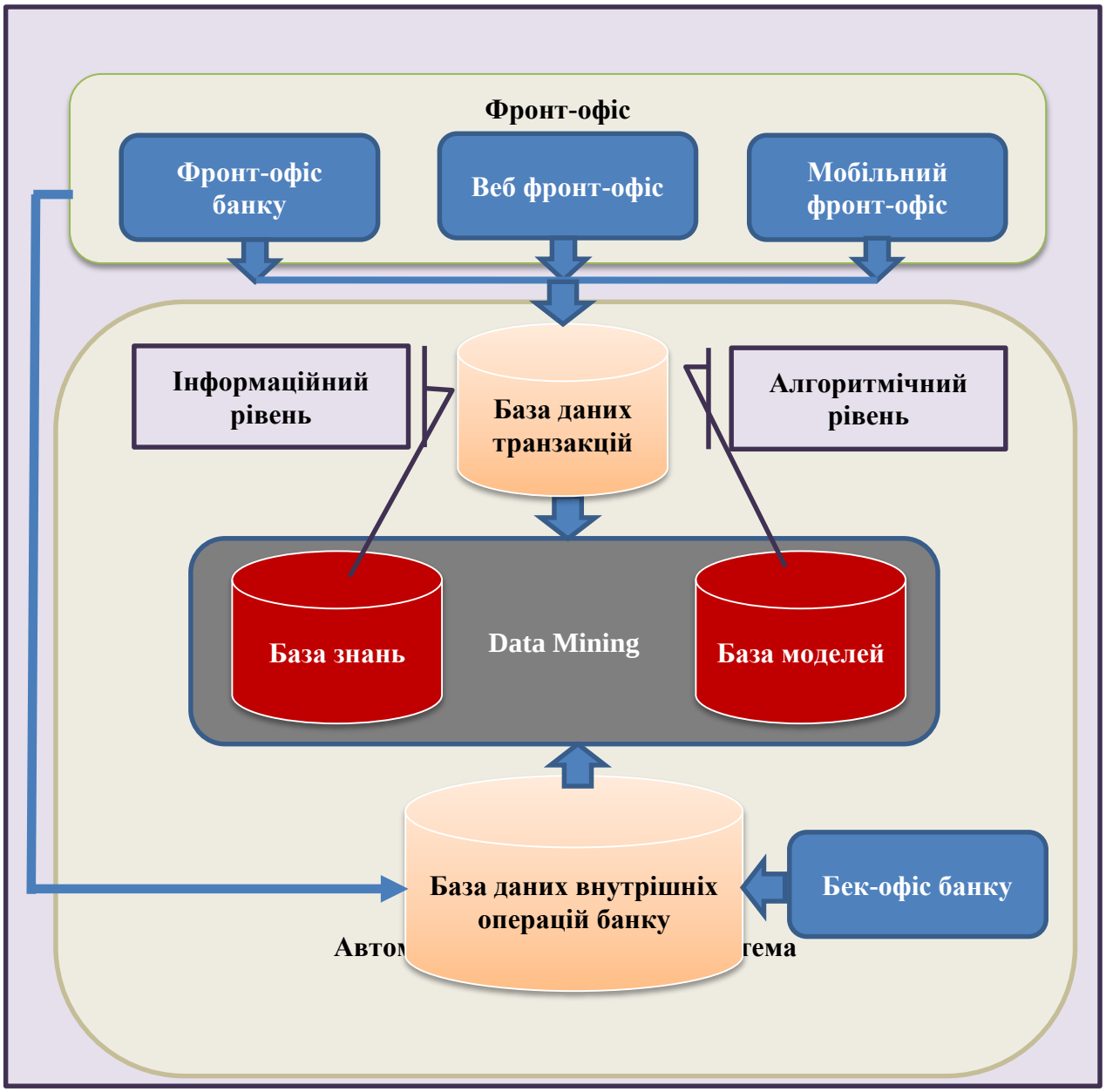

Рисунок 2.1 – Концептуальна модель трирівневої системи попередження фінансових кіберзагроз

Його головне призначення – виявляти потенційні фінансові кіберзагрози незалежно від природи ініціатора (зовнішнього – клієнта банку та його операцій “База даних транзакцій”, чи внутрішнього – персоналу банку та його операцій “База даних внутрішніх операцій банку”). Операції перевіряються на відповідність певним критеріям, які визначають, чи має операція ознаки кібершахрайської, які сформовані у базі знань та правил з урахуванням накопичених статистичних даних, чи не має. Означені процеси перевірки

відбуваються з урахуванням заходів організаційного рівня, на якому відбувається оптимізація бізнес-процесів інформаційного захисту, що дозволяє виявляти слабкі місця в системі захисту інформації. Виходячи з окреслених завдань трьох рівнів, розробимо конкретні пропозиції для їх реалізації.

Для забезпечення організаційного рівня трирівневої системи попередження фінансових кіберзагроз застосуємо методику моделювання бізнес-процесів, яка дозволить побудувати наочну модель будь-якого процесу та провести симуляцію його здійснення на практиці. Як результат, такий підхід сприятиме виявленню слабких місць та оптимізації з урахуванням різних варіантів.

Методика передбачає побудову та оптимізацію процесів інформаційної безпеки банківської установи, які будуть змодельовані виходячи із можливої інтеграції системи протидії легалізації кримінальних доходів (первинного фінансового моніторингу) та системи інформаційної безпеки (попередження кібершахрайств із зовнішніх та внутрішніх джерел).

Так, на першому кроці будується модель процесу на основі нотації BPMN 2.0, яка є стандартом бізнес-моделювання, що враховує попроцесний підхід. Тобто будь-яка діяльність компанії розглядається не з позиції функцій, з якими вона пов’язана, а з позицій учасників та їх дій, які вони здійснюють протягом певного періоду часу. Це дозволяє бачити – хто виконує, що робить, по відношенню до чого (кого) діє, протягом якого періоду, чим керується. Відповідно в процесі побудови моделі повинні визначатися:

– учасники процесу або його виконавці, які виступатимуть ресурсами компанії, оскільки від їх кількості залежатимуть витрати, пов’язані із процесом. Це можуть бути працівники різних відділів з різними посадами, які приймають рішення, оформлюють документи, здійснюють видачу коштів, вносять дані в систему, контролюють тощо. Також сюди відносяться постачальники, клієнти, банківські установи, та інші, тобто ті, хто є зовнішнім учасником бізнес-процесу. Окремо можна виділити автоматизовані інформаційні системи та їх модулі, які

можуть бути також виконавцями за умови автоматизації діяльності. В рамках одного бізнес-процесу може бути задіяно декілька різних учасників;

– операції, тобто конкретні дії виконавців, які здійснює учасник в рамках бізнес-процесу. На практиці вони стосуються конкретного об’єкта та виконуються особою, якій відповідає конкретна посада, а також здійснюються у відповідності з інструкціями установи. Наприклад, дії банківського працівника щодо укладення кредитного договору із клієнтом: вияснити мету отримання кредиту клієнтом; перевірити наявність клієнта в базі даних; ввести дані клієнта, якщо він відсутній у базі даних; перевірити дані клієнта, якщо він є у базі даних; відкоректувати дані; сформувати договір; узгодити умови із клієнтом; роздрукувати та підписати договір; передати його клієнту, тощо;

– події, які представляють собою дії, що відбуваються з метою ініціалізації конкретної операції процесу. Їх безпосередньо не здійснюють виконавці, оскільки вони можуть відбуватися автоматично або проявлятися у якості певного сигналу, щоб почати або закінчити операцію. Наприклад, початок та кінець бізнес-процесу є основними подіями будь-якого процесу; отримання повідомлення складської системи щодо оприбуткування матеріалів, яке запускає операцію оплати постачальнику, є також подією; відміна операції в результаті помилкового її виконання учасником – це подія, яка буде переривати процес, тощо;

– потоки управління, які дозволяють формувати логіку переходів від однієї операції до іншої. Це відбувається у випадку існування альтернативних варіантів дій учасників, якщо застосовується певна умова, сформована на основі нормативно-правового базису економічного агента (інструкцій, стандартів, законів, положень, тощо). На практиці потоки управління визначаються доволі складно. Це пов’язано із тим, що процес моделювання повинен передбачати різні варіанти дій, а за часту умови їх переходів важко формалізувати. Тому деякі компанії надають перевагу функціональному моделюванню, яке базується суто на посадових інструкціях, де чітко визначені функціональні обов’язки персоналу, та інших документах, пов’язаних із функціональною структурою.

Але такий підхід як раз і не дає можливості виділяти дії, які можуть виконуватися в межах однієї функції;

– дані, тобто весь той базис нормативно-правової документації або інформації, що міститься у базі чи сховищі даних, які використовуються для забезпечення виконання певних операцій, подій процесу чи потоків управління, або є їх прямим результатом. Як правило, сюди відносяться бухгалтерські документи, постанови, інструкції, стандарти, закони, положення, масиви, бази, сховища даних, тощо.

Для реалізації моделі застосовується спеціальне програмне забезпечення. Первинна її побудова, яка відображає реальний процес, що відбувається на практиці, називається моделлю “ЯК Є”.

На другому етапі задаються параметри моделі: час на виконання операцій, вартість ресурсів та ймовірності для потоків управління. Як правило, дана інформація береться, виходячи із наявних даних, що відповідають даному бізнес-процесу. Тобто час задається на основі заміру його фактичних значень, що витрачаються учасниками в процесі виконання ними операцій. Вартість фіксується, виходячи з тарифної сітки учасників або вартісних показників, які символізують витрати, понесені на здійснення тієї чи іншої операції. Ймовірність виставляється також з урахуванням статистичних даних або персональної оцінки учасника процесу.

Для підвищення ефективності моделювання доцільно накопичувати статистику часу та ймовірності для потоків управління. Це дозволить відслідковувати саме ті операції, здійснення яких є найбільш вірогідним та результат несприятливим. У випадку бізнес-процесів банківської інформаційної безпеки, це якраз можуть бути саме ті транзакції, які за певний проміжок часу були відхилені завдяки наявності ознак кіберзагроз або не пройшли первинний фінансовий моніторинг. В подальшому, в процесі оптимізації процесу цей результат може бути враховано для побудови моделі “ЯК БУДЕ”.

На третьому етапі проводиться симуляція за різними типами – “Аналіз часу” та “Аналіз ресурсів”. Результати “Аналіз часу” надають інформацію щодо

мінімального, максимального та середнього часу по кожній операції, а також загального часу, витраченого на заданий обсяг симуляції. Так, отримане значення середнього часу по кожній з операцій дозволить виявити слабку ланку, пов'язану із відхиленням від показників по типовим операціям, що сприятиме в подальшому оптимізації даної ділянки процесу.

Також можна отримати інформацію щодо кількості операцій, отриманих на виході та здійснених на кожному вузлі моделі. Так, дана кількість визначатиметься за формулою (2.1):

$$NO_{out} = (((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots - \left\lceil p_n^- \times ((((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots - \lceil p_{n-1}^- \times ((((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots \rceil\right\rceil \quad (2.1)$$

де NO_{out} – кількість операцій, отриманих після здійснення симуляції;

N_0 – кількість операцій на початку симуляції;

p_i^- $(\overline{1,n})$ – ймовірність негативного (альтернативного) випадку для потоків управління, коли відбувається розгалуження у моделі;

n – кількість розгалужень у моделі, які позначаються у вигляді шлюзів;

$\lceil \quad \rceil$ – округлення кількості операцій до найближчого цілого у більший бік.

У випадку моделювання основних бізнес-процесів системи інформаційної безпеки рекомендується визначати коефіцієнт результативності за формулою (2.2), який відображатиме якість її роботи:

$$KR = \frac{NO_{out}}{N_0}, \quad (2.2)$$

де KR – це коефіцієнт результативності окремих модулів системи інформаційної безпеки. Якщо KR = 1, то можна сказати, що операцій, які отримали статус загрозливих, шахрайських або підлягають фінансовому моніторингу, не виявлено. Або дійсно не відбувалися такі випадки, або система пропускає всі операції, оскільки має неефективні налаштування перевірок. Якщо KR = 0, то всі операції мають статус загрозливих. На практиці, якщо відбуватиметься така ситуація, то можна сказати, що система є неефективною, оскільки не пропускає всі операції. Граничні значення даного показника свідчать про неефективність роботи системи інформаційної безпеки. Якщо 0<KR<1, то це говорить про те, що деякі операції було заблоковано системою у зв'язку із знаходженням в них ознак загроз.

Системи, які використовують банки для фінансового моніторингу, можуть блокувати операції, які при подальшій їх перевірці не виявляють ознаки відмивання кримінальних доходів. Це можна пояснити тільки тим, що використовуються непрозорі критерії перевірки, тому система автоматично відносить такі транзакції в категорію підозрілих. Використання індексу (2.2) дозволить накопичувати статистику результативності системи та у випадку помилкового відбору операцій здійснювати коригування критеріїв перевірок.

Результати симуляції "Аналіз ресурсів" надають інформацію щодо завантаженості кожного з виду задіяних ресурсів та їх вартості. Це дозволяє сформувати уявлення щодо фінансових витрат, пов'язаних із виконанням даного процесу. Якщо задіяно декілька учасників (ресурсів), то можна визначити відповідні витрати на кожного з них окремо та порівняти вартісні показники у випадку вибору альтернатив, що дозволить визначити шляхи економії.

На четвертому етапі проводиться оптимізація бізнес-процесу шляхом внесення змін та коректувань у модель, які будуть враховувати слабкі місця, виявлені в результаті здійснення симуляції на попередньому кроці. Тобто будується модель "ЯК БУДЕ", яка буде відображати бажані елементи процесу. Далі здійснюється процес налаштування симуляції (другий етап) та сама симуляція (третій етап). Отримані результати порівнюються із результатами для

моделі “ЯК Є”. Це стосується даних часу та вартості ресурсів. Якщо значення показників покращилися, то отримана модель буде вважатися придатною для практичного використання. Якщо показники після оптимізації не змінилися у найкращий бік, то оптимізацію проводимо ще раз. Це відбуватиметься доти, доки результати моделювання не будуть придатними для практичного застосування.

Отримані моделі бізнес-процесів впроваджуються у діяльність банку або іншого економічного агента. Тобто внесені корективи запроваджуються до тих операцій та учасників, які було оптимізовано у моделі.

Дану методику використаємо для побудови моделей бізнес-процесів, які сьогодні є найбільш критичними для системи інформаційної безпеки банків: процес ідентифікації та верифікації клієнта; процес перевірки транзакцій на наявність ознак кібершахрайств; автоматизованого фінансового моніторингу; перевірки дій інсайдерів на ознаки кібершахрайств. Для моделювання було використано програмне забезпечення Bizagi Modeler. Перед тим, як проаналізувати отримані результати, зазначимо ті підходи, які було використано для побудови моделей.

По-перше, банківську установу розглядаємо як складну систему, складовими якої виступають внутрішнє середовище: персонал, менеджмент банку, його власники, автоматизована банківська система (АБС); та зовнішнє середовище: клієнти, кіберзлочинці, пов’язані особи, програмно-технічні пристрої. Тобто банк – це система взаємозв’язаних суб’єктів та об’єктів внутрішнього та зовнішнього середовища. До складу системи будь-якої природи входять елементи різного рівня надійності, які можуть вторгнутися в певний момент за певних умов, що може призвести до порушення її функціонування, а також порушення конфіденційності, цілісності та цінності інформації. По суті кожен з цих елементів може стати джерелом загрози безпеки інформації, потенційного шахрайства або ініціатором, або співучасником, або бути опосередковано залученим.

По-друге, різні дослідження в сфері банківського шахрайства розглядають в основному зовнішнє середовище як ініціатора шахрайства або порушення

інформаційної безпеки, що є не зовсім коректно. 80% від усього обсягу інцидентів пов’язано із персоналом банку. Тому можливості вторгнення повинні враховувати також і внутрішні аспекти загрози.

По-третє, при окресленні банківської системи будемо користуватись принципом професійного песимизму, яким керуються аудитори, і який не виключає зловживань на будь-якому робочому місці банку, ймовірності вторгнення сторонніх осіб задля здійснення шахрайства або шкоди. Тобто, джерелом інциденту може бути будь-хто, здійснення – будь-де та з використанням будь-яких інструментів та способів. Відповідно система повинна враховувати зміни негативного характеру та реагувати на них.

По-четверте, розглядаємо систему інформаційної безпеки, як систему, інтегровану із автоматизованою банківською інформаційною системою та системою протидії відмиванню кримінальних доходів.

Проводимо моделювання тих процесів, які задіяні безпосередньо у системі банківської безпеки. На рисунку 2.2 представлено бізнес-модель процесу ідентифікації та верифікації клієнта, яка є придатною у випадку здійснення дистанційних операцій. Вона вже є результатом “ЯК БУДЕ”.

Оскільки на практиці проводиться ідентифікація клієнтів, а верифікація здійснюється тільки для окремих операцій, то побудова моделі “ЯК Є” буде недоцільною в даному випадку, оскільки вона не враховуватиме багатьох параметрів та порівняння покаже неефективність моделі “ЯК БУДЕ” за рахунок її більш складної структури. Ця проблема буде стосуватися й інших запропонованих моделей, тому аналіз та порівняння буде проводитися для повністю автоматизованого процесу та процесу, де частина операцій виконується людиною, що є характерним для багатьох українських банків.

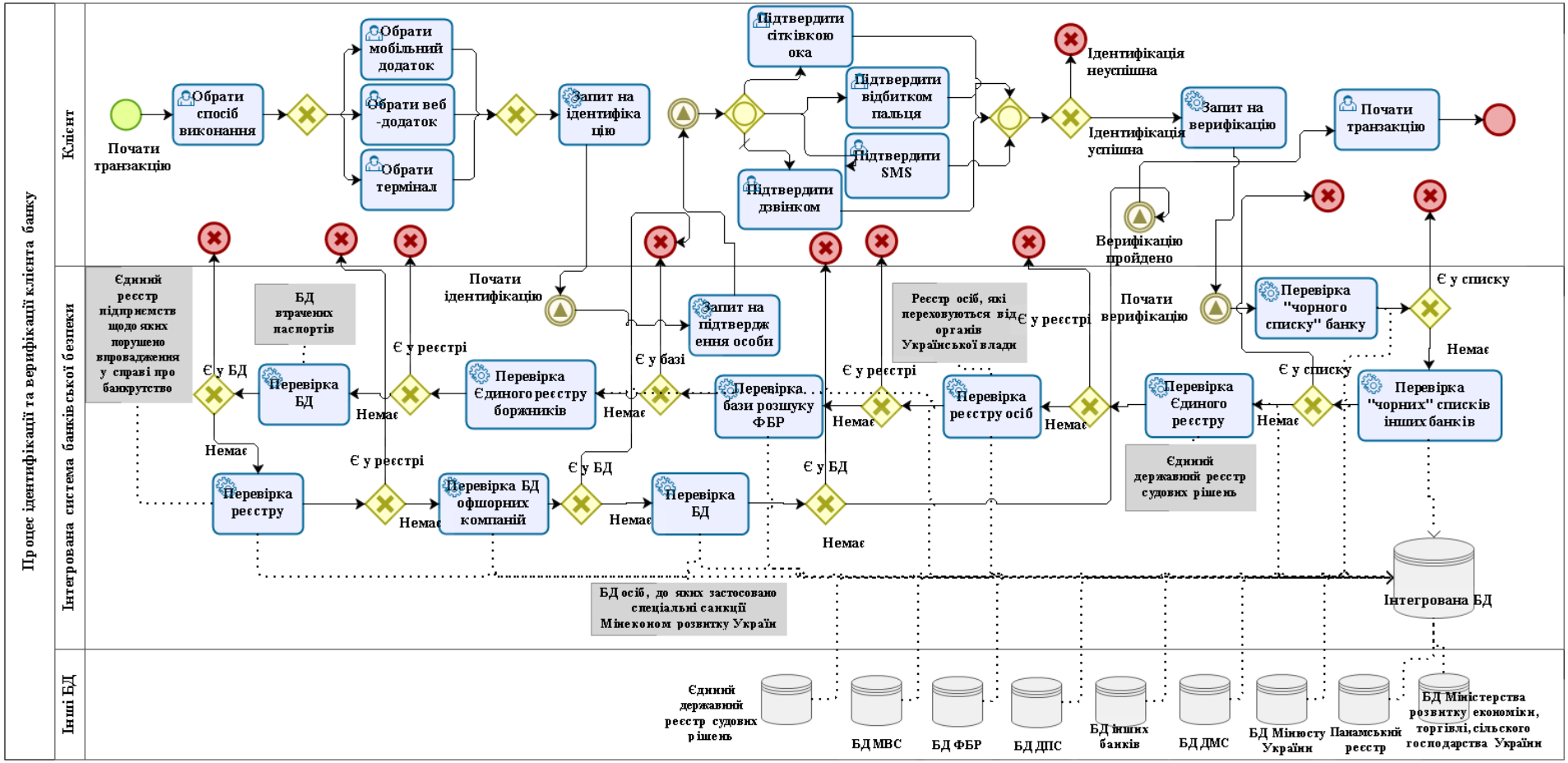

Рисунок 2.2 – Бізнес-модель процесу ідентифікації та верифікації клієнта в інтегрованій системі банківської безпеки

В моделі зазначено два етапи, які повинен пройти клієнт. На першому відбувається його ідентифікація, коли він входить у систему через мобільний додаток, або веб-банкінг, або термінал. Це здійснюється шляхом виконання запиту на підтвердження особи клієнта шляхом використання відбитка пальця, сітківки ока, або підтвердженням через СМС-повідомлення або телефонний дзвінок. Зараз в Україні використовується тільки два останні види підтвердження. У випадку, якщо шахрай намагається увійти до системи, використовуючи чужі дані, то ідентифікацію буде не пройдено, а операцію заблоковано.

Після успішного підтвердження, починається другий етап – верифікація, тобто здійснюється перевірка клієнта на наявність у (рисунок 2.2): «чорному списку» банку, де він є клієнтом, та у «чорних списках» інших банків; реєстрі судових рішень по клієнту; реєстрі осіб, які переховуються від органів української влади; базі розшуку ФБР; Єдиному реєстрі боржників; базі даних втрачених паспортів; базі даних офшорних компаній; Єдиному державному реєстрі підприємств, щодо яких порушено впровадження у справі про банкрутство; базі даних осіб, до яких застосовано спеціальні санкції Мінеконом розвитку України. Якщо клієнт успішно проходить верифікацію, то система надає йому дозвіл на здійснення операції, в протилежному випадку система його блокує та повідомляє відповідні органи безпеки.

Результати проведеної симуляції для даного бізнес-процесу представлені на рисунку А.1 у додатку А. В якості умов симуляції було задано: кількість операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); час на виконання операцій в інтегрованій системі банківської безпеки – 1 с. (це максимальний час на виконання 1 запиту у будь-якій системі) [39]; для операцій ідентифікації час виставлявся, виходячи із власних замірів максимального часу в процесі користування мобільним банкінгом. В результаті отримано, що середній час на ідентифікацію та верифікацію клієнта за умови впровадження даної схеми на практиці буде дорівнювати 69,75 с. Кількість операцій після перевірки – 903

(формула 2.1). Коефіцієнт результативності – 0,903 (формула 2.2). Тобто за умови визначення 1% операцій такими, які носять ознаки шахрайських по кожному з критеріїв перевірки, система буде ідентифікувати після верифікації та ідентифікації 90,3% операцій як таких, що пройшли моніторинг.

Після проходження ідентифікації та верифікації пропонується перевірка операцій у відповідності із їх сумами. Якщо сума транзакції перевищує 400 000 грн., то банк зобов'язаний здійснити її моніторинг за критеріями на предмет легалізації кримінальних доходів [17]. В протилежному випадку, рекомендується перевірити на наявність ознак шахрайства. Це актуально в умовах зростання кількості постраждалих від соціальної інженерії. Так, на 4 квартал 2019 року цей вид злочинності у поєднанні із шкідливим програмним забезпеченням використовувався у 54%. Для приватних осіб соціальна інженерія склала 67%, для приватних – 62%. При чому для різних компаній його доля є значною: для державних компаній – 66%, промислових – 88%, фінансових організацій – 94%, IT-компаній – 50%, торгівля – 36% [40].

На практиці установи зобов'язані здійснювати моніторинг, але процес перевірки організується банками самостійно. Тому більшість з них його проводить вручну. Згідно із Постановою НБУ №65 від 19.05.2020 «Про затвердження Положення про здійснення банками фінансового моніторингу» налаштування та автоматизацію відповідних процесів банки повинні організувати до 30.06.2021 року [41].

Науковці різних країн світу пропонують власні підходи до організації автоматизованого моніторингу. Так, авторським колективом Чен З., Ван Хоа Л.Д., Тео Е.Н. , Назір А., Каруппія Е.К., Лам К.С. досліджено техніки машинного навчання, як засіб протидії відмивання коштів [42]. Авторами Гао С., Сю Д., Ванг Х., Грін П. розроблено мультиагентну систему з використанням технології інтелектуальних агентів, яка може бути інтегрована в бізнес-процеси банку для виявлення операцій, пов'язаних з відмиванням грошей [43]. Робота Дівії Е. та Умадеві П. присвячена розробці інформаційної моделі, яка базується

на аналізі потоку транзакцій, що дозволяє здійснювати кластеризацію банківських операцій з точки зору ймовірності відмивання грошей [44].

Цікавий підхід представили у своїй роботі Калдера Х., Хейн Д. та Шерлок К., які запропонували платіжну систему з доповненим автоматизованим функціоналом протидії відмиванню незаконно отриманих коштів, яку було ними запатентовано [45]. Колхаткар Д., Фатнані С., Яо Ю. та Мацумото К. представили та запатентували багатоканальну систему протидії легалізації коштів для платіжних карт, яка здійснює моніторинг операцій у режимі реального часу [46]. В роботі Діонісія С. Деметиса розглянуто сучасний напрямок реалізації сучасних систем протидії відмиванню коштів (Anti-money laundering), які базуються на підходах визначення ризиків [47]. У дослідженні Коельо Р., Де Сімоні М. та Преніо Дж. представлений новий напрямок “Suptech”, який є передовим інструментом збору даних та їх аналізу на основі штучного інтелекту та машинного навчання, який застосовується у боротьбі з легалізацією кримінальних доходів [48]. У праці Йонг Лі висвітлені аспекти технічної реалізації AML-інформаційних систем, особливо планування їх впровадження, проектування, аналізу поточного та майбутнього стану, деяких технічних рішень та практичних підходів [49].

Не дивлячись на значний вклад закордонних вчених у вирішення проблеми протидії відмивання коштів, вітчизняна наука відстає в питанні створення, розвитку, удосконалення інформаційних систем та технологій моніторингу, які використовуються для виявлення кримінальних доходів в процесі їх легалізації. Тому вирішення даного питання є досить актуальним для економіки та наукової спільноти України. Практичного досвіду вітчизняних банків пропонується бізнес-модель процесу первинного фінансового моніторингу банку, який здійснюється в умовах автоматизованої обробки інформації (рисунок 2.3).

Запропонована модель (рисунок 2.3) демонструє здійснення автоматизованого моніторингу за 13-ма показниками. Якщо операція не проходить хоча б одну із запрограмованих перевірок, система її блокує та вводить до бази даних запис про ризик, пов'язаний із здійсненням даної транзакції, після чого дані надсилаються до Держфінмоніторингу.

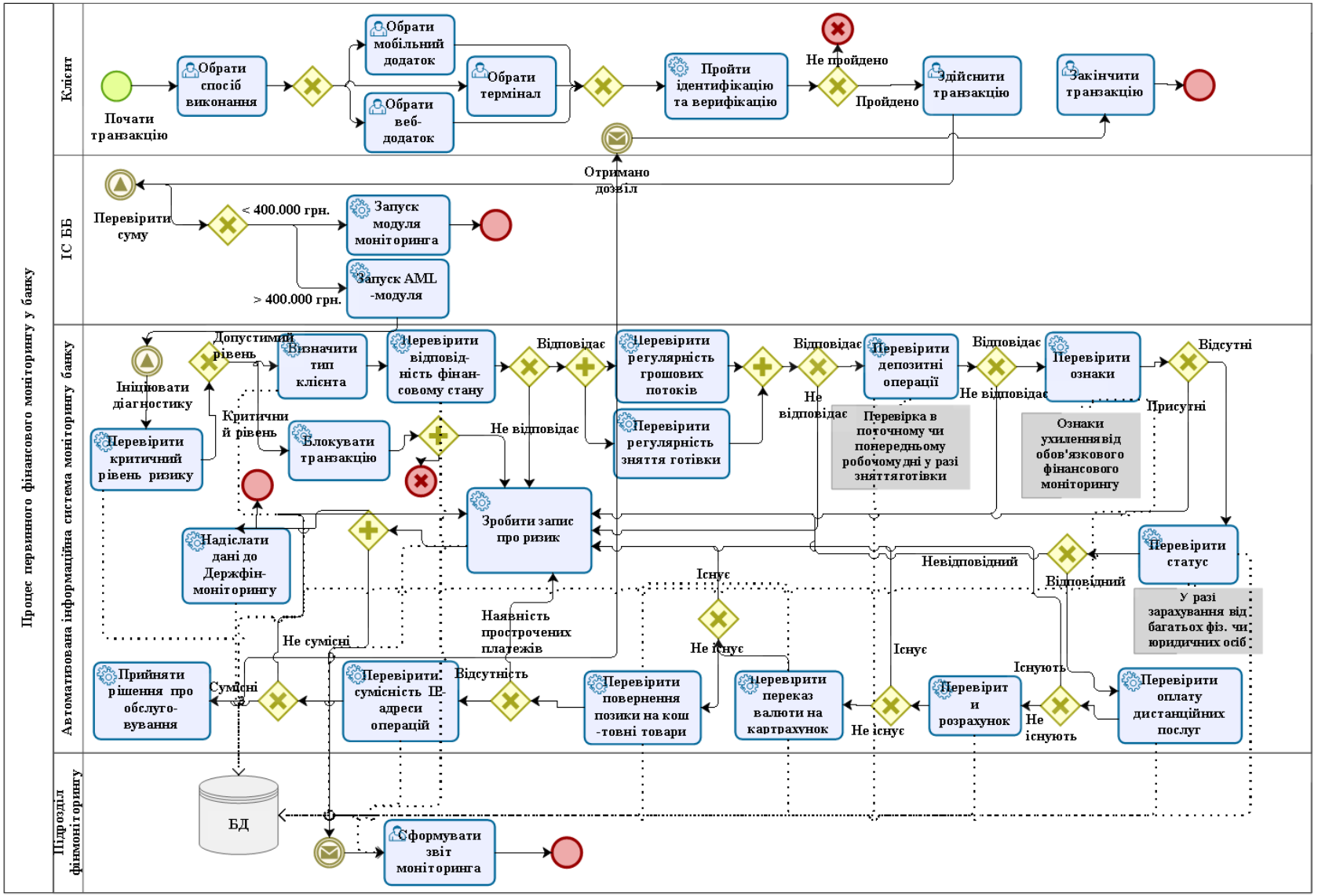

Рисунок 2.3 – Бізнес-модель процесу автоматизованого фінансового моніторингу банку

У разі проходження транзакцією всіх етапів перевірки, приймається рішення щодо обслуговування клієнта та ухвалення даної операції.

Впровадження запропонованої автоматизованої системи моніторингу дозволить розвантажити працівників фронт-офісу щодо перевірки потенційних операцій, пов'язаних з відмиванням грошей. Також її функціонування сприятиме підвищенню ефективності роботи персоналу банку під час проведення фінансового моніторингу. По-перше, це дозволить здійснювати онлайн-перевірку транзакцій на постійній основі. По-друге, вплив працівника на процес перевірки та приховування чи спотворення його результатів більше не буде можливим. Це відбудеться тому, що система передбачає застосування логіки бізнес-правил, яка сприятиме автоматичному вибору тих операцій, які не відповідають заданим умовам. Адміністратор системи несе відповідальність за їх налаштування, а інші банківські працівники не матимуть достатніх прав для цілеспрямованого впливу на процес верифікації. По-третє, запропонована система дозволяє перевіряти більші обсяги операцій щодо їх участі у відмиванні грошей та фінансуванні тероризму. Наприклад, оскільки обов’язковий моніторинг застосовується до операцій, сума яких перевищує 400 000 гривень, то операції з меншими сумами, які можуть мати кримінальні джерела походження та приймати участь у схемах з відмиванням, залишаються поза увагою.

Використання автоматизованої системи полегшить перевірку всього обсягу транзакцій, незалежно від їх суми. По-четверте, перевагою запропонованого рішення є гнучкість налагодження системи у разі зміни законодавства, положень НБУ, інструкцій банків щодо перевірки таких операцій.

При здійсненні симуляцій враховуються два важливих твердження:

– враховуємо, що час на виконання операцій автоматизованою системою та фахівцем є однаковим, що відповідає принципу співставності витрат, якого потрібно дотримуватися у разі визначення ефективності та порівняння витрат;

– симуляції результатів здійснюємо, виходячи з автоматизованої та ручної обробки даних, оскільки запропоновані бізнес-процеси мають вже елементи

оптимізації, тобто процеси, реалізовані на практиці є вже застарілими та прогнозуються удосконалюватися, виходячи із дотримання норм законодавства.

Результати проведеної симуляції по даному процесу представлені на рисунку А.2 у додатку А. Умовами симуляції були наступні: кількість операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); час на виконання 1 запиту в автоматизованій системі фінансового моніторингу – 1 с.; час було задано тільки для операцій перевірки, щоб виявити тільки той його обсяг, який буде витрачено на моніторинг. В результаті отримано, що середній час на перевірку 1 транзакції на предмет наявності ознак фінансового моніторингу 42,35 с., тобто на 1000 операцій буде витрачено 11,77 год. Оскільки симуляція не враховує потужність серверів, то даний показник в дійсності може бути завищеним. На практиці подібна перевірка досвідченим фахівцем займає 20 хвилин. Тобто людині буде потрібно витратити на перевірку 1000 операцій 333,33 годин: ((20 хв. * 1000 оп.) / 60 хв.). Тільки по показнику часу ефективність впровадженого запропонованого процесу буде наступною: автоматизована система у 28,33 рази швидше здійснюватиме перевірку операцій у розрахунку на 1000 транзакцій.

Кількість операцій після перевірки – 877, розрахованих за формулою (2.1), коефіцієнт результативності – 0,877 (за формулою (2.2)). Тобто за умови 1% операцій, які носять ознаки відмивання кримінальних доходів, по кожному з критеріїв перевірки, система буде позитивно ідентифікувати 87,7% операцій, що є високим результатом.

Проведемо симуляцію по ресурсам. Для цього задаємо фахівця, який здійснює моніторинг, та автоматизовану інформаційну систему фінансового моніторингу (AML-модуль). Визначимо їх вартісні оцінки, а саме вартість людино-години та машино-години. Для розрахунків використаємо дані, які відображають фактичні витрати азіатських банків, понесені на AML-систему (AML – Anti-Money Laundering – протидія відмиванню коштів), які за принципами роботи у даному напрямку схожі з українськими. Інформація

міститься у звіті компанії LexisNexis та охоплює період 09.2015 – 01.2016 [50]. Розрахунки наведені у таблиці 2.1:

Таблиця 2.1 – Розрахунки вартості людино-години та машино-години

Назва показника	Фактичне значення, узяте із звіту [50]	Розраховане значення
Кількість опитаних компаній	210	X
Кількість опитаних банків	50%	105
Витрати на AML по всім банкам, дол. США	1500000000	X
Середні витрати на 1 банк, дол. США	X	14285714,29
Витрати на програмне та технічне забезпечення (зовнішні та внутрішні), дол. США	19%	2714285,71
Витрати на персонал, задіяний в AML, дол. США	81%	11571428,57
Час функціонування AML-системи за рік за умови 24-годинної роботи, год.	X	8760
Вартість машино-години, дол. США	X	309,85
Вартість людино-години, дол. США	X	1320,94

Наведені у таблиці 2.1 розрахунки показують вартість машино-години, якщо задіяно увесь комплекс програмно-технічних засобів, та вартість людино-години, якщо задіяно увесь штат працівників. Оскільки значення вартісних показників є комерційною таємницею для банків, то можна скористатися тільки умовним визначенням витрат. Але й ці розрахунки можуть дати уявлення про ефективність. Використовуючи отримані значення вартості машино-години та людино-години, проведемо симуляцію «Аналіз ресурсів», результат якої представлений на рисунку 2.4.

Результати, представлені на рисунку 2.4, показують, що витрати на 1000 транзакцій, перевірених фахівцями фінансового моніторингу, у 4,26 разів вище, ніж витрати на 1000 транзакцій, перевірених AML-модулем.

Scenario information

Название	Scenario 1
Time unit	Seconds
Продолжительность	030,00:00:00

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Фахівець з фінансового моніторингу	100,00 %	0	15 223,83	15 223,83
AML-модуль	0,00 %	0	0	0
	Total	0	15 223,83	15 223,83

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Фахівець з фінансового моніторингу	0,00 %	0	0	0
AML-модуль	100,00 %	0	3 571,02	3 571,02
	Total	0	3 571,02	3 571,02

Рисунок 2.4 – Результати симуляції за ресурсами для бізнес-процесу автоматизованого фінансового моніторингу банку

Можна зробити висновок, що при реалізації запропонованого бізнес-процесу фінансового моніторингу, його ефективність буде вищою для автоматизованого варіанту, ніж для ручного. Для остаточних розрахунків важливо мати інформацію щодо витрат на придбання та впровадження такої системи, а також мати інформацію щодо її результативності.

Перед тим, як побудувати модель бізнес-процесу перевірки транзакцій на наявність ознак кібершахрайств, необхідно сформувати інформаційну модель виявлення ознак шахрайств для операцій, ініційованих зовнішнім середовищем, яка відображає функціонування інформаційних потоків у автоматизованому середовищі. Модель (рисунок 2.5) побудовано у нотації DFD (data flow diagrams), яка є одним із інструментів структурного моделювання та проектування інформаційних систем, із використанням програмного забезпечення “All Fusion Process Modeller” [51].

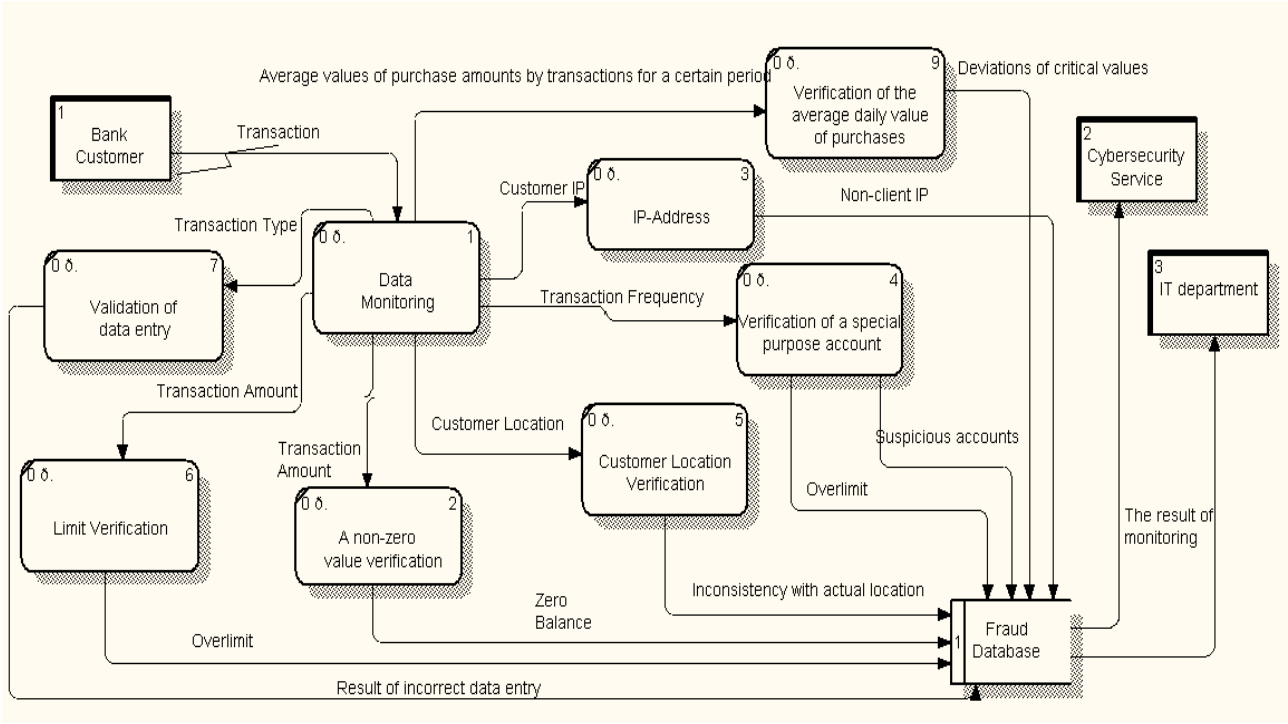

Рисунок 2.5 – Інформаційна модель виявлення ознак шахрайств клієнтів

Побудована на рисунку 2.5 модель відображає інформаційні потоки, які будуть задіяні в модулі перевірки (моніторингу) транзакцій для виявлення ознак шахрайств та їх попередження. Це відбувається шляхом перевірки банківської транзакції (“Transaction”), яку здійснює клієнт (сутність “Bank Customer”), із використанням функцій “Data Monitoring” (перевірка даних). Перевіряються:

– суми транзакцій (“Transaction Amount”) на предмет обнуління рахунку (“A non-zero value verification”). Частіше всього шахрай в процесі шахрайської операції знімає усі кошти з рахунку, що ймовірніше за все не є типовим для власника рахунку. В результаті отримується інформація про те, що на рахунку нульовий баланс “Zero Balance”;

– суми транзакцій (“Transaction Amount”) на перевищення встановлених лімітів (“Limit Verification”). В процесі шахрайства операції можуть перевищувати встановлені банком або клієнтом ліміти “Overlimit”, що дозволить сигналізувати про спробу здійснення незаконної операції;

– локації клієнта (“Customer Location Verification”), оскільки операція може здійснюватися з будь-якої країни, міста та може не відповідати фактичній геолокації клієнта;

– рахунку цільового призначення (“Verification of a special purpose account”). Рахунок може бути в “чорному списку” клієнтів (“Suspicious accounts”) або може бути перевищення лімітів по сумі транзакції (“Overlimit”), якщо цільовий рахунок відкрито в іншому банку;

– IP-адресу клієнта (“IP-address”). У випадку, коли операцію намагаються здійснити з IP-адреси, яка не належать клієнту (“Non-client IP”);

– правильності введених даних (“Validation of data entry”) в залежності від типу транзакції (“Transaction Type”). Результати неправильних спроб (“Result of incorrect data entry”) можуть сигналізувати про ймовірне зламування акаунту клієнта;

– перевищення середньоденної суми покупок (“Verification of the average daily value of purchases”). На вході аналізуються середньоденні значення витрачених коштів та у випадку критичного їх перевищення система може сигналізувати про можливості шахрайства.

Інформація щодо ймовірні порушення, шахрайства, зламування надходить до бази даних шахрайств (“Fraud Database”), обробляється. Результати моніторингу (“The Result of Monitoring”) передаються відділам IT (“IT Department”) та кібербезпеки банку (“Cybersecurity Service”).

У відповідністю із запропонованою інформаційною моделлю (рисунок 5) розроблено бізнес-модель процесу перевірки транзакцій на наявність ознак кібершахрайств у нотації BPMN 2.0 (рисунок 2.6).

Процес виглядатиме наступним чином (рисунок 2.6): клієнт банку або потенційний шахрай здійснює вхід до системи або з використанням веб-сайту, або мобільного пристрою, або терміналу; якщо він успішно пройшов ідентифікацію та верифікацію, система в залежності від суми транзакції буде перевіряти або на предмет відмивання коштів, або на ознаки шахрайства. Система перевіряє операцію на наявність ознак шахрайства із застосуванням модулю моніторингу за критеріями, які представлені на рисунку 2.6.

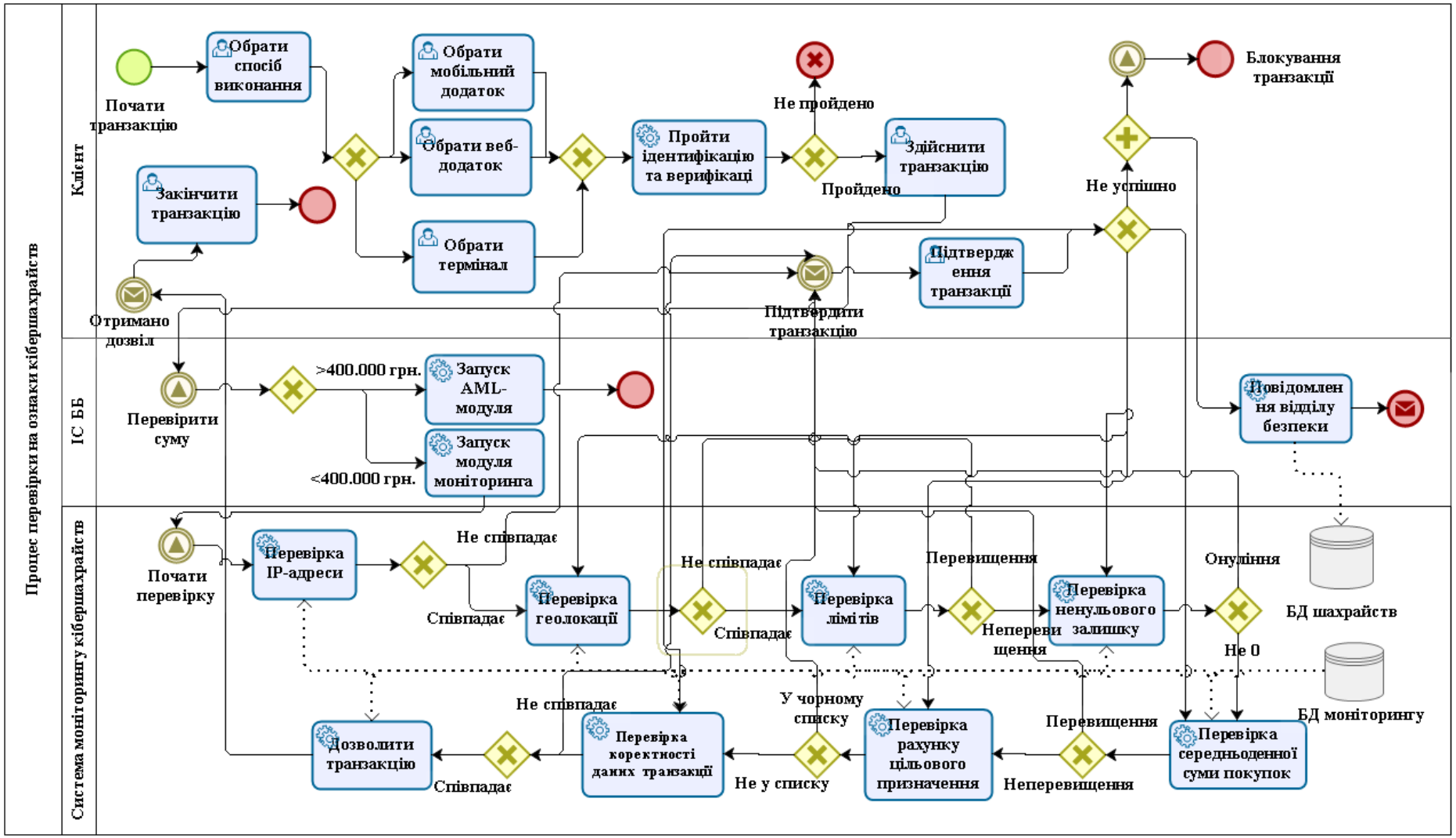

Рисунок 2.6 – Бізнес-модель процесу перевірки транзакцій на наявність ознак кібершахрайств

Якщо результат перевірки не виявляє ознак потенційного шахрайства, то система дозволяє здійснити операцію та клієнт її завершує; якщо результат перевірки виявляє ознаки шахрайства, система робить запит на підтвердження операції шляхом sms-повідомлення або дзвінка, або іншим способом; клієнт здійснює додаткову аутентифікацію; якщо операція була ініційована клієнтом, то її успішно буде завершено; у випадку, якщо клієнт виявиться шахраєм, тобто він не зможе пройти додаткову аутентифікацію, його буде заблоковано та проінформовано систему безпеки.

По даному процесу було проведено симуляції по витратам часу та вартісним витратам ресурсів (рисунок А.3 у додатку А). Умови симуляції: кількість операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); для вузла, який відповідає додатковій автентифікації після того, як система виявила потенційну загрозу, ймовірність була розподілена пропорційно; час на виконання 1 запиту в автоматизованій системі – 1 с. Виявлено, що середній час на перевірку 1 транзакції на предмет наявності ознак кібершахрайств дорівнює 9,86 с., тобто на 1000 операцій буде витрачено 2,71 год.

Виявилося, що 7 операцій не пройшли перевірок та повторної ідентифікації. Оскільки тільки 976 операцій із 1000 підлягали перевірці на ознаки кібершахрайств, то показник результативності склав 99,28%. Це значення може свідчити про високу ефективність системи. На практиці такий результат можливо досягти за рахунок ефективного налаштування параметрів моніторингу, що потребує постійної перевірки з боку відділу внутрішнього аудиту банку.

Проведемо симуляцію процесу по ресурсах. Для цього визначимо собівартість людино-години та машино-години. У звіті компанії Deloitte зазначається, що у 2020 році банки здійснювали витрати на інформаційну безпеку в розмірі від 0,6% всіх витрат, що склало приблизно 9,4% від IT-бюджету або $2688 на 1 людину на рік [52]. Виходячи із того, що у 2020 році було 251 робочий день, та беручи до уваги 8-годинний робочий день, визначаємо, що

вартість 1 машино-години буде дорівнювати $1,34: $2688 / (251 днів * 8 годин). Для порівняння даного процесу із ручною обробкою визначаємо, що заробітна плата банківського аналітика в Україні дорівнює 17500 грн. на місяць [53]. Виходячи із того, що у 2020 році було 251 робочий день, та беручи до уваги 8-годинний робочий день, визначаємо, що вартість 1 машино-людини буде дорівнювати $1,34: $2688 / (251 днів * 8 годин).

Результати проведеної симуляції по ресурсах представлено на рисунку 2.7.

Scenario information

Название	Scenario
Time unit	Seconds
Продолжительность	030,00:00:00

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Аналітик	99.99 %	0	9.12	9.12
Система моніторингу	0.00 %	0	0	0
	Total	0	9.12	9.12

Scenario information

Название	Scenario
Time unit	Seconds
Продолжительность	030,00:00:00

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Аналітик	0.00 %	0	0	0
Система моніторингу	99.99 %	0	3.27	3.27
	Total	0	3.27	3.27

Рисунок 2.7 – Результати симуляції за ресурсами для бізнес-процесу перевірки транзакцій на наявність ознак кібершахрайств

На рисунку 2.7. можна побачити, що у разі забезпечення практично 100% виконання транзакцій автоматизованою системою та аналітиком, витрати ресурсів для першого варіанту є меншими у 2,79 разів. Тобто економічно доцільним є здійснення перевірки із використанням автоматизованого модулю

(3,27 дол. витрат на 1000 операцій) у порівнянні із здійсненням перевірки фахівцем (9,12 дол. витрат на 1000 операцій).

Що стосується випадків внутрішніх шахрайств, то також було розроблено інформаційну модель виявлення шахрайства, якщо шахраєм виступає персонал банку, тобто інсайдери (рисунок 2.8).

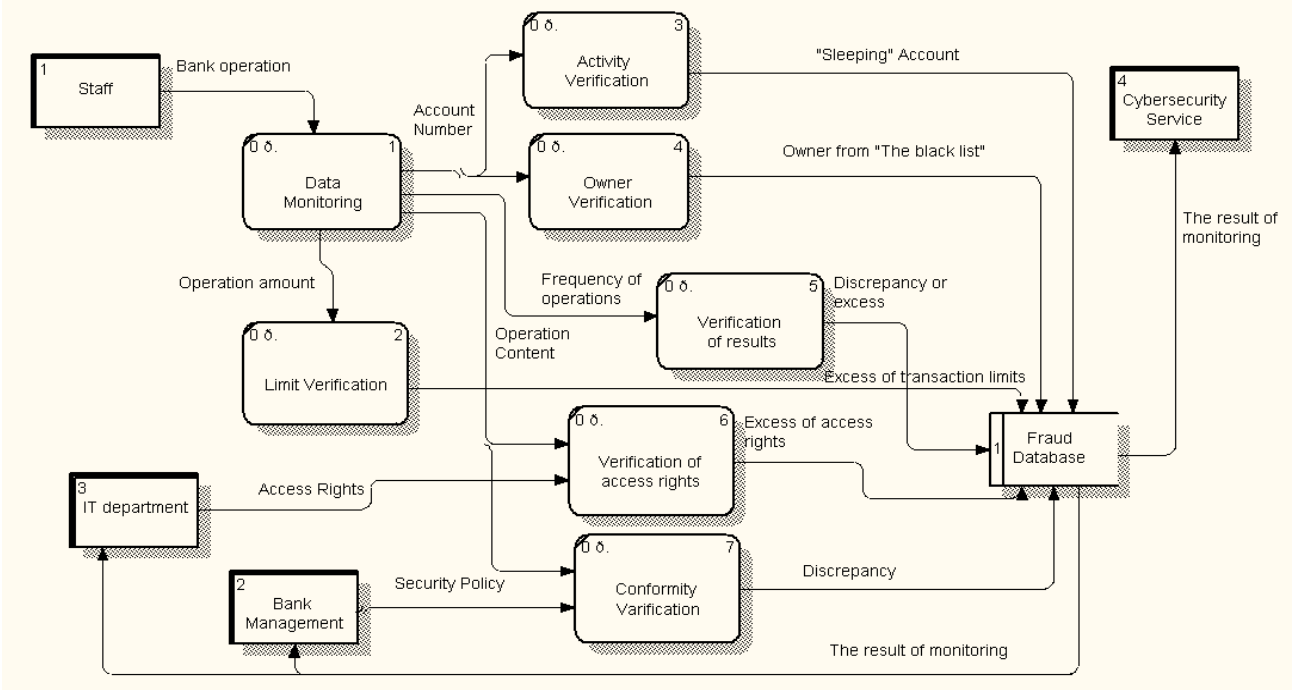

Рисунок 2.8 – Інформаційна модель виявлення ознак шахрайств персоналу банку

Модель, представлена на рисунку 2.8, відображає інформаційні потоки, які циркулюють в процесі перевірки модулем моніторингу (“Data Monitoring”) операцій (“Bank operation”), що здійснюються персоналом банку (“Staff”) на предмет виявлення ознак шахрайства. Перевіряються:

– активності рахунку (“Activity Verification”) у випадку, коли персонал у власних цілях використовує “сплячі рахунки” (“Sleeping Account”);

– власники рахунку (“Owner Verification”), якщо власник присутній у “чорному списку” або є іноземцем, померлим тощо (“Owner from “The black list””);

– ліміти по операціям, що здійснюються у відповідності із вимогами НБУ, політикою банку, посадовими інструкціями тощо (“Limit Verification”), в результаті чого виявляються надлишки по лімітам (“Excess of transaction limits”);

– активності банківських співробітників (“Frequency of operations”) на предмет дотримання банківських нормативів, які співробітник може перевищувати чи недовиконувати (“Discrepancy or excess”);

– операції працівників на відповідність належним їм правам доступу (“Verification of access rights”). Це може бути випадок, коли працівники перевищують свої права (“Excess of access rights”) і, наприклад, проводять операції, які не відповідають їх функціональним обов'язкам та посадовим інструкціям;

– операції працівників на відповідність політиці безпеці банку (“Conformity Verification”). Це можуть бути випадки копіювання бази даних, користування некорпоративною поштою, перегляду рахунків клієнтів, особливо VIP-клієнтів, тощо.

Результати накопичуються у базі даних шахрайств, обробляються та надсилаються відділу кібербезпеки банку (“Cybersecurity Service”), IT-відділу (“IT Department) та менеджменту банку (“Bank Management”).

У відповідністю із запропонованою інформаційною моделлю (рисунок 2.8) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рисунок 2.9).

Процес виглядатиме наступним чином:

– банківський співробітник, який може бути потенційним шахраєм, авторизується в банківській системі та здійснює банківську операцію;

– система моніторингу кібершахрайств перевіряє операцію на предмет кіберзлочину із використанням зазначених критеріїв перевірки, а саме: прав доступу, операцій на відповідність політики безпеки, особи працівника, дотримання банківських нормативів, сплячих рахунків, активностей рахунків та лімітів по операціях ;

– якщо операція відповідає всім критеріям та не містить ознаки шахрайства з боку персоналу, то система дозволяє її здійснення та працівник може її завершити;

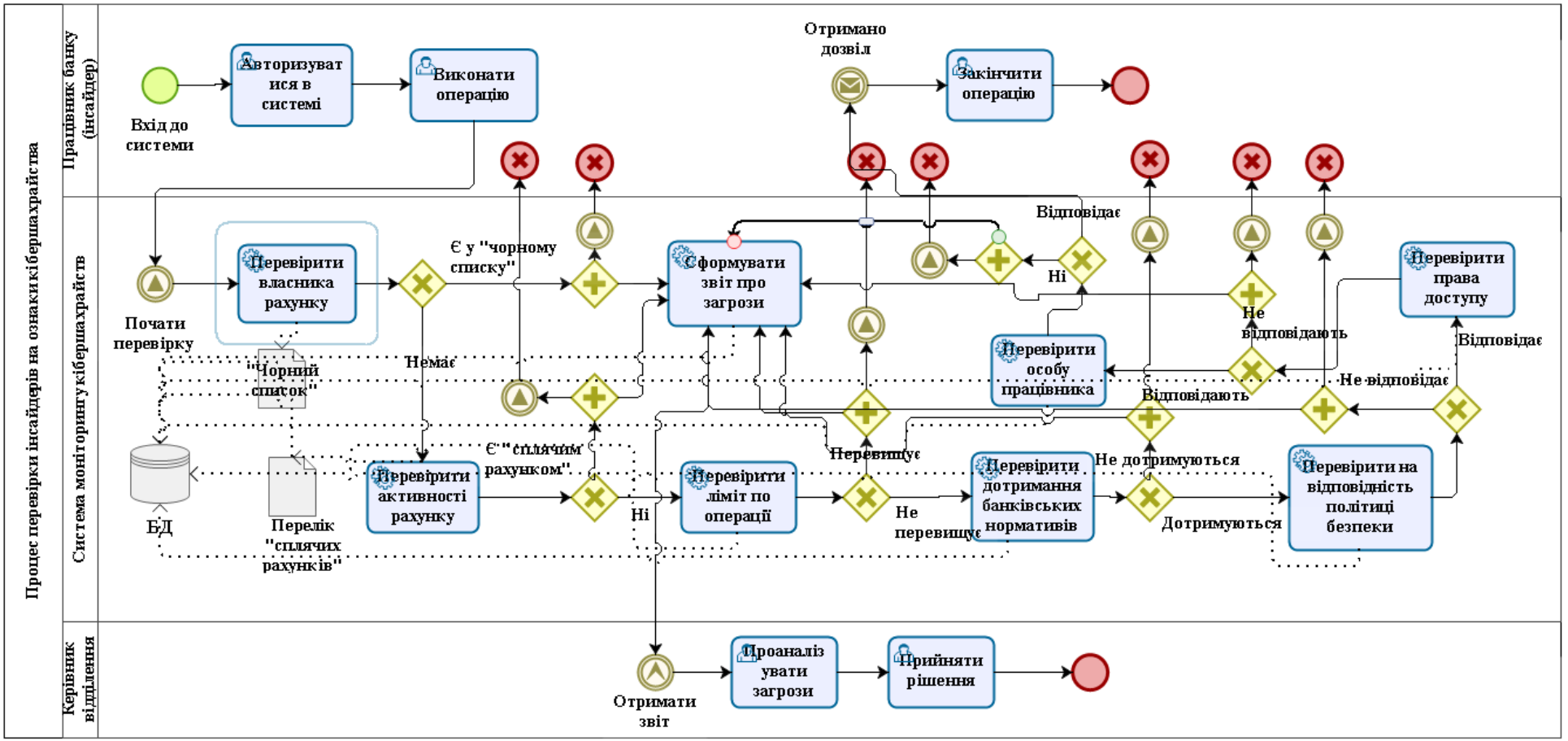

Рисунок 2.9 – Бізнес-модель процесу перевірки дій інсайдерів на ознаки кібершахрайств

– якщо система виявляє ознаки шахрайства, то вона повідомляє керівника відповідного департаменту, де було здійснено операцію, який аналізує інформацію та приймає рішення щодо потенційної ознаки кіберзлочину.

По даному процесу було проведено симуляції по витратам часу та ресурсів (рисунок А.4 у додатку А). За умовами: кількість операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); час на виконання 1 запиту в автоматизованій системі – 1 с. Виявлено, що середній час на перевірку 1 транзакції на предмет наявності ознак кібершахрайств з боку інсайдерів дорівнює 6,86 с., тобто на 1000 операцій буде витрачено 1,90 год. Було виявлено 65 операцій з ознаками шахрайств, відповідно показник результативності системи складає 93,5%. Результати симуляції по ресурсам (рисунок 2.10) показують, що ефективність автоматизованого виявлення ознак кіберзагроз є менш витратним в 2,79 разів.

Scenario information

Название Scenario 1

Time unit Seconds

Продолжительность 030,00:00:00

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Аналітик	100.00 %	0	7.12	7.12
Система моніторингу	0.00 %	0	0	0
	Total	0	7.12	7.12

Scenario information

Название Scenario 1

Time unit Seconds

Продолжительность 030,00:00:00

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Аналітик	0.00 %	0	0	0
Система моніторингу	100.00 %	0	2.55	2.55
	Total	0	2.55	2.55

Рисунок 2.10 – Результати симуляції за ресурсами для бізнес-процесу перевірки дій інсайдерів на ознаки кібершахрайств

Запропонована методика оптимізації бізнес-процесів представляє собою організаційний рівень ключових алгоритмів інтеграції систем фінансового моніторингу і кібербезпеки. Її реалізація дозволить формувати передумови виявлення транзакцій, наслідком яких може бути здійснення шахрайства з боку зовнішнього злочинця чи інсайдера, а також відмивання кримінальних доходів. Впровадження в практичну діяльність розроблених моделей дозволить охопити широке коло операцій незалежно від їх належності до зовнішнього чи внутрішнього середовища. Запропоновані алгоритми дозволять не тільки виявити слабкі місця в захисті інформації, але також вони слугують передумовою конвергенції систем кібербезпеки та фінансового моніторингу в рамках єдиної інтегрованої банківської автоматизованої системи. Це сприятиме здійсненню системного моніторингу для перевірки банківських транзакцій на предмет наявності ознак кібер- і фінансових злочинів. Врешті-решт впровадження запропонованого підходу до оптимізації бізнес-процесів підвищить ефективність й системи управління за рахунок своєчасного прийняття оперативного рішення.

Пункт 2.1 було виконано із використанням матеріалів публікацій виконавців [54].

2.2 Математичне забезпечення алгоритмів виявлення кібершахрайських операцій з кредитними картками

Економічна криза, низький рівень доходів населення, зростання кількості комерційних банків, спеціалізованих фінансових компаній та стрімкий розвиток інформаційних технологій сформували умови для появи банківських шахрайств. Їх мета полягає у незаконному привласненні коштів однією особою або групою осіб. Як правило, процес скоєння банківських шахрайств є прихованим. Масовість їх здійснення може вразити фінансову безпеку банку, призвести до

фінансових збитків та, як наслідок, викликати втрату довіри та репутації серед клієнтів, стати однією з причин банкрутства банківської установи.

Найбільш поширеним видом банківського шахрайства є ті, що пов'язані із кредитними операціями, тобто процесом кредитування клієнтів, а також кредитними картками клієнтів. Це відбувається завдяки спрощення процедури надання кредитів, а також створення гнучких умов для клієнтів щодо використання ними кредитних коштів та засобів платежу. Також судово-бухгалтерською експертизою фінансово-кредитних установ дедалі частіше фіксуються махінації, що стосуються незаконних кредитних операцій, до яких вдаються не тільки позичальники (юридичні та фізичні особи), але й кредитори (банки, фонди, асоціації). Останнім часом відсоток таких шахрайств зростає у порівнянні із іншими видами. Так, у 2020 році шахрайство з кредитними картками зайняло друге місце серед п'ятірки найбільш розповсюджених фінансових злочинів та становило 29,7% (шахрайства із державними пільгами, на які подано заявку, або отримано – 32,0%; різні крадіжки особистих даних – 22,9%; шахрайства із позиками для бізнесу/особистісного користування – 8,1%; податкове шахрайство – 7,3%) [55].

За часту шахрая виявляють вже після того, як було скоєно злочин, тому існує потреба саме у передбаченні потенційних шахрайств. Це можливо тільки в процесі оцінювання ймовірності їх виникнення в ході кредитування клієнтів банку. У контексті даної проблеми є потреба у створенні комплексу заходів для попередження кредитних шахрайств. З цією метою доцільно застосовувати математичні методи, за допомогою яких, можна створювати математичні моделі для проведення ідентифікації банківських транзакцій на предмет шахрайства, або ідентифікації потенційного клієнта банку, який може його скоїти. Використання новітніх інформаційних технологій та мов програмування дозволяє будувати моделі будь-якого рівня складності та спрощувати їх розрахунки.

Проблема виявлення та попередження шахрайств у банківській сфері є досить актуальним напрямом дослідження. Для виявлення його тенденцій

проведемо бібліометричний аналіз наукових досліджень, результати яких опубліковані в міжнародних виданнях, що були проіндексовані у базі даних Scopus. З цією метою було зроблено вибірку таких джерел та шляхом застосування аналітичного програмного забезпечення VOSviewer побудовано карту наукометричної бібліографії досліджень, присвячених проблемі шахрайств щодо кредитування клієнтів банків (див. рис. 2.11).

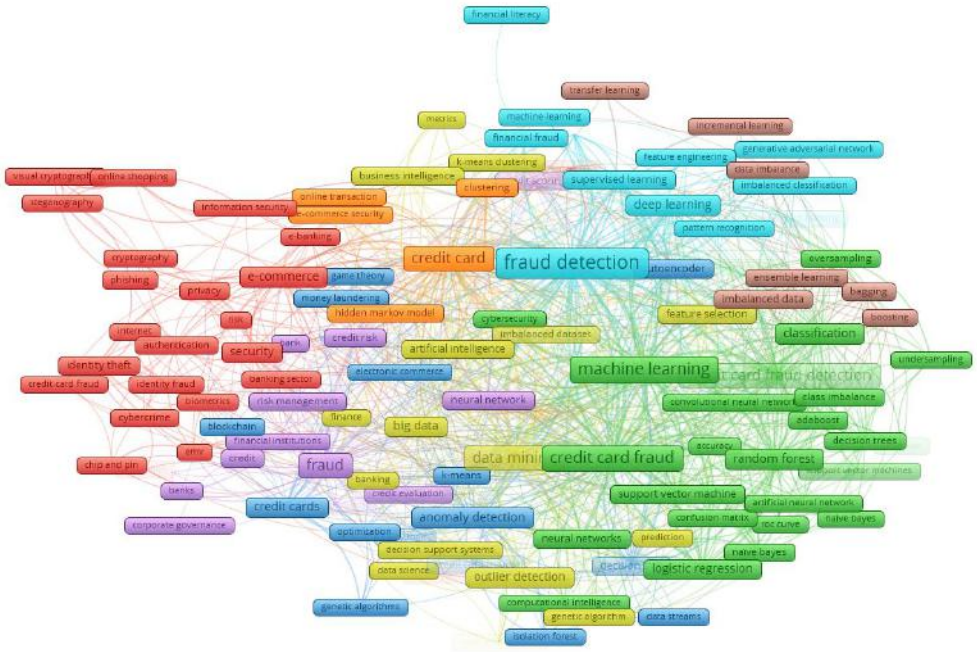

Рисунок 2.11 – Карта наукометричної бібліографії досліджень, присвячених проблемі шахрайств щодо кредитування клієнтів банків

Джерело дослідження: побудовано авторами на основі бази даних Scopus

Червоний кластер досліджень (див. рис. 2.11) охоплює публікації, які стосуються процесів захисту транзакцій електронного банкінгу, інтернет-банкінгу, електронної комерції, онлайн-магазинів, що відбуваються за допомогою засобів інформаційної безпеки – аутентифікації, ідентифікації, криптографії, стеганографії, біометрії, тощо. Тут можна виділити роботи Чжен Л., Лю Г., Ян Ч., Цзян Ч. [56], Пріша П., Нео Х.-Ф., Онг Т.-С., Тео Ч.-С. [57] та інші. Публікації зеленого кластеру (див. рис. 2.11) розкривають напрямки застосування машинного навчання для вирішення проблем кредитних шахрайств у банках. Так, застосовують такі інструменти, як кластерний аналіз, випадковий

ліс, логістична регресія, нейронні мережі, методи опорних векторів, тощо. В даному напрямку працювали Діліп М.Р., Наванет А.В., Абхішек М. [58], Цуй Ю., Сон З., Ху Дж. [59] та інших. Дослідження коричневого кластеру (див. рис. 2.11) перетинаються із попереднім кластером, оскільки вивчаються питання ансамблевого та інкрементного навчання, бегінг та бустінг, що застосовується до незбалансованих даних. Ці аспекти досліджували Ван Р., Лю Г. [60], Собанадеві В., Раві Г. [61] та інші. Роботи помаранчевого кластеру (див. рис. 2.11) стосуються проблематики операцій з кредитними картками, в яких вирішуються питання за допомогою байесівського підходу та моделі Марковіца. Тут можна виділити публікації Чжоу Ю., Сон Х., Чжоу М. [62], Мішра С.П., Кумарі П. [63], тощо. Дослідження синього кластеру стосуються процесів виявлення аномалій у операціях, пов’язаних із відмиванням незаконних коштів у банках та кредитними картками, для чого дана проблема вирішується за допомогою нечіткої логіки, теорії ігор, оптимізації, великих даних та блокчейнів. Ця проблема була розкрита такими науковцями, як Рачавеліас М.Г. [64], Нана З., Сюцзянь В., Чжунцю З. [65] та інші. Публікації блакитного кластеру (див. рис. 2.11) відображають напрям процесу знаходження шахрайств у фінансовій сфері, для чого застосовуються розпізнавання патернів, методи глибокого навчання, навчання з вчителем та без вчителя, feature engineering, тощо. В цій сфері працювали Зоу Х. [66], Мектерович І., Каран М., Пінтар Д., Бркіч Л. [67], тощо. Напрям бузкового кольору (див. рис. 1) розкриває дослідження процесу виявлення шахрайств у банках та інших фінансових інститутах за допомогою ризиків – кредитного та операційного. Тут можна виділити роботи Джанотті Е., Даміан да Сілва Е. [68], Цзоу В., Страуб Д., Венс А., Ян Дж. [69] та інших. Ключовою проблемою жовтого кластеру (див. рис. 2.11) є Data Mining та питання, які з ним пов’язані, а саме штучний інтелект, генетичні алгоритми, великі дані, системи прийняття рішень, бізнес-аналітика. Цим напрямом займалися Цзін Р., Тянь Х., Чжоу Г., Чжан Х., Чжен Х., Цзен Д.Д. [70], Уедраго А.-Ф., Геученн Ц., Нгуєн Ж.-Т., Тран Г. [71], тощо.

Не дивлячись на велику кількість досліджень щодо вирішення проблеми шахрайств, публікації в окреслених напрямах розкривають їх різні аспекти. Стосовно питання оцінювання ймовірності виникнення шахрайства щодо кредитування клієнтів банків, то воно потребує досліджень, особливо для реалій вітчизняних економічних відносин.

Метою дослідження є побудова математичних моделей для оцінювання ймовірності виникнення шахрайства щодо кредитування клієнтів банків, їх реалізація і візуалізація за допомогою мови програмування Python.

Для проведення дослідження окресленої проблеми було узято базу даних з відкритих джерел даних, яка відображає операції кредитування клієнтів та містить основні їх характеристики. Так, набір даних сформували 122 змінні та 307511 спостережень. До незалежних змінних ввійшли такі показники, як: вік, стать, наявність нерухомості, тип нерухомості, наявність рухомого майна, сімейний статус, кількість дітей, тип зайнятості, рівень освіти та ін. Цільовою виступає бінарна змінна, яка є індикатором ймовірного шахрайства в процесі кредитування, а саме: 0 – виявлено клієнта – ймовірного шахрая; 1 – не виявлено клієнта – ймовірного шахрая.

З метою подальшої побудови математичних моделей розроблено концептуальну модель оцінювання ймовірності виявлення ознак шахрайства в процесі кредитування клієнтів банку, яка відображає основні етапи роботи з масивом вхідних даних та представлена на рисунку 2.12.

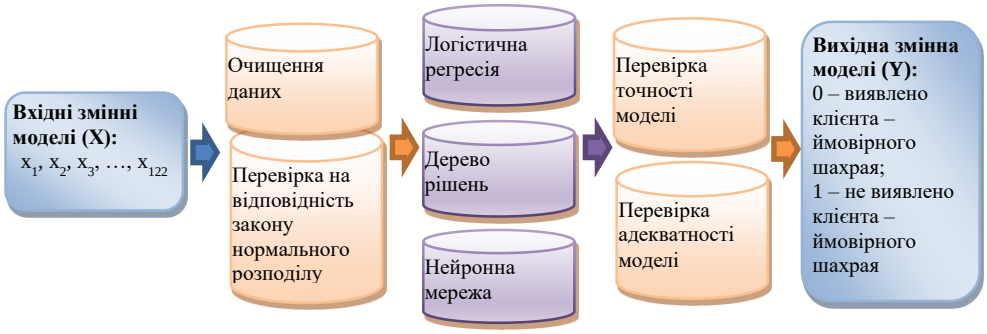

Рисунок 2.12 – Концептуальна модель оцінювання ймовірності виявлення ознак шахрайства в процесі кредитування клієнтів банку

Виходячи з інформації концептуальної моделі (рис. 2.12), процес моделювання передбачає:

– попередню обробку набору даних, а саме їх очищення від пропусків та перевірка на відповідність закону нормального розподілу;

– побудову математичних моделей для оцінки ймовірності виникнення шахрайства у процесі кредитування клієнтів банку: логістичну регресію; дерево рішень; нейронну мережу;

– верифікацію побудованих моделей, тобто перевірка їх точності та адекватності.

Оскільки дослідження стосується оцінки ймовірності виникнення шахрайства, то для вирішення даної проблеми найбільш ефективними є методи інтелектуального аналізу даних Їх переваги та недоліки представлені в таблиці 2.2.

Таблиця 2.2 – Переваги та недоліки математичних моделей

Назва моделі	Переваги	Недоліки
Логістична регресія	має один з найпростіших алгоритмів; є легкою у виконанні та інтерпретації; є простою у оновленні нових даних; є ефективнішою за лінійну регресію	алгоритм чутливий до викидів; необхідна мінімальне значення або відсутність мультиколінеарності між незалежними змінами
Дерево рішень	вимагає менше зусиль та часу на підготовку даних; є дуже легким у поясненні; не вимагає нормалізації даних; дозволяє мати пропущені дані	обчислення можуть бути набагато складнішими за інші алгоритми; передбачає багато часу для навчання моделі; є недостатнім для прогнозування безперервних значень
Нейронна мережа	досить стійка до шуму в навчальних даних; помилки в навчальному наборі не впливають на результат; використовується для швидкої оцінки функції	вимагає паралельної обробки даних; складнощі з відображенням; результативні значення не є оптимальними

Логістична регресія – це статистичний регресійний метод, що застосовується у випадку, коли залежна зміна являється бінарною, тобто може набувати значення 0 або 1. Логістична регресія є прогностичним аналізом та

використовується для опису даних та пояснення взаємозв'язку між одним залежним фактором (змінною) та однією або декількома незалежними. Її математичний вираз можна представити формулою (2.3):

$$\mathrm{P}(\hat{y}=1)=\frac{1}{1+exp^{-\hat{y}}}=\frac{1}{1+exp^{-(\beta_0+\beta_1 x_1+\cdots+\beta_n x_n)}}, \quad (2.3)$$

де $x_1, x_2, \ldots, x_n$ – множина незалежних змінних-факторів, які впливають на результатний показник;

$\beta_0, \beta_1, \ldots, \beta_n$ – множина параметрів регресії, які необхідно оцінити в процесі побудови моделі логістичної регресії;

$\hat{y}$ – залежна змінна-фактор, значення якої прогнозується в процесі моделювання;

$\mathrm{P}(\hat{y}=1)$ – ймовірність виникнення випадку, при якому значення результативної змінної дорівнює 1.

Для побудови логістичної регресії використовувалася мова програмування Python. Для її реалізації дані були очищені від пропущених значень та перевірені на відповідність закону нормального розподілу. Далі набір вхідних даних було розділено на дві вибірки – тестову та тренувальну. Після здійснення даної процедури було оцінено точність опису залежної змінної незалежними, результат чого представлений на рисунку 2.13.

```
print("Training set score: %f" % LogReg.score(X_train, Y_train))
print("Test set score: %f" % LogReg.score(X_train, Y_train))
```

Training set score: 0.930932
Test set score: 0.936000

Рисунок 2.13 – Точність опису залежної змінної

Результати показують, що частка правильних прогнозів у тренувальній вибірці становить 93,09%, а у тестовій – 93,60%, що свідчить про адекватність даних обох вибірок та високу точність прогнозування.

Після отримання придатного для моделювання набору, було побудовано модель логістичної регресії. Оскільки для отримання адекватної моделі необхідно, щоб її параметри були статистично значущими, то було проведено їх оцінку із використанням значення p-value та довірчих інтервалів. Статистично незначущі фактори було усунуто з моделі. Процедура повторювалася доти, доки було отримано модель із усіма статистично значущими параметрами. Так, було проведено 9 ітерацій. Результати логістичної регресії представлені на рисунку 2.14.

```
Optimization terminated successfully.
         Current function value: 0.627703
         Iterations 9
                           Logit Regression Results
==============================================================================
Dep. Variable:                 TARGET   No. Observations:                40416
Model:                          Logit   Df Residuals:                    40409
Method:                           MLE   Df Model:                            6
Date:                Fri, 11 Jun 2021   Pseudo R-squ.:                 -1.539
Time:                        11:24:35   Log-Likelihood:                -25369.
converged:                       True   LL-Null:                       -9992.8
Covariance Type:            nonrobust   LLR p-value:                    1.000
=====================================================================================================
                                        coef    std err          z      P>|z|      [0.025      0.975]
-----------------------------------------------------------------------------------------------------
NAME_TYPE_SUITE_Other_A               -4.1769      1.008     -4.145      0.000      -6.152      -2.202
NAME_FAMILY_STATUS_Widow              -3.4096      0.293    -11.622      0.000      -3.985      -2.835
Occupation type_Accountants           -2.8988      0.090    -32.302      0.000      -3.075      -2.723
Organization Type_Electricity         -5.2689      1.003     -5.255      0.000      -7.234      -3.304
Organization Type_Industry: type 3    -3.3706      0.322    -10.482      0.000      -4.001      -2.740
Organization Type_Military            -3.0647      0.184    -16.679      0.000      -3.425      -2.705
Organization Type_School              -2.6126      0.128    -20.489      0.000      -2.862      -2.363
=====================================================================================================
```

Рисунок 2.14 – Результати оцінки та відбору параметрів логістичної регресії

На рисунку 2.14 можна побачити, що найбільш значущими виявилися 7 параметрів логістичної регресії. Також було отримано від’ємне значення коефіцієнту детермінації. Оскільки в даному випадку розраховувався псевдо-R2,

то він не має корисності, тому що не обмежений знизу. Тому для перевірки моделі на адекватність доцільно використати ROC-криву. Результати її побудови представлені на рисунку 2.15.

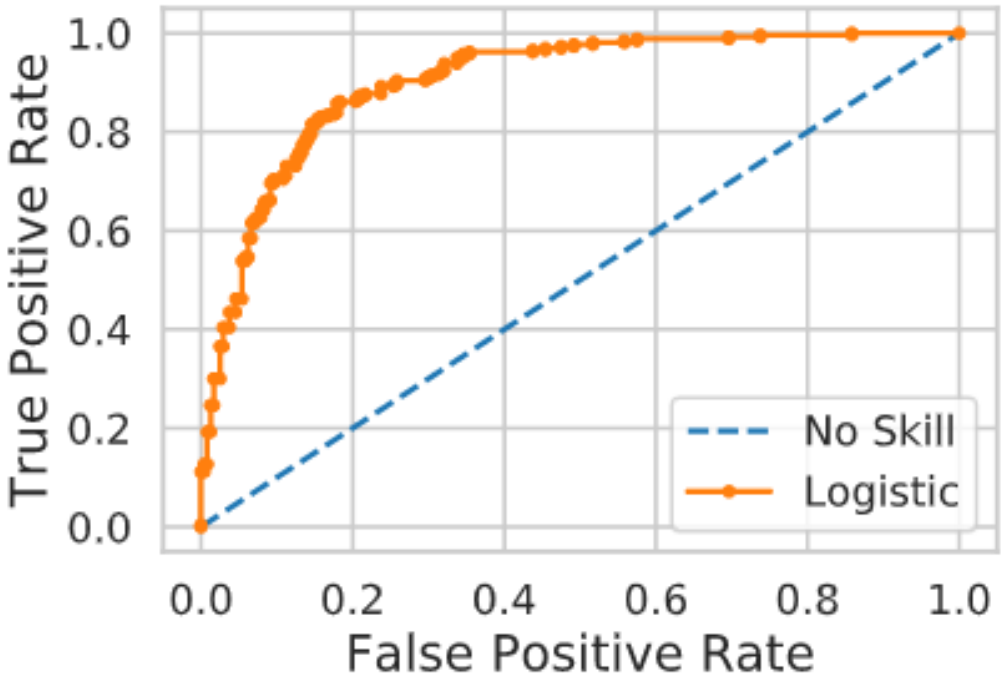

Рисунок 2.15 – ROC-крива для логістичної регресії

На рисунку 2.15 показано, що логістична модель має істинне позитивне значення, яке наближається до верхнього лівого кута (до 1), тобто ROC-крива показує високу залежність кількості правильно класифікованих позитивних прикладів від кількості неправильно класифікованих негативних прикладів. Результати логістичної регресії є придатними для оцінки ймовірності виникнення шахрайств в процесі кредитування. Отриманні значення запишемо у вигляді математичної моделі логістичної регресії – формули (2.4):

$$P = \frac{1}{1 + E^{-2.579 - 4.1769x_1 - 3.4096x_2 - 2.8988x_3 - 5.2689x_4 - 3.3706x_5 - 3.0647x_6 - 2.6126x_7}} \quad (2.4)$$

Прогнозні оцінки експоненти цієї моделі вказують на те, що коли буде змінюватися значення незалежних змінних $x_1, x_2, \dots, x_7$ на 1, ймовірність шахрайської операції буде зростати або зменшуватися у кількість разів, що відповідає визначеному значенню параметра. Наприклад, при зміні значення сімейного статусу (x_2), ймовірність шахрайства знизиться у 3,4096 разів.

Наступний метод математичного моделювання – дерево рішень. Спочатку для його побудови береться весь набір даних, що представляється кореневою вершиною. Потім визначаються варіанти розбивки даних на гілки, що відповідають кореневому вузлу. Дані гілки утворюють дерево, повернене корою вниз. Способи розбивки множини даних називають вирішальним правилом, яке відбувається за формулою (2.5):

$$a_{ik} = \begin{cases} 1, \ s_i = r_k; \\ 0, \ s_i \neq r_k, \end{cases} \tag{2.5}$$

де $a_{ik} = 1$, якщо умова s_i для правила r_k виконується;

$a_{ik} = 0$, якщо умова s_i для правила r_k не виконується;

$S\{s_i\}, i = \overline{1, l}$ – множина умов, що описують параметри обраної предметної області.

Дане правило фактично являє собою алгоритм «якщо, …то..» та ділить множину записів на дві частини [72].

Перевірка точності наборів даних виявила, що точність тестового набору дорівнює 0,9915, а тренувального – 1,0. Це означає, що точність прогнозування майже дорівнює 100%. Дерево рішень показало кращий результат ніж логістична регресія у значеннях точності опису залежної змінної незалежними змінними. Після цього проведемо побудову дерева рішень, а також здійснимо його навчання з метою отримання найкращої комбінації даних. Його результати представлені на рисунку 2.16.

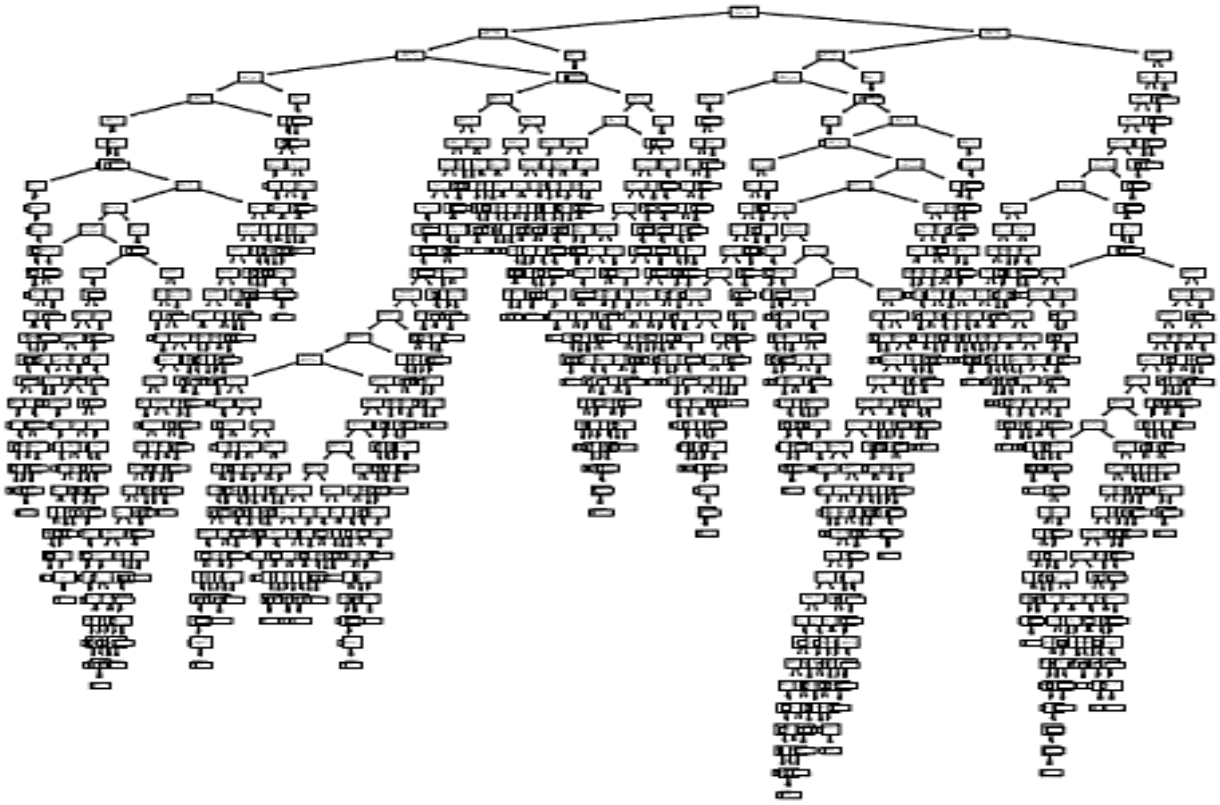

Рисунок 2.16 – Дерево рішень

Побудувавши дерево рішень можна зробити висновок, що воно має досить складну для інтерпретації структуру, хоча має високу точність прогнозування цільової змінної, ніж логістична регресія.

Третьою моделлю є нейронна мережа, яка представляє собою алгоритм, що поєднує в собі біологічні принципи та вдосконалену статистику для вирішення задач у різних сферах. Нейронна мережа приймає базову модель нейронних аналогів, пов'язаних між собою різними способами.

Проведена перевірка точності вибірок виявила, що нейронна модель забезпечує гарну точність, що є вищою за базову (66%): для тренувального набору 100,00 %, для тестового – 86,67%. Дана модель може бути удосконалена за допомогою зміни аргументів в процесі здійснення оцінювання параметрів нейронної мережі або шляхом перехресної перевірки.

В результаті побудови та проведення навчання нейронної мережі було отримано модель, графічна інтерпретація якої представлена на рисунку 2.17.

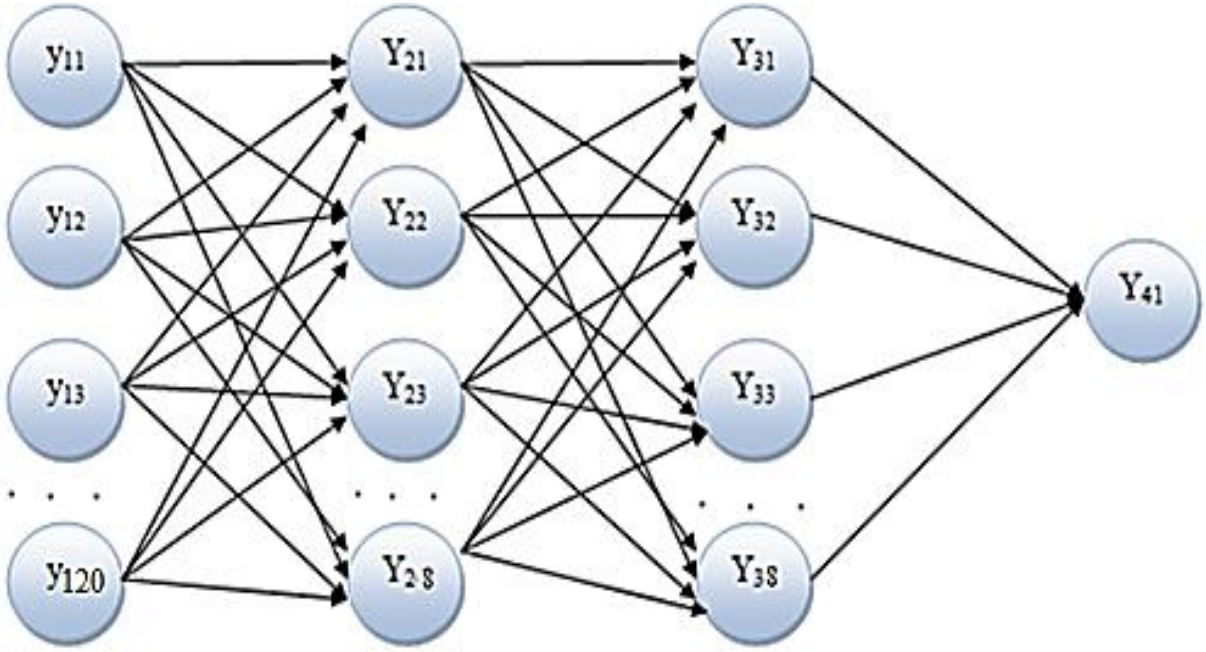

Рисунок 2.17 – Графічна інтерпретація отриманої нейронної моделі

На рисунку 2.17 можна побачити, що мережа має три приховані шари. В першому буде 120 вихідних змінних, у другому – 28, у третьому – 38. На виході отримаємо фінальне рівняння. Фрагмент математичної інтерпретації нейронної мережі представлений формулами (2.6)-(2.13):

$$y_{11} = -0.1161x_1 - 0.5501x_2 + 0.3569x_3 + \cdots + 0.2065x_8 \quad (2.6)$$

$$y_{12} = -0.6962x_1 + 0.3309x_2 + 0.2792x_3 + \cdots + 0.2065x_8 \quad (2.7)$$

…

$$y_{120} = 0.3499x_1 - 0.4575x_2 + 0.0761x_3 + \cdots + 0.3483x_8 \quad (2.8)$$

$$y_{21} = -0.3926x_1 - 0.6920x_2 + \cdots - 0.1789x_8 \quad (2.9)$$

…

$$y_{28} = 0.5144x_1 - 0.0822x_2 + \cdots - 0.2014x_8 \quad (2.10)$$

$$y_{31} = -4.4977x_1 + 9.19e^{-01}x_2 + 0.27 + \cdots - 3.5448e^{-01}x_8 \quad (2.11)$$

…

$$y_{38} = 4.44e^{-02}x_1 - 3.4965e^{-02} + \cdots + 3.4229e^{01}x_8 \quad (2.12)$$

$$y_{41} = 0.2948x_1 - 0.92x_2 + \cdots - 0.6388x_8 \quad (2.13)$$

Після побудови трьох моделей проведемо їх оцінку за точністю та якістю опису моделей тренувальним та тестовим набором даних (див. табл.2.3).

Таблиця 2.3 – Порівняння точності та якості побудованих моделей

Назва моделі	Точність, %		MSE	
	Тестові дані	Тренувальні дані	Тестові дані	Тренувальні дані
Дерево рішень	99,15	100,00	0,008	0,000
Логістична регресія	96,60	93,00	0,064	0,069
Нейронна мережа	86,70	100,00	0,089	0,004

Отримані результати точності моделей (див. табл. 2.3), дозволяють зробити висновок, що дерево рішень найкраще моделює ймовірність шахрайства в процесі кредитування банківських клієнтів, оскільки її точність і для тестового, і для тренувального практичного дорівнює 100%. Відповідно, значення середньоквадратичної похибки (MSE) є дуже малим та наближається до 0. Логістична регресія та нейронна мережа є майже рівноцінними, оскільки: логістична регресія має вищу точність для тестових даних, ніж нейронна мережа, а нейронна мережа, навпаки, має вищу точність для тренувального набору даних. Що стосується середньоквадратичної похибки, то її значення для обох моделей є також малим та наближається до 0. В цілому, усі три моделі дають гарні результати, тому їх можна застосовувати для оцінювання ймовірності виявлення шахрайства у процесі кредитування клієнтів банків.

Проблема шахрайств у фінансовому секторі на сьогоднішній день є досить актуальною, що пояснюється впливом різних факторів. Тому на практиці існує потреба не тільки у виявленні таких випадків, але й у попередженні їх настання. Це можливо здійснити тільки із використанням сучасних інформаційних технологій та математичних методів. У даному дослідженні ця проблема вирішувалася за допомогою побудови трьох математичних моделей, що належать до класу інтелектуального аналізу даних, а саме логістичної регресії, дерева рішень та нейронної мережі. Відповідні розрахунки було проведено із використанням сучасної мови програмування Python. Дослідження передбачало формування такого набору даних, який включав не тільки кількісні

характеристики клієнтів банку (дохід, депозити), але й якісні параметри – рівень освіти, тип зайнятості, сімейний стан, тип житла та ін. В результаті було отримано математичну модель логістичної регресії, яка показала досить високі значення частки правильних прогнозів у тренувальній вибірці (93,09%) та тестовій (93,60%). Тобто обидві вибірки є адекватними та демонструють високу точність прогнозування. В результаті проведеного відбору найбільш значущих параметрів було побудовано логістичну регресію із використанням семи змінних. Її гарну якість підтвердила ROC-крива. Також було побудовано дерево рішень, модель якого продемонструвала точність наборів даних вищу, ніж для логістичної моделі (для тестового набору – 0,9915, а для тренувального – 1,0). Не дивлячись на її кращі результати, модель виявилася дуже складною для інтерпретації. Нейронна мережа показала гарні показники точності вибірок: для тренувального набору 100,00 %, для тестового – 86,67%. На останньому етапі було проведено розрахунок точності та якості моделей, в результаті чого найкращі результати продемонструвала модель дерева рішень, а нейронна мережа та логістична регресії також показали гарні результати, хоча й дещо нижчі, ніж для дерева рішень. Щоб мати постійне уявлення про ймовірні шахрайства результати повинні регулярно доповнюватися, оновлюватися для використання їх у фінансових установах, що дозволить вчасно реагувати на злочинні дії та попереджати їх виникнення у процесі надання кредиту.

Пункт 2.2 було виконано із використанням матеріалів публікацій виконавців [54, 73].

3 АНАЛІЗ МОЖЛИВИХ СЦЕНАРІЇВ ВЗАЄМОДІЇ СИСТЕМ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ФІНАНСОВИМ ЗЛОЧИНАМ

3.1 Збалансованість детермінант розвитку країн: барицентрична модель

Динамічні процеси, які відбуваються зараз у суспільстві, призводять до того, що деякі сфери його життєдіяльності розвиваються не досить рівномірно. Це можна спостерігати на прикладі стрімкого розвитку інформаційних технологій, який за останнє десятиліття призвів до трансформації багатьох процесів економічної, політичної та соціальної сфер. В даному контексті його наслідки є в більшій мірі позитивними для суспільства та країни, оскільки призводять до побудови нових компаній сфери IT, створення нових робочих місць, розширення можливостей людини за рахунок використання нею останніх розробок. Що стосується інших аспектів, які також впливають на розвиток країни, то їх вплив може бути як позитивним, так й негативним. Відповідно ця проблема потребує вивчення та удосконалення в частині визначення тих детермінант, які впливають на забезпечення сталого розвитку країни за умови балансування між потребами суспільства та захистом інтересів майбутніх поколінь, а також рівномірного розвитку усіх сфер життєдіяльності суспільства. Так, це повинно узгоджуватися із цілями сталого розвитку Організації Об’єднаних Націй, які було оголошено 25 вересня 2015 року на Саміті ООН, а також із стратегіями розвитку країн, що розробляються відповідно до їх пріоритетів. Саме тому метою даного дослідження було обрано визначення рівня збалансованості соціальних, економічних, політичних детермінант та детермінант цифрової спроможності і кібербезпеки, як композитних таргетів, характерних для будь-якої країни світу. Побудова відповідної моделі дозволить визначити ті таргети, що впливають на незбалансованість розвитку країни, а також окреслити відповідні напрямки реалізації державної політики уряду країни щодо розробки ефективних стратегій, які зазначають пріоритети для

підвищення рівня добробуту населення, якості соціальних стандартів та рівня його життя, подолання політичних та військових конфліктів, вирішення екологічних проблем в умовах тих викликів перед суспільством, які генерують глобальні проблеми.

Збалансований розвиток країни передбачає, що зміни, які відбуваються, носять системний характер та мають рівномірний вплив на всі сфери. Це може забезпечуватися рядом детермінант, серед яких найбільший вплив мають економічні [74]. Суттєвий дисбаланс в економіці країн викликають недосконаліть законодавчої бази та наявність корупційної складової, вплив яких порушує макроекономічну стабільність [75]. Автори [76] емпірично довели, що криза довіри у фінансовому секторі також дестабілізує економіку. Автори [77] досліджували залежність макроекономічної стабільності від фіскальної децентралізації та зробили акцент на децентралізації витрат, децентралізації доходів та децентралізації витрат одночасно. Формування системи фінансування сталого розвитку є одним з головних стратегічних пріоритетів, що повинно відбуватися з урахуванням особливостей функціонування корпоративного сектору [78, 79]. Автори [80] доводять, що грошові кошти є не тільки платіжним засобом, але й виступають інструментом пропаганди та відмивання нелегальних доходів, що виступає фактором розвитку тіньового сектору. Це в свою чергу впливає на інноваційний потенціал [81]. Формування сприятливого інвестиційного клімату в країні є одним з напрямів підвищення рівня добробуту населення країни, що математично доведено в роботі [82]. Оптимальний розподіл частки приватних та державних інвестицій було змодельовано в контексті економічного розвитку [83].

Рівень розвитку країни суттєво впливає на умови забезпечення суспільного добробуту, формування стійких парадигм його покращення, а також призводить до якісних змін у суспільних відношеннях. З іншого боку, соціальні детермінанти формують відповідну модель суспільного життя, наслідки якої є драйвером сталого розвитку [84]. Для даного аспекту є важливим забезпечення саме соціальної безпеки, коли існують мінімальні ризики життєдіяльності населення

в країні [85]. Формування кращого соціального клімату в країні є одним з головних джерел залучення інвестицій [86]. Також забезпечення якісної освіти [87] (Lyeonov & Liuta, 2016) та системи охорони здоров'я [88] формують модель успішного суспільства. Тріада впливу економічних, соціальних та політичних детермінант в контексті забезпечення зростання економічної безпеки країн була проаналізована та із використанням методу експоненційного згладжування було зпрогнозовано рівень інноваційних змін [89].

Окрім економічних, політичних та соціальних детермінант на розвиток країни можуть впливати й екологічні фактори. Дане питання було досліджено [90] та визначено, що існує зв'язок між валовим внутрішнім продуктом на душу населення, викидами парникових газів, відновлюваними джерелами енергії у загальному кінцевому споживанні енергії та екологічні інвестиції, а також їх взаємодія позитивно впливає на розвиток окремих сфер життєдіяльності. Автори [91] досліджували взаємозв'язки між економічними, соціальними та екологічними аспектами розвитку та побудували для України та ЄС екологічну криву Кузнеця. Синергетичний ефект від взаємодії зелених інвестицій та інституційними детермінантами проявляється у національній економіці та призводить до зниження її енергоефективності [92]. Існування конвергенції між податковою та екологічною системами було доведено на основі бета- та сігма-конвергенцій [93].

Наслідки четвертої промислової революції сприяли цифровізації багатьох процесів, що впливає, в першу чергу, на динамічність розвитку економіки країни та підвищує рівень її національної безпеки. Новіковим В. [94] на основі бібліометричного аналізу досліджень довів, що збалансованість розвитку країни в більшій мірі залежить від її соціальної, економічної та інформаційної безпеки. Процеси цифровізації є актуальними також й для фінансового сектору економіки, де існують найбільші потреби у цифровізації фінансових послуг. В умовах зростання інформаційних потоків повинна забезпечуватися конфіденційність великих даних. Паралельно також зростають ризики фінансових втрат завдяки здійснення масових кібератак, що призводить до

дестабілізації процесів та систем, а також гальмування їх розвитку [95]. Хоча більшість країн намагаються вирішувати цю проблему шляхом застосування технологій штучного інтелекту, але нажаль попередження кібератак залишається важливою задачею забезпечення національної безпеки країн. Тому при визначенні детермінант слід враховувати не тільки ті фактори, що характеризують розвиток ІТ галузі, але й напрям інформаційної безпеки [96].

Для проведення дослідження збалансованості розвитку країн обираємо тріаду економічних, політичних та соціальних детермінант, а також детермінант, що характеризують розвиток інформаційних технологій та кібербезпеки, групу яких буде названо як цифрова спроможність а кібербезпека. Оскільки екологічні фактори мають більш вузько направлений вплив на розвиток країни, то в даній роботі їх не буде враховано для побудови моделі.

Для моделювання в сфері економічного, політичного, соціального, інформаційного розвитку застосовується широкий спектр математичних методів. Ці проблеми вирішувались науковцями шляхом побудови оптимізаційних моделей [97], структурного моделювання [98], методів інтелектуального аналізу даних [99], гравітаційного моделювання [100], нечітких множин [101], ймовірнісних методів [102], економетричного інструментарію [103], статистичного аналізу [104].

На збалансованість розвитку країн можуть впливати різні детермінанти, які або призводять до підвищення її рівня, або знижують його. Для обґрунтування їх вибору було застосовано методи наукового пізнання, які дозволили визначити найбільш релевантні показники для кожного композитного таргету. Так, вимір цифрової спроможності і кібербезпеки формується під впливом тенденцій розвитку ІТ-галузі та її складових, рівня цифрового розвитку та безпекової складової. Оскільки не існує єдиних підходів до визначення даного виміру, то в дану групу було віднесено 5 ключових індикаторів, які характеризують: слабкі сторони країн щодо кібербезпеки та покращення можливостей для них шляхом розробки стратегії кібербезпеки та відповідних стандартів (The Global Cybersecurity Index – GCI), рівень готовності країн

протидіяти кіберзагрозам та керувати кіберінцидентами (The National Cyber Security Index – NCSI), рівень розвитку інформаційних та комунікаційних технологій в країні (ICT Development Index – ICTDI), ступінь технологічної готовності країни для застосування новітніх інформаційно-комунікаційних технологій в різних сферах життєдіяльності (Networked Readiness Index – NRI), ступінь відповідності цифровізації країни рівню її кібербезпеки для формування рекомендацій щодо коректування програм кібербезпеки (Digital Development Level – DDL). Оскільки значення цих індикаторів позитивно впливає на інтегральне значення виміру цифрової спроможності і кібербезпеки, тобто із зростанням їх значення підвищується його рівень, то враховуємо їх як показники-стимулятори. Вважається, що країна, для якої характерне високе значення композитного таргету цифрової спроможності і кібербезпеки, має потужний розвиток інформаційних технологій та вважається країною із найвисоким рівнем інформаційної безпеки.

Фактори економічного розвитку країни є ключовим компонентом у здійсненні його збалансованості, оскільки дозволяють оцінити рівень добробуту громадян (The Global Competitiveness Index), умови ведення бізнесу у країні та захисту прав власності (Ease of Doing Business), вплив розвитку фінансових систем на зростання, стабільність та нерівність різних економік (Financial Development Index), етнічну, расову, регіональну, освітню, тощо нерівність, яка формує економічну різницю між даними групами, що врешті решт впливає на економічний розвиток країни (Uneven Economic Development Index), людські можливості контролювати власну працю та майно, рівень власного споживання та інвестування (Economic Freedom Index). Чим вище рівень економічного розвитку країни, тим більше можливостей для неї бути лідером на світових ринках та забезпечувати високий рівень життя її населення. Серед обраних індикаторів тільки Uneven Economic Development Index є показником дестимулятором, із збільшенням значення якого зростає інтегральний рівень таргету економічного розвитку. Інші індикатори є стимуляторами за своєю сутністю.

Соціальний вимір направлений на визначення спроможності країни забезпечити населенню високий рівень життя, що полягає у створенні сприятливих умов для отримання населенням таких соціальних благ, як освіта, якісні медичні послуги, рівень «екологічного сліду», забезпечення та підтримання миру в середині країни, тощо. Для аналізу даного композитного таргету було обрано індикатори, що вимірюють якість поточного життя населення (Happiness Index), рівень забезпечення країнами основних потреб людини, їх добробуту та можливостей для прогресу (Social Progress Index) та таких основних характеристик людського потенціалу, як рівень життя, грамотності, освіченості і довголіття (Human Development Index). Обрані детермінанти є показниками-стимуляторами, тому високе значення інтегрального рівня соціального виміру свідчитиме про високий рівень забезпечення соціальних стандартів для життя населення в даній країні.

Політичний розвиток будь-якої країни є неодмінна частина її загального розвитку, оскільки характеризує динаміку політичного життя країни, її можливості взаємодіяти із іншими країнами у зовнішньому політичному просторі, налаштовувати діалог між державою та населенням. Існування політичних коливань може призводити до дестабілізації соціальних настроїв населення та гальмування розвитку економіки, тому його вимірювання є вкрай важливим для визначення рівня збалансованого розвитку країни. Тому для визначення його інтегрального рівня було обрано індикатори, які вимірюють: рівень ймовірності того, що уряд країни може бути дестабілізований або зруйнований засобами, які носять неконституційний та насильницький характер (Political Stability Index), якість демократії у країні з урахуванням оцінок виборчого процесу, громадянської свободи, функціонування уряду, політичної культури (Democracy Index), якість діяльності уряду країни на основі оцінки якості державних послуг та органів, якості формування та реалізації політичних заходів, ступеня незалежності від політичного тиску, тощо (Government Effectiveness Index), рівень корупційної складової державного сектору (Corruption Perceptions Index). Зростання значень обраних детермінант впливає

на зростання рівня композитного таргету, що свідчить про політичну стабільність в країні та високий рівень її політичного розвитку.

Збалансованість будь-якої системи – це її стан, при якому забезпечується оптимальне співвідношення її компонентів, яке дозволяє їй знаходитися у рівновазі та бути стійкою у випадку впливу зовнішніх факторів. Відповідно збалансованість розвитку країни показує рівномірний або зважений розвиток її компонентів, що забезпечує його стійкість протягом тривалого часу. Для його моделювання найбільш оптимальними є моделі, які базуються на визначені центру мас. Тобто в залежності від кількості компонент, які приймають учать у вимірі збалансованості розвитку, будується геометрична фігура, вершинами якої виступають композитні їх значення, які в свою чергу формуються під впливом різних детермінант. В даному дослідженні було обрано чотири основні сфери – економічна, політична, соціальна та сфера цифрової спроможності і кібербезпеки, які представляють собою найбільш впливові на розвиток будь-якої країни компоненти або таргети. При цьому їх формування здійснюється на основі обраних детермінант, що найбільше характеризують їх розвиток. Відповідно модель, що будується у даному дослідженні, є барицентричною.

Популяризацією підходу визначення центру мас для економічних наук займалися автори праці [105]. Вони розробили модель трикутника для визначення стійкості ринку страхування та перестрахування, де зробили акцент на розрахунку та аналізі радіусу описаного кола. Методологію побудови барицентричної моделі для аналізу ділової активності компаній запропонували автори [106], де не передбачалася графічна інтерпретація моделі та були відсутні практичні розрахунки. Її розвиток було продовжено Яровенко Г.М. [54] для визначення рівня збалансованості розвитку національної економіки.

Методика базується на визначенні та проведенні аналізу трьох компонентів барицентричної моделі: значень композитних вимірів, збалансованості пар таргетів та збалансованості всіх чотирьох таргетів.

Для визначення значень композитних таргетів необхідно провести нормалізацію значень тих детермінант, які здійснюють вплив. Ця процедура необхідна, оскільки обрані фактори мають різну природу та відрізняються значеннями їх абсолютних величин. Проведення нормалізації дозволить звести значення всіх факторів в діапазоні від 0 до 1. Відповідно це спростить процес згортки даних для визначення композитного значення економічного, соціального, політичного вимірів та виміру цифрової спроможності та кібербезпеки, яке також буде знаходитися в діапазоні від 0 до 1. Якщо значення композитного таргету буде наближатися до 1, то це свідчитиме про потужний розвиток відповідної сфери життєдіяльності країни. В протилежному випадку, якщо воно буде ближчим до 0, то це показник гальмування розвитку.

Існують різні види нормалізації даних, але в даній роботі буде використано лінійну нормалізацію для показників-стимуляторів (3.1) та нормалізацію Севіджа для дестимуляторів (3.2), оскільки дані дослідження є просторовими:

$$\widetilde{x_{ik}} = \frac{x_{ik} - x_{min_i}}{x_{max_i} - x_{min_i}}, \tag{3.1}$$

$$\widetilde{x_{ik}} = \frac{x_{max_i} - x_{ik}}{x_{max_i} - x_{min_i}}. \tag{3.2}$$

де $\widetilde{x_{ik}}$ – нормалізоване значення *i*-го фактору економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для *k*-ої країни;

x_{ik} – вхідне значення *i*-го детермінанту економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для *k*-ої країни;

x_{min_i} та x_{max_i} – відповідно мінімальне та максимальне значення *i*-го детермінанту економічного, соціального, політичного вимірів та виміру

цифрової спроможності і кібербезпеки серед сукупності спостережень, тобто країн.

Розрахунок композитного таргету для економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки відбувається на основі середньогеометричної функції (3.3). Її вибір обумовлений тим, що в результаті отримуємо середнє пропорційне значення таргету для кожної країни:

$$G(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n}) = \left(\prod_{i=1}^{n} \widetilde{x_i} \right)^{1/n}, \tag{3.3}$$

де $G(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n})$ – середньогеометричне значення сукупності нормалізованих значень детермінант економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, визначене для *k*-ої країни;

n – кількість детермінант, які формують відповідний композитний таргет.

При визначенні середньогеометричного значення ті фактори, нормалізоване значення яких дорівнює 0, відбувається значне зміщення значення композитного таргету у бік 0. То для усунення цього фактору для таких значень можна скористатися формулою Мінковського (3.4):

$$R(x_i) = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left| 1 - \frac{x_{ij}}{x_{max_j}} \right|^2 + \sum_{j=k+1}^{n} \omega_j \left| 1 - \frac{x_{min_j}}{x_{ij}} \right|^2}, \tag{3.4}$$

де *R(xi)* – значення композитного таргету економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки;

ω_j – вага кожного детермінанту при формуванні композитного таргету при чому $\sum_{j=1}^{n} \omega_j = 1$. Для їх визначення можна провести канонічний аналіз,

побудувати стандартизоване рівняння регресії, або врахувати їх рівномірний вплив на формування таргету, що було використано в даній роботі.

Для визначення збалансованості пар таргетів та всіх чотирьох таргетів необхідно побудувати чотириполюсну барицентричну модель, що здійснюється як побудова геометричної фігури - чотирикутника та визначення його основних характеристик. Даний процес передбачає відкладення чотирьох точок на координатній площі, координати яких відповідають значенням композитних таргетів. Але щоб розуміти наскільки збалансованим є розвиток країни доцільно поряд із моделлю фактичних даних будувати й еталонну, в якості якої виступає квадрат, координати вершин якого дорівнюють максимальному значенню таргету, тобто 1. Для виміру цифрової спроможності і кібербезпеки це буде точка із координатами (1; 1), для соціального виміру – (1; -1), економічного – (-1; -1), політичного – (-1; 1). Точки з'єднуються прямими, які утворюють боки квадрату. Його центроїд або центр мас знаходиться у точці перетину його діагоналей ("Center of Mass"), яка співпадає із початком координатних вісей і має координатами (0; 0). Еталонна модель представлена на рисунку 3.1. Її було побудовано із використанням програмного забезпечення GeoGebra.

Для емпіричних даних побудувати барицентричну модель у вигляді квадрату досить складно, оскільки за таких умов країна має однаковий рівень розвитку економічної, соціальної, політичної сфери та сфери інформаційної безпеки.

На практиці для різних країн можна отримати різні форми чотирикутників, з різними довжинами боків та різними кутами. Тому також необхідно накреслити коло навколо чотирикутника. Це може бути можливим за умови, якщо сума його протилежних кутів дорівнює 180^{o}. В протилежному випадку даний факт свідчитиме про існування дисбалансу між парами вимірів.

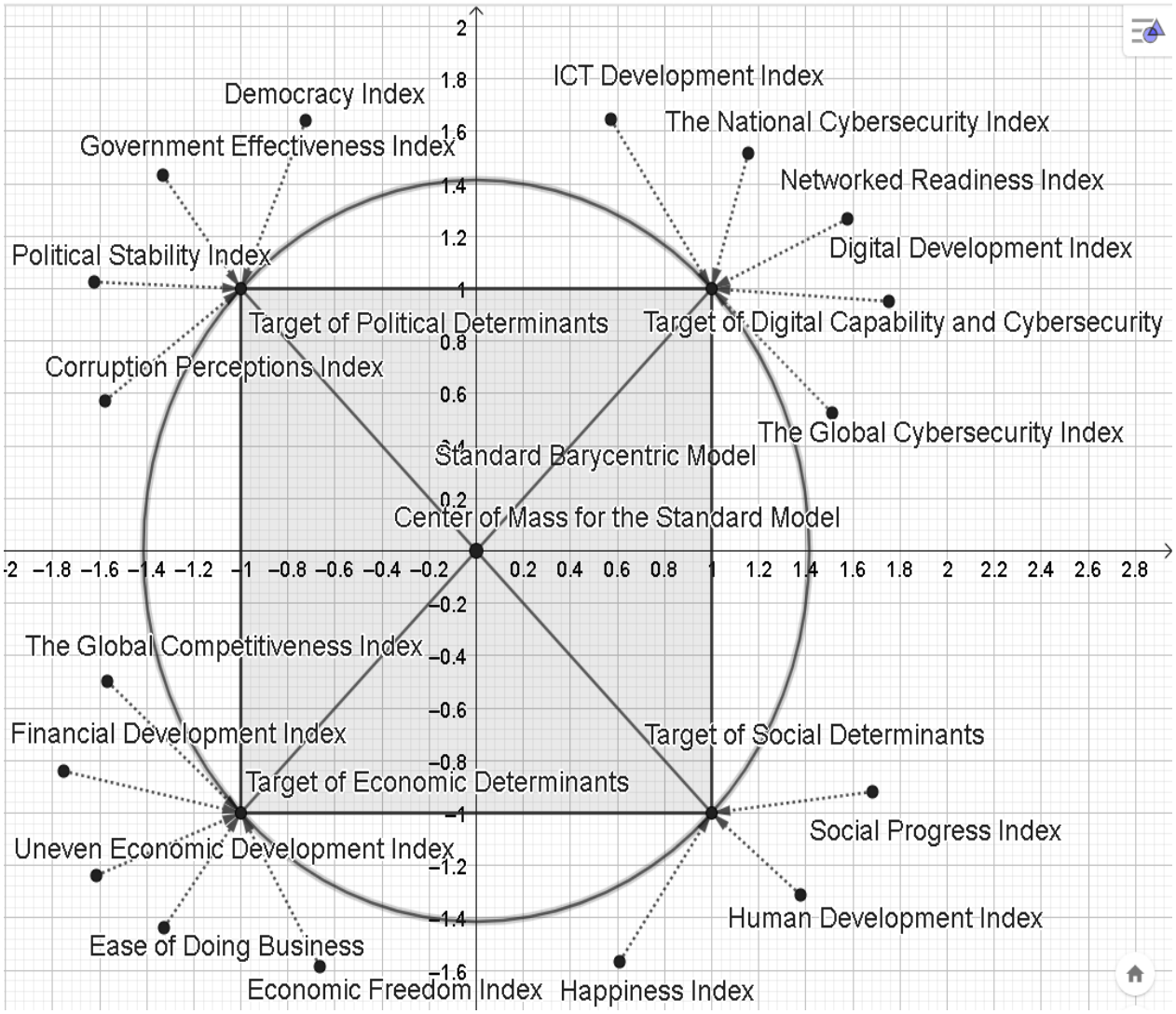

Рисунок 3.1 – Еталонна чотириполюсна барицентрична модель збалансованості розвитку країни

Для визначення градусної міри кутів чотирикутника і перевірки можливості побудувати коло навколо нього необхідно чотирикутник поділити на два трикутники та розрахувати їх довжину сторін як довжину відрізків за формулою (3.5):

$$AB = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}, \tag{3.5}$$

де AB – це довжина відрізку між двома точками A та B, які є вершинами одного з двох трикутників ABC;

$(x_a; y_a)$ – координати точки А, що є значеннями відповідних композитних таргетів;

$(x_b; y_b)$ – координати точки В, що є значеннями відповідних композитних таргетів.

Аналогічно знаходяться інші сторони трикутника АБС та сторони другого трикутника, що разом формують чотирикутник.

Розраховуємо косинуси кожного кута для кожного з двох трикутників за формулою (3.6):

$$\cos\alpha = \frac{b^2 + c^2 - a^2}{2 \cdot b \cdot c}, \tag{3.6}$$

де a, b, c – це значення довжин трьох сторін трикутника.

Отримані значення переводимо у градусну міру із використанням спеціальних таблиць або калькуляторів. У даному дослідженні розрахунки відбувалися із використанням програмного забезпечення MS Excel, де застосовуються відповідні функції.

Сумуємо значення градусної міри двох кутів, які знаходяться біля основи одного трикутника, із значеннями градусної міри кутів іншого, щоб отримати значення двох протилежних кутів чотирикутника. Спочатку проводимо перевірку, чи дорівнює сума чотирьох кутів 360 градусів, а потім перевіряємо умову збалансованості двох пар вимірів шляхом визначення суми пар протилежних кутів чотирикутника. У випадку, якщо їх суми дорівнюють 180 градусів, робимо висновок, що навколо даного чотирикутника можна описати коло, тобто пари вимірів є збалансованими.

Для визначення третьої компоненти барицентричної моделі (збалансованості чотирьох таргетів) необхідно визначити центр мас чотирикутника, що передбачає розрахунок значень його координат за формулами (3.7)-(3.8):

$$O_x = \frac{1}{6A}\sum_{i=0}^{n-1}((x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i)), \quad (3.7)$$

$$O_y = \frac{1}{6A}\sum_{i=0}^{n-1}((y_i + y_{i+1})(x_i y_{i+1} - x_{i+1} y_i)), \quad (3.8)$$

де *Ox* та *Oy* – координати точки О, яка є центром мас чотирикутника;

(x_i; y_i), (x_{i+1}; y_{i+1}) – координати вершин чотирикутника, де вершина з координатами (x_n; y_n) буде співпадати з вершиною з координатами (x_0; y_0);

A – площа чотирикутника, яка визначається за формулою (3.9):

$$\mathrm{A} = \frac{1}{2}\sum_{i=0}^{n-1}(x_i y_{i+1} - x_{i+1} y_i). \quad (3.9)$$

Визначення рівня збалансованості чотирьох таргетів здійснюється шляхом отримання різниці між центром мас, який відповідає даним певної країни, та центром мас еталонної моделі. Для цього розраховуємо дану відстань як довжину відрізку за формулою (3.5). Чим ближче отримане значення до 0, тим ближче центр мас барицентричної моделі країни до еталонного значення, що говорить про збалансований розвиток країни на основі її чотирьох композитних таргетів.

Для проведення дослідження та розрахунків було узято дані обраних детермінант для 127 країн світу за 2018 рік з джерел таких організацій, як Світовий банк, Міжнародний валютний фонд, Всесвітній економічний форум, незалежний шведський фонд «Gapminder», глобальна некомерційна організація «Імператив соціального прогресу». Даний період було обрано тому, що більшість детермінант не мають фактичних значень після нього, особливо індикатори виміру цифрової спроможності і кібербезпеки.

Для аналізу отриманих результатів проведемо групування країн за рівнем їх економічного розвитку відповідно до класифікації Міжнародного валютного фонду, згідно із якою вони поділяються на розвинені, ті, що розвиваються, та найменш розвинені. Також виділимо серед них групу країн, які вважаються новими індустріальними завдяки їх високих темпів технологічного розвитку, який виступає драйвером розвитку їх економіки. Сюди відносяться Аргентина, Бразилія, Мексика, Індія, Малайзія, Тайланд, Чилі, Індонезія, Туреччина, Китай, Іран, Філіппіни [107], та перспективні індустріальні країни з Групи одинадцяти (Нігерія, Єгипет, Пакистан, Бангладеш, В'єтнам) [108].

На рисунку 3.2 представлено результати значень розрахованих композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для двадцяти розвинених країн або країн із високим рівнем економіки, перелік яких було означено у відповідністю із Міжнародним валютним фондом [109, с. 132]. Перші десять країн мають найвище сумарне значення таргетів, друга десятка – найнижче з групи розвинених країн.

Порівняння значень композитних таргетів із еталонним рівнем (рисунок 3.2) показує, що для більшості розвинених країн їх значення прямують до 1, але не досягають його. На практиці цього досягти не можливо для будь-якої країни, тому чим ближче розраховані значення прямують до нього, тим вищий рівень розвитку даного виміру країни.

Слід відмітити, що найкращий результат демонструє Швейцарія, яка має найвище сумарне значення таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (3,735).

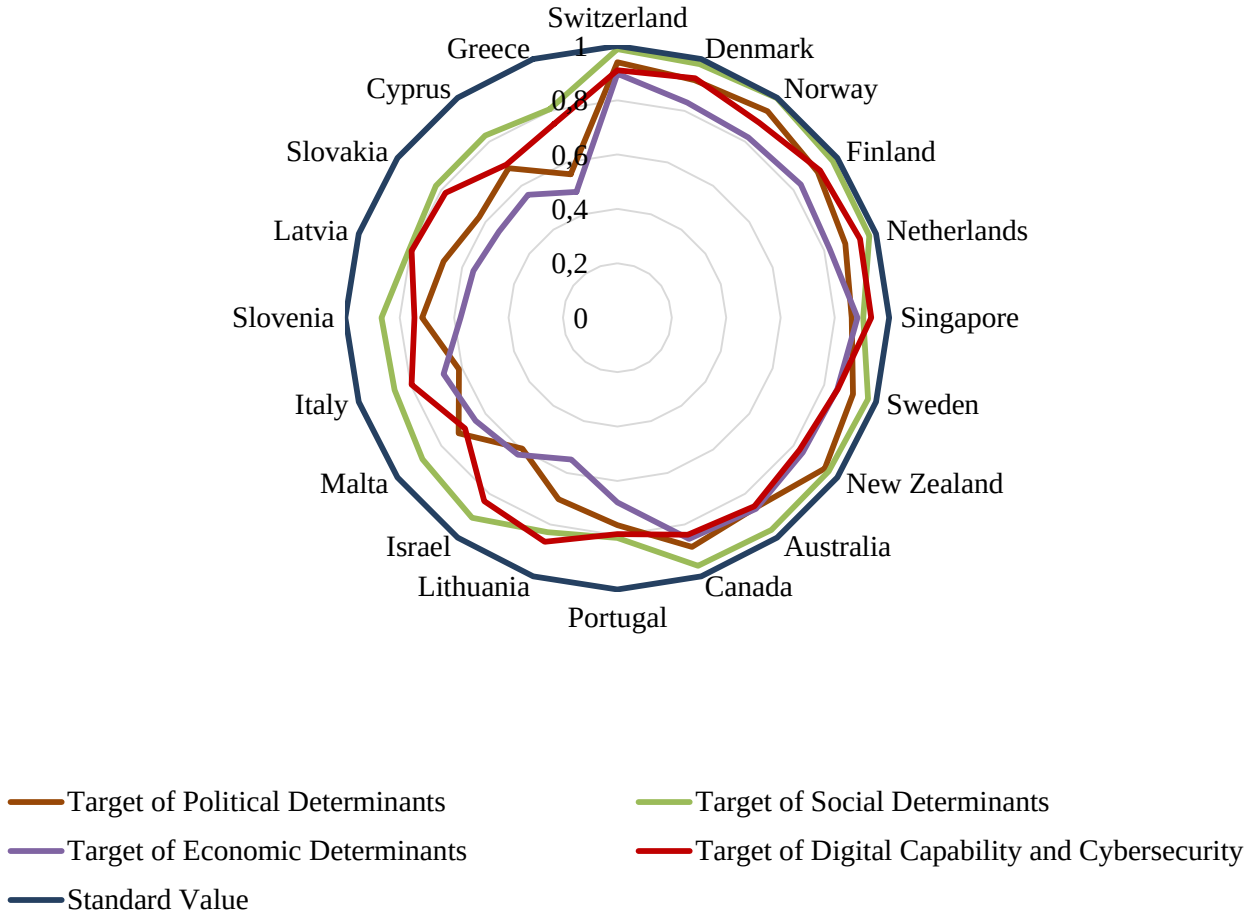

Рисунок 3.2 – Значення композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для розвинутих країн

Такі країни, як Данія, Фінляндія, Норвегія, Нідерланди, Сінгапур, Швеція, Нова Зеландія, Австралія, Канада, входять у топ-десять країн із найвищими значеннями композитних таргетів, що свідчить про досить високий рівень розвитку кожного з них. Найнижчі значення серед аналізованої групи розвинених країн демонструють Португалія, Литва, Ізраїль, Мальта, Італія, Словенія, Латвія, Словакія, Кіпр та Греція. Найвищий рівень розвитку демонструє соціальний вимір, що говорить про ефективну соціальну політику уряду цих країн по відношенню до їх населення. Політичний вимір та вимір цифрового розвитку і кібербезпеки для переважної кількості країн переважають

над значеннями економічного таргету. Це свідчить про те, що економічний потенціал цих країн надав поштовх для прискорення розвитку інших таргетів, що в подальшому сприятиме більш потужному економічному розвитку цих країн.

На рисунку 3.3 представлені результати розрахованих значень композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для країн, що розвиваються згідно із переліком Міжнародного валютного фонду. Було винесено десять країн із найвищими значеннями та десять – з найнижчими.

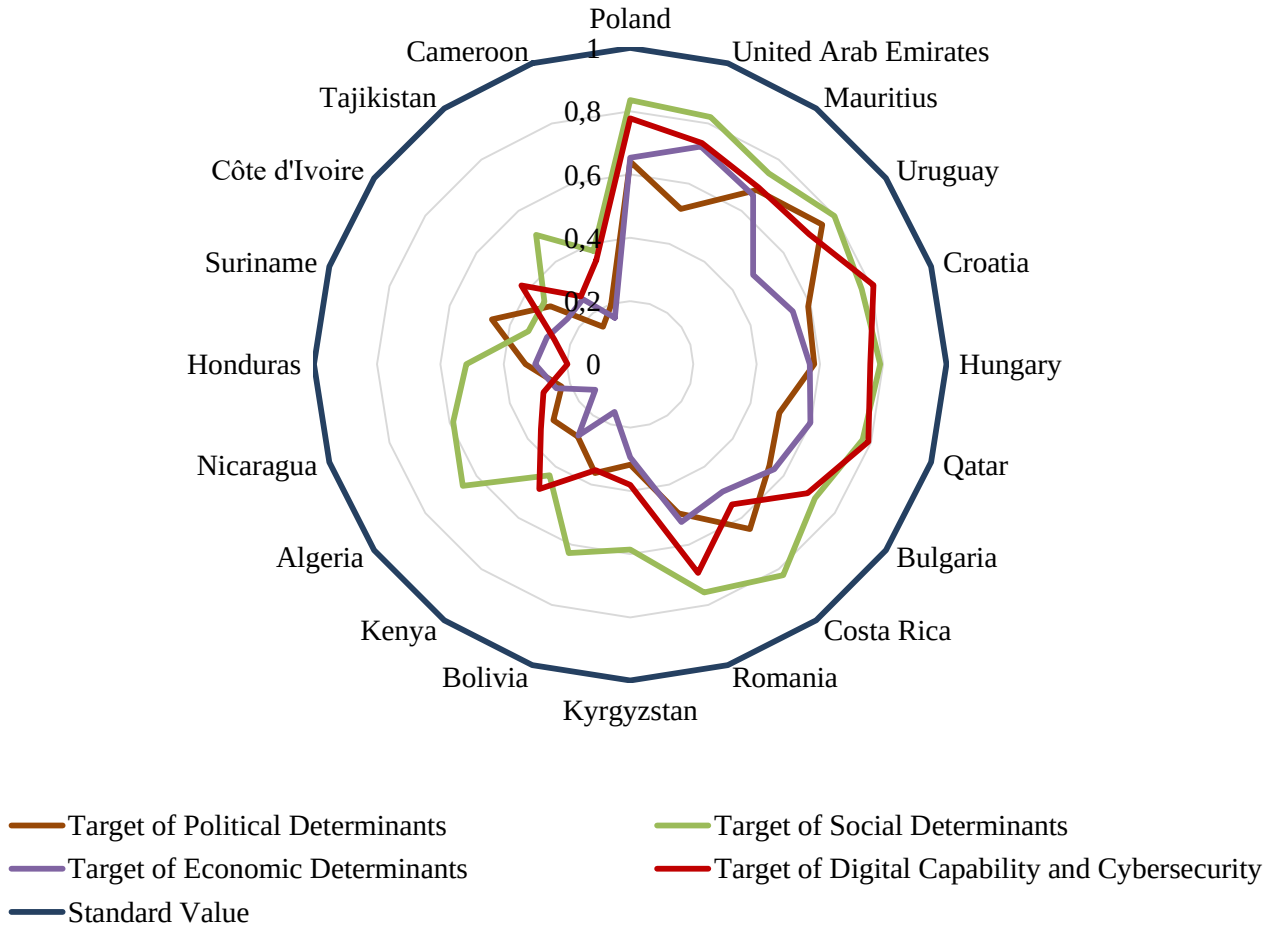

Рисунок 3.3 – Значення композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для країн, що розвиваються

Провідними в даній групі країн є Польща, Арабські Емірати, Маврикій, Уругвай, Хорватія, Угорщина, Катар, Болгарія, Коста Ріка та Румунія. Найменш розвиненими є таргети таких країн, як Киргизстан, Болівія, Кенія, Алжир, Нікарагуа, Гондурас, Сурінам, Кот-Д'Івуар, Таджикистан та Камерун. У порівнянні із даними, отриманими для розвинених країн, спостерігається значний дисбаланс, що виникає між соціальним виміром і виміром кібербезпеки та економіко-політичним. При чому різниці є досить суттєвими.

Наприклад, для Польщі таргет соціального виміру дорівнює 0,8357, цифрової спроможності і кібербезпеки – 0,7773, економічний – 0,6533, політичний – 0,6410, а для Алжиру – відповідно 0,6542, 0,3486, 0,1365, 0,3002. Тобто, розвиток економічної та політичної сфери є досить критичним для країн, що розвиваються. Це обумовлене або нестійкою політичною ситуацією, що склалася в них (наприклад, Україна, Гондурас, Гватемала), або неефективністю дій уряду та прийнятих ним політичних законів та рішень.

В свою, чергу нестабільність економічного розвитку таких країн є прямим наслідком кризи їх політичної сфери, що призводить до гальмування їх розвитку в цілому. Тобто для країн, що розвиваються, є важливим, в першу чергу, посилення політичного виміру шляхом трансформації законодавства, боротьби з корупційною складовою, прийняття урядом більш ефективних рішень, спрямованих на розвиток економіки та проведення реформ, тощо.

Результати розрахованих значень композитних таргетів для нових індустріальних країн представлені на рисунку 3.4.

У розвитку нових індустріальних країн також присутній дисбаланс (рисунок 3.4), при цьому явно спостерігається однаковий напрям розвитку у соціальному вимірі та вимірі цифрової спроможності і кібербезпеки, а також економіко-політичному.

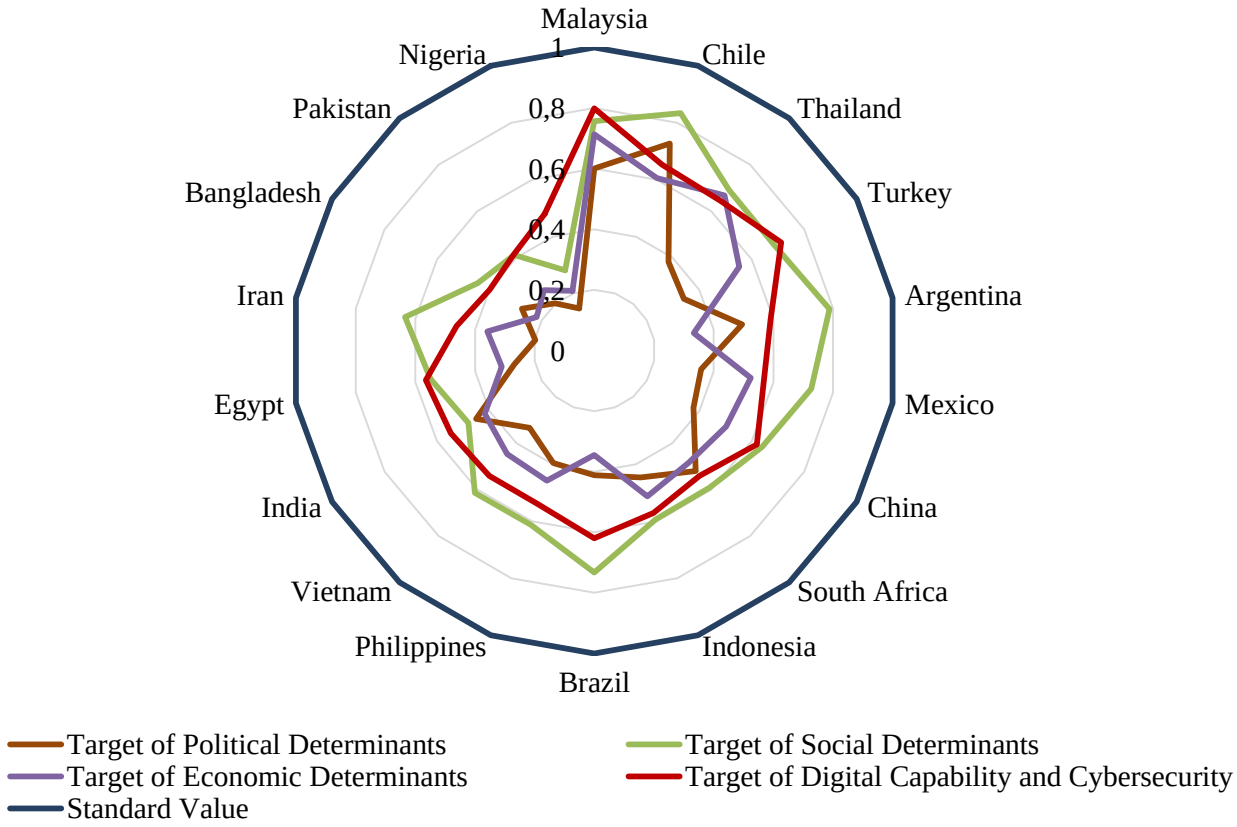

Рисунок 3.4 – Значення композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для нових індустріальних країн

Хоча на відмінність від значень композитних таргетів, представлених на рисунку 3.3, для більшості даних країн, окрім Чилі, Аргентини та Бразилії, характерний більш рівномірний розвиток обраних сфер, який не містить аномальних перепадів. Найвищі значення таргетів мають Малайзія, Чилі, Тайланд, Туреччина та Аргентина, найгірший результат характерний для Ірану, Бангладеш, Пакистану та Нігерії. Оскільки представлені країни вважаються такими, що вже пройшли певні етапи соціо-економічного розвитку та досягли успіхів, або мають всі шанси на індустріальний стрибок, то можна сказати, що для більшості із них, а саме Туреччині, Тайланду, Аргентині, Нігерії, Пакистану, Чилі, Бразилії, Бангладеш, Мексиці та Ірану, слід звернути увагу на політичний та економічний виміри для забезпечення розвитку соціальної сфери та сфери цифрової спроможності.

На рисунку 3.5 представлені побудовані композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для найменш розвинутих країн, перелік яких визначено Організацією Об’єднаних Націй (далі ООН) [110, с. 1]. Було виділено 10 країн із найвищими та найменшими значеннями показників серед своєї групи країн.

Практично усі країни, окрім Ботсвани та Бутану, мають дуже низькі значення чотирьох таргетів (рисунок 3.5). При цьому можна побачити нерівномірний розвиток усіх вимірів, особливо економічного. Отримані результати свідчать про існування реальних проблем економічного, соціального, політичного характеру та недостатній рівень розвитку інформаційних технологій, що потребує допомоги з боку всесвітніх та міжнародних організацій.

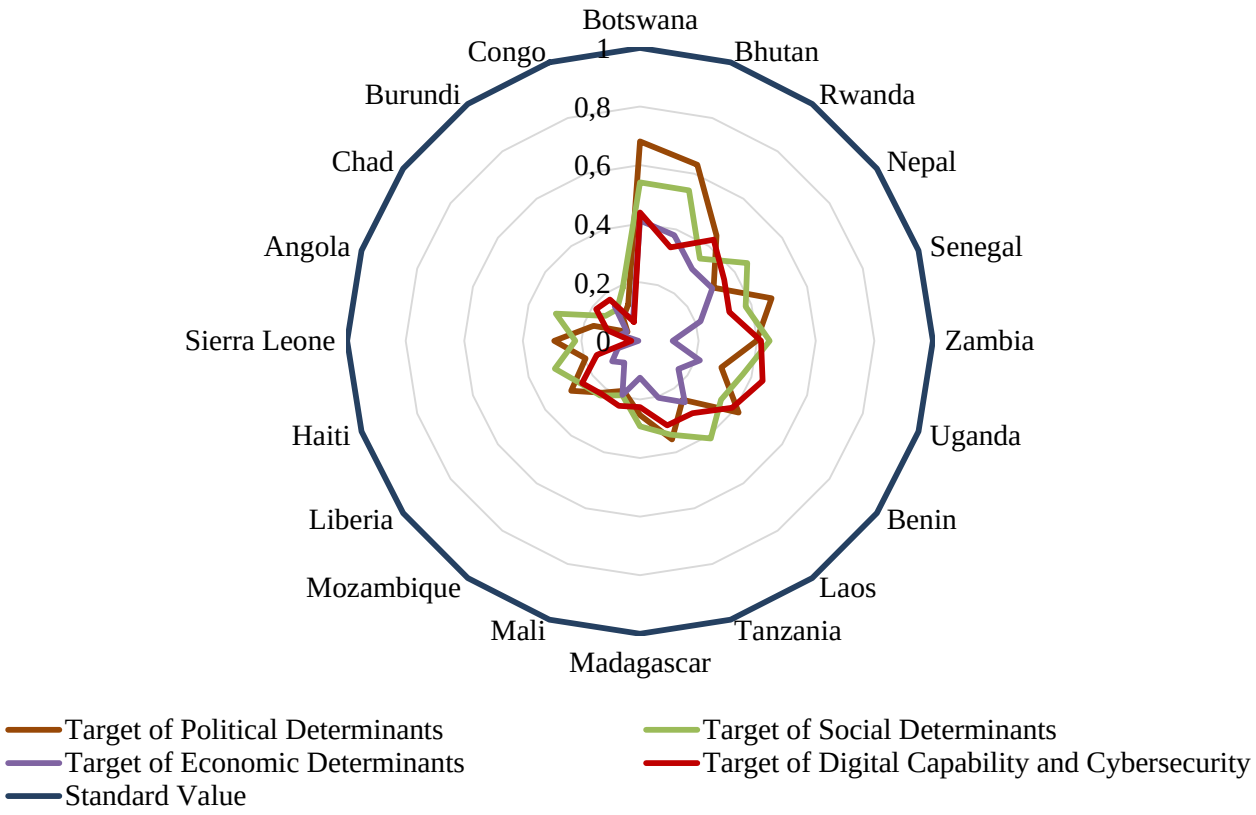

Рисунок 3.5 – Значення композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для найменш розвинених країн

Для проведення аналізу збалансованості пар таргетів було визначено градусну міру кутів чотирикутників для 127 країн світу та сформовано їх пари, які було обрано, виходячи із наступних міркувань. Найбільший поштовх сьогодні в економіці забезпечується за рахунок розвитку саме інформаційних технологій, що призводить до поступової її трансформації у цифрову. З іншого боку, саме економічний розвиток країни стимулює науково-технічний прогрес, наслідком якого є розвиток IT-сфери в країні. Також дані міркування були підкріплені шляхом розрахунку лінійного коефіцієнту кореляції між значеннями чотирьох композитних таргетів. Виявилося, що між інтегральними значеннями економічного виміру та виміру цифрової спроможності і кібербезпеки існує найтісніший кореляційний зв'язок (0.9144), між парою соціального та політичного вимірів цей зв'язок є також тісним (0.8343). Візуалізуємо дані отриманих розрахунків, які у відсотках показують співвідношення сум протилежних кутів чотирикутника, що дозволяє зробити висновок про збалансованість або незбалансованість розвитку пар вимірів – соціо-політичного та економіко-цифрового (для скорочення назви виміру цифрової спроможності та кібербезпеки застосовуємо «інформаційний»). Тобто, якщо значення буде прямувати до 50% (для пари соціального та політичного вимірів) та 100% (для пари економічного виміру та виміру цифрової спроможності і кібербезпеки), то це говорить, що сума пари кутів є рівною 180 градусів, в протилежному випадку, вона буде або більшою, або меншою ніж 180. Так, на рисунку 3.6 представлені результати розрахунків для розвинених країн.

Аналізуючи дані рисунку 6, можна зробити висновок про те, що такі країни як Італія, Японія, Франція та Ізраїль мають найбільш збалансовані пари таргетів, оскільки значення сум пар протилежних кутів прямують до 180 градусів. Тобто при побудові їх барицентричної моделі можна накреслити коло навколо їх чотирикутника. Для Іспанії, Сінгапуру, Естонії, Великобританії, Німеччини та США сума кутів має незначне відхилення від 180 градусів, але для інших країн розбіжність зростає.

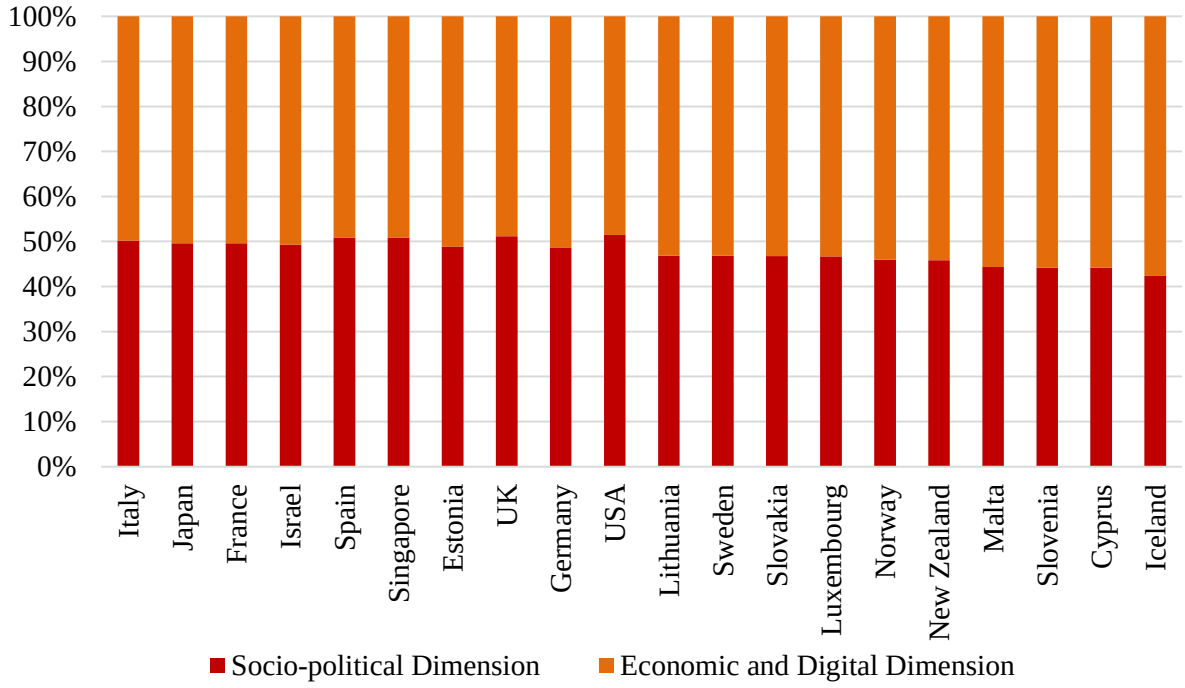

Рисунок 3.6 – Збалансованість пар композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для розвинених країн

При цьому можна побачити, що значення для соціально-політичного виміру є меншим для переважної кількості країн, що свідчить про більшу значущість цієї пари для збалансованого розвитку економічно розвинених країн, а також їх стрімкий розвиток в порівнянні з парою економічного виміру та виміру цифрової спроможності.

Результати розрахунків сум протилежних кутів для побудови барицентричної моделі країн, що розвиваються, представлені на рисунку 3.7, де можна побачити, що Ко-д'Івуар, Болгарія, Оман та Румунія мають значення, близькі до 180 градусів. Для інших країн розбіжність зростає, що свідчить про не можливість описати коло навколо чотирикутника моделі. Отримані результати показують, що для частини країн є превалюючою парою соціально-політичний вимір, а для таких, як Молдова, Грузія, Кенія, Вірменія, Катар, Арабські Емірати, Україна, Бахрейн, Казахстан, Саудівська Арабія, Азербайджан та Російська Федерація (частина з них не представлена на рисунку 3.7), превалює вимір

економічного розвитку та цифрової спроможності і кібербезпеки. Аналіз цієї пари вимірів для цих країн показав, що найбільш потужний розвиток вони мають в сфері ІТ, а економічний розвиток значно відстає. Тому у випадку цих країн економічний прорив можливий за рахунок потужного потенціалу ІТ сфери.

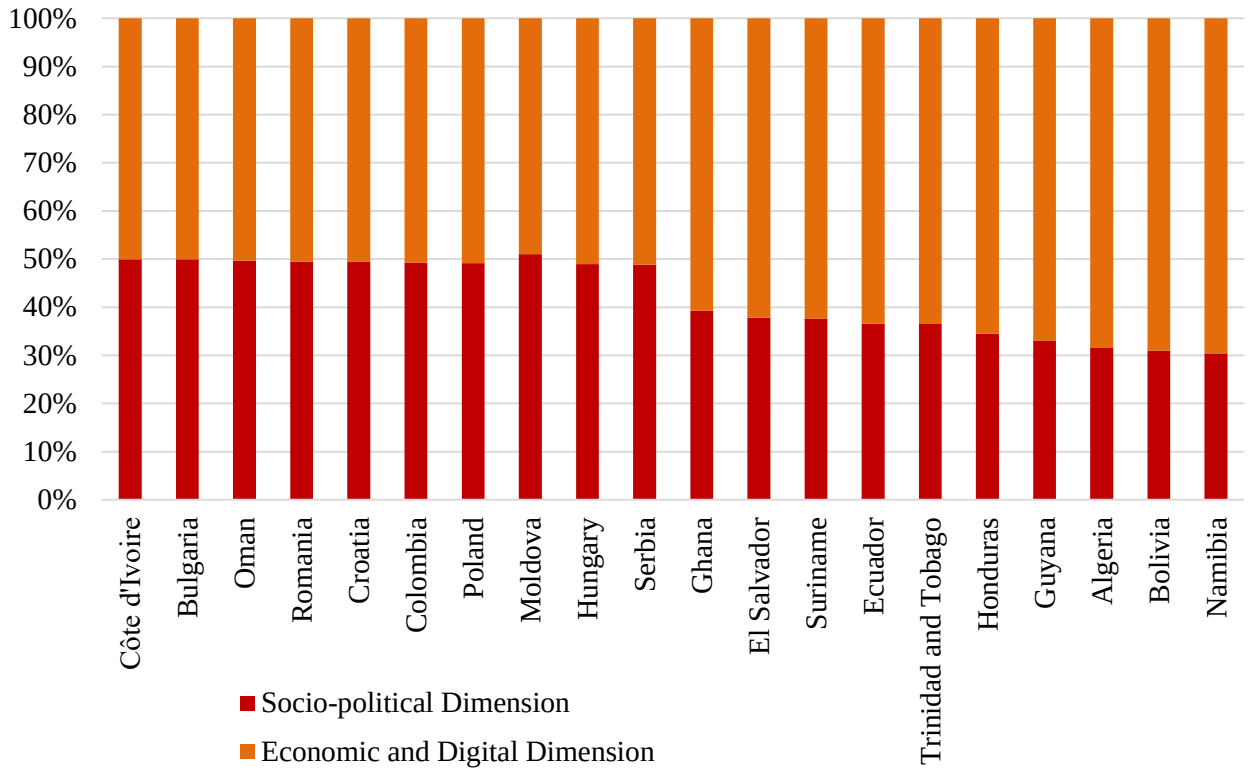

Рисунок 3.7 – Збалансованість пар композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для країн, що розвиваються

Розраховані значення сум протилежних кутів для нових індустріальних країн представлено на рисунку 3.8, де можна побачити, що тільки модель Філіппін та Індії мають значення сум протилежних кутів чотирикутника, які приблизно дорівнюють 180 градусів. Інші країни мають незбалансовані пари вимірів, причому для одних є характерним превалювання збалансованості економіко-цифрового виміру (Індія, Індонезія, Мексика, Єгипет, В'єтнам, Малайзія, Пакистан, Іран, Китай, Тайланд, Туреччина, Нігерія), для інших – соціально-політичного (Південна Африка, Аргентина, Бангладеш, Бразилія, Чилі). Аналіз окремих індикаторів показав, що такі країни, наприклад, як Китай,

Індія, Єгипет та інші, мають потужний розвиток ІТ-галузі та кібербезпеки. Такі країни, як Мексика та Малайзія мають розвиток економічної та сери ІТ приблизно на одному рівні. Для Бразилії, Чилі та Аргентини дестабілізуючим таргетом є політичний, що є наслідком політичної нестабільності цих країн. Тобто, група нових індустріальних країн має різні напрямки розвитку країн, що потрібно враховувати їх урядом для розробки стратегії розвитку.

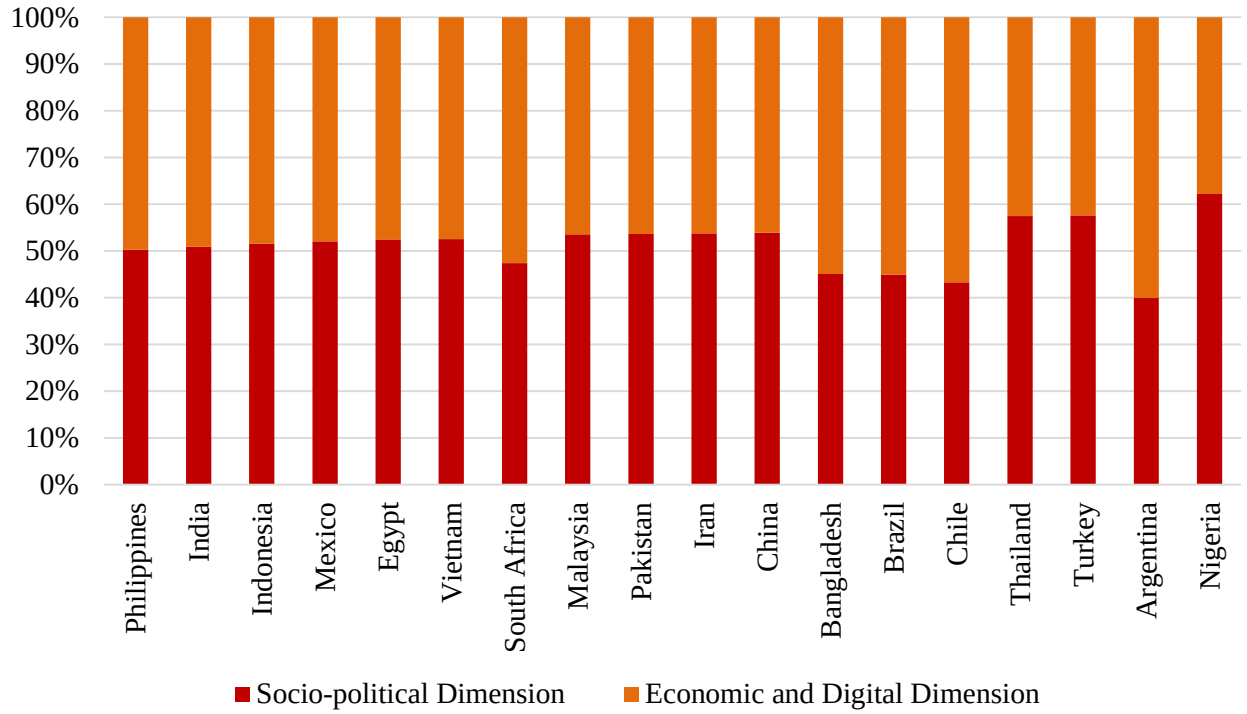

Рисунок 3.8 – Збалансованість пар композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для нових індустріальних країн

Значення сум протилежних кутів для найменш розвинених країн представлено на рисунку 3.9. Тільки для Камбоджі значення сум протилежних кутів чотирикутника дорівнюють 180 градусів, а для Ефіопії ці значення є близькими. Інші країни мають ярко виражену незбалансованість пар вимірів, причому для переважної більшості із них є характерним превалювання соціально-політичного виміру та незбалансованість економіко-цифрового. Для Чаду, Малі та Бурунді ситуація є зворотною. Незважаючи на те, що значення їх таргетів є низькими, можна спостерігати, що деякі країни мають урівноважений

розвиток таргетів для пар вимірів. Наприклад, Бутан (0.5400 – соціальний таргет, 0.6322 – політичний, 0.3800 – економічний, 0.3356 – цифрова спроможність і кібербезпека), який має соціально-політичний та економіко- цифровий розвиток на приблизно однаковому рівні, але між даними парами є суттєва різниця, що свідчить про недостатній потенціал економіко-цифрової сфери. Інші країни цієї групи можуть мати інші сценарії розвитку, де домінуватиме тільки один з таргетів, що пов’язано з їх історичними, культурними, політичними та іншими особливостями існування та розвитку.

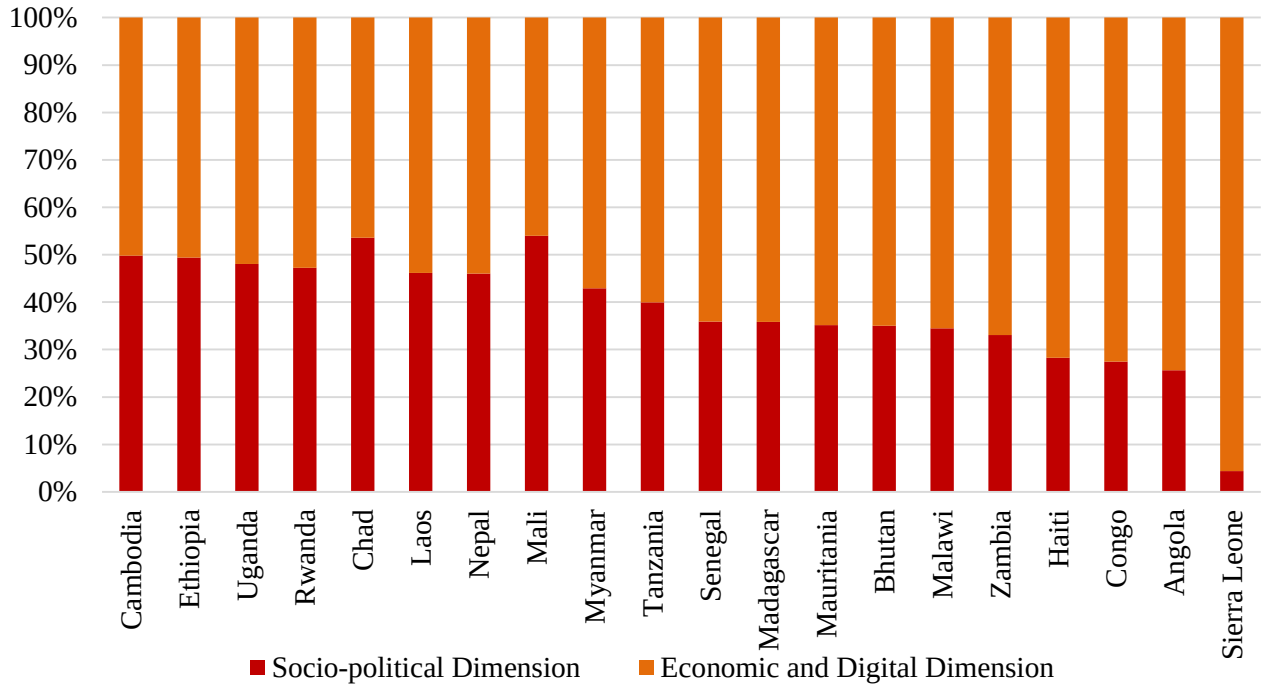

Рисунок 3.9 – Збалансованість пар композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для топ-двадцяти найменш розвинених країн

Розраховані значення відстаней між центрами мас для всіх країн, які представляють собою відхилення фактичних значень їх центрів мас від еталонного, представлені на рисунку 3.10.

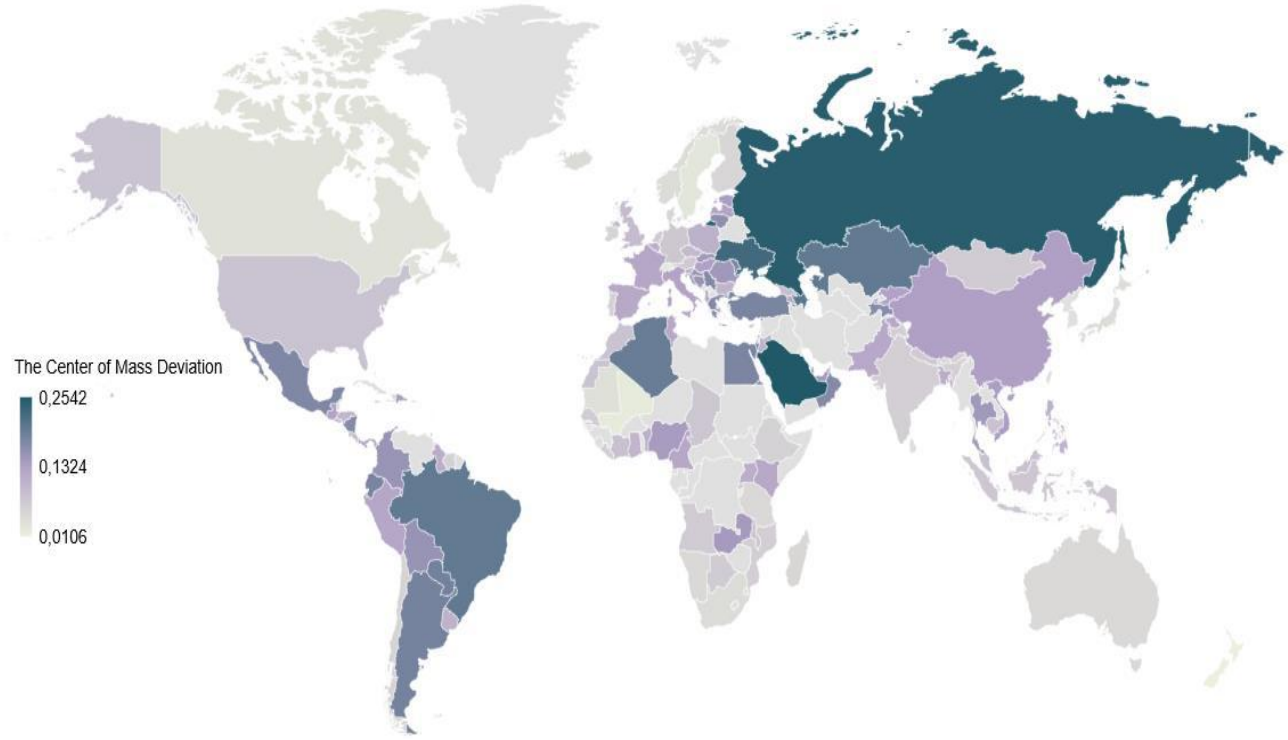

Рисунок 3.10 – Рівень збалансованості розвитку країн на основі відхилення центрів мас їх барицентричних моделей

Так, найбільш збалансованими є Нова Зеландія (0.0106), Малі (0.0196), Бурунді (0.0214), Швейцарія (0.0236), Швеція (0.0272), Сінгапур (0.0312), Маврикій (0.0340), Канада (0.0350), Мавританія (0.0357). Тобто, найбільш збалансованим є країни, як розвинуті, так й ті, що розвиваються, та найменш розвинені. Даний фактор свідчить про те, що не залежно від значень таргетів, рівня збалансованості їх пар, будь-яка країна не залежно від рівня її економічного розвитку може мати ефективне поєднання чотирьох таргетів. Наприклад, Малі має низькі значення таргетів, але їх комбінація є збалансованою, що в подальшому може виступати драйвером для їх більш стрімкому та динамічному розвитку. Найменш збалансованими виявилися Парагвай (0,1860), Алжир (0,1946), Бразилія (0,1990), Казахстан (0.1998), Азербайджан (0,2063), Бахрейн (0,2093), Іран (0,2113), Україна (0,2269), Російська Федерація (0,2467), Саудівська Аравія (0,2542). Цей результат говорить про те, що дані країни мають дисбаланс за рахунок превалювання

переважно одного (наприклад, як в Україні таргет цифрової спроможності і кібербезпеки) або двох таргетів над іншими, що свідчить про несистемність їх розвитку та необхідність трансформації їх стратегій з урахуванням отриманих даних.

Побудуємо чотириполюсні барицентричні моделі збалансованості розвитку країн з кожної чотирьох груп, які мають найменшу відстань розрахованого центру їх мас від еталонного значення. Для розвинених країн таким представником є Нова Зеландія (0.0106), для країн, що розвиваються – Маврикій (0.0340), нових індустріальних – Південна Африканська Республіка (0.0428), для найменш розвинених – Малі (0.0196). На рисунку 3.11 представлена барицентрична модель Нової Зеландії.

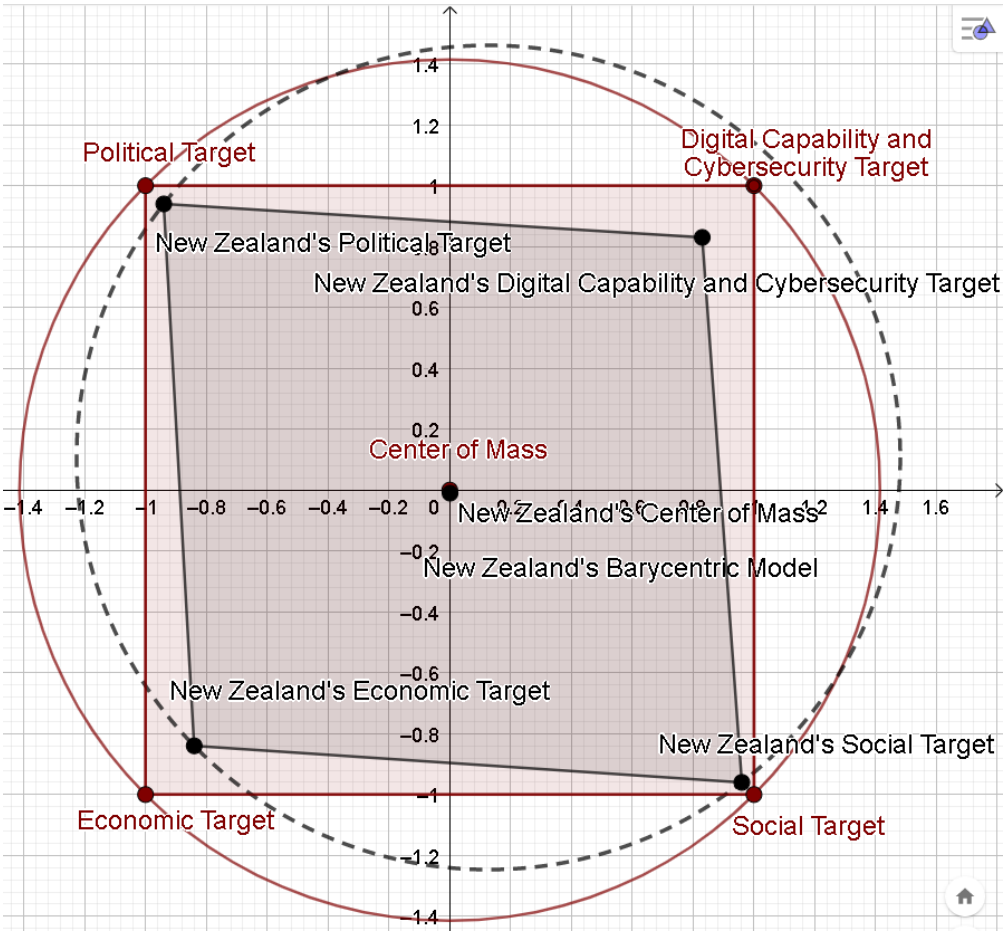

Рисунок 3.11 – Чотириполюсна барицентрична модель збалансованості розвитку Нової Зеландії

Барицентрична модель (рисунок 3.11) показує розвиток Нової Зеландії з урахуванням збалансованості чотирьох композитних таргетів – економічного, соціального, політичного та цифрової спроможності і кібербезпеки. Їх значення є досить високими та наближаються до 1, що свідчить про високий рівень розвитку економіки, соціальних стандартів, політичної стабільності, а також значний потенціал ІТ сфери та кібербезпеки. На рисунку 3.11 відмічено центр мас чотирикутника, координати якого практично дорівнюють координатам еталонного центру мас, що свідчить про повну збалансованість чотирьох таргетів. Але коло описати навколо даного чотирикутника не можливо, оскільки суми пар протилежних кутів не дорівнюють 180 градусів. Це відбувається за рахунок того, що вимір цифрової спроможності і кібербезпеки, а також економічний вимір мають значення значно нижче ніж соціальний та політичний. За даною моделлю можна зробити наступний висновок: розвиток країни є стійким, оскільки відстань між центрами мас є незначною. Співвідношення між парами вимірів (економіко-цифровим та соціо-політичним) є незбалансованим, але розвиток однієї сфери можна компенсувати за рахунок іншої. Значення композитних таргетів економічного та цифрового вимірів є слабкішими, тому країні треба змістити акцент у даний напрямок розвитку, особливо в частині цифровізації та автоматизації різних сфер діяльності економічних агентів. При цьому драйвером розвитку можуть виступати політичний та соціальний виміри.

Чотириполюсна барицентрична модель збалансованості розвитку Маврикія представлена на рисунку 3.12.

Отримана модель дозволяє зробити наступні висновки: розвиток країни є досить стійким, оскільки відстань між центрами мас дорівнює 0,0340, що практично наближає його до мінімального значення серед відстаней. Співвідношення між парами вимірів (економіко-цифровим та соціо-політичним) не є збалансованим, оскільки суми протилежних кутів не дорівнюють 180 градусів, причому дисбаланс є найбільшим для економіко-цифрового вимірів. Найменш ефективним в цій пар є таргет цифрової спроможності і кібербезпеки,

що свідчить про відставання рівня розвитку інформаційних технологій та заходів кібербезпеки від інших.

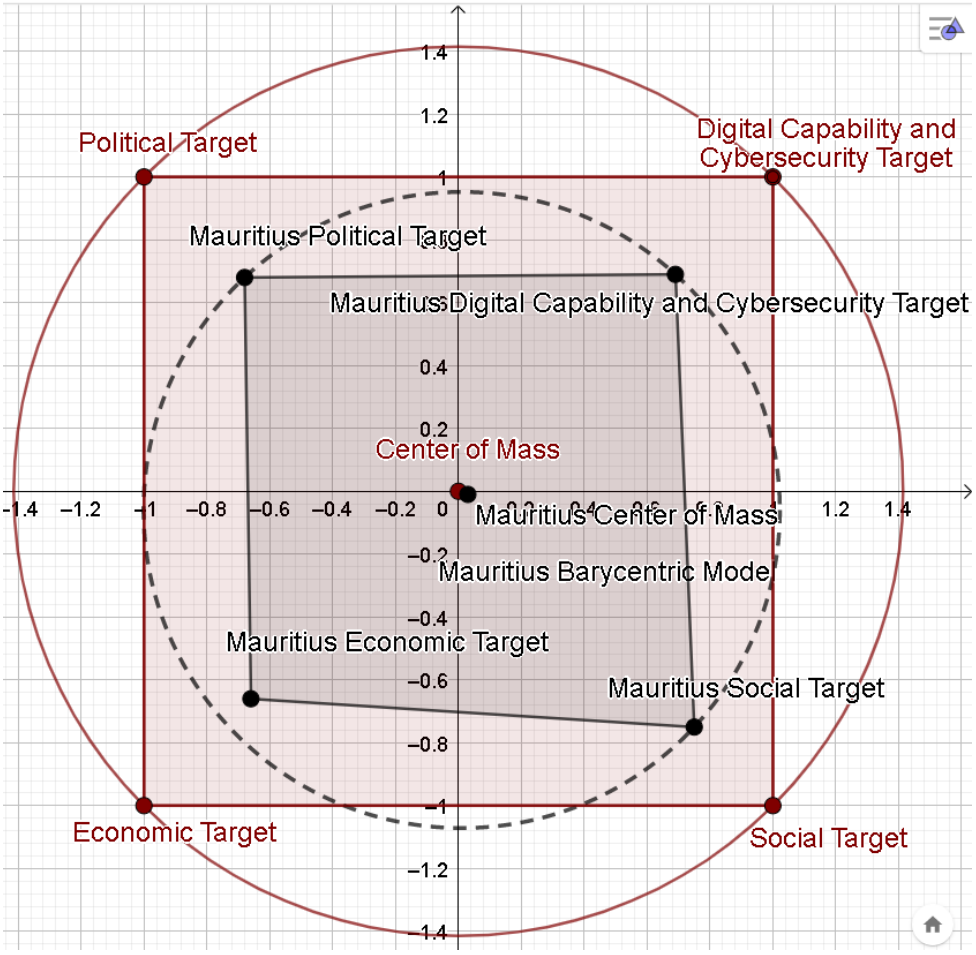

Рисунок 3.12 – Чотириполюсна барицентрична модель збалансованості розвитку Маврикія

Це пояснюється тим, що Маврикій є острівною державою, економіка якого орієнтується на розвиток туристичної галузі. Для даного таргету є важливим підвищення рівня національної кібербезпеки, оскільки в порівнянні з іншими даними його значення є низьким, що свідчить про можливі проблеми в системі державного кіберзахисту. Значення таргетів є вище середнього, серед яких найбільш ефективним є таргет соціального розвитку, що може бути відповідним драйвером для розвитку економіки та її цифровізації.

Побудуємо чотириполюсну барицентричну модель збалансованості розвитку однієї із нових індустріальних країн, а саме Південно Африканської Республіки, результат якої представлений на рисунку 3.13.

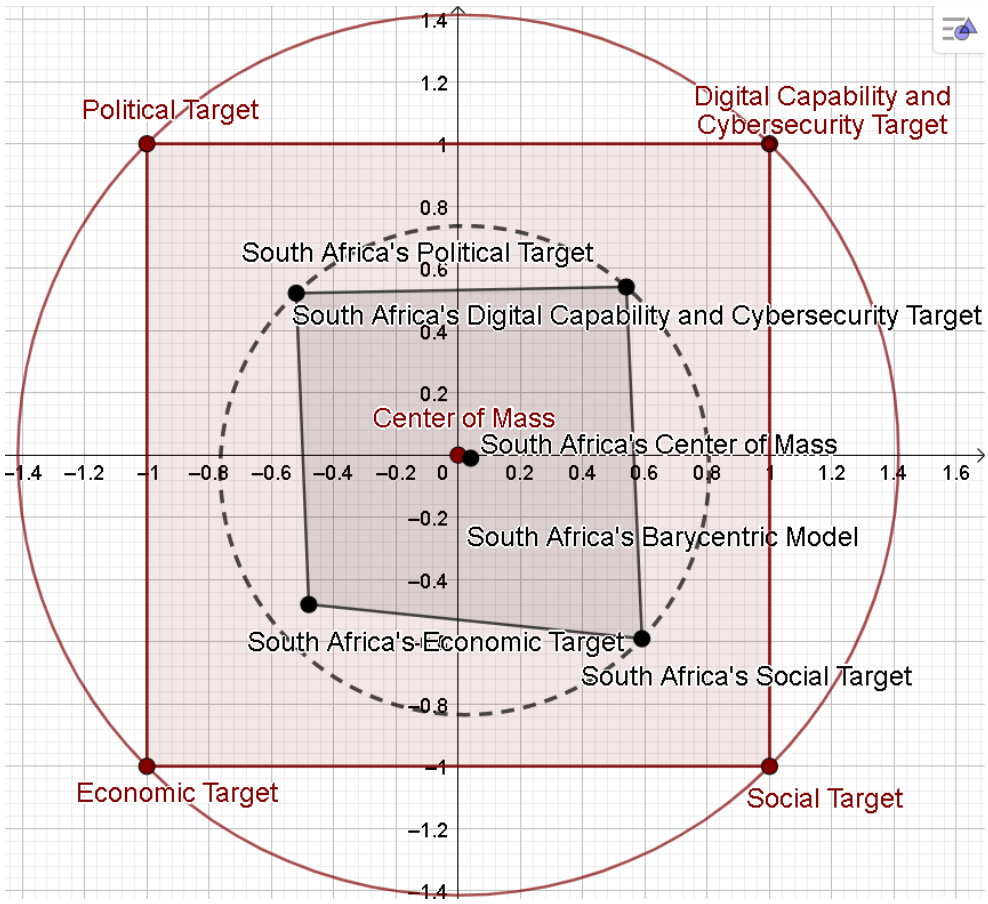

Рисунок 3.13 – Чотириполюсна барицентрична модель збалансованості розвитку Південно Африканської Республіки

За результатами моделі (рисунок 3.13) можна зробити наступні висновки: розвиток країни є стійким, оскільки відстань між центрами мас наближається до 0 і дорівнює 0,0428. Співвідношення між парами вимірів (економіко-цифровим та соціально-політичним) – незбалансоване, оскільки суми протилежних кутів не дорівнюють 180 градусів, причому дисбаланс є найбільшим для економіко-цифрового вимірів, ніж для соціально-політичного. Значення таргетів коливаються біля середнього рівня, але найбільш неефективним є таргет економічної сфери, що стримує розвиток країни та унеможливлює розвиватися комплексно.

Чотириполюсна барицентрична модель збалансованості розвитку Малі представлена на рисунку 3.14.

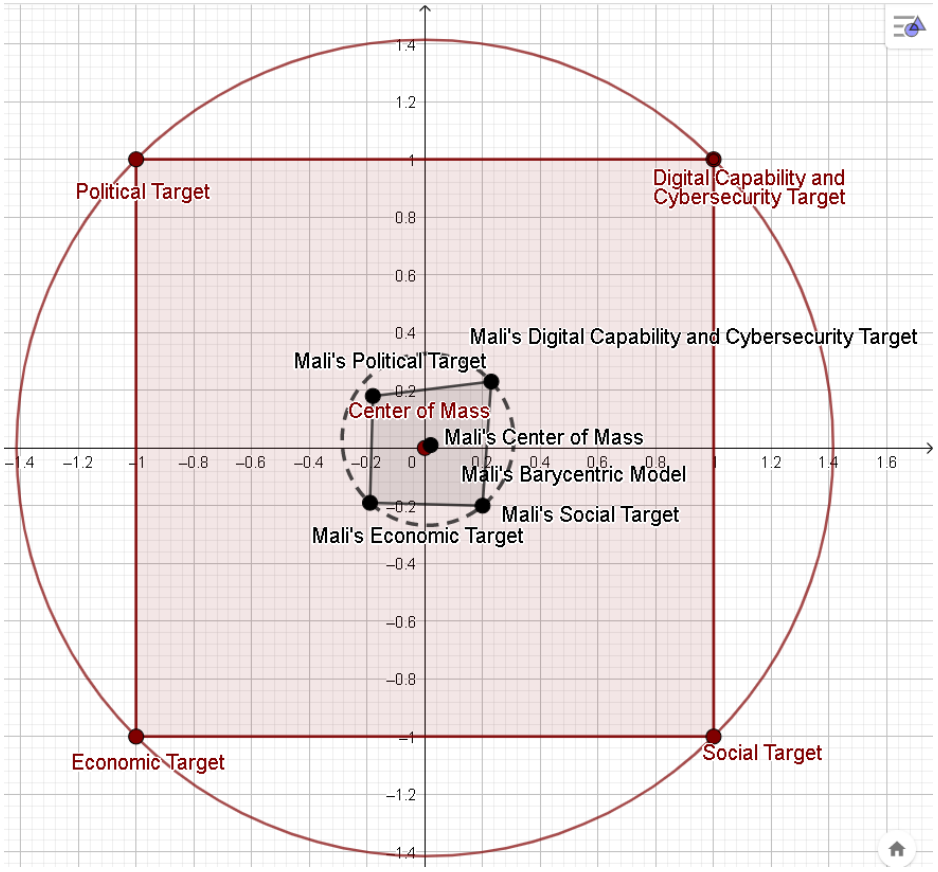

Рисунок 3.14 – Чотириполюсна барицентрична модель збалансованості розвитку Малі

За результатами моделі (рисунок 3.14) можна зробити наступні висновки: розвиток країни є збалансованим, оскільки відстань між центрами мас дорівнює 0.0196, але оскільки значення таргетів є досить низькими (0,2323 – для виміру цифрової спроможності та кібербезпеки; 0,1940 – для економічного; 0,1954 – для соціального; 0,1791 – для політичного) та наближаються до 0, то це говорить про досить слабкі темпи розвитку всіх сфер Малі. Співвідношення між парами вимірів незбалансоване, оскільки суми протилежних кутів не дорівнюють 180 градусів. За умови ефективних політичних рішень, фінансової допомоги міжнародних організації, трансформації стратегій умови збалансованості можуть сприяти більш динамічному подальшому розвитку країни.

В умовах динамічних змін, що відбуваються в різних сферах життєдіяльності суспільства, є важливим визначення ключових детермінант, які забезпечують збалансований розвиток економічної, політичної, соціальної сфер,

а також інформаційних технологій та кібербезпеки. Відповідно слід розуміти, що викликає дисбаланс та на скільки це може бути критичним. З цією метою автори даного дослідження використали підхід визначення центру мас геометричної фігури для моделювання рівня збалансованості розвитку країн, що відбувається на основі факторів економічного, соціального, політичного розвитку та цифрової спроможності і кібербезпеки. Модель представляє собою чотириполюсну барицентричну модель, сформовану на основі композитних таргетів, що формуються під впливом окреслених детермінант. Перелік факторів та таргети було обрано на основі проведеного аналізу літератури та методів наукового пізнання. Розрахунки проводилися для даних 127 країн світу, обраних за 2018 рік. Побудова барицентричної моделі відбувалася з урахуванням її трьох компонентів: значень композитних таргетів, рівня збалансованості пар таргетів та збалансованості всіх чотирьох таргетів, тобто визначення центру мас чотирикутника. В процесі аналізу отриманих значень було виявлено, що розвинуті країни мають інтегральні значення чотирьох композитних таргетів вищі, ніж для груп країн, що розвиваються, нових індустріальних та найменш розвинених. Це свідчить про високий рівень добробуту цих країн, соціального захисту їх населення, політичної стабільності, розвитку ІТ-сфери. Розраховані значення сум протилежних пар кутів для більшості країн не дорівнюють значення 180 градусів, що засвідчило про незбалансований рівень їх розвитку. Для розвинутих країн найбільш ефективною є пара соціально-політичного розвитку, що є наслідком високих темпів розвитку економіки. Але ця пара вимірів може слугувати також й драйвером для прискорення розвитку пари економічного таргету та таргету цифрової спроможності і кібербезпеки. Для країн, що розвиваються, та нових індустріальних незбалансованість може бути викликана різними детермінантами. Так, для більшості з них таким таргетом виступає цифрова спроможність та кібербезпека. Сюди відносяться Кот-д’Івуар, Хорватія, Грузія, Кенія, Молдова, Катар, Російська Федерація, Саудівська Аравія, Сербія, Україна, Єгипет, Індія, Малайзія, Пакистан, Туреччина. Цей факт може сприяти розвитку четвертинного сектору економіки цих країн та призвести

до поступової її трансформації у цифрову площину. Для більшості найменш розвинених країн незбалансованою є пара економіко-цифрового таргетів, в якій саме економічний є критичним для подальшого розвитку країни в цілому. Отримані висновки аналізу відстані розрахованого центру мас від еталонного значення показали, що є країни, для яких характерний збалансований розвиток на основі всіх чотирьох композитних таргетів. При цьому виявилося, що збалансованими можуть бути не тільки розвинені країни, але й ті, що розвиваються, та найменш розвинуті, такі як Малі й Бурунді. Але не дивлячись на цей факт, рівень розвитку їх таргетів відповідає їх класифікаційній групі, що дозволило зробити висновок про можливості подальшого динамічного розвитку таких країн за умови підтримки ефективності соціальної, політичної, економічної сфер, а також сфери цифрової спроможності і кібербезпеки. Тим країнам, розвиток яких є найбільш незбалансованим, наприклад, Саудівська Аравія, Україна, побудова барицентричної моделі дозволяє виявити той напрям або напрями, які призводять до цього. Це може бути викликано політичними коливаннями, військовими конфліктами, низькою якістю соціальної сфери, тощо. Результати даного дослідження слід прийняти до уваги відповідним державним органам, що відповідають за певну сферу розвитку країни, для розробки більш ефективних стратегій.

Пункт 3.1 було виконано із використанням матеріалів публікацій виконавців [54, 111].

3.2 Сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку

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 [112]. 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 [113]. Також рівень збитків від кіберзлочинності зростає у геометричній прогресії та за прогнозованими оцінками експертів він дорівнюватиме за 2021 рік 6 трлн. дол. [113]. 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.

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. [58], Ванг Р., Лью Дж. [60], Мішра С.П., Кумарі П. [63], Мектерович І., Каран М., Пінтар Д., Брккіч Л. [67], 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 [42]. Чжоу Ю., Сонг Кс., Чжоу М. запропонували метод бустінгу для прогнозування шахрайських операцій [62]. 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. [43]. 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 [25].

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 [31]. Діонісій С. Деметіс розглядав технології виявлення операцій з легалізації незаконних коштів, серед яких виділяв ризикологію та методи оцінювання ризиків [47]. Гальяні Г. досліджував поняття «технологічної нейтральності» по відношенню до кібербезпеки у контексті формування та забезпечення міжнародного правового поля з даного питання [30].

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 дослідження 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, що буде виконано в рамках формування сценаріїв конвергенції.

Для здійснення оцінки рівня конвергенції скористаємося підходом, запропонованим Яровенко Г.М. у роботі [54, 114] 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 [33] 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 (3.10)):

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \tag{3.10}$$

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 (3.11):

$$d_{ij} = \exp(-\exp(-Z_{ij})), \quad (3.11)$$

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 3.15 та 3.16.

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.

Рисунок 3.15 – Графік кривої першого типу для «Національного індексу кібербезпеки»

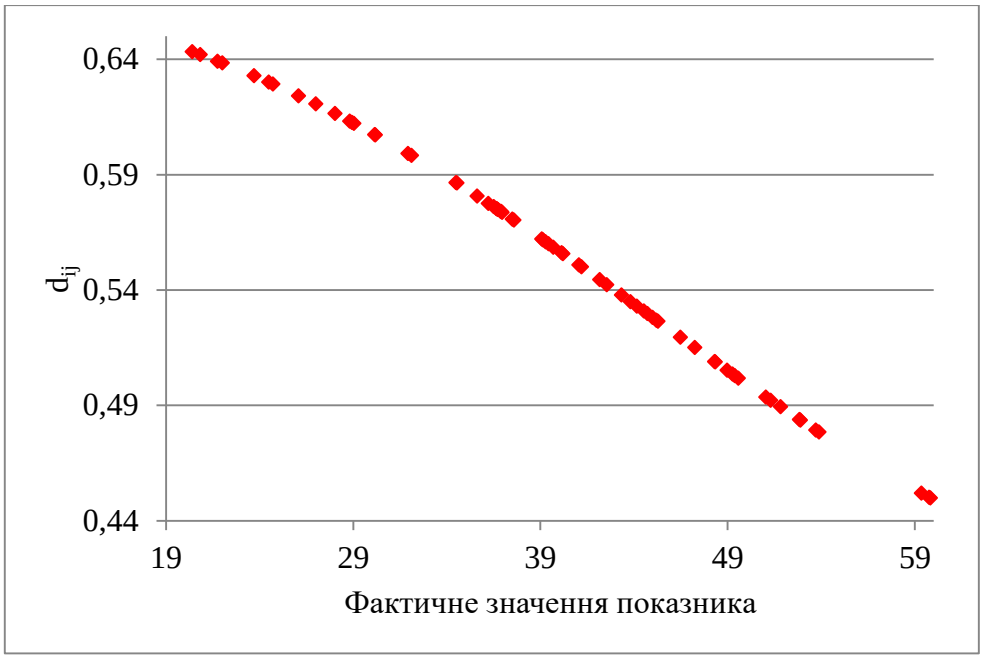

Рисунок 3.16 – Графік кривої четвертого типу для «Індексу злочинності»

Для показників, залежності для яких описуються кривою першого типу, використаємо формулу (3.12):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{Z_{ij}-\min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right), \quad (3.12)$$

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 (3.13):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_{i} Z_{ij}-Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right). \quad (3.13)$$

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 3.17.

З рисунку 3.17 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.

N=76	Canonical Analysis Summary (Konvergentcia2.sta) Canonical R: .93762 Chi²(24)=200.41 p=0.0000 **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

Рисунок 3.17 – Підсумки канонічного аналізу

Статистичну значимість коефіцієнта кореляції підтверджує високе значення критерію Пірсона ($\chi^2 = 200{,}00$), 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 [115, 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 3.18-3.19).

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

Рисунок 3.18 – 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

Рисунок 3.19 – 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 (3.14)-(3.15):

$$IC_i = \sqrt[\Sigma_{j=1}^{n} a_j]{\prod_{j=1}^{n} \left(d_{ij}^{*}\right)^{a_j}}, \qquad (3.14)$$

$$IP_i = \sqrt[\Sigma_{j=1}^{m} a_j]{\prod_{j=1}^{m} \left(d_{ij}^{*}\right)^{a_j}}, \qquad (3.15)$$

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 3.20-3.21.

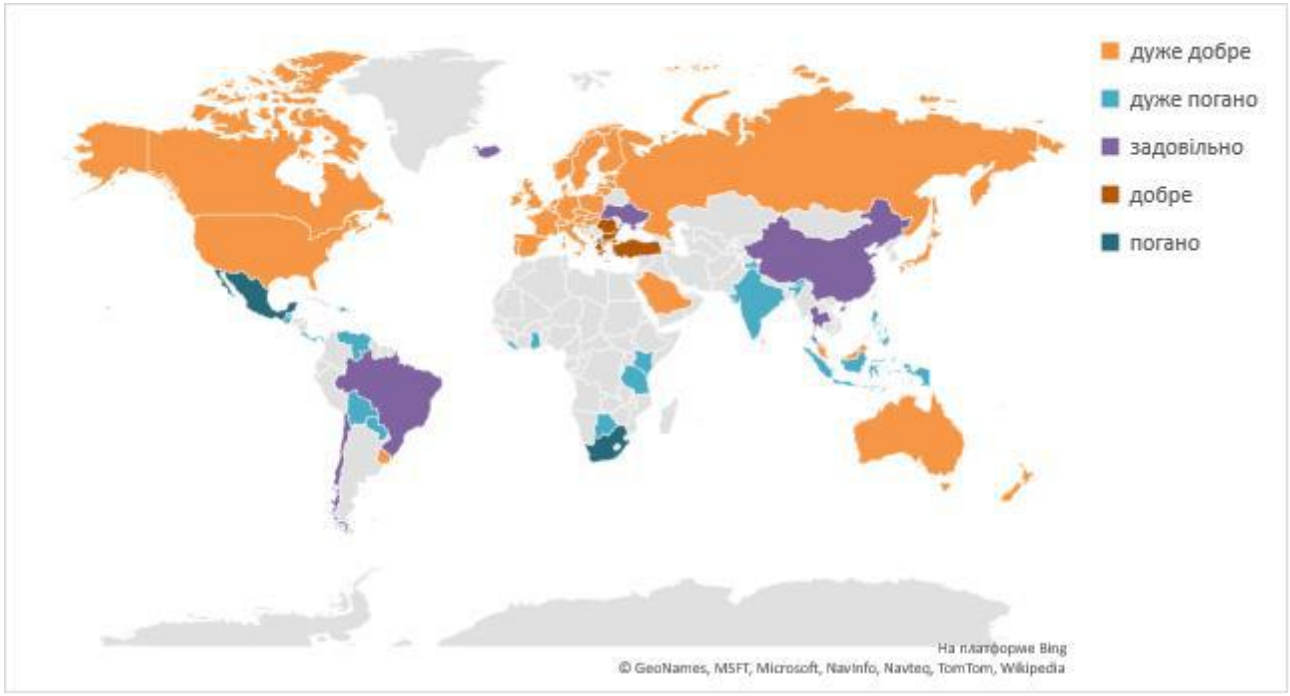

Рисунок 3.20 – Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку їх системи кібербезпеки

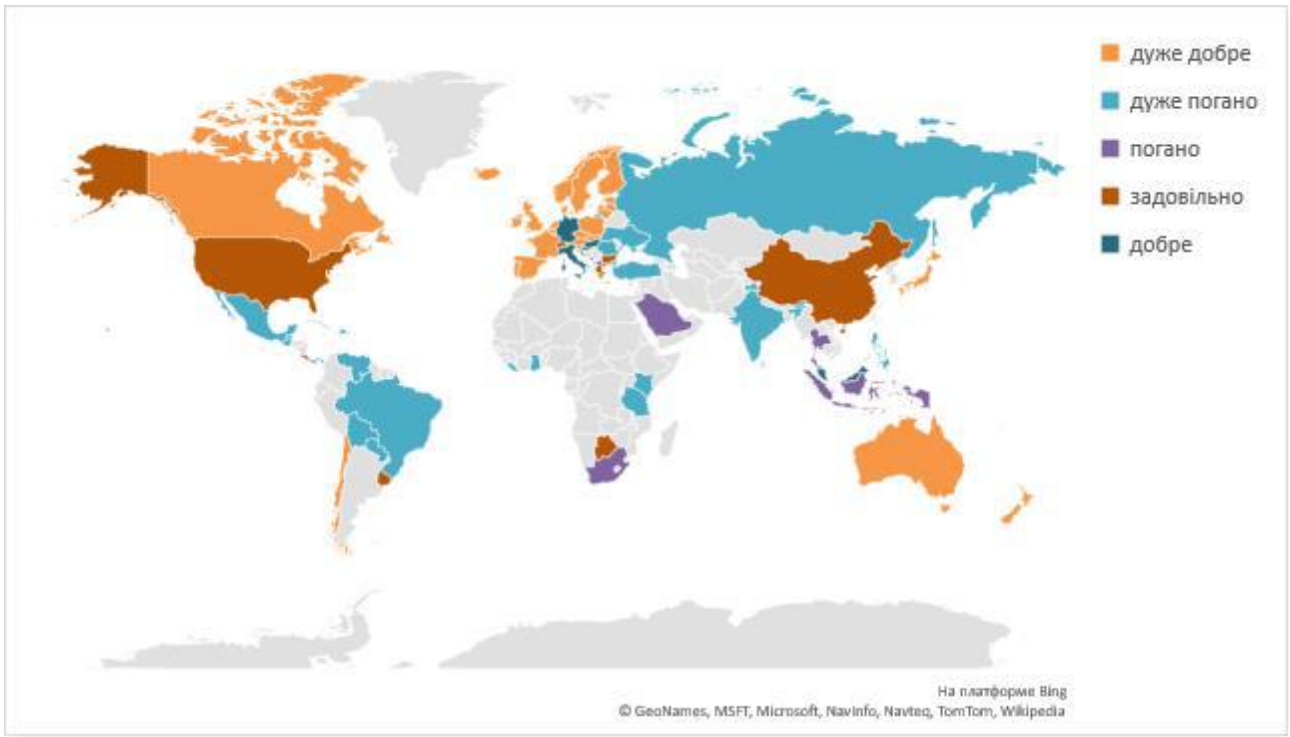

Рисунок 3.21 – Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку системи протидії легалізації кримінальних доходів

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. 3.20), 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.

За інтегральним рівнем протидії фінансовим шахрайствам оцінку «дуже добре» отримали 28 країн (див. рис. 3.21): 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. 3.22).

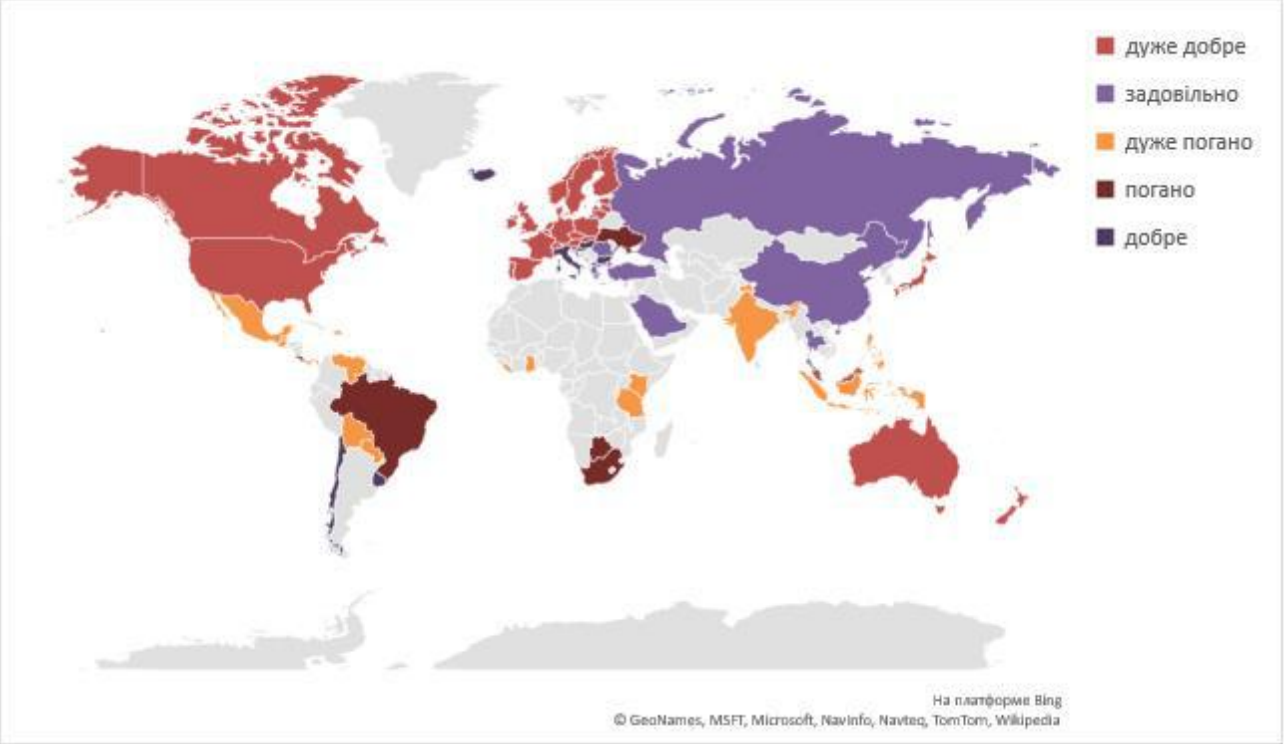

Рисунок 3.22 – Карта розподілу країн за рівнем конвергенції систем кібербезпеки та протидії легалізації кримінальних доходів

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.

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 дослідженні 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.

Пункт 3.2 було виконано із використанням матеріалів публікацій виконавців [54, 116].

4 ОЦІНКА СИНЕРГЕТИЧНОГО ЕФЕКТУ ВІД КОНВЕРГЕНЦІЇ МОДЕЛЕЙ ФІНАНСОВОГО МОНІТОРИНГУ ТА КІБЕРБЕЗПЕКИ

Запропонована методологія інтегрального оцінювання рівня конвергенції системи фінансового моніторингу та кібербезпеки дозволила розробити сценарії шляхом ранжування країн, використовуючи якісну шкалу оцінювання, запропоновану Харрінгтоном-Менчером. Але інтегральне уявлення не дозволяє повністю зробити висновки щодо ефективності системи забезпечення конвергенції системи фінансового моніторингу та кібербезпеки, тобто необхідно здійснити структурний аналіз її компонентів, який дозволить оцінити не тільки поточний стан складових інтегрального показника конвергенції системи фінансового моніторингу та кібербезпеки, але й визначити резерви для його підвищення. З цією метою необхідно провести аналіз ефективності системи забезпечення конвергенції системи фінансового моніторингу та кібербезпеки та надати рекомендації щодо напрямів її покращання.

В залежності від мети аналізу у науковій літературі та на практиці застосовують різні підходи. Традиційними вважаються: класична модель Дюпона «Рентабельність капіталу», процесно-орієнтований аналіз рентабельності М. Мейера та В. Маршала, «Управління результатами» Р. Каплана та Д. Нортона, методика аналізу, заснована на аналізі грошових потоків.

Основними недоліками перелічених методів є те, що їх використання доцільно для аналізу ефективності господарської діяльності та передбачає розрахунок різних коефіцієнтів, за результатами яких робиться висновок. У випадку оцінювання ефективності системи забезпечення конвергенції системи фінансового моніторингу та кібербезпеки доцільно використання саме математичних методів, які дозволяють проводити оцінювання параметрів відносно значень, які є найкращими у групі аналізованих об’єктів. Саме тому для проведення дослідження було використано DEA-метод (Data Envelopment

Analysis), який було запропоновано А. Чарнсом, В. Купером та Е. Родесом у 1978 році [117]. Цей інструмент не залежить від мети аналізу та використовується у багатьох галузях для оцінки ефективності складних систем, що відбувається шляхом рішення оптимізаційної задачі лінійного програмування. Її мета – це визначення ефективності системи на основі співвідношення її виходів та входів, при цьому необхідно врахувати максимальний вихід ресурсів при заданому рівні входів, або мінімальний рівень ресурсів при заданому рівні виходів.

Для проведення дослідження було обрано вхідні дані, які було відібрано у розділі 3 на основі канонічного аналізу та розрахунку інтегрального показника конвергенції системи фінансового моніторингу та кібербезпеки, а саме: глобальний індекс кібербезпеки; національний індекс кібербезпеки; індекс мережевої готовності; рівень цифрового розвитку; індекс політичної стабільності; індекс ефективності уряду; легкість ведення бізнесу; індекс злочинності; глобальний індекс тероризму; індекс фінансової таємниці. Дані показники сформували базу вхідних даних для 76 країн світу за 2018 рік. У якості вихідного параметру, який є індикатором узагальненого рівня ефективності, виступатиме запропонований у підрозділі 3.2 інтегральний індекс конвергенції системи фінансового моніторингу та кібербезпеки.

Оскільки DEA-метод є ефективним для даних, які мають близькі характеристики, то доцільно сформувати кластери країн. Було проведено сортування за інтегральним індексом конвергенції системи фінансового моніторингу та кібербезпеки та виділено 7 груп країн.

Так, до 0-го кластеру увійшли 12 країн: Фінляндія, Австралія, Австрія, Данія, Канада, Ірландія, Швеція, Нова Зеландія, Норвегія, Естонія, Бельгія, Португалія. До 1-го кластеру увійшли: Іспанія, Литва, Словенія, Латвія, Нідерланди, Японія, Великобританія, Франція, Кіпр, Чехія, Німеччина, Словаччина. До 2-го кластеру віднесено: Польща, Малайзія, Сінгапур, Швейцарія, США, Люксембург, Угорщина, Хорватія, Мавританія, Італія, Ісландія, Уругвай. До 3-го кластеру увійшли: Чилі, Мальта, Ізраїль, Болгарія, Греція, Саудівська Аравія, Росія, Чорногорія, Бруней, Північна Македонія,

Бахрейн, Китай. До 4-го кластеру віднесено: Туреччина, Таїланд, Румунія, Коста Рика, Південна Африка, Сейшельські острови, Україна, Бразилія, Ботсвана, Мексика, Індонезія, Панама. До 5-го кластеру: Тринідад і Тобаго, Барбадос, Філіппіни, Індія, Домініканська Республіка, Гана, Домініка, Парагвай, Кенія, Гренада, Вануату, Венесуела. До 6-го кластеру: Болівія, Гватемала, Танзанія, Ліберія.

Використання DEA-методу дозволить визначити ефективність конвергенції системи фінансового моніторингу та кібербезпеки з урахуванням потенціалу країни. Ефективність буде досягатися тоді, коли рівень протидії загрозам для окремої країни не можливо збільшити, при цьому залишивши рівень розвитку та безпеки країни на тому самому рівні. Також це можливо у випадку, коли зменшення рівня розвитку та безпеки країни призводить до змін рівня протидії кіберзагрозам. Виходячи з вище сказаного, можна сформувати початкову DEA-модель [117], яку буде використано для проведення оцінки ефективності рівня інформаційної безпеки країни за формулою (4.1):

$$\max \theta_s = \frac{\sum_{p=1}^{z} u_{ps} y_{ps}}{\sum_{i=1}^{m} v_{is} x_{is}}$$

$$\begin{cases} \dfrac{\sum_{p=1}^{z} u_{ps} y_{pj}}{\sum_{i=1}^{m} v_{is} x_i\, j} \le 1, \\ s, j = \overline{1, n}, \\ u_p, v_i \ge 0, \\ y_{p,} x_i \ge 0. \end{cases} \qquad (4.1)$$

де θ – рівень ефективності конвергенції системи фінансового моніторингу та кібербезпеки для конкретної країни, визначений як коефіцієнт між зваженою сумою виходів та входів;

u_p – ваги виходів, які максимізують показник ефективності оцінюваної одиниці θ;

v_p – ваги входів, які максимізують показник ефективності оцінюваної одиниці θ;

y_p – p-та характеристика умовних виходів, тобто значень індексу конвергенції системи фінансового моніторингу та кібербезпеки для кожної країни;

x_i – i-та характеристика умовних входів, тобто значень показників системи фінансового моніторингу та кібербезпеки.

Обмеження (4.1) говорять про те, що відношення виходу до входу не може перевищувати 1 для кожної θ. Тому представлену дробову задачу слід перетворити на лінійну, що значно спрощує її подальше використання. Відповідно до цього, розрізняють два типи DEA-моделі – CCR (Charnes A., Cooper W. and Rhodes E.), яку було запропоновано Чарнсом А., Купером У. та Родесом Е. [117] у 1978 році, та BCC (Banker R., Charnes A. and Cooper W.), яку було розроблено на основі CCR-моделі у 1984 році Банкером Р., Чарнсом А. та Купером У. [118]. Кожна з цих моделей (4.2) – (4.5) орієнтована на вхід (ресурси) та вихід (результуючі показники):

$$\max_{u,v} \theta_s = \sum_{p=1}^{z} u_{ps} y_{ps}$$

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} - \sum_{i=1}^{m} v_{is} x_{ij} \le 0 \\ u_p, v_i \ge \gamma \end{cases} \tag{4.2}$$

$$\max_{u,v,k} \theta_s = \sum_{p=1}^{z} u_{ps} y_{ps} + k_s$$

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} + k_s \le \sum_{i=1}^{m} v_{is} x_{ij} \\ u_p, v_i \ge \gamma \\ k_s - unconstrained \end{cases} \tag{4.3}$$

$$\min_{\alpha,\beta,k} \theta_s = \sum_{i=1}^{m} \beta_i x_{is} - k_s$$

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - k_s \geq \sum_{p=1}^{z} \alpha_p y_{pj} \\ \alpha_p, \beta_i \geq \gamma \\ k_s - \ unconstrained \end{cases} \quad (4.4)$$

$$\min_{\alpha,\beta} \theta_s = \sum_{i=1}^{m} \beta_i x_{is}$$

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - \sum_{p=1}^{z} \alpha_p y_{pj} \geq 0 \\ \alpha_p, \beta_i \geq \gamma \end{cases} \quad (4.5)$$

де γ – це невелике додатне дійсне число, яке виключає можливість набуття змінними нульового значення.

Моделі CCR (4.2) та BCC (4.3) є Input-oriented моделями, тобто направлені на оцінку ефективності розподілу показників, що характеризують системи фінансового моніторингу та кібербезпеки, що сприяє виявленню структурної неефективності заданих індексів. Моделі CCR (4.4) та BCC (4.5) є Output-oriented, тобто дозволяють здійснити оцінку ефективності конвергенції системи фінансового моніторингу та кібербезпеки країни шляхом визначення максимальних значень індексу конвергенції системи фінансового моніторингу та кібербезпеки за умови заданих значень показників, що характеризують системи фінансового моніторингу та кібербезпеки.

DEA-аналіз було проведено у аналітичному пакеті “Frontier Analyst”, який дозволяє здійснювати розрахунки за моделями CCR та BCC [119]. Оскільки було

використано демо-версію, то для дослідження в кожному кластері країн було обрано 12 представників, для яких проводився Data Envelopment Analysis. Мінімальне значення вагів у програмі було встановлено на основі результатів проведеного канонічного аналізу за допомогою аналітичної платформи “STATISTICA”, що дозволило визначити частки їх значень у загальній сукупності. Так, для глобального індексу кібербезпеки визначено вагу, що дорівнює 0,3133, індексу мережевої готовності – 0,2644, національного індексу кібербезпеки – 0,0213, рівня цифрового розвитку – 0,5578, індекс політичної стабільності – 0,2691; індекс ефективності уряду – 0,7808; легкість ведення бізнесу – 0,3417; індекс злочинності – 0,0501; глобальний індекс тероризму – 0,0093; індекс фінансової таємниці – 0,0915. Максимальне значення вагів було встановлено на рівні 100%, тому відповідні значення було перераховано у пропорції.

Модель CCR є більш обмежувальною ніж BCC. Це пов’язано із тим, що вона базується на постійності віддачі від масштабу, а також дає можливість масштабувати неефективні одиниці вибірки. BCC-модель базується на змінній віддачі від масштабу та дозволяє оцінити технічну ефективність. Така зміна її вхідних параметрів може призводити до непропорційної зміни вихідних, що дозволяє оцінювати більшість об’єктів як ефективні. Тому для визначення синергетичних ефектів будемо використовувати тільки BCC-модель.

Проаналізуємо структурну ефективність вхідних показників для країн 0-го кластеру, отриману в результаті проведення аналізу за Input-oriented CCR-model (рисунок 4.1). Отримані значення всіх показників є від’ємними, тобто забезпечення поточного рівня конвергенції системи фінансового моніторингу та кібербезпеки країн 0-го кластеру відбувається із досягненням ефективності по кожному напряму – фінансового моніторингу та кібербезпеки. При чому можна побачити, що є потенціал для забезпечення рівня конвергенції (8,51%). Слід відмітити, що для даних країн найбільший резерв формується саме за глобальним індексом тероризму, що свідчить про те, що для даних країн відсутні

сприятливі умови для легалізації кримінальних доходів та фінансування тероризму.

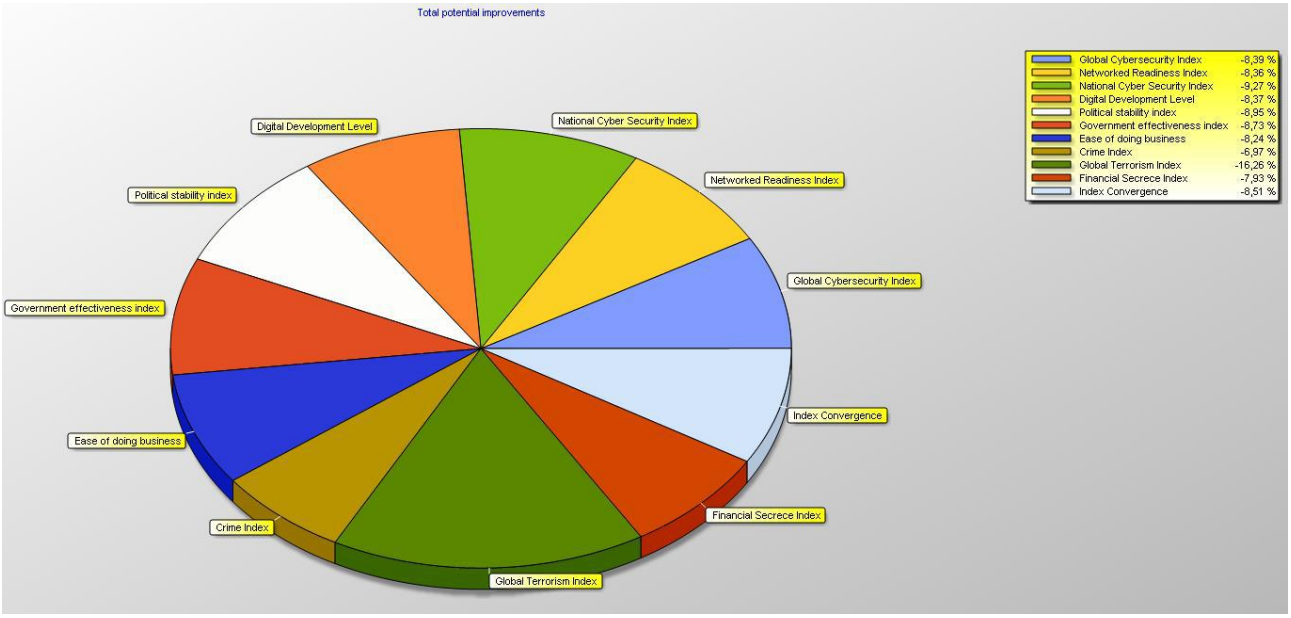

Рисунок 4.1 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 0-го кластеру (за Input-oriented CCR-моделлю)

Проведемо аналіз потенціалу покращання ефективності конвергенції системи фінансового моніторингу та кібербезпеки 0-го кластера за умови максимізації інтегрального індексу конвергенції системи фінансового моніторингу та кібербезпеки. Результати Output-oriented CCR-model представлено на рисунку 4.2, де можна побачити, що максимальне зростання індексу конвергенції системи фінансового моніторингу та кібербезпеки можливе на 6,6%. Це можливо забезпечити за рахунок резервів потенціалу за показниками: національний індекс кібербезпеки (-4,18%), індекс злочинності (-36,48%). Тобто країни 0-го кластеру мають, з одного боку, високий потенціал розвитку кібербезпеки в країні, достатній для забезпечення підвищення рівня конвергенції, а з іншого боку, низький рівень злочинності створює передумови для формування ефективної системи фінансового моніторингу.

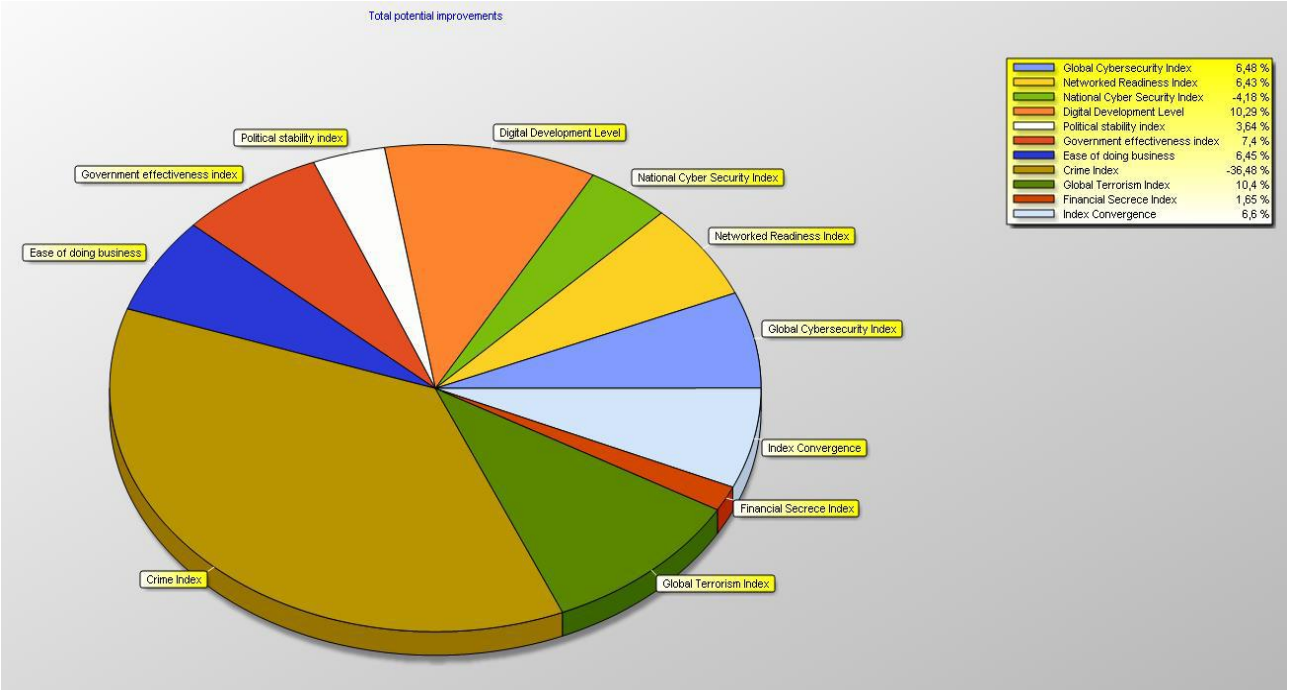

Рисунок 4.2 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 0-го кластеру (за Output-oriented CCR-моделлю)

Проаналізуємо структурну ефективність вхідних показників для країн першого кластеру (рисунок 4.3). Отримані значення всіх показників є додатними, що свідчить про те, що не можливо досягти рівня конвергенції системи фінансового моніторингу та кібербезпеки за рахунок поточного стану їх функціонування. Хоча країни даного кластеру мають розвинену економіку, але існують проблеми на національному рівні, які переважають здійснення конвергенції систем.

Найбільшого удосконалення потребує індекс ефективності уряду, який необхідно підвищити на 11,67%, а також індекс мережевої готовності (10,24%). Для забезпечення поточного рівня конвергенції систем країн 1-го кластеру необхідно підвищити ефективність функціонування всіх відповідних напрямів, які характеризують систему кібербезпеки в країні та протидії фінансовим кіберзлочинам.

Проаналізуємо структурну ефективність вихідних показників для країн першого кластеру (рисунок 4.4).

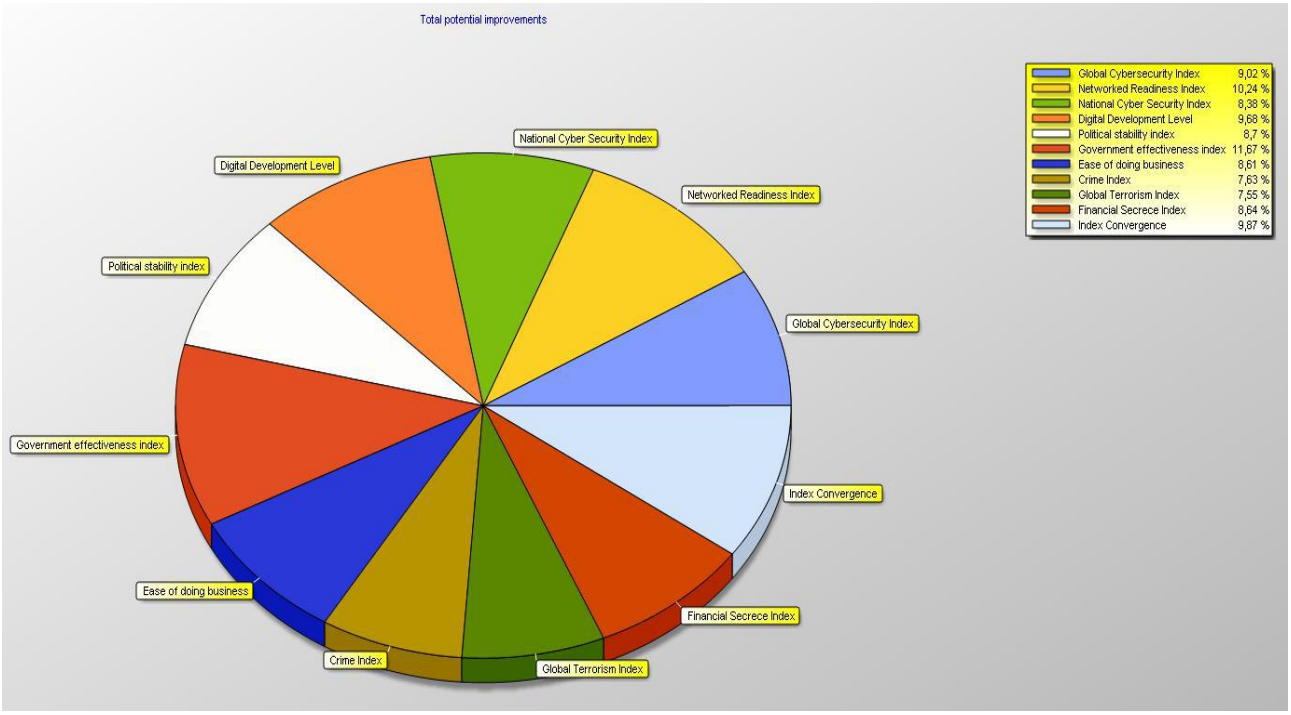

Рисунок 4.3 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 1-го кластеру (за Input-oriented CCR-моделлю)

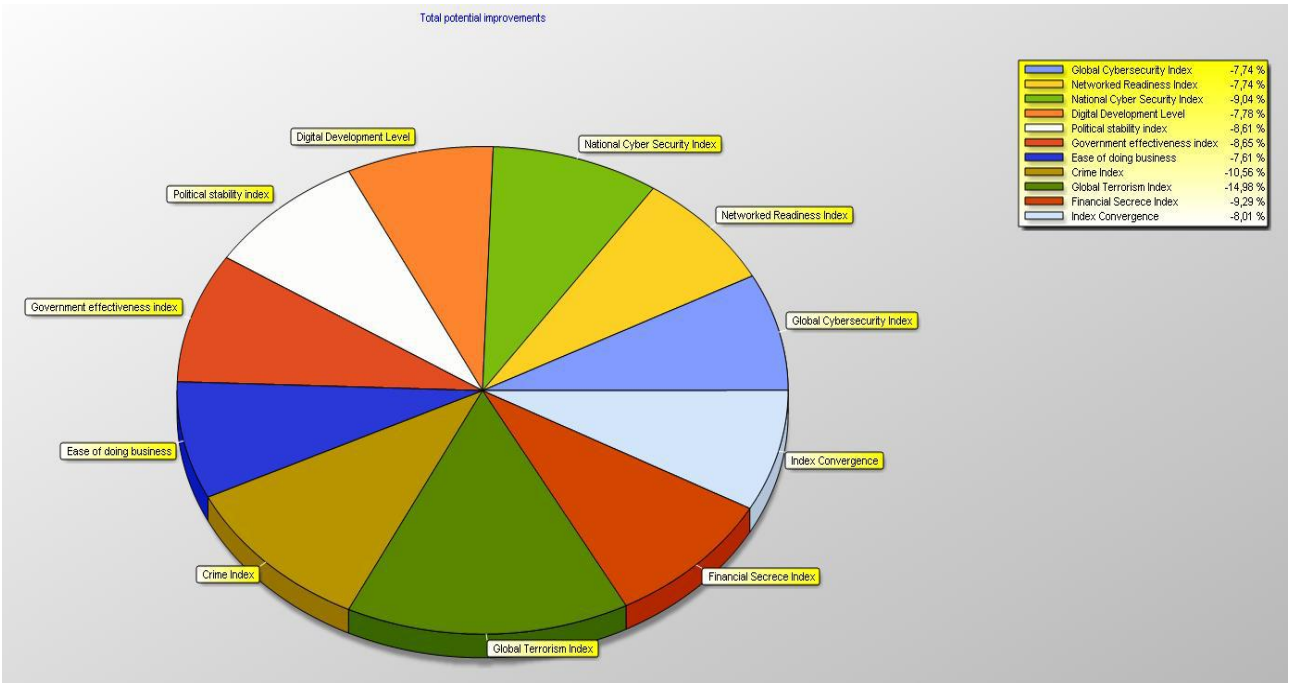

Рисунок 4.4 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 1-го кластеру (за Output-oriented CCR-моделлю)

Аналіз потенціалу покращання ефективності конвергенції систем фінансового моніторингу та кібербезпеки першого кластера за умови максимізації інтегрального індексу конвергенції показує, що його максимальне зростання можливе на 8,01%. Це можливо забезпечити за рахунок резервів потенціалу за показниками: глобальний індекс кібербезпеки (-7,74%), мережевий індекс готовності (-7,74%), рівень цифрового розвитку (-7,78%) та національний індекс кібербезпеки (-9,04%). Тобто країни першого кластеру мають значний потенціал системи кібербезпеки, достатній для забезпечення підвищення рівня конвергенції систем. Щодо системи протидії фінансовим злочинам, то ці країни в даній сфері також мають значний потенціал, а саме: індекс політичної стабільності (-8,61%); індекс ефективності уряду (-8,65%); легкість ведення бізнесу (-7,61%); індекс злочинності (-10,56%); глобальний індекс тероризму (-14,98%); індекс фінансової таємниці (-9,29%).

Тобто, країни 1-го кластеру не можуть досягнути поточного рівня конвергенції, але існуючий потенціал може забезпечити максимальний рівень, який є нижче поточного.

Проаналізуємо структурну ефективність вхідних показників для країн другого кластеру (рисунок 4.5). Отримані значення всіх показників є додатними, що свідчить також про те, що країни цього кластеру не можуть досягти поточного рівня конвергенції системи фінансового моніторингу та кібербезпеки, який потребує зростання на 12,4%. Найбільшого удосконалення потребують індекси кібербезпеки, які необхідно підвищити вище ніж на 10% кожний. Результати показують, що для забезпечення ефективного процесу інтеграції необхідно звернути увагу саме на рівень кібербезпеки. Наприклад, в даному кластері знаходиться США, які сьогодні займають перше місце серед країн, які є атакованими з боку інших країн. При цьому ця країна є також лідером щодо здійснення кібератак на інші країни. Тому проблема, пов’язана із кіберзахистом, є актуальною для країн даного кластеру.

Проаналізуємо структурну ефективність вихідних показників для країн другого кластеру (рисунок 4.6).

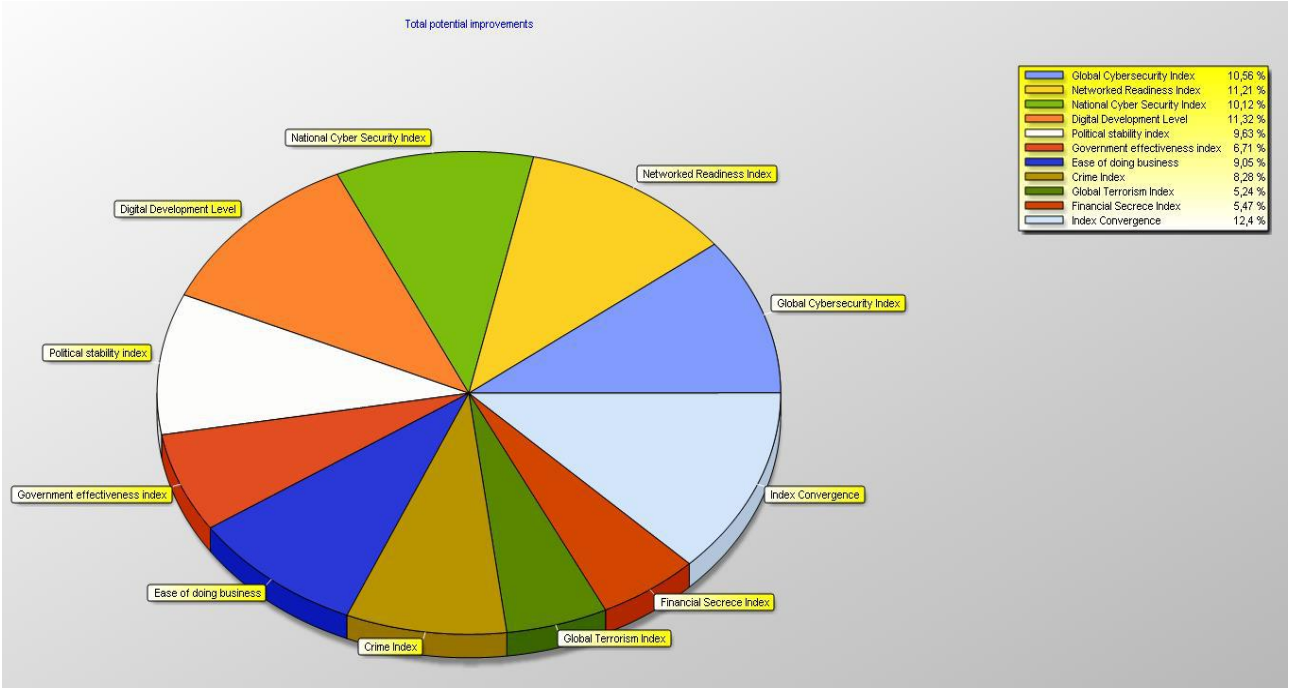

Рисунок 4.5 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 2-го кластеру (за Input-oriented CCR-моделлю)

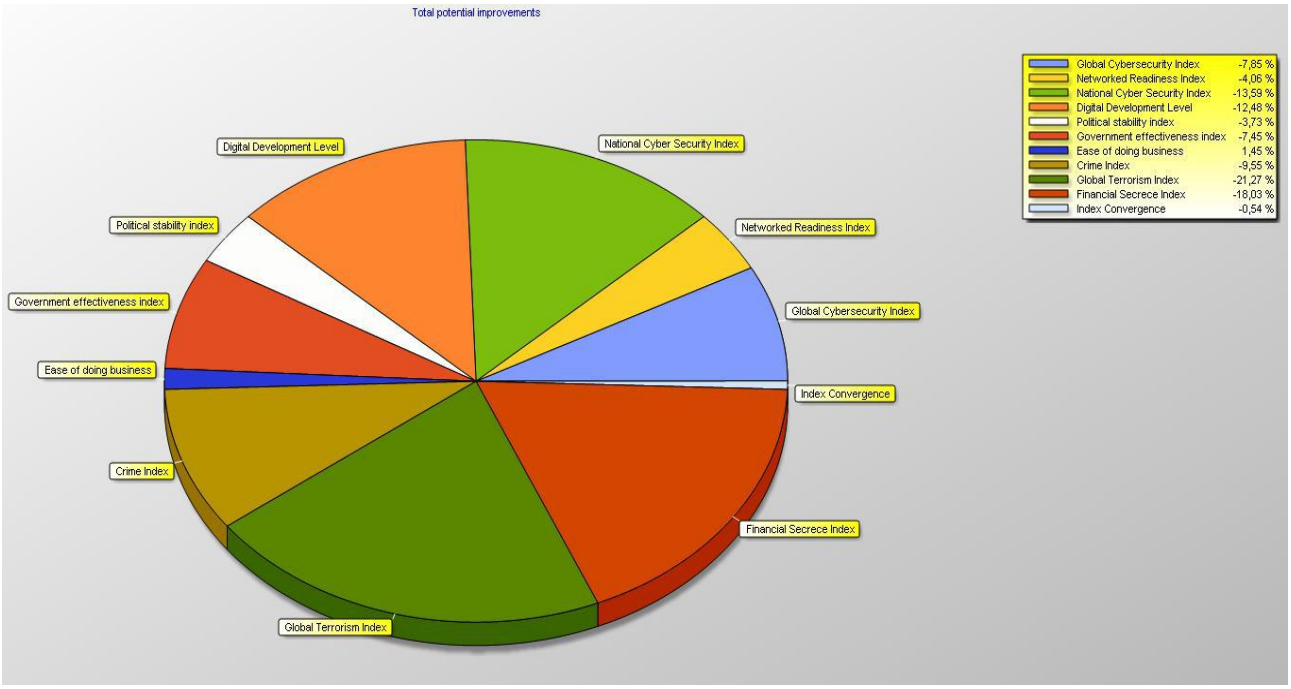

Рисунок 4.6 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 2-го кластеру (за Output-oriented CCR-моделлю)

Аналіз потенціалу покращання ефективності конвергенції систем фінансового моніторингу та кібербезпеки другого кластера за умови максимізації інтегрального індексу конвергенції показує, що його максимальне зростання можливе тільки на 0,54%. Це можливо забезпечити за рахунок резервів потенціалу за показниками: глобальний індекс кібербезпеки (-7,85%), мережевий індекс готовності (-4,06%), рівень цифрового розвитку (-12,48%) та національний індекс кібербезпеки (-13,59%). Тобто країни даного кластеру мають потенціал системи кібербезпеки, достатній для незначного підвищення рівня конвергенції систем. Дані країни мають потенціал системи протидії фінансовим злочинам, а саме: індекс політичної стабільності (-3,73%); індекс ефективності уряду (-7,45%); індекс злочинності (-9,55%); глобальний індекс тероризму (-21,27%); індекс фінансової таємниці (-18,03%).

Тобто, країни 2-го кластеру не можуть досягнути поточного рівня конвергенції, але досягнення максимального рівня ефективності є досить незначним, оскільки спостерігається розбалансованість систем фінансового моніторингу і кібербезпеки.

Проаналізуємо структурну ефективність вхідних показників для країн 3-го кластеру (рисунок 4.7). Отримані значення всіх показників є від’ємними, що свідчить не тільки про забезпечення поточного рівня конвергенції системи фінансового моніторингу та кібербезпеки, але й його перевищення на 10,94%. При цьому спостерігається досягнення ефективності по всім показникам, що характеризують систему фінансового моніторингу та кібербезпеки. Найбільше значення характерне для індексу ефективності уряду, яке дозволяє його підвищення на 11,22%. Тобто політика уряду цих країн є настільки ефективною, що створюються можливості для протидії легалізації кримінальних доходів. Але, оскільки рівень конвергенції країн цього кластеру є нижче, ніж для країн 2-го кластеру, то отриманий результат говорить тільки про те, що країни досягли певного рівня конвергенції, який відповідає рівню їх економічного розвитку.

Проаналізуємо структурну ефективність вихідних показників для країн третього кластеру (рисунок 4.8).

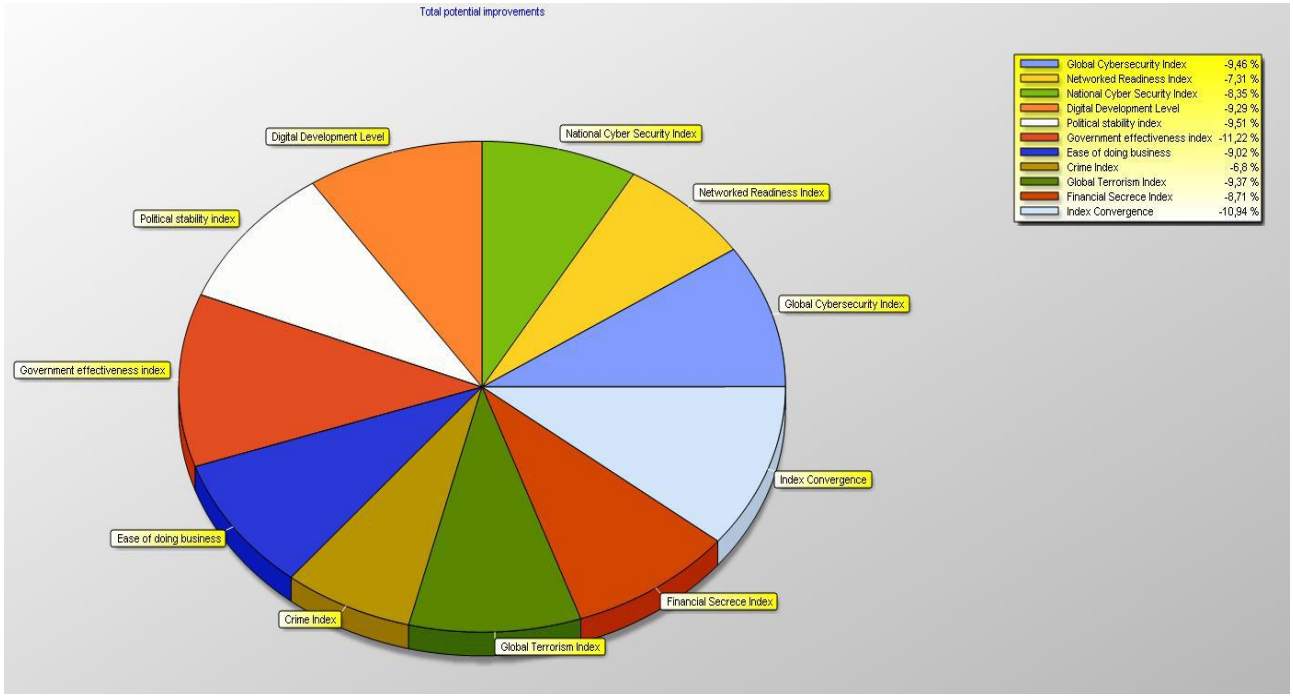

Рисунок 4.7 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 3-го кластеру (за Input-oriented CCR-моделлю)

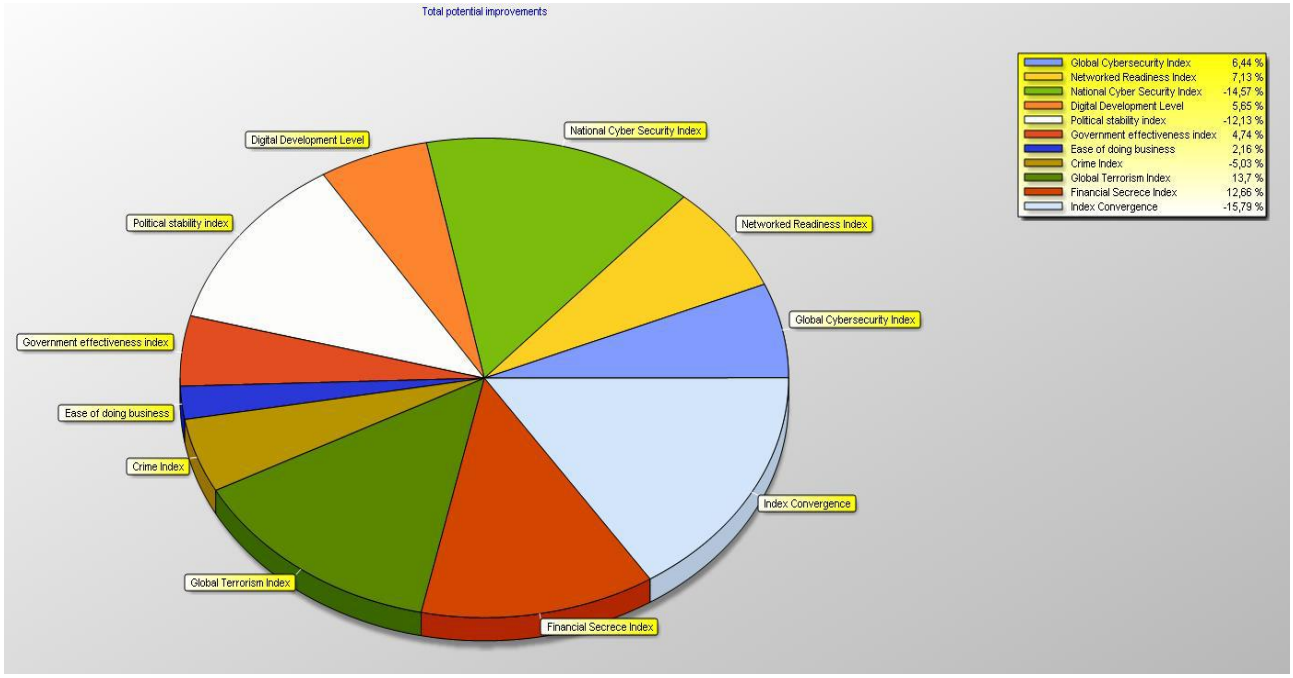

Рисунок 4.8 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 3-го кластеру (за Output-oriented CCR-моделлю)

Результати Output-oriented CCR-model (рис. 4.8) показують, що максимальне зростання індексу конвергенції системи фінансового моніторингу та кібербезпеки можливе на 15,79%. Це можливо забезпечити за рахунок резервів за показниками: національний індекс кібербезпеки (-14,57%), індекс політичної стабільності (-12,13%) та індексу злочинності (-5,03%). Всі інші фактори потребують відповідного покращення, щоб забезпечити максимальний рівень конвергенції систем. Оскільки фактичний рівень конвергенції забезпечується та спостерігається його перевищення, то країни 3-го кластеру мають значний потенціал для ефективного рівня інтеграції двох систем.

Проаналізуємо структурну ефективність вхідних показників для країн четвертого кластеру (рисунок 4.9). Отриманий інтегральний рівень свідчить про те, що його фактичне значення не може бути забезпечено на 0,12%. Це відбувається за рахунок високого рівня злочинності в даних країнах (93,69%). При чому показники, що характеризують систему фінансового моніторингу є додатними, тобто для даних країн характерні сприятливі умови для легалізації кримінальних доходів та фінансування тероризму. Але система кібербезпеки має незначний резерв в межах 1% по кожному показнику безпеки, що свідчить про можливості підтримки системи фінансового моніторингу за рахунок системи кібербезпеки.

Проаналізуємо структурну ефективність вихідних показників для країн другого кластеру (рисунок 4.10). Результати Output-oriented CCR-model показують, що можливе тільки максимальне зниження індексу конвергенції системи фінансового моніторингу та кібербезпеки на 13,23%. Показники не мають резервів зростання, оскільки отримані значення є додатними. Така ситуація може свідчити тільки про те, що країни цього кластеру мають серйозні проблеми, пов’язані із організацією системи протидії фінансовим кібершахрайствам, а також забезпечення кіберзахисту. Тому інтеграція цих систем не сприятиме отриманню синергетичного ефекту.

До даного кластеру відноситься Україна. Показники її ефективності представлені на рисунках 4.11-4.12.

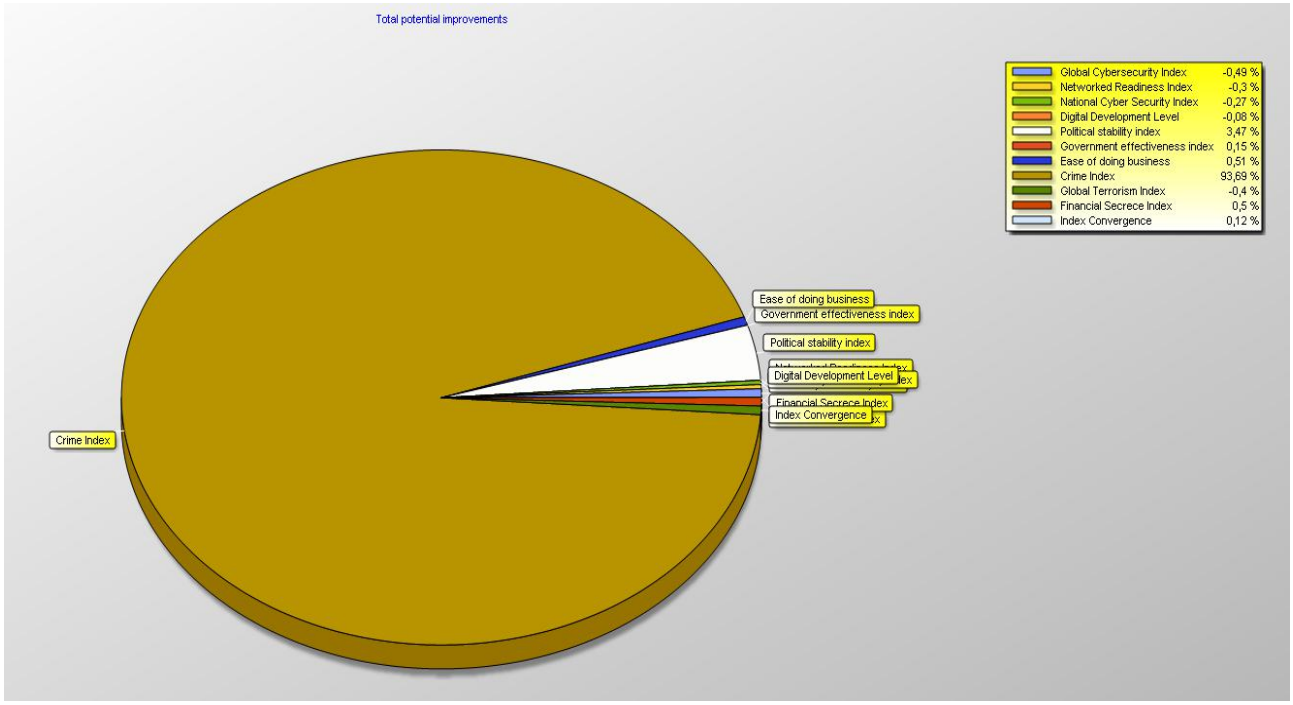

Рисунок 4.9 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 4-го кластеру (за Input-oriented CCR-моделлю)

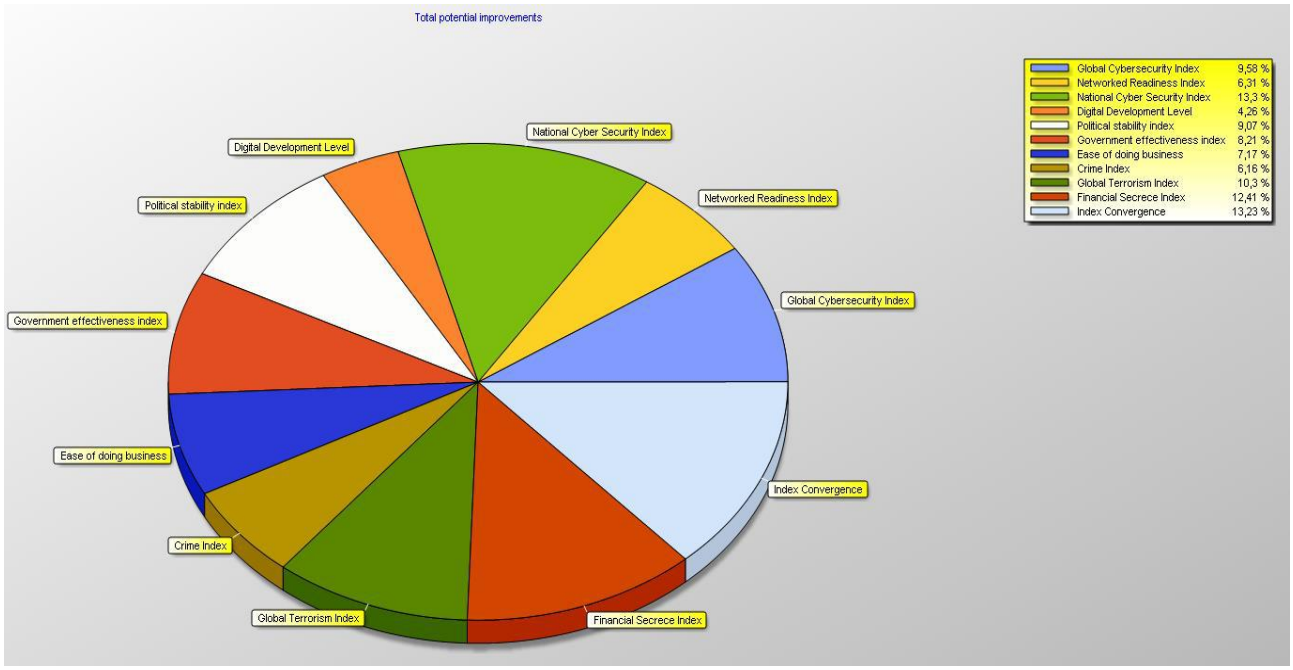

Рисунок 4.10 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 4-го кластеру (за Output-oriented CCR-моделлю)

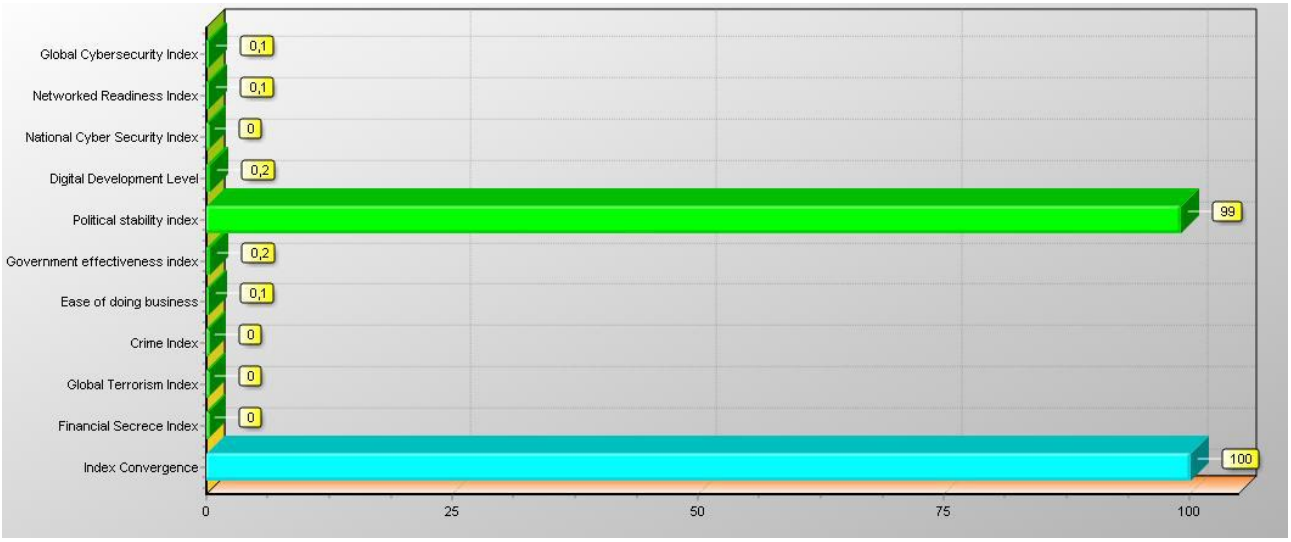

Рисунок 4.11 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки України (за Input-oriented CCR-моделлю)

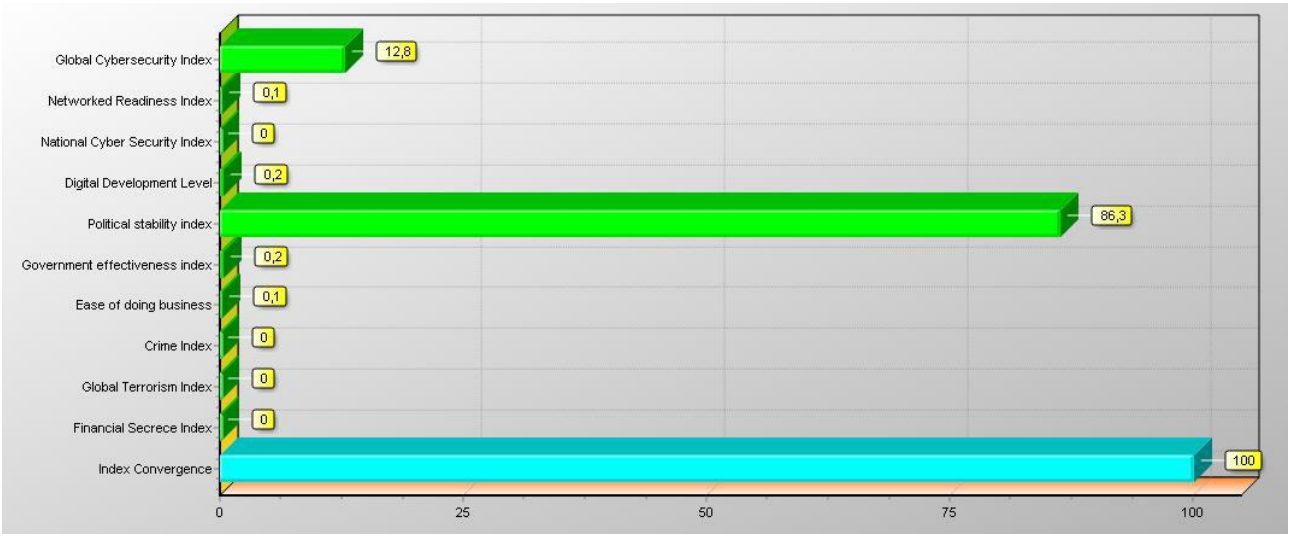

Рисунок 4.12 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки України (за Output-oriented CCR-моделлю)

Україна є представником 4-го кластеру. Ефективність конвергенції її системи фінансового моніторингу та кібербезпеки забезпечується на рівні 100,0% по відношенню до інших країн кластеру (рисунок 4.11). Всі показники або близькі до 0 або є додатними, що свідчить про відсутність резервів зростання рівня інтеграції для України. Але такий показник, як індекс політичної

стабільності, має критичне значення - 99%. Тобто він потребує значного покращання для забезпечення ефективності системи інформаційної безпеки на фактичному рівні. Дана ситуація обумовлюється кризою політичної влади та наявністю військового конфлікту в країні. Оскільки вплив даного показника є досить вагомим, то першочерговим завданням для забезпечення ефективності конвергенції систем повинно бути саме урегулювання даної ситуації.

Що стосується максимального рівня, який може досягнути Україна, то на слайді можна побачити, що на даному етапі Україна досягла максимального рівня конвергенції. Не можливо покращити це значення за рахунок глобального рівня кібербезпеки (12,8%) та індексу політичної стабільності (86,3%). Це є цілком логічним, оскільки ті ризики, які на сьогодні сформовані в країні, мають значний вплив й на глобальне середовище. Відповідно така ситуація вимагає розробки спеціальних заходів кібербезпеки, а також налагодження політичної ситуації в країні.

Аналіз структурної ефективність вхідних показників для країн 5-го кластеру (рисунок 4.13) показав, що в даних країнах забезпечується поточний рівень конвергенції системи фінансового моніторингу та кібербезпеки та відбувається його перевищення на 4,7%. Ефективність досягається за такими показниками, як: мережевий індекс готовності (-27,41%), національний індекс кібербезпеки (-15,22%), індекс ефективності уряду (-3,75%); легкість ведення бізнесу (-5,4%); глобальний індекс тероризму (-2,89%). Тобто країни даного кластеру мають потенціал розвитку національної системи кібербезпеки, а також можливості до впровадження сучасних інформаційних технологій, що необхідно для забезпечення відповідного рівня конвергенції систем. Також сформовані умови, сприятливі для ведення бізнесу. Рівень конвергенції країн цього кластеру є нижчим у порівнянні з країнами попередніх кластерів. Отриманий результат свідчить тільки про невеликі позитивні кроки, необхідні для конвергенції систем.

Проаналізуємо структурну ефективність вихідних показників для країн 5-го кластеру (рисунок 4.14).

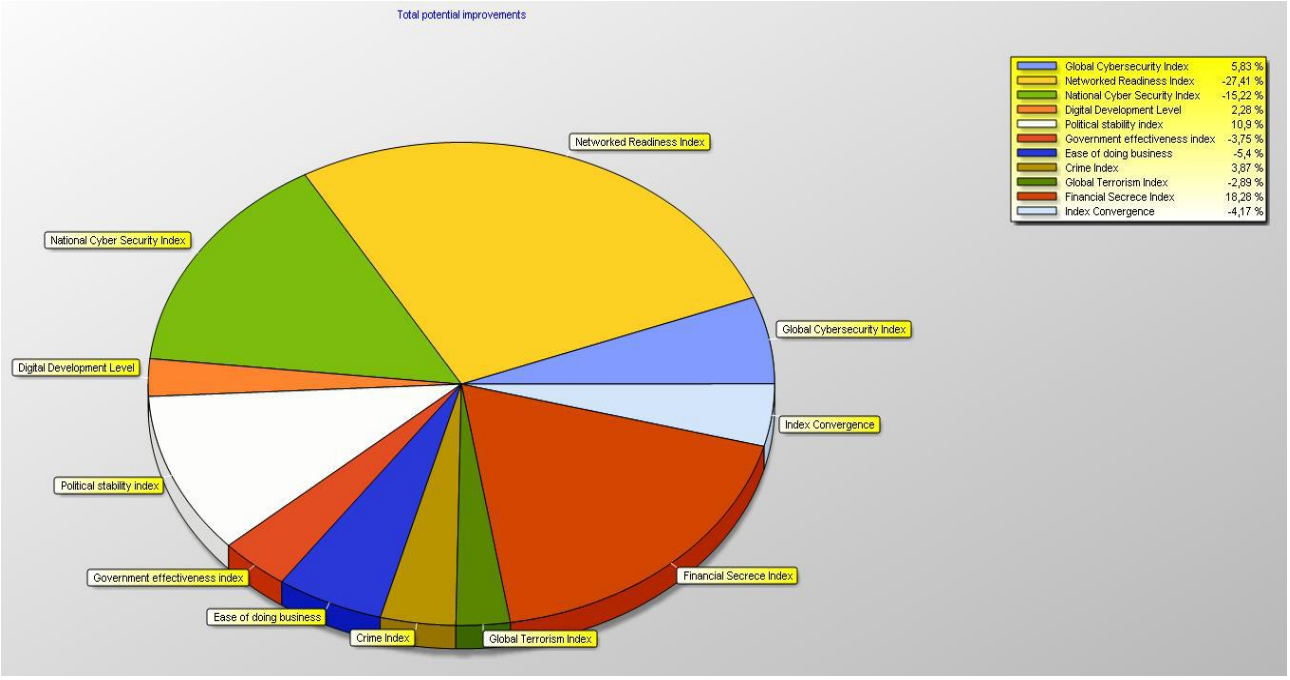

Рисунок 4.13 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 5-го кластеру (за Input-oriented CCR-моделлю)

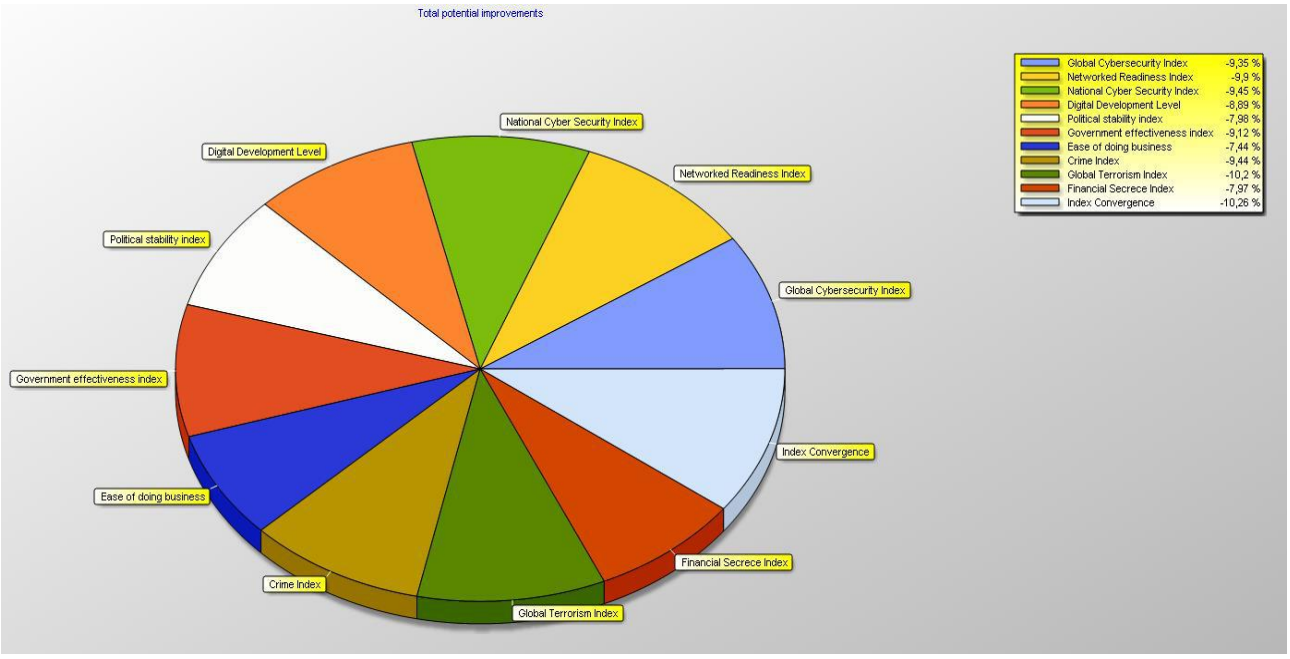

Рисунок 4.14 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 5-го кластеру (за Output-oriented CCR-моделлю)

Результати Output-oriented CCR-model (рис. 4.14) показують, що максимальне зростання індексу конвергенції системи фінансового моніторингу та кібербезпеки можливе на 10,26%. Це можливо забезпечити за рахунок резервів за всіма показниками. Оскільки фактичний рівень конвергенції забезпечується та спостерігається його перевищення, то країни 5-го кластеру також мають потенціал для ефективної інтеграції двох систем.

Шостий кластер сформували тільки 4 країни із найнижчим рівнем конвергенції систем. Аналіз структурної ефективність їх вхідних показників для (рисунок 4.15) показав, що в даних країнах забезпечується поточний рівень конвергенції системи фінансового моніторингу та кібербезпеки. Ефективність досягається за такими показниками, як: мережевий індекс готовності (-0,14%), національний індекс кібербезпеки (-0,36%), рівень цифровізації (-0,35%), індекс ефективності уряду (-0,24%), індекс фінансової таємниці (-0,13%). Тобто країни даного кластеру можуть мати певний успіх в розвитку, який буде досягатися шляхом системної інтеграції системи фінансового моніторингу і кібербезпеки. Але значна проблема, пов’язана з тероризмом та забезпеченням глобального рівня кібербезпеки сигналізує про необхідність прийняття чітких заходів на рівні держави щодо усунення цих питань або зменшення їх впливів.

Проаналізуємо структурну ефективність вихідних показників для країн 6-го кластеру (рисунок 4.16). Результати Output-oriented CCR-model показують, що максимальне зростання індексу конвергенції системи фінансового моніторингу та кібербезпеки можливе на 8,66%. Це можливо забезпечити за рахунок резервів за всіма показниками. Тобто для країн даного кластеру є можливості розвитку за рахунок підвищення ефективності від конвергенції систем протидії фінансовим злочинам та кібершахрайствам.

Питання підвищення ефективності системи національної безпеки у частині конвергенції систем фінансового моніторингу і кібербезпеки є досить актуальним, що пов’язано із зростанням рівня інформатизації, цифровізації та комп’ютеризації суспільства.

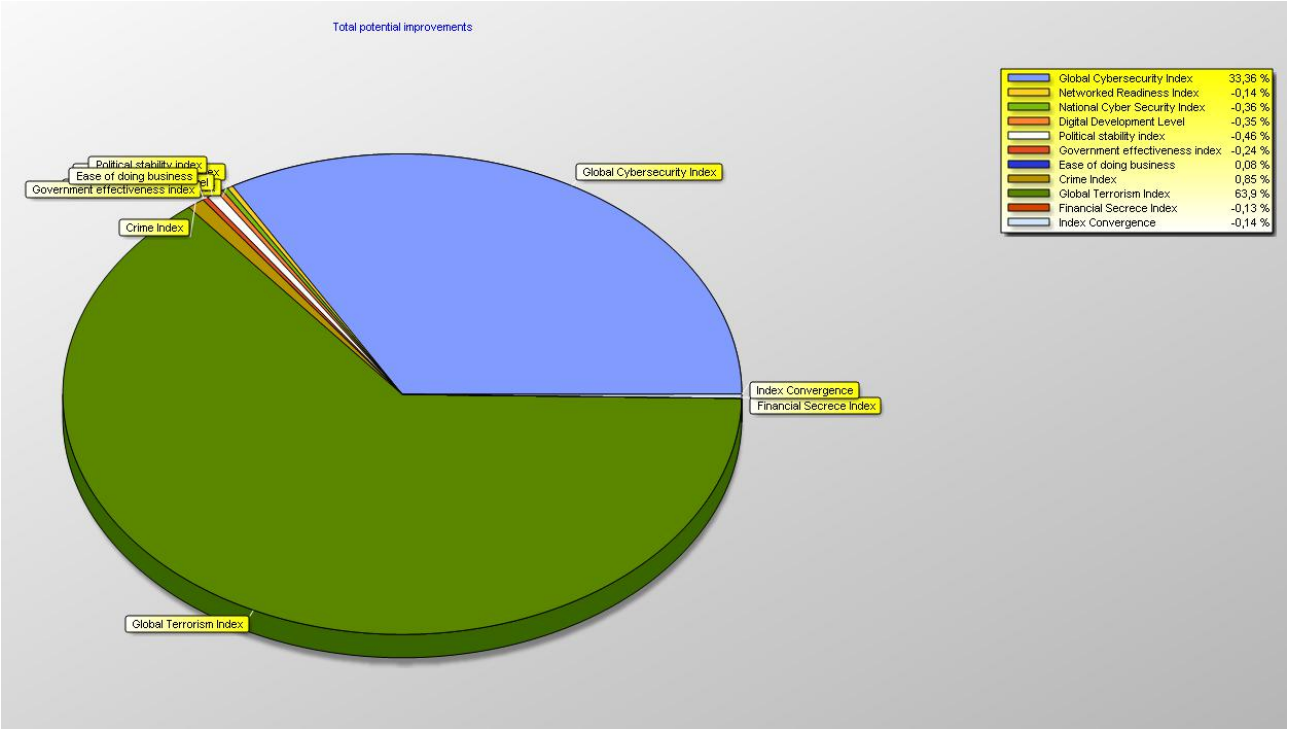

Рисунок 4.15 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 6-го кластеру (за Input-oriented CCR-моделлю)

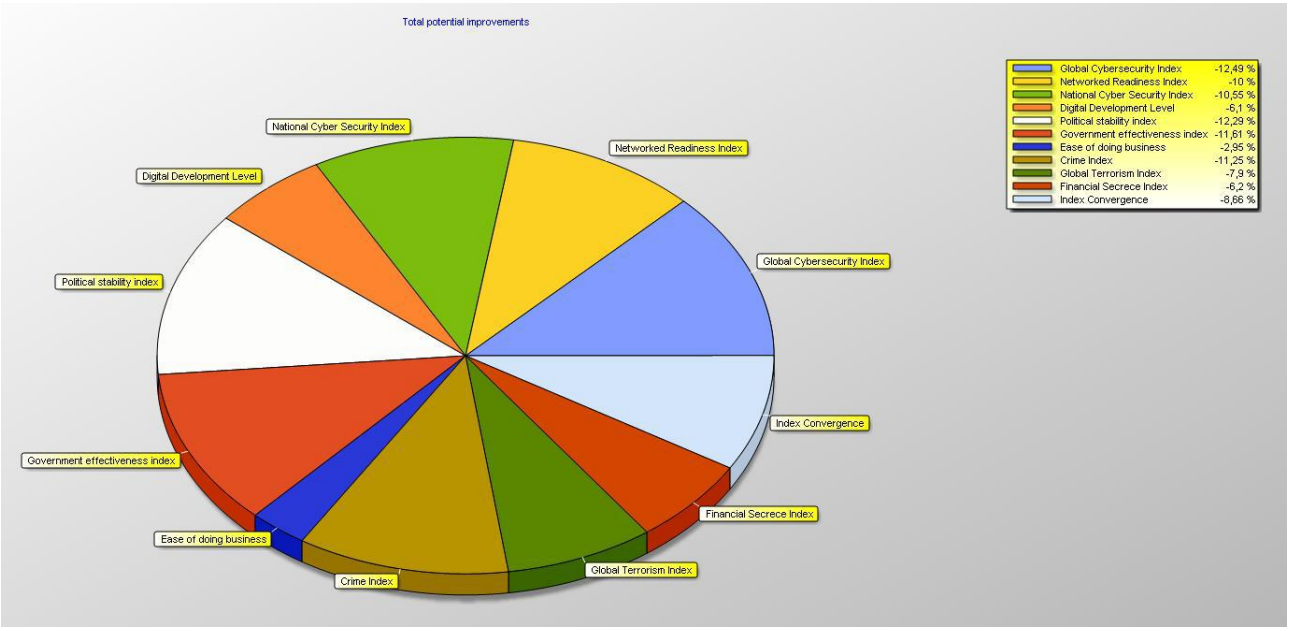

Рисунок 4.16 – Результати ефективності за складовими конвергенції системи фінансового моніторингу та кібербезпеки країн 6-го кластеру (за Output-oriented CCR-моделлю)

Застосування Data Envelopment Analysis у даному дослідженні дозволило визначити ефективність таких процесів. Використана модель CCR надала можливість проаналізувати структурну ефективність показників, що характеризують рівень розвитку системи кіберзахисту та протидії легалізації кримінальних доходів. Також дана модель дозволили оцінити максимальний рівень його зростання за наявного ресурсного потенціалу країни. Модель CCR є більш обмежуючою, ніж BCC, для визначення ефективності, що сприяло формуванню більш критичної оцінки щодо існуючих резервів країн, необхідних для забезпечення інтеграційних процесів. Саме тому вона була використана для проведення аналізу усіх кластерів країн.

Розділ 4 було виконано із використанням матеріалів публікацій виконавців [54].

ВИСНОВКИ

Представлені у першому розділі наукові результати створюють передумови оцінювання зрілості діючої системи протидії фінансовим та кібер-шахрайствам, а також для побудови фазових портретів їх «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості». Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити наступні:

- проведений аналіз та характеристика поняття, цілей, задач, напрямів та моделей конвергенції систем фінансового моніторингу і кібербезпеки дозволив сформувати фундаментальне підґрунтя для досліджуваної проблеми. В результат встановлено, що поглиблені дослідження вектору фінансового моніторингу та вектору кібербезпеки дозволять зорієнтувати дослідження на створення комплексних заходів, пов’язаних із інтеграцією систем кібербезпеки та фінансового моніторингу на основі узагальнення, структурування теоретичних надбань світової та вітчизняної літератури;
- проведене оцінювання умов, сформованих в різних країнах світу, які характеризують поточний рівень їх кібербезпеки та фінансового моніторингу, дозволив провести попередній аналіз процесу конвергенції систем фінансового моніторингу і кібербезпеки. Результати статистичного аналізу дозволили виявити неоднорідність ряду показників, що обумовлено нерівномірністю розвитку країн в напрямку забезпечення ефективної системи кіберзахисту та фінансового моніторингу. Результати канонічного аналізу дозволили встановити, що між групами обраних показників існує тісний зв'язок, при цьому рівень кібербезпеки виступає наслідком, а рівень фінансового моніторингу – причиною. Результати кореляційного аналізу дозволили провести оптимізацію даних та виключити із дослідження такі показники, як індекс розвитку інформаційно-комунікаційних технологій та індекс сприйняття корупції;

- на основі біфуркаційного аналізу побудовані фазові портрети «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» діючої системи протидії фінансовим та кібершахрайствам. Це дозволило побудувати інтегральний індекс конвергенції систем на основі методу згортки Сундаровського; ідентифікувати релевантні предиктори впливу на інтегральний індекс кібербезпеки за допомогою методу сигма-обмеженої параметризації та Парето-оптимізації; побудувати залежності інтегрального індексу кібербезпеки від релевантних предикторів на основі нелінійної регресії з покроковим виключенням; провести біфуркаційний аналіз зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазові портрети її «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості»; довести доцільність опису динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, за допомогою фазового портрету типу «нестійкий фокус» та «нестійкий вузол» в залежності від розглянутої проекції в розрізі «зрілості» та «релаксаційних коливань втрати стійкості».

Представлені у другому розділі наукові результати створюють передумови визначення ключових алгоритмів систем фінансового моніторингу та кібербезпеки. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

- розроблено ключові алгоритми систем фінансового моніторингу та кібербезпеки в розрізі ідентифікації та верифікації клієнта, моніторингу транзакцій, реакції на спробу-злочин, перевірки дій інсайдерів на ознаки кібершахрайств. Запропонований підхід дозволив провести моделювання існуючих процесів захисту інформації; здійснити симуляційні експерименти залежно від витрат часу та ресурсів при здійсненні окремої операції та виявлення на цій основі «вузьких» місць; провести моделювання процесів захисту інформації з урахуванням проведених оптимізаційних процедур та ліквідації виявлених недоліків; здійснити повторні симуляційні експерименти із метою підтвердження ефективності внесених змін до системи захисту інформації;

- розроблено математичне забезпечення алгоритмів виявлення кібершахрайських операцій з кредитними картками як найбільш поширених видів кіберзагроз. Це дозволило побудувати із застосуванням інтелектуального аналізу логістичну регресію, дерево рішень та нейронну мережу, які можна використовувати як універсальні інструменти для виявлення кібершахрайських операцій.

Представлені у третьому розділі наукові результати створюють передумови розробки можливих сценаріїв взаємодії систем кібербезпеки та протидії фінансовим злочинам. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

- із використанням методу визначення центра мас розроблено чотириполюсні барицентричні моделі збалансованого розвитку національної економіки, що інтегрують композитні індикатори економічного, соціального й політичного розвитку країни, а також рівня її протидії фінансовим шахрайствам та кібербезпеки. Це дозволило провести розрахунки моделей з урахуванням трьох компонентів: значень композиційних цілей (як середнє геометричне), рівня парного балансу (як суми протилежних пар чотирикутних кутів) та всіх чотирьох цілей (як відстань між фактичним і нормативним значенням центру мас). За результатами аналізу було виявлено країни з найбільш ефективними таргетами, країни з дисбалансом цільових пар, а також розподіл країн за аналізом відстаней центрів мас;
- проведено 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. Це дозволило визначити сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку в залежності від інтегрального рівня кібербезпеки, інтегрального рівня протидії легалізації кримінальних доходів, загального рівня конвергенції.

Представлені у четвертому розділі наукові результати створюють передумови оцінки синергетичного ефекту від конвергенції моделей фінансового моніторингу та кібербезпеки. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

- розроблена методика оцінювання ефекту від конвергенції систем фінансового моніторингу та кібербезпеки з урахуванням потенційних зон вразливості та аберацій в інтеграційній моделі на основі методу лінійного непараметричного програмування DEA. Практичне запровадження такої моделі надасть можливість провести аналіз ефективності процесу конвергенції систем фінансового моніторингу і кібербезпеки для різних кластерів країн, побудувати візуалізацію результатів ефективності, визначити слабкі та сильні сторони системи за умови формування резервів наявних ресурсів, а також досягнення максимально можливого ефекту від здійснення інтеграційних процесів системи протидії фінансовим кібершахрайствам і кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Morse J.C. Blacklists, market enforcement, and the global regime to combat terrorist financing. *International Organization*. 2019, № 73 (3). P. 511—545.

2. Radygin V. Y., Kupriyanov D. Y., Bessonov R. A., Ivanov M. N., Osliakova, I. V. Application of text mining technologies in russian language for solving the problems of primary financial monitoring. In the *Procedia Computer Science*. 2021, № 190. P. 678-683. DOI: https://doi.org/10.1016/j.procs.2021.06.078

3. Yashina N. I., Kashina O. I., Pronchatova-Rubtsova N. N., Yashin S. N., Kuznetsov V. P. (2021). *Financial monitoring of financial stability and digitalization in federal districts*. 2021, № 155. P. 1045-1051. DOI: https://doi.org/10.1007/978-3-030-59126-7_115.

4. Грабчук О., Супрунова І. Фінансовий моніторинг як умова забезпечення державної безпеки країни: поняття, складові, етапи розвитку. *Аспекти публічного управління*. 2020, № 8(4). С. 75–83. DOI: https://doi.org/10.15421/152082.

5. Першин В. Г. Роль фінансового моніторингу в межах протидії легалізації доходів, одержаних злочинним шляхом. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2019, № 4(88), С. 250-257. DOI: https://doi.org/10.33766/2524-0323.88.250-257.

6. Рисін В. В., Степанова А. В. Інструменти протидії фінансуванню тероризму з використанням фінансових установ. *Економіка та держава*. 2020, № 6. С. 80–86. DOI: https://doi.org/10.32702/2306-6806.2020.6.80.

7. Shackelford S., Dockery R., Prabhakar B., Raymond A. Cybersecurity in crisis. *Business Horizons*. 2021, № 64(6). P. 725-727. DOI: https://doi.org/10.1016/j.bushor.2021.07.003

8. Uchendu B., Nurse J. R. C., Bada M., Furnell S. Developing a cyber security culture: Current practices and future needs. *Computers and Security*. 2021, № 109. DOI: https://doi.org/10.1016/j.cose.2021.102387.

9. Han C.-H., Han C. Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis. *Process Safety and Environmental Protection.* 2021, № 155. P. 306-316. DOI: https://doi.org/10.1016/j.psep.2021.09.028.

10. Mokhor V., Honchar S., Onyskova A. Cybersecurity risk assessment of information systems of critical infrastructure objects. In the *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 – Proceedings.* 2021. P. 19-22. DOI: https://doi.org/10.1109/PICST51311.2020.9467957.

11. Gimenez-Aguilar M., de Fuentes J. M., Gonzalez-Manzano L., Arroyo D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems.* 2021, № 124. P. 91-118. DOI: https://doi.org/10.1016/j.future.2021.05.007

12. Repetto M., Striccoli D., Piro G., Carrega A., Boggia G., Bolla, R. An autonomous cybersecurity framework for next-generation digital service chains. *Journal of Network and Systems Management.* 2021, № 29(4). Article number: 37. DOI: https://doi.org/10.1007/s10922-021-09607-7

13. Madeira P. M., Vale M., Mora-Aliseda J. Smart specialisation strategies and regional convergence: Spanish extremadura after a period of divergence. *Economies.* 2021, № 9(4). DOI: https://doi.org/10.3390/economies9040138

14. Ibrahim A. E. A., Elamer A. A., Ezat A. N. The convergence of big data and accounting: Innovative research opportunities. *Technological Forecasting and Social Change.* 2021, № 173. DOI: https://doi.org/10.1016/j.techfore.2021.121171

15. Dong F., Li Y., Qin C., Sun J. How industrial convergence affects regional green development efficiency: A spatial conditional process analysis. *Journal of Environmental Management.* 2021, № 300. DOI: https://doi.org/10.1016/j.jenvman.2021.113738

16. Guilbeault D., Baronchelli A., Centola D. Experimental evidence for scale-induced category convergence across populations. *Nature Communications.* 2021, № 12(1). DOI: https://doi.org/10.1038/s41467-020-20037-y

17. Закон України № 361-IX від 16.08.2020 «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.

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

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

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

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

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

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

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

25. 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.

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

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

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

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

30. 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.

31. 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.

32. Augustinos T.P. Developing cybersecurity requirements in banking (And Other financial services). *Banking Law Journal*. 2018, № 135(3). P. 155–159.

33. 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: 10.32782/2524-0072/2021-32-3.

34. Trend Report «Financial Cyber Threats Q1 2017». *ElevenPaths* : website. URL: https://www.elevenpaths.com/wp-content/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

35. Статистика платежного мошенничества — итоги 2017-го года (ИНФОГРАФИКА). *Украинская межбанковская ассоциация членов платежных систем ЕМА* : вебсайт. URL: https://ema.com.ua/cyberfraud-ema-statistics-results-2017/.

36. Постанова НБУ № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28.09.2017. *Верховна Рада України* : офіційний вебсайт. URL: http://zakon3.rada.gov.ua/laws/show/v0095500-17.

37. SAS Fraud Management. *SAS* : website. URL: https://www.sas.com/en_us/software/fraud-management.html.

38. Unuchek R., Sinitsyn F., Parinov D., Liskin A. IT threat evolution Q3 2017. *Statistics* : The official website of the company “AO Kaspersky Lab”. URL: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/.

39. Глинников Н. Оптимизация нагрузки создаваемой сайтом на виртуальном хостинге. *ActiveCloud* : вебсайт. URL: https://my.activecloud.com/ru/index.php?/Knowledgebase/Article/View/317/36/optimizcija-ngruzki-sozdvemojj-sjjtom-n-virtulnom-khostinge.

40. Актуальные киберугрозы: IV квартал 2019 года. *Positive Technologies* : вебсайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q4/#id7.

41. Постанова НБУ №65 «Про затвердження Положення про здійснення банками фінансового моніторингу» від 19.05.2020. *Верховна Рада України* : офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/v0065500-20#Text.

42. 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.

43. 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.

44. Umadevi P., Divya, E. Money laundering detection using TFA system. In the *International Conference on Software Engineering and Mobile Application Modelling and Development* (ICSEMA 2012). Chennai, India. 2012. P. 1-8. DOI: https://doi.org/10.1049/ic.2012.0150.

45. Caldera J., Hain J., Sherlock K. Enhanced automated anti-fraud and anti-money-laundering payment system: patent US20160071108A1 United States. Filed 04.09.2015, pub. date 10.03.2016. URL: https://patentimages.storage.googleapis.com/a7/34/0c/64cca0829ed4ea/US20160071108A1.pdf.

46. Kolhatkar J., Fatnani S., Yao Yi., Matsumoto K. Multi-channel data driven, real-time anti-money laundering system for electronic payment cards: patent US8751399B2. United States. Filed 15.07.2012, pub. date 10.06.2014. URL: https://patentimages.storage.googleapis.com/20/52/22/4f12c57929b368/US8751399.pdf.

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

48. Coelho R., De Simoni M., Prenio J Suptech applications for anti-money laundering. *FSI Insights on policy implementation*. 2019, № 18. P. 1-18. URL: https://www.bis.org/fsi/publ/insights18.pdf.

49. Yong Li. Implementation of Anti-Money Laundering Information Systems. *AuthorHouse*. 2016. P. 188.

50. Uncover the True Cost of Anti-Money Laundering & KYC Compliance. *LexisNexis* : website. URL: https://www.lexisnexis.com/risk/intl/en/resources/research/true-cost-of-aml-compliance-apac-survey-report.pdf.

51. AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2. *The company CA* : website. URL: https://supportcontent.ca.com/cadocs/0/e002761e.pdf.

52. Bernard J., Nicholson M. Reshaping the cybersecurity landscape. How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. *Deloitte* : website. URL: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

53. Средняя зарплата по категории «Финансы, банк» в Украине. *Work.ua* : вебсайт. URL: https://www.work.ua/ru/salary-banking-finance/.

54. Яровенко Г.М. Інформаційна безпека як драйвер розвитку національної економіки : дис. ... д-ра екон. наук : 08.00.03. Суми, 2021. С. 590. URL: https://essuir.sumdu.edu.ua/handle/123456789/83664.

55. How victims' information is misused. *Insurance Information Institute* : website. URL: https://www.iii.org/table-archive/20279.

56. Zheng L., Liu G., Yan C., Jiang C. Transaction fraud detection based on total order relation and behavior diversity. *IEEE Transactions on Computational Social Systems*. 2018, № 5(3). P. 796–806. DOI: https://doi.org/10.1109/TCSS.2018.2856910.

57. Prisha P., Neo H.-F., Ong T.-S., Teo C.-C. E-Commerce security and identity integrity: The future of virtual shopping. *Advanced Science Letters*. 2017, № 23(8). P. 7849–7852. DOI: https://doi.org/10.1166/asl.2017.9592.

58. Dileep M.R., Navaneeth A.V., Abhishek M. A novel approach for credit card fraud detection using decision tree and random forest algorithms. In *the 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.

59. Cui Y., Song Z., Hu J. Research on credit card fraud classification based on GA-SVM. In *the Proceedings - 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2021*. 2021. P. 1076–1080. DOI: https://doi.org/10.1109/AEMCSE51986.2021.00220.

60. Wang R., Liu G. Ensemble Method for Credit Card Fraud Detection. In *the Proceedings - 2021 4th International Conference on Intelligent Autonomous*

Systems, ICoIAS 2021. 2021. P. 246–252. DOI: https://doi.org/10.1109/ICoIAS53694.2021.00051.

61. Sobanadevi V., Ravi G. Handling data imbalance using a heterogeneous bagging-based stacked ensemble (hbse) for credit card fraud detection. *Advances in Intelligent Systems and Computing*. 2021, № 1167. P. 517–525. DOI: https://doi.org/10.1007/978-981-15-5285-4_51.

62. 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.

63. 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.

64. Rachavelias M.G. Online financial crimes and fraud committed with electronic means of payment – a general approach and case studies in Greece. *ERA Forum.* 2019, № 19(3). P. 339–355. DOI: https://doi.org/10.1007/s12027-018-0519-2.

65. Sadgali I., Sael N., Benabbou F. Human behavior scoring in credit card fraud detection. *IAES International Journal of Artificial Intelligence.* 2021, № 10(3). P. 698–706. DOI: https://doi.org/10.11591/IJAI.V10.I3.PP698-706.

66. Zou H. Analysis of Best Sampling Strategy in Credit Card Fraud Detection Using Machine Learning. In *ACM International Conference Proceeding Series*. 2021. P. 40–44. DOI: https://doi.org/10.1145/3460179.3460186.

67. 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.

68. Gianotti E., Damião da Silva E. Strategic management of credit card fraud: stakeholder mapping of a card issuer. *Journal of Financial Crime*. 2021, № 28(1). P. 156–169. DOI: https://doi.org/10.1108/JFC-06-2020-0121.

69. Zou W., Straub D., Vance A., Yan J. The differential role of alternative data in SME-focused fintech lending. In *International Conference on Information*

Systems, ICIS 2020 - Making Digital Inclusive: Blending the Local and the Global, *ICIS*. 2021. Code 167844.

70. Jing R., Tian H., Zhou G., Zhang X., Zheng X., Zeng D.D. A GNN-based few-shot learning model on the credit card fraud detection. In *Proceedings 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence, DTPI 2021*. 2021. P. 320–323. DOI: https://doi.org/10.1109/DTPI52967.2021.9540093.

71. Ouedraogo A.-F., Heuchenne C., Nguyen Q.-T., Tran H. Data-Driven Approach for Credit Card Fraud Detection with Autoencoder and One-Class Classification Techniques. *IFIP Advances in Information and Communication Technology*. 2021, № 630 IFIP. P. 31–38. DOI: https://doi.org/10.1007/978-3-030-85874-2_4.

72. Обґрунтування господарських рішень та оцінка ризиків : навчальний посібник / М. Д. Балджи та ін. Одеса : ОНЕУ, 2013. 670 с.

73. Яровенко Г.М., Радько В.В. Оцінка ймовірності виникнення шахрайства в процесі кредитування клієнтів банку. *Вісник Сумського державного університету. Серія Економіка*. 2021, № 3. С. 151−161. DOI: https://doi.org/10.21272/1817-9215.2021.3-17

74. Kendiukhov I., Tvaronaviciene M. Managing innovations in sustainable economic growth. *Marketing and Management of Innovations*. 2017, № 3. P. 33-42. DOI: https://doi.org/10.21272/mmi.2017.3-03.

75. Lyulyov O., Lyeonov S., Tiutiunyk I., Podgórska J. The impact of tax gap on macroeconomic stability: Assessment using panel VEC approach. *Journal of International Studies*. 2021, № 14(1). P. 139-152. DOI: https://doi.org/10.14254/2071-8330.2021/14-1/10.

76. Brychko M., Bilan Y., Lyeonov S., Mentel G. Trust crisis in the financial sector and macroeconomic stability: A structural equation modelling approach. *Economic Research-Ekonomska Istrazivanja*. 2021, № 34(1). P. 828-855. DOI: https://doi.org/10.1080/1331677X.2020.1804970.

77. Melnyk L., Sineviciene L., Lyulyov O., Pimonenko T., Dehtyarova I. Fiscal decentralization and macroeconomic stability: The experience of Ukraine's

economy. *Problems and Perspectives in Management*. 2018, № 16(1). P. 105-114. DOI: https://doi.org/10.21511/ppm.16(1).2018.10.

78. Chigrin O., Pimonenk, T. The ways of corporate sector firms financing for sustainability of performance. *International Journal of Ecology and Development*. 2014, № 29(3). P. 1-13. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-84904394388&origin=resultslist.

79. Brychko M. Governance of stakeholder's financial relationships: Evidence fom ukrainian banking sector. *Corporate Ownership and Control*. 2013, № 11(1). P. 706-714. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85027024173&origin=resultslist.

80. Kobushko I., Tiutiunyk I., Kobushko I., Starinskyi M., Zavalna Z. The triadic approach to cash management: Communication, advocacy, and legal aspects. *Estudios De Economia Aplicada*. 2021, № 39(7). DOI: https://doi.org/10.25115/eea.v39i7.5071.

81. Vysochyna A., Kryklii O., Minchenko M., Aliyeva A. A., Demchuk K. Country innovative development: impact of shadow economy. *Marketing and Management of Innovations*. 2020, № 4. P. 41-49. DOI: https://doi.org/10.21272/mmi.2020.4-03.

82. Leonov S., Frolov S., Plastun V. Potential of institutional investors and stock market development as an alternative to households' savings allocation in banks. *Economic Annals-XXI*. 2014, № 11-12. P. 65-68. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-84928552512&origin=resultslist.

83. Hrytsenko L. L. Rationale for priority sources of investment support of the national economy of Ukraine. *Actual Problems of Economics*. 2014, № 159(9). P. 84-91. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-84917678385&origin=resultslist.

84. Dave H. An Inquiry on Social Issues – Part 2. *Business Ethics and Leadership*. 2017, № 1(3). P. 45-63. DOI: https://doi.org/10.21272/bel.1(3).45-63.2017.

85. Didenko I., Paucz-Olszewska J., Lyeonov S., Ostrowska-Dankiewicz A., Ciekanowski Z. Social safety and behavioral aspects of populations financial inclusion: A multicountry analysis. *Journal of International Studies*. 2020, № 13(2). P. 347-359. DOI: https://doi.org/10.14254/2071-8330.2020/13-2/23.

86. Bagmet K.V., Haponova O. Assessing the Impact on Social Sector: A Macroeconomic Approach. *SocioEconomic Challenges*. 2018, № 3(2). P. 103-108. DOI: https://doi.org/10.21272/sec.3(2).103-108.2018.

87. Lyeonov S., Liuta O. Actual problems of finance teaching in Ukraine in the post-crisis period. *The financial crisis: Implications for research and teaching*. 2016. P. 145-152. DOI: https://doi.org/10.1007/978-3-319-20588-5_07.

88. Samoilikova A., Kunev R. The impact of health care financing on the economic growth: EU countries analysis. *Health Economics and Management Review*. 2020, № 1(2). P. 24-32. DOI: https://doi.org/10.21272/hem.2020.2-03.

89. Sineviciene L., Shkarupa O., Sysoyeva L. Socio-economic and Political Channels for Promoting Innovation as a Basis for Increasing the Economic Security of the State: Comparison of Ukraine and the Countries of the European Union. *SocioEconomic Challenges*. 2018, № 2(2). P. 81-93. DOI: https://doi.org/10.21272/sec.2(2).81-93.2018.

90. Lyeonov S., Pimonenko T., Bilan Y., Štreimikiene D., Mentel G. Assessment of green investments' impact on sustainable development: Linking gross domestic product per capita, greenhouse gas emissions and renewable energy. *Energies*. 2019, № 12(20). DOI: https://doi.org/10.3390/en12203891.

91. Vasylieva T., Lyulyov O., Bilan Y., Streimikiene D. Sustainable economic development and greenhouse gas emissions: The dynamic impact of renewable energy consumption, GDP, and corruption. *Energies*. 2019, № 12(17). DOI: https://doi.org/10.3390/en12173289.

92. Lyulyov O., Pimonenko T., Kwilinski A., Dzwigol H., Dzwigol-Barosz M., Pavlyk V., Barosz P. The impact of the government policy on the energy efficient gap: The evidence from ukraine. *Energies*. 2021, № 14(2). 373. DOI: https://doi.org/10.3390/en14020373.

93. Vysochyna A., Samusevych Y., Starchenko L. Convergence trends of environmental taxation in European countries. In *the E3S Web of Conferences*. 2020, 202. DOI: https://doi.org/10.1051/e3sconf/202020203031.

94. Novikov V. Bibliometric Analysis of Economic, Social and Information Security Research. *SocioEconomic Challenges*. 2021, № 5(2). P. 120-128. DOI: https://doi.org/10.21272/sec.5(2).120-128.2021.

95. Yarovenko H., Bilan Y., Lyeonov S., Mentel G. Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management*. 2021, № 22(2). P. 369-387. DOI: https://doi.org/10.3846/jbem.2021.13925.

96. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. In *the CEUR Workshop Proceedings*. 2019, 2422. P. 297-307. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85071081226&origin=resultslist.

97. Kozmenko O., Kuzmenko O. The modelling of equilibrium of the reinsurance markets in Germany, France and Ukraine: Comparative characteristics. *Investment Management and Financial Innovations*. 2011, № 8(2). P. 8-16. DOI: https://doi.org/10.21511/imfi.8(2).2011.01.

98. Samusevych Y., Maroušek J., Kuzmenko O., Streimikis J., Vysochyna A. Environmental taxes in ensuring national security: A structural optimization model. *Journal of International Studies*. 2021, № 14(2). P. 292-312. DOI: https://doi.org/10.14254/2071-8330.2021/14-2/19.

99. Kuzmenko O., Šuleř P., Lyeonov S., Judrupa I., Boiko A. Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions. *Journal of International Studies*. 2020, № 13(3). P. 332-339. DOI: https://doi.org/10.14254/2071-8330.2020/13-3/22.

100. Lyeonov S., Żurakowska-Sawa J., Kuzmenko O., Koibichuk V. Gravitational and intellectual data analysis to assess the money laundering risk of

financial institutions. *Journal of International Studies*. 2020, № 13(4). P. 259-272. DOI: https://doi.org/10.14254/2071-8330.2020/13-4/18.

101. Boyko A., Roienko V. Risk assessment of using insurance companies in suspicious transactions. *Economic Annals-XXI*. 2014, № 11-12. P. 73-76. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-84928553132&origin=resultslist.

102. Levchenko V., Kobzieva T., Boiko A., Shlapko T. Innovations in Assessing the Efficiency of the Instruments for the National Economy De-Shadowing: the State Management Aspect. *Marketing and Management of Innovations*. 2018, № 4. P. 361-371. DOI: https://doi.org/10.21272/mmi.2018.4-31.

103. Aljaloudi J. A., Warrad T.A. Economic Growth and the Optimal Size of the Public sector in Jordan. *Financial Markets, Institutions and Risks*. 2020, № 4(3). P. 72-79. DOI: https://doi.org/10.21272/fmir.4(3).72-79.2020.

104. Esmanov O., Dunne P. Prior to the Financial Security through Control over the Use of Public Funds, Assessment Methodology and Practical Experience in Ukraine. *Financial Markets, Institutions and Risks*. 2017, № 1(3). P. 65-74. DOI: https://doi.org/10.21272/fmir.1(3).65-74.2017.

105. Kozmenko O., Merenkova O., Boyko A. The analysis of insurance market structure and dynamics in Ukraine, Russia and European Insurance and Reinsurance Federation (CEA) member states. *Problems and Perspectives in Management*. 2009, № 7(1). P. 29-39. URL: https://www.businessperspectives.org/index.php/journals/problems-and-perspectives-in-management/issue-24/the-analysis-of-insurance-market-structure-and-dynamics-in-ukraine-russia-and-european-insurance-and-reinsurance-federation-cea-member-states.

106. Berzin P., Shyshkina O., Kuzmenko O., Yarovenko H. Innovations in the Risk Management of the Business Activity of Economic Agents. *Marketing and Management of Innovations*. 2018, №4. P. 221-233. DOI: https://doi.org/10.21272/mmi.2018.4-20.

107. Newly Industrialized Country (NIC). A subcategory of countries that are still developing but show greater economic growth. *Corporate Finance Institute* : website. URL: https://corporatefinanceinstitute.com/resources/knowledge/economics/newly-industrialized-country-nic/

108. O'Neill J., Wilson D., Purushothaman R., Stupnytska A. How Solid are the BRICs? *Global Economics Paper*. 2021, 134. URL: https://www.goldmansachs.com/insights/archive/archive-pdfs/how-solid.pdf.

109. International Monetary Fund. *World Economic Outlook. October 2018. Challenges to Steady Growth.* 2021. URL: https://www.imf.org/en/Publications/WEO/Issues/2019/08/30/World-Economic-Outlook-October-2018-Challenges-to-Steady-Growth-46081.

110. The United Nations. *LDCs at a Glance*. 2021. URL: https://www.un.org/development/desa/dpad/least-developed-country-category/ldcs-at-a-glance.html.

111. Васильєва Т.А., Яровенко Г.М. Свідоцтво про реєстрацію авторського права на твір №109664 від 22.11.2021 "Сбалансованість детермінант розвитку країн: барицентрична модель".

112. Відмивання грошей. *Anti-corruption walks Kyiv* : веб-сайт. URL: https://acwalks.com.ua/knowledgebase/vidmyvannia-hroshey/.

113. Morgan S. Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. *Cybersecurityventures* : website. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

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

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

116. Яровенко Г.М., Колотіліна О.В., Світлична А.О. Оцінка рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів.

Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм. 2021, № 14.

117. Charnes A., Cooper W.W., Rhodes E. Measuring the efficiency of decision making units. *European Journal of Operational Research*. 1978, № 2. P. 429-444.

118. Banker R.D., Charnes A., Cooper W.W. Some Models for Estimating Technical and Scale Inefficiencies in Data Envelopment Analysis. *Managment Science*. 1984, № 30(9). P. 1031-1142. DOI: https://doi.org/10.1287/mnsc.30.9.1078.

119. Frontier Analyst. *Banxia Software* : website. URL: https://banxia.com/frontier/resources/demodownload/

120. Litsman M., Yarovenko H. Statistical analysis and modeling of the process of detecting credit card fraud. In *The driving force of science and trends in its development: collection of scientific papers «SCIENTIA» with Proceedings of the I International Scientific and Theoretical Conference* (Vol. 1), January 29, 2021. Coventry, United Kingdom: European Scientific Platform. P. 76-78.

121. Svitlychna A., Yarovenko H. Statistical analysis and forecasting of cyber attacks. In *The driving force of science and trends in its development: collection of scientific papers «SCIENTIA» with Proceedings of the I International Scientific and Theoretical Conference* (Vol. 3), January 29, 2021. Coventry, United Kingdom: European Scientific Platform. P. 17-19.

122. Bozhenko V.V., Yarovenko H.M. Drivers of cybercrime in the financial sphere. *Міжнародний науковий журнал «Грааль науки»*. 2021, № 8 : за матеріалами II Міжнародної науково-практичної конференції «An integrated approach to science modernization: methods, models and multidisciplinarity», що проводилася 24 вересня 2021 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ «International Centre Corporative Management» (Відень, Австрія). С. 49-51.

123. Кузьменко О.В., Яровенко Г.М. Ідентифікація причинно-наслідкових зв'язків між фінансовими транзакціями і фінансовими злочинами. *Міжнародний науковий журнал «Грааль науки»*. 2021, № 8 : за матеріалами II

Міжнародної науково-практичної конференції «An integrated approach to science modernization: methods, models and multidisciplinarity», що проводилася 24 вересня 2021 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ «International Centre Corporative Management» (Відень, Австрія). С. 51-54.

124. Яровенко Г.М., Боженко В.В. Конвергенція систем фінансового моніторингу та кібербезпеки. *Міжнародний науковий журнал «Грааль науки»*. 2021, № 8 : за матеріалами II Міжнародної науково-практичної конференції «An integrated approach to science modernization: methods, models and multidisciplinarity», що проводилася 24 вересня 2021 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ «International Centre Corporative Management» (Відень, Австрія). С. 205-208.

125. Кузьменко О.В., Доценко Т.В., Боженко В.В., Світлична А.О. Закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил. *Вісник СумДУ. Серія Економіка*. 2021, №1. С. 95-103.

126. Кузьменко О. В., Доценко Т.В., Миненко С.В., Шрамко Е.В. Взаємозалежність Fintech інновацій, фінансових, кібернетичних злочинів та легалізації кримінальних доходів за посередництва фінансових установ. *Вісник СумДУ. Серія Економіка*. 2021, №1. С.195-207.

127. Кузьменко О.В., Овчаренко В.О. Аналіз циклічності показників діяльності банківських установ в розрізі впровадження інноваційних технологій обслуговування клієнтів. *Вісник СумДУ. Серія Економіка*. 2021, №1. С. 179-187.

128. Kuzmenko O.V., Dotsenko T.V., Skrynka L.O. Economic and mathematical modelling of the effectiveness of the national system for combatting cyber fraud and legalisation of criminal proceeds based on survival analysis methods. *Scientific Bulletin of Mukachevo State University. Series "Economics".* 2021, №8(1). P. 144-153. DOI: https://doi.org/10.52566/msu-econ.8(1).2021.144-153

129. Bozhenko V. Enhancing business integrity as a mechanism for combating corruption and shadow schemes in the country. *Business Ethics and Leadership*. 2021. № 5(3). P.97-101.

130. Боженко В.В., Пігуль Є.І. Вплив цифровізації на розвиток фінансових технологій. *Вісник Хмельницького національного університету. Серія: економічні науки*. 2021, №2. С.11-15.

131. Боженко В.В., Кушнерьов О.С., Кільдей А.С. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум.* 2021, № 4. С. 166-121.

132. Pakhnenko O., Rubanov P., Hacar D., Yatsenko V., Vida I. Digitalization of financial services in European countries: Evaluation and comparative analysis. *Journal of International Studies*. 2021, № 14(2). P. 267-282. DOI: https://doi.org/10.14254/2071-8330.2021/14-2/17.

133. Dovbysh A., Shelechov I., Khibovska J., Matiash O. Information and Analytical System for Assessing the Compliance of Educational Content Specialties Ciber Security With Modern Requirements. *Radioelectronic and Computer Systems*. 2021, № 1. P. 70–80.

134. Vasilyeva T., Kuzmenko O., Kuryłowicz M., Letunovska N. Neural network modeling of the economic and social development trajectory transformation due to quarantine restrictions during COVID-19. *Economics and Sociology*. 2021, № 14(2). P. 313-330. DOI: https://doi.org/10.14254/2071-789X.2021/14-2/17.

135. Lyeonov S., Vasilyeva T., Bilan Y., Bagmet K. Convergence of the institutional quality of the social sector: The path to inclusive growth. International *Journal of Trade and Global Markets*. 2021, № 14(3). P. 272-291. DOI: https://doi.org/10.1504/IJTGM.2021.115712.

ДОДАТКИ

Додаток А

Результати симуляцій побудованих моделей бізнес-процесів конвергенції систем моніторингу і кібербезпеки

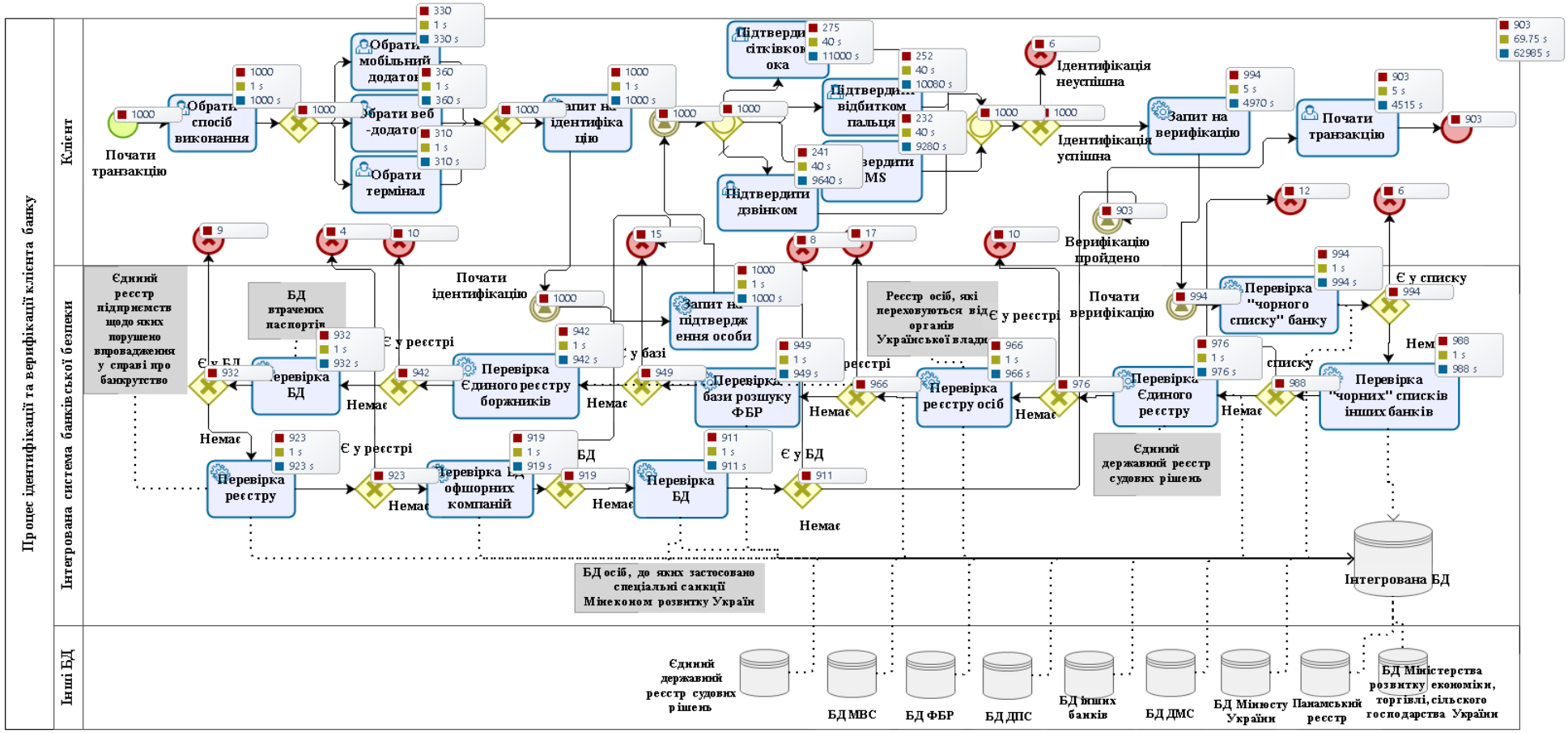

Рисунок А.1 – Результати симуляції за часом для бізнес-моделі процесу ідентифікації та верифікації клієнта

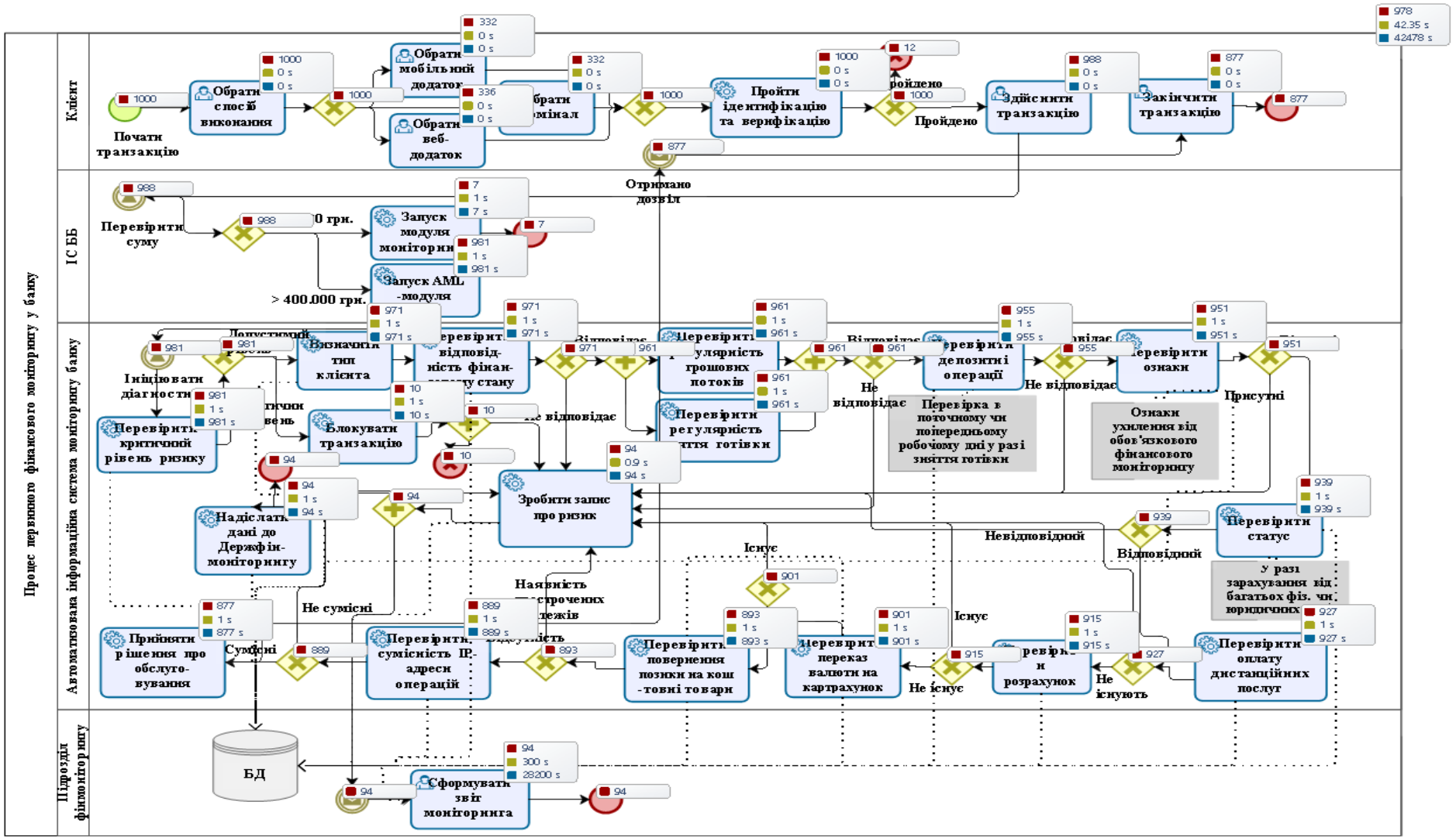

Рисунок А.2 – Результати симуляції за часом для бізнес-моделі процесу автоматизованого фінансового моніторингу

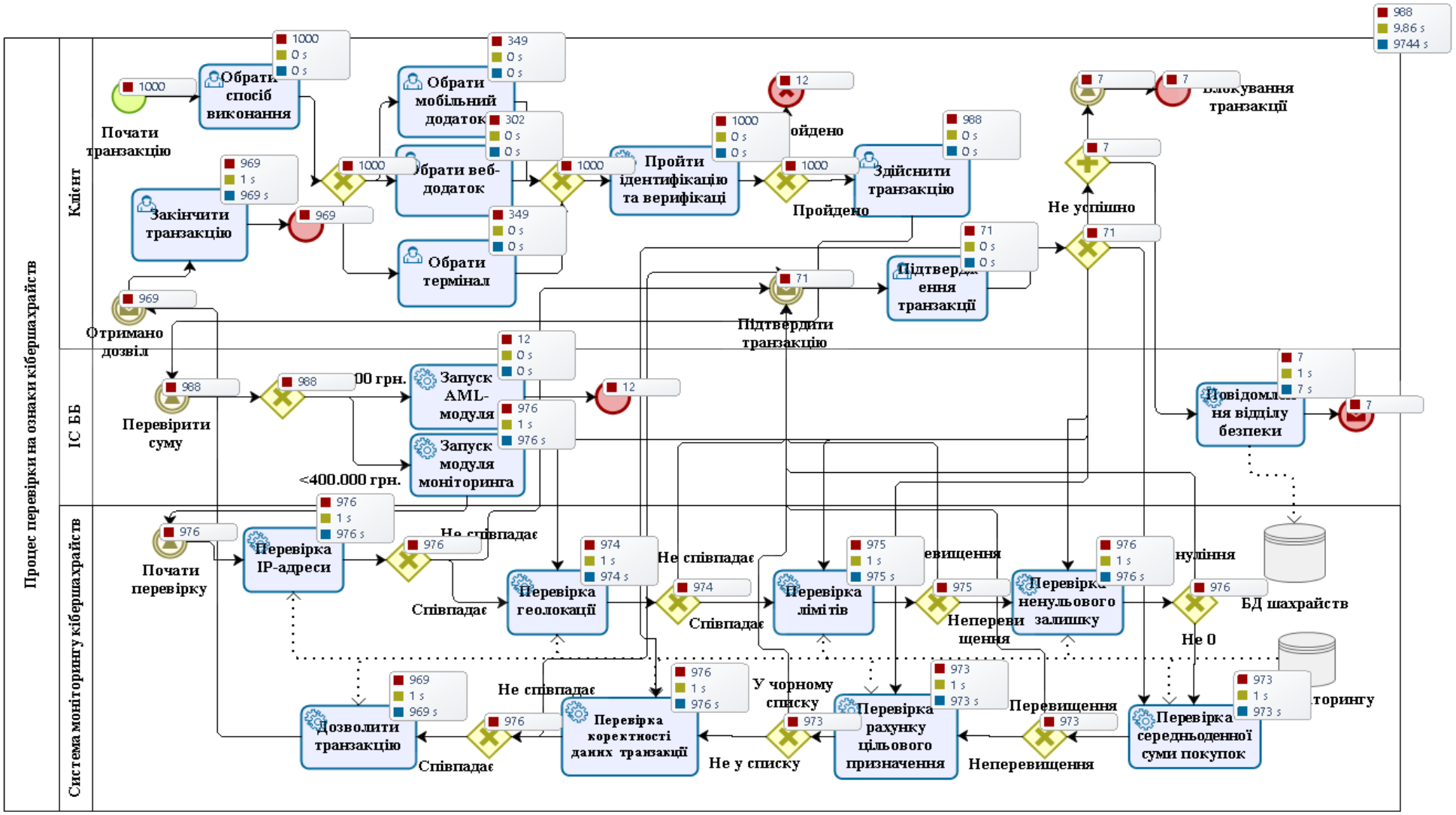

Рисунок А.3 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки зовнішніх кібершахрайств

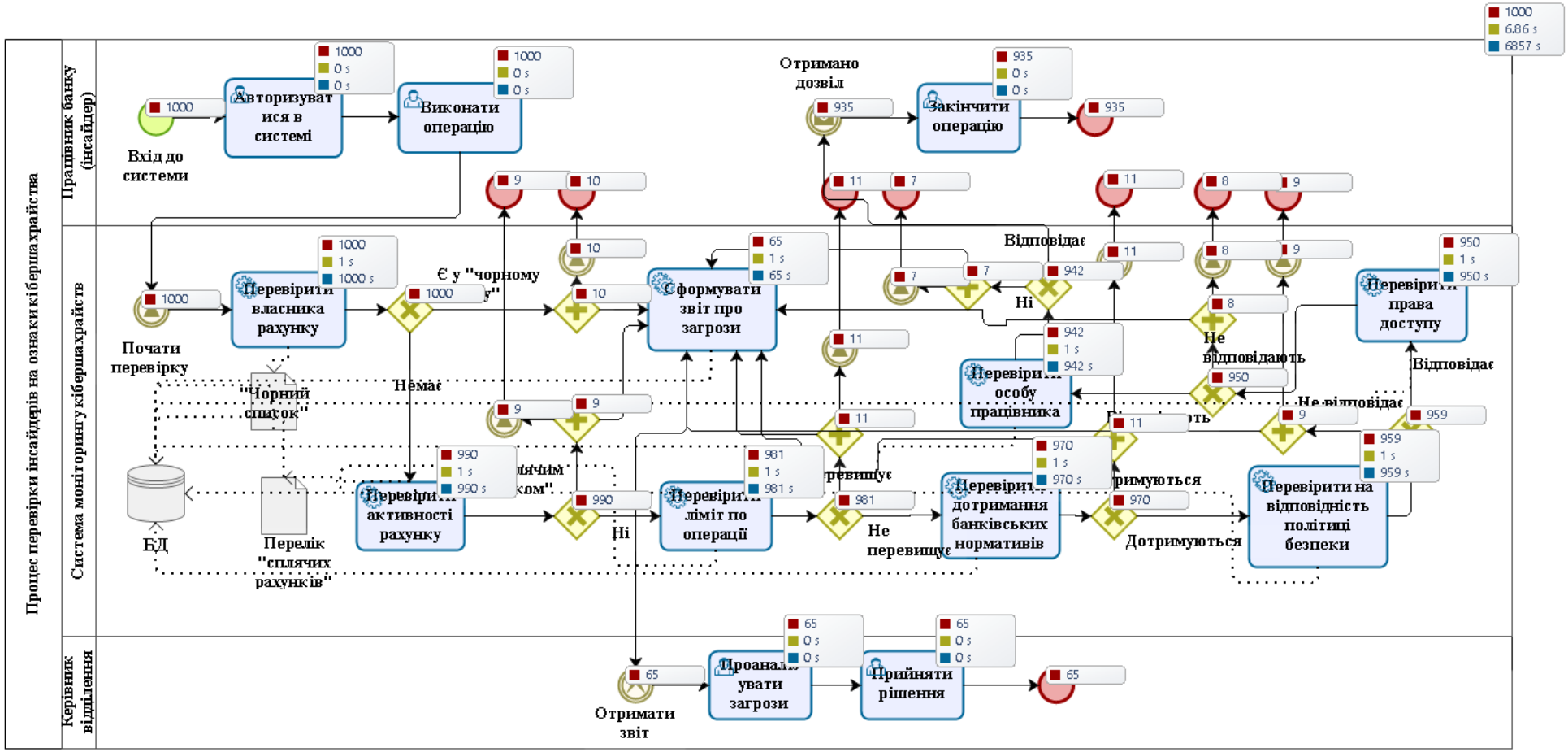

Рисунок А.4 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки кібершахрайств з боку інсайдерів