Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

ТЕОРІЯ ТА ПРАКТИКА ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ КІБЕРПРОСТОРУ КРАЇНИ

Монографія

За загальною редакцією О. В. Кузьменко, Г. М. Яровенко

Рекомендовано вченою радою Сумського державного університету

Суми
Сумський державний університет
2020

УДК 303.09:004.056:330.34; 334.012:339.194

Авторський колектив:
О. В. Кузьменко, доктор економічних наук;
Г. М. Яровенко, кандидат економічних наук;
О.А. Криклій, кандидат економічних наук;
К. Г. Гриценко, кандидат технічних наук;
Т. В. Доценко, аспірант кафедри економічної кібернетики;
О. В. Колотіліна, аспірант кафедри економічної кібернетики;
В. О. Ковач, аспірант кафедри економічної кібернетики;
С. О. Кушнєрьов, аспірант кафедри економічної кібернетики

Рецензенти:
С. В. Лєонов – доктор економічних наук, професор, начальник департаменту бізнес-процесів Сумського державного університету (м. Суми);
С. В. Агаджанова – кандидат технічних наук, доцент, завідувач кафедри кібернетики та інформатики Сумського національного аграрного університету (м. Суми);

Рекомендовано до видання вченою радою
Сумського державного університету як монографія
(протокол № 5 від 12 листопада 2020 року)

Теорія та практика забезпечення розвитку кіберпростору країни : Монографія / О. В. Кузьменко, Г. М. Яровенко, О. А. Криклій, К. Г. Гриценко та ін.; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : Сумський державний університет, 2020. 197 с.

Монографія присвячена розробці теоретичних та практичних засад забезпечення розвитку кіберпростору країни, а саме: бібліометричного аналізу досліджень інформаційної безпеки в розрізі розвитку національної економіки; канонічного аналізу взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни; аналізу із використанням карт Кохонена для оцінки рівня інформаційної безпеки країн з урахуванням їх розвитку; організаційно-інституційних засад забезпечення стійкості фінансового кіберпростору; системно-динамічного підходу трансформації систем захисту на основі блокчейнів; нечітко-множинного методу виявлення ризиків порушення кібербезпеки банку; гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом; підходу ігромоделювання процесів оптимізації державного регулювання економічної безпеки національної економіки; моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. Монографія призначена для студентів і викладачів вищих навчальних закладів, аналітиків, фахівців з питань кібербезпеки.

УДК 303.09:004.056:330.34; 334.012:339.194
ISBN

ЗМІСТ

ВСТУП

В сучасних умовах цифровізації економіки, стійкого розвитку комп'ютерних та інформаційних технологій, банкоцентричності фінансового ринку, великої концентрації грошей, різноманітності on-line послуг банківська діяльність не лише робить банки привабливими для кіберзлочинців та призводить до «інтелектуалізації» банківських шахрайств, але й виступає об'єктом тих фінансових шахрайств, які здійснюються як зовнішніми по відношенню до банку шахраями, так і внутрішніми, в якості яких виступає керівництво та персонал банку. Все це значно знижує довіру до фінансових інституцій, зменшує обсяги ресурсів в економіці, негативно впливає на фінансово-економічну безпеку України та її імідж надійного фінансового партнера в євроінтеграційних процесах. Поєднання в межах даного проекту наукового потенціалу дослідників з різних сфер (ІТ-аналітика, кібернетика, економіко-математичне моделювання, фінанси, банківська справа) відкриває нові можливості для її міждисциплінарного вирішення на системному рівні.

Світовою та вітчизняною науковою спільнотою напрацьовано значний інструментарій по застосуванню методів кібербезпеки для постфактум-реагування на виникнення шахрайств в банках. Даний проект враховує існуючі напрацювання, але спрямований на вирішення проблеми ранньої діагностики потенційних джерел кібершахрайських операцій, оцінки їх ймовірності, організації незалежного моніторингу дій банківського персоналу та формування організаційно-інституційного забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні, що сприятиме підвищенню рівня захисту споживачів та зменшенню втрат національної економіки.

Дуже поширеним видом шахрайства є соціальна інженерія, коли злочинець ошукує клієнтів банку шляхом виманювання даних карток та злому особистих акаунтів клієнтів. Хоча банки активно намагаються протидіяти цьому виду шахрайств, але злочинці знаходять нові способи здійснення шахрайств. Окрім

зовнішніх шахраїв значну шкоду завдають й внутрішні. Статистика свідчить, що близько 85% шахрайств в банківський сфері належить банківським працівникам, які мають доступ до різного роду інформації про рахунки, клієнтів та до внутрішньої та зовнішньої документації. Вони також мають змогу вилучати інформацію та продавати її стороннім компаніям, що також сприяє появі слабких місць в системі кіберзахисту банку.

Одним з напрямів банківського шахрайства є також здійснення процесу відмивання коштів, які були отримано незаконним шляхом. Проблема полягає як раз в процесі виявлення таких операцій. Тобто в цьому напрямі повинна працювати система внутрішнього моніторингу, основна мета якої виявлення операцій, що мають ознаки легалізації коштів. Але якщо банківські працівники знаходяться у зговорі з кримінальними структурами або зацікавлені у процесі відмивання коштів через пов’язаних осіб, то цей аспект також потребує врахування в процесі організації системи кібербезпеки банку.

На сьогодні система внутрішнього аудиту банків є досить розвинутою та добре організованою. Але її основна задача – це перевірка фінансово-господарської діяльності банку на предмет її відповідності законодавству, банківським нормативам, стандартам. Потужний інструментарій аудиту, сформований фахівцями роками, сприяє виявленню різного роду відхилень. Тому цей підхід можна також реалізовувати й для виявлення шахрайств у банку, як з боку зовнішніх шахраїв, так й з боку внутрішніх.

Враховуючи останні тенденції, банки зобов'язані інвестувати значною мірою в модернізацію системи кіберзахисту шляхом придбання або створення сучасних систем виявлення та попередження шахрайств, які врешті-решт також можуть виявитися неефективними. Тому для боротьби із шахрайствами банки повинні підходити послідовно та системно. По-перше, необхідна чітка регламентація дій персоналу щодо доступу до даних, що дозволить уникнути фактів його доступу до персональної інформації клієнтів та відповідно викрадення її. По-друге, вводити стратегії, які включають проведення тренінгів з

обізнаності про шахрайство, роз'яснення серед населення через засоби масової інформації та Інтернет, оцінку ризиків шахрайства та безперервний моніторинг. По-третє, удосконалити програмне та інформаційне забезпечення автоматизованої банківської системи з урахуванням інтелектуальних алгоритмів обробки, що дозволить на етапі здійснення шахрайства ідентифікувати шахрая та жертву, попередити здійснення такої операції та виявити злочинця.

Монографія складається із чотирьох частин. У першій частині «Інформаційна безпека як основа формування кіберпростору країни» проведено бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки, канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни, на основі використання карт Кохонена проаналізовано рівень інформаційної безпеки країн з урахуванням їх розвитку. У другій частині «Організаційно-інституційні засади забезпечення стійкості фінансового кіберпростору» зосереджено увагу на розробці науково-методичних засад формування механізму забезпечення кіберстійкості банків. Третя частина «Сучасні технології внутрішньої кібербезпеки економічних агентів» стосується розгляду перспектив застосування технології блокчейн в системах забезпечення кібербезпеки банків, розробці системно-динамічного підходу трансформації систем захисту на основі блокчейнів, нечітко-множинної моделі виявлення ризиків порушення кібербезпеки банку з боку його персоналу, гравітаційної моделі оцінки ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом. У четвертій частині «Механізм регулювання безпеки держави як детермінанта її розвитку» здійснено оцінку ризиків соціо-економіко-політичного розвитку України, ігромоделювання процесів оптимізації державного регулювання економічної безпеки національної економіки, розроблено інтегральний індекс загрози національної економіки за допомогою метода Кернела.

Окремі підрозділи монографії підготували: підрозділи 3.4, 4.2 - доктор економічних наук, професор Кузьменко О.В.; розділ 1, підрозділи 3.1, 4.1, 4.3,

вступ та висновки - кандидат економічних наук, доцент Яровенко Г.М.; розділ 2 - кандидат економічних наук, доцент Криклій О. А.; підрозділ 3.3 – кандидат технічних наук, доцент Гриценко К.Г.; підрозділи 3.4, 4.2, 4.3 - аспірант кафедри економічної кібернетики Доценко Т.В.; підрозділ 3.1 - аспірант кафедри економічної кібернетики Колотіліна О.В.; підрозділ 3.1 - аспірант кафедри економічної кібернетики Ковач В.О.; підрозділ 3.4, 4.3 - аспірант кафедри економічної кібернетики Кушнєрьов О.С.

Монографія виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

РОЗДІЛ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВА ФОРМУВАННЯ КІБЕРПРОСТОРУ КРАЇНИ

1.1. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки

Стрімкий розвиток комп’ютерних технологій призвів до автоматизації багатьох сфер, особливо пов’язаних із економікою. Так, більшість платіжних операцій переведено не тільки у безготівкову форму, але їх здійснення тепер можливе через мобільний та Інтернет-банкінг із будь-якої точки світу. Значні обсяги нарощує електронна торгівля, яка дозволяє здійснювати будь-які операції купівлі-продажу через мережу Інтернет. Більшість прогресивних компаній переводить своїх співробітників у роботу в дистанційному режимі, що дозволяє знизити витрати на оренду та експлуатацію приміщень, комп’ютерної техніки, та підвищити мобільність працівників. Дані приклади свідчать про розширення можливостей програмного забезпечення, комп’ютерних та мобільних технологій для вирішення потреб бізнесу, людини та країни в цілому.

Але є й негативний бік, пов'язаний із зростанням різного роду інформаційних загроз, які призводять до втрати інформації в результаті здійснення хакерських атак, її незаконного використання у кримінальних цілях. Це може спричинити появу інформаційних війн, які призводять до дестабілізації настроїв у суспільстві, гальмування економічного розвитку країни та зниження довіри міжнародних партнерів. Саме тому виникає необхідність у створенні ефективної системи інформаційної безпеки, яка б забезпечувала захист даних компаній, окремої людини, країни. Відповідно дана потреба заслуговує на увагу з боку науковців, що повинно проявлятися у збільшенні не тільки кількості наукових публікації з даної тематики, але й підвищенні їх якості та рівня за умови їх оприлюднення у виданнях, які індексуються у міжнародних базах, таких як

Scopus та Web of Science. Але цінності набувають ті наукові праці, які висвітлюють результати дослідження проблеми не у загальному вигляді, а її вирішення для певної сфери діяльності. Тому важливо вивчити питання інформаційної безпеки в розрізі різних аспектів, особливо економічної сфери. Це пов’язано із тим, що в першу чергу, наслідки інформаційних загроз відчуваються через втрати особистих коштів клієнтів банків, секретних даних компанії щодо фінансових операцій, недоотримання прибутків через відновлення втрачених даних та відтік клієнтів, тощо. Тобто спостерігається певний зв'язок між рівнем інформаційної безпеки та економікою країни. Саме тому даний аспект потребує детального вивчення.

Дослідження проводилося на основі бази даних Scopus, яка включає публікації фахівців з усіх країн світу та яка надає можливість відслідковувати тенденції щодо вирішення різних проблем різними науковими спільнотами. Вбудовані інструменти пошуку та аналізу дозволяють дослідити географію публікацій, сфери дослідження даної проблеми, рівень цитування, динаміку публікаційної активності.

На першому кроці було досліджено динаміку публікацій, які присвячені темі «Інформаційна безпека». Так, однією з перших публікацій у базі даних Scopus, яка розкриває проблематику захисту інформації та інформаційної безпеки, була стаття 1968 року Дж. Б. Денніса під назвою «A position paper on computing and communications» [1]. Автор цієї праці розглядав аспекти розробки положень інформаційної безпеки для розвитку публічних комунікаційних послуг з комутацією повідомлень. Популярність цього напрямку досліджень починає зростати з 2000 року, тому для подальшого аналізу було узято період 2000-2019 р.р. Для порівняння тенденцій публікаційної активності також було використано дані бази даних Dimensions, яка представляє собою інформаційну платформу для пошуку та доступу академічних та інших результатів досліджень. Вона містить більш ніж 128 млн. публікацій, баз даних, грантів, патентів, політик тощо. Результати дослідження представлені на рисунку 1.

Було виявлено, що за останні 20 років спостерігається стрімке зростання зацікавленістю проблемами інформаційної безпеки у світі серед науковців (див. рис. 1.1).

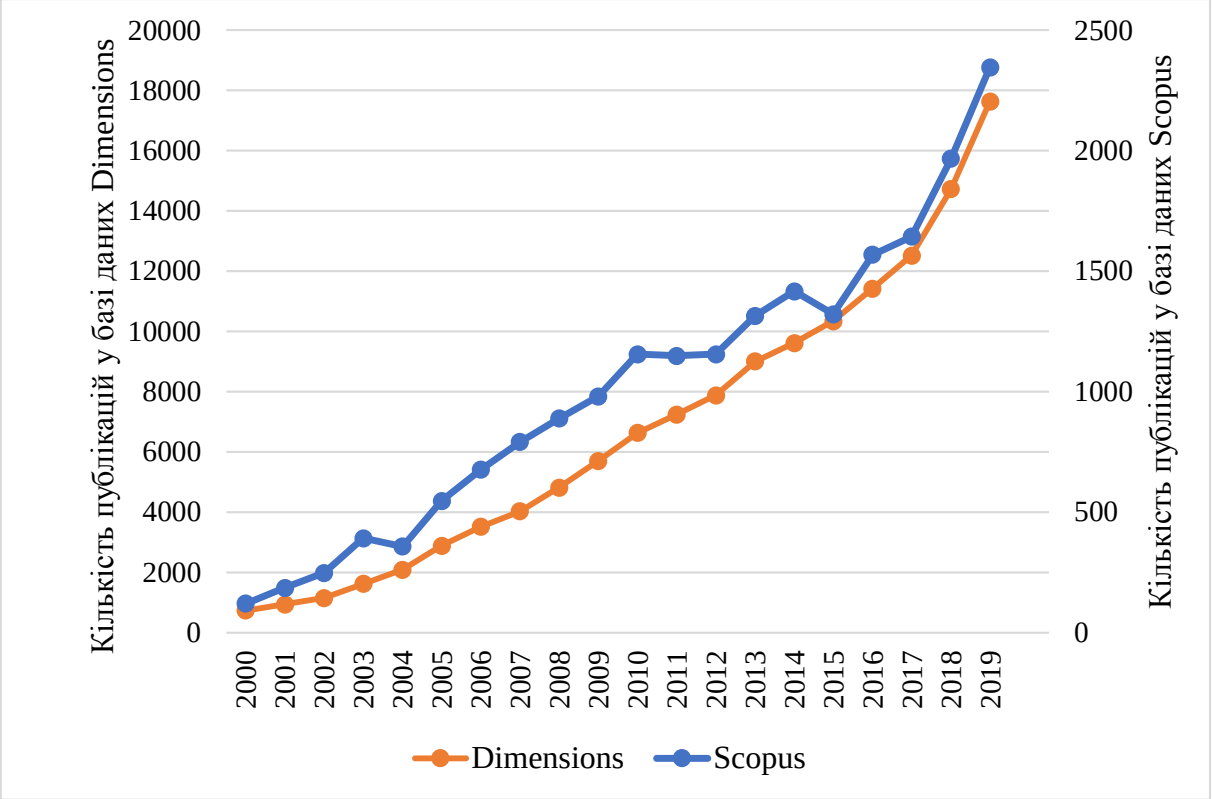


Рисунок 1.1 – Динаміка публікацій, присвячених темі «Інформаційна безпека»

Так, у 2019 році було опубліковано 2347 наукових праць, індексованих у базі Scopus, у порівнянні із 120 публікаціями 2000 року. Різке зростання також спостерігається й по даним Dimensions: 17643 наукових праць у 2019 році на противагу 728 публікацій у 2000 році. Дана тенденція пояснюється тим, що якраз в останні роки відбувається стрімке збільшення комп'ютеризації та цифровізації різних сфер діяльності суспільства. Зросла кількість користувачів Інтернету, мобільних телефонів, програмних додатків. Основну масу платіжних операцій переведено на мобільні та комп'ютерні платформи. Як наслідок, підвищився рівень кіберзлочинів, що вплинуло на забезпечення потреби інформаційної безпеки для бізнесу, населення та держави в цілому. З розвитком технологій

штучного інтелекту, віртуальної, доповненої реальності, роботизації ця потреба тільки зростатиме.

Які ж сфери, де гостро стоїть питання підвищення ефективності системи інформаційної безпеки, досліджуються вченими? Так, на рисунку 2 представлена діаграма розподілу публікацій, присвячених даній проблемі, за предметною областю.

40% публікацій досліджують проблематику інформаційної безпеки у сфері комп'ютерних наук, тобто вивчаються різні сучасні комп'ютерні технології, які дозволяють підвищувати ефективність системи інформаційної безпеки, знижувати ризики втрати інформації, забезпечувати захист даних, попереджати виникнення різного роду загроз, тощо (див. рис. 1.2).

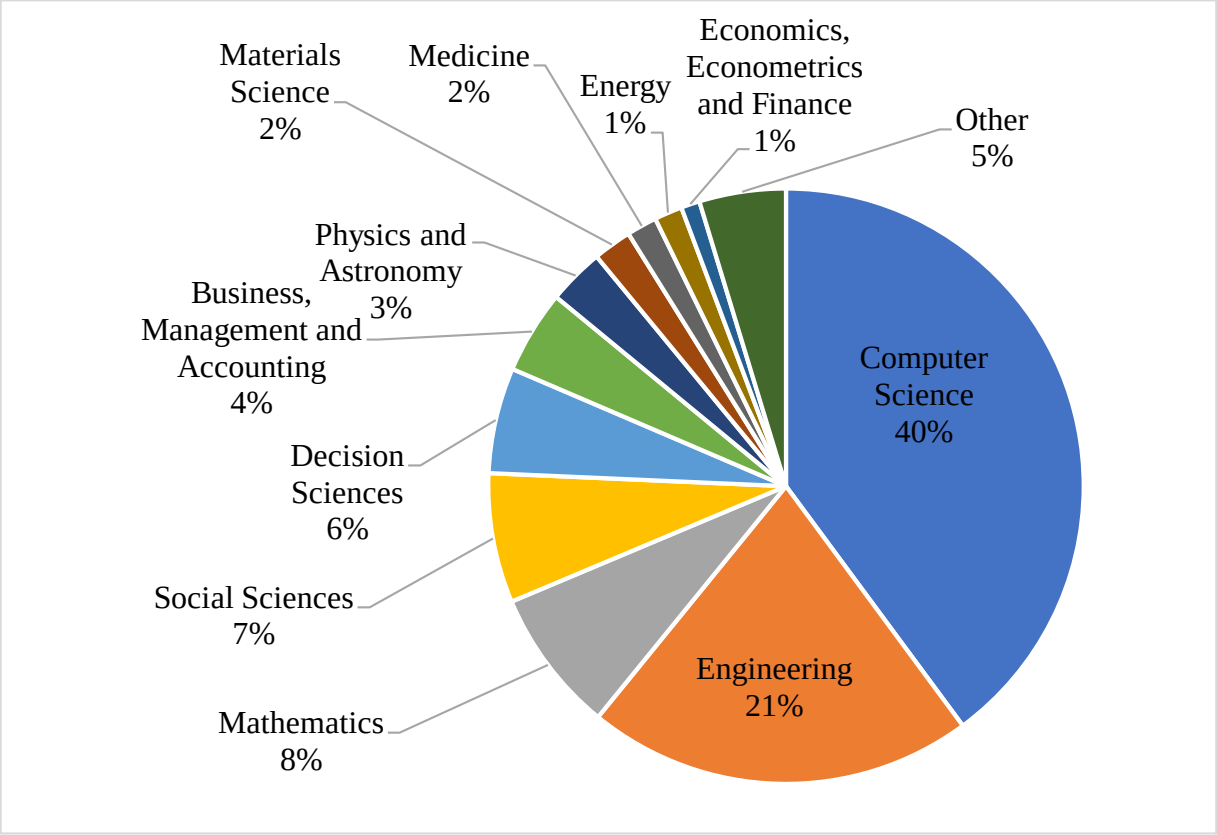


Рисунок 1.2 – Діаграма розподілу публікацій, присвячених темі «Інформаційна безпека», за предметною областю

Наступний сектор – це інженерія (21%), де проводяться дослідження щодо розробки, удосконалення технічних пристроїв, функціонування яких

забезпечують захист інформації на належному рівні. Також можна відмітити вклад науковців (8%), який стосується дослідження проблем інформаційної безпеки із використанням математичних методів та алгоритмів. Що стосується сфери економічного розвитку, то кількість наукових досліджень становить приблизно 1 %, що говорить про незначний рівень зацікавленості з боку наукової спільноти щодо вивчення взаємозв'язків між розвитком економіки країни та рівнем її інформаційної безпеки. Але динаміка публікацій за останні 20 років змінилася (див. рис. 1.3).

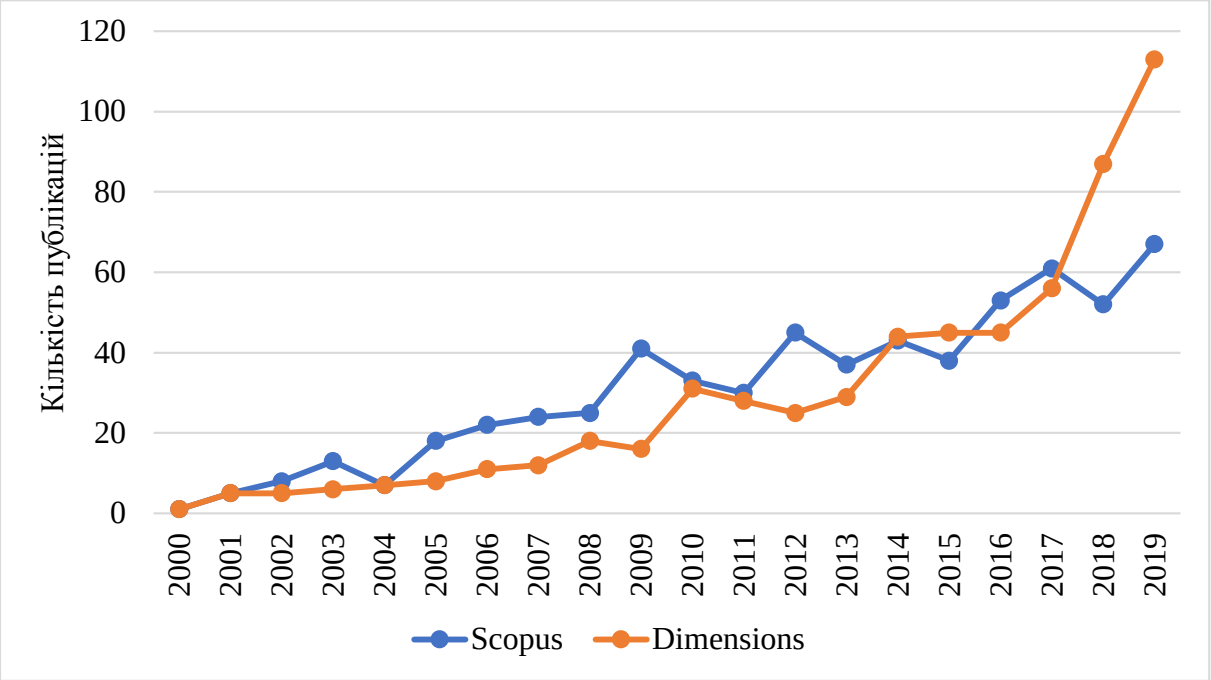


Рисунок 1.3 – Динаміка публікацій, присвячених темі «Інформаційна безпека» з урахуванням мети економічного розвитку

Так, при порівнянні даних бази Scopus та Dimensions можна побачити поступове збільшення кількості наукових праць, що свідчить про формування нових векторів розвитку економіки з урахуванням впливу сучасних комп'ютерних технологій, появи суттєвих проблем захисту фінансової інформації компаній та населення країни. Оскільки деякі аналітичні компанії, такі як "Juniper Research", прогнозують збільшення фінансових втрат завдяки підвищенню рівня кіберзлочинності до 5 трлн. дол. у 2024 році [2], то можна з упевненістю сказати,

що питання впливу інформаційної безпеки на розвиток економіки буде привертати до себе більше уваги, ніж зараз.

Якщо проаналізувати географію проведених досліджень, то можна виділити 10 країн, науковцям із яких належить найбільша кількість публікацій, присвячених вивченню проблеми інформаційної безпеки та її впливу на розвиток економіки країни (див. рис. 1.4).

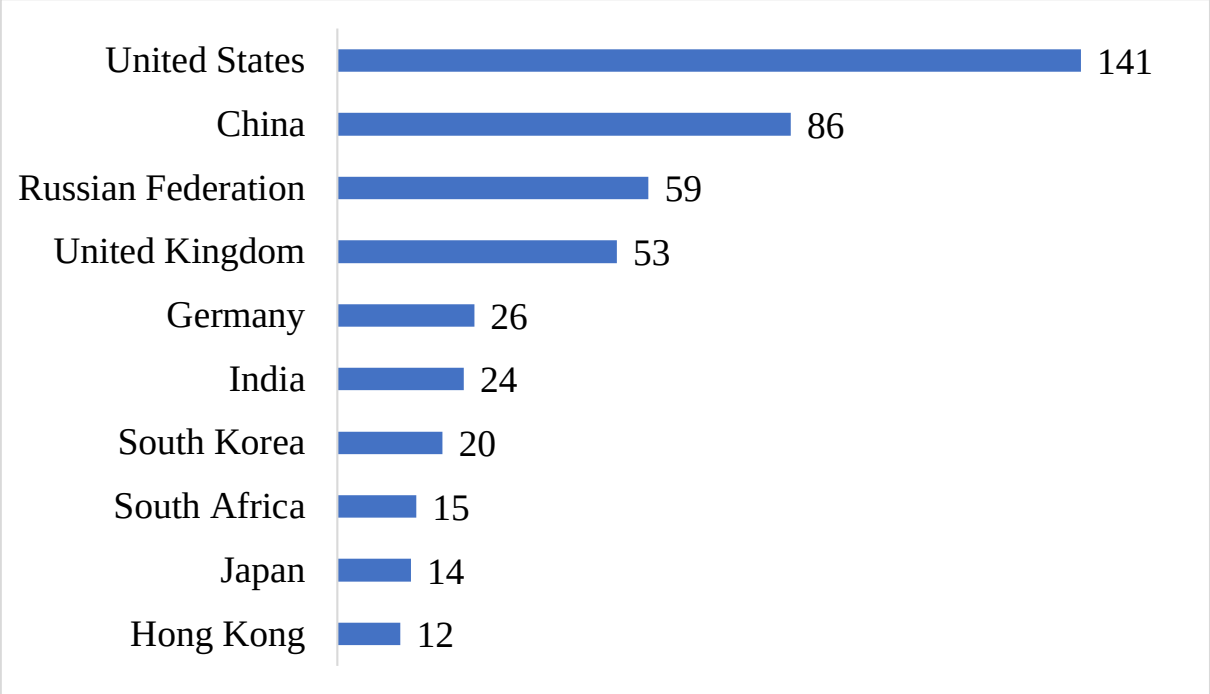


Рисунок 1.4 – Географія проведених досліджень, присвячених проблемі інформаційної безпеки у розрізі її впливу на економічний розвиток

Найбільша кількість досліджень проводиться вченими США. Це відбувається у зв'язку із тим, що ця країна є передовою в сфері розробки інноваційних технологій. Також саме в цій країні функціонують інноваційні компанії-гіганти, як Apple, Google, Microsoft, IBM, Oracle Corporation, Intel, Cisco Systems та інші, які займаються дослідженнями та практичною реалізацією сучасних програмних, комп'ютерних, електронних та інших технологій в сфері захисту інформації. Друге місце в даній сфері належить китайським вченим. Це обумовлюється стрімким розвитком Китаю та його прагненням бути найсильнішим лідером у світі, що проявляється у створенні корпорацій-гігантів,

таких як Lenovo, Huawei, Tencent, Megvii Technology. Також уряд Китаю запровадив програму, згідно з якою відбуватиметься інвестування 1,4 трлн. дол. протягом 6 років до 2025 року приватних технологічних компаній [3], що може визвати сплеск наукових досліджень в сфері інформаційної безпеки.

Що стосується академічних результатів, то було обрано ряд університетів, які опублікували найбільшу кількість статей, присвячених проблемі інформаційної безпеки в розрізі її впливу на економіку країни. Результати представлені у таблиці 1.1.

Таблиця 1.1

Рейтинг університетів за кількістю публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

№	Назва університету	Країна	Кількість публікацій
1	Університет Карнегі Меллона	США	13
2	Південно-східний університет Нанкіна	Китай	11
3	Кембриджський університет	Великобританія	10
4	Міський університет Гонконгу	Китай	8
5	Університет штату Меріленд	США	6
6	Північно-китайський університет електроенергетики	Китай	6
7	Санкт-Петербурзький державний економічний університет	Російська Федерація	6
8	Техаський університет у Сан-Антоніо	США	5
9	Університет Пердью	США	5
10	Норвезький університет науки і техніки	Норвегія	5
11	Флоридський Атлантичний університет	США	5
12	Токійський університет	Японія	5
13	Російський економічний університет імені Р.В. Плеханова	Російська Федерація	5
14	Indian Institute of Technology Delhi, India	Індія	5
15	Robert H. Smith School of Business, USA	США	5

Серед наведених у таблиці 1 університетів, найбільша кількість наукових праць належить саме університетам Сполучених Штатів Америки, що підтверджує попередні висновки стосовно провідної ролі даної країни у сфері дослідження інформаційної безпеки. Тобто й бізнес, й академічна спільнота цієї

країни працюють більш продуктивно, ніж інші країни, й намагаються синхронізувати результати науки та практики.

Окрім розгляду загальних показників також було проаналізовано рейтинг журналів, в яких було опубліковано найбільшу кількість статей з теми дослідження (див. табл. 1.2).

Таблиця 1.2

Рейтинг журналів за кількістю публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

№	Назва журналу	Країна видання	SNIP	SJR	Кількість статей	% до загальної кількості
1	Lecture Notes in Computer Science	Швейцарія	0,776	0,427	30	4,41
2	Information and Computer Security	Великобританія	0,858	0,293	11	1,62
3	Computers and Security	Нідерланди	2,536	0,984	10	1,47
4	Journal of Physics: Conference Series	Великобританія	0,574	0,227	9	1,32
5	Advances in Intelligent Systems and Computing	Германія	0,429	0,184	8	1,17
6	Information Systems Frontiers	Нідерланди	1,926	1,020	8	1,17
7	IEEE Security and Privacy	США	1,445	0,555	7	1,03

Три журнали мають досить високий імпакт-фактор – SNIP > 1 (кількість публікацій складає 3,67%), три журнали мають значення SNIP > 0,5 (кількість публікацій складає 7,34%). Тобто близько 11% статей було опубліковано у достатньо рейтингових журналах, що не є високим показником. Це можна пояснити тим, що проблеми інформаційної безпеки найбільше вирішуються для комп’ютерної та програмної сфер, тому такий результат обумовлюється специфікою дослідження захисту інформації саме для потреб економіки.

Також було виділено 10 найбільш цитованих публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни (див. табл. 1.3).

Таблиця 1.3

Десять найбільш цитованих публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

№	Найменування публікації	Автор(и) / Країна	Найменування видання	Рік	Кількість цитувань
1	The Economics of Information Security Investment	Gordon L.A., Loeb M.P. / USA	ACM Transactions on Information and System Security	2002	667
2	Why information security is hard - An economic perspective	Anderson R. / UK	Annual Computer Security Applications Conference	2001	358
3	The economics of information security	Anderson R., Moore T. / UK	Science	2006	331
4	The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application	Au Y.A., Kauffman R.J. / USA	Electronic Commerce Research and Applications	2008	210
5	Sharing information on computer systems security: An economic analysis	Gordon L.A., Loeb M.P., Lucyshyn W. / USA	Journal of Accounting and Public Policy	2003	184
6	Secure or insure? a game-theoretic analysis of information security games	Grossklags J., Christin N., Chuang J. / USA	Proceeding of the 17th International Conference on World Wide Web 2008	2008	145
7	An empirical analysis of the impact of software vulnerability announcements on firm stock price	Telang R., Wattal S. / USA	IEEE Transactions on Software Engineering	2007	130
8	Circuits of power in creating De Jure standards: Shaping an international information systems security standard	Backhouse J. / UK, Hsu C.W. / Taiwan, Silva L. / USA	MIS Quarterly: Management Information Systems	2006	127
9	User behaviour towards protective information technologies: The role of national cultural differences	Dinev T., Goo J., Hu Q. / USA, Nam K. / South Korea	Information Systems Journal	2009	117
10	Management's role in information security in a cyber economy	Dutta A., McCrohan K. / USA	California Management Review	2002	105

Серед найбільш рейтингових публікацій можна виділити 2 напрями наукового дослідження: економічні аспекти забезпечення інформаційної безпеки та вивчення взаємозв'язків системи інформаційної безпеки із економічним середовищем. Так, до першого напрямку належать публікації 1, 3, 4, 6, до другого – 2, 5, 7, 8, 9, 10 (див. табл. 1.3).

Представлені рейтингові публікації відносяться до періоду 2000-2010 р.р., тобто за останні 10 років публікації такого рівня відсутні, що говорить про зниження зацікавленості наукової спільноти до даної проблеми або зміни вектору досліджень.

Якщо аналізувати десятку публікацій за період 2011-2020, які є менш цитованими, то можна виділити такі напрямки дослідження, як інвестування у галузь захисту інформації, розвитку сервісів для користувачів мобільних додатків, Інтернету, застосування сучасних технологій для забезпечення безпеки даних в різних сферах бізнесу, тощо. Тобто, дослідження охоплюють й програмну, технічну та економічну сфери у сукупності, тобто є більш мультидисциплінарними.

Для більш чіткого розуміння тенденцій сучасних досліджень обрані публікації бази даних Scopus, які присвячені проблемі інформаційної безпеки в розрізі економічного розвитку країни, було проаналізовано з використанням аналітичної платформи VOSviewer [4]. Даний інструмент дозволяє здійснювати візуалізацію бібліометричних мереж на основі цитувань, співцитувань, бібліографічних зв'язків. Так, було побудовано карту бібліографічних досліджень, присвячених інформаційній безпеці в розрізі її взаємозв'язків з економікою (див. рис. 1.5).

На карті виділено 7 кластерів існуючих досліджень, які було сформовано на основі ключових слів, зазначених авторами публікацій. Кожен з них надає уяву про напрями, за якими відбуваються дослідження проблеми інформаційної безпеки у розрізі економічного розвитку країни. Так, червоний кластер вміщує найбільшу кількість ключових слів, пов'язаних із захистом даних. Він

характеризує напрям створення, удосконалення, застосування та розвитку сучасних технологій інформаційної безпеки. Дослідження даної групи стосуються: блокчейн та хмарних технологій, big data, систем контролю, автоматизації, виявлення вторгнень, прогнозування кібератак, технологій криптографії, шифрування, data mining, нейронних мереж. Даний кластер охоплює також напрям створення програмного забезпечення та комп'ютерних мереж для забезпечення потреб інформаційної безпеки. Окрім цього визначається також економічна ефективність заходів в сфері безпеки та вплив їх на економіку.

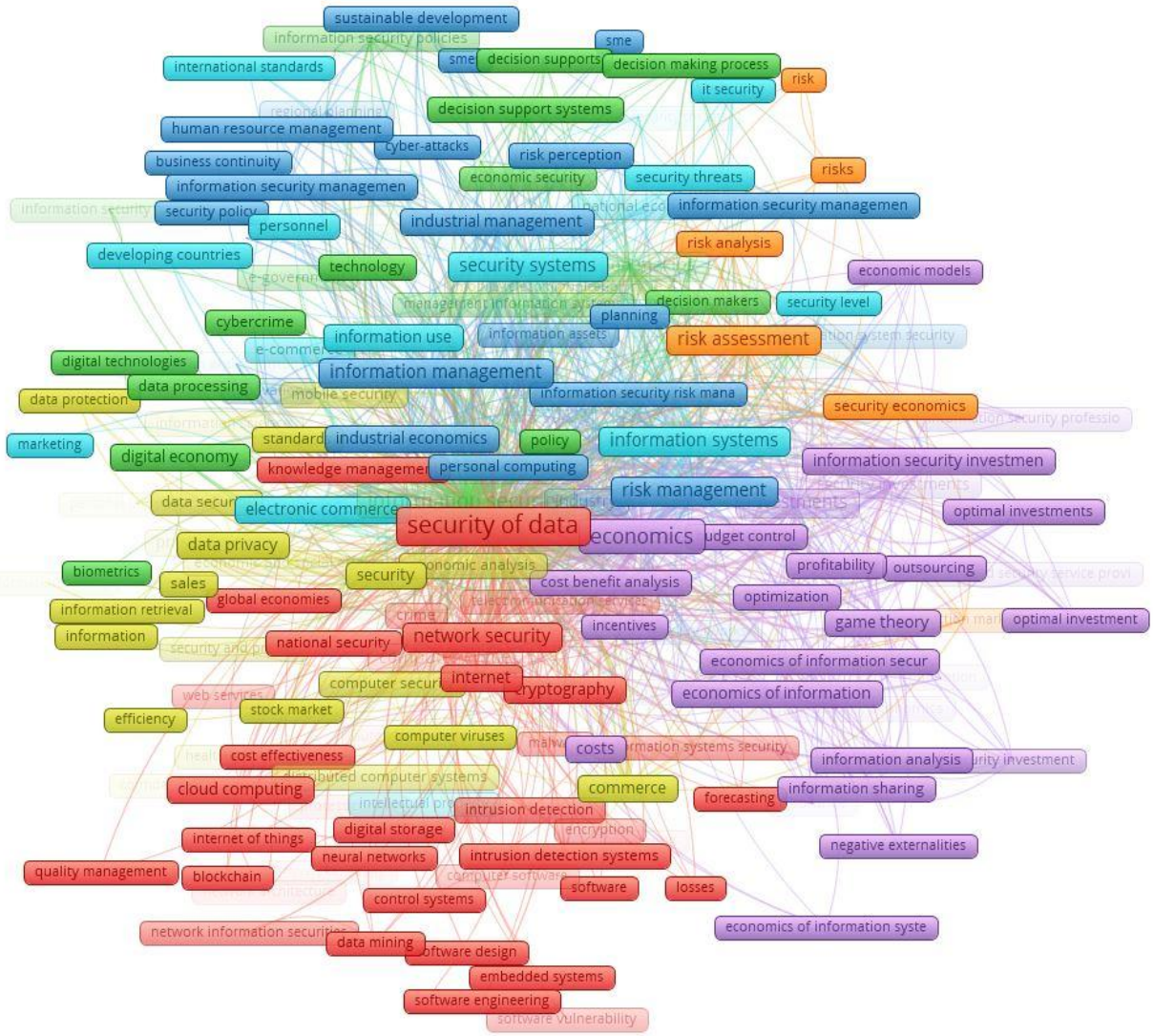


Рисунок 1.5 – Карта наукометричної бібліографії досліджень, присвячених проблемі інформаційної безпеки у розрізі економічного розвитку країни

Зелена група містить ключові слова, пов’язані із прийняттям рішення в сфері інформаційної безпеки та впровадженням ряду технологічних рішень для аутентифікації користувачів, їх біометрії, підвищення рівня інформаційної культури, попередження вразливостей систем, кіберзлочинів. При цьому дані поняття стосуються також й сфери електронного уряду, цифровізації економіки. Синій кластер охоплює напрям інформаційного менеджменту. Тобто тут проводяться дослідження, які стосуються управління людськими ресурсами, ризиками, політикою захисту; планування; створення ефективної інфраструктури компанії, тощо. Жовта група характеризує специфіку досліджень щодо питань обробки, відновлення, захисту, забезпечення конфіденційності персональної інформації. Дана проблематика розкривається для користувачів мобільних пристроїв, комп’ютерів, платіжних додатків, інтернет-магазинів. Бузковий кластер містить ключові слова, які стосуються економічних аспектів забезпечення інформаційної безпеки – економіці інформації, економіці інформаційних систем, економіці інформаційного захисту. Тут можна виділити проблеми витрат, пов’язаних із системами захисту даних, побудови ефективних економічних моделей, страхування, інвестування, оптимізації, прибутковості, аутсорсингу, управління в цілому. Бірюзова група охоплює напрям, пов'язаний із забезпеченням інформаційної безпеки на рівні підприємств та національної економіки через розробку інформаційних систем, стандартів, правових норм. Помаранчевий кластер характеризує напрям дослідження ризиків інформаційної безпеки, а саме їх передбачення, аналіз, оцінка.

Аналіз кластерів карти показав, що існує доволі широкий спектр проблем, які досліджуються в публікаціях, присвячених інформаційній безпеці у розрізі забезпечення економічного розвитку країни.

Отримані результати дозволили прийти до наступних висновків. Проблематика, пов’язана із інформаційною безпекою, є досить актуальною у наукових колах, про що свідчить зростання зацікавленістю даної теми протягом останніх 20 років. Це підтверджено збільшенням наукових досліджень у

міжнародних виданнях, які індексуються у базі даних Scopus, а також зростанням наукових публікацій у академічних виданнях, інформація про які міститься у базі даних Dimensions. Дослідженнями інформаційної безпеки у розрізі підвищення економічного розвитку країн займається приблизно 1% науковців, хоча тенденція з цього питання є позитивною. Серед країн, науковці яких вивчають проблематику інформаційної безпеки саме з позиції її взаємозв'язку із економічним розвитком, провідними є США та Китай, що обумовлено їх спрямованістю до лідерства у сфері розробки сучасних інформаційних та комп'ютерних технологій. Даний висновок також підтвердив аналіз рейтингу університетів, науковці яких займаються досліджуваною темою. Левова частка належить науковим лабораторіям університетів США.

Аналіз журналів, в яких було опубліковано статті, присвячені проблемі інформаційної безпеки в сфері економіки, показав, що з даного напрямку тільки близько 11% статей надруковано у рейтингових журналах, що говорить про здійснення локальних досліджень та отримання результатів, прийнятних для окремих країн чи інститутів. Виділення 10 найбільш цитованих публікацій дозволило окреслити 2 напрями, які стосуються економічних аспектів забезпечення інформаційної безпеки та дослідження взаємозв'язків системи інформаційної безпеки із економічним середовищем. Це характерно для періоду 2000-2010, в який було видано дані статті. Хоча публікації останнього десятиріччя не мають такого рівня цитувань, але вони охоплюють більш різноманітні напрямки дослідження. Це було підтверджено й картою бібліографічних досліджень, яка дозволила виділити 7 кластерів-напрямів: розвиток технологій безпеки, прийняття рішення, інформаційний менеджмент, персональна безпека, економіка інформаційної безпеки, інформаційна безпека на рівні підприємств та національної економіки, інформаційні ризики.

Отримані результати дослідження можна використовувати в подальшому з метою виявлення найбільш перспективних напрямів дослідження проблематики інформаційної безпеки з урахуванням різних сфер – економічної, соціальної,

політичної, тощо. В подальшому дослідження планується розширити за рахунок проведення аналізу бази даних Web of Science, що дозволить також здійснити кластеризацію за вибіркою найбільш цитованих наукових публікацій.

1.2. Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни

У сучасному світі на тлі промислової революції 4.0 більшість процесів переводиться у цифровий або віртуальний світ. Це пов'язано із тим, що в різних сферах соціального, економічного, політичного розвитку країни знаходять масу переваг у використанні комп'ютерних, інтелектуальних, кібер-фізичних та інших технологій для вирішення нагальних проблем суспільства. Так, завдяки поширення Інтернету речей та Інтернет-торгівельних платформ, компанії збільшують обсяги збуту, нарощують клієнтські бази, що сприяє отриманню надприбутків. Впровадження систем типу «електронна адміністрація», дозволяє знижувати час та грошові витрати на обслуговування громадян, підвищувати якість адміністративних послуг. Переведення платіжних засобів у безготівкову площину сприяє також зниженню витрат для банків на здійснення операцій, підвищує зручності для клієнтів щодо сплати за товари, послуги, отримання та погашення кредитів, здійснення комунальних платежів, тощо. Ці приклади та багато інших показують, на скільки сучасне суспільство є залежним від мобільних пристроїв, комп'ютерних технологій та інформаційних систем.

З іншого боку, цифровізація та комп'ютеризація суспільства призводить до того, що отримання інформації стає метою злочинців та шахраїв, які здійснюють хакерські атаки для незаконного отримання інформації компанії, викрадають дані клієнтів платіжних систем, провадять вірусні атаки для руйнування інформаційного середовища та усунення конкурентів компанії, тощо. Тому зростає необхідність підвищення заходів кібербезпеки зокрема та інформаційної безпеки в цілому. Дане питання є актуальним не тільки для окремих компаній,

різних установ, банків, але це є важливим й для країни в цілому. Інформаційна безпека на рівні держави є доволі складним поняттям, яке уособлює ряд інститутів, заходів, які сприяють захисту інформаційного простору країни та суспільства від здійснення зовнішніх, незаконних інформаційних атак, кібер-тероризму, які завдають шкоди національним інтересам, соціальному, економічному та політичному життю країни. Тому для ефективної організації системи інформаційної безпеки важливо розуміти, яким чином вона формується та від яких чинників залежить. Відповідно, можна сформувати гіпотезу про те, що ефективність системи інформаційної безпеки на державному рівні обумовлюється факторами соціально-економічного розвитку країни, тобто розвинуті країни із потужним соціально-економічним потенціалом та стабільною політичною ситуацією мають підвищений рівень інформаційної безпеки та навпаки, збільшення рівня інформаційної безпеки впливає на розвиток країни. Дана гіпотеза потребує перевірки та підтвердження або відхилення.

Проблема, присвячена різним аспектами інформаційної безпеки, є досить актуальною. Вона привертає увагу науковців зі всього світу. Так, аналізуючи наукові статті в міжнародних журналах, які індексуються у базі даних Scopus, було виявлено, що однією з перших публікацій, які розкривають проблематику захисту інформації та інформаційної безпеки, була стаття 1967 року Дж. Б. Денніса під назвою «A position paper on computing and communications». Автор торкався напрямку розробки положень інформаційної безпеки для розвитку публічних комунікаційних послуг з комутацією повідомлень.

З появою новітніх технологій та із збільшенням кількості та видів кібершахрайств зросла й кількість публікацій, присвячених теоретичним та практичним питанням інформаційної безпеки на рівні підприємств, банків та держави. Так, за даними бази Scopus за останні 10 років було опубліковано 16025 наукових праць, присвячених проблематиці інформаційної безпеки. З них приблизно 1700 статей розглядають концепції кібербезпеки в рамках інформаційної безпеки [5]. Галузі, в яких здійснювалися дослідження науковців,

пов’язані із різними напрямками інформаційної безпеки, – це комп’ютерні науки (39,2%), інженерії (20,9%), математики (8,1%), соціальних наук (6,4%), прийняття рішень (5,7%), бізнесу, менеджменту, бухгалтерського обліку (4,4%), фізики та астрономії (3,4%), матеріалознавства (2,3%), енергетики (1,8%), медицини (1,7%), та інших (6,2%) [6]. Тобто, інформаційна безпека є актуальною передусім для комп’ютерної галузі, оскільки саме ця сфера відповідає за програмну, технічну, методологічну та інформаційну складову захисту інформації, не залежно від сфери діяльності людини.

Якщо провести аналіз наукових праць дослідників за останні 10 років за географічним охопленням, то найбільшу увагу до цієї проблеми приділяють вчені Китаю (3968 публікацій), США (2070), Індії (1419), Росії (1086), Великобританії (670), Південної Кореї (478), Австралії (451), Тайваню (429), Германії (418), Малазії (399), тощо [7]. На сьогодні більшість з цих країн є лідерами у розробці потужних програмно-технічних комплексів та комп’ютерних систем захисту, тому виправдано, що їх вчені висвітлюють свій практичний досвід у цій сфері. Так, найвагоміший внесок у дослідження різних аспектів інформаційної безпеки було зроблено такими закордонними фахівцями, як: N. Miloslavskaya, A. Ahmad, R. Von Solms, T. Ahmad, R. Amirtharajan, M. Warkentin, A. Tolstoy, S. Furnell, J.B.B. Rayappan, S. Mansfield-Devine, K. Parsons, A. McCormac, M. Pattinson, S.M.T. Toapanta, M. Butavicius, G. Dhillon, P.B. Lowry, L.E.M. Gallegos, S.B. Maynard та інші [8]. Кожним з них було опубліковано 20 і більше наукових праць у міжнародних виданнях, які індексуються у базі Scopus, що свідчить про їх значний науковий доробок у дослідження проблематики інформаційної безпеки.

Серед українських вчених можна виділити ряд науковців, які також займаються проблемою інформаційної безпеки. Так, М. Бешлей, О. Кочан, А. Прислупський в своїх працях торкаються аспектів розробки програмного забезпечення для виявлення аномалій. Моделі діагностики інформаційних систем досліджують С. Гохонянц, А. Зідан, О. Лаптієв, І. Саланда, Г. Шуклін. Питання

удосконалення засобів криптографії вирішували в свої статтях С. Гнатюк, Т. Охріменко. Методами оцінки кіберзагроз займаються П. Сніцаренко, О. Захорка, А. Корецький, Ю. Саричев, В. Ткаченко. Можна також виділити проблему персональної безпеки та захисту особистої інформації, розробки різних методик та технік для здійснення процесу аутентифікації користувачів. Цими питаннями займаються І. Бальченко, М. Дорош, М. Войцеховська, О. Оксіюк, А. Фесенко, В. Чайковська та інші. Серед цих та інших перелічених проблем є ряд науковців, які займаються дослідженням державної інформаційної безпеки, а саме: О. Дніпров, О. Коротюк, О. Сидоренко, К. Чижмар, Р. Шаповал та інші.

Не дивлячись на вагомий науковий внесок закордонних та вітчизняних вчених, є ряд питань, які потребують уточнення та дослідження. Сюди слід віднести аспект інформаційної безпеки, що здійснюється на рівні держави. Особливої уваги потребує визначення впливу цієї сфери на розвиток країни.

Для доведення висунутої гіпотези у якості показника, що характеризує рівень інформаційної безпеки країни, було обрано національний індекс кібербезпеки, який використовується для оцінки підготовленості країни протидіяти різним кіберзагрозам та можливості керувати різними кібер-інцидентами. Хоча даний показник звужує рамки прийнятого в Україні поняття інформаційної безпеки, але в світовій практиці саме він застосовується для надання актуальної та точної інформації щодо розвитку національних систем кібербезпеки (інформаційної безпеки), порівняння дій влади в галузі безпеки інформації та отримання інформації щодо найкращих практик в цій сфері [9]. Також складові національного індексу кібербезпеки характеризують безпеку за 12 напрямкам: розробка політики та стратегії в галузі кібербезпеки; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; оцінка внеску у глобальну кібербезпеку; рівень захисту цифрових послуг: відповідальність, стандарти, органи; організація захисту основних послуг; електронна ідентифікація та послуги довіри; захист персональних даних; реагування на кібер-інциденти; кіберрегулювання кризи;

боротьба з кіберзлочинністю; військові кібер-операції [9]. Тому даний індикатор та його складові дозволять в повному обсязі зробити оцінку щодо рівня інформаційної безпеки країни в цілому.

Використовуючи значення національного індикатора кібербезпеки за 2018 рік для 159 країн світу, побудуємо карту, яка дозволить зробити візуальний аналіз географії країн та дозволить оцінити, для яких країн характерний високий рівень безпеки, а для яких країн низький (рис. 1.6).

Рисунок 1.6 – Карта країн світу із визначеним національним індексом кібербезпеки

Джерело дослідження: побудовано автором на основі [10]

Аналізуючи дані, представлені на рисунку 1.6, можна сказати, що держави, які відносяться до розвинутих, а саме країни Європи, США, Канада, Австралія та інші, мають високі значення національного індексу кібербезпеки. Хоча, якщо порівнювати країни, що розвиваються, наприклад, Україна, яка має індекс, рівний 64, та розвинуту країну Австралію з індексом 60, то можна дійти висновку, що рівень безпеки в Україні вищий. Також цей показник у України є вищим у порівнянні з такими розвинутими країнами, як Канада (57), Швеція (57), Норвегія (62), Японія (62). Це характерно й для Малайзії, Росії, Індії та ряду інших країн, що розвиваються, тобто за рівнем національного індексу кібербезпеки вони випереджають ряд розвинутих країн. Можна виділити й Нігерію, показник якої дорівнює 55, тобто за рівнем кібербезпеки дана країна наздоганяє Канаду та Швецію. Що стосується країн, які є найменш розвинутими, то вони мають доволі низькі показники кібербезпеки. Тобто візуальний аналіз нам дозволив зробити висновок, що в основному країни, які є розвинутими мають дійсно високі показники національного рівня кібербезпеки, що говорить про її високий рівень в цілому. Частина країн, які вважаються тими, що розвиваються, також мають високий рівень кібербезпеки. Можна попередньо прийняти нашу гіпотезу щодо існування впливу рівня економіко-соціо-політичного розвитку країн на рівень інформаційної безпеки країни.

Для подальшого підтвердження гіпотези проведемо канонічний аналіз, який дозволить нам математично прийняти або відхилити висунуту гіпотезу. Даний інструмент дозволяє досліджувати залежності між двома множинами змінних та виявляти зв’язки між ними, що дозволить оцінити ступінь впливу однієї множини на іншу та обґрунтувати її статистичну значимість [11, с. 185].

Для проведення дослідження було обрано ряд показників для 159 країн світу. Їх вибір здійснювався, виходячи з того, яким чином дані індикатори відображають розвиток країни: економічний, або соціальний, або політичний. Так, базу даних сформували індикатори економічного розвитку за 2018 рік, а саме [12]: ВВП на душу населення (у поточних доларах США); загальнодержавні

витрати на кінцеве споживання (% від ВВП); чисті портфельні інвестиції (платіжний баланс, у поточних доларах США); загальний рівень безробіття (% від загальної робочої сили); інфляція, дефлятор ВВП (річний у %); загальні резерви (включаючи золото, у поточних доларах США); сальдо поточного рахунку (платіжний баланс, у поточних доларах США); оплачувані та наймані працівники (% від загальної кількості зайнятих); індекс GINI; експорт товарів та послуг (% від ВВП); високотехнологічний експорт (% від промислового експорту); запаси зовнішньої заборгованості, загальна (погашена та непогашена заборгованість, у поточних доларах США); чистий приплив прямих іноземних інвестицій (платіжний баланс, у поточних доларах США); ВВП (поточні долари США); приріст ВВП (річний у %); ВНД на душу населення, за паритетом купівельної здатності (у поточних міжнародних доларах); ВНД, за паритетом купівельної здатності (у поточних міжнародних доларах); валовий капітал (% від ВВП); імпорт товарів та послуг (% від ВВП); промисловість, включаючи будівництво, додана вартість (% від ВВП); дохід, без урахування грантів (% від ВВП); податкові надходження (% від ВВП).

Також було обрано індикатори, які характеризують соціо-політичний рівень розвитку країни [12]: оцінка контролю корупції; оцінка ефективності уряду; оцінка політичної стабільності та відсутності насильства / тероризму; оцінка якості регуляторів; оцінка верховенства права; оцінка потужності статистичної системи країни; ймовірна тривалість життя; кількість підписок на послуги мобільного зв'язку (на 100 осіб); кількість осіб, які користуються Інтернетом (% від населення країни); кількість захищених Інтернет-серверів (на 1 мільйон людей); плата за використання інтелектуальної власності, платежі (BoP, поточні долари США); збори за використання інтелектуальної власності, квитанції (BoP, поточні долари США); патентні заявки, нерезиденти; патентні заявки, резиденти; статті науково-технічних журналів.

На першому кроці було проведено кореляційний аналіз у аналітичному пакеті “STATISTICA” між обраними соціо-економіко-політичними показниками

розвитку країн та складовими індикатора національної кібербезпеки. Даний аналіз дозволив нам вибрати саме ті показники, між якими існує статистичний зв'язок. Як правило, на практиці пріоритет надається тільки тим показникам, між якими існує тісний зв'язок, але нами було враховано всі показники, які мали хоча б, як мінімум, слабкий зв'язок, тобто значення коефіцієнта кореляції для них перевищувало рівень 0,3. Це було зроблено з метою визначення всього набору показників, які мають хоча б якійсь зв'язок з інформаційною безпекою. В результаті було обрано тільки 19 показників соціо-економіко-політичного розвитку та 12 складових національного індикатору кібербезпеки.

На наступному кроці було проведено канонічний аналіз, мета якого полягає у визначенні лінійних залежностей між групами змінних, що дозволяє оцінити вплив однієї групи факторів на іншу та навпаки. Загальну ідею аналізу зобразимо у вигляді наступних рівнянь (формула 1.1):

$$Y = a_1 y_1 + a_2 y_2 + \cdots + a_{12} y_{12};\ X = b_1 x_1 + b_2 x_2 + \cdots + b_{19} x_{19}, \qquad (1.1)$$

де $y_1, y_2, \dots, y_{12}$ – множина змінних, які відображають складові національного індексу кібербезпеки;

$x_1, x_2, \dots, x_{19}$ – множина змінних, які відображають відібрані показники соціо-економіко-політичного розвитку країни;

Y та X – зважені суми змінних кожної множини, які є канонічними змінними та які визначають канонічний корень;

$a_1, a_2, \dots, a_{12}$; $b_1, b_2, \dots, b_{19}$ - вагові коефіцієнти, які розраховуються виходячи з максимальної корельованості обох множин.

В результаті виконання модуля канонічного аналізу у пакеті “STATISTICA” отримано підсумки, представлені на рисунку 1.7.

N=159	Canonical Analysis Summary (Data_Stat.sta) Canonical R: .89935 Chi²(228)=535.10 p=0.0000 Left Set	Right Set
No. of variables	12	19
Variance extracted	100.000%	74.8349%
Total redundancy	49.1399%	38.4118%
Variables: 1	1. Cyber Security Policy Development (7)	GDP per capita
2	2. Cyber Threat Analysis and Information (5)	General government expenditure
3	3. Education and Professional Development (9)	Life expectancy
4	4. Contribution to global cyber security (6)	Wage and salaried workers
5	5. Protection of digital services	Control of Corruption: Estimate
6	6. Protection of essential services	Government Effectiveness: Estimate
7	7. E-identification and trust services	Political Stability and Absence of Violence/Terrorism: Estimate
8	8. Protection of personal data	Regulatory Quality: Estimate
9	9. Cyber incidents response	Rule of Law: Estimate
10	10. Cyber crisis management	Exports of goods and services (% of GDP)
11	11. Fight against cybercrime	GNI per capita, PPP (current international $)
12	12. Military cyber operations	High-technology exports (% of manufactured exports)
13		Mobile cellular subscriptions (per 100 people)
14		Revenue, excluding grants (% of GDP)
15		Statistical Capacity score (Overall average)
16		Tax revenue (% of GDP)
17		Individuals using the Internet (% of population)
18		Secure Internet servers (per 1 million people)
19		Charges for the use of intellectual property, payments (BoP, current US$)

Рисунок 1.7 – Підсумки канонічного аналізу

З рисунку 1.7 можна побачити, що значення канонічної кореляції R = 0,89935, тобто між множиною відібраних соціо-економіко-політичних факторів та складових індексу кібербезпеки існує сильний кореляційний зв'язок. Як результат, збільшення впливу соціо-економіко-політичних факторів викликає підвищення рівня кібербезпеки країни та навпаки, посилення рівня кібербезпеки позитивно впливає на соціо-економіко-політичний розвиток країни. Значимість коефіцієнта кореляції підтверджує високе значення критерію Пірсона ($\chi^2 =$ 535,10), рівень значущості якого не перевищує 0,05 (p = 0,0000). Також можна побачити, що значення надмірності для лівої множини, яка відповідає складовим показника кібербезпеки, дорівнює 49,1399%, тобто змінні правої множини, які відповідають обраним індикаторам соціо-економіко-політичного розвитку країни, на 49,1399% пояснюють мінливість показників кібербезпеки, що є досить високим показником. В свою чергу, фактори кібербезпеки на 38,4118% пояснюють мінливість факторів соціо-економіко-політичного розвитку країни, тобто приблизно на 40% розвиток країни залежить також від рівня захищеності інформаційного та кібернетичного простору держави, що є досить значним для такої специфічної сфери, як інформаційна безпека.

Для подальшого аналізу необхідно обрати ті канонічні корені, які є статистично значущими. Результат отриманих коренів та перевірки їх статистичної значущості представлений на рисунку 1.8.

	Chi-Square Tests with Successive Roots Removed (Data_Stat.sta)					
Root Removed	**Canonicl R**	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0.899347	0.808825	535.1017	228	0.000000	0.023091
1	0.688300	0.473757	300.1535	198	0.000004	0.120783
2	0.576003	0.331780	208.9906	170	0.022707	0.229520
3	0.499428	0.249428	151.7451	144	0.313391	0.343480
4	0.472961	0.223692	111.0024	120	0.709467	0.457624
5	0.431163	0.185902	75.0473	98	0.958868	0.589487
6	0.322475	0.103990	45.8415	78	0.998612	0.724099
7	0.280212	0.078519	30.2494	60	0.999520	0.808137
8	0.209031	0.043694	18.6377	44	0.999719	0.876998
9	0.205652	0.042293	12.2935	30	0.998235	0.917068
10	0.162657	0.026457	6.1572	18	0.995513	0.957566
11	0.128105	0.016411	2.3497	8	0.968367	0.983589

Рисунок 1.8 – Оцінка статистичної значущості канонічних коренів

З рисунку 1.8 визначаємо, що Хі-квадрат у першому рядку, який відповідає аналізу без видалення коренів, є статистично значущим ($p < 0,05$), тому хоча б один канонічний корень є також статистично значущим. При видаленні першого найбільш значущого кореня (другий рядок таблиці на рисунку 1.8) отримали, що інші корені, які залишилися, є також значущими. Процедуру повторюємо доти, доки $p > 0,05$. В результаті отримали три статистично значущих корені, тобто доцільно розглядати три пари канонічних змінних. Але для отримання достовірних оцінок навантажень канонічних факторів для трьох пар канонічних змінних, необхідно мати вибірку, яка буде перевищувати в 40-60 раз кількість початкових даних [11, с. 190]. Тому приймаємо рішення, що будемо розглядати тільки перший найбільш значущий корень. Для підтвердження своїх висновків визначимо факторну структуру та надмірність (рис. 1.9-1.10).

Root	Factor Structure, left set (Data_Stat.sta)											
Variable	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8	Root 9	Root 10	Root 11	Root 12
1. Cyber Security Policy Development (7)	0.760024	0.002491	-0.186045	0.051609	-0.238320	-0.049832	-0.221542	-0.234207	0.021718	-0.335502	0.110512	-0.310840
2. Cyber Threat Analysis and Information (5)	0.804363	0.223792	-0.221587	0.151369	-0.142565	0.015762	-0.072058	0.318598	0.091062	0.196997	-0.132340	-0.197535
3. Education and Professional Development (9)	0.829012	-0.085878	0.070746	-0.187170	-0.166473	-0.178946	0.150962	0.173048	0.169616	-0.206811	-0.061250	0.278504
4. Contribution to global cyber security (6)	0.687848	0.309192	-0.028693	-0.335910	0.049708	-0.090566	-0.102833	-0.450301	0.170550	0.245427	-0.061554	-0.021849
5. Protection of digital services	0.481421	0.564479	0.326512	0.240932	-0.038570	-0.172479	0.071828	0.019601	0.272460	-0.177525	0.377135	0.013407
6. Protection of essential services	0.640548	0.376292	0.366621	-0.073345	-0.242679	0.251753	0.249293	-0.008182	-0.111853	-0.259545	-0.063670	-0.199741
7. E-identification and trust services	0.693371	-0.233652	0.395539	0.346565	-0.101198	0.219727	-0.066441	-0.115610	0.309802	0.023597	-0.073443	0.099283
8. Protection of personal data	0.677602	-0.036897	0.190406	0.201487	0.560966	-0.026191	-0.112577	-0.159802	-0.294084	-0.109574	0.024057	0.099966
9. Cyber incidents response	0.616932	-0.004646	0.156909	0.098019	-0.481988	-0.172326	0.045943	-0.080467	-0.205076	0.281689	0.405317	0.169895
10. Cyber crisis management	0.690835	-0.005328	0.244479	-0.295109	-0.074948	0.083761	-0.379324	0.326203	0.036145	0.095224	0.264116	-0.181110
11. Fight against cybercrime	0.795608	-0.300298	0.119870	-0.006050	0.090516	-0.163109	0.250698	-0.110302	0.105014	0.079520	0.098333	-0.354386
12. Military cyber operations	0.659978	0.026670	-0.313077	-0.103899	0.004385	0.474282	0.283758	-0.028016	0.216443	-0.045708	0.305308	0.080560

Рисунок 1.9 – Факторна структура для складових національної кібербезпеки

Root	Factor Structure, right set (Data_Stat.sta)											
Variable	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8	Root 9	Root 10	Root 11	Root 12
GDP per capita	0.690718	0.287945	-0.094678	-0.107102	0.053564	-0.007716	0.134322	-0.125077	-0.062143	-0.191470	-0.212388	0.042324
General government expenditure	0.582425	0.012476	0.040691	0.122926	0.301848	0.057419	-0.083220	0.333374	0.230369	-0.176095	0.182320	0.515583
Life expectancy	0.560505	-0.073121	0.092636	-0.003275	-0.045289	-0.214084	-0.002089	-0.042246	0.210654	0.256902	0.386897	0.154499
Wage and salaried workers	0.689980	-0.055039	0.015387	0.035455	-0.141280	-0.056756	-0.125431	0.015432	0.331435	-0.227224	0.157316	-0.001677
Control of Corruption: Estimate	0.670031	0.287895	-0.102873	-0.225532	0.218710	0.154650	0.074692	0.071763	-0.143386	-0.011767	0.071138	-0.042668
Government Effectiveness: Estimate	0.828089	0.155910	-0.005329	-0.191045	0.113098	-0.045128	0.119633	0.097483	-0.107037	-0.077001	0.064634	-0.122560
Political Stability and Absence of Violence/Terrorism: Estimate	0.386819	0.291094	0.076111	-0.046471	0.206451	0.108845	0.144648	0.188094	0.004943	0.004702	0.102241	-0.393756
Regulatory Quality: Estimate	0.857579	0.086692	0.056519	-0.143422	0.321309	0.005298	0.100129	-0.041911	-0.081142	-0.009868	-0.021731	-0.157498
Rule of Law: Estimate	0.751873	0.300340	-0.058753	-0.210310	0.184472	-0.007508	0.002279	0.021636	-0.111098	-0.016052	0.024833	-0.168624
Exports of goods and services (% of GDP)	0.422173	0.302194	0.706982	0.061401	0.078238	0.034840	-0.091449	-0.043332	-0.096989	-0.217581	-0.084025	0.005929
GNI per capita, PPP (current international $)	0.778433	0.178293	0.027060	-0.146257	0.002825	0.065960	0.074127	0.080053	-0.114887	-0.202721	-0.117215	-0.042700
High-technology exports (% of manufactured exports)	0.533411	0.270292	0.166244	-0.275034	-0.012061	0.037870	0.046638	-0.016499	-0.029068	0.032581	-0.326975	0.060067
Mobile cellular subscriptions (per 100 people)	0.526399	-0.278181	0.250180	-0.089930	-0.041404	0.023736	0.057854	0.078482	-0.036813	0.166880	-0.175414	0.294128
Revenue, excluding grants (% of GDP)	0.643730	0.081836	0.122554	0.464898	0.097816	0.155986	0.309381	-0.082375	-0.054656	-0.092901	0.114859	0.082283
Statistical Capacity score (Overall average)	-0.408921	-0.592820	0.198385	0.052162	-0.084049	0.242478	-0.165242	-0.170750	-0.019052	0.070653	0.038622	-0.090867
Tax revenue (% of GDP)	0.520408	0.027981	0.075796	0.422743	0.264763	0.021191	0.317097	-0.149851	-0.212226	-0.150837	0.136300	0.148818
Individuals using the Internet (% of population)	0.775450	0.060895	0.247898	0.270714	-0.302487	0.026021	-0.196339	0.043057	-0.112618	0.054117	-0.014353	0.091492
Secure Internet servers (per 1 million people)	0.396156	0.382797	-0.107892	0.048519	0.188674	0.221766	-0.018269	-0.242228	-0.341539	-0.064963	0.167762	0.157743
Charges for the use of intellectual property, payments (BoP, current US$)	0.334831	0.253151	0.071409	-0.520211	-0.132963	0.067005	0.350825	-0.413787	0.066276	-0.225246	0.196509	0.161827

Рисунок 1.10 – Факторна структура для факторів розвитку країни

Найбільші факторні навантаження мають показники, що відповідають першому кореню, як для лівої, так й для правої множини. Оскільки факторні навантаження представляють собою кореляції між показниками множини, то показники національної безпеки демонструють середній та вище середнього кореляційний зв'язок. Що стосується факторів розвитку, то між ними зустрічаються ті, які демонструють слабкий зв'язок. Але оскільки нам важливо виявити показники, які мають будь-який рівень зв’язку, то будемо мати на увазі, що оцінка політичної стабільності та відсутності насильства / тероризму, експорт товарів та послуг, оцінка потужності статистичної системи країни, кількість

захищених Інтернет-серверів, платежі за використання інтелектуальної власності, чинять слабкий вплив на рівень національної кібербезпеки.

Проаналізуємо частки та надмірності дисперсії (рис. 1.11-1.12).

Variance Extracted (Proportions), left set (Data_Stat.sta)

Root Factor	Variance extractd	Reddncy.
Root 1	0.491119	0.397229
Root 2	0.063349	0.030012
Root 3	0.060004	0.019908
Root 4	0.042092	0.010499
Root 5	0.061563	0.013771
Root 6	0.039442	0.007332
Root 7	0.038450	0.003998
Root 8	0.046189	0.003627
Root 9	0.036422	0.001591
Root 10	0.038554	0.001631
Root 11	0.043870	0.001161
Root 12	0.038946	0.000639

Рисунок 1.11 – Дисперсія та надмірність для складових національної кібербезпеки

Variance Extracted (Proportions), right set (Data_Stat.sta)

Root Variable	Variance extractd	Reddncy.
Root 1	0.382117	0.309065
Root 2	0.064626	0.030617
Root 3	0.040610	0.013474
Root 4	0.054468	0.013586
Root 5	0.031369	0.007017
Root 6	0.012409	0.002307
Root 7	0.026130	0.002717
Root 8	0.025575	0.002008
Root 9	0.024686	0.001079
Root 10	0.021229	0.000898
Root 11	0.028015	0.000741
Root 12	0.037116	0.000609

Рисунок 1.12 – Дисперсія та надмірність для факторів розвитку країни

У випадку аналізу складових національної кібербезпеки 100% дисперсії будуть пояснювати усі вилучені корені (рис. 1.11), у випадку факторів розвитку країни – тільки 74,8% (рис. 1.12). Перший канонічний корень вилучає 49,1119% дисперсії із складових національної кібербезпеки та 38,2117% дисперсії з факторів розвитку країни, тобто пояснює 49,1119% та 38,2117% зміни рівня національної кібербезпеки та рівня соціо-економіко-політичного розвитку. Інші корені, хоча ми не прийматимемо їх до уваги, пояснюють від 2 до 6% змін, що є незначним. З огляду на надмірність, 39,7229% факторів розвитку пояснюють зміни показників лівої множини, тобто складових національної кібербезпеки (рис. 1.11). 30,9065% факторів національної кібербезпеки пояснюють зміни, що пов’язані із розвитком країни. Як результат, фактори розвитку є більш інформативними для передбачення рівня національної кібербезпеки країни.

Для подальшого аналізу визначимо канонічні ваги, які є коефіцієнтами регресійних рівнянь, де канонічні змінні є відповідними відкликами (рис. 1.13-1.14).

Variable	Canonical Weights, left set (Data_Stat.sta)											
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8	Root 9	Root 10	Root 11	Root 12
1. Cyber Security Policy Development (7)	0.093381	-0.185643	-0.532721	0.210320	-0.455671	-0.145498	-0.668439	-0.502856	-0.058467	-0.921333	0.147364	-0.365770
2. Cyber Threat Analysis and Information (5)	0.276326	0.439113	-0.584769	0.645837	-0.017059	-0.068688	-0.005700	0.677231	-0.093292	0.594011	-0.628846	-0.216963
3. Education and Professional Development (9)	0.256820	-0.243435	-0.077787	-0.511477	-0.129206	-0.645390	0.224682	0.425462	0.208718	-0.634045	-0.422408	0.858202
4. Contribution to global cyber security (6)	0.107176	0.440184	0.010013	-0.583614	0.095860	-0.096554	-0.219510	-0.780383	0.317228	0.545809	-0.361198	0.153747
5. Protection of digital services	-0.094643	0.609075	0.196664	0.373903	0.271319	-0.472612	0.080767	0.129610	0.674538	-0.235680	0.644233	-0.039081
6. Protection of essential services	0.058188	0.392554	0.564118	-0.259782	-0.336548	0.554353	0.516767	-0.049513	-0.658640	-0.244868	-0.487915	-0.352386
7. E-identification and trust services	0.050683	-0.385354	0.517350	0.574200	-0.251821	0.557280	-0.385968	-0.311036	0.663148	0.177002	-0.388059	0.237021
8. Protection of personal data	0.280400	0.059237	-0.014170	0.286797	0.792022	0.035162	-0.174000	-0.026077	-0.804609	-0.141437	0.015409	0.374874
9. Cyber incidents response	0.098364	-0.082615	0.004520	0.225636	-0.624973	-0.148112	0.127089	-0.216619	-0.744401	0.538478	0.482879	0.388610
10. Cyber crisis management	0.028405	-0.169556	0.449290	-0.678455	0.141893	0.284436	-0.754298	0.550210	0.076163	0.081742	0.513800	-0.245047
11. Fight against cybercrime	0.071589	-0.551104	0.212369	-0.077036	0.332967	-0.528362	0.865639	-0.006552	0.248701	0.297143	0.221630	-0.976421
12. Military cyber operations	0.100034	-0.036566	-0.537026	-0.104790	0.222332	0.825385	0.374173	-0.025889	0.181149	-0.013681	0.642870	0.254344

Рисунок 1.13 – Канонічні ваги для складових національної кібербезпеки

Variable	Canonical Weights, right set (Data_Stat.sta)											
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8	Root 9	Root 10	Root 11	Root 12
GDP per capita	-0.033104	-0.138295	-0.614914	0.653993	-0.21975	-0.33937	0.13634	-1.24871	0.94691	-0.01991	-1.61061	0.440867
General government expenditure	0.090716	-0.054161	-0.008651	-0.034255	0.45169	0.06064	-0.29111	0.55164	0.48676	-0.42355	0.02163	0.633128
Life expectancy	0.070309	-0.128029	0.196566	-0.113723	0.03148	-0.31791	0.06694	-0.12624	0.10339	0.83946	0.45889	0.140092
Wage and salaried workers	0.028595	0.016751	-0.389475	0.184296	-0.05490	0.09868	-0.65901	-0.51765	0.73307	-0.70711	0.19387	-0.278929
Control of Corruption: Estimate	-0.399981	0.020568	-0.051804	-0.538909	0.21090	2.36121	0.10754	0.19747	-0.75354	0.66515	0.49227	0.858484
Government Effectiveness: Estimate	0.339411	-0.387680	-0.341282	-0.113949	-1.45118	-1.41698	1.33163	1.26795	-0.90196	-1.00150	0.50313	-0.585369
Political Stability and Absence of Violence/Terrorism: Estimate	-0.285751	0.132452	0.139113	0.415708	0.17612	0.14029	0.41484	0.29026	0.49167	0.23548	0.01588	-0.475395
Regulatory Quality: Estimate	0.532497	-0.646778	0.240597	0.304070	2.07964	0.41011	0.24623	-0.80422	0.56443	0.88479	-0.30093	-0.861717
Rule of Law: Estimate	0.253941	0.914662	-0.036946	-0.708188	-0.40529	-1.43133	-2.12080	-0.68596	0.40366	-0.18551	-0.05838	0.007632
Exports of goods and services (% of GDP)	-0.191654	0.353281	1.079455	-0.080992	0.14497	-0.12664	-0.23008	-0.12131	-0.03218	-0.29435	0.04612	0.020324
GNI per capita, PPP (current international $)	0.210886	-0.734044	0.204656	-0.665747	-0.03172	0.67169	0.09478	1.36928	-1.22552	-0.89858	0.37390	-0.371983
High-technology exports (% of manufactured exports)	0.058820	0.398051	-0.099102	-0.216849	0.05722	0.16519	-0.07188	0.13917	0.15234	0.13136	-0.55684	0.100973
Mobile cellular subscriptions (per 100 people)	-0.033339	-0.192015	0.207310	-0.131576	-0.19937	-0.17762	0.28216	-0.04035	0.10626	0.65356	-0.40441	0.488864
Revenue, excluding grants (% of GDP)	0.524632	0.682581	0.044147	0.567882	-0.82976	1.51154	1.10092	0.11973	1.54177	0.82381	-0.28979	-0.591056
Statistical Capacity score (Overall average)	0.060800	-0.836141	0.019507	-0.250046	-0.16382	0.68230	-0.52732	-0.39786	-0.05436	-0.41536	-0.08264	-0.134874
Tax revenue (% of GDP)	-0.448721	-0.601972	-0.002488	0.044858	0.71068	-1.39675	-0.28469	-0.24705	-1.71874	-1.09968	0.42494	0.708018
Individuals using the Internet (% of population)	0.205069	-0.022148	0.064643	0.466014	-0.52917	0.01446	-0.41923	-0.02762	-0.62348	0.32075	0.13718	0.199173
Secure Internet servers (per 1 million people)	0.087222	0.364151	-0.423961	0.315806	0.12995	0.24235	-0.37843	-0.38352	-0.20223	0.16395	0.29515	-0.115129
Charges for the use of intellectual property, payments (BoP, current US$)	-0.027525	0.078019	0.300656	-0.505085	-0.24913	0.09657	0.45620	-0.37488	0.13878	-0.24141	0.49560	0.254321

Рисунок 1.14 – Канонічні ваги для факторів розвитку країни

Так, значення канонічних вагів дозволяє визначити вклад кожного показника у формування значень канонічних змінних. В національну кібербезпеку вноситимуть найбільший вклад (рис. 1.13): захист персональних даних; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки. Найменший вклад здійснюватимуть: організація захисту основних послуг; електронна ідентифікація та послуги довіри; кіберрегулювання кризи. Що стосується факторів розвитку, то найбільший вклад втілюватимуть (рис. 1.14): оцінка якості регуляторів; дохід, без урахування грантів; податкові надходження; найменший вклад – оплачувані та наймані працівники; платежі за використання інтелектуальної власності; ВВП на душу

населення; кількість підписок на послуги мобільного зв'язку. При цьому треба враховувати знак значення показника. Якщо вага має знак «+», то із збільшенням фактору значення кореня збільшується, якщо «–», навпаки, значення кореня зменшується. Наприклад, якщо платежі за використання інтелектуальної власності будуть збільшуватися, то це буде зменшувати внесок даного вкладу у значення кореня.

Значення канонічних вагів дозволило нам визначити рівняння регресії для канонічних змінних лівого та правого множин (формула 1.2):

$$\begin{aligned} Y\ (1\ \text{корень}) = {} & 0{,}0934\ y_1 + 0{,}2763\ y_2 + 0{,}2568\ y_3 + 0{,}1072\ y_4 - 0{,}0946\ y_5 \\ & + 0{,}0582\ y_6 + 0{,}0507\ y_7 + 0{,}2804\ y_8 + 0{,}0984\ y_9 + 0{,}0284\ y_{10} \\ & + 0{,}0716\ y_{11} + 0{,}1000\ y_{12}, \\ X\ (1\ \text{корень}) = {} & -0{,}0331\ x_1 + 0{,}0907\ x_2 + 0{,}0703\ x_3 + 0{,}0286\ x_4 - 0{,}4000\ x_5 \\ & + 0{,}3394\ x_6 - 0{,}2858\ x_7 + 0{,}5324\ x_8 + 0{,}2539\ x_9 - 0{,}1917\ x_{10} \\ & + 0{,}2109\ x_{11} + 0{,}0588\ x_{12} - 0{,}0334\ x_{13} + 0{,}5246\ x_{14} \\ & + 0{,}0608\ x_{15} - 0{,}4487\ x_{16} + 0{,}2051\ x_{17} + 0{,}0872\ x_{18} \\ & - 0{,}0275\ x_{19} \end{aligned} \quad (1.2)$$

Якщо є потреба у визначенні для кожної країни значення канонічних змінних, то необхідно підставити в отриманні рівняння 1.2 значення факторів розвитку та складових національного індикатору кібербезпеки. Це дозволить знайти зважену суму факторів з урахуванням впливу множин один на одну.

На наступному кроці побудуємо діаграму розсіювання канонічних значень для першої пари канонічних коренів (рис. 1.15), в якій горизонтальна вісь – це складові національного індексу кібербезпеки, а вертикальна – показники соціо-економіко-політичного розвитку. На діаграмі 1.15 можна побачити, що скупчення спостережень є характерним для лінійної залежності, при цьому графік не містить значних викидів. Це свідчить про те, що між складовими національної кібербезпеки та факторами соціо-економіко-політичного розвитку є досить тісний зв'язок, який говорить про те, що рівень національної кібербезпеки, а в нашому

випадку інформаційної безпеки, залежить від рівня розвитку країни, при цьому рівень безпеки може також впливати й на розвиток країни.

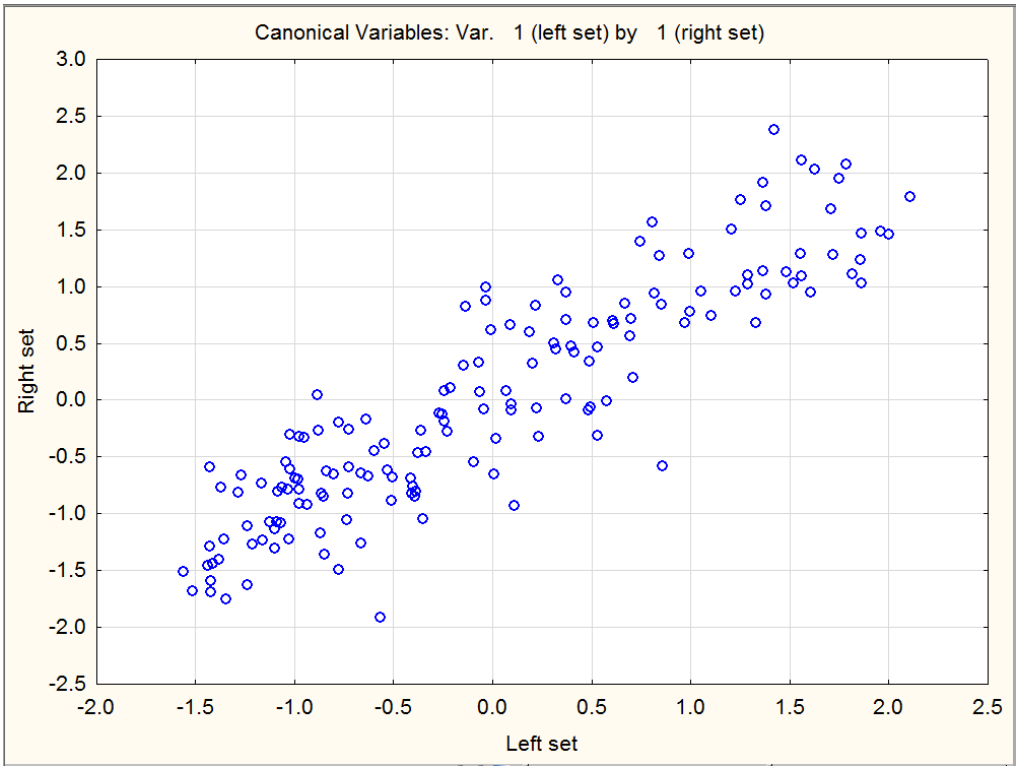


Рисунок 1.15 – Діаграма розсіювання канонічних значень

Виходячи з результатів проведеного дослідження, можна прийняти гіпотезу щодо обумовленості ефективності системи інформаційної безпеки факторами соціально-економічного розвитку країни. Дану гіпотезу було підтверджено візуальним аналізом карти країн світу, розподілених за національним індексом кібербезпеки. Даний аналіз підтвердив, що країни, які відносяться до розвинутих, мають найвище значення національного індексу кібербезпеки. Найменш розвинуті країни мають найнижчі значення індексу. В результаті проведеного канонічного аналізу було визначено, що приблизно 49% множини складових показника кібербезпеки пояснюються факторами соціо-економіко-політичного розвитку. Оскільки дані фактори оцінюють спроможність країни протистояти різним кіберзагрозам, то у країн із високим економічним потенціалом збільшуються можливості їм протидіяти, а також зростає фінансова спроможність для організації додаткових заходів, залучення більш сучасних технологій,

кваліфікованих фахівців. Але з іншого боку, саме у таких країнах підвищується ризик кібератак, інформаційного тероризму та кібершахрайства. Тому треба провести додаткове дослідження щодо аналізу впливу рівня кіберзагроз на різні країни світу.

Також було визначено, що 38% множини факторів розвитку країни пояснюється за рахунок складових національної кібербезпеки. Тобто підвищення рівня інформаційної безпеки в цілому та кібербезпеки зокрема сприятиме розвитку країни в частині соціального, економічного чи політичного розвитку. Чим вище рівень захищеності персональних даним, тим вище довіра населення до держави та різних інститутів. Якщо це фінансові дані людини, тим вище надійність банківської системи та менше втрати від кібершахраїв.

Отримані в роботі результати сприятимуть виробленню ряду стратегічних заходів саме в тих напрямках, де цей зв'язок є тіснішим. Як наслідок, це призведе до посилення інститутів безпеки, впровадження нових методів та заходів безпеки, що, в свою чергу, позитивно впливатиме на політичну стабільність в країні, соціальну захищеність населення від кібершахрайств, зниження збитків економіки держави та суб’єктів господарювання від незаконного використання ресурсів. Впровадження спеціалізованих програм навчання, створення ефективних інститутів для боротьби з кібертероризмом, розробка відповідних норм законодавства, які підвищують відповідальність за кіберзлочини, впровадження потужних аналітичних систем та інше – все це напрямки впливу на успішний розвиток будь-якої країни.

1.3. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку

Сьогодні дуже важко уявити різні сфери діяльності суспільства без використання комп’ютерних та інформаційних технологій. Особливо це відчувається в бізнесі, політиці, повсякденному житті людини. Процесу

інформатизації та комп’ютеризації також сприяють й результати четвертої промислової революції, яка впливає на підвищення можливостей кіберфізичних систем для вирішення потреб країни, суспільства, суб’єктів господарювання, окремої людини. Але такий стрімкий розвиток призводить також й до того, що новітні технології стають інструментами для незаконного збагачення різного роду злочинців. Це проявляється у збільшенні випадків хакерських атак на бізнес підприємств з метою отримання фінансової інформації. Також збільшується кількість кібер-шахраїв, які застосовують програмно-технологічні можливості для ошукування населення. Це може бути й інформаційний вплив на суспільство із використанням соціальних мереж, що призводить до інформаційних війн та політичної дестабілізації у країні.

Перелічені факти є одними з видів загроз, які призводять до зниження ефективності інформаційної безпеки, як окремого суб’єкта, так й країни в цілому. Тому важливо розуміти, які проблеми в галузі інформаційної безпеки існують, що є фактором їх виникнення, та як його наслідки впливатимуть на рівень розвитку країни в цілому. Поняття інформаційної безпеки є комплексним, яке охоплює мікро- та макрорівень, а також включає різні її аспекти: правову, освітню, інституційну, програмно-технологічну та інші. Досліджуючи рівень інформаційної безпеки країни, слід також враховувати й ці аспекти. Варто зазначити, що фактори економічного, соціального та політичного розвитку країни також можуть впливати на рівень безпеки, оскільки країна із високими соціальними стандартами та рівнем життя запроваджує найбільш ефективні заходи безпеки. Таким чином, дослідження рівня інформаційної безпеки країн з урахуванням їх розвитку є актуальним та потребує системного вивчення.

Сучасними проблемами інформаційної безпеки займається широке коло закордонних та вітчизняних вчених. Загальні питання в цій сфері висвітлювали Е. Косевич [13], В. Кіріленко, Г. Алексєєв [14], А. Сінгх, М. Гупта [15], А. Ключніков, Л. Мура, Д. Скленар [16] та інші.

Ряд вчених досліджували специфічні сфери інформаційної безпеки. Так, М. Садігов, О. Кузьменко, Г. Яровенко вивчали питання застосування блокчейн-технологій в галузі кібербезпеки [17]. М. Дорош, М. Войцеховська, І. Бальченко досліджували підхід використання методу Fuzzy Logic для підвищення ефективності персонального захисту [18]. С. Шмітц та С. Пейп запропонували предметно-орієнтовану структура для для підтримки прийняття рішень з інформаційної безпеки [19]. Також можна виділити роботу С. Євсєєва, В. Алексієва, С. Балакірєва, Ю. Пелешка, О. Милова, О. Петрова, О. Раєвнєвої, Б. Томашевського, І. Тишика, О. Шматька, яка стосується розробки інформаційної системи захисту [20].

Незважаючи на велику кількість досліджень, є ряд питань, які слабо висвітлені у наукових працях та потребують уточнення. Серед них можна виділити проблему аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. Це пов’язано із тим, що в ряді країн не приділяється належна увага таким аспектам. Також більшість науковців спрямовують свої дослідження щодо удосконалення системи інформаційної безпеки для економічних суб’єктів, а макрорівень ототожнюють тільки з окремими сферами, такими як кібербезпека. Саме тому дане питання потребує подальшого вивчення.

Для проведення дослідження було обрано вхідні дані, які характеризують два аспекта: рівень інформаційної безпеки країни та рівень розвитку. З цією метою проведено дослідження офіційних джерел в галузі інформаційної безпеки, в результаті чого було виділено 5 основних показників, які характеризують її окремі сфери: Global Cybersecurity Index характеризує рівень кібербезпеки для країн-членів Міжнародного союзу електрозв’язку; National Cyber Security Index визначає рівень готовності країни протидіяти кіберзагрозам; ICT Development Index вимірює рівень розвитку інформаційних технологій в країні; Networked Readiness Index визначає ступінь технологічної готовності країни для застосування новітніх інформаційно-комунікаційних технологій в різних сферах; Digital Development Level характеризує рівень цифровізації країни [21]. Оскільки

на практиці не існує показника, який би вимірював рівень інформаційної безпеки, то поєднання наведених індексів можна використовувати для оцінки окремих її напрямків.

У якості показників розвитку було проаналізовано базу даних Світового банку, серед яких було виділено 37 індикаторів, для яких було зроблено припущення, що вони мають зв'язок із показниками безпеки. В результаті проведеного кореляційного аналізу було виділено 12 показників, для яких рівень їх статистичного зв’язку із показниками безпеки характеризується як тісний, тобто коефіцієнт кореляції перевищує 0,5 або -0,5. Таким чином, було відібрано: GDP per capita (current US$); Life expectancy; Wage and salaried workers, total (% of total employment); Control of Corruption: Estimate; Government Effectiveness: Estimate; Regulatory Quality: Estimate; Rule of Law: Estimate; GNI per capita, PPP (current international $); Mobile cellular subscriptions (per 100 people); Revenue, excluding grants (% of GDP); Individuals using the Internet (% of population); General government expenditure (% of GDP) [12].

Розрахунки проводилися для 159 країн світу. У якості розрахункового періоду було обрано 2018 рік. Це було зроблено, виходячи з повноти наявності даних для кожного з обраних показників.

Для того, щоб дані можна було піддавати подальшому аналізу, необхідно провести їх нормалізацію, оскільки кожен з відібраних показників має різні виміри та значення. З цією метою було обрано метод нелінійної нормалізації, оскільки він дозволяє отримати більш ефективні оцінки, ніж лінійна нормалізація, в межах [0, 1]. Дану процедуру було проведено за формулою 1.3:

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \tag{1.3}$$

де Z_{ij} – нормалізоване значення j-го показника 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.

Після проведення нормалізації вхідних даних, необхідно здійснити їх перевірку на якість, виявлення викидів, дублікатів та протиріч. Даний процес було проведено за допомогою аналітичної платформи Deductor Academic. В результаті аналізу якості даних було виявлено 3 викиди за індикатором «Life expectancy», що свідчить про необхідність коректування даних за цим показником. Але в цілому отриманий показник якості знаходиться в межах (0,7299; 0,9842), що говорить о високій якості початкового набору даних. Перевірка даних на наявність дублікатів та протиріч виявила, що вони відсутні у наборі даних. В результаті проведених перевірок було здійснено коректування тільки даних індикатора «Life expectancy», для чого було обрано розрахунок ймовірного значення для спостережень, які є викидами.

Після підготовки даних проведено аналіз рівня інформаційної безпеки країн з урахуванням їх розвитку, що здійснювалося із використанням самоорганізованих карт Кохонена на платформі Deductor Academic. Карти Кохонена представляють собою вид нейронної мережі з некерованим навчанням, яка проектує дані з багатовимірного простору у двовимірний. Даний інструментарій було розроблено фінським вченим Теуво Кохоненом у 1982 році [22].

В процесі побудови карти було експериментальним шляхом випробувано різні способи її побудови. В результаті було враховано наступні опції:

1) для усіх змінних було задано призначення «Вхідні», тільки змінну «Назва країни» було враховано, які «Інформаційне»;

2) розбиття даних на навчальну множину та тестову не проводилося з урахуванням того, що будь-який алгоритм кластеризації, в тому числі й карти Кохонена, є доволі суб'єктивним;

3) при налаштуванні параметрів карти було обрано розміри 24:18, оскільки стандартний розмір 16:12 не дозволив виявити всіх кластерів;

4) кількість епох було обрано 500 та рівень похибки для розпізнавання було обрано менше 0,05;

5) для визначення початкових вагів нейронів було обрано спосіб «З власних векторів», який дозволяє ініціалізувати початкові ваги нейронів значеннями підмножини гіперплощини, через яку проходять два власних вектори матриці коваріації вхідних значень вибірки. Результати з використанням цього способу виявилися кращими для матриці похибок квантування та матриці щільності квантування у порівнянні із способами «З навчальної множини» та «Випадковими значеннями»;

6) у якості функції сусідства було «Ступінчату», оскільки результати порівняння матриці похибок квантування та матриці щільності квантування для даної функції виявилися кращими ніж для функції «Гауссова»;

7) при порівнянні результатів автоматичного визначення кількості кластерів та ручного визначення, врешті-решт було обрано автоматичне визначення з рівнем значущості 0,5%. Кількість кластерів при ручному режимі виставлялося рівним 5, бо саме стільки кластерів було отримано при ручній перевірці з використанням методу k-means. Але результати автоматичного визначення виявилися кращими.

Після виконання процедур алгоритму побудови карт Кохонена отримано 7 кластерів та для кожного з відібраних показників побудовано карту. Результати представлені на рисунку 1.16. Також було виведено спеціальні карти, які дозволили зробити порівняння із іншими варіантами карт, побудованих для різних функцій сусідства та методів ініціалізації початкових вагів. Кінцевий

результат матриць помилок квантування, щільності попадання та відстаней представлено на рисунку 1.17.

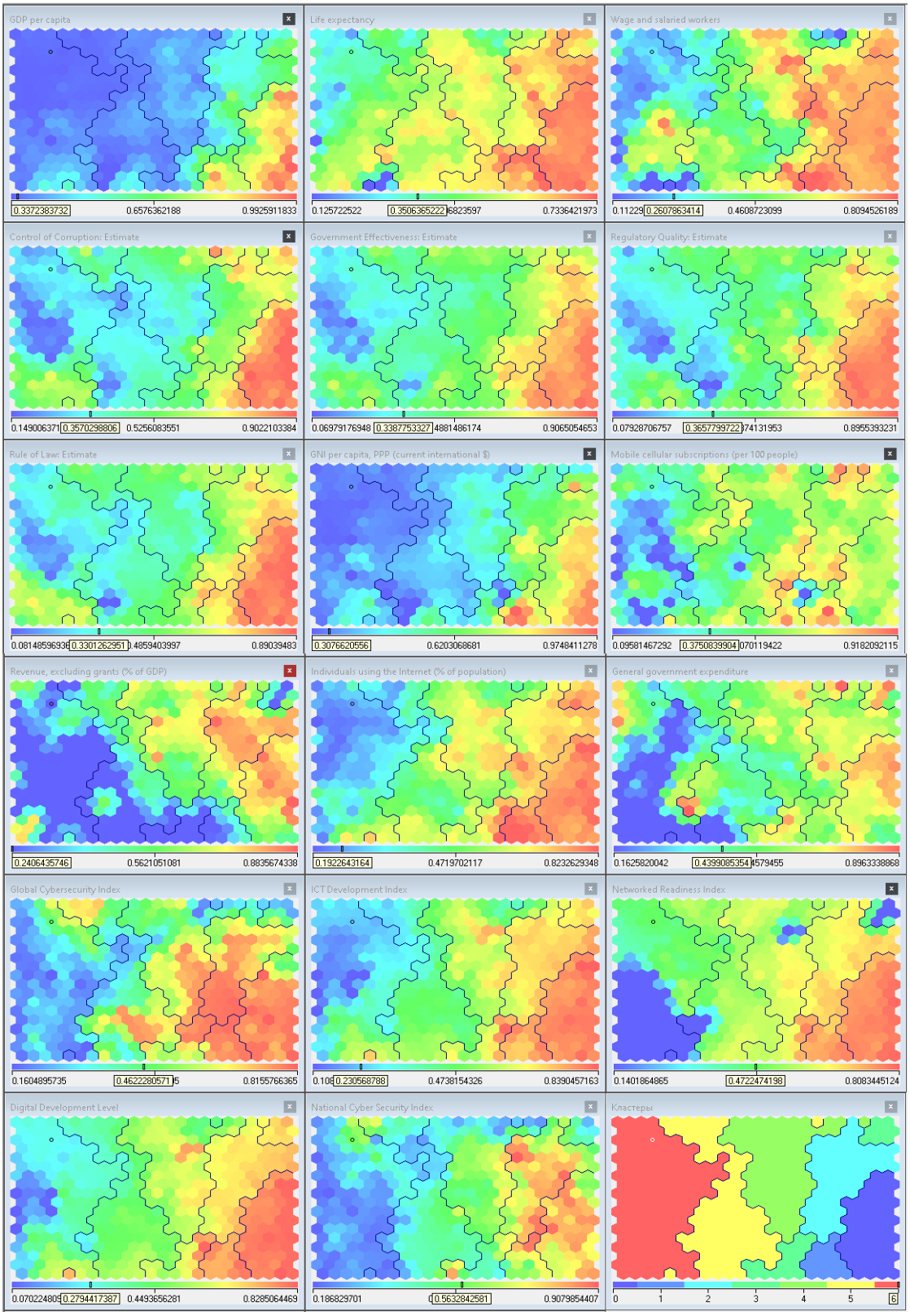


Рисунок 1.16 – Карти Кохонена показників інформаційної безпеки та розвитку

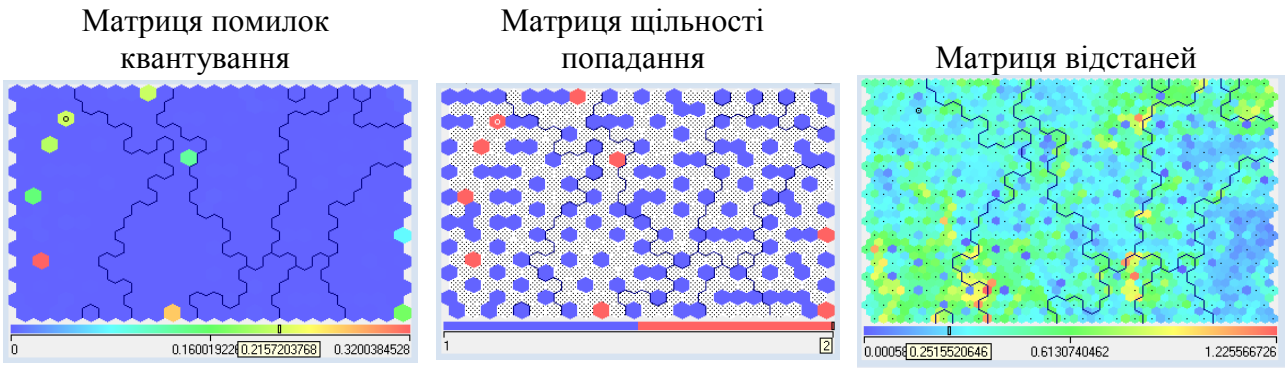


Рисунок 1.17 – Матриці помилок квантування, щільності попадання, відстаней

В процесі аналізу даних карт, було виявлено 16 країн, помилка квантування для яких перевищує 10%, що складає близько 10% від загальної кількості країн. Можна вважати, що це допустимий рівень відхилення для моделей кластеризації.

Так, до 0-го кластеру увійшла 21 країна: Австралія, Австрія, Бельгія, Великобританія, Данія, Естонія, Ізраїль, Ісландія, Ірландія, Канада, Люксембург, Нідерланди, Німеччина, Нова Зеландія, Норвегія, Сінгапур, США, Фінляндія, Франція, Швеція, Швейцарія. Даний кластер сформували розвинуті країни з потужним економічним потенціалом та високим рівнем інформаційної безпеки (див. рис. 1.16 та табл. 1.4). Тобто, при виникненні різного роду загроз інформаційній безпеці, ці країни зможуть швидше подолати наслідки інформаційної кризи. Також високий рівень їх безпеки говорить про те, що вони для системи безпеки застосовуються сучасні комп’ютерні технології та програмні засоби, які дозволяють їм швидко попереджати загрози.

Кластер 1 сформували 4 країни: Японія, Іспанія, Катар та Арабські Емірати. Вони мають також високі показники розвитку та інформаційної безпеки, які представлені у таблиці 1.4 та на рисунку 1.16. Але у порівнянні із країнами 0-го кластеру, країни 1-го кластеру мають рівень інформаційної безпеки значно нижчим, що проявляється у таких показниках, як ICT Development Index, Networked Readiness Index, Digital Development Level, National Cyber Security Index. Це говорить про те, що ймовірно є певні проблеми в системі інформаційної

безпеки даних країн, які потребують вирішення шляхом зміни стратегії інформаційної безпеки.

Таблиця 1.4

Середні значення показників у відповідності із профілем кластера

Назва показника	0 кластер	1 кластер	2 кластер	3 кластер	4 кластер	5 кластер	6 кластер
GDP per capita	58179,42	45353,09	19481,37	21216,71	7133,42	5018,98	2825,30
Life expectancy	81,85	81,36	78,12	77,29	73,82	69,87	63,90
Wage and salaried workers	87,59	92,34	82,18	84,82	63,97	49,86	32,86
Control of Corruption	1,81	0,98	0,43	0,46	-0,22	-0,40	-0,70
Government Effectiveness	1,64	1,19	0,71	0,50	0,01	-0,23	-0,87
Regulatory Quality	1,67	0,93	0,79	0,45	0,05	-0,40	-0,80
Rule of Law	1,68	1,01	0,64	0,40	-0,21	-0,44	-0,69
GNI per capita	56525,24	61757,50	32200,00	27756,25	16200,77	9450,69	5560,59
Mobile cellular subscriptions	122,33	151,94	128,07	111,12	124,97	106,35	58,79
Revenue, excluding grants	32,38	8,21	34,35	2,05	27,40	9,98	6,06
Individuals using the Internet	90,45	93,87	77,35	85,17	66,51	53,09	26,28
General government expenditure	19,72	16,85	17,42	19,46	16,26	11,57	6,26
Global Cyber-security Index	84,00	86,25	72,25	56,88	55,81	46,45	20,73
ICT Develop-ment Index	82,81	76,50	70,20	70,63	57,19	43,38	24,73
Networked Readiness Index	80,29	74,75	65,05	41,50	56,35	47,79	22,65
Digital Develop-ment Level	81,50	75,62	67,50	68,97	58,21	48,15	31,04
National Cyber Security Index	71,37	61,69	67,53	38,47	38,81	30,32	15,89

До 2-го кластеру увійшли 20 країн: Болгарія, Чилі, Хорватія, Кіпр, Чехія, Греція, Угорщина, Італія, Латвія, Литва, Малайзія, Мальта, Маврикій, Польща, Португалія, Румунія, Саудівська Аравія, Словакія, Словенія, Уругвай. Тобто сюди ввійшла частина розвинутих країн та ті, що розвиваються, які мають середні

показники розвитку, що говорить про їх достатні можливості подолання інформаційної кризи (див. рис. 1.16 та табл. 1.4). Але показники безпеки є нижчими у порівнянні із країнами 1-го кластеру, особливо це стосується ICT Development Index, Networked Readiness Index, Digital Development Level, Global Cyber Security Index. Проблемами інформаційної безпеки країн даного кластеру можуть бути ті, які пов'язані із правовими аспектами в даній сфері, рівнем організації освіти, недостатнім рівнем інвестування у новітні інформаційні технології, тощо.

До 3-го кластеру увійшли 8 країн: Багами, Бахрейн, Барбадос, Бруней, Південна Корея, Монтенегро, Оман, Сербія. Ряд показників розвитку країн даного кластеру перевищую показники країн 2-го кластеру, а саме: GDP per capita, Wage and salaried workers, Individuals using the Internet, General government expenditure (див. рис. 1.16 та табл. 1.4). Це свідчить про те, що ці країни знаходяться на стадії свого активного розвитку, як і країни 2-го кластеру. Але що стосується рівня інформаційної безпеки, то є проблеми в частині розвитку загальної стратегії інформаційної безпеки, про що свідчать низькі показники National Cyber Security Index, Global Cybersecurity Index та Networked Readiness Index. Окрім цього можна виділити проблему, пов'язану із низьким рівнем технологічної готовності країни до забезпечення надійної системи інформаційної безпеки.

До 4-го кластеру увійшли 26 країн: Албанія, Аргентина, Вірменія, Азербайджан, Беларусь, Боснія та Герцеговина, Ботсвана, Бразилія, Колумбія, Коста Ріка, Грузія, Ямайка, Йорданія, Казахстан, Мексика, Молдова, Монголія, Марокко, Намібія, Північна Македонія, Російська Федерація, Сейшели, Південна Африка, Тайланд, Туреччина, Україна. Частину країн даного кластеру сформували колишні республіки Радянського Союзу, а також ряд країн, які пережили становлення через минулі військові події. На даний момент їх усіх можна віднести до групи країн, що розвиваються, але вони мають ряд суттєвих проблем в економічній, соціальній та політичній сфері. Це підтверджується їх низькими значеннями показників розвитку у порівнянні із країнами попередніх

кластерів (див. рис. 1.16 та табл. 1.4). Що стосується їх стану інформаційної безпеки, то отримані показники безпеки свідчать про їх невисокий рівень. Тобто для розвитку сфери безпеки є потреба у залученні коштів для забезпечення змін не тільки на рівні стратегії інформаційної безпеки, але й на рівні її окремих складових – рівня технологічного розвитку, впровадження нових комп'ютерних програм, зміни стандартів, реформування законодавства, тощо.

До 5-го кластеру увійшли 29 країн: Алжир, Бутан, Болівія, Китай, Кот-д'Івуар, Куба, Домініканська республіка, Еквадор, Єгипет, Ель Сальвадор, Гана, Гватемала, Індія, Індонезія, Іран, Кенія, Киргизстан, Панама, Парагвай, Перу, Філіппіни, Руанда, Сан Кітс и Невіс, Сенегал, Тринідад і Тобаго, Туніс, Узбекистан, Венесуела, В'єтнам. Даний кластер сформували країни, які розвиваються, але мають низькі показники розвитку та низький рівень інформаційної безпеки (див. рис. 1.16 та табл. 1.4). Хоча до даного кластеру увійшли також й країни, які є новими індустріальними, - Індія, Індонезія, Китай, Філіппіни, але й вони мають досить низький рівень безпеки, що дозволило віднести їх до даної групи. Головними проблемами цього кластеру є передусім вирішення питань, пов'язаних із економічним розвитком, але ці країни мають відповідний потенціал для розвитку й інформаційної безпеки. Про це свідчить їх достатній рівень розвитку інформаційних технологій, цифровізації різних сфер та технологічної готовності.

До 6-го кластеру увійшла 51 країна, які відносяться до групи найменш розвинутих країн, що характеризуються дуже низькими показниками розвитку економіки, соціальної та політичної сфери (див. рис. 1.16 та табл. 1.4). Більшість країн даного кластеру – це країни Африки та Близького Сходу, де тривають озброєні конфлікти. Для таких країн першочерговим є подолання конфліктів у суспільстві та розвиток економіки. Для підвищення рівня їх інформаційної безпеки їм необхідно долучатися до програм та стартапів, які сприятимуть припливу інвестицій та зміни програмно-технічної інфраструктури на мікро-рівні, а потім й на рівні держави.

Проблеми, пов’язані із інформаційною безпекою, є досить актуальними у світі, тому дійсно є потреба у проведенні аналізу країн на предмет відповідності їх рівня розвитку рівню інформаційної безпеки. Це дозволить виділити не тільки групи країн, які слабко розвиваються у напрямку підвищення ефективності системи інформаційної безпеки, але й виділити ті сфери, які потребують додаткової уваги з боку відповідних державних органів, які займаються питаннями безпеки країни. Одним із дієвих інструментів для проведення такого аналізу є самоорганізовані карти Кохонена, які дозволяють не тільки зробити візуалізацію кластерів, але й детально проаналізувати отримані профілі у відповідності із досліджуваними показниками.

В результаті проведеного кластерного аналізу та побудови карт Кохонена для 159 країн світу із використанням показників розвитку та інформаційної безпеки, було отримано 7 кластерів країн. Кожна країна однієї групи характеризується близьким рівнем розвитку та інформаційної безпеки. Так, країни 0-го та 1-го кластеру характеризуються найвищими показниками розвитку та безпеки, країни 2-го кластеру мають показники вище середнього, країни 3-го кластеру можна охарактеризувати, як країни із середнім рівнем розвитку та інформаційної безпеки, країни 4-го кластеру відповідають нижче середнього рівню, рівень розвитку та інформаційної безпеки 5-го кластеру можна охарактеризувати як низький, 6-го – дуже низький. Експериментальне дослідження із зміною різних опцій налаштувань нейронної мережі та аналізом матриць помилок квантування, щільності попадання та відстаней дозволило визначити розподіл даних на 7 кластерів, як найбільш ефективним.

В подальшому дослідження планується спрямувати на розробку конкретних рекомендацій для кожного кластеру країн, виходячи із більш детального аналізу складових інформаційної безпеки та показників їх розвитку, що сприятиме виробленню конкретних моделей удосконалення та розвитку діючої системи інформаційної безпеки для відповідної групи країн.

РОЗДІЛ 2 ОРГАНІЗАЦІЙНО-ІНСТИТУЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФІНАНСОВОГО КІБЕРПРОСТОРУ

Банки відіграють надважливу роль у забезпеченні сталого розвитку економіки, адже саме вони є тими фінансовими посередниками, що забезпечують постачання ліквідності на фінансовий ринок та забезпечують кредитування реального сектору економіки.

Зважаючи на це, особливої уваги набуває забезпечення їх стійкості з урахуванням впливу всього комплексу факторів зовнішніх та внутрішніх факторів, у тому числі технологічного та інформаційного характеру.

На сучасному етапі розвитку світової економіки в умовах переходу на шостий технологічний уклад та пов'язаного з цим застосування технологій Індустрії 4.0 (штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR тощо) з'являються нові види загроз стійкості економічних агентів, що умовно формують групу кіберзагроз, ландшафт яких постійно трансформується та оновлюється. У фінансовому секторі проблема ускладняється наступним:

- мотивація кіберзловмисників зміщується від досягнення прямих фінансових вигід до руйнування критичної інфраструктури, до якої відносяться банківські та фінансові установи, що становить загрозу для національної та міжнародної стабільності фінансових систем та вимагає координації дій в сфері забезпечення кіберстійкості з боку як фінансових посередників, так і фінансових регуляторів на національному та наднаціональному рівнях;
- приваблива сфера для реалізації кібератак, зважаючи на можливі обсяги потенційних прямих фінансових вигід у разі їх успішної реалізації. У [5] шляхом проведення актуарних розрахунків визначено, що сукупні збитки від кібератак на 7947 банків у світі складають 97 млрд доларів на рік (9 % чистого прибутку), а вартість ризику (VaR) коливається від 147 до 201 млрд доларів

(14 % - 19 % від чистого прибутку). Зазначене призводитиме до зростання кількості кібератак, що будуть відбуватись у фінансовому секторі з постійним збільшенням кількості клієнтів, які зазнаватимуть втрат від реалізації кіберзагроз;

- модуляризація фінансових та банківських послуг, що пов'язує між собою фінансові установи та різноманітні організації (клієнти, контрагенти, постачальники ресурсів та послуг), рівень зрілості яких у здатності протистояти кіберзагрозам сильно відрізняється. Це формує слабкі елементи в механізмі забезпечення кіберстійкості фінансових посередників та ускладнює задачі банківських менеджерів щодо формування ефективного інструментарію протистояння кіберзагрозам та абсорбції їх наслідків в разі реалізації;
- наявна інфраструктура інформаційних та комунікаційних технологій не була розроблена з пріоритетом кіберстійкості, що потребуватиме її адаптації до нових умов діяльності, вимагатиме значних витрат та формуватиме внутрішні вразливості фінансових посередників до кіберризиків;
- значні прямі фінансові та непрямі репутаційні, соціальні, фізичні втрати фінансових посередників у разі втрати кіберстійкості.

Зважаючи на зазначене вище, банки мають формувати комплекс заходів, інструментів та механізмів для забезпечення кіберстійкості як здатності протистояти зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них. При цьому забезпечення кіберстійкості є окремим завданням в забезпеченні стійкості банка в цілому, що має концентруватись на виявленні та протидії кібератакам, мінімізації та швидкому подоланні їх наслідків.

Дослідження кіберстійкості банків є відносно новим напрямом у науковій літературі, як вітчизняній, так і закордонній, а системні дослідження в цій сфері практично відсутні. У фінансовій сфері кібератаки належать до складу операційних ризиків, опосередковано призводячи до підвищення інших ризиків насамперед ризику ліквідності та кредитного ризику, тому при дослідженні цієї

теми доцільно використовувати науковий доробок у сфері управління операційними ризиками.

Фундаментальні основи забезпечення стійкості банків сформовано в працях вітчизняних (О. Барановський, В. Вербенський, О. Дзюблюк та Р. Михайлюк, Ж. Довгань, В. Зінченко, О. Іващук, В. Коваль, В. Коваленко, В. Лавренюк, Д. Хоружий, С. Шумська) та закордонних (Е. Дж. Долан, Р. Дж. Кемпбелл, Р. Л. Міллер, П. С. Роуз, Дж. Ф. Сінкі, Дж. К. Ван Хорн) науковців. Базуючись на отриманих ними результатах, можливо сформувати базові постулати формування механізму забезпечення кіберстійкості банків.

Ґрунтовне дослідження концепції кіберстійкості фінансових посередників зроблено Б. Дюпоном [23]. Ним обґрунтовується необхідність забезпечення кіберстійкості в фінансовому секторі, систематизуються типи загроз та різноманітні прояви їх негативного впливу на діяльність фінансових посередників. На підставі цього автор зробив висновок про те, що базова парадигма «запобігати та захищати» є неадекватною, і що для забезпечення ефективного функціонування фінансових посередників слід орієнтуватись на активне забезпечення кіберстійкості.

Т. Шугунов, А. Жуков, Ф. Хочуєва у [24] визначили основні проблеми забезпечення кібербезпеки банківського сектора Російської Федерації у правовому та методологічному аспектах. Також ними проведеного поглиблений аналіз стану системи забезпечення кіберстійкості кредитно-фінансової системи в умовах становлення та розвитку цифрової економіки.

Важливі висновки щодо необхідності забезпечення кіберстійкості індустрії 4.0 зроблені С. Петренком у [25]. Він визначив, що якщо «…забезпечення кібербезпеки …, в основному, орієнтоване на оцінку ймовірності виникнення інцидентів та запобігання можливих загроз безпеки, то забезпечення кіберстійкості … спрямоване на збереження цільової поведінки та працездатності кіберсистем в умовах як відомих (приблизно 45 %), так і невідомих кібератак (решта 55 %).

М. Дубина, І. Середюк, Н. Білоус у [26] акцентують увагу на тому, що «…виникнення кібератак … зумовлюють створення нових кіберризиків для роботи комерційних банків. Це … вимагає пошуку нових механізмів, інструментів для їх попередження та протидії».

За результатами дослідження визначено, що рекомендовані підходи для забезпечення кіберстійкості значно різняться, але, як правило, більшість наукових наголошують на цілісному системному уявленні про кіберризики [27]. Також науковці акцентують увагу на необхідності розвитку можливостей реагування на кібератаки та відновлення після них, а не виключно на виявленні та підготовці до них для підвищення кіберстійкості [28].

М. Богославський у [29] досліджував ступінь протидії банківським кібератакам на світовому та вітчизняному рівнях, в результаті чого виявив базові постулати забезпечення кіберстійкості банків: обмін інформацією за поточними кіберзагрозами у реальному часі; постійна фінансова підтримка для забезпечення найліпшого результату боротьби з кіберзагрозами; взаємодія органів банківського нагляду та регулювання інформаційних технологій; протидія кібератакам на глобальному рівні з міжвідомчою кооперацією; розширення спектру дій банків при кібератаках для оперативної допомоги клієнтам.

Ряд наукових праць присвячені дослідженню окремих інструментів забезпечення кіберстійкості, зокрема кіберстрахування [26, 30]

Зважаючи на початковий етап наукових розробок, присвячених забезпеченню кіберстійкості банків на сучасному етапі розвитку цифрової економіки, подальшого розвитку потребує комплекс питань щодо теоретико-методологічного підґрунтя та практичного впровадження механізму забезпечення кіберстійкості, що дозволяє здійснити формалізацію ландшафту реальних і потенційних кіберзагроз; забезпечує узгодженість механізмів та інструментів для протистояння загрозам, спричинених кібератаками, адаптації та / або відновлення після них; дозволяє не лише адекватно реагувати на наявні кіберзагрози, а й

ідентифікувати негативні фактори, що можуть призвести до виникнення та реалізації нових кіберзагроз та кібератак.

При формуванні механізму забезпечення кіберстійкості слід розуміти, що вона є складовою загальноекономічної стійкості, під якою розуміємо «…системну якісну характеристику стану банку, що обумовлений дотриманням збалансованості, взаємозв'язку і взаємоузгодженості складових елементів: фінансових (власного капіталу, активів та зобов'язань, ліквідності, платоспроможності, прибутковості, ризиків) й організаційних компонентів (організаційна структура, кадровий потенціал, інформаційні технології та рівень контролю і банківської безпеки), і відображає здатність витримувати непередбачені втрати й забезпечує досягнення тактичних і стратегічних цілей та високі соціально-економічні результати функціонування» [31].

Виходячи з наведеного, кіберстійкість є складовою організаційної стійкості банку та, поряд з фінансовою стійкістю, визначає стійкий стан банку.

При розгляді питання щодо сутності поняття «кіберстійкість банку» застосовуються якісний та оцінювальний підходи.

За результатами проведеного дослідження з'ясовано, що у визначенні поняття «кіберстійкість» за якісним підходом спостерігається неоднозначність трактувань, що демонструє таблиця 2.1.

Результати дослідження щодо визначення сутності поняття «кіберстійкість банку», враховуючи необхідність її розгляду в якісному та оцінювальному розрізах, систематизовано та схематично зображено на рисунку 2.1.

На основі узагальнення напрацювань щодо визначення сутності поняття «кіберстійкість» пропонуємо визначати кіберстійкість банку за якісним підходом як здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Таблиця 2.1

Підходи до трактування поняття «кіберстійкість»

№	Джерело	Визначення
1	Європейський центральний банк	здатність продовжувати виконувати свою місію, прогнозуючи кіберзагрози та інші відповідні зміни в операційному середовищі та адаптуючись до них, а також витримуючи, стримуючи кіберінциденти та швидко відновлюючись після них.
2	Комітет з питань платежів та ринкової інфраструктури	здатність прогнозувати, протистояти, стримувати та швидко відновлюватися після кібератак
3	Д. Бодо, Р. Граубарт	здатність підтримувати свої основні функції і цілісність при впливі потенційних атак з загрозою її інформаційної безпеки. Кіберстійка організація – … здатна запобігати, виявляти, стримувати кібератаки та відновлюватися після них, мінімізуючи вразливість до атаки та її вплив на бізнес
		здатність передбачати, витримувати, відновлюватись та пристосовуватися до несприятливих умов, стресів, атак або компромісів щодо кіберресурсів
4	Комісія з цінних паперів та інвестицій Австралії	здатність підготуватися до кібератак, відреагувати на них і відновитися після них. .. це більше, ніж просто запобігання кібератаки або реагування на неї – вона також бере до уваги здатність функціонувати під час такої події, а також адаптуватися та відновлюватися після неї
5	Рада з фінансової стабільності	здатність продовжувати виконувати свою місію, передбачаючи та пристосовуючись до кіберзагроз та інших відповідних змін в операційному середовищі, витримуючи, стримуючи та швидко відновлюючись від кіберінцидентів.
6	Р.Коллінз; К.О'Коннор-Клоуз; А.Чжан	здатність протистояти, стримувати кіберінциденти та швидко відновлюватися після них шляхом прогнозування кіберзагроз та інших змін в операційному середовищі та адаптації до них.
7	Комітет «Кіберстійкості бізнесу»	здатність зберігати працездатність до кібератаки (підготуватися до неї і зробити її максимально дорогою для кіберзлочинців), ефективно реагувати на дії «чорних» хакерів під час кібератаки, а також швидко і з мінімальними втратами відновитися після неї
8	NIST	здатність передбачати, витримати, відновитися і адаптуватися до несприятливих умов, атак або компрометації систем, що використовують або активують різні компоненти незалежно від їх джерела
9	Колосок І. Н., Гуріна Л. А.	здатність стримувати локальний вплив кібератак, ідентифікувати та затримувати потік спотворених даних в межах сфери, чутливої до кібератаки, без подальшої передачі і використання цих даних при управлінні фізичною підсистемою, щоб не привести до виникнення аварійних ситуацій, зокрема великих системних

Джерело: систематизовано на основі [32-40]

Рисунок 2.1 – Підходи до визначення сутності поняття «кіберстійкість банку»

Відповідно до оцінювального підходу пропонуємо розглядати кіберстійкість у розрізі якісного та кількісного оцінювання.

Якісне оцінювання передбачає визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку. Вона базується на деталізованих даних щодо типів, рівнів та частоти кібератак, типи атакованих активів та профілів кіберзловмисників. Отримані значення також можуть доповнюватися експертними судженнями.

Кількісне оцінювання кіберстійкості банку здійснюється за допомогою аналізу різних наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні.

При цьому в контексті кількісного оцінювання кіберстійкості банку важливим є визначення її видів за рівнями, а саме:

- нормальний рівень кіберстійкості банку, що характеризується цільовим рівнем всіх параметрів кіберстійкості, контрольованим рівнем кіберризиків, безперервністю та стійкістю банківського бізнесу;
- низький рівень кіберстійкості банку, що характеризується стійким погіршенням всіх її параметрів, зростанням рівня кіберризиків, зростанням строків, необхідних для відновлення безперервності банківського бізнесу;
- критичний рівень кіберстійкості банку, що характеризується зниженням параметрів до критично низького рівня, невиконанням державних регуляторних вимог, значними порушеннями в безперебійності банківського бізнесу.

При характеристиці кіберстійкості вважаємо за доцільне базуватись на підході Б. Дюпона [23], який зазначив, що кіберстійкість має:

- динамічний характер: формування механізму забезпечення кіберстійкості вимагає її вивчення через часовий аспект з аналізом заходів, реалізованих до, під час і після кібератаки. Забезпечення кіберстійкості має передбачати постійний циклічний процес підготовки до кібератак, нівелювання їх наслідків та адаптації для запобігання зниженню її рівня до катастрофічного значення;
- мережевий характер: забезпечення кіберстійкості базується на мережі внутрішньоорганізаційних та міжорганізаційних зв'язків, що можуть бути активовані в короткі терміни в надзвичайній ситуації для надання додаткових ресурсів та досвіду;
- постійний характер: забезпечення кіберстійкості має передбачати регулярні репетиції кризових сценаріїв реалізації кіберзагроз. Це дозволить сформувати інструментарій та навички персоналу, необхідні для роботи в умовах постійного зростання кібератак;
- адаптивний характер: забезпечення кіберстійкості має базуватись на ретельному аналізі реалізованих кібератак, їх причин та наслідків, що дозволить

банку підвищувати рівень готовності до кіберзагроз, що можуть виникнути в майбутньому;

- суперечливий характер: мета забезпечення необхідного рівня кіберстійкості може вступати в розбіжність з іншими цільовими показниками діяльності банку, зокрема такими як прибутковість, що вимагає компромісу між ефективністю та адаптованістю до кіберзагроз при формуванні механізму забезпечення кіберстійкості банку.

Механізм забезпечення кіберстійкості є складовою механізму забезпечення стійкості банку та розглядається як цілісна система взаємопов'язаних елементів, що відбивають відповідні заходи з забезпечення кіберстійкості банків на макро- та мікрорівнях (рис. 2.2).

Особливість кіберстійкості банку в механізмі її забезпечення полягає в тому, що, з одного боку, вона є об'єктом застосування регуляторних та управлінських впливів (керівна підсистема), з іншого – є системним параметром функціонування, без якої банк не матиме змогу продовжувати виконувати свою місію та здійснювати безперервну діяльність. Відповідно до цього, показники кіберстійкості мають включатись до загальної стратегії банку та узгоджуватись з цільовими кількісними та якісними параметрами стратегічних планів.

Зовнішні рамки механізму забезпечення кіберстійкості банків формують органи банківського регулювання та нагляду національного та наднаціонального рівнів. Зокрема, ними сформовано широкий спектр інструментів оцінки та відповідності, спрямованих на підвищення кіберстійкості. Банк міжнародних розрахунків, Європейський центральний банк і національні регулятори в Великобританії, США, Нідерландах, Данії, Австралії та Канаді підвищили свої вимоги до кіберстійкості фінансових посередників.

При цьому в більшості випадків вважається за доцільне застосовувати диференційований підхід з ескалацією регуляторного та наглядового впливу залежно від рівня кіберзагроз, що створюються фінансовим посередником для стійкості фінансової системи в цілому. Базова стратегія регулювання та нагляду в

цьому випадку – це делеговане регулювання, що сприятиме співпраці між фінансовими посередниками та саморегулюванню, дозволяючи їм самостійно визначати шляхи досягнення регуляторних цілей у сфері підвищення кіберстійкості.

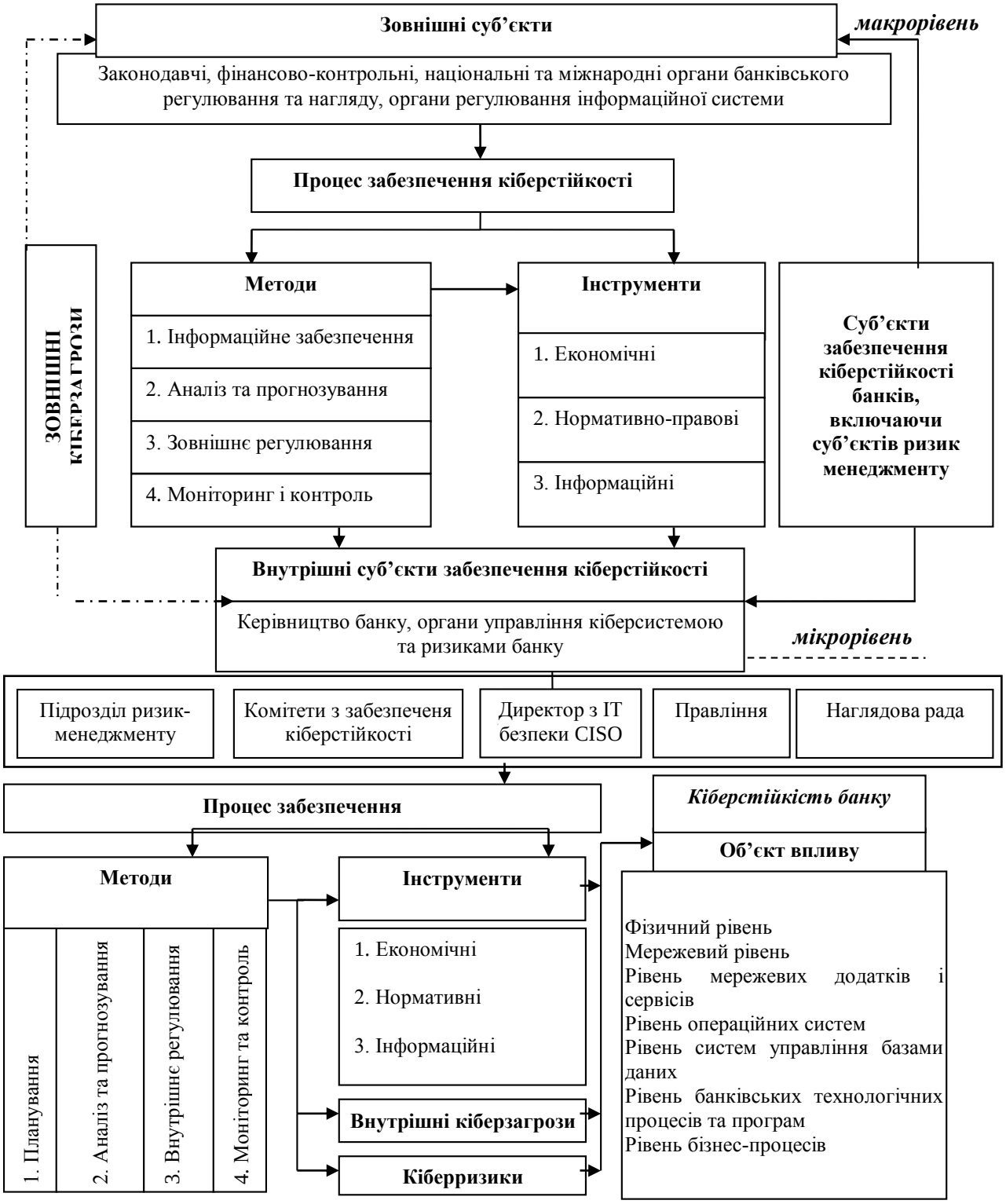


Рисунок 2.2 – Механізм забезпечення кіберстійкості банку

У тому випадку, коли фінансові посередники не бажають або не можуть реалізовувати ефективні стратегії забезпечення кіберстійкості, суб'єкти регулювання та нагляду здійснюючи посилення рівня інтервенціонізму, переходячи до жорсткіших норм регулювання та контролю, в тому числі штрафних санкцій.

Важливим напрямом при формуванні механізму забезпечення кіберстійкості банків на макрорівні формування регуляторної та рекомендаційної бази та стандартів.

У [41] визначено, що більшість наглядових органів використовують раніше розроблені національні або міжнародні стандарти, а саме: рамки кібербезпеки Національного інституту стандартів і технологій США (NIST), серію стандартів ISO 27000 та керівництво CPMI-IOSCO 2016 (Committee on Payments and Market Infrastructures- International Organisation of Securities Commissions) для забезпечення кіберстійкості інфраструктури фінансового ринку. Групою Світового банку підготовлено збірник нормативних документів, що систематизує наявні нормативні та наглядові практики з кібербезпеки для фінансового сектора [42] та документ про регулювання й нагляд кібербезпеки фінансового сектора [43].

Європейський центральний банк (ЄЦБ) у 2018 році опублікував документ «Очікування щодо нагляду за кіберстійкістю» (CROE) [32], що наразі застосовується практично всіма операторами фінансової інфраструктури в Європі. Світовий банк офіційно прийняв CROE, щоб забезпечити кіберстійкість інфраструктур фінансових ринків та сприяти глобальної гармонізації в рамках Глобальної ініціативи фінансової доступності (FIGI) [44]. Також ЄЦБ розробив стандарт для перевірки стійкості фінансового сектора до кібератак шляхом симуляції їх наслідків на критичні системи в банківській системі Європейського союзу (Threat Intelligence-based Ethical Red Teaming, TIBER-EU). Він передбачає,

що за допомогою «етичного злому» так звана «червона команда» допомагає оцінити здатність фінансової установи протистояти кібератаці [45].

Для забезпечення кіберстійкості на макрорівні важливим є формування відповідного інформаційного забезпечення, а саме збору даних щодо кіберінцидентів та їх наслідків, належного обміну інформацією між зацікавленими сторонами з державного та приватного секторів, включаючи фінансовий. У цьому відношенні такі ініціативи, як FS ISAC (Центр обміну інформацією та аналізу фінансових послуг), FSARC (Центр фінансового системного аналізу та стійкості) і SABRIC (Південноафриканський центр інформації про банківські ризики), вже грають важливу роль у полегшенні збору даних та обміну інформацією в різних юрисдикціях по всьому світу.

Але при цьому слід наголосити на тому, що не в усіх країнах та не всіма фінансовими посередниками визнано необхідність обміну інформацією щодо реалізації кіберзагроз, кібератак та їх наслідків. Це зумовлено значною кількістю факторів, одним з яких є відсутність довіри між всіма учасниками обміну інформацією. Зважаючи на це, органам банківського регулювання та нагляду спільно з іншими організаціями, долученими до протидії кіберзагрозам, необхідно реалізувати комплекс заходів, що мотивуватимуть всіх організацій та установ державного та приватного секторів, включаючи фінансовий, здійснювати обмін інформацією щодо кіберзагроз, кіберінцидентів, стратегій та інструментів їх виявлення, попередження та подолання їх негативних наслідків.

За результатами вивчення теоретичних підходів до забезпечення кіберстійкості банків ми розробили модель механізму забезпечення кіберстійкості на мікрорівні, адекватну сучасному стану та умовам, в яких працюють банки України, у наочному вигляді представлену на рисунку 2.3. Розроблена концептуальна модель механізму забезпечення кіберстійкості банку на мікрорівні забезпечує цілісний підхід до захисту від кібератак. Замість того, щоб зосередитись лише на запобіганні кібератакам, механізм забезпечення кіберстійкості має зосереджуватися на адаптивних та компенсаційних

інструментах, що дозволять забезпечити безперервність банківського бізнесу в разі реалізованої кібератаки.

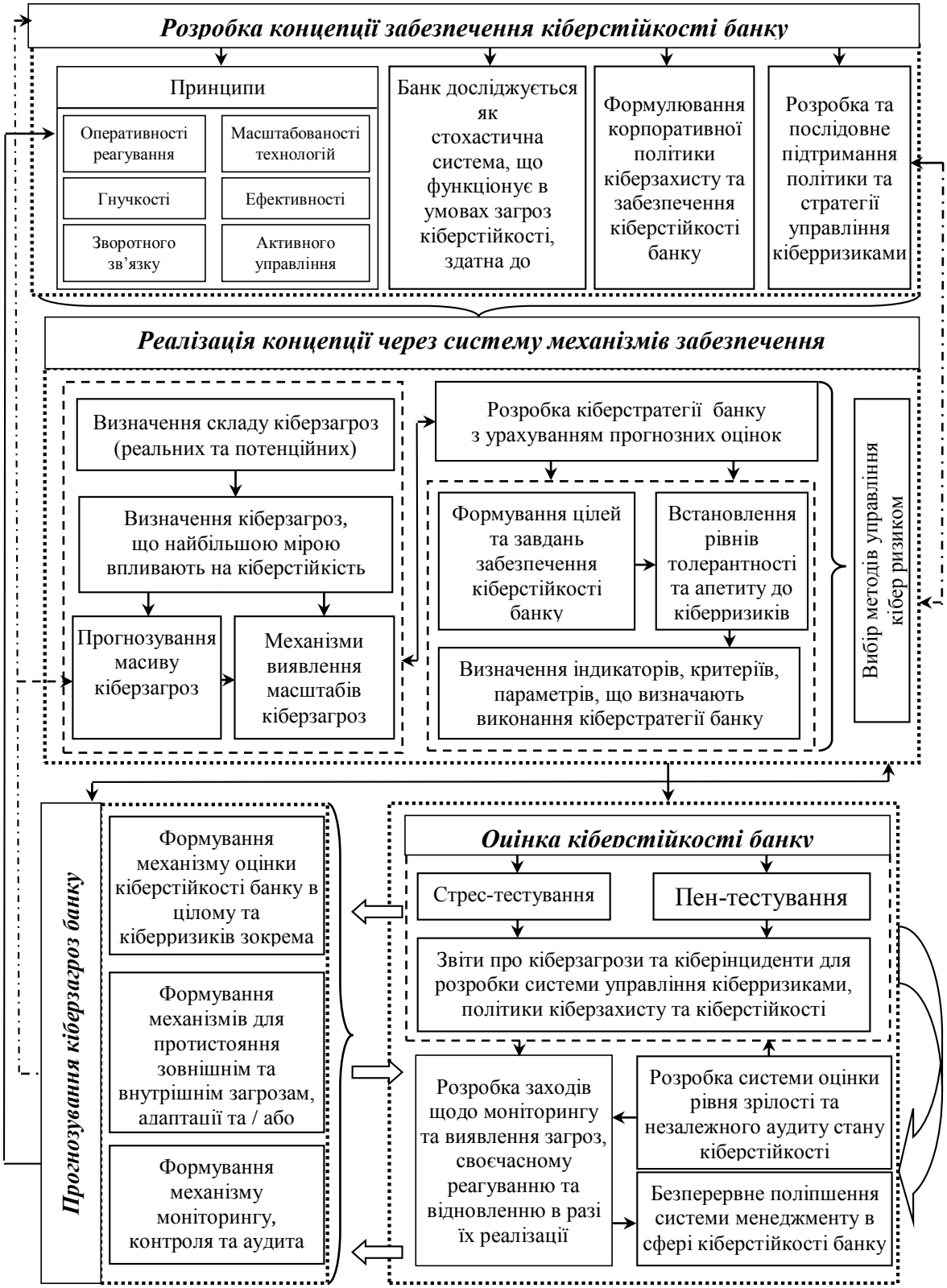


Рисунок 2.3 – Концептуальна модель механізму забезпечення кіберстійкості банку на мікрорівні

Кіберстійкість в найбільш загальному вигляді включає комплекс заходів, що банки реалізують для запобігання зовнішнім загрозам та виникненню внутрішніх кібервразливостей, заходи реагування, що дозволяють пом'якшити наслідки реалізації кіберзагроз, та збільшують можливості відновлення безперебійності банківського бізнесу після кібератаки.

Розроблений механізм забезпечення кіберстійкості банку дозволяє: ідентифікувати ландшафт реальних кіберзагроз та прогнозувати потенційні кіберзагрози; забезпечує узгодженість механізмів та інструментів їх попередження, адаптації та / або відновлення від кібератак; дозволяє не тільки адекватно реагувати на наявні кіберзагрози, а й виявляти негативні фактори, що можуть призвести до появи та реалізації нових кіберзагроз та кібератак.

Ми визначили, що важливим для забезпечення кіберстійкості банку є належне організаційне забезпечення. Воно має поєднати всіх суб'єктів банківського менеджменту, долучених до процесів забезпечення кібербезпеки, управління кіберризиками та безперервності банківського бізнесу. При цьому слід наголосити на тому, що кожен банк обирає таку модель організаційної будови, що найкращим чином відповідає особливостям його діяльності, характеру та обсягу банківських послуг, їх цифровізації, рівню розвитку та структурі інформаційних систем, а також наявним можливостям та потребам у сфері забезпечення кіберстійкості банку та ризик-менеджменту.

За результатами дослідження вважаємо за необхідне створювати в банках спеціалізований комітет забезпечення кіберстійкості як колегіальний орган з ключовими повноваженнями у цій сфері, до складу якого доцільно включити представників підрозділів, які відповідають за безперервність банківського бізнесу, кібербезпеку, управління кіберризиками та якість IT систем. Це дозволить домогтися синергетичного ефекту та об'єднати зусилля всіх суб'єктів банківського менеджменту різних бізнес-напрямків, центрів інфраструктури та забезпечення бізнес-процесів шляхом створення єдиної взаємозалежної процесно-орієнтованої моделі, включаючи метрики кіберстійкості та KPI, а також

інструменти для моніторингу, контролю та протидії зовнішнім та внутрішнім кіберзагрозам, адаптації та / або відновлення після кібератак.

До функцій цього спеціалізованого колегіального підрозділу доцільно віднести:

- інтеграцію процесів безперервності банківського бізнесу, якості ІТ, управління кіберризиками та кібербезпеки в єдиний механізм забезпечення кіберстійкості;
- нормативне, методологічне та інформаційне забезпечення механізму кіберстійкості банку;
- розробка звітних форм та створення бази даних щодо кіберінцидентів, їх фінансових та нефінансових наслідків;
- розробка багатоетапних та багатофакторних сценаріїв реагування на кіберінциденти;
- координація підрозділів банку у сфері реагування на кіберінциденти, прийняття рішення про ескалацію реагування на кіберінциденти на рівень топменеджменту банку;
- формування інструментів прогнозування, ідентифікації, попередження кібератак та відновлення після них;
- розробка планів розвитку механізму забезпечення кіберстійкості, моніторинг та аудит їх виконання.

На мікрорівні забезпечення кіберстійкості також важливим є брати участь в обміні надійною та дієвою інформацією про кіберзагрози та кіберінциденти з ключовими внутрішніми та зовнішніми зацікавленими сторонами (включаючи інші фінансові установи та державні органи банківського регулювання та нагляду) [46]. При цьому суб’єкти забезпечення кіберстійкості банку мають відстежувати актуальні оновлення інформації про кіберзагрози, кібервразливості, кіберінциденти, які відбувались в інших організаціях приватного та державного секторів, та заходи, що вживались для їх попередження та подолання наслідків [46].

Отже, банкам України необхідно сформувати комплекс заходів щодо формування механізму забезпечення кіберстійкості та його належного організаційного забезпечення.

Кіберстійкість банку доцільно розглядати за якісним та оцінювальним підходами. За якісним підходом кіберстійкість банку – це здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Відповідно до оцінювального підходу кіберстійкість запропоновано розглядати в розрізі якісного (визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку) та кількісного (формування наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні) оцінювань.

Запропонована автором модель механізму забезпечення кіберстійкості банку передбачає розробку концепції забезпечення кіберстійкості банку та її реалізацію через систему механізмів оцінки, моніторингу, контроля та аудита кіберстійкості, адаптації та / або відновлення після реалізації кіберзагроз.

Встановлено, що важливим для забезпечення кіберстійкості банку є належне організаційне забезпечення, зокрема створення спеціалізованого комітету забезпечення кіберстійкості як ключового колегіального органу в цій сфері.

РОЗДІЛ 3. СУЧАСНІ ТЕХНОЛОГІЇ ВНУТРІШНЬОЇ КІБЕРБЕЗПЕКИ ЕКОНОМІЧНИХ АГЕНТІВ

3.1. Перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків

В умовах активного становлення четвертої промислової революції, прогресивного розвитку нових цифрових технологій та комунікацій, їх комплексної інтеграції в глобальний бізнес, питання кібербезпеки стає все більш актуальним та в певній мірі критичним для деяких сфер діяльності. З впровадженням нових інформаційних технологій сфера кіберзагроз суттєво розширюється, не тільки за рахунок вже існуючих видів, але й за рахунок нових, досі неідентифікованих та невивчених кіберзагроз. За даними досліджень мультинаціональної консалтингової компанії Accenture Security [47] з 2017 по 2018 роки кількість потенційних «гілок» кіберзагроз зросла з 130 до 145, що дорівнює 11% приросту за рік. Відповідно середньорічні втрати від кіберзлочинності за той самий період зросли на 12%, і становили в межах 13 мільйонів доларів США в розрахунку на одне підприємство, що на 72% більше ніж 5 років тому. Вищенаведені показники свідчать про необхідність посилення заходів кібербезпеки, створення та дослідження нових технологій, які б дозволяли забезпечувати високий рівень кіберзахисту в умовах постійного росту кіберзлочинності в світі.

Впродовж десятиліть індустрія фінансових послуг залишається найбільш привабливою мішенню для кіберзлочинців, особливо діяльність банків. IBM X-Force Threat Intelligence Report [48] за 2017 рік показав, що серед клієнтів, які обслуговуються IBM Security Services, компанії, які надають фінансові послуги, зазнавали на 65% більше кібератак, ніж представники усіх інших галузей. Діяльність банків пов’язана із генерацією підвищеного кіберризику, що

передбачає високу імовірність серйозних фінансових втрат від кіберзлочинів, як для банків, так й для клієнтів, які у них обслуговуються. Тенденція зростання кіберзлочинності у банківському секторі спостерігається серед країн всього світу. З 2014 року кіберугрупування все більше зазіхають на бізнесові банківські рахунки, використовуючи при цьому таке зловмисне програмне забезпечення, як Dyre, Dridex, GozNym and TrickBot. Навіть міжнародна міжбанківська система передачі інформації та здійснення платежів SWIFT, якою користуються тисячі банків та окремих компаній по всьому світу, щороку потерпає від зростаючої кількості атак, як окремих зловмисників, так й професійних організованих злочинних кіберугрупувань. Так, у 2016 році спостерігався значний спалах організованих масових атак, в результаті яких мільйони доларів США були виведені з різних міжнародних банків шахрайським шляхом за допомогою клієнтського зловмисного програмного забезпечення, яке одночасно видаляло будь-які сліди таких транзакцій. Як повідомляє незалежна організація IT моніторингу ISACA в Україні, в 2016 році хакери через міжнародну банківську систему SWIFT вкрали 10 мільйонів доларів з рахунків одного із українських банків [49]. Таким же чином хакери свого часу вкрали з Центрального банку Бенгладешу 81 мільйон доларів. Це лише кілька прикладів, які вказують на існування проблем, пов’язаних із кіберзахистом, особливо фінансових установ.

Ефективне управління ризиками, пов’язаними з кіберзлочинністю, є однією з першочергових задач банківського управління, а побудова надійної системи кібербезпеки є критично важливим завданням. Банки повинні забезпечувати кіберзахист всіх здійснюваних операцій перш за все задля захисту активів власних клієнтів. Зростає кількість безготівкових операцій, користувачів онлайн банкінгу, що суттєво підвищує ризик перехоплення транзакцій та персональних даних клієнтів зловмисниками, що несе за собою величезні фінансові втрати як для клієнтів банків, так і для самих банків. В результаті шахрайських дій банки втрачають довіру своїх клієнтів та інших фінансових установ.

З моменту публікації у 2008 році праці Сатоші Накамото «Bitcoin: A Peer-to-Peer Electronic Cash System», в якій вперше було досить детально описано основи технології блокчейн, інтерес до даної технології та можливостей її застосування почав стрімко зростати серед науковців по всьому світу. Так, за даними бази Scopus у 2019 році було опубліковано 5738 наукових праць, присвячених блокчейн-технології, проти 1 статті, опублікованої у 2012 році, що свідчить про зростання зацікавленості науковців до даної теми. Якщо проаналізувати ті сфери, в яких здійснювалися дослідження науковців та в яких вирішувалися питання, пов'язані із застосуванням та розвитком блокчейн-технології, то найбільший відсоток належить науковим працям в сфері комп'ютерних наук (36%), інженерії (18%), математичних методів (9%), прийняття рішень (9%), бізнесу, менеджменту та бухгалтерського обліку (6%) та інших (рис. 3.1).

Рисунок 3.1 – Публікації закордонних науковців за сферами дослідження

Джерело: складено на основі бази даних Scopus

Тобто, на сьогодні більшість дослідників пов’язують технологію блокчейн саме із комп’ютерними науками, хоча дана технологія набуває свого розвитку й у інших сферах діяльності людини.

Аналізуючи публікації вчених за географічним охопленням, можна дійти висновку, що найбільша кількість публікацій належить вченим Китаю та США (рис. 3.2). Це пов’язано із тим, що сьогодні Китай є прогресивною країною із потужним економічним, технічним та людським потенціалом, яка намагається зайняти провідні позиції у світі. Відповідно, вчені даної країни є вкрай зацікавленими у вивченні останніх новітніх технологій у світі.

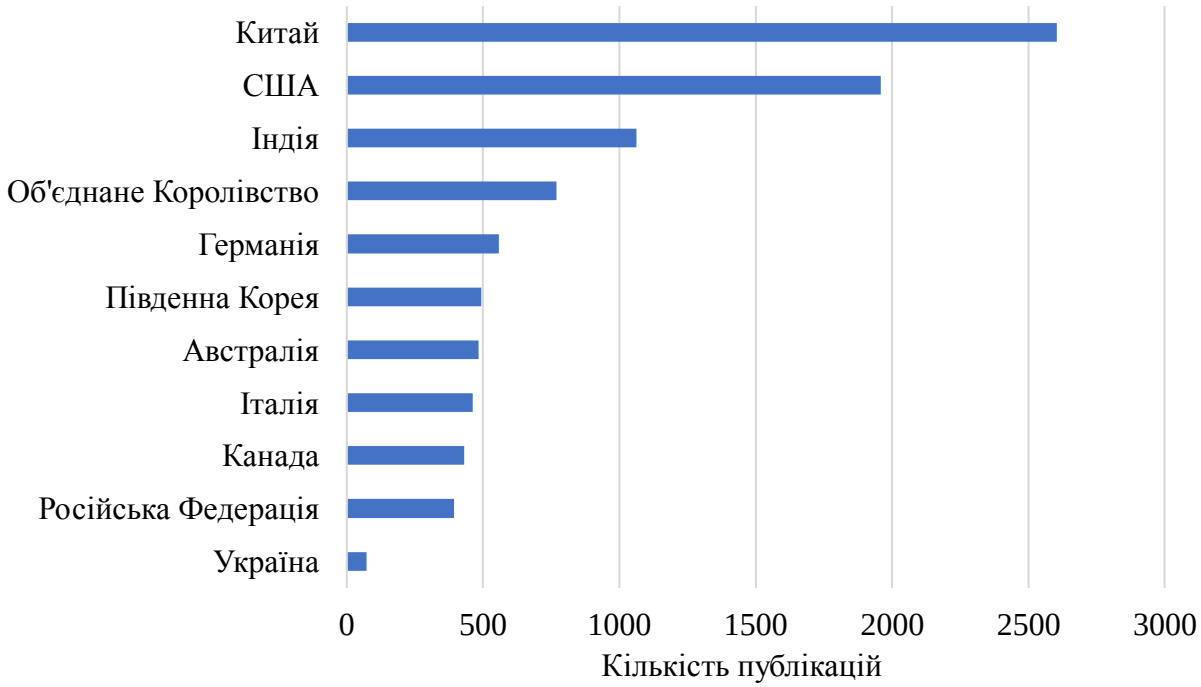


Рисунок 3.2 – Розподіл публікацій закордонних науковців за країнами, в яких здійснювалося дослідження

Джерело: складено на основі бази даних Scopus

Китайським науковцям не уступають також й американські дослідники, які за кількістю публікацій займають друге місце. Так, найбільший внесок у дослідження блокчейн-технології було зроблено такими закордонними фахівцями, як: K.K.R. Choo, F.Y. Wang, M. Guizani, Y. Yuan, N. Javaid, K. Salah,

D. Niyato, B. Stiller, N. Kumar, Z. Zheng, X. Xu, I. Weber, X. Du, J.H. Park, L. Zhu, S. Shetty, P. Wang, L. Njilla, A. Kiayaias, A. Norta, R. State, R.M. Parizi, Y. Zhang, L. Xu. Кожним з них було опубліковано більше 20 наукових праць у Scopus міжнародних виданнях, що свідчить про їх безперечний науковий внесок у дослідження блокчейн-технологій.

Українські вчені тільки набирають обертів. За останні 10 років ними було опубліковано лише 70 статей у міжнародних виданнях, що індексуються у базі Scopus (рис. 3.2). Це свідчить про недостатній інтерес до даної сфери з боку українського наукового осередку. Так, значний науковий доробок з питання розвитку та використання блокчейн-технології належить таким українським вченим, як: О. Летичевський, Р. Олійников, В. Пещаненко, М. Родінко, Д. Кайдалов, Л. Ковальчук, А. Кузнєцов, А. Настенко, Н. Полуяненко, В. Радченко, О. Шевцов, П. Кравченко, О. Курбатов, О. Шаповал, які опублікували більше ніж 3 статті у міжнародних виданнях, що індексуються у базі Scopus.

Можна також зазначити, що дослідженнями у галузі блокчейн-технологій займаються й провідні міжнародні компанії та організації. Так, технологічні консалтингові компанії світу, такі як IBM, Microsoft, Accenture та Deloitte проводять численні статистичні дослідження, спрямовані на вивчення перспектив залучення технології до різних сфер бізнесу, зокрема, і в галузі кібербезпеки фінансових організацій. Такі міжнародні організації як OECD, The World Economic Forum та The World Trade Organization публікують ряд досліджень стосовно напрямів застосування технології блокчейн на рівні міжнародної співпраці задля вирішення глобальних економічних питань.

Зважаючи на всю серйозність кіберзагроз для сектору фінансових послуг, банки та інші організації фінансового сектору в порівнянні з представниками інших галузей інвестують набагато більше коштів у створення та розвиток власної системи кібербезпеки [50]. Сучасні системи кібербезпеки банків є досить складними та багаторівневими, враховуючи природу та механізми формування

ризиків в кіберпросторі. Вони повинні враховувати постійно зростаючу тенденцію розширення поля кіберзагроз, наявність багатьох відомих і невідомих потенційних каналів здійснення атак. Слід зазначити, що джерела кіберзагроз можуть бути не тільки зовнішніми, але і внутрішніми, що також передбачає інтеграцію окремих різнонаправлених механізмів захисту.

Основним завданням існуючих систем кібербезпеки є максимальна протидія усім можливим кібератакам, за допомогою яких могли б бути здійснені кіберзлочини. В ідеалі, системи кіберзахисту повинні не тільки виступати бар'єром для всіх відомих видів кіберзагроз, але вміти ідентифікувати досі невідомі види кібератак до того, як вони могли б завдати шкоди банку та його клієнтам. Зазвичай система кібербезпеки банку являє собою комплексне програмне рішення, яке базується на ряді технологій, здатних захистити інформаційний простір банку від окремих видів та типів загроз, в залежності від їх характеру дії та області виникнення. Використання цілого портфелю технологій дозволяє максимально мінімізувати існуючий загальний рівень кіберризику, оскільки не існує єдиної технології, яка б ефективно спрацьовувала проти усіх можливих типів загроз.

На даний момент до ключових технологій, які використовуються для забезпечення кібербезпеки в банківському секторі, можна віднести: збір і аналіз даних щодо безпеки та обміну загрозами; автоматизація, штучний інтелект та машинне навчання; розширене прогресивне управління ідентифікацією та доступом; аналітика кібер-поведінки користувачів; криптографічні технології; управління виконанням процесів та ризиком на підприємствах; автоматизоване стратегічне управління; попередження втрат даних та розширений контроль периметру. Всі вищенаведені технології можуть бути дуже ефективними в протидії окремим видам кіберзагроз, на різних рівнях функціонування банківських інформаційних систем. Вони активно застосовуються різними банками по всьому світу, постійно доопрацьовуються та вдосконалюються у

відповідь на постійне посилення рівня кіберзлочинності та безперервне розширення поля кіберзагроз.

На сьогодні найбільш прогресивними технологіями, які застосовуються для забезпечення кібербезпеки банків, є технології штучного інтелекту та машинного навчання. Основною їх перевагою є можливість об'єднання різних каналів, таких як цифровий банкінг, аутентифікація, картковий банкінг та відкритий банкінг. За допомогою технології штучного інтелекту можна в одному місці опрацьовувати величезні обсяги інформації з різних каналів, що дає змогу набагато ефективніше моніторити та виявляти кібератаки, аналізуючи при цьому комплексну картину усіх існуючих транзакцій в різних каналах. Аналіз активності в окремих каналах часто не здатен ідентифікувати окрему підозрілу злочинну транзакцію. Зазвичай кібератаки реалізуються шляхом здійснення ряду дій із застосуванням різних каналів. Кожна така окрема дія може не викликати жодних підозр, але відслідковування цілої послідовності дій може ідентифікувати злочинний сценарій кібератаки. Багато спеціалістів в сфері банкінгу та кібербезпеки вважають, що саме застосування технології штучного інтелекту стане передовою тенденцією для постачальників фінансових послуг.

Поряд з технологіями, які вже активно використовуються в системах кібербезпеки, можна виділити технологію блокчейн, яка є відносно новою та перспективною. Допоки вона не знайшла широкого розповсюдження, але її використання, на нашу думку, в системах забезпечення кіберзахисту банку змогла б суттєво підвищити рівень їх ефективності. Блокчейн став широко відомим завдяки активному розвитку криптовалют, більшість з яких базується саме на даній технології. На сьогоднішній день по всьому світу вже існує ряд стартапів, які намагаються реалізовувати та тестувати концепції різнонаправлених проектів на базі технології блокчейн. Зокрема її починають використовувати при побудові прогресивних систем електронного голосування, ведення різних глобальних реєстрів (наприклад реєстрів нерухомості, земельних ділянок), в маркетингових системах, в системах управління ланцюгами поставок, та інше [51].

Технологія блокчейн, яку ще називають технологією розподілених реєстрів, є досить універсальним інструментом, який може бути використаним для вирішення широкого спектру задач. До основних її переваг відносять децентралізованість, повну прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізацію компромісу. Всі вищенаведені переваги можуть бути спрямованими на вирішення існуючих проблем забезпечення кібербезпеки банків. Тому їх було перекладено на площину проблематики кібербезпеки банків (табл. 3.1).

Аналізуючи переваги, можна стверджувати, що застосування технології блокчейн в інформаційних системах банків може суттєво підвищити рівень їх захищеності від кібератак різного роду. Також використання технології блокчейн здатне усунути основні вразливості сучасних банківських систем, які роблять можливим здійснення таких основних типів кібератак, як Malware, веб-атаки, DOS, атаки зловмисних інсайдерів, зловмисний код та ін [52].

Основними недоліками банківських інформаційних систем є їх централізованість та непрозорість. В таких системах, як і в більшості корпоративних, всі основні дані знаходяться в одному місці. Для того, щоб повністю захопити систему або критично її уразити, достатньо успішно атакувати її центральний сервер даних. Отримавши доступ до центрального реєстру даних, зловмисник отримує можливість без перешкод здійснювати всі можливі маніпуляції із системою. Ця проблема вирішується технологією блокчейн шляхом створення численних копій розподілених реєстрів даних, які розміщуються в різних вузлах системи. За таких умов ураження одного реєстру не може призвести до краху всієї системи. Припустимо, якщо інформаційна система банку матиме численну кількість копій реєстрів даних в різних відділеннях, вузлах системи, то захоплення кіберзлочинцем реєстру в одному з відділень, ніяк не вплине на всю інформаційну систему банку, і будь-які підміни існуючих записів даних будуть заблоковані у зв’язку з невідповідністю численним копіям даних в інших реєстрах інших відділень.

Таблиця 3.1

Переваги застосування технології блокчейн в системах кібербезпеки банків

Перевага	Сутність переваги	Значення переваги для систем кібербезпеки банків
Децентралізація	Відсутність єдиного головного серверу зберігання даних; всі записи зберігаються у кожного учасника системи, на кожному її вузлі.	Сучасні системи кібербезпеки банків є централізованими, мають головні сервери даних, що породжує їх основну вразливість. Блокчейн-технологія дозволить при атаці одного вузла зберегти дані на інших вузлах.
Повна прозорість системи	Всі транзакції, які відбуваються в системі, можуть відслідковуватися на всіх вузлах системи.	Технологія блокчейн в банківській системі надасть можливість аналізувати всі транзакції на кожному окремому вузлі. При цьому, кожна наступна транзакція перед її виконанням перевіряється всіма вузлами системи, і не може бути здійснена при виявленні найменшої невідповідності до усіх попередньо здійснених транзакцій.
Конфіденційність	Всі дані зберігаються в зашифрованому вигляді. Користувач, відслідковуючи всі транзакції, не може розпізнати окремі дані про них, а для здійснення операцій потрібний унікальний ключ доступу.	Застосування в банківських системах блокчейнів дозволить захистити від зовнішніх кіберзлочинців та інсайдерів-співробітників особисті дані клієнтів, про їх банківські рахунки, оскільки, маючи всю історію транзакцій, злочинці не зможуть нею скористатись та ідентифікувати дані.
Захищеність від несанкціонованого доступу	Будь-яка спроба внесення несанкціонованих змін автоматично відхиляється системою через невідповідність численним копіям даних, розміщених на різних вузлах системи. Для легального внесення змін в систему та здійснення транзакцій необхідно мати спеціальний унікальний код, який видається та підтверджується системою.	Зловмисники часто здійснюють маніпуляції та фальсифікації даних в системі банку, доступ до якої отримують обхідним шляхом, використовуючи вразливості системи. Якщо зловмисник заволодіє спеціальним унікальним кодом системи, що малоймовірно, в системі завжди зберігатиметься інформація про кожну транзакцію. Будь-яке зловживання правами в системі буде відоме всім іншим її членам, і зловмисник не матиме можливості приховати сліди власного злочину.
Компроміс	Компроміс реалізується шляхом попередньої перевірки кожним членом системи даних, які додаються до неї. Прийняття рішення щодо додавання нового блоку відбувається за умови згоди всіх учасників. Досягнення консенсусу здійснюється у відповідності до одного протоколу консенсусу з урахуванням особливостей та специфіки системи.	З точки зору кібербезпеки банківських операцій, проведення процедури перевірки кожної транзакції іншими вузлами системи створює додатковий бар'єр для реалізації атак. Будь-яка спроба підміни даних в одному з вузлів системи буде заблокована іншими вузлами системи, які мають свої копії усіх даних в системі. Цей механізм може захистити банківську систему від таких типів афер, як підміна кредитної історії, реквізитів рахунків, махінації із банківською звітністю, тощо.

Джерело: складено на основі [53, 54]

Непрозорість банківських інформаційних систем створює суттєві перешкоди при ідентифікації злочинних сценаріїв кібератак. За таких умов навіть системи штучного інтелекту та машинного навчання не можуть працювати максимально ефективно.

Також непрозорість банківських систем створює сприятливі умови для шахрайств з боку співробітників банків. Відомо, що близько 48% кібератак на банківські установи здійснюється саме зловмисними інсайдерами [55]. Саме атаки з їх боку вважаються найбільш небезпечними та призводять до найбільших грошових втрат. Але в умовах інформаційної системи, що функціонує на базі блокчейн, жоден співробітник не зміг би внести зміни до системи, будучи непоміченим, а всі його маніпуляції з системою постійно фіксувалися б та зберігалися в кожній копії реєстру даних на кожному вузлі. За таких умов будь-яка спроба перевищення службових повноважень досить швидко стає відомою на всіх вузлах системи.

Враховуючи всі вищенаведені переваги та перспективи технології блокчейн, можна стверджувати, що майбутні напрями її застосування у банківських системах є цілком прогнозованими. Якщо порівнювати можливості технології штучного інтелекту, що зараз масово впроваджується, та блокчейнів, то можна з впевненістю сказати, що обидві не можуть замінити один одного, оскільки вони спрямовані вирішувати різні задачі. Але їх комбінація є можливою та взаємодоповнюючою, тому логічним є підвищення рівня зацікавленості до цих технологій з боку різних суб'єктів господарювання, в тому числі й банківських установ. Так, було проведено аналіз рівня інтересу до технології блокчейн та технологій штучного інтелекту, щодо їх застосування у сфері комп'ютерної безпеки та у банківській діяльності за останні 5 років з використанням бази даних Google Trends [56].

На рисунку 3.3 представлено зміну за часом рівня зацікавленості до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Комп'ютерна безпека». Графік динаміки вказує на те, що відбувається підвищення інтересу до

блокчейн-технології в порівнянні з 2015 роком. На кінець 2017 року припадає значний стрибок, що обумовлено збільшенням кількості кібератак, хоча на сьогодні спостерігається певний спад.

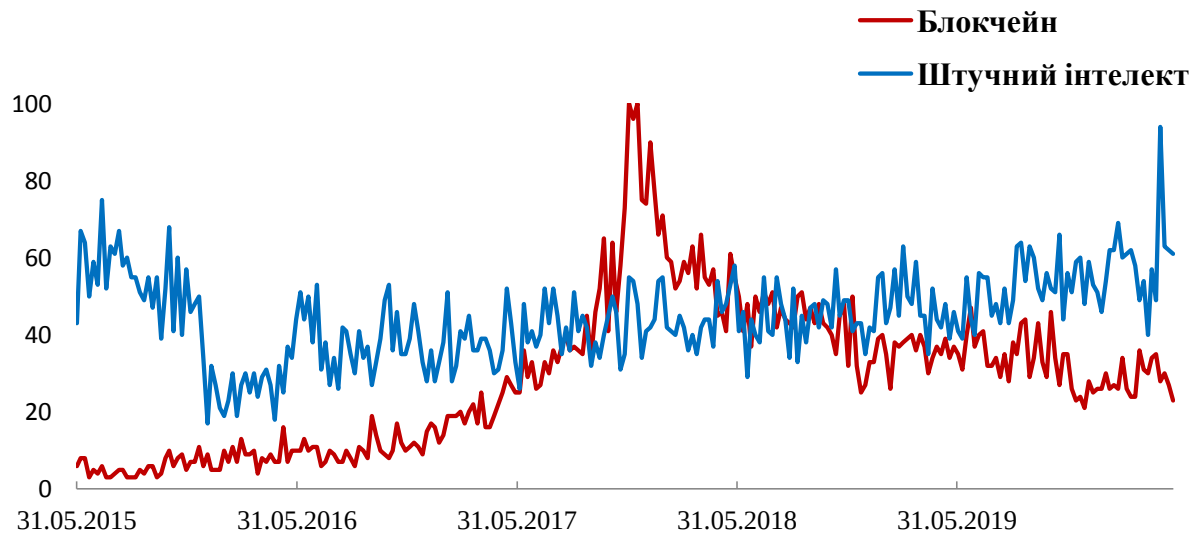


Рисунок 3.3 – Зміни рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Комп'ютерна безпека» за часом

Джерело: складено на основі бази даних Google Trends

Якщо порівнювати інтерес до обох технологій, то тема штучного інтелекту досі значно переважає тему блокчейн в категорії запитів, які стосуються комп'ютерної безпеки. Це можна пояснити тим, що технологія штучного інтелекту вже стала активно застосовуватися в сфері комп'ютерної безпеки, є досить вивченої та вже показала фактичну результативність та досить високу ефективність вкладених інвестицій. А технологія блокчейн досі є недостатньо вивченою на практиці, не має такої великої кількості вже реалізованих проектів, також імплементація та ефективність інвестування в технологію блокчейн досі є невизначеною.

Якщо порівнювати інтерес до цих двох технологій в різних країнах, то можна помітити, що в таких країнах світу, як Нідерланди, Франція, Швейцарія,

Китай, Австралія Сінгапур, Німеччина, Україна та інші, інтерес до технології блокчейн в категорії комп'ютерної безпеки переважає (рис. 3.4).

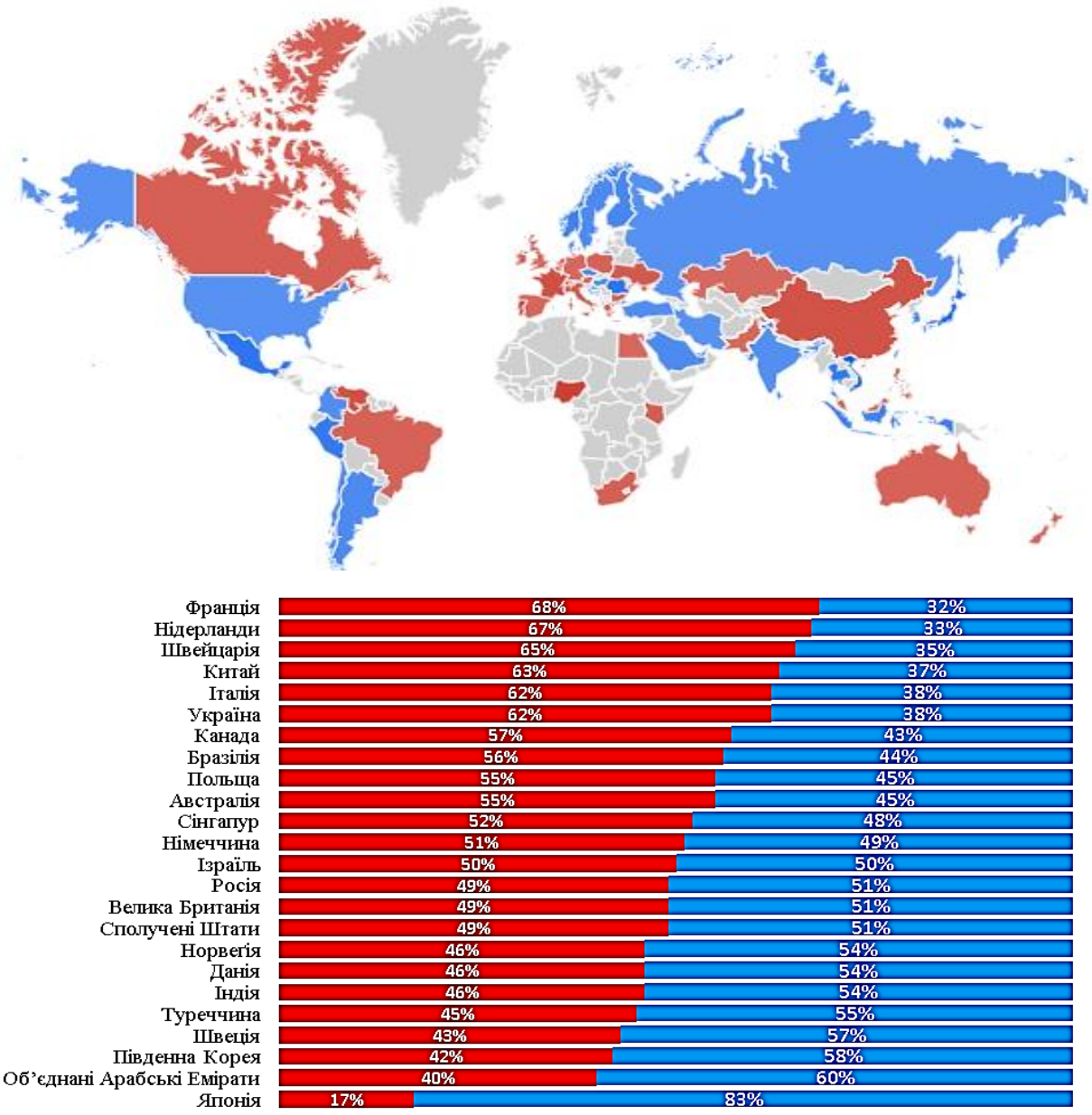


Рисунок 3.4 – Інфографіка рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Комп'ютерна безпека» за географією

Джерело: складено на основі бази даних Google Trends

Але такі країни, як Росія, Велика Британія, Сполучені Штати, Норвегія, Данія, Індія, Туреччина, Швеція, Південна Корея, Об'єднані Арабські Емірати,

Японія, зосередили свою увагу саме на технологіях штучного інтелекту у сфері комп'ютерної безпеки (рис. 3.4). Такий розкид обумовлений тим, що різні країни намагаються сформувати власні ніші на ринку систем комп'ютерної безпеки та намагаються використовувати останні розробки сучасних технологій.

В категорії запитів «Банківська діяльність» інтерес до обох технологій знаходиться приблизно на одному рівні вже більше одного року (рис. 3.5). Це говорить про те, що банки вбачають перспективи в застосуванні технології блокчейн поряд із штучним інтелектом. Обумовлені стрибки протягом 2017-2018 років, які показали значне зростання зацікавленістю технологією блокчейн, пояснюються зростанням в цей період популярності криптовалют на фінансових ринках.

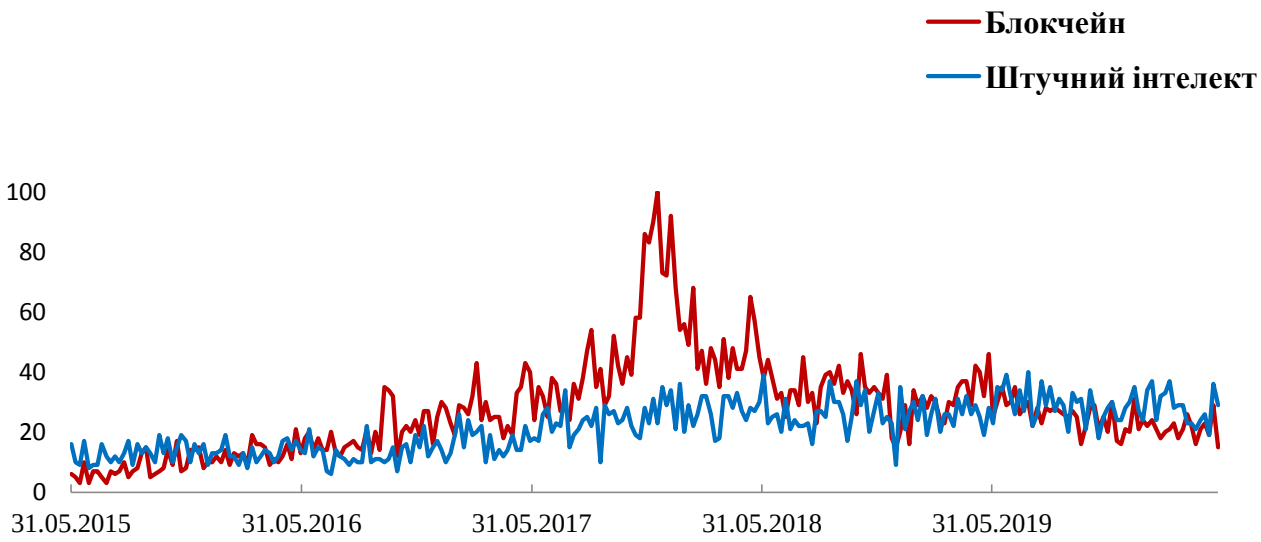


Рисунок 3.5 – Зміни рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Банківська діяльність» за часом

Джерело: складено на основі бази даних Google Trends

Карта порівняння інтересу до технологій в різних країнах вказує та те, що все ж таки в більшості країн світу інтерес до технології блокчейн в категорії запитів «банківська діяльність» переважає інтерес до технології штучного інтелекту (рис. 3.6). Це є цілком зрозумілим, адже технологія блокчейн має досить

високий потенціал застосування в сфері банкінгу, а не тільки як засіб забезпечення кібербезпеки. Слід такої зазначити, що інтерес до технології блокчейн загалом досить високий серед найбільш економічно та технологічно розвинених країнах, які можуть стати досить потужною базою для практичної реалізації потенціалу технології блокчейн.

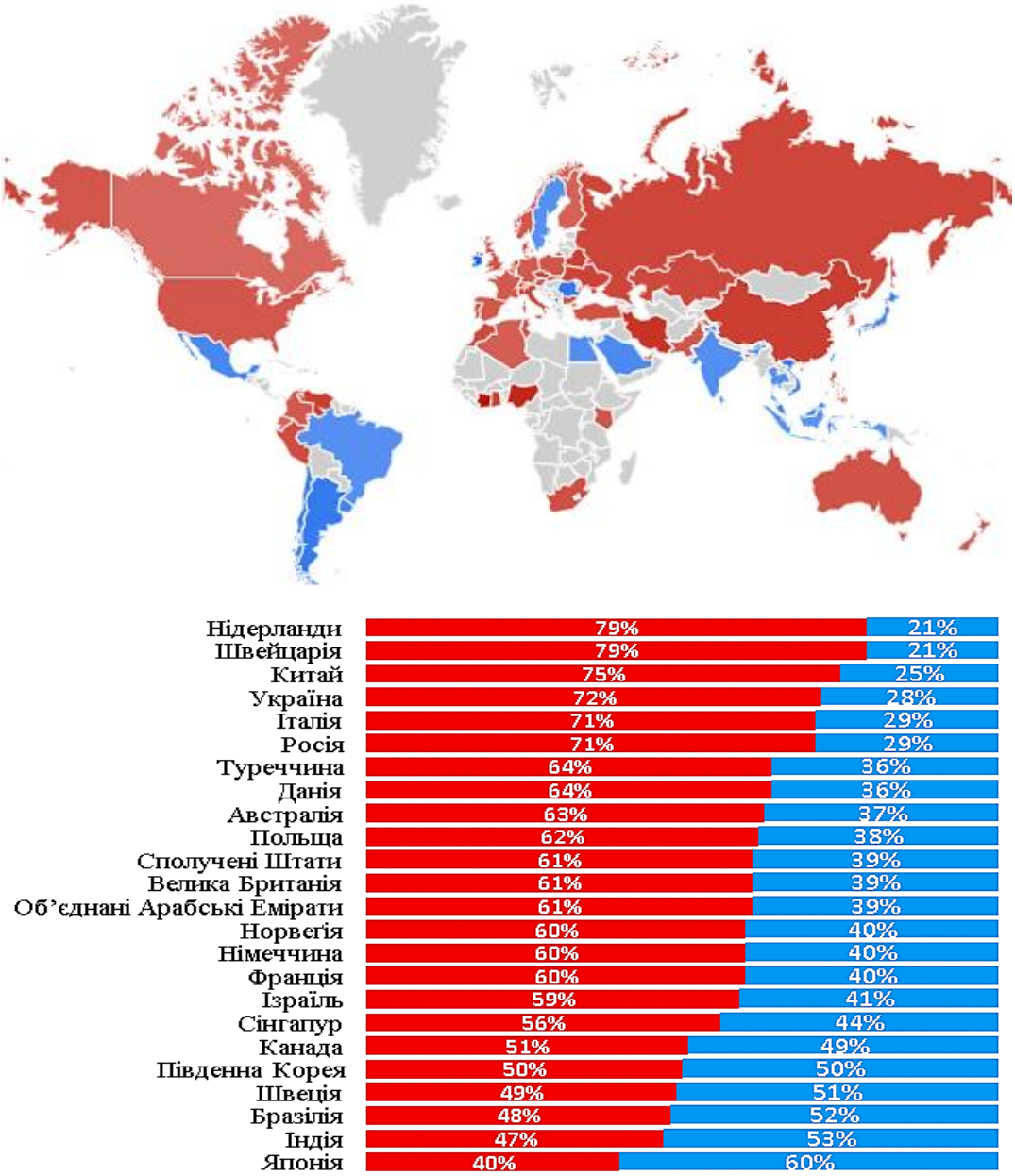


Рисунок 3.6 – Інфографіка рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Банківська діяльність» за географією

Джерело: складено на основі бази даних Google Trends

Якщо порівнювати технологію блокчейн з іншими технологіями, які застосовуються в системах кібербезпеки, то можна стверджувати, що вона може бути не менш ефективною, а деякі технології здатна успішно замінити. Технологія блокчейн спроможна вирішувати ті ж задачі, що зараз вирішуються за допомогою таких технологій, як розширене управління ідентифікацією та доступом, криптографічні технології, попередження втрат даних, автоматизоване управління політиками та ін. Ланцюг блоків транзакцій, кожен з яких має хеш з даними про попередні транзакції, здатен фіксувати кожну найменшу зміну в системі та зберігати історичні дані про будь-які зміни в системі на кожному її вузлі. І якщо на сьогодні розслідування кіберзлочинів в банківському секторі займає від кількох місяців до року, то використання технології блокчейн може в рази або навіть в десятки разів пришвидшити процедуру розслідування злочинів.

Технологія блокчейн має значний потенціал застосування в інформаційних системах кібербезпеки банків. Аналіз основних її переваг, таких як децентралізованість, прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізація компромісу, показав, що вони можуть бути спрямовані на вирішення широкого спектру проблем кібербезпеки банків. Впровадження технології блокчейн у банківських системах може усунути ряд їх головних вразливостей з точки зору кібербезпеки. Результати аналізу даних Google Trends показали, що інтерес до питання її застосування в сферах кібербезпеки та банківської діяльності є достатньо значним в порівнянні з інтересом до технології штучного інтелекту, яка вже досить активно застосовується за цими напрямками, хоча їй надають перевагу саме в реалізації заходів комп'ютерної безпеки, що пов’язано з результативністю штучного інтелекту та ефективністю вкладених в нього інвестицій. Більшість економічно та технологічно розвинених країн світу проявляють суттєвий інтерес до застосування технології блокчейн саме в сфері банкінгу, що зумовлює формування та розвиток значних перспектив практичної реалізації її потенціалу.

Можна припустити, що блокчейн-технологія може бути не менш ефективною в боротьбі з кіберзлочинністю, аніж інші, які наразі активно застосовуються в банківських інформаційних системах, причому вона може доповнювати існуючі системи для рішення задач з протидії кіберзагрозам.

3.2. Системно-динамічний підхід трансформації систем захисту на основі блокчейнів

Більшість компаній стикаються з такою проблемою, як зниження рівня надійності системи кіберзахисту, що призводить до появи вразливостей корпоративної інформаційної системи підприємства та порушенні конфіденційності, цілісності та доступності даних. У сучасному світі такі проблеми, як правило, призводять до втрати інформації, та, як наслідок, компанії втрачають клієнтів, фінанси, репутацію. Це відбувається, як правило, за рахунок втручання зовнішніх кібершахраїв з метою викрадання або знищення інформації, яка стосується в основному особистих даних клієнтів та банківської інформації – даних рахунків, транзакцій, карток тощо. Окрім стороннього по відношенню до компанії втручання, також є поширеними випадки здійснення кіберзлочинів із боку персоналу підприємства. Особливо такі випадки трапляються серед працівників, які мають доступ до бухгалтерської та фінансової інформації, при цьому вони мають широкі повноваження щодо використання необмежених прав доступу, а також в компаніях, які використовують віддалений доступ, мобільні додатки, хмарні технології. Тому компанії зацікавлені у створенні ефективної системи кібербезпеки, яка б дозволила знизити кількість інцидентів, попереджати кіберзагрози та таким чином знизити фінансові втрати.

Але практика свідчить про те, що не зважаючи на зростання обсягу інвестицій у побудову та розвиток інформаційної безпеки, поточні рішення для захисту даних не відповідають потребам бізнесу. Це підтверджують результати

дослідження, проведеного компанією Dell Technologies, за результатами якого до такого висновку прийшли 81% респондентів （DELLTechnologies, 2020）. Головною причиною є зростання обсягів інформації, якою володіють компанії. Так за 2019 рік її обсяг зріс майже на 40% по відношенню до 2018 року, при цьому орієнтована загальна вартість втрати даних зросла до понад 1 млрд. доларів на одну організацію за останні 12 місяців (（DELLTechnologies, 2020）). Інформація є цінним ресурсом, втрата якого впливає на всі бізнес-процеси компанії. Згідно дослідження “ X-Force Threat Intelligence Index 2020”, проведеного компанією IBM та опублікованого у 2020 році, 60% первинних проникнень у інформаційну систему компанії відбувалося за рахунок облікових даних, вкрадених раніше, або вразливостей програмного забезпечення （IBM Security, 2020）. Так, у 2019 році близько 29% випадків трапилося за рахунок викрадення облікової інформації, що призвело до втрати 8,5 млрд. записів, якими заволоділи кіберзлочинці. Також у 30% випадків ними було використано вразливості системи, що збільшилось у порівнянні з 2018 роком на 22%.

Проблема, пов’язана з підвищенням рівня ефективності системи кібербезпеки компаній є глобальною, оскільки середній розмір фінансових втрат від зломів та витоків інформації на червень 2019 року для підприємств середнього бізнесу світу склав близько $3.92 million （Ponemon Institute, 2019）. Тому компанії зацікавлені у залученні новітніх технологій з метою забезпечення надійності та безпеки інформації. Так, найбільше застосування у 2019 році знайшли такі технології, як: cloud-native applications (58%); artificial intelligence and machine learning (53%); software-as-a-service applications (51%); 5G and cloud edge infrastructure (49%); and Internet of Things/end point (36%) （DELLTechnologies, 2020）. Але оскільки проблема існує та не знижуються наслідки від неї, то відповідно є потреба у залученні інших підходів, хоча за опитуванням 71% респондентів вважають, що нові технології створюють більшу

складність захисту даних, тоді як 61% заявляють, що нові технології становлять ризик для захисту даних （DELLTechnologies, 2020）.

На нашу думку, компаніям варто звернути увагу на технологію blockchain, яка зарекомендувала себе у фінансовій сфері. Так, інвестиції в розробників корпоративних blockchain -рішень у 2019 році сягнули майже $434 mln, що перевищує на 62% інвестиції 2018 року （Ledger Insights, 2020）. Ця інформація говорить про зростання попиту на дану технологію. Аналітична платформа CB Insights виділила 58 галузей, в яких можливе застосування blockchain, серед яких також зазначено й напрямок кібербезпеки （CBINSIGHTS, 2020）. Також фахівці компанії Goldman Sachs вважають, що за рахунок впровадження даної технології, в процесі передачі даних відбувається зниження ймовірності кіберзлому. Це можливо за рахунок того, що blockchain передбачає відкритість реєстрів, просунуті методи криптографії, має потужні засоби кіберзахисту у порівнянні з традиційними системами （TADVISER, 2020）. Оскільки авторський колектив вбачає перспективи застосування технології blockchain для підвищення надійності системи кіберзахисту компаній, то в даному дослідження пропонується системно-динамічне моделювання, яка застосовує blockchain - технологію.

Питання кібербезпеки та blockchain досліджуються вченими всього світу. Так, аналізуючи дані з бази даних Scopus, було встановлено, що перша публікація на тему кібербезпеки була здійснена у 1999 році. За останні десять років спостерігається зростання публікаційної активності на цю тему у 17.67 разів, що говорить про підвищення зацікавленості до широкого кола питань кібербезпеки, які потребують вирішення. Подібна тенденція спостерігається у наукових працях, присвячених blockchain технологіям, які стали активно досліджуватися з 2016 року. За останні чотири року кількість публікацій, присвячених даній тематиці, зросла у 30.93 рази, що обумовлюється збільшенням обсягів інвестицій в дану технологію, набуттям розповсюдженості криптовалют, розширенням

можливостей застосування для різних сфер. Найбільша кількість праць охоплює галузі Computer Science and Engineering.

Для аналізу наукових досліджень щодо можливостей застосування технології blockchain для вирішення проблем кібербезпеки, було сформовано карту наукової бібліографії за допомогою програмного продукту VOSviewer （VOSviewer, 2020）. Вона була побудована на основі даних публікацій, обраних у поєднанні із проблемами cybersecurity and blockchain та згенерованих у базі даних Scopus. Карта відображає кластери публікацій за ключовими словами, які також поєднуються із заданими (рис. 3.7).

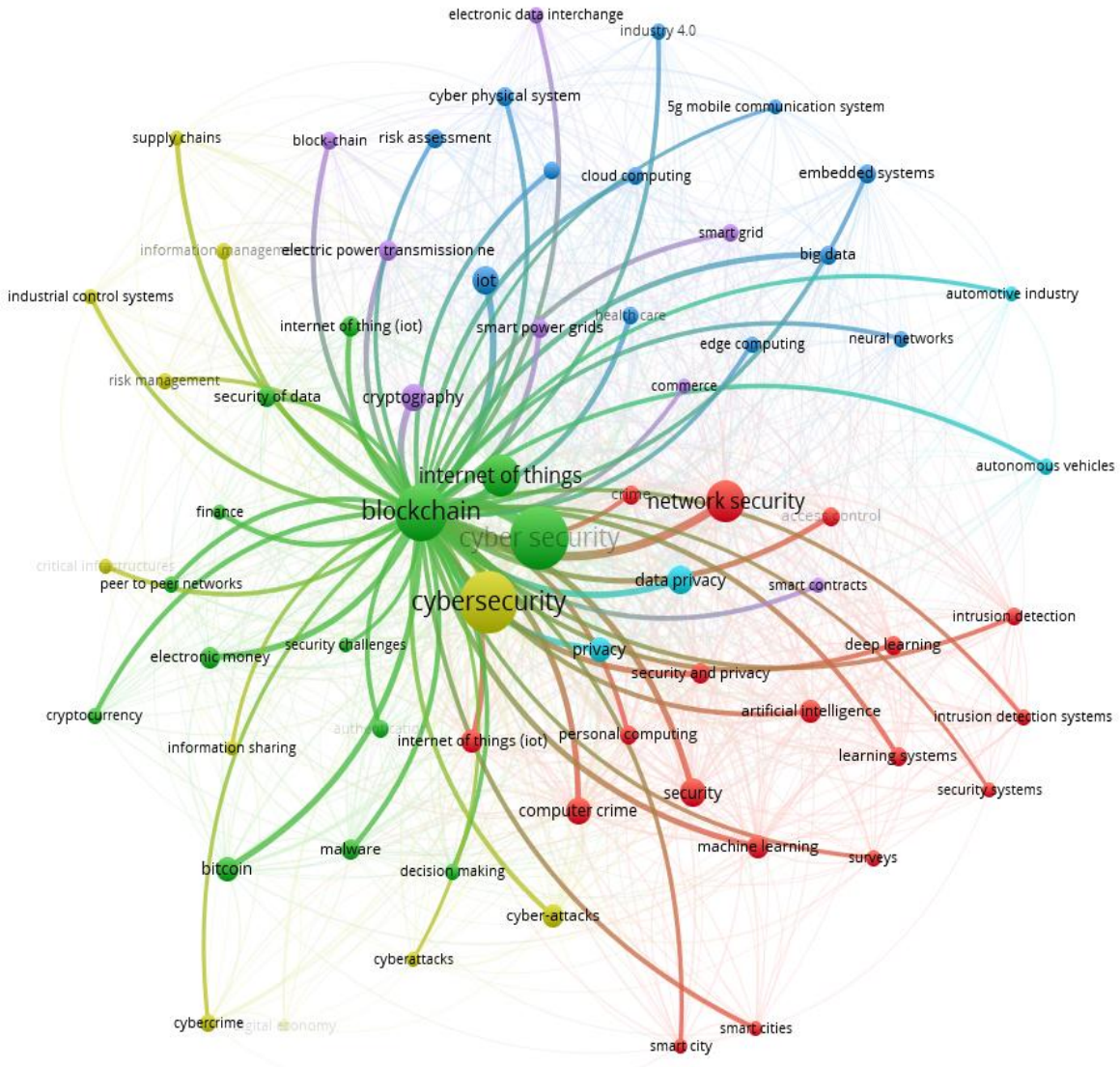


Рисунок 3.7 – Карта наукометричної бібліографії, побудована за ключовими словами

В результаті було виділено 6 кластерів ключових слів, кожен з яких виділено кольором, відмінним від інших. Вчені, які розглядають питання, пов’язані із blockchain and cybersecurity, досліджують їх у поєднанні з фінансовими ринками, криптовалютами, інтернетом речей, електронними грошами. Ними вирішуються проблеми malware, захисту даних, аутентифікації, peer to peer networks, які виникають у даних сферах, що є зрозумілим, оскільки фінансова сфера потребує потужних методів захисту інформації. Другий кластер поєднує blockchain, cryptography, electronic data interchange, smart contracts, smart grid, smart power grid, commerce, тобто науковці при дослідженні блокчейн-технологій роблять акцент на програмно-технічну його сторону та їх реалізацію в сфері комерції. Якщо аналізувати інші кластери, то вони виділяють широке коло технологій, які пов’язують з можливостями застосування блокчейнів в системах кіберзахисту: artificial intelligence, deep learning, intrusion detection systems, machine learning, 5G mobile communications, big data, cloud computing, edge computing, etc.

Вчені досліджують різні аспекти, пов’язані із кібербезпекою. Особливий акцент робиться на дослідженні шляхів виявлення ризиків в IT-сфері. Так, в роботі （Establishment of the new digital world and issues of cyber-risks management , 2017） досліджується даний аспект, при цьому зазначається один з його можливих напрямів, а саме підвищення вразливості систем управління підприємством.

Актуальним є питання цифровізації бізнес-процесів, що сприятиме підвищенню вимог до систем кібербезпеки. Це відбувається під впливом Industry 4.0 on entrepreneurship in developed and developing countries （Research on the impact of industry 4.0 on entrepreneurship in various countries worldwide, 2019）. Також це є однією з головних прерогатив держави, оскільки відчувається вплив наслідків кіберзлочинів на систему економічної безпеки держави, що потребує певних регулюючих заходів （State regulation of the economic security by applying

the innovative approach to its assessment, 2019). Оскільки потреба у забезпеченні надійності системи кібербезпеки зростає, то є необхідність подальшого удосконалення та розвитку механізмів інвестування таких проектів, як впровадження блокчейн-технології в діяльність компаній, що зазначено в роботі (Investment Management of Business Digital Innovations, 2020). Хоча деякі автори (The fifth global Kondratiev: low economic performance, instability and monopolization in the digital age, 2018) засуджують стрімкі темпи цифровізації та автоматизації компаній та зазначають, що це призводить до того, що такі технології перетворюються у фактор, який є руйнуючим, а не інтегруючим, та сприяє появі нових кіберзагроз для компаній та держав в цілому. Інша група авторів (The influence of industry 4.0 on financial services: Determinants of alternative finance development | [Wpływ przemysłu 4.0 na usługi finansowe: determinanty rozwoju alternatywnych finansów], 2019) (Cluster analysis of development of alternative finance models depending on the regional affiliation of countries, 2019) виділяє залежність між обсягами фінансування та рівнем розвитку інформаційних технологій.

Одним з проблемних аспектів, пов'язаних з кібербезпекою, є людський фактор, тобто участь людини у безпосередньому здійсненні злочину, спрямованого на викрадення, знищення або викривлення інформації. Головною з причин є отримання певної фінансової винагороди за кібершахрайства. Деякі автори (Tendencies and features of development of companies in digital epoch, 2017) відмічають, що сьогодні людина стала частиною складної інформаційної системи, що підвищує її інтелектуальні можливості в напрямку несанкціонованого втручання в систему. Дану ідею підтримують також й науковці (Financial, business and trust cycles: The issues of synchronization | [Ciklusi financiranja, poslovanja i povjerenja: pitanja za sinkronizaciju], 2019). Як зазначено в праці (The Influences of the Digital Revolution on the Educational

System of the EU Countries, 2019), цифрова революція впливає на різні аспекти життєдіяльності, в тому числі й на рівень обізнаності людей в питаннях кібербезпеки. Цей вплив, з одного боку є стимулом розвитку IT-literacy, як стверджують науковці (INVESTMENTS IN THE SYSTEM OF LIFELONG EDUCATION AS AN EFFECTIVE FACTOR OF SOCIO-ECONOMIC DEVELOPMENT, 2017), а з іншого боку це сприятиме появі нових форм кібершахрайств, що є однією із загроз.

В роботі (Leonov, S. V., Vasilyeva, T. A. and Shvindina, H. O., 2017) стверджується, що рівень організації інформаційних систем впливає на рівень розвитку компанії. Це призводе до того, що системи класу ERP у поєднанні із системами штучного інтелекту, системами Інтернет-речей, хмарними технологіями, що відповідає рівню компанії-лідера, як наслідок, сприяють підвищенню надійності їх системи кібербезпеки. Це є актуальним й для банківських установ, які стикаються з масовими кібератаками, соціальною інженерією, тому вони зацікавлені у розвитку сучасних засобів захисту та протидії шахрайству (BANK 3.0 CONCEPT: GLOBAL TRENDS AND IMPLICATIONS, 2017) (THE INFLUENCE OF FINANCIAL INNOVATIONS ON EU COUNTRIES BANKING SYSTEMS DEVELOPMENT, 2019). Так, одним з перспективних напрямків з вирішення цього питання є використання сучасних математичних методів, таких як гравітаційне моделювання (The innovative approach to increasing cybersecurity of transactions through counteraction to money laundering, 2019), яке використовується авторами з метою протидії процесу легалізації кримінальних доходів, оскільки це робить вразливості у системі. Сьогодні приділяють увагу новим підходам розвитку сучасних інженерних знань, створення та побудови баз даних та баз знань (Paradigm modeling studies of the formation of a knowledge economy in the information society

, 2017）, що є актуальним у світлі збільшення ризиків для підприємств щодо надійності системи кіберзахисту.

Для проведення дослідження щодо можливостей використання блокчейн-технології в компаніях з метою підвищення надійності системи кібербезпеки було обрано метод системно-динамічного моделювання. Перевагою цього методу є його можливість моделювати поведінки систем на високому рівні, виходячи з їх інформаційно-логічної структури та на основі потокового підходу. Методологія дослідження включає виконання наступних етапів:

1 етап – розробка діаграми причинно-наслідкових зв’язків. З цією метою було виділено основні елементи системи: намір людини здійснити кіберзлочин; фактори впливу на збільшення або зменшення кіберзлочину; дії людини для здійснення кіберзлочину (несанкціонований доступ, копіювання, знищення та зміна інформації, користувацькі помилки, навмисне незбереження інформації); запис інформації у блокчейн та базу даних традиційної інформаційної системи; функції користувача, політика компанії та вразливості системи. Між основними елементами було встановлено причинно-наслідкові зв’язки, які у сукупності із встановленими елементами сформували параметри системи. Причинно-наслідковий зв'язок є позитивним, якщо збільшення (зменшення) параметру впливає на збільшення (зменшення) того параметру, на який впливають, або від’ємним у випадку, коли збільшення (зменшення) параметру впливає на зменшення (збільшення) того параметру, на який впливають.

2 етап – розробка діаграми потоків. На цьому етапі було виділено рівні, тобто параметри, на які здійснюють вплив більша кількість інших параметрів з урахування позитивної та від’ємної дії. При цьому було враховано спеціальні параметри, тобто ті, які викликають збільшення або зменшення відповідного рівня. Також використовувалися додаткові змінні та константи. Для кожної змінної було задане рівняння, яке відповідає заданій системі рівнянь (формула 3.1):

$$
\begin{cases}
\dfrac{dI}{dt} = \big(II(t) - IR(t)\big)\,|_{\,II(t)>IR(t)} \vee \dfrac{dI}{dt} = \big(IR(t) - II(t)\big)\,|_{IR(t)>II(t)} \\
II(t) = \dfrac{1}{1 + EXP\Big(-\big(0.50288 - 2.75474 * (P_1 + P_2 + P_3 + P_4) + 4.8164 * (V(t) + V_1 + V_2 + V_3)\big)\Big)} \\
IR(t) = 1 - II(t) \\
A_1(t) = 1\,|_{\,V_2 \geq 0.5 \vee V_3 \geq 0.5 \vee P_4 < 0.5 \vee I(t) \geq 0.5} \vee A_1(t) = 0\,|_{V_2 < 0.5 \vee V_3 < 0.5 \vee P_4 \geq 0.5 \vee I(t) < 0.5} \\
A_2(t) = 1\,|_{P_3 < 0.5 \vee V_2 \geq 0.5 \vee V_3 \geq 0.5 \vee I(t) \geq 0.5} \vee A_2(t) = 0\,|_{P_3 \geq 0.5 \vee V_2 < 0.5 \vee V_3 < 0.5 \vee I(t) < 0.5} \\
A_3(t) = 1\,|_{P_2 < 0.5 \vee P_3 < 0.5 \vee V_2 \geq 0.5 \vee V_3 \geq 0.5 \vee I(t) \geq 0.5} \vee A_3(t) = 0\,|_{P_2 \geq 0.5 \vee P_3 \geq 0.5 \vee V_2 < 0.5 \vee V_3 < 0.5 \vee I(t) < 0.5} \\
A_4(t) = 1\,|_{\,P_1 < 0.5 \vee V_1 \geq 0.5 \vee V_3 \geq 0.5 \vee I(t) \geq 0.5} \vee A_4(t) = 0\,|_{P_1 \geq 0.5 \vee V_1 < 0.5 \vee V_3 < 0.5 \vee I(t) < 0.5} \\
A_5(t) = 1\,|_{I(t) \geq 0.5 \vee V_1 \geq 0.5} \vee A_5(t) = 0\,|_{I(t) < 0.5 \vee V_1 < 0.5} \\
A_6(t) = 1\,|_{I(t) \geq 0.5 \vee V_3 \geq 0.5} \vee A_6(t) = 0\,|_{I(t) < 0.5 \vee V_3 < 0.5} \\
E(t) = A_1(t) + A_2(t) + A_3(t) + A_4(t) + A_5(t) + A_6(t) \\
\dfrac{dB}{dt} = \left(\dfrac{1}{2} + \dfrac{1}{2} * \left[\dfrac{1}{6} * E(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \vee \dfrac{dB}{dt} = 0\,|_{E(t) < 1} \\
O(t) = A_1(t) + 4 * A_2(t) + 2 * A_3(t) + 3 * A_4(t) + 5 * A_5(t) + 6 * A_6(t) \\
\dfrac{dS}{dt} = \left(\dfrac{1}{4} + \dfrac{1}{4} * \left[\dfrac{1}{6} * O(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \vee \dfrac{dS}{dt} = 0\,|_{E(t) < 1} \\
\dfrac{dV}{dt} = \big(VI(t) - VR(t)\big)\,|_{VI(t)>VR(t)} \vee \dfrac{dV}{dt} = \big(VR(t) - VI(t)\big)\,|_{VR(t)>VI(t)} \\
VI(t) = 1\,|_{B(t)>0.5 \vee S(t)>0.5} \vee VI(t) = 0\,|_{B(t) \leq 0.5 \vee S(t) \leq 0.5} \\
VR(t) = 1\,|_{B(t) \leq 0.5 \vee S(t) \leq 0.5} \vee VR(t) = 0\,|_{B(t)>0.5 \vee S(t)>0.5} \\
P_1, P_2, P_3, P_4, V_1, V_2, V_3 \in [0,1]
\end{cases}
\tag{3.1}
$$

3 етап – встановлення параметрів системи та тестове моделювання. З цією метою встановлюються граничні значення початкових параметрів, які показують стан системи в результаті намірів людини здійснити кіберзлочин. Тому змін потребують наступні параметри: заборона на завантаження інформації, заборона на відкриття та запуск невідомих файлів, заборона на використання зовнішніх носіїв, обмежений доступ, апаратні помилки, відкритість бази даних, наявність віддаленого доступу. Якщо виникає потреба, то проводиться відладка відповідних рівнів. Далі здійснюється симуляція, в результаті чого отримуємо візуалізацію поведінки системи, коли є потенційні наміри здійснити кіберзагрози та ймовірності реакції системи у випадку запису даних у блокчейн та у випадку використання традиційної інформаційної системи. Також отримуємо результат,

який показує реакцію системи на її вразливості в результаті використання блокчейн-технології та традиційної інформаційної системи.

Системно-динамічне моделювання було проведене у програмному середовищі Vensim, яке використовується у наукових цілях задля здійснення такого роду моделювання （Ventana Systems, Inc., 2015）. В результаті було побудовано діаграму причинно-наслідкових зв’язків (рис. 3.8), яка відображає логіку функціонування потоків між елементами системи.

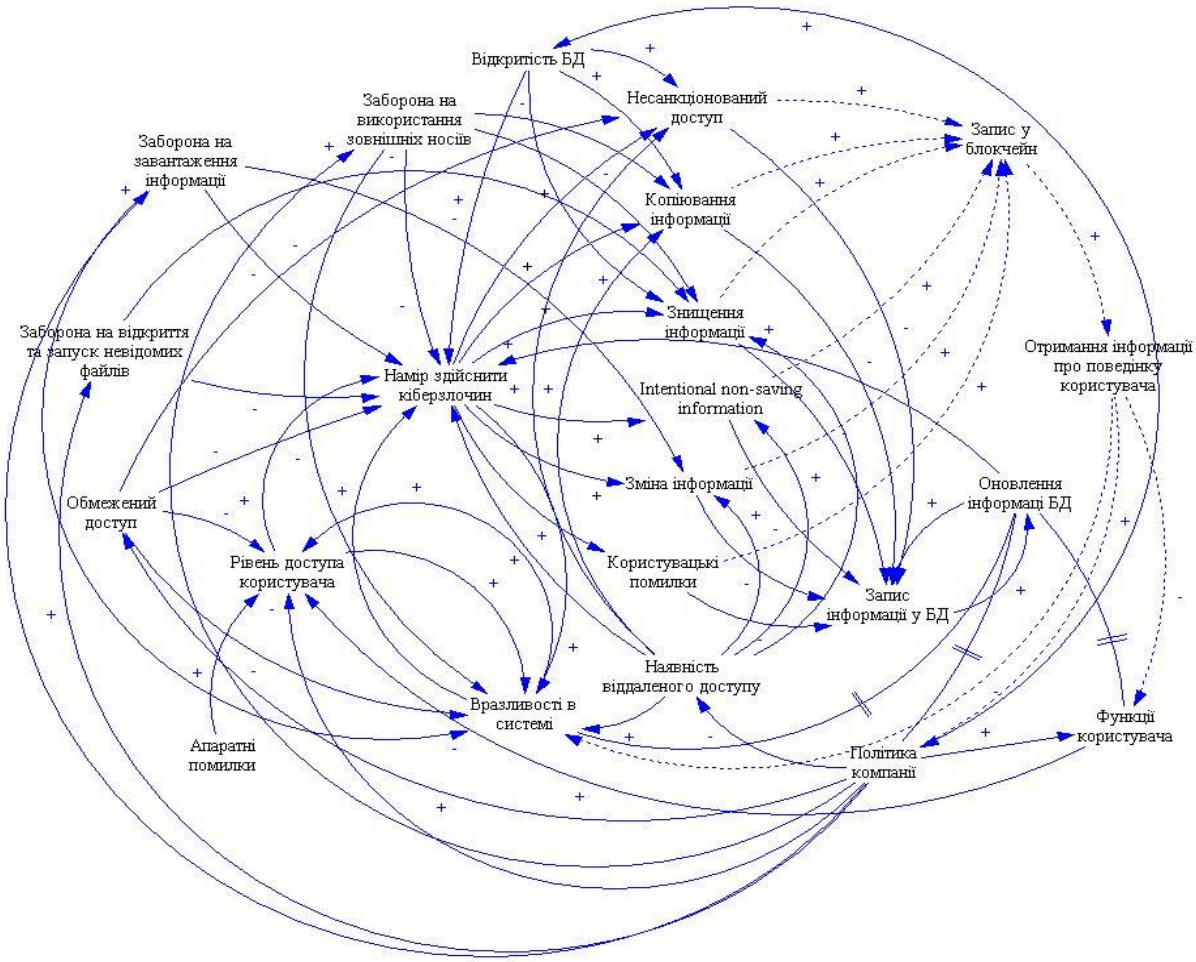


Рисунок 3.8 – Діаграма причинно-наслідкових зв’язків

Так, головним елементом є «Намір здійснити кіберзлочин», який виникає у людини. На стан цього елементу впливають фактори, такі як заборона на завантаження інформації, заборона на відкриття та запуск невідомих файлів, заборона на використання зовнішніх носіїв, обмежений доступ, рівень доступу

користувача, відкритість бази даних, наявність віддаленого доступу. В залежності від стану цих факторів, намір може збільшуватися, якщо користувач знає або про відсутність таких заборон, або має безмежні права доступу, тощо. Намір може зменшуватися у випадках, коли підприємство має високий рівень захисту, встановлює різні заборони, надає права доступу у відповідності до функціональних обов'язків працівника, тощо. Модель передбачає, що кіберзлочинець має намір вкрасти інформацію шляхом її копіювання, або знищити дані, або змінити інформацію, або здійснити intentional non-saving, несанкціонований доступ, або здійснити викривлення інформації шляхом допущення помилок. Перераховані незаконні дії обрано, як найбільш популярні незаконні дії, які сприяють появі вразливостей системи та зниженню рівня її кібербезпеки. Якщо технологія блокчейну буде впроваджена у компанію, то вона передбачає, що всі дії записуються до блокчейну та не підлягають ніяким змінам. Відповідно, використовуючи систему штучного інтелекту, дані з блокчейну можуть швидко надати інформацію про поведінку користувачів та, як результат, виявити порушення. Модель передбачає, що запис також може відбуватися і в інформаційній системі, але якщо відбуватиметься оновлення інформації, то запис в системі не буде зберігатися. Системі кібербезпеки знадобиться досить тривалий час на перевірку журналів активностей, щоб виявити порушення. В залежності від результатів, змінюється політика компанії, функції користувачів та стан вразливостей системи, як в свою чергу впливають на намір здійснення кіберзлочину.

На другому етапі було отримано діаграму потоків (рис. 3.9) та при її побудові було використано математичний апарат, представлений формулою 3.1.

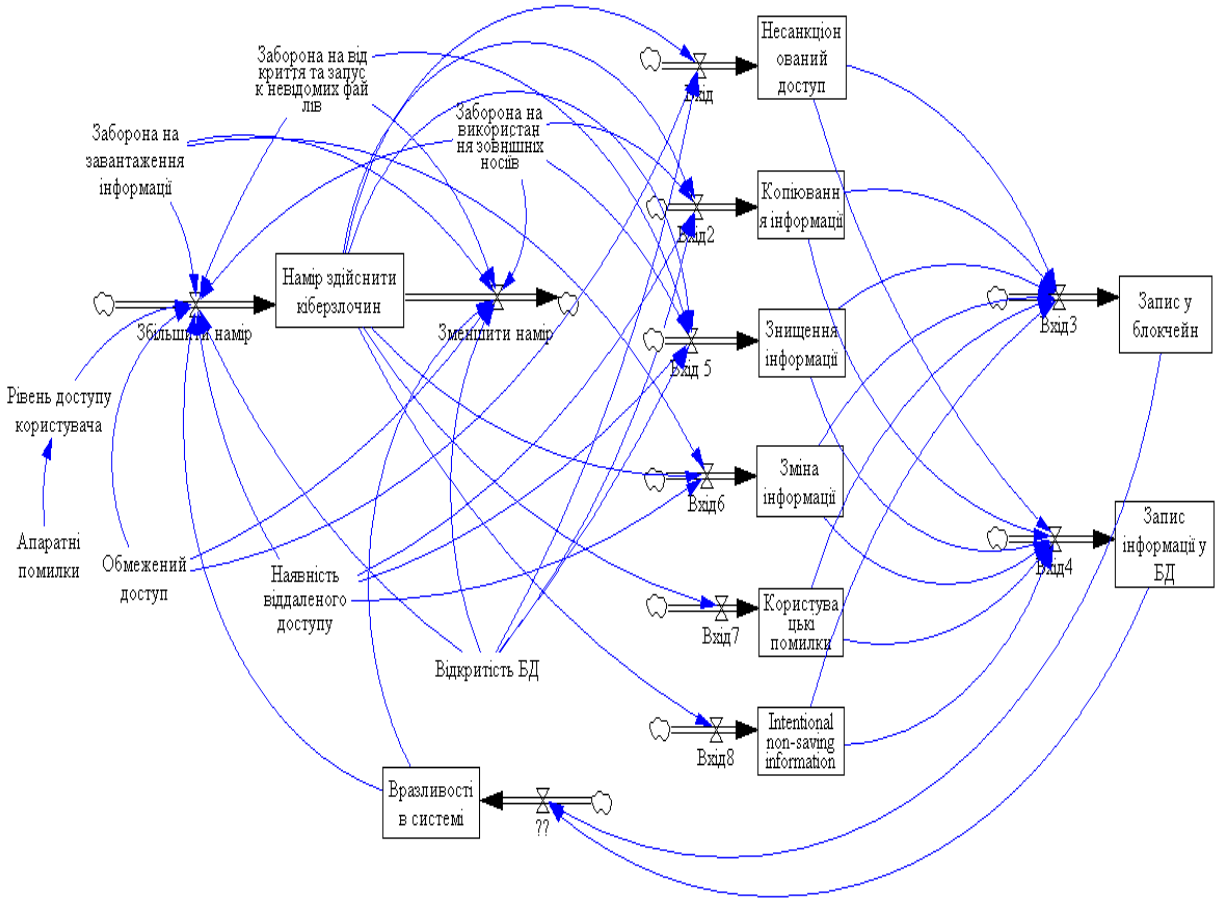


Рисунок 3.9 – Діаграма потоків

В результаті це нам дало змогу провести симуляцію. З цією метою було змінено значення початкових параметрів та узято їх 128 комбінацій граничних значень. Значення таких параметрів, як заборона на завантаження інформації, заборона на відкриття та запуск невідомих файлів, заборона на використання зовнішніх носіїв, обмежений доступ дорівнювало 1, що свідчить про наявність встановлених заборон та обмежень, або 0, тобто їх відсутність у компанії. Значення для апаратних помилок, відкритості бази даних, наявності віддаленого доступу дорівнювало 1 у випадку, якщо ці параметри є типовими для системи, та 0, якщо ці параметри відсутні. Симуляція відбувалася на однаковому проміжку часі. В результаті було зібрано 128 випадків поведінки системи для використання блокчейн-технологій та традиційної інформаційної системи. Результат симуляції представлений на рисунку 3.10.

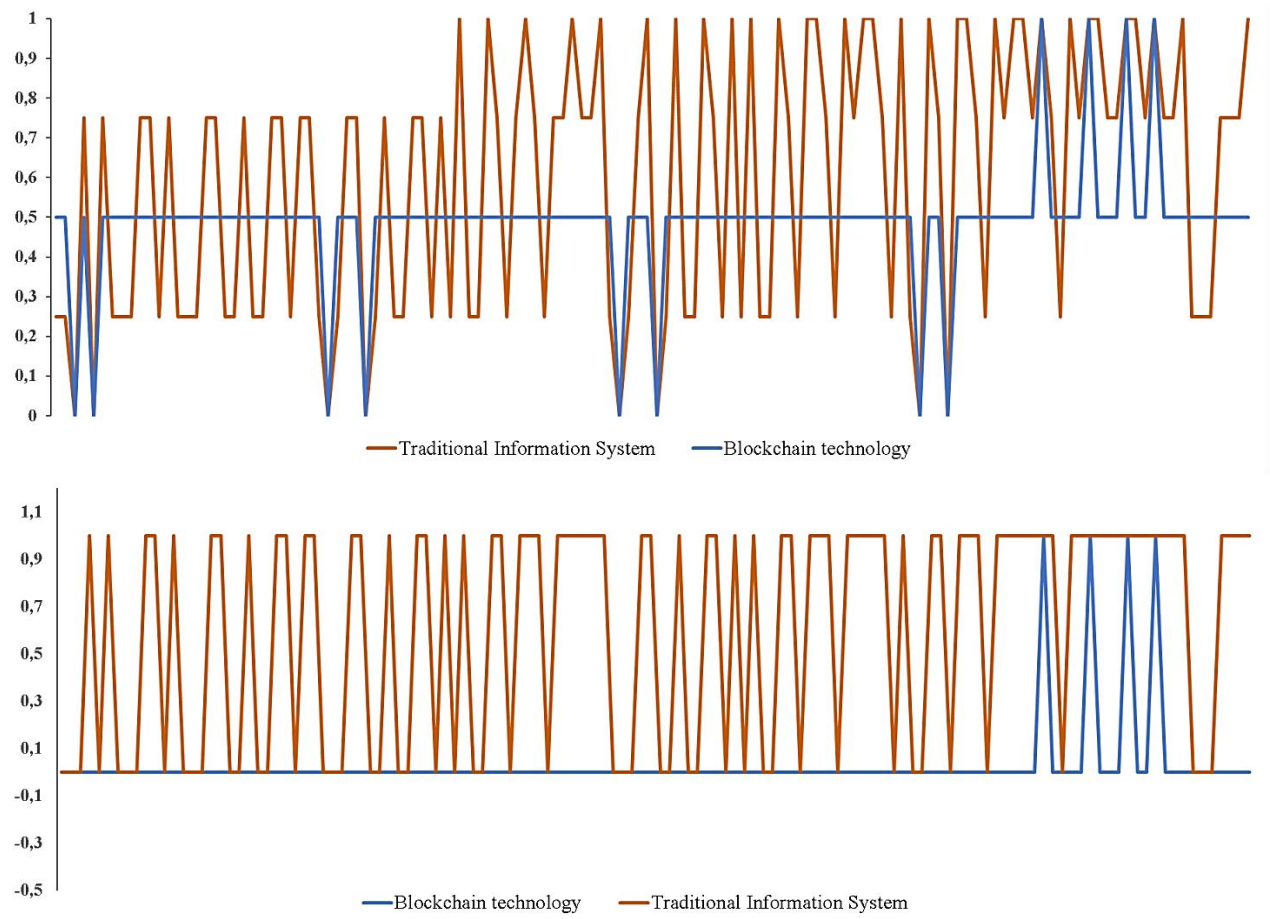


Рисунок 3.10 – Результати моделювання

На верхньому графіку рисунку 3.10 бачимо рівень ризику, який визначає система, яка використовує блокчейн-технологію та традиційна інформаційна система. За реалізованою методикою, якщо значення наближається до 0, тим нижче ризик не виявити кіберзлочинну активність, якщо значення наближається до 1, ризик є вищим. Тобто практично у всіх випадках система, що використовує технологію блокчейн має рівень ризику нижчий, ніж традиційна інформаційна система. Випадки, в яких обидві системи мають рівень ризику рівний 1, це випадки, коли компанія не встановлює заборони, надає необмежений доступ користувачам, тобто це варіант, коли відсутні всі заходи безпеки. Відповідно, в цьому випадку жодна технологія не спроможна позитивно вплинути на систему кіберзахисту. На нижньому графіку рисунку 4 представлений результат впливу виявлених даних на вразливості системи. Значення, яке дорівнює 0, свідчить про

зменшення вразливостей, 1 – про їх збільшення. Тобто, застосування блокчейн-технології дозволить зменшити вразливості системи практично у більшості випадків, а застосування традиційної інформаційної системи тільки в частині випадків. Тобто, застосування блокчейнів є більш ефективним в порівнянні із традиційними базами даних, що позитивно сприятиме на надійність системи кіберзахисту компанії.

Таким чином, проблеми, пов’язані із порушенням надійності системи кібербезпеки компанії є актуальними. Наслідками можуть бути втрата фінансових ресурсів, довіри клієнтів, зниження репутації та рівня конкурентоздатності. Тому фахівці із кіберзахисту повинні вчасно реагувати у випадках появи нових видів кіберзагроз або збільшення ймовірності появи вразливостей в системі. Унікальних інструментів, які допоможуть повністю вирішити проблеми кіберзахисту не існує. Тобто це повинен бути комплекс заходів, які сприятимуть ефективності та надійності системи захисту. Більшість компаній збільшують інвестиції в напрямку застосування сучасних технологій, що засуджується деякими фахівцями. На нашу думку, це правильний підхід, тому що зростання обсягів інформації, рівня обізнаності людини в питаннях застосування сучасних технологій та пристроїв, вимагають нових та нестандартних підходів. На сьогодні технологія блокчейн нарощує темпи використання та розширює сфери застосування. Тому є досить гарна перспектива щодо її використання для підвищення рівня надійності системи кіберзахисту в компаніях. Проведене в роботі системно-динамічне моделювання дозволяє робити припущення щодо переваг даної технології над традиційними інформаційними системами. Насамперед, дана технологія не буде замінювати існуючу, а доповнювати її, оскільки її головна прерогатива – це зберігання інформації у первинному вигляді без змін, що дозволить виявляти відхилення при спробі здійснення змін. В подальшому планується розширити запропоновану модель шляхом врахування інших параметрів: активностей, особливо зовнішніх користувачів; факторів впливу на рівні запису інформації у блокчейні та традиційній інформаційні базі.

3.3. Нечітко-множинний метод виявлення ризиків порушення кібербезпеки банку з боку його персоналу

Згідно з визначенням Базеля II, шахрайство являється частиною операційного ризику банку та класифікується як внутрішнє та зовнішнє. Найбільше збитків у світі в 2018 році (рис. 3.11) було заподіяно через такі типи шахрайства персоналу, як [57]: неправдиве відображення фінансової звітності (10% випадків), корупція (38% випадків) і незаконне привласнення активів (89% випадків).

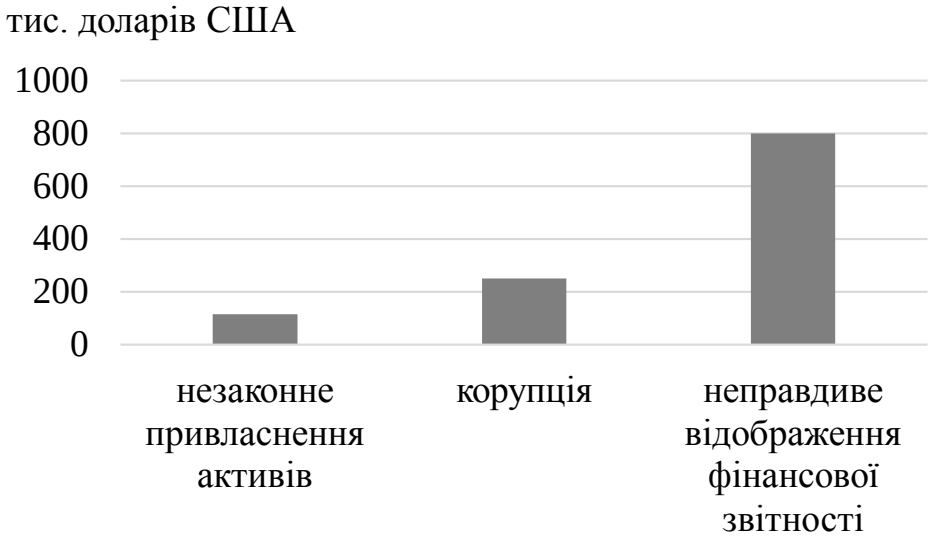


Рисунок 3.11 – Медіана фінансових збитків за типами шахрайства персоналу

Згідно зі звітом Асоціації сертифікованих фахівців із розслідування шахрайства [58], найбільша кількість випадків шахрайства у фінансовому секторі фіксується в банках, причому кількість виявлених випадків шахрайства за участі банківського персоналу набагато перевищує кількість випадків зовнішнього шахрайства. На жаль, попередити шахрайство банківського персоналу на рівні внутрішньобанківських технологічних засобів або регламентів сьогодні практично неможливо. Небезпечність шахрайств персоналу у банківській діяльності обумовлює необхідність активної протидії їм, одним із інструментів

якої є незалежний аудит, який в тому числі оцінює рівень ризику шахрайства банківського персоналу.

У випадку шахрайства персоналу службі внутрішнього аудиту банку важко забезпечити повну незалежність в діях і неупередженість у судженнях, тому особливого значення набуває зовнішній аудит банку незалежними експертами, що є поширеною практикою в іноземних банках. До того ж в Міжнародному стандарті професійної практики внутрішнього аудиту 1200 «Професійна компетентність та належна ретельність» зазначено, що «внутрішні аудитори повинні мати достатні знання для того, щоб оцінити ризик шахрайства та спосіб управління таким ризиком в організації, але не передбачається, що внутрішній аудитор повинен володіти такою ж компетенцією, що й особа, основним обов'язком якої є виявлення та розслідування фактів шахрайства» [59]. Основними характеристиками зовнішнього аудиту є:

1) незалежність і об'єктивність (незаангажованість у судженнях);

2) вдосконалення системи кібербезпеки банку, що передбачає можливість оцінити ризики шахрайства банківського персоналу, слабкі сторони системи кібербезпеки банку та дати рекомендації, спрямовані на підвищення ефективності системи кібербезпеки банку.

Левова частка банківських шахрайств відбувається з кредитними картками. У роботі [60] зазначено, що сьогодні для виявлення таких шахрайств широко застосовуються: логістична регресія, метод опорних векторів, дерева рішень, випадковий ліс, самоорганізовані карти Кохонена та нечітка логіка. На нашу думку, при наявності невизначеностей найкращі результати дає застосування нечітких методів. Однак слід зважати на те, що основним недоліком останніх є їх не надто висока точність, тому краще використовувати гібридні нейро-нечіткі системи. В роботі [61] для моніторингу поведінки власників карткових рахунків використовується прихована марківська модель (HMM, Hidden Markov Model), яка спочатку навчається нормальним діям власника картки, а потім використовується для виявлення шахрайської поведінки. В свою чергу для

виявлення викривлень фінансової звітності в банківській сфері широко застосовуються: нейронні мережі, байєсові мережі, генетичні алгоритми та текст майнінг.

Результати порівняльного аналізу економіко-математичних методів виявлення шахрайств у банках, що здійснюються персоналом банку, представлено у вигляді таблиці 3.2.

Таблиця 3.2

Порівняльний аналіз економіко-математичних методів виявлення шахрайств у банках, що здійснюються персоналом банку

Група методів виявлення шахрайств у банках	Основні характеристики	Урахування невизначеності
Кількісні (використання закону Бенфорда, асоціативний аналіз, логістична регресія, прихована марківська модель)	Базується на традиційному математичному апараті	Невизначеність враховується за допомогою засобів статистики та теорії ймовірностей
Машинне навчання (метод опорних векторів, дерево рішень, нейронні мережі, самоорганізовані карти Кохонена, байєсові мережі, генетичні алгоритми, текст-майнінг)	Базуються на технологіях штучного інтелекту (навчання з учителем і без нього)	Невизначеність враховується за допомогою засобів статистики та теорії ймовірностей
Якісні (нечітка логіка)	Базуються на експертних оцінках	Невизначеність враховується за допомогою експертних оцінок
Гібридні (нейро-нечіткі системи)	Базуються на синергетичному підході (використовуються сильні сторони різних методів)	Невизначеність враховується за допомогою кількісного та якісного математичного апарату

Згідно Положення з міжнародної практики аудиту 1006 «Аудит фінансових звітів банку» типові шахрайські дії управлінського персоналу та працівників банку включають в себе [62]:

1) незаконне привласнення активів:

– депозитні операції: маскування вкладів; невідображення депозитів у обліку; крадіжка депозитів клієнтів; неправильне визначення відсотків за вкладами;

– кредитні операції: надання кредиту на підроблені чи незаконно отримані документи; позики фіктивним позичальникам; продаж заставного майна за ціною, що нижча за ринкову; підкупи для отримання звільнення від застави чи для зменшення суми позову; не подання інформації про заставне майно для внесення її у державні реєстри обтяжень; завищення вартості активів, що оцінюються з метою передачі у заставу для отримання кредиту; помилки у визначенні фінансового стану та класу позичальника;

– поточні рахунки: незаконне привласнення коштів з рахунків, за якими часто проводяться транзакції;

2) неправдиве відображення фінансової звітності:

– навмисні викривлення;

– пропуск загальних сум;

– виправлення облікових записів;

– некоректне відображення позик на рахунках простроченої чи строкової заборгованості.

Таким чином, для попередження шахрайств банківського персоналу складовою частиною системи незалежного аудиту має бути оцінювання ризику шахрайства персоналу в напрямах неправдивого відображення фінансової звітності та незаконного привласнення активів. Це створює умови для використання ризик-орієнтованого підходу при побудові плану аудиту.

В роботі [63] для кожного виду шахрайства персоналу (викривлення фінансової звітності та незаконне заволодіння активами) виділено пов’язані з ним умови: спонукання до шахрайства, сприятливі можливості для шахрайства, схильність співробітника до шахрайства. Кожна комбінація виду шахрайства та

умови його виникнення пов’язана зі специфічними факторами ризику шахрайства, які, в свою чергу, характеризуються певними індикаторами ризику шахрайства. Ключовою відмінністю між фактором ризику шахрайства та індикатором ризику шахрайства є той факт, що індикатор ризику шахрайства спостерігається аудитором безпосередньо, в той час як фактор ризику шахрайства спостерігається аудитором лише опосередковано через присутність пов’язаних з ним індикаторів ризику шахрайства. Аудитор використовує індикатори ризику шахрайства та власні міркування для прийняття рішення щодо існування специфічного фактору ризику шахрайства персоналу.

На основі опрацювання [64] в роботі [63] запропоновано інноваційний підхід до оцінки ризику шахрайства персоналу, зокрема, вводиться бінарне та нечітке оцінювання аудиторами індикаторів ризику шахрайства персоналу, а також пропонується система оцінювання ризику шахрайства персоналу, побудована на засадах теорії нечіткої логіки. В той же час запропонована в роботі [63] система нечіткого логічного висновку вимагає побудови та відповідного обґрунтування експертної бази нечітких правил. Ми вважаємо, що більш раціональною є побудова узагальнюючої оцінки ризику шахрайства персоналу на основі агрегування нечітких оцінок індикаторів ризику шахрайства з використанням ієрархічного дерева. Агрегований опис містить порівняно з початковим менше інформації, при цьому корисна інформація залишається, а надмірна звужується [65]. Модель оцінювання рівня ризику шахрайства банківського персоналу пропонується представити у вигляді деревоподібного графа з двома рівнями ієрархії (рис. 3.12).

На першому рівні ієрархії фактори ризику шахрайства банківського персоналу характеризуються наборами своїх складових – індикаторів ризику шахрайства банківського персоналу (вхідними змінними X_{ij}), що групуються за відповідними факторами ризику X_i, рівні яких визначаються в результаті агрегування вхідних змінних X_{ij}. На другому рівні ієрархії рівень ризику

шахрайства банківського персоналу в цілому Y визначається в результаті агрегування отриманих на попередньому етапі оцінювання рівнів факторів ризику X_i.

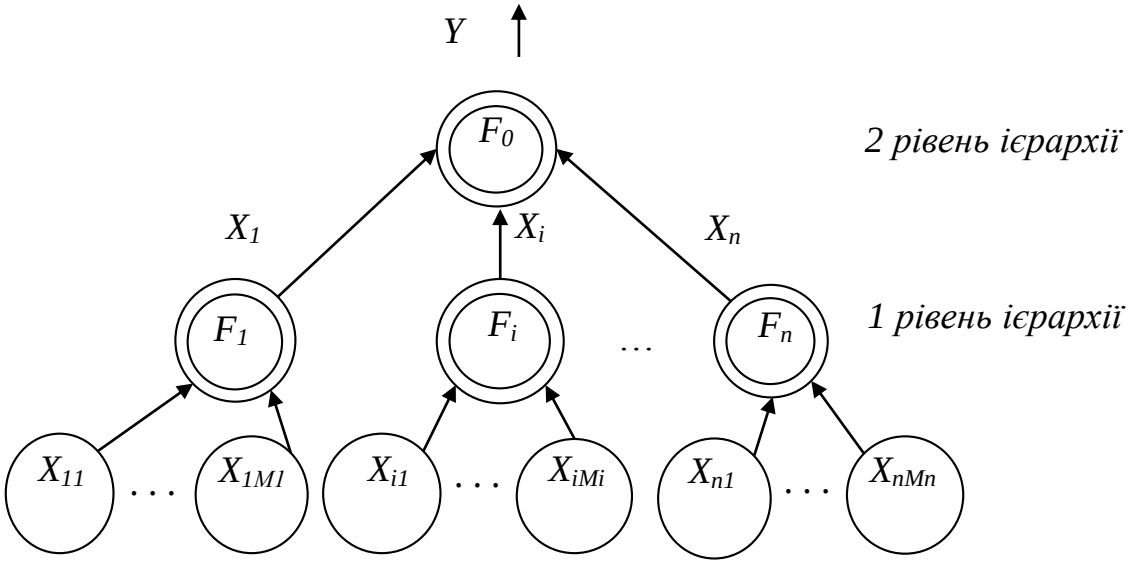


Рисунок 3.12 – Ієрархічна структура моделі оцінювання рівня ризику шахрайства банківського персоналу

Елементи деревоподібного графа (рис. 1) інтерпретуються таким чином:

- кінцеві вершини X_{ij} – оцінки індикаторів ризику, пов'язаних з *i*-тим фактором ризику, $i=\overline{1,n};\ j=\overline{1,M_i}$, де n – кількість факторів ризику, M_i – кількість індикаторів ризику, що пов'язані з *i*-тим фактором ризику через некінцеву вершину F_i;
- некінцеві вершини F_i - функції згорток за факторами ризику X_i, $i=\overline{1,n}$;
- дуги, що виходять із нетермінальних вершин (X_i), – рівні відповідних факторів ризику шахрайства банківського персоналу.
- некінцева вершина F_0 – функція згортки факторів ризику X_i, $i=\overline{1,n}$.
- дуга *Y*, що виходить з кореня дерева, – рівень ризику шахрайства банківського персоналу в цілому;

Кількісне оцінювання індикаторів ризику шахрайства X_{ij} передбачає використання анкет, в яких аудитор зазначає рівень присутності відповідного індикатора ризику в діапазоні від 0 до 1. Якщо аудитор використовує іншу кількісну шкалу, то можна виконати перехід від цієї шкали до 01-носія на основі простого лінійного перетворення. Ми пропонуємо виконати агрегування анкетних оцінок індикаторів ризику шахрайства персоналу за рівнями ієрархії графа, представленого на рис. 3.13, із пересуванням від нижніх рівнів ієрархії до верхніх. Рівень ризику шахрайства банківського персоналу в цілому опишемо наступною нечіткою ієрархічною моделлю:

$$Y=<G, L, S, F>, \qquad (3.2)$$

де G – ієрархічний граф, показаний на рис. 3.12;

L – терм-множина можливих значень лінгвістичних змінних;

S – система відношень пріоритетів індикаторів ризику та факторів ризику;

F – функція згортки нечітких оцінок у відповідних вершинах графа G. Ваги дуг графа відповідають ступеню впливу відповідних індикаторів ризику та факторів ризику на результуючу оцінку.

Оцінки рівнів індикаторів ризику X_{ij}, оцінки рівнів факторів ризику X_i, а також оцінку рівня ризику шахрайства банківського персоналу в цілому Y представимо у вигляді лінгвістичних змінних L_{ij}, L_i та L_Y відповідно. З метою спрощення моделі сформуємо одну терм-множину можливих значень для всіх лінгвістичних змінних L_{ij}, L_i та L_Y з п’яти якісних термів T_{ij}^k, T_i^k, T_Y^k, відповідно: “дуже низький” ($k=1$), “низький” ($k=2$), “середній” ($k=3$), “високий” ($k=4$), “дуже високий” ($k=5$). Кожному нечіткому терму T_{ij}^k лінгвістичної змінної L_{ij} поставимо

у відповідність трапецієподібну функцію належності $\mu_k\left(X_{ij}\right)$ з параметрами $\underline{t_{ij}^k};\overline{t_{ij}^k};a_{ij}^k;b_{ij}^k$ $(k=\overline{1,5})$, наведену на рис. 3.13.

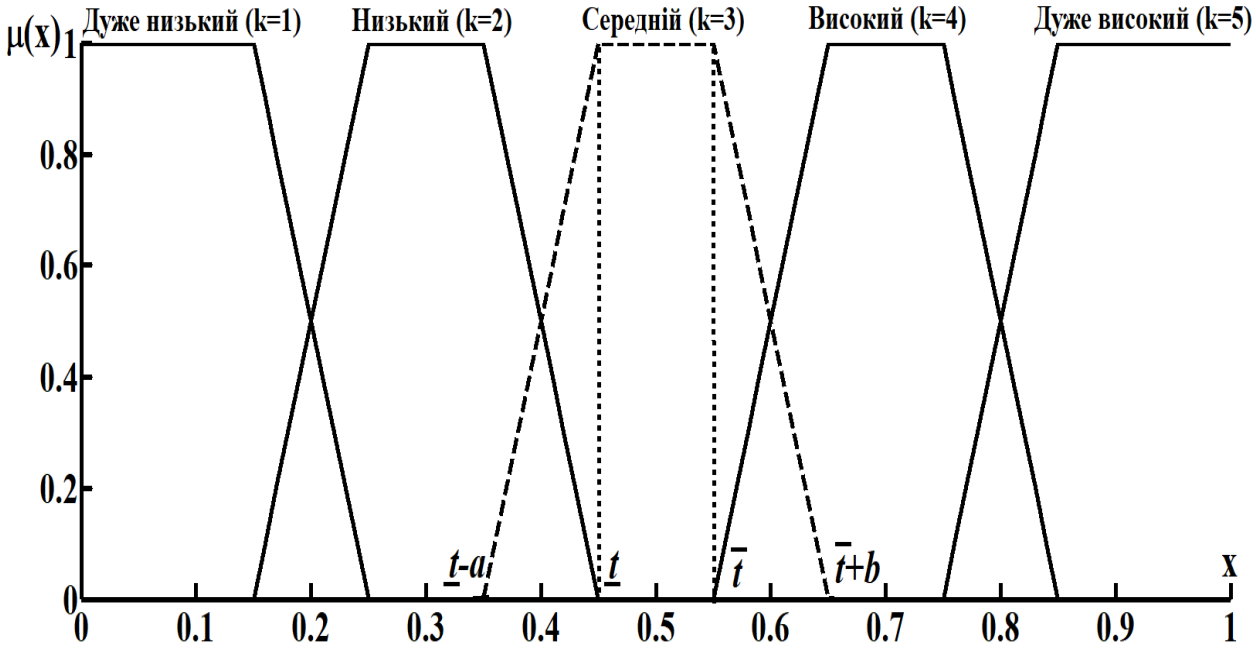


Рисунок 3.13 – Нечітка терм-множина

$$\mu_k\left(X_{ij}\right)=\begin{cases} 0,\ якщо\ X_{ij}\le \underline{t_{ij}^k}-a_{ij}^k\ або\ X_{ij}\ge \overline{t_{ij}^k}+b_{ij}^k \\ \dfrac{X_{ij}-\left(\underline{t_{ij}^k}-a_{ij}^k\right)}{a_{ij}^k},\quad якщо\quad \underline{t_{ij}^k}-a_{ij}^k<X_{ij}<\underline{t_{ij}^k} \\ 1,\quad якщо\quad \underline{t_{ij}^k}\le X_{ij}\le \overline{t_{ij}^k} \\ \dfrac{\left(\overline{t_{ij}^k}+b_{ij}^k\right)-X_{ij}}{b_{ij}^k},\ якщо\quad \overline{t_{ij}^k}<X_{ij}<\overline{t_{ij}^k}+b_{ij}^k \end{cases} \tag{3.3}$$

Аналогічно поступимо і з нечіткими термами T_i^k, T_Y^k $(k=\overline{1,5})$ лінгвістичних змінних L_i і L_Y.

В якості множини функцій належності (3.3) пропонується обрати стандартний нечіткий п’ятирівневий 01-класифікатор з трапецієвидними функціями належності 3.4 – 3.8 [66]:

$$\mu_1\left(X_{ij}\right)=\begin{cases}0, \quad якщо \quad X_{ij}\geq 0,25\\ 10\cdot\left(0,25-X_{ij}\right), \quad якщо \quad 0,15<X_{ij}<0,25\\ 1, якщо\ 0\leq X_{ij}\leq 0,15\end{cases} \tag{3.4}$$

$$\mu_2\left(X_{ij}\right)=\begin{cases}0, якщо\ X_{ij}\leq 0,15\ або\ X_{ij}\geq 0,45\\ 10\cdot\left(X_{ij}-0,15\right), \quad якщо \quad 0,15<X_{ij}<0,25\\ 1, \quad якщо \quad 0,25\leq X_{ij}\leq 0,35\\ 10\cdot\left(0,45-X_{ij}\right), \quad якщо \quad 0,35<X_{ij}<0,45\end{cases} \tag{3.5}$$

$$\mu_3\left(X_{ij}\right)=\begin{cases}0, якщо\ X_{ij}\leq 0,35\ або\ X_{ij}\geq 0,65\\ 10\cdot\left(X_{ij}-0,35\right), \quad якщо \quad 0,35<X_{ij}<0,45\\ 1, \quad якщо \quad 0,45\leq X_{ij}\leq 0,55\\ 10\cdot\left(0,65-X_{ij}\right), \quad якщо \quad 0,45<X_{ij}<0,65\end{cases} \tag{3.6}$$

$$\mu_4\left(X_{ij}\right)=\begin{cases}0, якщо\ X_{ij}\leq 0,55\ або\ X_{ij}\geq 0,85\\ 10\cdot\left(X_{ij}-0,55\right), \quad якщо \quad 0,55<X_{ij}<0,65\\ 1, \quad якщо \quad 0,65\leq X_{ij}\leq 0,75\\ 10\cdot\left(0,85-X_{ij}\right), \quad якщо \quad 0,75<X_{ij}<0,85\end{cases} \tag{3.7}$$

$$\mu_5\left(X_{ij}\right)=\begin{cases}0, \quad якщо \quad X_{ij}\leq 0,75\\ 10\cdot\left(0,85-X_{ij}\right), \quad якщо \quad 0,75<X_{ij}<0,85\\ 1, якщо\ 0,85\leq X_{ij}\leq 1\end{cases} \tag{3.8}$$

Стандартний нечіткий п’ятирівневий 01-класифікатор робить проекцію лінгвістичного опису на 01-носій (відрізок [0,1] дійсної вісі), розташовуючи симетрично вузли класифікації (0.1, 0.3, 0.5, 0.7, 0.9), в яких значення відповідної

функції належності дорівнює одиниці, а всіх інших – нулю (рис. 3.13). Невпевненість аудитора в класифікації лінійно убуває (зростає) при видаленні від вузла (з наближенням до вузла, відповідно). Сума значень функцій належності нечітких термів в усіх точках 01-носія дорівнює одиниці [66].

Агрегування нечітких оцінок лінгвістичних змінних здійснюється за рівнями ієрархії з пересуванням від нижніх рівнів графа *G* (рис. 1) до верхніх. Попередньо аудитор кількісно оцінює рівні вхідних змінних X_{ij} (від 0 до 1) для кінцевих вершин графа.

Для агрегування нечітких оцінок використаємо матричну схему, наведену в [66]. Якщо по рядках матриці відкладені лінгвістичні змінні L_{ij} індикаторів ризику, а по стовпцях – їх нечіткі терми T_{ij}^k $(k=\overline{1,5})$, виражені відповідним набором функцій належності $\mu_k\left(X_{ij}\right)$, то кількісна оцінка фактору ризику X_i в діапазоні від 0 до 1 розраховується за формулою подвійного згортання 3.9 – 3.11:

$$X_i = \sum_{j=1}^{M_i} \omega_{ij} \sum_{k=1}^{5} \left(\alpha_k \cdot \mu_k(X_{ij}) \right), \tag{3.9}$$

$$\sum_{k=1}^{5} \mu_k(X_{ij}) = 1, \tag{3.10}$$

$$\sum_{j=1}^{M_i} \omega_{ij} = 1, \tag{3.11}$$

де ω_{ij} – вага індикатора ризику X_{ij} в оцінюванні фактора ризику X_i;

M_i – кількість індикаторів ризику, що пов'язані з фактором ризику X_i;

$\alpha_k = 0,2 \cdot k - 0,1$ – ваги нечітких термів (так звані вузлові точки стандартного нечіткого п'ятирівневого класифікатора: 0,1; 0,3; 0,5; 0,7; 0;9).

Вагові коефіцієнти ω_{ij} можуть бути отримані на основі побудови системи ваг Фішберна або матриці парних порівнянь. Можна також оцінити вагу відповідних індикаторів ризику X_{ij} з використанням певної бальної шкали, а потім нормалізувати одержані результати.

Розраховане за формулами 3.4-3.11 значення фактору ризику X_i знаходиться в діапазоні від 0 до 1, тому його можна лінгвістично розпізнати за формулами 3.4-3.8. Пройшовши послідовно знизу вгору по всіх рівнях ієрархії *G* і застосовуючи формули 3.4-3.11 ми одержуємо лінгвістичну інтерпретацію оцінки рівня ризику шахрайства банківського персоналу в цілому.

Розглянемо приклад оцінювання ризику шахрайства персоналу щодо викривлення фінансової звітності. Всі фактори ризику шахрайства персоналу класифіковані за такими категоріями:

1. Спонукання до викривлення фінансової звітності.

2. Сприятливі можливості для викривлення фінансової звітності.

3. Обґрунтування викривлення фінансової звітності.

Значущість всіх категорій і факторів ризику вважаємо однаковою. Нормалізовані ваги індикаторів факторів ризику та оцінки аудитором рівнів присутності відповідних індикаторів у об’єкта аудиту наведені в табл. 3.3-3.5.

Таблиця 3.3

Спонукання до викривлення фінансової звітності

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 1.1. Прибутковість знаходиться під загрозою економічних умов діяльності			
1.1.1	Високий ступінь конкуренції або насичення ринку супроводжується зниженням прибутковості	0,128	0,9
1.1.2	Висока чутливість до швидких змін, таких як зміни в технології або зміни процентних ставок	0,128	0,3
1.1.3	Значне зниження споживчого попиту та зростання банкрутств як у галузі, так і в економіці в цілому	0,128	0,1

Продовження таблиці 3.3

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
1.1.4	Операційні збитки, які становлять загрозу банкрутства або недружнього поглинання	0,179	
1.1.5	Повторювані негативні грошові потоки від операцій або неможливість генерувати грошові потоки від операцій при одночасному звітуванні про прибутки та зростання доходів	0,205	
1.1.6	Швидке зростання або незвичайна прибутковість, особливо в порівнянні з іншими установами тієї ж галузі	0,179	0,3
1.1.7	Нові бухгалтерські або нормативні вимоги.	0,052	
Фактор 1.2. Надмірний тиск на керівництво з метою виконання очікувань третіх сторін			
1.2.1	Очікування інвестиційних аналітиків, інституційних інвесторів, великих кредиторів або інших зовнішніх сторін, що стосуються прибутковості, включаючи очікування, створені керівництвом у занадто оптимістичних прес-релізах і щорічних звітах	0,267	0,8
1.2.2	Необхідність отримання додаткового фінансування для забезпечення конкурентоспроможності	0,233	0,2
1.2.3	Гранична здатність погашати борги	0,25	
1.2.4	Негативні наслідки звітування про погані фінансові результати важливих зупинених операцій, таких як злиття або заключення контрактів	0,25	0,2
Фактор 1.3. Отримана інформація свідчить про те, що особистий фінансовий стан керівництва залежить від фінансового стану об’єкта аудиту			
1.3.1	Значні фінансові інтереси в об’єкті аудиту	0,313	0,9
1.3.2	Значна винагорода (наприклад, бонуси, акції), що залежить від досягнення агресивних цілей щодо ціни акцій, операційних результатів, фінансового становища або грошового потоку	0,374	0,9

Продовження таблиці 3.3

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
1.3.3	Особисті гарантії по заборгованості об’єкта аудиту	0,313	
Фактор 1.4. Надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених керівництвом, включаючи цілі стимулювання збуту			
1.4.1	Присутній надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених керівництвом, включаючи цілі стимулювання збуту	1	0,8

Таблиця 3.4

Сприятливі можливості для викривлення фінансової звітності

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 2.1. Характер діяльності об’єкта аудиту надає можливості для викривлення фінансової звітності			
2.1.1	Важливі операції з пов’язаними сторонами здійснюються не за правилами звичайного бізнесу або операції з пов’язаними суб’єктами господарювання не перевірені або перевірені іншою організацією	0,188	
2.1.2	Сильна фінансова присутність або здатність домінувати в певному секторі економіки, яка дозволяє об’єкту аудиту диктувати умови клієнтам, що може призвести до шахрайських операцій	0,141	
2.1.3	Активи, зобов’язання, доходи або витрати базуються на оцінках, що включають суб’єктивні судження або невизначеності, які важко підтвердити	0,165	
2.1.4	Важливі, незвичайні або надзвичайно складні операції, особливо ті, що здійснюються в кінці періоду, які створюють питання “пріоритету змісту над формою”	0,188	
2.1.5	Важливі операції, проведені через міжнародні кордони в юрисдикціях,	0,141	

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
	де існують різні бізнес-середовища та культури		
2.1.6	Значні банківські рахунки або допоміжні операції в юрисдикціях офшорів, для яких немає чіткого ділового обґрунтування	0,176	
Фактор 2.2. Неефективний моніторинг з боку керівництва			
2.2.1	Домінування в управлінні однієї особи без компенсаційних елементів управління	0,548	0,6
2.2.2	Неефективний нагляд з боку правління або комітету з питань аудиту за процесом фінансової звітності та внутрішнього контролю	0,452	
Фактор 2.3. Складна організаційна структура			
2.3.1	Труднощі у визначенні організації або окремих осіб, які мають контрольний пакет акцій в об’єкті аудиту	0,304	
2.3.2	Надмірна організаційна структура, що включає незвичайні юридичні особи або управлінські гілки	0,348	
2.3.3	Висока плинність вищого керівництва та юрисконсультів	0,348	
Фактор 2.4. Недостатні компоненти внутрішнього контролю			
2.4.1	Неадекватний моніторинг, включаючи автоматизований контроль та контроль за проміжною фінансовою звітністю (там, де потрібна зовнішня звітність)	0,333	0,8
2.4.2	Високий коефіцієнт плинності кадрів або використання неефективного обліку, внутрішнього аудиту або ІТ-персоналу	0,333	
2.4.3	Неефективний облік і інформаційні системи, включаючи ситуації, які стосуються умов, що підлягають звітуванню	0,333	

Таблиця 3.5

Обґрунтування викривлення фінансової звітності

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 3.1. Наявність у керівництва або співробітників поглядів, що дозволяють їм брати участь або обґрунтовувати викривлення фінансової звітності			
3.1.1	Неефективне впровадження, підтримка або дотримання цінностей або етичних норм об'єкта аудиту керівництвом	0,058	0,8
3.1.2	Надмірна участь нефінансового менеджменту у виборі принципів бухгалтерського обліку або визначенні важливих оцінок	0,079	
3.1.3	Відома історія порушень законів і нормативних актів або претензій до об'єкту аудиту, його вищого керівництва, які стверджують про шахрайство або порушення законів і правил	0,092	
3.1.4	Надмірна зацікавленість керівництва в збільшенні цін акцій або доходів суб'єкта аудиту	0,089	0,8
3.1.5	Практика керівництва щодо надавання аналітикам, кредиторам та іншим третім сторонам агресивних або нереальних прогнозів	0,089	0,8
3.1.6	Неспроможність керівництва своєчасно виправити ситуацію, що підлягає звітуванню	0,079	
3.1.7	Інтерес керівництва до використання невідповідних засобів для мінімізації податків	0,089	
3.1.8	Повторні спроби керівництва виправдати невідповідний облік на об'єкті аудиту	0,079	
3.1.9	Часті суперечки з поточним або попереднім аудитором з питань бухгалтерського обліку, аудиту або звітності	0,074	
3.1.10	Невиправдані вимоги до аудитора, такі як необґрунтовані часові	0,088	

Продовження таблиці 3.5

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
	обмеження щодо завершення аудиту або видачі аудиторського звіту		
3.1.11	Формальні або неформальні обмеження аудитора, які неналежним чином обмежують його доступ до людей або інформації або здатність аудитора ефективно спілкуватися з керівництвом або комітетом з аудиту	0,092	
3.1.12	Домінуюча поведінка керівництва в роботі з аудитором, особливо в тому, що стосується спроб вплинути на масштаб роботи аудитора або на вибір персоналу, призначеного для аудиту	0,092	

Розрахунок кількісних оцінок факторів ризику шахрайства персоналу здійснено за формулами 3.5-3.12 з використанням інформації, наведеної в таблицях 3.3-3.5. Інтерпретація рівнів кількісних оцінок факторів ризику шахрайства персоналу здійснена за формулами 3.5-3.9. Результати наведені в табл. 3.6.

Таблиця 3.6

Розпізнавання рівнів факторів ризику шахрайства персоналу

I	Фактор ризику шахрайства персоналу	Кількісна оцінка	Функції належності для рівнів *i*-го фактору ризику шахрайства персоналу				
			Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
1	Фактор 1.1	0,22	0,3	0,7			
2	Фактор 1.2	0,31		1			
3	Фактор 1.3	0,618			0,32	0,68	
4	Фактор 1.4	0,8				0,5	0,5
5	Фактор 2.2	0,329		1			
6	Фактор 2.4	0,266		1			
7	Фактор 3.1	0,189	0,61	0,39			

Розрахунок кількісної оцінки ризику шахрайства персоналу по категоріях здійснено за формулами 3.4-3.11 з використанням інформації, наведеної в таблиці 3.6. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу по категоріях здійснена за формулами 3.4-3.8. Результати наведені в табл. 3.7.

Таблиця 3.7

Розпізнавання рівнів ризику шахрайства персоналу по категоріях

Категорія ризику шахрайства	Кількісна оцінка	Функції належності для рівнів категорій ризику шахрайства				
		Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
Категорія 1	0,5	-	-	1	-	-
Категорія 2	0,3	-	1	-	-	-
Категорія 3	0,178	0,72	0,28	-	-	-

Розрахунок кількісної оцінки ризику шахрайства персоналу в цілому здійснено за формулами 3.4-3.11 з використанням інформації, наведеної в таблиці 3.6. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу в цілому здійснена за формулами 3.4-3.8. Результати наведені в табл. 3.8.

Таблиця 3.8

Розпізнавання рівня ризику шахрайства персоналу в цілому

Кількісна оцінка	Функції належності для рівнів ризику шахрайства персоналу в цілому				
	Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
0,4		0,5	0,5		

Згідно з наведеними в таблицях 3.6-3.8 результатами рівень ризику шахрайства персоналу в цілому – проміжний між лінгвістичними оцінками «Середній» і «Низький», але об’єкт аудиту характеризується високим рівнем фактору ризику 1.3 (особистий фінансовий стан керівництва залежить від фінансового стану об’єкта аудиту) та високим рівнем фактору ризику 1.4 (надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених

керівництвом, включаючи цілі стимулювання збуту). Це означає, що існує високий рівень ризику викривлення фінансової звітності через спонукання до викривлення фінансової звітності, бо саме до цієї категорії належать фактори ризику 1.3 і 1.4. Тому аудитор повинен ретельно дослідити саме цю сферу.

3.4. Використання гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом

На сьогоднішній день найважливішими питаннями, що турбують усе світове співтовариство, є розвиток економіки на всіх рівнях, глобалізація, забезпечення суспільного економічного добробуту. Та всі етапи такого розвитку постійно супроводжуються відповідними негативними процесами та явищами. Так як поряд із збільшенням об'ємів операцій, що проводяться через фінансові ринки, зростанням активів, грошових потоків, збільшенням обсягів торгівельних процесів, у злочинців з'являється можливість здійснювати вільний обіг незаконних коштів. Отже, зростання злочинності, переміщення нелегальних грошей, розвиток тероризму наразі є найголовнішими питаннями для вирішення світовою спільнотою. Ці проблеми перетворились у глобальні загрози для всього фінансового світу, та, відповідно, економічної безпеки національної економіки.

Об'єднання в одну систему обігу капіталу, товарів та послуг, а також різних напрямів фінансових сегментів для подальшого розвитку, покращення добробуту суспільства, забезпечення безпеки, характеризують категорію економічної безпеки. Протягом останніх років через трансформацію світової економічної системи проблемі забезпечення економічної безпеки притаманні новітні аспекти. Сьогоденні тренди, що описують сучасну модернізацію економічної системи, суттєво впливають на забезпечення економічної безпеки за нових умов [67, 68, 69, 70].

Протягом останніх років міжнародне співтовариство у економіці багато уваги та дій проводить у частині дослідження та аналізу взаємовідносин політики та

злочинного світу [71, 72, 73, 74, 75]. Для виявлення та зупинення потоків незаконних коштів по всіх можливих каналах, заходи по перешкоджанню фінансуванню злочинних зв'язків потрібно проводити не тільки у середині країни, а й за її межами. Відмивання нелегальних коштів, «тінізація» економіки, фінансування тероризму вкрай руйнівно позначаються на економічній безпеці країни, викликають суспільний дисбаланс, погіршують економічний устрій. У світовій економічній науковій літературі науковцями та дослідниками висвітлюються відповідні намагання зробити кількісний вимір процесів і дій, що стосуються відмивання нелегальних коштів [76, 77, 78,79]. Але через те, що процеси відмивання грошей здійснюються доволі приховано, непомітно, таємно, то оцінити ефективність, достатність, результативність, адекватність таких моделей дуже складно і проблематично.

Не дивлячись на те, що вже проведено багато роботи стосовно вивчення питання дослідження незаконних операцій з грошовими коштами, наразі не розроблено достатньо ефективних систем та моделей управління фінансово-економічною системою стосовно легалізації злочинних коштів та фінансування терористичної діяльності. Наряду з цим немає інструментів, що могли б попереджувати завчасно процеси легалізації. Це призводить до руйнування національної економічної безпеки. Вирішення питань економіки відмивання злочинних доходів, направлених на дослідження об'ємів і впливу нелегальних грошей, виступає доволі новою сферою і тому вимагає поглибленого вивчення та аналізу. Використання гравітаційних моделей для проведення оцінки ризику легалізації нелегальних коштів і фінансування тероризму між країнами, в якості одного з дієвих інструментів системи національної економічної безпеки, зараз є вкрай актуальним і далі тільки загострюється [80, 81, 82,83].

Для проведення дослідження було сформовано набір даних по 65 банкам України за 2019 рік. Набір даних представляє собою статистичну інформацію, яку було отримано за результатом запиту до Національного банку України. Так, було узято 6 показників: К1 - частка фінансових операцій, зареєстрованих за ознаками

внутрішнього фінансового моніторингу; К2 - Порушення ПП НБУ; К3 - Порушення ЗУ "Про легалізацію"; К4 - ЗУ "Про банки"; К5 - Частка надходжень готівкових коштів від загальної суми надходжень; К6 - Частка видатків готівкових коштів від загальної суми видатків.

Розглянемо методику розрахунку кожного із зазначених числових характеристик діяльності комерційних банків:

$$K_1 = \frac{K_{ФОВФМ}}{K_{ЗКФО}} \qquad (3.12)$$

де $К_1$ - частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу;

$К_{ФОВФМ}$- кількість фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу;

$К_{ЗКФО}$- загальна кількість зареєстрованих фінансових операцій.

Даний показник дозволяє певною мірою оцінити якість здійснення банком внутрішнього фінансового моніторингу (*далі – ВФМ*), який через свій комплементарний характер є менш формальним на відміну від обов'язкового фінансового моніторингу (*далі – ОФМ*), а, отже, і більш ризиковим напрямком фінансового моніторингу банку.

$К_2$– кількість порушень ПП НБУ.

$К_3$- кількість порушень ЗУ «Про запобігання».

$К_4$- кількість порушень ЗУ «Про банки».

Показники, що розглядаються, свідчать про кількість виявлених в ході останньої інспекційної перевірки Національного банку України порушень банком законодавства України в сфері протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму в розрізі конкретних нормативно-правових актів.

$К_5$- частка надходжень готівкових коштів на рахунки за вкладами фізичних осіб (символ 16) від загальної суми надходжень на рахунки фізичних осіб (за символами 16 та 88).

Дане співвідношення розкриває структуру надходжень коштів на користь фізичних осіб, уможливлюючи здійснення оцінки обсягів внесених фізичними особами готівкових коштів.

$К_6$- частка видатків коштів за вкладами фізичних осіб (символ 55) від загальної суми видатків фізичних осіб (за символами 55 та 95).

Вище зазначений показник також слугує одним із базових індикаторів ризику залучення банку до так званої «конвертаційної» схеми.

Для оцінки ризику легалізації кримінальних доходів та фінансування тероризму пропонуємо методику, в основі якої знаходиться *гравітаційне моделювання*.

На першому етапі необхідно провести нормалізацію даних в межах другого, третього та четвертого показників. Це пов'язано з тим, що показники, які ми використовуємо для побудови моделі, мають різну розмірність. Тому їх треба привести до вигляду від 0 до 1. Також треба врахувати той факт, що дані показники впливають по різному на ризик легалізації кримінальних доходів. Тобто, збільшення значення показника призводить до покращення ситуації, тобто зменшення значення ризику, і навпаки. Відповідно, ми маємо справу із стимулятором. Якщо зміни значення показника призводять до погіршення обставин, тобто із збільшенням показника ризик збільшується, і навпаки, то мова йде про дестимулятор. Для нормалізації використаємо рівняння абсолютної нормалізації 3.13, що дозволить нам здійснити її як для стимуляторів, так й де стимуляторів [84].

$$x_{ij}^{+} = \frac{x_{ij}}{x_{max_j}}, x_{ij}^{-} = \frac{x_{min_j}}{x_{ij}}, \quad (3.13)$$

де x^{+}_{ij} , x^{-}_{ij} – нормалізоване значення j-го показника характеристики рівня ризику легалізації кримінальних доходів та фінансування тероризму, як для стимуляторів (+), так й для дестимуляторів (-), для і-ого розглянутого банку;

x_{ij} – початкове (емпіричне) значення j-го показника характеристики рівня ризику легалізації для і-ого банку;

x_{minj} – мінімальна величина j-го показника характеристики визначення рівня ризику легалізації для всіх банків дослідження;

x_{maxj} – максимальна величина j-го показника характеристики визначення рівня ризику легалізації для всіх банків дослідження.

На другому етапі методики розрахунку визначаємо вагові коефіцієнти для обраних показників. З цією метою використовується метод головних компонент. Для реалізація даного етапу пропонується застосувати наступну послідовність обчислень: 1) за допомогою інструментарію програмного пакету Statistica 8.0 Statistica, Multivariate Exploratory Techniques, Principal Components&Classification Analysis побудувати графік кам'янистого осипу, таблицю власних значень, таблицю факторних навантажень; 2) за допомогою графіку кам'янистого осипу визначення релевантних факторів, сумарна дисперсія впливу в розрізі яких складає не менше 70%; 3) на основі значень факторних навантажень та дисперсії впливу факторів обчислення суми добутків факторних навантажень на дисперсію впливу відповідних факторів (графа 4 таблиці 3.9); 4) визначення вагових коефіцієнтів пріоритетності показників оцінювання ризику легалізації банків за допомогою формули (3) (графа 5 таблиці 3.9).

Таблиця 3.9

Проміжні розрахунки обчислення вагових коефіцієнтів показників оцінювання рівня ризику легалізації

	Factor 1	…	Factor m	Сума добутків факторних навантажень на дисперсію впливу відповідних факторів	Ваги показників
A	1	2	3	4	5
x_1	f_{11}	…	f_{1m}	$\sum_{k=1}^{m} f_{1k} \cdot \sigma_k^2$	$\frac{\sum_{k=1}^{m} f_{1k} \cdot \sigma_k^2}{\sum_{j=1}^{n} \sum_{k=1}^{m} f_{1k} \cdot \sigma_k^2}$
…	…	…	…	…	…
x_j	f_{j1}	…	f_{jm}	$\sum_{k=1}^{m} f_{jk} \cdot \sigma_k^2$	$\frac{\sum_{k=1}^{m} f_{jk} \cdot \sigma_k^2}{\sum_{j=1}^{n} \sum_{k=1}^{m} f_{jk} \cdot \sigma_k^2}$
…	…	…	…	…	…
x_n	f_{n1}	…	f_{nm}	$\sum_{k=1}^{m} f_{nk} \cdot \sigma_k^2$	$\frac{\sum_{k=1}^{m} f_{nk} \cdot \sigma_k^2}{\sum_{j=1}^{n} \sum_{k=1}^{m} f_{1k} \cdot \sigma_k^2}$
Дисперсія впливу факторів	σ_1^2	…	σ_m^2		

Таким чином, розрахункова формула для обчислення вагових коефіцієнтів пріоритетності показників оцінювання ризику легалізації банків набуває вигляду 3.14:

$$\omega_j = \frac{\sum_{k=1}^{m} f_{jk} \cdot \sigma_k^2}{\sum_{j=1}^{n} \sum_{k=1}^{m} f_{jk} \cdot \sigma_k^2}, \quad (3.14)$$

де ω_j–ваговий коефіцієнт пріоритетності j-го показника оцінювання ризику легалізації кримінальних доходів банків;

f_{jk}– значення факторного навантаження k-го фактору в розрізі j-го показника;

σ^2_k– дисперсія впливу k-го фактору.

Після знаходження вагових коефіцієнтів *на третьому етапі* визначається інтегральний показник кількісної оцінки рейтингу певної країни щодо характеристики визначення рівня ризику легалізації кримінальних доходів та фінансування тероризму за допомогою метрики Мінковського (формула 3.15) [85], який дозволяє враховувати вплив факторів на основі їх позицій, як стимуляторів, так і дестимуляторів:

$$IRA_i = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left|1 - x_{ij}^{+}\right|^2 + \sum_{j=k+1}^{n} \omega_j \left|1 - x_{ij}^{-}\right|^2}, \quad (3.15)$$

де IRA_i– інтегральна рейтингова оцінка характеристики рівня ризику легалізації для і-ого банку;

ω_j– вагові коефіцієнти для j-го показника.

З урахуванням того, що для оцінки ризику легалізації кримінальних доходів та фінансування тероризму було обрано 6 показників, формула для визначення інтегрального показника матиме наступний вигляд (формула 3.16):

$$IRA(x_i) = 1 - \sqrt{\begin{matrix}\omega_1(1-x_1^{+})^2 + \omega_2(1-x_2^{+})^2 + \omega_3(1-x_3^{+})^2 + \omega_4(1-x_4^{-})^2 + \\ \omega_5(1-x_5^{+})^2 \quad + \omega_6(1-x_6^{+})^2\end{matrix}}, \quad (3.16)$$

де x^{+}_i - це фактичне значення частки фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу, як фактора-стимулятора;

x^{+}_2- це нормалізоване значення показника порушення ПП НБУ, як фактора-стимулятора;

x^{+}_3- це нормалізоване значення показника порушення ЗУ "Про легалізацію", як фактора-стимулятора;

x^+_4- це нормалізоване значення показника порушення ЗУ "Про банки", як фактора-стимулятора;

x^+_5- це фактичне значення частки надходжень готівкових коштів від загальної суми надходжень, як фактора-стимулятора;

x^+_6- це фактичне значення частки видатків готівкових коштів від загальної суми видатків, як фактора-стимулятора.

Отримане значення інтегрального показника буде варіюватися в межах від 0 до 1.

Наступним *четвертим етапом* буде побудова гравітаційної моделі ризику легалізації. З цією метою за основу використаємо рівняння закону гравітаційного тяжіння та гравітаційної сили в суспільних явищах, тобто формулу 3.17:

$$M_{ij} = k\frac{p_i p_j}{d_{ij}^2}, \tag{3.17}$$

де M_{ij}– показник взаємодії між об’єктами і та j;

k – коефіцієнт відповідності;

p – деяка значимість об’єкта;

d^2_{ij}– відстань між об’єктами.

Даний підхід було розглянуто у праці Walter Isard "Location Theory and Trade Theory: Short-RunAnalysis" (1954) для міжнародної торгівлі у міжнародній економіці.

Ризик легалізації ідентифікується наступним чином: окремий банк «притягує» ризикові операції з силою, що прямо пропорційна рейтинговій оцінці характеристики рівня ризику легалізації розглянутого банку та «нормативного» банку, а також обернено пропорційна квадрату величини «відстань» (кількісна оцінка відмінності) між даним банком та «нормативним» банком у процесі здійснення ризикових операцій (формула 3.18):

$$SVA_r = \frac{IRA_k \cdot IRA_r}{d_{kr}^2},, \tag{3.18}$$

де SVAr – кількісна оцінка величини (сили) взаємодії між певним розглянутим банком та k-им «нормативним» банком в розрізі ризику легалізації;

IRAk – інтегральна рейтингова оцінка характеристики рівня ризику легалізації k-ого банку, яка передає ризик у цесію;

IRAr – інтегральна рейтингова оцінка характеристики рівня ризику легалізації r-ого банку, яка приймає ризик легалізації;

dkr – величина, яка представляє собою нормалізовану різницю між «нормативним» k-им та r-им банками.

В розрізі даного дослідження формула (3.18) трансформується наступним чином:

варіант 1 (формула 3.19 і 3.20), де в якості «нормативного» банку розглядаються показники максимального можливого значення інтегральної рейтингової оцінки характеристики рівня ризику легалізації за метрикою Мінковського;

варіант 2 (формула 3.21 і 3.22), де в якості «нормативного» банку розглядаються показники середнього значення інтегральної рейтингової оцінки характеристики рівня ризику легалізації за метрикою Мінковського.

Отже, для оцінювання ризику легалізації за першим варіантом, використовується формула 3.19:

$$SVA_i = \frac{IRA_i \cdot \max\limits_i IRA_i}{d_r^2}, \tag{3.19}$$

для обчислення знаменнику використовується рівняння 3.20:

$$d_r = \left| 1 - \frac{VK_r}{\max\limits_r VK_r} - \sigma\left(\frac{VK_r}{\max\limits_r VK_r}\right) \right| \ , \tag{3.20}$$

де VK_r – значення власного капіталу для банку k;

$\sigma(\frac{VK_r}{\max\limits_r VK_r})$ – середньоквадратичне відхилення нормалізованого відносним методом (для показника стимулятора) значення власного капіталу для банку r.

Для оцінювання ризику легалізації за першим варіантом, використовується формула 3.21:

$$SVA_i = \frac{IRA_i \cdot \frac{\sum_i IRA_i}{65}}{d_r^2}, \tag{3.21}$$

для обчислення знаменнику використовується рівняння 3.22:

$$d_r = \left| \frac{\sum_r \frac{VK_r}{\max\limits_r VK_r}}{62} - \frac{VK_r}{\max\limits_r VK_r} - \sigma(\frac{VK_r}{\max\limits_r VK_r}) \right| \tag{3.22}$$

де $\frac{\sum_r \frac{VK_r}{\max\limits_r VK_r}}{62}$ – середнє значення нормалізованого відносним методом (для показника стимулятора) значення власного капіталу для банку r.

Але при побудові даної матриці необхідно значення знов нормалізувати, оскільки кількісна оцінка ризику повинна бути від 0 до 1. Для цього використовуємо рівняння нормалізації Харрінгтона (формула 3.23) для першого та другого варіантів, яка дозволить нам врахувати розкид в отриманих значеннях, тобто:

$$SVA_i' = \exp(-\exp(-SVA_i)). \tag{3.23}$$

Отримане значення буде знаходитися в межах від 0 до 1 та свідчити: якщо значення наближається до 0, то банк, в якому здійснюється легалізація коштів,

буде мати підвищений рівень привабливості для легалізації; якщо значення наближається до 1, то банк матиме низький рівень привабливості.

Останнім етапом обчислень в розрізі оцінювання ризику легалізації кримінальних доходів за і-им банком виникає необхідність виведення узагальнюючої характеристик з оцінок, визначених за першим і другим варіантами, шляхом визначення середньої арифметичної величини 3.24:

$$SVA_i^* = \frac{SVA'_{1i} + SVA'_{2i}}{2}. \quad (3.24)$$

де SVA^*_i- узагальнююча оцінка ризику використанням і-го банку для легалізації кримінальних доходів;

SVA'_i - оцінка ризику використанням і-го банку для легалізації кримінальних доходів за першим варіантом, який ґрунтується на максимально можливих величинах метрики Мінковського;

SVA'_{2i} - оцінка ризику використанням і-го банку для легалізації кримінальних доходів за другим варіантом, який ґрунтується на максимально можливих величинах метрики Мінковського.

Розрахунки проводилися із використанням MS Excel, для чого використано дані в розрізі 65 банків України за 2019 рік (табл. 3.10).

Таблиця 3.10

Вхідна статистична база дослідження ризику використання банків для легалізації кримінальних доходів

нумерація банків	К1 – частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу	К2 - Порушення ПП НБУ	К3 - Порушення ЗУ "Про легалізацію"	К4 - ЗУ "Про банки"	К5 – Частка надходжень готівкових коштів від загальної суми надходжень	К6 – Частка видатків готівкових коштів від загальної суми видатків
1	0,0760	20	48	0	0,6305	0,1815
2	0,2013	100	100	34	0,5588	1,0000
3	0,0798	25	29	6	0,7306	0,2668
4	0,1107	38	86	7	0,5571	0,2163
5	0,1376	7	0	0	0,7043	0,2532
6	0,1239	0	0	0	0,7919	0,3932
7	0,0525	1	0	0	0,8879	0,4456
8	0,1739	0	29	3	0,7715	0,4377
9	0,0514	6	97	27	0,9017	0,4259
10	0,0260	0	37	100	0,8243	0,4176
…	…	…	…	…	…	…
56	0,0557	0	0	0	0,9748	0,4518
57	0,1591	0	0	0	0,7433	0,2615
58	0,4023	0	0	1	0,9921	0,3738
59	0,2313	0	0	0	0,8924	0,4091
60	0,0000	0	0	0	0,6902	0,7707
61	0,0506	0	0	0	0,8704	0,3992
62	0,0096	2	0	0	0,9421	0,2653
63	0,0000	0	0	0	0,8368	0,2434
64	0,1231	0	0	0	0,9675	0,4132
65	0,0000	7	0	0	0,0000	0,0632

На першому етапі методики проведено нормалізацію факторів-стимуляторів для другого, третього та четвертого показників (табл. 3.11).

Таблиця 3.11

Нормалізовані значення показників оцінювання ризику використання банків для легалізації кримінальних доходів

нумерація банків	К1 – частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу	К2 - Порушення ПП НБУ	К3 - Порушення ЗУ "Про легалізацію"	К4 - ЗУ "Про банки"	К5 – Частка надходжень готівкових коштів від загальної суми надходжень	К6 – Частка видатків готівкових коштів від загальної суми видатків
1	0,0760	0,2	0,48	0	0,6305	0,1815
2	0,2013	1	1	0,34	0,5588	1,0000
3	0,0798	0,25	0,29	0,06	0,7306	0,2668
4	0,1107	0,38	0,86	0,07	0,5571	0,2163
5	0,1376	0,07	0	0	0,7043	0,2532
6	0,1239	0	0	0	0,7919	0,3932
7	0,0525	0,01	0	0	0,8879	0,4456
8	0,1739	0	0,29	0,03	0,7715	0,4377
9	0,0514	0,06	0,97	0,27	0,9017	0,4259
10	0,0260	0	0,37	1	0,8243	0,4176
…	…	…	…	…	…	…
56	0,0557	0	0	0	0,9748	0,4518
57	0,1591	0	0	0	0,7433	0,2615
58	0,4023	0	0	0,01	0,9921	0,3738
59	0,2313	0	0	0	0,8924	0,4091
60	0,0000	0	0	0	0,6902	0,7707
61	0,0506	0	0	0	0,8704	0,3992
62	0,0096	0,02	0	0	0,9421	0,2653
63	0,0000	0	0	0	0,8368	0,2434
64	0,1231	0	0	0	0,9675	0,4132
65	0,0000	0,06	0	0	0,0000	0,0632

На другому етапі – отримано результати важливості факторів. Так, на основі аналізу графіку кам’янистого осипу (рис. 3.14) та матриці власних значень (рис. 3.15) можна зробити висновок про необхідність врахування трьох перших головних компонент для подальшого визначення вагових коефіцієнтів показників оцінювання ризику використання банків з метою легалізації кримінальних доходів, оскільки саме врахування трьох перших головних компонент забезпечить досягнення дисперсії впливу рівня, не менше 70%.

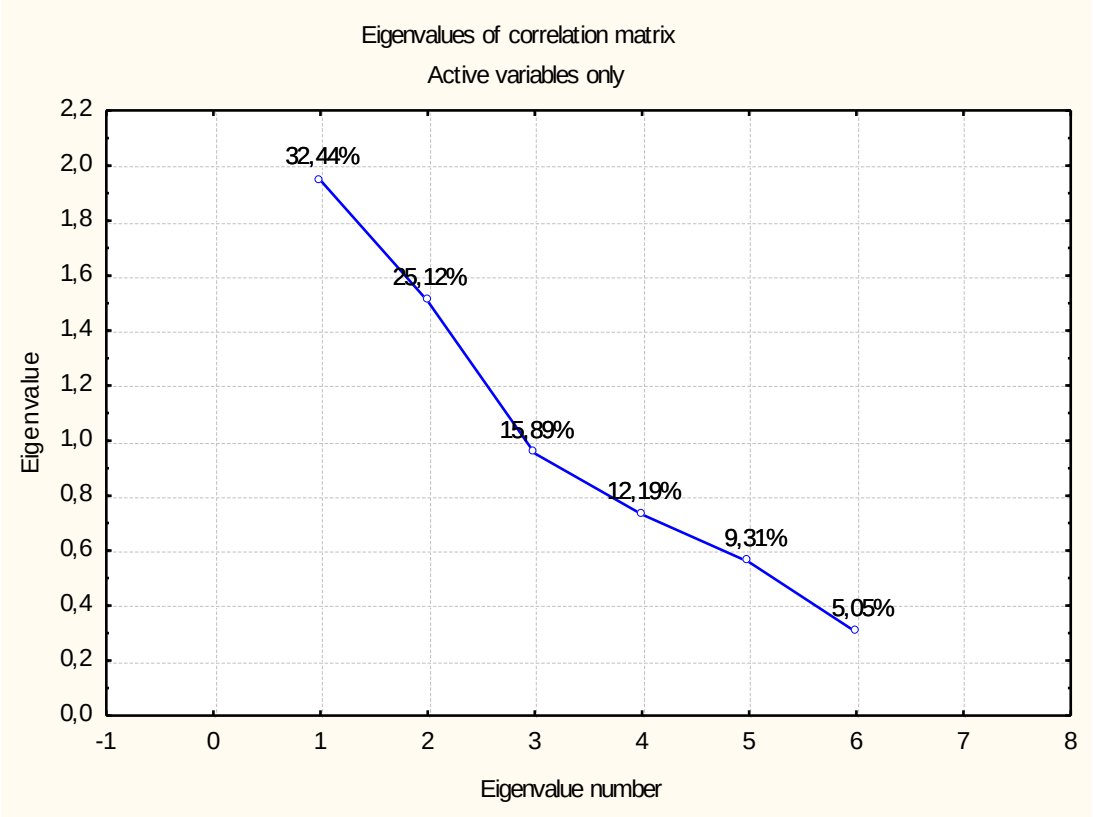


Рисунок 3.14 – Графік кам’янистого осипу в розрізі методу головних компонент оцінювання ризику використання банків з метою легалізації кримінальних доходів

Value number	Eigenvalues of correlation matrix, and related stati Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	1,94662	32,4436	1,94662	32,443
2	1,50744	25,1240	3,45406	57,567
3	0,95339	15,8898	4,40745	73,457
4	0,73114	12,1858	5,13860	85,643
5	0,55832	9,3054	5,69693	94,948
6	0,30306	5,0511	6,00000	100,000

Рисунок 3.15 – Матриця власних значень в розрізі методу головних компонент оцінювання ризику використання банків з метою легалізації кримінальних доходів

Обчислення вагових коефіцієнтів пріоритетності показників оцінювання ризику використання банків з метою легалізації кримінальних доходів

ґрунтується на використанні факторних навантажень в розрізі 6 обраних для дослідження показників за трьома першими головними компонентами (рис. 3.16).

Variable	Variable contributions, based on correlations (2019 vlasn					
	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6
Var1	0,00401	0,23020	0,44013	0,28899	0,01225	0,02438
Var2	0,30083	0,04395	0,19474	0,05279	0,00121	0,40645
Var3	0,36923	0,02727	0,00009	0,00032	0,22337	0,37968
Var4	0,19721	0,01040	0,24588	0,39663	0,11975	0,03010
Var5	0,00749	0,44214	0,10469	0,00016	0,32888	0,11661
Var6	0,12120	0,24601	0,01444	0,26108	0,31451	0,04274

Рисунок 3.16 – Матриця факторних навантажень в розрізі методу головних компонент оцінювання ризику використання банків з метою легалізації кримінальних доходів

Таким чином, узагальнення проміжних розрахунків обчислення вагових коефіцієнтів показників оцінювання рівня ризику легалізації представимо в таблиці 3.12.

Таблиця 3.12

Проміжні розрахунки обчислення вагових коефіцієнтів показників оцінювання рівня ризику легалізації

	Factor1	Factor2	Factor m	Сума добутків факторних навантажень на дисперсію впливу відповідних факторів	Ваги показників
A	1	2	3	4	5
x_1	0,0040	0,2302	0,4401	12,9078	0,1757
x_2	0,3008	0,0440	0,1947	13,9590	0,1900
x_3	0,3692	0,0273	0,0001	12,6662	0,1724
x_4	0,1972	0,0104	0,2459	10,5670	0,1439
x_5	0,0075	0,4421	0,1047	13,0152	0,1772
x_6	0,1212	0,2460	0,0144	10,3425	0,1408
Дисперсія впливу факторів	32,4437	25,1241	15,8899		

За результатами отриманих вагів видно, що найбільшу вагу має показник Порушення ПП НБУ, Частка надходжень готівкових коштів від загальної суми надходжень, частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу. Тобто дані показники чинять найбільший вплив на оцінку ризику легалізації кримінальних доходів. Розраховані ваги дозволили авторам розрахувати інтегрований показник оцінки ризику та знайти кількісну оцінку величини (сили) взаємодії між певним розглянутим банком та «нормативним» k-тим банком в розрізі ризику легалізації.

Для проведення аналізу авторами було обрано Україну станом на 2019 рік. В таблицях 3.13 – 3.14 та рисунку 3.17 представлено результати проміжних розрахунків.

Таблиця 3.13

Проміжні розрахунки оцінювання ризику використання банків для легалізації кримінальних доходів

$\omega_1(1-x_1^+)^2$	$\omega_2(1-x_2^+)^2$	$\omega_3(1-x_3^+)^2$	$\omega_4(1-x_4^-)^2$	$\omega_5(1-x_5^+)^2$	$\omega_6(1-x_6^+)^2$	$IRA(x_i)$	Norm reserv	SVA_{1i}	SVA'_{1i}	SVA_{2i}	SVA'_{2i}	SVA_i^*
1	2	3	4	5	6	7	8	9	10	11	12	13
0,150	0,122	0,047	0,144	0,024	0,094	0,238	1,000	6,971	0,999	0,037	0,381	0,443
0,112	0,000	0,000	0,063	0,034	0,000	0,543	0,352	1,123	0,722	0,526	0,554	0,460
0,149	0,107	0,087	0,127	0,013	0,076	0,253	0,181	0,294	0,475	0,671	0,600	0,487
0,139	0,073	0,003	0,124	0,035	0,086	0,321	0,152	0,344	0,492	1,079	0,712	0,488
0,131	0,164	0,172	0,144	0,015	0,079	0,160	0,239	0,222	0,449	0,285	0,472	0,495
0,135	0,190	0,172	0,144	0,008	0,052	0,163	0,150	0,174	0,431	0,555	0,563	0,497
0,158	0,186	0,172	0,144	0,002	0,043	0,160	0,151	0,171	0,430	0,541	0,559	0,519
0,120	0,190	0,087	0,135	0,009	0,045	0,234	0,124	0,233	0,453	1,015	0,696	0,528
0,158	0,168	0,000	0,077	0,002	0,046	0,328	0,143	0,343	0,492	1,198	0,740	0,537

Продовження таб. 3.13

1	2	3	4	5	6	7	8	9	10	11	12	13
0,167	0,190	0,068	0,000	0,005	0,048	0,308	0,095	0,283	0,471	1,827	0,851	0,546
0,137	0,190	0,172	0,144	0,024	0,042	0,157	0,058	0,131	0,416	1,493	0,799	0,574
0,174	0,190	0,172	0,144	0,047	0,105	0,088	0,060	0,074	0,395	0,814	0,642	0,588
0,175	0,186	0,140	0,135	0,002	0,061	0,163	0,072	0,142	0,420	1,272	0,755	0,602
0,137	0,186	0,005	0,135	0,003	0,018	0,304	0,047	0,248	0,458	3,377	0,966	0,607
0,114	0,190	0,172	0,144	0,072	0,087	0,117	0,079	0,103	0,406	0,840	0,649	0,616
0,158	0,190	0,146	0,144	0,001	0,005	0,198	0,017	0,149	0,423	3,775	0,977	0,638
0,000	0,141	0,172	0,144	0,002	0,027	0,303	0,035	0,239	0,455	4,150	0,984	0,643
0,152	0,190	0,156	0,054	0,004	0,013	0,246	0,012	0,184	0,435	5,265	0,995	0,646
0,176	0,190	0,172	0,144	0,119	0,025	0,091	0,007	0,067	0,393	2,179	0,893	0,647
0,164	0,186	0,140	0,124	0,007	0,072	0,167	0,008	0,124	0,413	3,889	0,980	0,649
0,176	0,190	0,172	0,144	0,014	0,100	0,108	0,007	0,080	0,397	2,540	0,924	0,651
0,149	0,110	0,036	0,141	0,003	0,025	0,319	0,007	0,235	0,454	7,649	1,000	0,661
0,170	0,190	0,166	0,144	0,028	0,112	0,101	0,166	0,112	0,409	0,300	0,477	0,661
0,101	0,190	0,172	0,144	0,003	0,042	0,193	0,052	0,159	0,426	1,987	0,872	0,671
0,145	0,186	0,172	0,144	0,005	0,014	0,183	0,031	0,143	0,420	2,668	0,933	0,673
0,136	0,190	0,172	0,135	0,015	0,017	0,184	0,047	0,150	0,423	2,045	0,879	0,674
0,117	0,190	0,172	0,144	0,012	0,116	0,133	0,026	0,103	0,406	2,132	0,888	0,677
0,148	0,190	0,172	0,144	0,002	0,019	0,178	0,016	0,134	0,417	3,449	0,969	0,680
0,176	0,190	0,172	0,144	0,013	0,038	0,144	0,017	0,109	0,408	2,762	0,939	0,680
0,134	0,190	0,172	0,144	0,014	0,044	0,164	0,017	0,124	0,413	3,129	0,957	0,680
0,139	0,179	0,016	0,102	0,018	0,042	0,297	0,014	0,223	0,449	6,032	0,998	0,682
0,165	0,190	0,172	0,141	0,023	0,073	0,126	0,010	0,093	0,402	2,768	0,939	0,682
0,119	0,190	0,172	0,141	0,047	0,091	0,128	0,024	0,098	0,404	2,141	0,889	0,683
0,168	0,190	0,172	0,144	0,003	0,024	0,162	0,006	0,120	0,412	3,915	0,980	0,685
0,173	0,186	0,166	0,144	0,067	0,012	0,135	0,007	0,100	0,405	3,179	0,959	0,689
0,049	0,190	0,156	0,119	0,001	0,026	0,264	0,009	0,196	0,440	5,981	0,997	0,690
0,157	0,190	0,172	0,144	0,000	0,014	0,177	0,007	0,130	0,416	4,237	0,986	0,690
0,172	0,190	0,166	0,144	0,021	0,063	0,131	0,005	0,096	0,403	3,247	0,962	0,691
0,174	0,088	0,172	0,135	0,054	0,087	0,157	0,010	0,117	0,411	3,466	0,969	0,691
0,154	0,190	0,172	0,144	0,007	0,055	0,150	0,015	0,113	0,409	3,006	0,952	0,692
0,084	0,190	0,172	0,144	0,001	0,017	0,220	0,019	0,167	0,429	4,042	0,983	0,693

Продовження таб. 3.13

1	2	3	4	5	6	7	8	9	10	11	12	13
0,154	0,190	0,172	0,144	0,057	0,043	0,128	0,006	0,095	0,403	3,141	0,958	0,694
0,079	0,190	0,172	0,144	0,067	0,111	0,126	0,005	0,093	0,402	3,131	0,957	0,696
0,145	0,116	0,156	0,144	0,019	0,030	0,220	0,006	0,162	0,427	5,274	0,995	0,696
0,077	0,190	0,172	0,144	0,006	0,016	0,222	0,004	0,163	0,427	5,579	0,996	0,696
0,173	0,190	0,172	0,144	0,001	0,075	0,131	0,011	0,098	0,404	2,862	0,944	0,696
0,176	0,190	0,166	0,144	0,109	0,132	0,043	0,005	0,032	0,380	1,079	0,712	0,697
0,131	0,190	0,172	0,144	0,002	0,031	0,181	0,004	0,133	0,417	4,560	0,990	0,700
0,152	0,190	0,172	0,144	0,002	0,094	0,131	0,006	0,097	0,403	3,208	0,960	0,700
0,153	0,190	0,146	0,144	0,000	0,098	0,145	0,004	0,106	0,407	3,654	0,974	0,700
0,160	0,190	0,172	0,144	0,000	0,065	0,144	0,006	0,107	0,407	3,499	0,970	0,701
0,088	0,179	0,172	0,144	0,003	0,127	0,156	0,004	0,115	0,410	3,960	0,981	0,703
0,142	0,190	0,172	0,144	0,015	0,020	0,173	0,006	0,128	0,415	4,182	0,985	0,704
0,176	0,157	0,172	0,119	0,177	0,141	0,029	0,008	0,022	0,376	0,672	0,600	0,705
0,119	0,186	0,166	0,133	0,006	0,079	0,170	0,005	0,125	0,414	4,220	0,985	0,706
0,157	0,190	0,172	0,144	0,000	0,042	0,160	0,005	0,118	0,411	3,968	0,981	0,710
0,124	0,190	0,172	0,144	0,012	0,077	0,152	0,006	0,112	0,409	3,704	0,976	0,711
0,063	0,190	0,172	0,141	0,000	0,055	0,212	0,005	0,156	0,425	5,284	0,995	0,711
0,104	0,190	0,172	0,144	0,002	0,049	0,187	0,005	0,137	0,418	4,658	0,991	0,712
0,176	0,190	0,172	0,144	0,017	0,017	0,154	0,005	0,113	0,409	3,854	0,979	0,712
0,140	0,190	0,172	0,144	0,003	0,013	0,186	0,003	0,136	0,418	4,857	0,992	0,715
0,169	0,183	0,172	0,144	0,001	0,041	0,158	0,004	0,116	0,410	4,046	0,983	0,719
0,176	0,190	0,172	0,144	0,005	0,047	0,144	0,004	0,105	0,407	3,684	0,975	0,720
0,096	0,190	0,172	0,144	0,000	0,011	0,217	0,004	0,159	0,426	5,467	0,996	0,723
0,176	0,168	0,172	0,144	0,177	0,111	0,026	0,004	0,019	0,375	0,671	0,600	0,727

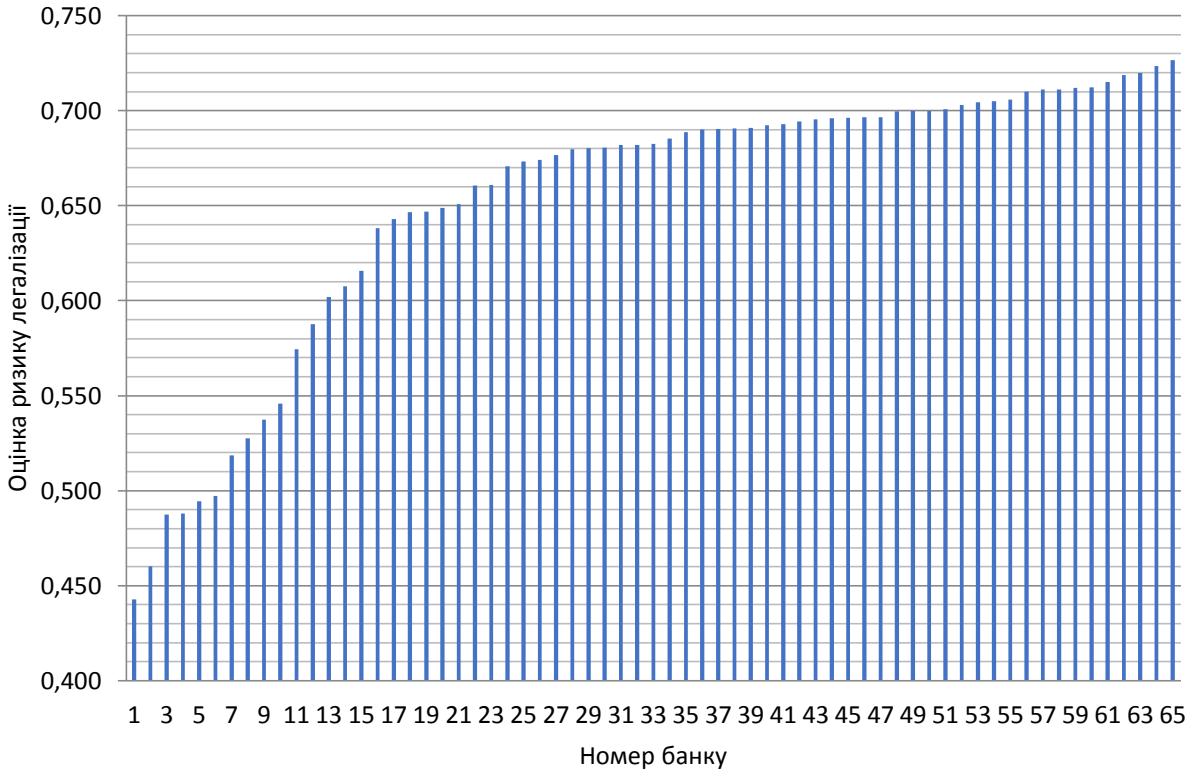


Рисунок 3.17 – Візуалізація спектрального представлення банків в розрізі оцінювання ризику легалізації кримінальних доходів

Таблиця 3.14

Візуалізація спектрального представлення банків в розрізі оцінювання ризику легалізації кримінальних доходів

Діапазон значень	<0,5	0,5-0,6	0,6-0,7	0,7-0,8
Кількість банків	6	6,000	38,000	15,000
Питома вага банків	0,0923	0,0923	0,5846	0,2308

Таким чином, найбільша питома вага банків України 58,46% мають кількісну оцінку ризику легалізації кримінальних доходів в межах від 0,6 до 0,7 частки одиниці, тобто мають високий рівень даного ризику. 23,08% банків мають критичний рівень ризику в межах від 0,7 до 0,8 частки одиниці. Незначна частки банків по 9,23% складають банки з рівнем ризику легалізації менше 0,5 та в проміжку від 0,5 до 0,6 частки одиниці.

В реаліях сьогодення для всіх країн світу, процес легалізації кримінальних доходів та фінансування тероризму, зазвичай, має небезпечний характер, і в першу чергу для національної економічної безпеки. По-перше, такий процес спричиняє посилення обігу коштів через тіньовий сектор економіки, бо значна частка доходів приховується. По-друге, національний бюджет кожної країни втрачає суттєві кошти, так як з отриманих кримінальних доходів податки не сплачуються. По-третє, процес легалізації незаконних доходів тягне за собою створення та розширення шахрайських схем обігу та функціонування фінансових потоків. По-четверте, скорочується притік інвестицій та зменшується привабливість бізнесу. По-п’яте, зростають державні витрати на здійснення боротьби з фінансово-економічною злочинністю.

Розроблена методика допомагає в процесі зменшення ризиків для країни зі сторони легалізації кримінальних доходів, отриманих незаконним шляхом, та фінансування тероризму. Її впровадження на державному рівні надасть можливість створити інформаційну базу даних щоб допомогти у прийнятті управлінських рішень стосовно покращення рівня національної економічної безпеки, так як це дає спроможність концентрувати увагу особливо на ті держави, що є доволі привабливими з боку легалізації кримінальних доходів, отриманих злочинним шляхом. Все це допоможе побудувати ефективний механізм співпраці з іншими державами в частині вибору цільових напрямів діяльності, витоків походження наявних ресурсів, тощо. Поряд з цим, такі процеси потребуватимуть перегляду, зміни та удосконалення законодавчої нормативно-правової бази для всіх фінансових і кредитних організацій, суб’єктів господарювання, осіб, що купують нерухоме майно, акції закордоном, чи пов’язані з будь-якими іншими посередниками.

Сформована база даних, що є результатом розробленої методики, виступає основою для проведення дій по удосконаленню стандартів економічної політики держави в частині посилення національної економічної безпеки, а також посилення партнерських взаємозв’язків із іншими державами світу. Все це можна

забезпечити завдяки розвитку новітніх інформаційних технологій та засобів по збиранню, обробці та обміну інформацією, причому не лише в межах однієї держави, відносно фінансових потоків, а й по всьому світу, шляхом підключення до процесу нових учасників. Таким чином, запровадження The Automatic Exchange ofInformation допомагає вирішувати окремі питання ухилення від сплати обов'язкових податків, але при обігу даних не розкривається відповідна інформація стосовно потоку коштів на рахунках з умовою дотримання нормативно закріпленої банківської таємниці. В плані такого обігу можна запровадити новітню електронну ідентифікацію певних джерел доходів і відповідного характеру операцій, що надасть можливість, дотримуючись банківської таємниці, вибрати операції, шо мають сумнівні джерела доходу, а також повідомляти правоохоронним органам про спробу їх проведення. Таку ідентифікацію слід застосовувати впроваджувати на банківському рівні, як нормативно затверджену обов'язкову частину звітності банків перед державою. Надалі заплановано запровадити розроблену методику в подальшу роботу Національної комісії, що виконує державне регулювання у діяльності ринків фінансово-економічних послуг, Національного банку України, Державної служби фінансового моніторингу.

РОЗДІЛ 4. МЕХАНІЗМ РЕГУЛЮВАННЯ БЕЗПЕКИ ДЕРЖАВИ ЯК ДЕТЕРМІНАНТА ЇЇ РОЗВИТКУ

4.1. Оцінка ризиків соціо-економіко-політичного розвитку України

Сучасні реалії соціальних, політичних та економічних змін, що спостерігаються у всіх сферах суспільного життя та діяльності країни, супроводжуються падінням добробуту громадян, соціальною диференціацією та розшаруванням суспільства, формуванням залежності країни від мінливості її репутації на міжнародній арені, монополізацією, корупцією, веденням бойових дій на сході України, тінізацією національної економіки, зростанням внутрішнього та зовнішнього боргу держави, тощо. Перелічені явища спричиняють гальмування розвитку економіки, погіршення соціального становища населення та недовіру до влади. Саме тому Україна в наші дні потребує системних драйверів, які б дозволили нівелювати вплив негативних ризиків та запустити докорінні зміни та потужний розвиток соціальної, економічної та політичної сфер країни.

Одним з драйверів, на нашу думку, є досконале вивчення та виявлення ризиків, які супроводжують соціо-політико-економічний розвиток країни та які можуть здійснювати як позитивний, так й негативний вплив. Тобто це можуть бути непередбачувані, негативні наслідки, події невизначеності, що спричиняють структурно-системні зміни щодо впровадження заходів реформування соціо-політико-економічого життя держави в умовах здійснення її інтеграційних процесів. Також важливим є визначення тих чинників, які впливають на ризик, тобто виявлення певних умов, за яких відбуватиметься зростання або зменшення ризиків. Як наслідок, оцінка ризиків дозволить визначити їх критичний рівень, який несе певну загрозу соціальній або економічній, або політичній сферам, що в подальшому сприятиме розробці превентивних заходів, спрямованих на

зменшення ризику для створення умов стабільного розвитку українського соціуму. Виходячи з вище сказаного, питання щодо обґрунтованої оцінки ризиків набуває актуальності та необхідності реалізації відповідно до сучасних напрямів реформування та розвитку соціо-політико-економічної системи України з метою майбутнього членства в ЄС.

Коло дослідження питань, пов'язаних із ризиками, є досить широким. Так, значна кількість наукових праць присвячується загальним поняттям ризику. Тут можна виділити таких науковців, як А. Бойко, Т. Васильєва, О. Кузьменко, С. Лєонов, О. Люта, І. Школьник та інші. Питання впливу системних ризиків на розвиток України розглядали в своїх роботах Ю. Кальниш, О. Кіндратець, М. Михальченко, І. Петренко та ін. Основні етапи управління ризиками на різних рівнях та у різних галузях досліджували: на державному рівні – Т. Васильєва, С. Лєонов, Г. Швіндіна; в банківській системі України – А. Бойко, В. В. Васюренко, В. Вітлінський, М. Клапків

Значний внесок у дослідження ризиків, їх впливу на соціальну, економічну та політичну сфери, підходів до їх оцінки зробили зарубіжні вчені, такі як Ф. Ахмедов, П. Бернстайн, С. Гібе, Дж. Дворський, Е. Дживок, Д. Зверенс, М. Зейтун, А. Котаскова, З. Петракова, Д. Террі, Л. Хаммерштрем, М. Хєлічек, Дж. Шонфелд, та інші. Для оцінки ризиків використовуються різні методики та математичні методи. Так, К. Бармута, О. Кузьменко, Ф. Ахмедов розглядали оптимізаційні методи для визначення ризиків. М. Худакова, Т. Васильєва застосовували статистичні методи, Х. Джин – системно-динамічне моделювання, Дж. Полак – ймовірнісні методи, М. Субех, Г. Яровенко – інтелектуальний аналіз, тощо. Незважаючи на актуальність теми ризиків та вагомість проведених досліджень, питання оцінки ризиків впливу на соціо-політико-економічний розвиток України потребує детального аналізу та розробки більш ефективних підходів.

Для визначення оцінки ризику потрібно виділити ті чинники, які здійснюють вагомий вплив на нього, в результаті чого спостерігається його

збільшення або зменшення [86, с. 14]. У даній роботі будемо розглядати саме ті фактори впливу, що провокують, створюють національні негаразди в сфері соціо-політичного стану та економічного зростання України, оскільки саме такі чинники сприяють гальмуванню розвитку та впливають на дестабілізацію держави.

Існує безліч методів для оцінки ризиків, кожен з яких має суттєві переваги та недоліки. Тому в процесі вибору метода автори керувалися такими критеріями, як простота інтерпретації результатів та швидкість оцінки. З цією метою було обрано метод аналізу ієрархій Томаса Сааті, який дозволяє визначити рівень ризику для кожної сфери з урахуванням вагомості кожного фактору впливу на загрози національного добробуту [87, 88]. При цьому результат оцінювання показує оцінку впливу кожного фактору в структурі ризику.

Для проведення оцінювання було створено два кластери ризиків, до яких схильні соціо-політична сфера та економічна складова держави. Соціальну сферу та політичну було об’єднано в один кластер, оскільки для України є характерним прямий тісний зв'язок між цими двома сферами. В якості альтернатив виступатимуть саме ризики, з якими пов’язані виділені сфери. Для знаходження розв’язку метод Т. Сааті потребує здійснення декомпозиції чинників за рівнем ієрархії.

Рівень 1. Оцінка рівня соціо-політичних ризиків, визначення найвагомішого ризику.

Рівень 2. Визначення факторів (критеріїв), які впливають на соціо-політичні ризики:

1) поглиблення соціальної диференціації суспільства (Φ_1);

2) занепад вітчизняної науки, ослаблення науково-освітнього потенціалу, перетікання мізків за кордон (Φ_2);

3) ведення військових дій на сході України (Φ_3);

4) дефіцит влади (репутаційні втрати органів влади, неефективність, децентралізація влади, зниження функціональності) ($Ф_4$);

5) втрата іміджу країни на світовій арені ($Ф_5$);

6) формування середнього прошарку, сприяння розвитку малого і середнього бізнесу, створення додаткових робочих місць ($Ф_6$).

Рівень 3. Формування соціо-політичних ризиків [89, с. 57-58]:

1) зростання соціальної нерівності (A_1);

2) зростання соціально-політичної нестабільності (A_2);

3) зростання міграції робочої сили (A_3);

4) ризики влади (A_4);

5) міжнародні ризики (A_5);

6) політичні ризики (політична нестабільність в умовах війни) (A_6).

Аналогічно побудуємо ієрархію для економічної сфери, для чого виконаємо ранжування чинників, які впливають на формування економічних загроз розвитку України, та сформуємо економічні ризики.

Рівень 1. Оцінка рівня економічних ризиків, визначення найвагомішого ризику.

Рівень 2. Визначення факторів (критеріїв), які впливають на економічні ризики:

1) суперечливість норм законодавства, факти здійснення нераціональних дій державних органів (F_1);

2) нестабільність фінансової та податкової системи (F_2);

3) корупція, «державний рекет», небезпечні дії конкурентів, легалізація кримінальних доходів (F_3);

4) стрімке зростання науково-технічного прогресу (F_4);

5) низький рівень заробітної плати та платоспроможності населення України, зниження користувацького попиту (F_5);

6) втрата виробничого потенціалу підприємств східних регіонів за рахунок ведення військових дій (F_6);

7) збільшення вичерпування природних ресурсів без можливостей їх подальшого відновлювання (F_7);

8) неконтрольована динаміка кон'юнктури зовнішнього та внутрішнього ринку (F_8);

9) негативні зміни обсягів основного фонду та капіталу (F_9).

Рівень 3. Формування економічних системних ризиків [90]:

1) скорочення ВВП, зниження рівня науково-технічного потенціалу, низький рівень інноваційної та інвестиційної активності, зниження техніко-технологічного потенціалу підприємств, відсутність дослідження інноваційного розвитку України (B_1);

2) нестабільність законодавства, яке регулює економічні відносини, нестале регулювання фіскальної політики України (B_2);

3) зростання значення кредитного ризику (B_3);

4) високий темп падіння обсягів основних виробничих фондів в структурі промисловості, агропромисловій виробничій системі, у всіх сферах життєзабезпечення (B_4);

5) залежність національної економіки від кон'юнктури коливань на світовому ринку, низький темп розвитку внутрішнього ринку (B_5);

6) сировинний характер національного експорту продукції з низькою питомою вагою та з високою часткою доданої вартості (B_6);

7) боргова залежність країни, великі обсяги внутрішнього та зовнішнього боргу національної економіки України (B_7);

8) залучення інвестицій в сферу економічної діяльності, зростання в країні частки іноземного капіталу у провідних галузях економіки (B_8) ;

9) відсутність спрямованої політики на енергозбереження, неефективне використання власного потенціалу паливно-енергетичних ресурсів, диверсифікація енергопостачання, загроза національної безпеки держави в енергетичній сфері України (B_9);

10) тінізація економічної сфери України (B_{10}).

Основна ідея методу аналізу ієрархій – це надання важливості кожному фактору (соціо-політичному або економічному) в порівнянні з іншими. Для цього використовується шкала відносної вагомості (табл. 4.1), яка формується незалежно від виду факторів.

Таблиця 4.1

Шкала відносної вагомості впливу факторів на ризики

Інтенсивність відносного впливу	Визначення
1	Рівнозначний вплив
2	Між рівнозначним впливом та помірною перевагою одного над іншим
3	Помірна перевага одного над іншим
4	Між помірною та середньою перевагою одного над іншим
5	Середня перевага одного над іншим
6	Між середньою та перевагою вище середньої одного над іншим
7	Вище середнього рівня перевага одного над іншим
8	Між вище середньою та значною перевагою одного над іншим
9	Значна перевага одного над іншим
Зворотні величини інтенсивності відносного впливу $1;\frac{1}{2};\frac{1}{3};\frac{1}{4};\frac{1}{5};\frac{1}{6};\frac{1}{7};\frac{1}{8};\frac{1}{9}$	При порівнянні відносної вагомості впливу одного фактора з іншим отримаємо оцінку від 1 до 9, то при порівнянні другого фактору з першим отримаємо зворотну величину

Джерело дослідження: побудовано авторами на основі [87,88,91,92]

На основі експертних оцінок, які було отримано від осіб – провідних економістів і фахівців з питань соціо-економіко-політичного розвитку держави, будуємо матрицю попарних порівнянь відносної вагомості впливу факторів з урахуванням інтенсивності відносного впливу. З цією метою використаємо обернено-симетричну матрицю, загальний вигляд якої представлений формулою 4.1 [87, с. 27]:

$$\Phi = \begin{bmatrix} 1 & \phi_{12} & \phi_{13} & \phi_{14} & \dots & \phi_{1m} \\ \frac{1}{\phi_{12}} & 1 & \phi_{23} & \phi_{24} & \dots & \phi_{2m} \\ \frac{1}{\phi_{13}} & \frac{1}{\phi_{23}} & 1 & \phi_{34} & \dots & \phi_{3m} \\ \frac{1}{\phi_{14}} & \frac{1}{\phi_{24}} & \frac{1}{\phi_{34}} & 1 & \dots & \phi_{4m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{\phi_{1m}} & \frac{1}{\phi_{2m}} & \frac{1}{\phi_{3m}} & \frac{1}{\phi_{4m}} & \dots & 1 \end{bmatrix}, \quad (4.1)$$

де Φ – матриця порівнянь відносної вагомості впливу факторів на соціально-політичні ризики України;

$\phi_{ij(i,j=1\div m)}$ – експертні оцінки вагомості впливу одного фактору у порівнянні з іншими з точки зору дії на соціально-політичні ризики України;

m – кількість факторів ($m=6$ для соціально-політичних ризиків).

Використовуючи формулу 4.1, для другого рівня ієрархії побудовано матрицю для соціо-політичної сфери (табл. 4.2).

Таблиця 4.2

Матриця попарних порівнянь відносної вагомості факторів впливу на соціо-політичні ризики України

Інтенсивність відносного впливу	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6
Φ_1	1	5	$\frac{1}{7}$	2	$\frac{1}{9}$	6
Φ_2	$\frac{1}{5}$	1	$\frac{1}{9}$	$\frac{1}{4}$	$\frac{1}{9}$	1
Φ_3	7	9	1	8	3	8
Φ_4	$\frac{1}{2}$	4	$\frac{1}{8}$	1	$\frac{1}{6}$	6
Φ_5	9	9	$\frac{1}{3}$	6	1	9
Φ_6	$\frac{1}{6}$	1	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{9}$	1

Аналогічно, побудовано матрицю попарних порівнянь відносної вагомості факторів впливу на економічні ризики України (табл. 4.3). Для цього використано формулу 1, в якій $\Phi = F$; $\phi_{ij(i,j=1\div m)} = f_{ij(i,j=1\div m)}$ – експертні оцінки вагомості впливу одного фактору у порівнянні з іншими факторами з точки зору дії на економічні ризики; m=9.

Таблиця 4.3

Матриця попарних порівнянь відносної вагомості факторів впливу на економічні ризики України

Інтенсивність відносного впливу	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
F_1	1	$\frac{1}{3}$	6	4	$\frac{1}{7}$	$\frac{1}{7}$	2	$\frac{1}{3}$	$\frac{1}{3}$
F_2	3	1	8	9	7	$\frac{1}{2}$	6	3	2
F_3	$\frac{1}{6}$	$\frac{1}{8}$	1	3	$\frac{1}{7}$	$\frac{1}{9}$	$\frac{1}{3}$	$\frac{1}{8}$	$\frac{1}{5}$
F_4	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{3}$	1	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{3}$	$\frac{1}{8}$	$\frac{1}{3}$
F_5	7	$\frac{1}{7}$	7	4	1	$\frac{1}{8}$	2	$\frac{1}{8}$	$\frac{1}{3}$
F_6	7	2	9	8	8	1	8	1	5
F_7	$\frac{1}{2}$	$\frac{1}{6}$	3	3	$\frac{1}{2}$	$\frac{1}{8}$	1	$\frac{1}{8}$	$\frac{1}{6}$
F_8	3	$\frac{1}{3}$	8	8	8	1	8	1	7
F_9	3	$\frac{1}{2}$	5	3	3	$\frac{1}{5}$	6	$\frac{1}{7}$	1

На наступному кроці необхідно визначити вектор пріоритетів, що являє собою відносну вагомість впливу кожного фактору на ризики та розраховується за формулою 4.2:

$$X_i = \sum_{j=1}^{m} \frac{\Phi_{ij}}{\sum_{i=1}^{n} \Phi_{ij}} \Big/ m, \qquad (4.2)$$

де $X_{i\,(i=1\div n)}$ – значення вектору пріоритетів, тобто безмірна величина, яка приймає значення від 0 до 1. Сума всіх пріоритетних елементів становить 1;

n – кількість рядків матриці пріоритетів, що відповідає кількості факторів (6 факторів для соціально-політичної сфери, 9 – для економічної);

m – кількість стовпчиків матриці пріоритетів, що відповідає кількості факторів (6 факторів для соціально-політичної сфери, 9 – для економічної).

В результаті проведених розрахунків отримано вектор пріоритетів для соціо-політичної сфери $(X_1, X_2, X_3, ...X_6)$, тобто $(X_1 \approx 0{,}106535;\ X_2 \approx 0{,}029576;\ X_3 \approx 0{,}438412;\ X_4 \approx 0{,}086992;\ X_5 \approx 0{,}308757;\ X_6 \approx 0{,}029728)$. Найбільший пріоритет серед інших факторів має фактор Φ_3 - ведення військових дій на сході України ($X_3 \approx 0{,}438412$), тобто здійснення військових дій на сході України матиме найбільший вплив на розвиток соціально-політичної сфери. Наступним релевантним чинником є втрата іміджу (авторитету) країни на світовій арені (Φ_5), що зумовлено входженням держави в різні союзи та коаліції з іншими країнами ($X_5 \approx 0{,}308757$); третім пріоритетним фактором є поглиблення соціальної диференціації суспільства (Φ_1) ($X_1 \approx 0{,}106535$) і т.д.

Вектор пріоритетів відносної вагомості впливу факторів на національні економічні ризики розраховується аналогічно за формулою 4.2, в якій $X_{i\,(i=1\div n)} = Y_{i\,(i=1\div n)};\ \phi_{ij} = f_{ij}$. В результаті отримано його наступні значення – ($Y_1 \approx 0{,}056601$; $Y_2 \approx 0{,}211259$; $Y_3 \approx 0{,}022763$; $Y_4 \approx 0{,}017872$; $Y_5 \approx 0{,}089268$; $Y_6 \approx 0{,}262376$; $Y_7 \approx 0{,}032413$; $Y_8 \approx 0{,}216471$; $Y_9 \approx 0{,}090977$). Найбільш впливовим чинником на досліджувану сферу є втрата виробничого потенціалу підприємств східних регіонів за рахунок ведення військових дій (F_6) ($Y_6 \approx 0{,}262376$); наступний релевантний чинник є неконтрольована динаміка кон'юнктури зовнішнього та внутрішнього ринку (F_8) ($Y_8 \approx 0{,}216471$); нестабільність фінансової та податкової системи (F_2) ($Y_2 \approx 0{,}211259$) і т.д.

На наступному кроці будуємо матриці парних зіставлень соціально-політичних ризиків по кожному фактору впливу, тобто кожна матриця буде відображати оцінку одного виду ризику у порівнянні з іншим видом відносно впливу одного з факторів [92, с. 112]. Оцінку було визначено на основі експертного судження професіоналів з питань соціо-економіко-політичного розвитку країни. Для побудови використаємо формулу 4.1. У таблиці 4.4 наведемо приклад побудови такої матриці попарних порівнянь соціально-політичних ризиків відносно фактору ($Ф_3$) – ведення військових дій на сході України, оскільки було визначено, що він має найбільший вплив на групу соціо-політичних ризиків.

Таблиця 4.4

Матриця парних зіставлень соціально-політичних ризиків відносно фактору ведення військових дій на сході України

Інтенсивність відносного впливу	A_1	A_2	A_3	A_4	A_5	A_6
A_1	1	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{9}$
A_2	8	1	$\frac{1}{5}$	$\frac{1}{8}$	1	$\frac{1}{9}$
A_3	8	5	1	1	$\frac{1}{7}$	1
A_4	8	8	1	1	$\frac{1}{7}$	$\frac{1}{9}$
A_5	4	1	7	7	1	$\frac{1}{6}$
A_6	9	9	1	9	6	1

Подібним чином будуємо матриці попарних порівнянь економічних ризиків по кожному з раніше розглянутих факторів, використовуючи формулу 4.1, в якій ($B_1, B_2, \dots, B_{10}$) – економічні ризики України, *m, n = 10*.

Далі необхідно визначити вектори пріоритетів впливу факторів на кожний з ризиків ($U_{11}, U_{21}, \dots, U_{61}; U_{12}, U_{22}, \dots, U_{62}; \dots; U_{16}, U_{26}, \dots, U_{66}$), для чого

скористаємося формулою 4.2, в якій $X_{i\ (i=1\div n)} = U_{ij\ (i=1\div n;j=1\div m;m,n=6)}$; $\phi_{ij} = u_{ij}$, де u_{ij} – це оцінки з матриці парних зіставлень соціально-політичних ризиків по кожному фактору впливу. Отримані значення скомпонуємо таким чином, щоб отримати дані впливу усіх факторів на окремий вид ризику. Відобразимо результати оцінки соціо-політичних ризиків на рисунку 4.1 у вигляді нормованої гістограми з накопиченням.

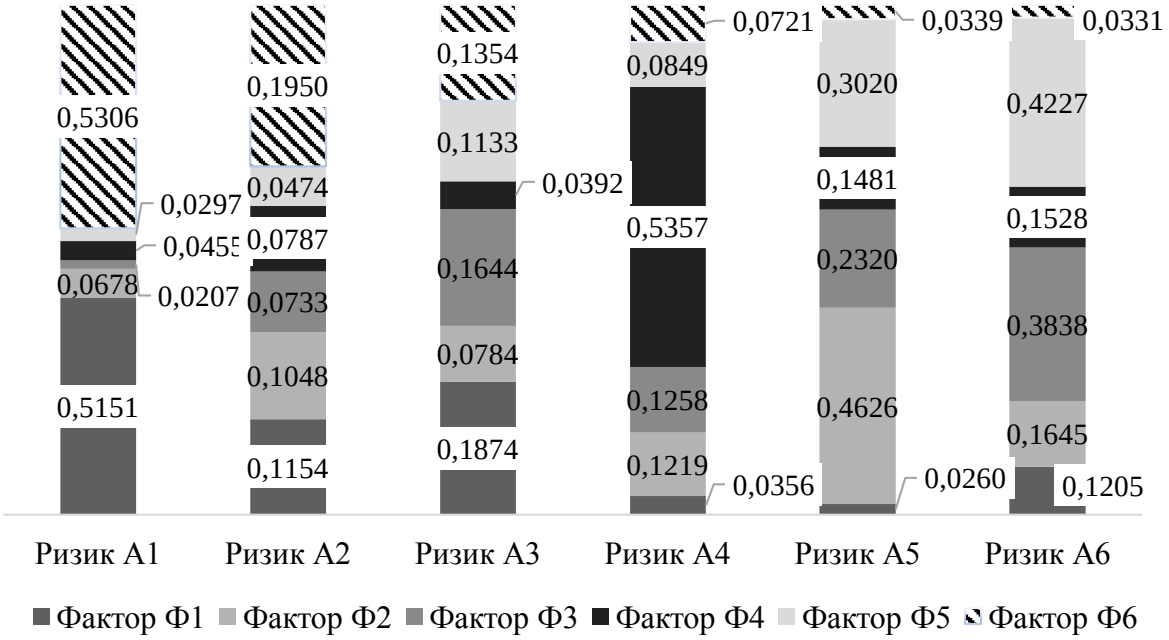


Рисунок 4.1 – Оцінки соціо-політичних ризиків з урахуванням впливу факторів

Таким чином, найбільший вплив на ризик зростання соціальної нерівності (A_1) здійснюють фактори - поглиблення соціальної диференціації суспільства (Φ_1) та формування середнього прошарку (Φ_6). На ризик зростання соціально-політичної нестабільності (A_2) впливає формування середнього прошарку, сприяння розвитку малого і середнього бізнесу, створення додаткових робочих місць (Φ_6). Ризик зростання міграції робочої сили (A_3) залежить від практично однакового впливу факторів Φ_1, Φ_3, Φ_5 та Φ_6, що говорить про комплексність його формування. Репутаційні втрати органів влади, її неефективність та децентралізація, зниження функціональності (Φ_4) здійснює найбільший вплив на

ризик влади (A_4). Міжнародний ризик (A_5) залежить від Φ_2 та Φ_5, а політичний ризик (A_6) – Φ_3 та Φ_5.

Аналогічним чином визначимо вектори пріоритетів впливу факторів на кожний з економічних ризиків. Відобразимо результати на рисунку 4.2 у вигляді нормованої гістограми з накопиченням. Така структура ризику дозволить виділити найбільш впливові фактори, що сприятиме виробленню рекомендацій з боку держави щодо усунення негативного впливу цих факторів. Наприклад, на ризик B_1 найбільший вплив здійснює фактор стрімкого зростання науково-технічного прогресу (F_4), тобто державі слід підтримувати ІТ-галузь, що стимулюватиме здійснення позитивного впливу на досліджуваний ризик.

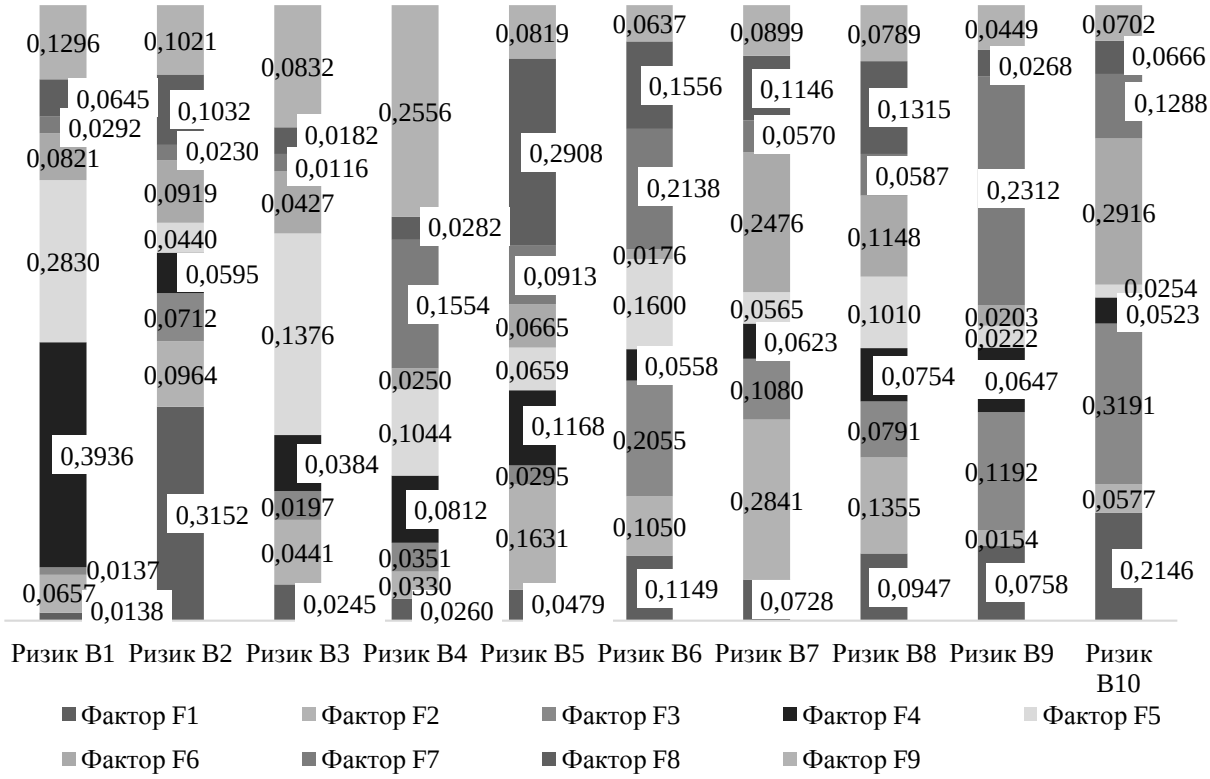


Рисунок 4.2 – Оцінки економічних ризиків з урахуванням впливу факторів

На останньому кроці обчислимо загальне значення вектору пріоритетів соціально-політичних та економічних ризиків з використанням формули 4.3:

$$Z_i = \sum_{i=1}^{n} X_i \cdot U_{ij}, \qquad (4.3)$$

де $Z_{i\ (i=1\div n;n=6)}$ – значення вектору пріоритетів соціально-політичних ризиків, сума значень якого становить 1;

$X_{i\ (i=1\div n;n=6)}$ – значення вектору пріоритетів відносної вагомості впливу факторів на соціо-політичні ризики;

$U_{ij\ (i=1\div n;j=1\div m;n,m=6)}$ – значення векторів пріоритетів впливу факторів на кожний з соціо-політичних ризиків.

Результати розрахунку вектору пріоритетів соціально-політичних ризиків представлено на рисунку 4.3.

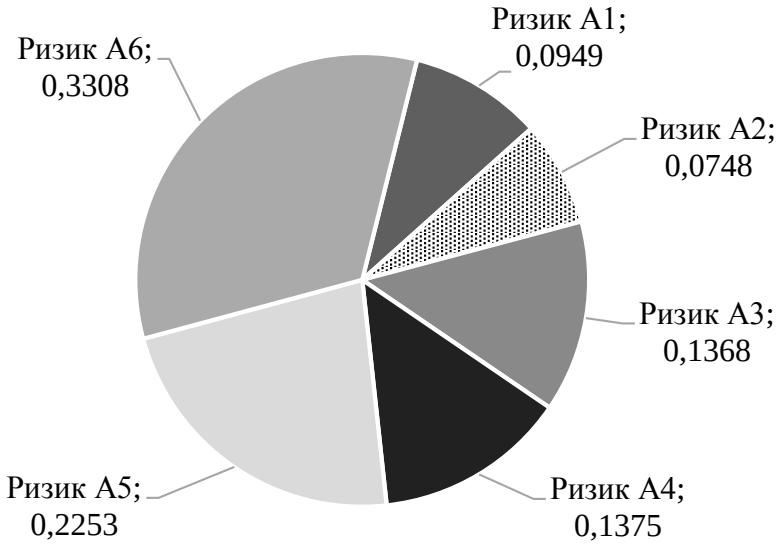


Рисунок 4.3 – Пріоритет соціо-політичних ризиків

На підставі отриманих пріоритетних значень (рис. 4.3), виявлено, що найвагоміший вплив на розвиток соціальної та політичної системи країни здійснює політичний ризик, який пов'язаний із політичною нестабільністю в країні та веденням бойових дій на сході України (*0,3308*). Іншим за пріоритетом є міжнародні ризики (*0,2253*), зниження якого відбуватиметься за рахунок підвищення довіри до України з боку міжнародних партнерів та за рахунок її становлення як повноцінного гравця на міжнародній арені, а також створення

умов праці для науково-освітніх працівників, що сприятиме зниженню еміграції фахівців з країни.

Аналогічний підхід використовуємо для знаходження пріоритетів економічних ризиків, результати яких представимо на рисунку 4.4.

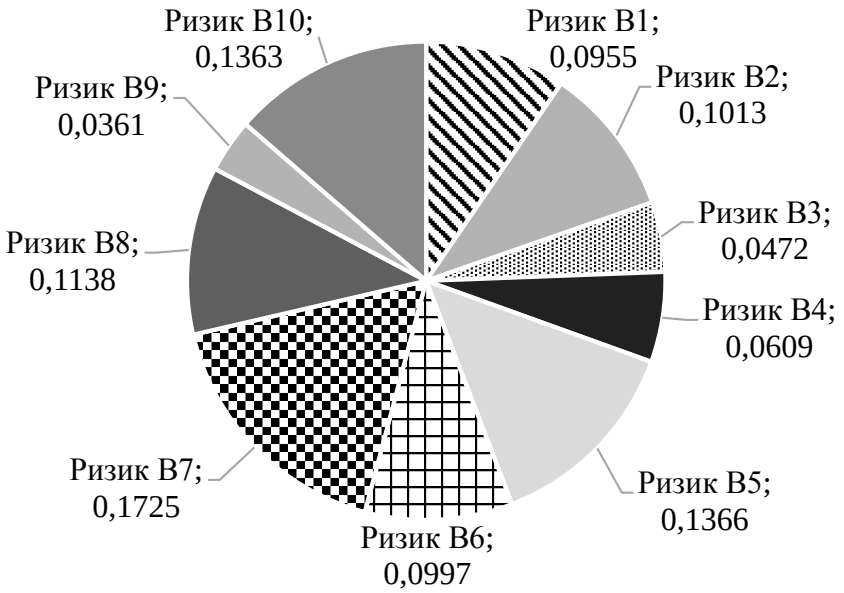


Рисунок 4.4 – Пріоритет економічних ризиків

Отримані значення стверджують, що найвищий пріоритет має ризик збільшення внутрішньої та зовнішньої боргової залежності країни (*0,1725*), що формуватиме залежність країни від зовнішніх міжнародних кредитів. Також можна виділити ризик залежності національної економіки від кон'юнктури коливань на світовому ринку (*0,1366*), на зниження рівня якого впливатиме ступінь збалансованості попиту та пропозиції на ринку, тенденції розвитку, ступінь ділової активності, масштаби ринкових операцій, тощо. Ризик підвищення рівня тінізації економіки є також пріоритетним (*0,1363*), збільшення рівня якого свідчитиме про те, що більшість фінансових операцій здійснюється у тіні, що гальмує економічний розвиток.

Для забезпечення стійкого розвитку країни існує потреба ідентифікації та оцінки тих ризиків, які негативно впливають на соціальну, економічну та політичну сфери держави, стримують їх розвиток та сповільнюють процеси інтеграції в новітній соціо-економіко-політичний простір розвинутих країн. Саме

тому використання таких методів, як аналіз ієрархій, дозволить проводити оцінку ризиків з урахуванням тих факторів, що здійснюють негативний чи позитивний вплив на них. Застосування на практиці запропонованого у статті підходу забезпечує визначення пріоритетності факторів впливу на ризик. Як результат, їх аналіз сприятиме визначенню саме тих чинників, які найбільше впливають. Це допоможе уряду виробити ряд якісних та ефективних дій щодо усунення їх впливу на збільшення рівня ризику соціо-політичної або економічної сфер.

Також запропонований підхід дозволяє визначити структуру ризику з урахуванням впливу факторів, що може стати підґрунтям для виділення саме тих критичних чинників, які є характерними для цього типу ризику. На основі цих оцінок можна проводити диференціацію факторів впливу та акцентувати увагу на тих, які є критичними. На останньому кроці підхід надає можливість визначити також й пріоритет соціо-політичних та економічних ризиків по відношенню один до одного, що дозволяє виділити саме ті ризики, які сьогодні здійснюють найбільший вплив. Тобто, використовуючи таку оцінку ризиків, отримуємо також й їх пріоритетність та пріоритетність факторів впливу, що сприятиме розробці комплексних та системних заходів для нівелювання негативного впливу ризиків на розвиток соціо-економіко-політичної сфер країни.

4.2. Ігромоделювання процесів оптимізації державного регулювання економічної безпеки національної економіки

В сучасних умовах організації світових макроекономічних процесів, з урахуванням виникаючих фінансових криз, під час розроблення та впровадження середньо та довгострокової стратегії економічного, фінансового, соціального розвитку країн, важливе місце посідає їх економічна безпека [93, 94, 95]. Так, саме економічна безпека виступає однією з найважливіших ознак якісного функціонування фінансово-економічних систем у кожній країні по всьому світу. Також рівень економічної безпеки характеризує здатність держави забезпечувати

необхідні, достойні умови життєдіяльності суспільства; сталу достатність потрібних для розвитку національного господарства ресурсів; врегульоване, послідовне виконання національних державних інтересів. Однією з основних проблем економічної безпеки при цьому виділяють удосконалення існуючих не достатньо ефективних та результативних механізмів функціонування, регулювання фінансово-економічної діяльності на державному рівні [96, 97, 98, 99, 100, 101].

Тому, на сьогоднішній день, в умовах зростаючої глобалізації світового господарства, формування ефективної, дієвої системи державного регулювання економічної безпеки національної економіки, як складової частини державної національної безпеки, є особливо актуальним напрямом, що потребує пріоритетної уваги. Отже, питання та проблемні аспекти, що виникають при державному регулюванні економічної безпеки національної економіки, ще не достатньо вивчені та розроблені, і тому потребують пошуку нових підходів та методик до забезпечення належного рівня економічної безпеки держави.

Так постає потреба у здійсненні формалізації системи заходів Державного регулювання економічної безпеки національної економіки, щодо знаходження компромісної точки у тріаді таких напрямів: зведення до мінімуму величини інтегрального індексу загрози національної економіки, мінімізації рівня використання банків з метою легалізації кримінальних доходів за рахунок максимізації рівня ефективності внутрішньобанківської системи фінансового моніторингу в розрізі певного банку та одночасної мінімізації узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів. Здійснювати таку формалізацію запропоновано шляхом такого інструментарію, як «теорія ігор». Тому, сформульовано постановку задачі для апарату «теорія ігор» для проведення Державного регулювання економічної безпеки національної економіки. На цьому етапі методики першим кроком постає ідентифікація існуючої конфліктної ситуації. Перший гравець (держава) переслідує мету мінімізації інтегрального індексу загрози національної економіки шляхом

державного регулювання, що в свою чергу суперечить існуючій стратегії функціонування другої групи учасників (економічних агентів, які намагаються легалізувати кримінальні доходи), які відповідно свідомо чи не свідомо призводять до фактів порушень, і в кінцевому підсумку спричиняють збільшення рівня використання банків з метою легалізації кримінальних доходів. Також, потрібно відмітити, що відповідний взаємозв'язок інтегрального індексу загрози національної економіки та рівня використання банків з метою легалізації кримінальних доходів пропонується формалізувати за рахунок узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів, що у дослідження представлений у якості результативного показника та яку держава намагається мінімізувати.

Далі другим кроком постановки задачі дослідження виступає створення платіжної матриці, що показує результати функціонування учасників у кількісному вираженні. Показниками такої матриці (SVA_{ji}^{*}) є певні математичні сподівання узагальнюючої оцінки ризику використанням банків для легалізації кримінальних доходів, що в свою чергу подібна до стратегії країни, та описується досягнутим розміром інтегрального індексу загрози національної економіки, як регресант впровадження стратегії економічних агентів, які намагаються легалізувати кримінальні доходи, формалізованої у вигляді рівня використання банків з метою легалізації кримінальних доходів (таблиця 4.5).

Таблиця 4.5

Платіжна матриця гри «державного регулювання економічної безпеки національної економіки»

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		Рік 1	…	Рік i	…	Рік n
		D_1	…	D_i	…	D_n
Банк 1	θ_1	SVA_{11}^{*}	…	SVA_{1i}^{*}	…	SVA_{1n}^{*}
…	…	…	…	…	…	…
Банк j	θ_j	SVA_{j1}^{*}	…	SVA_{ji}^{*}	…	SVA_{jn}^{*}
…	…	…	…	…	…	…
Банк m	θ_m	SVA_{m1}^{*}	…	SVA_{mi}^{*}	…	SVA_{mn}^{*}

Примітка: D_i – інтегральний індекс загрози національної економіки за і-тий рік; θ_j – рівень використання банківської системи для легалізації злочинних доходів; SVA^*_{ji} - узагальнююча оцінка ризику використанням j-го банку для легалізації кримінальних доходів за і-тий рік.

В якості фактичних даних практичної побудови платіжної матриці гри «державного регулювання економічної безпеки національної економіки» пропонується обрати вибірку банків України, кожен з яких характеризується показником рівня використання з метою легалізації кримінальних доходів. Вони дозволять сформувати рядки платіжної матриці. В межах стовбців платіжної матриці обрано динаміку показника інтегральний індекс загрози національної економіки з 2008 по 2019 рр. Сформувати внутрішній діапазон платіжної матриці зазначеної конфліктної ситуації між державою та економічними агентами, які намагаються легалізувати кримінальні доходи, пропонується шляхом використання узагальнюючої оцінки ризику використання в розрізі обраного переліку банків для легалізації кримінальних доходів станом на 2019 рік. Для обчислення даного ризику за 2008 – 2018 роки пропонується використати дані 2019 року, скориговані на співвідношення інтегрального індексу загрози поточного та 2019 року в розрізі кожного із вибраних для аналізу банків. Фрагмент результатів проведених розрахунків приведемо у вигляді таблиці 4.6.

Останнім кроком постановки задачі у «теорії ігор» під час проведення державного регулювання економічної безпеки національної економіки є існування визначених правил у грі, що спричиняють наслідки використання кожного серед учасників своїх власних «чистих стратегій». Так, залежність узагальнюючої оцінки ризику використання банків для легалізації злочинних доходів від рівня загрози національної економіки та рівня використання банків для легалізації доходів, отриманих злочинним шляхом, формалізуємо за допомогою інструментарію регресійного аналізу пакету MS Excel у вигляді побудови лінійного багатофакторного регресійного рівняння.

Таблиця 4.6

Фрагмент фактичних даних платіжної матриці гри «державного регулювання економічної безпеки національної економіки»

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		2008	2009	2010	…	2017	2018	2019
		0,8148	0,2566	0,5144	…	0,5538	0,4557	0,6195
Bank 8	68,75	0,6939	0,2185	0,4381	⋯	0,4717	0,3881	0,5276
Bank 13	100,00	0,8148	0,2566	0,5144	⋯	0,5538	0,4557	0,6019
Bank 16	4,37	0,7142	0,2249	0,4509	⋯	0,4855	0,3995	0,6382
Bank 20	88,69	0,6736	0,2122	0,4253	⋯	0,4579	0,3768	0,6489
…	…	…	…	…	…	…	…	…
Bank 39	100,00	0,8822	0,2778	0,5570	⋯	0,5997	0,4934	0,6909
Bank 41	100,00	0,6222	0,1960	0,3929	⋯	0,4230	0,3480	0,6929
Bank 36	100,00	0,6204	0,1954	0,3917	⋯	0,4217	0,3470	0,6900
Bank 54	100,00	0,6230	0,1962	0,3933	⋯	0,4235	0,3484	0,7051

Залежність узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів від рівня загрози національної економіки та рівня використання банків для легалізації доходів, отриманих злочинним шляхом, формалізуємо з використанням приведеного нижче рівняння множинної регресії (формула 4.4):

$$\mathrm{SVA}^{*}_{j\mathrm{i}} = -0{,}0150 + 0{,}0001 \cdot \theta_j + 0.9089 \cdot D_i, \qquad (4.4)$$

де $\mathrm{D_i}$ – інтегральний індекс загрози національної економіки за і-тий рік;

θ_j – рівень використання j-го банку з метою легалізації кримінальних доходів;

SVA^{*}_{ji} - узагальнююча оцінка ризику використанням j-го банку для легалізації кримінальних доходів за і-тий рік.

Подальше вирішення задачі удосконалення системи державного регулювання економічної безпеки національної економіки вимагає проведення формалізації стратегій поведінки як з бору держави щодо заходів державного регулювання, так і з боку економічних агентів щодо використання банків з метою легалізації кримінальних доходів. Так, в таблиці 4.7 наведемо перелік відповідних стратегій для обох гравців розглянутої конфліктної ситуації.

Таблиця 4.7

Стратегії держави та економічних агентів щодо запобігання використання банків з метою легалізації кримінальних доходів

Стратегія	Рівень використання банківз метою легалізації кримінальних доходів	Держава
Стратегія А	Активного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія активної протидії легалізації кримінальних доходів
Стратегія В	Помірного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія помірної протидії легалізації кримінальних доходів
Стратегія С	Мінімального використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія мінімальної протидії легалізації кримінальних доходів

Переходячи до визначення кількісної відповідності значень рівня використання банків для легалізації кримінальних доходів якісній характеристиці, представленій в таблиці 4.7 за відповідною шкалою інтервалів, виникає необхідність перевірки вхідних даних нормальному закону розподілу в розрізі як рівня використання банків для легалізації кримінальних доходів, так і інтегрального індексу загрози національної економіки. Для реалізації даного кроку використаємо інструментарій програмного пакету Statistica: Statistics, Distribution Fitting, що дозволяє побудувати гістограму розподілу значень досліджуваного показника та за допомогою критерію Chi-Square перевірити

відповідність нормальному закону розподілу з подальшою формалізацією шкали інтервалів значень.

Так в розрізі рівня використання банків для легалізації кримінальних доходів гістограма розподілу значень набуває вигляду рисунку 4.5 і дозволяє стверджувати про підтвердження гіпотези щодо відповідності нормальному закону розподілу рівнів даного ряду.

Рисунок 4.5 – Гістограма розподілу значень рівня використання банків для легалізації кримінальних доходів

Виходячи з доцільності виділення саме трьох стратегій поведінки економічних агентів в межах рівня використання банківз метою легалізації кримінальних доходів, відповідну шкалу інтервалів представимо у вигляді таблиці 4.8.

Таблиця 4.8

Шкала інтервалів значень рівня використання банків для легалізації кримінальних доходів

Показник	$(\bar{\theta} - 2\sigma k;\ \bar{\theta} + 2\sigma(k+1))$		
Якісна інтерпретація	Стратегія активного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія помірного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія мінімального використання фінансових посередників з метою легалізації кримінальних доходів
Шкала значень	[0; 30)	[30; 70)	[70; 100]

Аналогічно описаному вище підходу проведено шкалювання інтервалів значень інтегрального індексу загрози національної економіки в розрізі стратегій поведінки держави (таблиця 4.9).

Таблиця 4.9

Шкала інтервалів значень інтегрального індексу загрози національної економіки

Показник	$(\bar{\theta} - 2\sigma k;\ \bar{\theta} + 2\sigma(k+1))$		
Якісна інтерпретація	Стратегія активної протидії легалізації кримінальних доходів	Стратегія помірної протидії легалізації кримінальних доходів	Стратегія мінімальної протидії легалізації кримінальних доходів
Шкала значень	[0; 0,43)	[0,43; 0,67)	[0,67; 100]

Виконавши процедуру формалізації процесу державного регулювання економічної безпеки національної економіки, розглянемо методику вирішення поставленої задачі. У межах методики «теорії ігор» для обрання раціональної ефективної стратегії поведінки держави, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та економічними агентами,

які намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів вирішено застосувати критерій: мінімаксу та максиміну відповідно. Цей критерій надає можливість встановити мінімально, а також максимально можливий певний середнійрівень ризику використання банків для легалізації кримінальних доходів. Такі умови з математичної сторони можна відобразити у подібним способом (формула 4.5):

$$\alpha = \max_i \left(\min_j a_{ij} \right), \qquad \beta = \min_j \left(\max_i a_{ij} \right), \tag{4.5}$$

де α (β) – мінімально (максимально) можливий рівень ризику використання банків для легалізації кримінальних доходів, досягнутий за результатами регулюючих дій держави, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та відповідних дій економічних агентів, які намагаються збільшити рівень використання банків з метою легалізації кримінальних доходів.

У ситуації, за якої $\alpha = \beta$ є змога встановити розмір максимального допустимого узагальнюючого рівня ризику використання банків для легалізації кримінальних доходів, а саме встановити її точкову величину. В цій ситуації набуття визначеного рівня ризику можливе за рахунок застосування кожним із учасників їх власних чистих стратегій. У протилежному випадку можна встановити розмір інтервальної оцінки максимального ризику використання банків для легалізації кримінальних доходів, і як результат використання економічними агентами, які намагаються збільшити рівень використання банків з метою легалізації кримінальних доходів (формула 4.6) та державою, яка намагається мінімізувати інтегральний індекс загрози національної економіки (формула 4.7) власних змішаних типів стратегій, що прогнозують їх відповідну комбінацію.

$$S_A^* = (p_1^*, p_2^*, ..., p_m^*), \quad (4.6)$$

де S_A^* – оптимальний змішаний тип стратегії «учасника А»;

p_i^* –певна імовірність використання *i-ї* чистої стратегії учасника А.

$$S_B^* = (q_1^*, q_2^*, ..., q_n^*), \quad (4.7)$$

де S_B^* – оптимальний змішаний тип стратегія «учасника Б»;

q_i^* – імовірність використання *i-ї* чистої стратегії учасника Б.

І як результат того, що держава застосовує мінімаксний тип стратегії, а економічні агенти використовують протилежний максимінний тип стратегії, розрахунок ціни гри (максимальний середнійрівеньризику використання банків для легалізації кримінальних доходів)здійснюється з використанням теореми Неймана у вигляді формули 4.8:

$$v = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} p_i^* q_j^*, \quad (4.8)$$

де v – мінімальна величина максимально можливого рівня ризику використання банків для легалізації кримінальних доходів.

Переходячи до практичного впровадження максимінної та мінімаксної стратегій гри «державного регулювання економічної безпеки національної економіки» як конфліктної ситуації між державою, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та економічними агентами, які намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів, побудуємо таблицю 4.10, де візуально зобразимо описаний вище механізм пошуку оптимальних стратегій дій гравців.

Таблиця 4.10

Візуалізація механізму впровадження максимінної та мінімаксної стратегій гри

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		Рік 1	…	Рік і	…	Рік n	Нижня межа ризику використання банку для ЛКД	
		D_1	…	D_i	…	D_n	min	maxmin
Банк 1	θ_1	SVA^*_{11}	…	SVA^*_{1i}	…	SVA^*_{1n}	$\min_i \mathrm{SVA}^*_1$	$\max_j \min_i \mathrm{SVA}^*_{ji}$
…	…	…	…	…	…	…	…	
Банк j	θ_j	SVA^*_{j1}	…	SVA^*_{ji}	…	SVA^*_{jn}	$\min_i \mathrm{SVA}^*_{ji}$	
…	…	…	…	…	…	…	…	
Банк m	θ_m	SVA^*_{m1}	…	SVA^*_{mi}	…	SVA^*_{mn}	$\min_i \mathrm{SVA}^*_m$	
Верхня межа ризику використання банку для ЛКД	Max	$\max_j \mathrm{SVA}^*_{j1}$	…	$\max_j \mathrm{SVA}^*_j$	…	$\max_j \mathrm{SVA}^*_{jn}$		
	Min max	$\min_i \max_j \mathrm{SVA}^*_{ji}$						

Переходячи до практичного впровадження максимінної та мінімаксної стратегій гри «державного регулювання економічної безпеки національної економіки», побудуємо, фрагмент якої представимо у вигляді таблиці 4.11.

Таким чином, економічні агенти намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів. Тому в розрізі рядків таблиці 4.11 ми спочатку визначаємо мінімально можливий рівень ризику використання банків для легалізації кримінальних доходів, який держава в свою чергу намагається знизити за рахунок регулюючих заходів, що передбачає необхідність пошуку максимального з мінімально можливих рівнів ризику. Це передбачає необхідність для економічних агентів застосування чистої стратегії, кількісною мірою якої виступає рівень використання банків з метою легалізації кримінальних доходів на рівні 69,09%, що відповідає стратегії

помірного використання фінансових посередників з метою легалізації кримінальних доходів.

Таблиця 4.11

Фрагмент практичного впровадження максимінної та мінімаксної стратегій гри

Рівень використання Банківської системи з метою легалізації кримінальних доходів/ Інтегральний Індек сзагрози		2008	2009	2010	…	2018	2019	min	max min
		0,8148	0,2566	0,5144	…	0,4557	0,6195		
Bank 8	68,75	0,6939	0,2185	0,4381	…	0,3881	0,5276	0,2185	0,3058
Bank 13	100,00	0,8148	0,2566	0,5144	…	0,4557	0,6019	0,2566	
Bank 16	4,37	0,7142	0,2249	0,4509	…	0,3995	0,6382	0,2249	
Bank 20	88,69	0,6736	0,2122	0,4253	…	0,3768	0,6489	0,2122	
Bank 50	100,00	0,6624	0,2086	0,4182	…	0,3705	0,7000	0,2086	
Bank 1	100,00	0,6141	0,1934	0,3878	…	0,3435	0,4428	0,1934	
Bank 4	69,09	0,9708	0,3058	0,6130	…	0,5430	0,4880	0,3058	
…	…	…	…	…	…	…	…	…	
	Max	0,9708	0,3058	0,6130	…	0,5430	0,7266		
	Minmax	0,3058			.				

Держава намагається мінімізувати інтегральний індекс загрози національної економіки, застосовуючи мінімаксну стратегію. Спочатку обчислюється максимально можливий рівень ризику використання банків для легалізації коштів, отриманих злочинним шляхом, як результат дій економічних агентів, які цьому сприяють. Далі визначаємо мінімально можливе значення, що відповідає намірам держави за рахунок регулювання зменшити узагальнюючу оцінку даного ризику, обираючи таку стратегію поведінки, яка дозволяє мінімізувати інтегральний індекс загрози національної економіки. Пропонується використовувати оптимальну чисту стратегію для держави, яка відповідає інтегральному індексу загрози національної економіки на рівні 0,2566, тобто стратегії активної протидії легалізації кримінальних доходів. При цьому загальна оцінка ризику використання банків для легалізації кримінальних доходів становитиме 0,3058.

Враховуючи вищевикладене, сформовано висновок, що для удосконалення Державного регулювання економічної безпеки національної економіки, запропоновано застосовувати інструментарій «теорія ігор». Практичне застосування такої методики дозволить вирішити ряд існуючих проблемних питань у напрямі сучасного, новітнього розвитку країни. Це допоможе створити дієві інструменти для стабільного розвитку національної економіки,забезпечить стійку макроекономічну позицію, дозволить зменшити економічну, технологічну та виробничу залежність держави, знизити рівень інфляції, скоротити ресурсну заборгованість країни, збільшити імпорт, зменшити експорт,сприятиме розвитку міжнародних ділових відносин, залучення іноземних інвестицій, допоможе знизити рівень корупції та впливу її негативних наслідків на економіку, зменшити розрив у фінансовому рівні забезпечення серед населення країни, забезпечить збалансованість бюджету, скорочення дефіцит бюджету, сприятиме збільшенню податкових надходженьдо бюджету, дозволить забезпечити конкурентоспроможність країни, допоможе забезпечити стійкість до дестабілізуючих факторів.

4.3. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела

В останні 35-40 років на макроекономічному рівні спостерігається активне вивчення та розвиток питань економічної небезпеки, що супроводжується безперервними змінами сутності, понять та методик забезпечення відповідних показників безпеки економіки. Основні матеріали цих досліджень в більшій частині ґрунтуються на розрахунку загального рівня економічної безпеки країн та відповідного ранжування держав згідно визначеного рівня. Паралельно з цим формуються основні відмінності таких досліджень, що полягають у різних наборах факторів та чинників, що впливають на рівень безпеки кожної країни,

визначення сили впливу та розміру вагомості таких факторів загрози національним економікам держав.

Відомі сучасні методики визначення рівня загрози економіки країн світу, наразі враховують основні тенденції функціонування та розвитку світової економічної системи, сучасних інформаційних технологій, останні досягнення в напряму економічної теорії. У сучасних умовах розвитку кожна окремо взята держава піддається впливу всіх цих процесів, що визначають тенденції сьогодення, визначаючи, диверсифікуючи та ускладнюючи проблеми економічної небезпеки. Так, аналіз існуючих методик оцінки загрози національної економіки вказує на відсутність в економічній літературі досконалого дієвого та якісного підходу до методик визначення загроз економіці країни, що викликає гостру необхідність розробки ефективної методології забезпечення національної економічної безпеки країни.

Для вивчення категорії індексу загрози національної економіки проведено аналіз наявної літератури шляхом побудови карти наукової бібліографії терміну «threatindex» (індекс загрози) [102, 103, 104, 105,106] за період останніх п’яти років, тобто 2016 - 2020 рр. у частині таких галузей як економіка, економетрика, фінанси та бізнес, управління та бухгалтерський облік за допомогою програми VOSViewerv.1.6.10. Відповідні результати аналізу зображено у вигляді графіку (рис. 4.6). Формування карти наукової бібліографії зазначеного поняття базується на даних трактатів [107, 108,109], знайдених, відібраних та побудованих у архіві зібрань Scopus.

Аналіз рисунку 4.6 надає можливість здійснити висновки про те, що дослідження теми визначення індексу загрози національної економіки є актуальним, а доказом цього є велика чисельність праць вчених за напрямком цієї сфери [110, 111, 112, 113]. На карті зображено кластери видань, сформованих по ключовими словам. Таким чином було виділено 14 кластерів, включаючи ключові слова, що різняться між собою кольорами. Особливо великими є кластери, що мають зв’язок з такими поняттями, як оцінювання ризику, стабільний розвиток,

економічна безпека, прийняття рішень, системи безпеки, банкрутство, інфляція, безробіття тощо [114, 115, 116, 117,118].

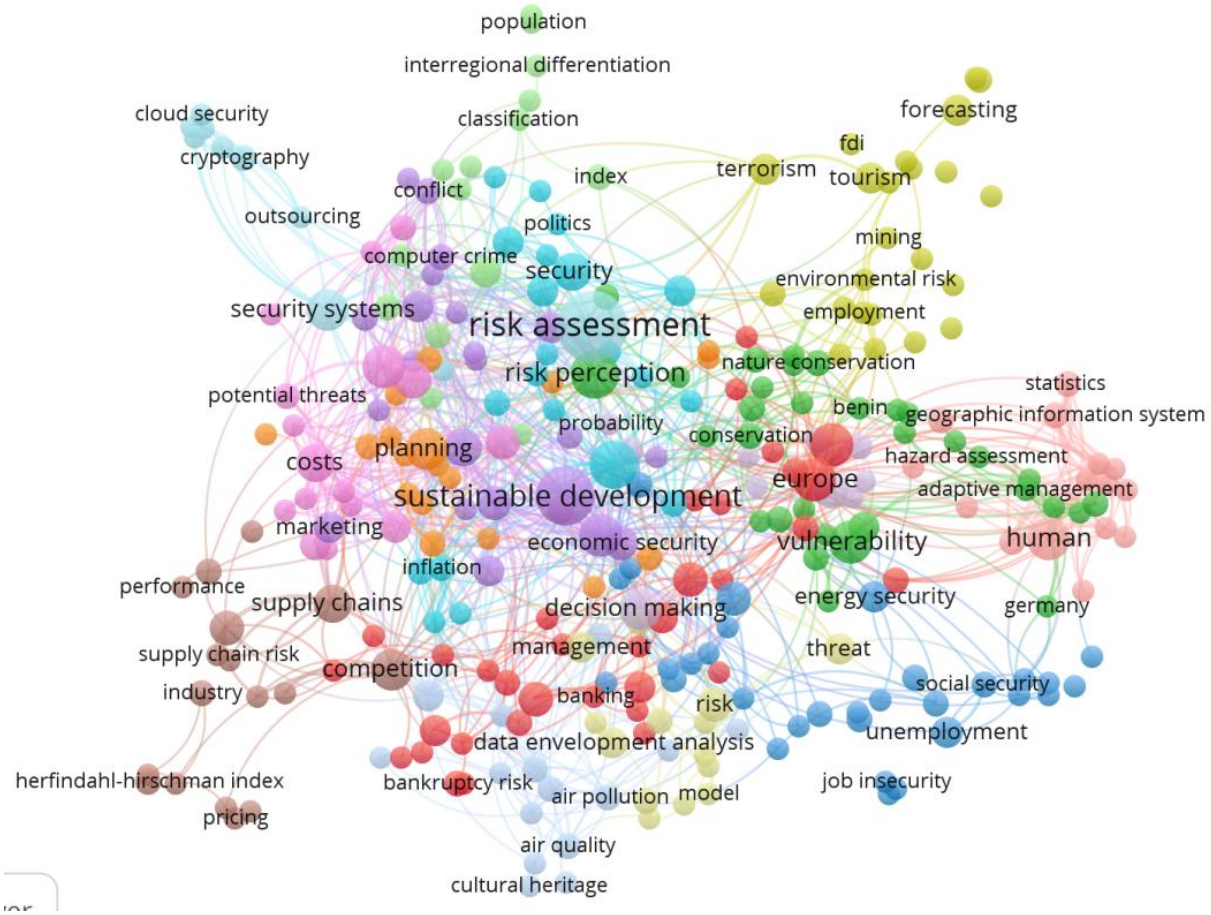


Рисунок 4.6 – Карта наукового бібліографічного поняття «threatindex» (індекс загрози) за період останніх п’яти, тобто 2016 - 2020 рр. за використанням програмного забезпечення VOSViewerv.1.6.10

З метою здійснення оцінки індексу загрози національної економіки пропонується побудувати структурно-логічну математичну модель, що включає відповідну послідовність певних етапів дослідження.

Етап 1. Створення інформаційної бази вхідних предикторів за період з 2008 по 2019 рр. у динаміці, а саме: Дефіцит державного бюджету, % до ВВП; Обсяг загального боргу, % до ВВП; Частки іноземного капіталу у статутному капіталі банків; Міжнародні резерви країни в місяцях імпорту; Рівень доларизації, частка іноземної валюти у грошовій масі, %; Контроль корупції; Політична стабільність

та відсутність насильства / тероризму; Верховенство права; Рівень інфляції, %; Рівень безробіття,%; Індекс GINI; Рівень тіньової економіки, % ВВП (таблиця 4.12).

Таблиця 4.12

Динаміка показників

Індикатор	Рік					
	2008	2009	2010	2011	2012	2013
Дефіцит державного бюджету, % до ВВП	1,43	3,93	5,99	1,77	3,62	4,34
Обсяг загального боргу, % до ВВП	19,12	33,57	40,05	36,40	36,70	39,91
Частки іноземного капіталу у статутному капіталі банків	36,70	35,80	40,60	41,90	39,50	34,00
Міжнародні резерви країни в місяцях імпорту	6,70	4,40	5,00	3,60	2,90	2,40
Рівень доларизації, частка іноземної валюти у грошовій масі, %	30,73	31,70	29,19	30,30	32,10	27,10
Контроль корупції	-0,84	-1,04	-1,03	-1,05	-1,08	-1,13
Політична стабільність та відсутність насильства / тероризму	0,04	-0,30	0,01	-0,07	-0,09	-0,78
Верховенство права	-0,68	-0,76	-0,81	-0,82	-0,78	-0,80
Рівень інфляції, %	25,23	15,88	9,37	7,96	0,57	-0,24
Рівень безробіття,%	6,36	8,84	8,10	7,85	7,53	7,17
Індекс GINI	26,60	25,30	24,80	24,60	24,70	24,60
Рівень тіньової економіки, % ВВП	34,00	39,00	38,00	34,00	34,00	36,00
Дефіцит державного бюджету, % до ВВП	4,54	1,55	2,30	1,41	1,91	1,96
Обсяг загального боргу, % до ВВП	69,37	79,06	80,90	71,78	60,93	67,71
Частки іноземного капіталу у статутному капіталі банків	32,50	43,30	51,20	35,80	28,18	27,51
Міжнародні резерви країни в місяцях імпорту	1,30	3,20	3,70	3,60	3,40	3,20
Рівень доларизації, частка іноземної валюти у грошовій масі, %	32,20	32,20	32,90	31,90	29,20	29,07
Контроль корупції	-0,99	-0,98	-0,81	-0,78	-0,87	-0,88
Політична стабільність та відсутність насильства / тероризму	-2,02	-1,96	-1,86	-1,87	-1,83	2,57
Верховенство права	-0,79	-0,81	-0,77	-0,71	-0,72	-0,72
Рівень інфляції, %	12,07	48,70	13,91	14,44	10,95	7,89
Рівень безробіття,%	9,27	9,14	9,35	9,51	8,78	9,06
Індекс GINI	24,00	25,50	25,00	26,00	26,10	26,06
Рівень тіньової економіки, % ВВП	43,00	40,00	35,00	32,00	30,00	29,66

2 етап. Приведення показників вхідної інформаційної бази дослідження до співставного вигляду шляхом проведення нелінійної нормалізації 4.9:

$$I_{ij} = \left(1 + e^{\frac{\overline{x_j} - x_{ij}}{\sigma(x_j)}}\right)^{-1}, \quad (4.9)$$

де I_{ij}– нормалізоване значення j-го показника характеристики загрози національної економіки за і-ий рік;

$\overline{x_j}$– середнє значення j-го показника характеристики загрози національної економіки за досліджуваний часовий діапазон;

x_{ij} – фактичне значення j-го показника характеристики загрози національної економіки за і-ий рік;

$\sigma(x_j)$ – середнє квадратичне відхилення j-го показника характеристики загрози національної економіки за досліджуваний часовий діапазон.

Розрахунки нормалізованих значень представимо в таблиці 4.13.

Таблиця 4.13

Нормалізовані значення показників характеристики індексу загрози

Показник	Рік					
	2008	2009	2010	2011	2012	2013
Дефіцит державного бюджету, % до ВВП	0,28	0,66	0,88	0,32	0,62	0,72
Обсяг загального боргу, % до ВВП	0,16	0,28	0,35	0,31	0,31	0,35
Частки іноземного капіталу у статутному капіталі банків	0,48	0,45	0,62	0,67	0,58	0,38
Міжнародні резерви країни в місяцях імпорту	0,91	0,64	0,74	0,50	0,37	0,29
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0,50	0,64	0,30	0,44	0,69	0,11
Контроль корупції	0,74	0,33	0,35	0,31	0,26	0,18
Політична стабільність та відсутність насильства / тероризму	0,63	0,57	0,63	0,61	0,61	0,48
Верховенство права	0,86	0,53	0,28	0,24	0,40	0,30
Рівень інфляції, %	0,71	0,54	0,41	0,39	0,26	0,25
Рівень безробіття,%	0,11	0,60	0,42	0,36	0,29	0,22
Індекс GINI	0,84	0,51	0,35	0,30	0,33	0,30
Рівень тіньової економіки, % ВВП	0,41	0,71	0,66	0,41	0,41	0,54

Продовження таблиці 4.13

Показник	Рік					
	2014	2015	2016	2017	2018	2019
Дефіцит державного бюджету, % до ВВП	0,75	0,29	0,40	0,27	0,34	0,35
Обсяг загального боргу, % до ВВП	0,69	0,78	0,79	0,71	0,59	0,67
Частки іноземного капіталу у статутному капіталі банків	0,33	0,71	0,89	0,45	0,20	0,19
Міжнародні резерви країни в місяцях імпорту	0,15	0,42	0,52	0,50	0,46	0,42
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0,70	0,70	0,78	0,66	0,30	0,28
Контроль корупції	0,42	0,45	0,78	0,82	0,67	0,67
Політична стабільність та відсутність насильства / тероризму	0,27	0,28	0,29	0,29	0,30	0,92
Верховенство права	0,36	0,26	0,49	0,76	0,73	0,72
Рівень інфляції, %	0,46	0,94	0,50	0,51	0,44	0,39
Рівень безробіття,%	0,70	0,67	0,72	0,75	0,59	0,66
Індекс GINI	0,17	0,57	0,41	0,72	0,74	0,73
Рівень тіньової економіки, % ВВП	0,87	0,76	0,48	0,30	0,21	0,19

3 етап. Відбір релевантних показників оцінювання індексу загрози національної економіки на базі комбінації методів Парето та діаграми розсіювання. Переходячи до реалізації даного етапу побудови структурно-логічної математичної моделі оцінювання індексу загрози національної економіки, розглянемо теоретичні аспекти застосування зазначених методів до фільтрації релевантних предикторів вхідної інформаційної бази дослідження. Так, діаграма Парето використовується для відображення відносної важливості всіх можливих проблемних аспектів з метою знаходження початкової точки для подальшого спостереження за результатами, пошуку головної причини проблеми, результативного розв’язання питання.

Досить цікавими є історичне становлення та застосування діаграми Парето. Так, італійським вченим Парето В. у 1897 р. сформульовано закон розподілення доходів, що передбачає нерівномірний розподіл усіх наявних благ. Американським науковцем Лоренцом М. зображено таку теорію у вигляді

діаграми. Економіст Джуран Д. вивчав особливості якості, та використав діаграму з метою класифікації певних проблем якості, а саме: небагаточисленні, але є суттєво важливими, та багаточисленні, але не суттєво важливі. Він назвав свій метод аналіз Паретто.

Отже, передбачається, що зосередження уваги на найбільш важливих проблемах сильніше впливає на отримання бажаних результатів. Відомим є правило з назвою 20/80, що означає: зосередження 20% зусиль на найважливіших питаннях призводить до можливості отримати 80% результатів. А решта 80% зусиль дозволяють отримати тільки решту 20% від усіх результатів.

Слід зазначити, що діаграма Парето виступає особливим типом вертикального стовпчикового графіка, що дозволяє знайти порядок вирішення виникаючих проблем. В цьому випадку є можливість досягти значно більших результатів, опрацьовуючи найвищий стовпчик, а не розподіляючи увагу ще й на менші стовпчики .

Побудова діаграми Парето передбачає використання наступної методики: спочатку здійснити відбір проблемних питань, що необхідно між собою порівняти та розмістити за ступенями важливості; визначити певний єдиний стандартний масштаб для можливості здійснити порівняння одиниць виміру; визначити період часу для дослідження; зібрати всі необхідні дані; визначити та порівняти частоти появи відповідних категорій; перерахувати категорії проблем на горизонтальній осі графіка зліва направо в порядку спадання ознаки критерію; відмітити на вертикальній осі графіку зазначеного масштабу від 0% до 100%, за якого 100% включає загальна сумарна частота виникнення всіх можливих категорій проблем.

Таким чином, переходячи до побудови діаграми Парето з метою вибору релевантних предикторів оцінювання індексу загрози національної економіки проведемо ряд проміжних кроків, а саме:

1) діапазон можливих нормалізованих значень вхідних предикторів розіб’ємо на 10 рівномірних інтервалів (від 0 до 0,1; від 0,1 до 0,2; від 0,2 до 0,3;

від 0,3 до 0,4; від 0,4 до 0,5; від 0,5 до 0,6; від 0,6 до 0,7; від 0,7 до 0,8; від 0,8 до 0,9; від 0,9 до 1,0);

2) обчислимо кількість випадків протягом досліджуваного часового діапазону попадання нормалізованих значень предикторів характеристики рівня загрози національної економіки визначеним інтервальним межам (таблиця 4.12);

3) обчислимо частоти використання предикторів (графа «Сума всього» таблиці 4.14);

4) визначимо частоти попадання нормалізованих значень предикторів у кожен з визначених на першому кроці інтервалів, результати представимо у рядку «Сума» таблиці 4.14. На основі аналізу розрахованих частот визначимо 20% інтервалів, якими можна знехтувати при визначенні пріоритетності вхідних предикторів – тобто інтервали від 0 до 0,1 та від 0,1 до 0,2, оскільки саме не них припадає найменша кількість частот;

5) обчислимо 80% значущих частот використання предикторів (графа «Сума 80%» таблиці 4.14).

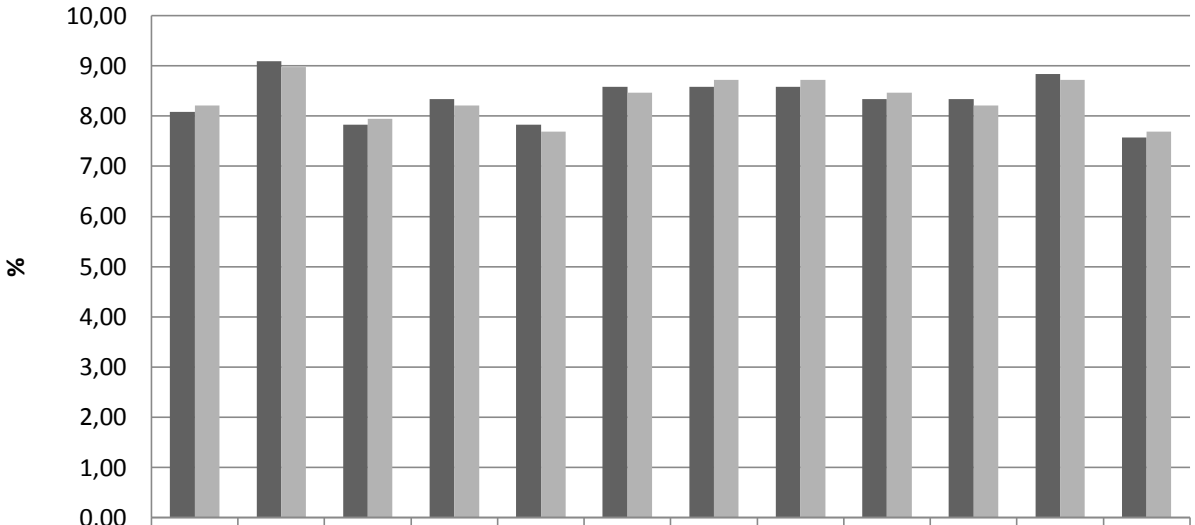
Так, на основі результатів проведення даного кроку визначимо, що найменші значення частот за сумою 80%, тобто значення в розмірі 30 одиниць, мають 2 предиктори: Рівень доларизації, частка іноземної валюти у грошовій масі, % та Рівень тіньової економіки, % ВВП. Саме ці два предиктори пропонується вилучити з подальших розрахунків індексу загрози національної економіки.

На основі даних таблиці 4.14 (графи «Сума всього» та «Сума 80%») побудуємо діаграму Парето (рис. 4.7), яка візуально дозволяє визначити 80% релевантних і 20% нерелевантних предикторів вхідної бази дослідження. Для побудови даної діаграми обчислимо відносний показник структури в розрізі зазначених граф таблиці 4.14. Діаграма Парето виступає підтвердженням доцільності вилучення таких пре дикторів, як Рівень доларизації, частка іноземної валюти у грошовій масі, % та Рівень тіньової економіки, % ВВП.

Таблиця 4.14

Частота попадання нормалізованих значень показників предикторів характеристики рівня загрози національної економіки

Показник \ Інтервал можливих значень	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Сума всього	Сума 80%
Дефіцит державного бюджету, % до ВВП	0	0	3	2	4	2	6	4	7	4	32	32
Обсяг загального боргу, % до ВВП	0	1	1	5	1	6	2	9	2	9	36	35
Частки іноземного капіталу у статутному капіталі банків	0	0	1	2	4	3	6	4	7	4	31	31
Міжнародні резерви країни в місяцях імпорту	0	1	1	2	5	3	6	4	6	5	33	32
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0	1	2	1	3	2	8	3	8	3	31	30
Контроль корупції	0	1	1	4	3	4	4	6	5	6	34	33
Політична стабільність та відсутність насильства / тероризму	0	0	5	0	6	1	10	1	10	1	34	34
Верховенство права	0	0	4	1	6	2	6	4	7	4	34	34
Рівень інфляції, %	0	0	2	1	5	4	5	5	5	6	33	33
Рівень безробіття,%	0	1	2	2	3	3	5	6	5	6	33	32
Індекс GINI	0	1	2	3	3	5	3	7	4	7	35	34
Рівень тіньової економіки, % ВВП	0	0	1	1	5	2	6	4	7	4	30	30
Сума	0	6	25	24	48	37	67	57	73	59		



	Дефіцит державного бюджету, % до ВВП	Обсяг загального боргу, % до ВВП	Частки іноземного капіталу у статутному капіталі банків	Міжнародні резерви країни в місяцях імпорту	Рівень доларизації, частка іноземної валюти у грошовій масі, %	Контроль корупції	Політична стабільність та відсутність насильства / тероризму	Верховенство права	Рівень інфляції, %	Рівень безробіття,%	Індекс GINI	Рівень тіньової економіки, % ВВП
Сума всього	8,08	9,09	7,83	8,33	7,83	8,59	8,59	8,59	8,33	8,33	8,84	7,58
Сума 80%	8,21	8,97	7,95	8,21	7,69	8,46	8,72	8,72	8,46	8,21	8,72	7,69

Рисунок 4.7 – Діаграма Парето вибору релевантних предикторів оцінювання індексу загрози національної економіки

В розрізі дослідження окресленої проблематики визначення релевантності предикторів окрема увага віддається діаграмі розсіювання (розкиду). Ця діаграма використовується для зображення тих процесів, що відбуваються з однією з аналізованих змінних категорій, у випадку за якого інша змінна категорія також змінюється; проведення перевірки припущення щодо взаємозв’язку двох аналізованих змінних категорій, оцінювання величини сили такого взаємозв’язку. При цьому діаграма розкиду не дозволяє встановити причинно-наслідковий взаємозв’язок.

Так побудуємо діаграму розсіювання (рис. 4.8), аналіз якої дозволяє підтвердити висновок про доцільність акцентування уваги при виборі релевантних предикторів саме інтервалів нормалізованих значень від 0,2 до 1.

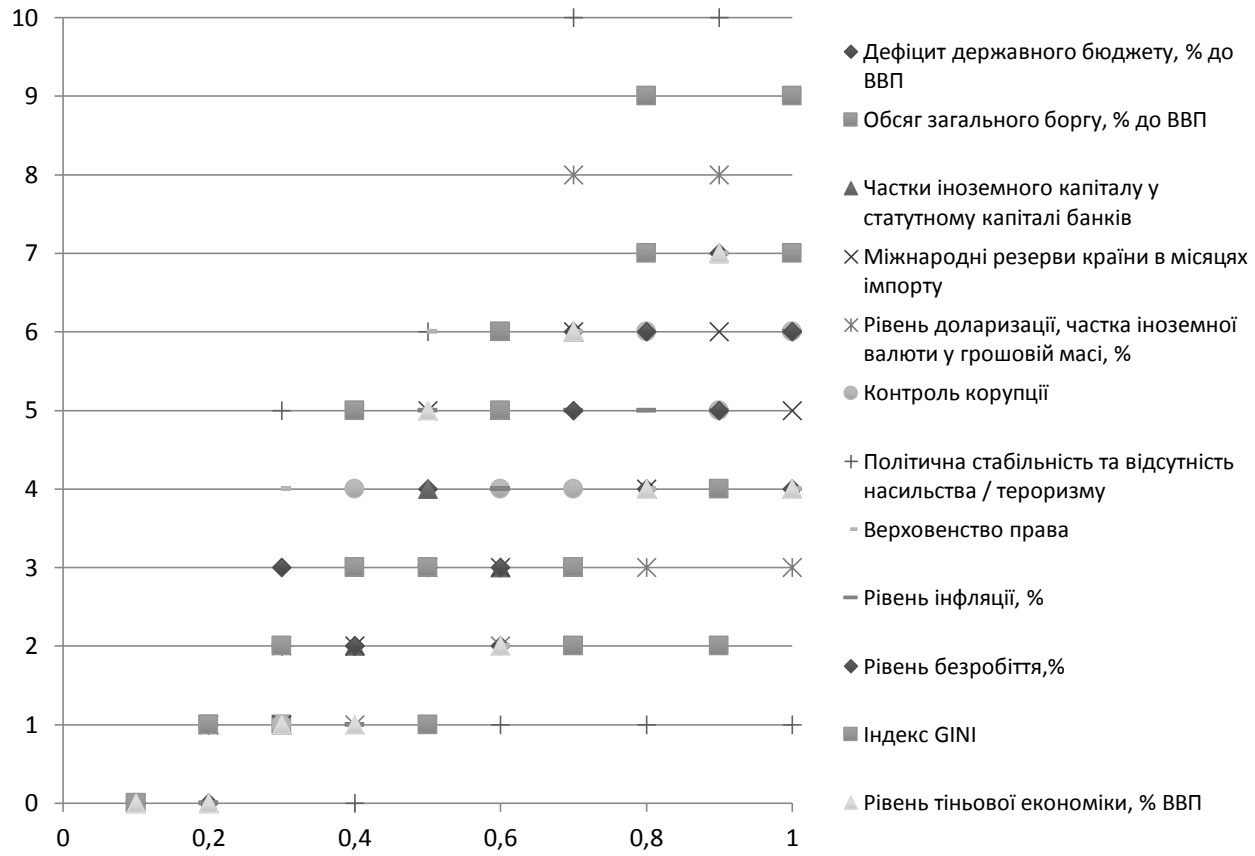


Рисунок 4.8 – Діаграма розсіювання вибору релевантних предикторів оцінювання індексу загрози національної економіки

4 етап. Оцінювання інтегрального індексу загрози національної економіки за допомогою функції Кернела та мультиплікативної форми згортки. Так, функція Кернела являє собою новий метод, що в своїй основі використовує концепцію регресії Кернела [119,120]. Така концепція дозволяє ефективно моделювати періодичні явища та процеси, враховуючи та долаючи при цьому обмеження певних методів.

Функція Кернела застосовується при вимірюванні подібності між парами певних показників. При цьому метою такого дослідження є моделювання періодичних процесів та явищ у визначених часових рядах, тому функцію Кернела [119,120] можна представити у вигляді формули 4.10:

$$k(t_i, t_j) = exp\left[-\frac{2}{l^2} sin\left(\pi \frac{t_i - t_j}{\rho}\right)^2\right], \quad (4.10)$$

де t – показник часу;

$k(t_i, t_j) \in (0, 1)$ – вихідний результат функції Кернела. Він вимірює відповідну схожість двох часових показників t_i і t_j, у вигляді функції відстані, що є між ними, а також функції двох певних параметрів;

$\theta = \{p, \ell\}$ - період і довжина функції Кернела.

Переходячи до застосування функції Кернела в розрізі оцінювання складових індексу загрози національної економіки за предикторами, представимо пару показників - з одного боку, нормалізованого значення j-го показника характеристики загрози національної економіки за і-ий рік та, з іншого боку, середнього нормалізованого значення $\overline{I_J}$ даного показника (формула 4.11):

$$k(I_{ij}, \overline{I_J}) = exp\left[-\frac{2}{l^2} sin\left(\pi \frac{I_{ij} - \overline{I_J}}{\rho}\right)^2\right], \quad (4.11)$$

$$\overline{I_J} = \frac{\sum_{i=1}^{m} I_{ij}}{m},$$

де $k(I_{ij}, \overline{I_J})$ – функція Кернела залежності від нормалізованого значення j-го показника характеристики загрози національної економіки за і-ий рік та середнього нормалізованого значення $\overline{I_J}$;

$\overline{I_J}$ – середнє арифметичне значення j-го нормалізованого показника характеристики загрози національної економіки за досліджуваний проміжок часу;

m – кількість показників характеристики загрози національної економіки;

l, ρ – параметри функції Кернела.

Обчисливши значення функції Кернела в розрізі кожного відібраного предиктора індексу загрози національної економіки за кожен рік досліджуваного часового діапазону, виникає необхідність їх згортки до єдиного узагальнюючого

індикатора за допомогою мультиплікативної форми згортки на основі методики середнього геометричного. В той же час, індекс загрози інтерпретується як індекс-дестимулятор національної економіки, саме тому для відображення даного негативного аспекту розрахункового індексу, необхідно розглянути її величину як одиниця мінус середнє геометричне функцій Кендела кожного релевантного предиктора (формула 4.12):

$$D_i = 1 - \sqrt[n-1]{\prod_{j=1}^{n} k\left(I_{ij}, \overline{I_{\iota J}}\right)}, \tag{4.12}$$

де D_i – інтегральний індекс загрози національної економіки за і-тий рік;

n – кількість років досліджуваного часового діапазону;

m – кількість показників характеристики загрози національної економіки;

Формула 4.12 з урахуванням умовних позначень набуває вигляду 4.13:

$$\begin{aligned} D_i &= 1 - \sqrt[n-1]{\prod_{j=1}^{n} k\left(I_{ij}, \overline{I_{\iota J}}\right)} \\ &= 1 - \sqrt[n-1]{\prod_{j=1}^{n} exp\left[-\frac{2}{l^2} sin\left(\pi \frac{I_{ij} - \overline{I_J}}{\rho}\right)^2\right]} \end{aligned} \tag{4.13}$$

Обираючи в якості параметрів функції Кернела $l = 0{,}2, \rho = 5$, результати розрахунків за формулою (5) та усі проведені проміжні обчислення систематизуємо в таблиці 4.15.

Таблиця 4.15

Динаміка проміжних розрахунків та інтегрального індексу загрози національної економіки з 2008 по 2019 рр.

Показник	порогове значення	Рік					
		2008	2009	2010	2011	2012	2013
Дефіцит державного бюджету, % до ВВП	не більше 3-4	0,40	0,56	0,05	0,58	0,74	0,36
Обсяг загального боргу, % до ВВП	не більше 60	0,11	0,39	0,64	0,49	0,51	0,63
Частки іноземного капіталу у статутному капіталі банків	не більше 30	0,99	0,95	0,72	0,56	0,86	0,77
Міжнародні резерви країни в місяцях імпорту	не меньше 3	0,04	0,64	0,31	1,00	0,74	0,44
Контроль корупції		0,32	0,57	0,66	0,49	0,33	0,14
Політична стабільність та відсутність насильства / тероризму		0,68	0,88	0,70	0,75	0,76	1,00
Верховенство права		0,08	0,97	0,42	0,27	0,85	0,47
Рівень інфляції, %	не більше 7	0,38	0,94	0,91	0,83	0,38	0,35
Рівень безробіття,%	не більше 7,6	0,05	0,84	0,86	0,66	0,40	0,20
Індекс GINI		0,10	1,00	0,67	0,46	0,56	0,46
Integralindex		0,81	0,26	0,51	0,42	0,42	0,58
Дефіцит державного бюджету, % до ВВП	не більше 3-4	0,28	0,46	0,86	0,40	0,65	0,68
Обсяг загального боргу, % до ВВП	не більше 60	0,50	0,22	0,19	0,42	0,84	0,57
Частки іноземного капіталу у статутному капіталі банків	не більше 30	0,58	0,39	0,05	0,95	0,19	0,16
Міжнародні резерви країни в місяцях імпорту	не меньше 3	0,10	0,91	0,99	1,00	0,98	0,91
Контроль корупції		0,89	0,96	0,22	0,13	0,54	0,57
Політична стабільність та відсутність насильства / тероризму		0,39	0,42	0,47	0,47	0,49	0,03
Верховенство права		0,71	0,34	1,00	0,25	0,33	0,37
Рівень інфляції, %	не більше 7	0,99	0,02	0,99	0,99	0,97	0,83
Рівень безробіття,%	не більше 7,6	0,49	0,59	0,43	0,32	0,87	0,65
Індекс GINI		0,12	0,90	0,87	0,39	0,31	0,35
Integralindex		0,5962	0,6287	0,556	0,5538	0,4557	0,619505

Розрахувавши значення інтегрального показника за формулою (8) як індикатора загрози національної економіки в динаміці з 2008 по 2019 рр., виникає

необхідність візуалізації як загальної тенденції поведінки даного індексу в часі, так і варіації в межах від мінімально та максимально можливих рівнів. Для цього побудуємо рисунок 4.9.

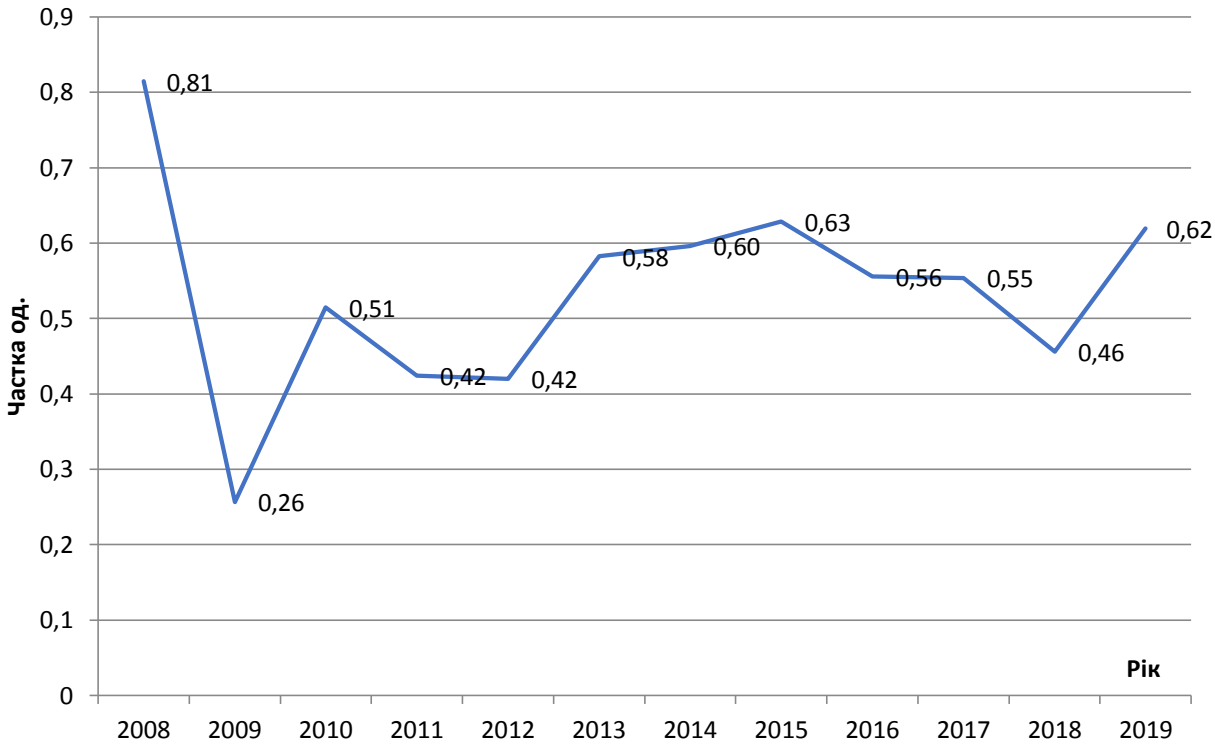


Рисунок 4.9 – Динаміка індексу загрози національної економіки з 2008 по 2019 рр.

Аналіз рисунку 4.9 дозволяє стверджувати, що загальна тенденція індексу загрози національної економіки характеризується як зростаюча.

Усі країни в більшому чи меншому ступені прагнуть забезпечити довготривалі вигідні стратегічні переваги в напрямку економічних стабільності. А процеси, що відбуваються в глобальному світовому співтоваристві, гостро впливають на становлення та розвиток світового господарства, політичні та економічні відносини у суспільстві. Все це спричиняє формування нових загроз і ризиків для розвитку національної економіки та забезпечення безпечного функціонування держави. Забезпечення економічної безпеки передбачає, передусім, створення оптимального, ефективного механізму та методології формування національної економічної безпеки країни на основі побудови

структурно-логічної математичної моделі, що включає відповідну послідовність певних етапів дослідження факторів та показників загроз національної економіки.

Так , формування, розрахунок , оцінка та аналіз узагальненого показника індексу загрози національної економіки, дозволить допомогти у вирішенні основних поставлених цілей ефективного, стабільного, а головне безпечного функціонування національної економіки, таких як: стабільне зростання обсягів національного виробництва; стабілізація рівня цін; забезпечення стабільно о високого рівня зайнятості населення; підтримка рівноваги у зовнішньоторговельному балансі. Запропонована методологія дозволить своєчасно та оперативно забезпечувати підтримку необхідних організаційних, інституційних, нормативно-правових умов, що передбачають спроможність системи національної економіки до протистояння зовнішніх та внутрішніх загроз та навантажень, подальшої якісної адаптації до проблем та дестабілізуючих факторів, і як результат швидкому відновленню після впливу негативних чинників.

ВИСНОВКИ

Представлені у першому розділі наукові результати створюють передумови забезпечення інформаційної безпеки як основи формування кіберпростору країни. Так, проведений аналіз кіберзагроз дозволив визначити найбільш проблемні діялнки банківської діяльності, які піддаються найбільшого впливу з боку шахраїв. В результат виявлено, що проблемними є операції, які здійснюються за допомогою Інтернет-банкінгу та мобільного банкінгу, а найбільш розповсюдженими методами шахрайства є соціальна інженерія, в результаті чого населення України, які є клієнтами банків, все частіше становиться об'єктом шахрайства. Проведений первинний аналіз даних щодо загальних сум транзакцій; типів пристроїв, з яких здійснювалася транзакція; місцеположення пристрою, з якого проведено транзакцію; країни, яка була вказана користувачем мобільного або інтернет-банкінгу при реєстрації; суми, що знаходиться на балансі клієнта після проведення транзакції; суми, що знаходилась на балансі клієнта до проведення транзакції; типу транзакції, яку було проведено користувачем мобільного або інтернет-банкінгу. Результати аналізу дозволили виділити ті вузькі місця в системі кіберзахисту, які піддаються шахрайствам.

Розроблено модель впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері, яка включає три сфери – економічну (мінімальна заробітна плата населення, індекс економічної свободи, ВВП на душу населення), політичну (рівень сприйняття корупції, індекс цивільної свободи, рівень злочинності в країні та індекс недієздатності держави), соціальну (індекс цивільно свободи, індекс процвітання, індекс миру, населення, яке проживає в країні, індекс щастя та індекс людського розвитку). В результаті побудовано трикутник з урахуванням даних сфер, за допомогою якого на основі аналізу центру мас визначається схильність до шахрайства з банківськими продуктами. Запропонована методика дозволяє прогнозувати та попереджати

шахрайські операції на макрорівні, шляхом розробки превентивних заходів контролю, як частини системи кібербезпеки.

Проведено канонічний аналіз взаємозв'язку кібербезпеки та соціо-економіко-політичного розвитку країни: для дослідження обрано дані національного індексу кібербезпеки та фактори соціо-економіко-політичного розвитку для 159 країн світу; побудовано карту країн світу із зазначенням національного індексу кібербезпеки; визначено канонічні корені, факторну структуру, дисперсію та надмірність, канонічні ваги для факторів, регресійні рівняння. Результати аналізу підтвердили справедливість гіпотези, що фактори розвитку обумовлюють рівень інформаційної безпеки та навпаки, рівень безпеки може впливати на розвиток країни. Практичне значення отриманих результатів полягає у виробленні ряду стратегічних заходів: посилення інститутів безпеки, впровадження нових методів та заходів безпеки, що, в свою чергу, позитивно впливатиме на політичну стабільність в країні, соціальну захищеність населення від кібершахрайств, зниження збитків економіки держави та суб'єктів господарювання від незаконного використання ресурсів.

Проведено оцінку рівня інформаційної безпеки країни з урахуванням їх розвитку, що відбуватиметься з використанням самоорганізованих карт Кохонена: обрано дві групи показників – індекси інформаційної безпеки та розвитку для 159 країн світу; для виявлення показників із тісним статистичним зв'язком проведено кореляційний аналіз, за результатами якого було відібрано 12 показників розвитку; для приведення даних у співставні величини було проведено нелінійну нормалізацію; за допомогою аналітичної платформи Deductor Academic дані було перевірено на якість, наявність викидів, дублікатів та протиріч. На основі побудованих карт Кохонена отримано 7 кластерів країн: 0-й та 1-ий включає країни з найвищими показниками розвитку та безпеки, 2-й – країни з показниками вище середнього, 3-й – із середнім рівнем розвитку та безпеки, 4-й – рівнем нижче середнього, 5-й – низьким рівнем, 6-й – дуже низьким. Практичне застосування отриманих результатів дозволить виділити групи країн, які слабко

розвиваються у напрямку підвищення ефективності системи інформаційної безпеки, а також ті сфери, які потребують додаткової уваги з боку відповідних державних органів, які займаються питаннями безпеки країни.

Проведене рейтингування 160 країн світу за рівнем кібербезпеки та ефективності системи інформаційної безпеки країни за допомогою використання багатоатрибутних методів прийняття рішень (методи TOPSIS, VIKOR та MAAM). В результаті встановлено, що рейтинг за методом MAAM має близько 25% подібності із значеннями реального рейтингу. Найбільш ефективним для рейтингування країн виявився метод TOPSIS, який нівелює недоліки методу реальної оцінки та дозволяє визначати найкращу та найгіршу альтернативу, що сприяє здійсненню аналізу окремо й для показників. Застосування запропонованого підходу дозволяє вирішити ряд проблем, пов'язаних із розмірністю даних, визначенням вагів показників, врахуванням різнонаправленості значень показників та їх кардинальних відмінностей. Практичні результати показали, що країни Естонія та Чеська Республіка мають найвищі рейтинги та значення їх показників найбільше наближається до ідеальних, тобто доцільно звернути увагу на їх практику щодо формування стратегії кібербезпеки, особливо в частині тих показників, які для кожної окремої країни значно відхиляються від ідеальних та мають критичні значення. Країною із самим низьким рейтингом, що було підтверджено розрахунками за всіма методами, є Південний Судан. Оскільки вона має проблеми політичного, військового, соціально-економічного характеру, то це підтверджує відсутність пріоритету забезпечення її кіберзахисту.

Представлені у другому розділі наукові результати відображують організаційно-інституційні засади забезпечення стійкості фінансового кіберпростору в розрізі розробки науково-методичних засад формування механізму забезпечення кіберстійкості банків.

Представлені у третьому розділі результати присвячені сучасним технологіям внутрішньої кібербезпеки економічних агентів. Так, визначено

доцільність застосування заходів впливу у сфері фінансового моніторингу для забезпечення банківської безпеки, а саме: скорочення кількості фінансових злочинів і відповідних втрат від них; зниження об'єму тіньової економіки; посилення надійності банків; посилення контрою за міждержавними переказами; контроль за діяльністю конвертаційних центрів; збільшення сум сплачених податків від викритих нелегальних доходів; покращення ефективного застосування бюджетних ресурсів; скорочення корупційного рівня; зростання показника конкурентоспроможності країни; боротьба з кіберзлочинністю; контроль операцій з цінними паперами; зосередження уваги на можливих шахрайствах у банківській сфері; посилення протидії фінансуванню тероризму, військових дій.

Встановлено, що в системі аудиту доцільно використовувати сучасні методи виявлення та попередження шахрайства персоналу: стандарт ISO/IEC 27001 «Управління інформаційною безпекою», метод аналізу розривів, метод оцінки ризиків, система фрод-моніторингу, якісні методи, кількісні методи, методи машинного навчання. Доведено, що найбільш оптимальними для врахування невизначеності та виявлення шахрайств у банках є гібридні методи, що використовують сильні сторони різних підходів, застосування яких дозволяє знизити рівень шахрайства та підвищити відповідальність банківського персоналу.

Розроблено нечітко-множинну модель, як надає аудитору можливість оцінити ризик шахрайства банківського персоналу та визначити основні сфери, що найбільше сприяють шахрайству. Модель було розроблено для оцінювання ризику шахрайства персоналу щодо викривлення фінансової звітності. З цією метою виділено три групи індикаторів ризику: спонукання до викривлення фінансової звітності; сприятливі можливості для викривлення фінансової звітності; обґрунтування викривлення фінансової звітності. Використання даної моделі на практиці дозволить підвищити загальну ефективність аудиту та сприятиме попередженню шахрайств.

Розроблено гравітаційну модель оцінки привабливості країни для легалізації кримінальних доходів, що дозволить зменшити ризики для держави з боку легалізації кримінальних доходів та фінансування тероризму, які здійснюються за допомогою банківського сектору. Її застосування дозволить сформувати інформаційну базу для прийняття управлінських рішень щодо підвищення рівня кіберзахисту, оскільки це надає можливості концентрувати увагу саме на тих країнах, з якими ризик легалізації є підвищеним. Впровадження даної методики сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових операцій, здійснення яких можливе за межами країни;

Представлені у четвертому розділі наукові результати відображують механізм регулювання безпеки держави як детермінанта її розвитку. Так, побудовано економіко-математичну модель вибору стратегій державного регулювання економічної безпеки національної економіки як основи для подальшого формування внутрішньобанківських інструкцій щодо організації AML-системи та системи кіберзахисту на основі застосування інструментарію теорії ігор (максимінний та мінімаксний критерії за допомогою теореми Неймана). Модель здійснює формалізацію системи заходів Державного регулювання економічної безпеки національної економіки, щодо знаходження компромісної точки у тріаді таких напрямів: зведення до мінімуму величини інтегрального індексу загрози національної економіки, мінімізації рівня використання банків з метою легалізації кримінальних доходів за рахунок максимізації рівня ефективності внутрішньобанківської системи фінансового моніторингу в розрізі певного банку та одночасної мінімізації узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів. Практичне застосування такої методики допоможе створити дієві інструменти для стабільного розвитку національної економіки, забезпечить стійку макроекономічну позицію, допоможе знизити рівень корупції, зменшити розрив у фінансовому рівні забезпечення серед населення країни, сприятиме збільшенню

податкових надходженьдо бюджету, допоможе забезпечити стійкість до дестабілізуючих факторів;

Проведено оцінку інтегрального індексу загрози національної економіки як одного із векторів стратегії забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні на основі застосування функції Кернела. Для здійснення оцінки індексу загрози національної економіки побудовано структурно-логічну математичну модель, що включає послідовність етапів дослідження: створено інформаційну базу вхідних предикторів за досліджуваний період часу; приведено показники вхідної інформаційної бази дослідження до співставного вигляду шляхом проведення нелінійної нормалізації; відібрано релевантні показники оцінювання індексу загрози національної економіки на базі комбінації методів Парето та діаграми розсіювання; проведено оцінювання інтегрального індексу загрози національної економіки за допомогою функції Кернела та мультиплікативної форми згортки. Здійснено візуалізацію як загальної тенденції поведінки інтегрального індексу загрози в часі, так і варіації в межах від мінімально та максимально можливих рівнів. Практичне застосування запропонованої методології дозволить своєчасно та оперативно забезпечувати підтримку необхідних організаційних, інституційних, нормативно-правових умов, що передбачають спроможність системи національної економіки до протистояння зовнішніх та внутрішніх загроз та навантажень, подальшої якісної адаптації до проблем та дестабілізуючих факторів, швидкому відновленню після впливу негативних чинників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Dennis J.B. A position paper on computing and communications. *Communications of the ACM*. 1968. Vol. 11. Issue 5. P. 370-377. DOI: 10.1145/363095.363147.

2. Morrow S., Crabtree T. The future of cybercrime & security. Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024. *Juniperresearch* : веб-сайт. URL: https://www.juniperresearch.com/researchstore/key-vertical-markets/cybercrime-cybersecurity-research-report?utm_campaign=pr1_thefutureofcybercrime_technology_aug19&utm_source=businesswire&utm_medium=pr (дата звернення: 30.08.2020).

3. China's Got a New Plan to Overtake the U.S. in Tech. *Bloomberg :* веб-сайт. URL: https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech#:~:text=In%20the%20masterplan%20backed%20by,develop%20AI%20software%20that%20will (дата звернення: 30.08.2020).

4. Download VOSviewer. *VOSviewer* : веб-сайт. URL: https://www.vosviewer.com/download (дата звернення: 30.08.2020).

5. Analyze search results. *Scopus* : веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=37680dfe405b9a71ae81f77b9206fbdb&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22 %29&sort=plf-f&sdt=sisr&sot=b&sl=37&count=1787&analyzeResults=Analyze+results&ref=%28cybersecurity%29&txGid=205846568ffb28df0797b696453a07d8 (дата звернення: 20.07.2020).

6. Documents by subject area. *Scopus* : веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=420e4f1dc693161a54f75c803f0df182&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22% 29&sort=plf-f&sdt=b&sot=b&sl=37&count=21774&analyzeResults=Analyze+results&txGid=fd91a0e77a7c0d166c04e9bc60297cea (дата звернення: 20.07.2020).

7. Documents by country or territory. *Scopus* : веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=420e4f1dc693161a54f75c803f0df182&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22% 29&sort=plf-f&sdt=b&sot=b&sl=37&count=21774&analyzeResults=Analyze+results&txGid=907f30981e6718dcfdee105b7c052420 (дата звернення: 20.07.2020).

8. Documents by authors. *Scopus* : веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=420e4f1dc693161a54f75c803f0df182&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22% 29&sort=plf-f&sdt=b&sot=b&sl=37&count=21774&analyzeResults=Analyze+results&txGid=907f30981e6718dcfdee105b7c052420 (дата звернення: 20.07.2020).

9. Rikk R. National Cyber Security Index 2018. *E-governance Academy* : веб-сайт. URL: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (дата звернення: 20.07.2020).

10. National Cyber Security Index. *NCSI* : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 20.07.2020).

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

12. World Development Indicators. *The World Bank* : веб-сайт. URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (дата звернення: 20.07.2020).

13. Kosevich, E. Cyber security strategies of Latin America countries. *Iberoamerica (Russian Federation).* 2020. Vol. 1. P. 137-159. DOI: 10.37656/S20768400-2020-1-07.

14. Kirilenko, V.P., Alexeyev, G.V. Political technologies and international conflicts in the information space of the Baltic Sea region. *Baltic Region*. 2018. Vol. 10. № 4. P. 20-38. DOI: 10.5922/2079-8555-2018-4-2.

15. Singh, A.N., Gupta, M.P. Information Security Management Practices: Case Studies from India. *Global Business Review*. 2019. Vol. 20. № 1. P. 253-271. DOI: 10.1177/0972150917721836.

16. Ključnikov, A., Mura, L., Sklenár, D. Information security management in smes: Factors of success. *Entrepreneurship and Sustainability Issues*. 2019. Vol. 6. № 4. P. 2081-2094. DOI: 10.9770/jesi.2019.6.4(37)

17. Sadigov, M., Kuzmenko, O., Yarovenko, H. Blockchain technology based system-dynamicsimulation modeling of enterprise's syber security system. *55th International Scientific Conference on Economic and Social, Baku, Azerbaijan, 18-19 June 2020.*, Varazdin Development and Entrepreneurship Agency. 2020. Vol. 1/4. P. 399-408. URL: https://www.esd-conference.com/upload/book_of_proceedings/Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf (дата звернення: 20.08.2020).

18. Dorosh, M., Voitsekhovska, M., Balchenko, I. Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. *2nd International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2019, Kiev, Ukraine, 29 March 2019.* Advances in Intelligent Systems and Computing. 2019. Vol. 938. P. 503-512. DOI: 10.1007/978-3-030-16621-2_47.

19. Schmitz, C., Pape, S. LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers and Security.* 2020. Vol. 90. № 101656. DOI: 10.1016/j.cose.2019.101656.

20. Yevseiev S., Aleksiyev V., Balakireva S., Peleshok Y., Milov O., Petrov O., Rayevnyeva O., Tomashevsky B., Tyshyk I., Shmatko O. Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. *Eastern-European Journal of Enterprise Technologies.* 2019. Vol. 3. № 9-99. P. 49-63. DOI: 10.15587/1729-4061.2019.169527.

21. National Cyber Security Index. *NCSI* : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 20.08.2020).

22. Kohonen, T. Self-Organized Formation of Topologically Correct Feature Maps. *Biological Cybernetics.* 1982. Vol. 43. № 1. P. 59-69. DOI: 10.1007/BF00337288.

23. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Volume 5, Issue 1. URL: https://doi.org/10.1093/cybsec/tyz013 (дата звернення: 23.09.2020).

24. Шугунов Т., Жуков А., Хочуева Ф. Проблемы обеспечения киберустойчивости банковской системы Российской Федерации: правовой и методологический аспекты. *Пробелы в российском законодательстве*. 2019. № 6: С. 250-253.

25. Петренко С. Киберустойчивость индустрии 4.0. The 2018 symposium on cybersecurity of the digital economy (CDE'18). Вторая международная научно-техническая конференция. 2018. С. 370-381.

26. Дубина М., Середюк І., Білоус Н. Роль кіберстрахування в системі ризик-менеджменту банківських установ. П*роблеми і перспективи економіки та управління.* 2020. № 1 (21). С.183-196.

27. Gray A., Mee P. Large-scale cyber attacks on the Financial System. Oliver Wyman. URL:https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf (дата звернення: 23.09.2020).

28. Gracie A. Managing cyber risk – the global banking perspective. British Bankers' Association Cyber Conference. London.

29. Богославський М. Ю. Дослідження ступеню протидії банківським кібератакам на світовому та вітчизняному рівнях. *Агросвіт*. 2018. № 2. С. 88-92.

30. Приказюк Н. В., Кукурудзяк М. В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування. *Вісник Одеського національного університету*. Серія : Економіка. 2016. Т. 21, Вип. 2. С. 164-168.

31. Михайлюк Р. В. Механізм управління фінансовою стійкістю комерційних банків: автореф. дис. ... канд. екон. наук : 08.00.08. Тернополь, 2008. 22 с.

32. Cyber resilience oversight expectations for financial market infrastructures. *European Central Bank*. 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (дата звернення:23.09.2020).

33. Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO. *Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions*. 2016. URL:https://www.bis.org/cpmi/publ/d146.pdf. (дата звернення: 23.09.2020).

34. Bodeau D., Graubart R. Cyber Resiliency Design Principles. Mitre technical report. 2017. 98 P. URL: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf (дата звернення: 23.09.2020).

35. Cyber resilience: Health check. *Australian Securities and Investments Commission*. 2015. URL: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf (дата звернення: 28.09.2020).

36. Cyber Lexicon. *Financial Stability Board*. 2018. URL: https://www.fsb.org/wp-content/uploads/P121118-1.pdf (дата звернення: 23.09.2020).

37. Collins R., O'Connor-Close C., Zhang A. Cyber incident cost estimates and the importance of building resilience. *The Reserve Bank of New Zealand*. 2020. Vol 84, №2. URL: https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2020/rbb2020-84-02 (дата звернення: 28.09.2020).

38. Комітет «Кіберстійкості бізнесу». URL: https://corporatesecurity.org.ua/uk-UA/Novyny/Vidbulos-zasidannya-komitetu-Kiberstijkosti-biznesu.aspx?ID=272 (дата звернення: 28.09.2020).

39. NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. *NIST*. URL:

https://www.tenable.com/whitepapers/adhering-to-the-nist-framework-with-tenable-ot?utm_campaign=00019887&utm_promoter=tenable-enterprise-comp-00019887&utm_source=google&utm_medium=cpc&utmgeo=emea &gclid =CjwKCAjww5r8BRB6EiwArcckC3rzHgkmtvFh4oj-fRYHlBtX0ZAB-0z0uZK4NGFvER8qlpE-iJFkzRoCaIQQAvD_BwE (дата звернення: 28.09.2020).

40. Колосок И. Н., Гурина Л. А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы. *Информационные и математические технологии в науке и управлении*. 2019. №2 (14). URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy (дата звернення: 14.10.2020).

41. Cyber-resilience: Range of practices. *Basel Committee on Banking Supervision*. 2018. URL: https://www.bis.org/bcbs/publ/d454.pdf (дата звернення: 23.09.2020).

42. Financial Sector's Cybersecurity: A Regulatory Digest. *The World Bank Group.* 2017. URL: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (дата звернення: 23.09.2020).

43. Almansi A. A. Financial sector's cybersecurity: regulations and supervision. FCI Insight Washington, D.C. World Bank Group. 2018. 38 P.

44. World Bank adopts ECB's cyber resilience oversight expectations. *European Central Bank*. 2020. URL: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html (дата звернення: 23.09.2020).

45. TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. *European Central Bank*. 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (дата звернення: 23.09.2020).

46. Fundamental Elements of Cybersecurity for the Financial Sector. *G7*, October 11, 2016. URL: https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf (дата звернення: 23.09.2020).

47. Bissel K., Lassale R.M., Dal Cin P. Ninth Annual Cost of Cybercrime Study. *Accenture* : веб-сайт. URL: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (дата звернення: 15.06.2020).

48. IBM X-Force Threat Intelligence Index. *IBM Security* : веб-сайт. URL: https://www.ibm.com/security/data-breach/threat-intelligence (дата звернення: 15.06.2020).

49. Spaic I. Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift. *Organized Crime and Corruption Reporting Project* : веб-сайт. URL: https://www.occrp.org/en/daily/5419-ukraine-us-10-million-stolen-from-unnamed-bank-via-swift (дата звернення: 15.06.2020).

50. Culp S., Kim F., Gomes R. Banking Risk: Evolving ecosystem, evolving threats. *Accenture* : веб-сайт. URL: https://www.accenture.com/us-en/insights/financial-services/banking-global-risk-study (дата звернення: 15.06.2020).

51. Casino F., Dasaklis T.K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*. 2019. Vol. 36. P. 55-81. DOI: https://doi.org/10.1016/j.tele.2018.11.006.

52. Bahou A.J. Blockchain and Applications in Information Security. *Information Systems Security Association* : веб-сайт. URL: https://issa-

midtn.org/resources/Documents/AJ%20Bahou%20-%20Blockchain%20Applications%20in%20Information%20Security.pdf (дата звернення: 15.06.2020).

53. Sari A. Use of Blockchain in Strengthening Cybersecurity And Protecting Privacy. *International Journal of Engineering and Information Systems (IJEAIS).* 2018. Vol. 2. Issue 12. P. 59-66.

54. English E., Kim A.D., Nonaka M. Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. *Microsoft Corporation* : електронний документ. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G (дата звернення: 15.06.2020).

55. Building confidence: solving banking`s cybersecurity conundrum. *Accenture* : веб-сайт. URL: https://www.accenture.com/_acnmedia/pdf-44/accenture-building-confidence-solving-banking-cybersecurity-conundrum.pdf (дата звернення: 15.06.2020).

56. Google Trends. *Google Trends* : веб-сайт. URL: https://trends.google.com/trends (дата звернення: 15.06.2020).

57. Report to the nations on occupational fraud and abuse, Association of Certified Fraud Examiners (ACFE). URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf (дата звернення: 16.10.2020).

58. Zuraidah Mohd Sanusi, Mohd Nor Firdaus Rameli, Yusarina Mat Isa (2015) Fraud schemes in the banking institutions: prevention measures to avoid severe financial loss. *Procedia economics and finance*. № 28. P. 107-113.

59. Міжнародні стандарти професійної практики внутрішнього аудиту. URL: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Ukrainian.pdf (дата звернення: 16.10.2020).

60. Zuraidah Mohd Sanusi, Mohd Nor Firdaus Rameli, Yusarina Mat Isa (2015) Fraud schemes in the banking institutions: prevention measures to avoid severe financial loss. *Procedia economics and finance*. № 28. P. 107-113.

61. Jarrod West, Maumita Bhattacharya, Rafigul Islam. Intelligent financial fraud detection practices: an investigation. *Proceedings of the international conference on security and privacy in communication networks*. 2014. Volume 153. P. 186-203. DOI: 10.1007/978-3-319-23802-9_16.

62. Усач Б.Ф., Маркевич М.А. Виявлення фактів шахрайства у контексті аудиту фінансових звітів банків. *Вісник Житомирського державного технологічного університету. Серія «Економічні науки»*. 2010. № 3 (53). С. 253-255.

63. Christie L. Comunale, Rebecca L. Rosner, Thomas R. Sexton. The Auditor's Assessment of Fraud Risk: A Fuzzy Logic Approach. Journal of Forensic & Investigative Accounting. 2010. Vol. 2, Issue 3, Special Issue. P.95-140.

64. Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit. URL: https://www.aicpa.org/research/standards/auditattest/downloadabledocuments/au-00316.pdf (дата звернення: 16.10.2020).

65. Пономаренко В.С., Малярець Л.М. Багатовимірний аналіз соціально-економічних систем: [навчальний посібник]. Харків: ХНЕУ, 2009. 384 с.

66. Недосекин А.О. Оценка риска бизнеса на основе нечетких данных: [монография]. Санкт-Петербург, 2004. 100 с.

67. Andruseac, G. *Economic Security – New Approaches In The Context Of Globalization*, CES Working Papers, Centre for European Studies, AlexandruIoanCuza University, 2015, 7(2), 232-240.

68. Kahler, M. Economic security in an era of globalization: definition and provision. *The Pacific Review* 2006, *17, 4, 485-502.*

69. Rotaru, M.P. *Economic Security - Organic Dimension of National Security*,MPRA Paper17936, University Library of Munich, Germany, 2009.

70. Navarro, P. Why Economic Security Is National Security. *RealClearPolitics*2018.

71. Haigner, S.D.; Schneider, F.; Wakolbinger, F. *Combating money laundering and the financing of terrorism: A survey*, Economics of Security Working Paper 65, Berlin: Economics of Security, 2012.

72. Schneider, F. The Dark Side: Crime Has Gone Global. Trilogue Salzburg, 2017. Available online: https://www.bertelsmann-stiftung.de/fileadmin/files/Faktencheck/Leaders__Dialogues/Salzburger_Trilog_2017/8_The_Dark_Side.pdf (accessed on 30 December 2018).

73. Buriak, A.; Lyeonov, S.;Vasylieva, T. Systemically Important Domestic Banks: An Indicator-Based Measurement Approach For The Ukrainian Banking System. *Prague economic papers* 2015,*24, 6*, 715-728.

74. Stokes, R. Anti-Money Laundering Regulations and Emerging Payment Technologies. *Banking & Financial Service Policy Report*, 2013, *32, 5*, 2-6.

75. Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Van Eeten, M.J.G.; Levi, M.; Moore, T. and Savage, S. *Measuring the Cost of Cybercrime.* The Economics of Information Security and Privacy, Springer Verlag Berlin Heidelberg, 2013, pp. 265–300.

76. Mazloumfard, H.; Glans, V. The Influenceof Tax Burdenonthe Profitof Banksin Conditionsof Monopolistic Competition: Economic-Mathematical Modeling. *Financial Markets, Institutions and Risks* 2017, 1, 4, pp. 28-36.

77. Krykliy, O.; Luchko, I. Model of Stress-testing of Banks' Liquidity Risk in Ukraine. *Financial Markets, Institutions and Risks* 2018, 2, 2, pp.123-132.

78. Subeh, M.A.; Yarovenko, H. Data Miningof Operations with Card Accounts of Bank Clients. *Financial Markets, Institutions and Risks* 2017, 1, 4, pp. 87-95.

79. Dean, J.; Syniavska, O.; Minenko, S.; Using economic-mathematical modeling in the study of the economic component of terrorism. *SocioEconomic Challenges* 2017, 1, 2, pp. 103-109.

80. Anderson, J.E. The Gravity Model. *Annual Review of Economics* 2011,3(1), pp. 133-160.

81. Asgharzadeh, M.F.; Hashemi, H.; Frese R.B. Comprehensive gravitational modeling of the vertical cylindrical prism by Gauss–Legendre quadrature integration. *Geophysical Journal International* 2018, 1, 212, pp. 591–611.

82. Ferwerda, J.; Kattenberg, M.; Chang, H.-H.; Unger, B.; Groot, L.; Bikker, A.J. Gravity Models of Trade-based Money Laundering. *DNB Working Paper* 2011, 318, pp. 1-28.

83. Brisard, J.-C.; Martinez, D. ISIS Financing in 2015. Center for the Analysis of Terrorism, 2016.

84. Кузьменко О.В. *Економіко-математичне забезпечення функціонування пере страхового ринку*; Університетська книга: Суми, Україна, 2014.

85. 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, pp. 221-233.

86. Моделювання оцінки операційного ризику комерційного банку / О.С. Дмитров та ін. ; за ред. С.О. Дмитрова. Суми : Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України», 2010. 277 с.

87. Саати Т. Принятие решений. Метод анализа иерархий / пер. с англ. Р.Г. Вачнадзе. Москва: Радио и связь, 1993. 278 с.

88. Saaty T.L. Decision making with the analytic hierarchy process. *Int. J. Services Sciences.* 2008. Vol. 1. No. 1. P. 83–98. URL: http://www.rafikulislam.com/uploads/resourses/197245512559a37aadea6d.pdf.

89. Горбатенко В.П. Політичні ризики: від теорії до практики. *Суспільно-політичні процеси*. 2016. Вип. 2. С. 55-69.

90. Акімова Л.М. Сутнісна характеристика основних загроз в економічній безпеці держав. *Державне управління: удосконалення та розвиток.* 2016. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=1247 (дата звернення: 01.07.2020).

91. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations*. 2019. №3. P. 308-326. DOI: http://doi.org/10.21272/mmi.2019.3-24.

92. Гладун Т.М. Застосування методу аналізу ієрархій для вибору франчайзингової мережі. *Інституціональний репозиторій Львівського політехнічного національного університету.* URL: http://ena.lp.edu.ua/bitstream/ntb/36011/1/19_109-115.pdf (дата звернення: 01.07.2020).

93. Геєць, В. М. Моделювання економічної безпеки: держава, регіон, підприємство [Текст] : монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, Т. С. Черняк; Н. -д. центр індустр. пробл. розвитку НАН України. — Х. : ВД "ИНЖЭК", 2006. — 240 с.

94. Каламбет С. В., Кириленко Б. О. Економічна безпека як багаторівнева система. Економіка і суспільство. 2016. № 5. С. 344-349.

95. Пономаренко, В. С. Концептуальні основи економічної безпеки: монографія / В. С. Пономаренко, С. В. Кавун. – Харків : Видавництво ХНЕУ, 2008. – 256 с.

96. Акімова Л. М. Теоретичні основи державного управління розвитком національної безпеки / Л. М. Акімова // Державне управління: удосконалення та розвиток: електронне наукове фахове видання. – 2015. – № 5.

97. Майстро С.В. Напрями удосконалення механізму державного управління фінансово-економічною безпекою України в сучасних умовах. Актуальні проблеми державного управління. 2015. Вип. 1. Ч. 46. С. 210–218.

98. Матвійчук І.О. Інституціоналізація управління економічною безпекою держави / І.О. Матвійчук // Вісник Академії митної служби України. Сер.: Економіка. — 2012. — № 2. — С. 131—141.

99. Плакіда А. О. Реалізація державної політики у сфері економічної безпеки національної економіки : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : спец. 25.00.02 «Механізми державного управління» / А. О. Плакіда. - Запоріжжя, 2008. − 20 с.

100. Сороківська О. А. Інноваційні напрями підвищення економічної безпеки підприємств малого бізнесу в умовах конфліктних ситуацій. Дисертація на здобуття наукового ступеня доктора економічних наук: 08.00.04 / Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль, 2016. 488 с.

101. Ткачова Н. М. Механізм державного регулювання економічної безпеки регіону : автореф. дис. на здобуття наук. ступеня доктора наук з держ. упр. : спец. 25.00.02 «Механізми державного управління» / Н. М. Ткачова. – Запоріжжя, 2009. – 40 с.

102. Michael A. Rigdon, Franz R. Epting, Robert A. Neimeyer & Seth R. Krieger. The threat index: A research report, Death Education. 1979. №3, pp.245-270.

103. Paul J. Robinson, Keith Wood. The Threat Index: An Additive Approach. Omega. 1985. Vol. 15, issue 2, pp. 139-144.

104. Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, and Greg Wiseman, Phillipa Gill, Ronald J. Deibert. Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware. USENIX Security Symposium. 2014. №23. Pp.527-541.

105. Oakleaf, J. R., C. M. Kennedy, S. Baruch-Mordo, P. C. West, J. S. Gerber, L. Jarvis, and J. Kiesecker. Development Threat Index. Palisades, NY: NASA Socioeconomic Data and Applications Center (SEDAC). Available online: https://doi.org/10.7927/61jv-th84. (Accessed 07 June 2020).

106. Мартинюк В. П. Оцінка стану національної економіки на основі інтегрального показника економічної безпеки держави / В. П. Мартинюк // Економіка, менеджмент, підприємництво. – 2013. – № 25 (1). – С. 179–188.

107. Berglund, A., Guidolin, M., Pedio, M. Monetary policy after the crisis: A threattohedge funds'alphas? Journal of Asset Management. 2020. №21(3), pp. 219-238.

108. Bukhtiarova, A., Semenog, A., Razinkova, M., Nebaba, N., Haber, J.A. Assessment of financial monitoring efficiency in the banking system of Ukraine. Banks and Bank Systems. 2020. №15(1), pp. 98-106.

109. Hkilchenko, N.V., Atamanova, E.A., Slavikovskaya, Y.O. Diagnostics of environmental and social threatstothe territory's development. Economy of Region. 2020. №16(1), pp. 43-58.

110. Бесчастний А. В. Економічна безпека України у контексті світової економічної кризи. Економіка і держава : наук. журн. 2009. №15. С. 67-69.

111. Гбур З.В. Актуальні гібридні загрози економічній безпеці України / З.В. Гбур // Інвестиції:практика та досвід. — 2018. — № 7. — С. 97—99.

112. Макарчук І.М. Оцінка сучасного стану та актуальні загрози економічній безпеці в Україні. Економічний аналіз. 2015. Т. 21. No. 1. С. 83-89.

113. Варналій З. С., Буркальцева Д. Д., Наєнко О. С. Економічна безпека України: проблеми та пріоритети зміцнення: монографія. Київ, 2011. 299 с.

114. Акімова Л.М. Сутнісна характеристика основних загроз в економічній безпеці держави / Л.М. Акімова // Державне управління: удосконалення та розвиток: електронне наукове фахове видання. — 2016. — № 10.

115. Комеліна О.В., Онищенко С. В., МатковськийА. В. Економічна безпека держави: оцінювання та стратегічні орієнтири забезпечення : монографія. Полтава: ПолтНТУ, 2013. 202 с.

116. Мамалуй О. О. Про пріоритетні напрями забезпечення економічної безпеки держави. Вісник Національної юридичної академії України імені Ярослава Мудрого : зб. наук. праць. Харків : Вид-во НЮА України ім. Я. Мудрого, 2011. №4. С. 18-28.

117. Петрушевська, В. В. Економічна безпека держави: зміст і класифікація загроз. Ефективність державного управління : зб. наук. праць. Львів, 2012. Вип. 32. С.441-448.

118. Третяк В.В. Економічна безпека : сутність та умови формування. Економіка і держава : наук. журн. 2010. №1. С. 6-8.

119. Henderson, D. J., and Parmeter, C. F. Applied Nonparametric Econometrics. Cambridge University Press. 2015.

120. Luong Ha Nguyen, Ianis Gaudot, Shervin Khazaeli, James-A. Goulet. A Kernel-Based Method for Modeling Non-harmonic Periodic Phenomena in Bayesian Dynamic Linear Models. Frontiers in Built Environment. 2019, 5. Available online: https://doi.org/10.3389/fbuil.2019.00008. (accessed on 06 June 2020).

121. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. №1. С. 68-75.

122. Варналій З. С., Буркальцева Д. Д., Наєнко О. С. Економічна безпека України: проблеми та пріоритети зміцнення: монографія. Київ, 2011. 299 с.

123. Вашай Ю.В., Самедова Л.Р. Інформаційна безпека та її вплив на стан економічної безпеки держави. *Глобальні та національні проблеми економіки.* 2018. Вип. 22. С. 3-6. URL: http://global-national.in.ua/archive/22-2018/3.pdf (дата звернення: 30.08.2020).

124. Економічна безпека держави: сутність та напрями формування : монографія / Л. С. Шевченко та ін. ; за ред. д-ра екон. наук, проф. Л.С. Шевченко. Х. : Право, 2009. 312 с.

125. Кузьменко О.В., Доценко Т.В, Кушнерьов О.С. Оцінювання ризику використання банків з метою легалізації кримінальних доходів на основі гравітаційного моделювання // Проблеми і перспективи економіки та управління. Випуск № 1 (21). – Чернігів, 2020. С.205-219.

126. КузьменкоО.В., ДоценкоТ.В. Удосконалення системи державного регулювання економічної безпеки національної економіки // "БІЗНЕС-ІНФОРМ". Випуск№7 (510). 2020. С.36-43.

127. Любохинець Л.С., Поплавська О.В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. Науково-виробничий журнал «Бізнес-навігатор». 2017. Вип. 4-1 (43). С. 93-97.

128. Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* 2016. №2. С. 24-31.

129. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. 2017. №24-1. С. 137-140.

130. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: затверджений постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text (дата звернення: 23.09.2020).

131. Світлична В.Ю. Інформаційна безпека: сутність та порядок реалізації. Young Scientist. 2014. №11(14). С. 97-100.

132. Яровенко Г.М. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*. 2020. № 8(40). С. 53-63. DOI: 10.25313/2520-2294-2020-8-6245.

133. Яровенко Г.М. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. *Економічний простір*. 2020. № 157. С. 118-124. DOI: 10.32782/2224-6282/157-21.

134. Яровенко Г.М., Доценко Т.В., Кушнерьов О.С. Формування інтегрального індексу загрози національної економіки. *Журнал "Вісник Сумського державного університету. Серія "Економіка"*. 2020. №2. С. 16-28.

135. Яровенко Г.М. Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни. *Науковий вісник УжНУ. Серія: Міжнародні економічні відносини та світове господарство*. 2020. № 31. С. 160-167. DOI: 10.32782/2413-9971/2020-31-26.

136. Яровенко Г.М., Ковач В.О. Перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків. *Підприємництво та інновації.* 2020. № 12. С. 206-214. DOI: 10.37320/2415-3583/12.36.

137. Яровенко Г.М., Колотіліна О.В. Оцінка ризиків соціо-економіко-політичного розвитку України. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Економіка і управління*. 2020. Том 31 (70). N 4. С. 151-159. DOI: 10.32838/2523-4803/70-4-50.

138. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate / I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, D. Upton. *Journal of Cybersecurity*. 2018. Volume 4, Issue 1. URL: https://doi.org/10.1093/cybsec/tyy006 (дата звернення: 23.09.2020).

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

140. Bilan, Y., Brychko, M., Buriak, A. and Vasilyeva, T. Financial, business and trust cycles: The issues of synchronization | [Ciklusi financiranja, poslovanja i povjerenja: pitanja za sinkronizaciju]. Zbornik Radova Ekonomskog Fakultet au Rijeci. 2019. №37(1), pp. 113-138. DOI: http://doi.org/10.18045/zbefri.2019.1.113.

141. Bilan, Y., Đšuzmenko, Đž. and Boiko, A. Research on the impact of industry 4.0 on entrepreneurship in various countries worldwide. Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision. 2020. pp. 2373-2384. URL: https://ibima.org/accepted-paper/research-on-the-impact-of-industry-4-0-on-entrepreneurship-in-various-countries-worldwide/.

142. Bilan, Y., Rubanov, P., Vasylieva, T. and Lyeonov, S. The influence of industry 4.0 on financial services: Determinants of alternative finance development | [Wpływ przemysłu 4.0 na usługi finansowe: determinanty rozwoju alternatywnych finansów]. Polish Journal of Management Studies. 2019. №19(1), pp. 70-93. DOI: http://doi.org/10.17512/pjms.2019.19.1.06.

143. Boiarko, I. and Samusevych, Y. Role of intangible assets in company's value creation. Actual Problems of Economics. 2011. №3(117), pp. 86-94. URL: https://www.researchgate.net/publication/292366060_Role_of_intangible_assets_in_company's_value_creation.

144. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*. 2018. WP/18/143. P. 28. URL: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (дата звернення: 23.09.2020).

145. CBINSIGHTS. Banking Is Only The Beginning: 58 Big Industries Blockchain Could Transform. Retrieved 01.05.2020 from https://www.cbinsights.com/research/industries-disrupted-blockchain/.

146. Cosmulese, C.G., Grosu, V, Hlaciuc, E. and Zhavoronok, A. The Influences of the Digital Revolution on the Educational System of the EU Countries. Marketing and Management of Innovations. 2019. № 3, pp. 242-254. DOI: http://doi.org/10.21272/mmi.2019.3-18.

147. DELLTechnologies. Data Protection in a Multi-Cloud World. Retrieved 01.05.2020 from https://www.dellemc.com/lv-lv/collaterals/unauth/infographic/products/data-protection/global-data-protection-index-2020-snapshot.pdf.

148. Druhov, O., Druhova, V. and Pakhnenko, O. The influence of financial innovations on eu countries banking systems development. Marketing and Management of Innovations. 2019. №3, pp. 167-177. DOI: http://doi.org/10.21272/mmi.2019.3-13.

149. Duvenaud, D. Automatic Model Construction With Gaussian Processes. Ph.D. thesis, University of Cambridge. 2014.

150. EY. Cybersecurity: more than protection? EY International Information Security Survey 2018-2019. Retrieved 01.05.2020 from https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/$FILE/ey-global-information-security-survey-rus.pdf.

151. Grenčíková, A., Bilan, Y., Samusevych, Y. and Vysochyna, A. Drivers and Inhibitors of Entrepreneurship Development in Central and Eastern European Countries. Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020, pp. 2536-2547. URL: https://ibima.org/accepted-paper/drivers-and-inhibitors-of-entrepreneurship-development-in-central-and-eastern-european-countries/.

152. Grytsenko, L. and Vysochina, A. Balanced Scorecard as an assessment tool for enterprise strategy. Actual Problems of Economics. 2012. №3, pp. 161-167.

153. Grytsenko, L., Boyarko, I. and Roenko, V. Controlling of enterprises cash flows. Actual Problems of Economics. 2010. №3, pp. 14-154.

154. IBM Security. X-Force Threat Intelligence Index 2020. Retrieved 01.05.2020 from https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf.

155. Kendiukhov, I. and Tvaronavičienė, M. Managing innovations in sustainable economic growth. Marketing and Management of Innovations. 2017. №3, pp. 33-42. DOI: http://doi.org/10.21272/mmi.2017.3-03.

156. Korablinova, I. A. Tendencies and features of development of companies in digital epoch. Marketing and Management of Innovations. 2017. №1, pp. 289-299. DOI: http://doi.org/10.21272/mmi.2017.1-26.

157. Ledger Insights. CB Insights says enterprise blockchain funding less than 20% of cryptocurrencies. But is it?. Retrieved 01.05.2020 from https://www.ledgerinsights.com/cb-insights-enterprise-blockchain-funding/.

158. Leonov, S. V., Vasilyeva, T. A. and Shvindina, H. O. Methodological approach to design the organizational development evaluation system. Scientific Bulletin of Polissia. 2017. №3(11), P.2, pp. 51-56. DOI: http://doi.org/10.25140/2410-9576-2017-2-3(11)-51-56.

159. Levchenko, V., Boyko, A., Savchenko, T., Bozhenko, V., Humenna, Yu. and Pilin, R. State regulation of the economic security by applying the innovative approach to its assessment. Marketing and Management of Innovations. 2019. №4, pp. 364-372. DOI: http://doi.org/10.21272/mmi.2019.4-28.

160. Levchenko, V., Kobzieva, T., Boiko, A., and 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, pp. 361-371. DOI: http://doi.org/10.21272/mmi.2018.4-31.

161. Lyeonov, S., Kuzmenko, O., Yarovenko, H. and Dotsenko, T. The innovative approach to increasing cybersecurity of transactions through counteraction to money laundering. Marketing and Management of Innovations. 2019. №3, pp. 308-326. DOI: http://doi.org/10.21272/mmi.2019.3-24.

162. Melnyk, L. Paradigm modeling studies of the formation of a knowledge economy in the information society. Marketing and Management of Innovations. 2017. Volume 2, pp. 269 - 279. DOI: http://doi.org/10.21272/mmi.2017.2-25.

163. Pakhnenko, O., Liuta, O. and Pihul, N. Methodological approaches to assessment of the efficiency of business entities activity. Business and Economic Horizons (BEH). 2018. №14(1), pp. 143-151. DOI: http://doi.org/10.15208/beh.2018.12.

164. Ponemon Institute. Cost of a Data Breach Report 2019. Retrieved 01.05.2020 from https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.

165. Rios, R., Lopez, J. B. L. and Veiga, J. G. The fifth global Kondratiev: low economic performance, instability and monopolization in the digital age. Marketing and Management of Innovations. 2018. №2, pp. 270-291. DOI: http://doi.org/10.21272/mmi.2018.2-22.

166. Rubanov, P., Vasylieva, T., Lyeonov, S. and Pokhylko, S. Cluster analysis of development of alternative finance models depending on the regional affiliation of countries. Business and Economic Horizons. 2019. №15(1), pp. 90-106. DOI: http://doi.org/10.22004/ag.econ.287251.

167. Sadigov M., Kuzmenko O., Yarovenko H. Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system. Economic and Social Development: Book of Proceedings. 2020. P. 399-408. URL: https://www.esd-conference.com/upload/book_of_proceedings/Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf.

168. Semenova, K. D. and Tarasova, K. I. Establishment of the new digital world and issues of cyber-risks management. Marketing and Management of Innovations. 2017. № 3, pp. 236-244. DOI: http://doi.org/10.21272/mmi.2017.3-22.

169. Sotnyk, I., Zavrazhnyi, K., Kasianenko, V., Roubík, H. and Sidorov O. Investment Management of Business Digital Innovations. Marketing and Management of Innovations. 2020. №1, pp. 95-109. DOI: http://doi.org/10.21272/mmi.2020.1-07.

170. TADVISER, 2020. Blockchain. | [Blokcheyn]. Retrieved 01.05.2020 from http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain)#.D0.9A.

D0.B8.D0.B1.D0.B5.D1.80.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D1.8C.

171. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *Accenture*. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (дата звернення: 23.09.2020).

172. The Global Risks Report 2020. *World Economic Forum.* URL:http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата звернення: 23.09.2020).

173. Vasylieva, T. A., Leonov, S. V., Kryvych, Ya. N. and Buriak, A. V. Bank 3.0 concept: global trends and implications. Financial and credit activity: problems of theory and practice. 2017. №1(22), pp. 4-10. DOI: https://doi.org/10.18371/fcaptp.v1i22.107714.

174. Vasylieva, T. A., Lieonov, S. V., Petrushenko, Yu. M. and Vorontsova, A. S. Investments in the system of lifelong education as an effective factor of socio-economic development. Financial and credit activity: problems of theory and practice. 2017. №2(23), pp. 426-436. DOI: DOI: https://doi.org/10.18371/fcaptp.v2i23.121202.

175. Ventana Systems, Inc. Vensim. Retrieved 01.05.2020 from http://vensim.com.

176. VOSviewer. Welcome to VOSviewer. Retrieved 01.05.2020 from https://www.vosviewer.com.

Монографія

Кузьменко Ольга Віталіївна,
Яровенко Ганна Миколаївна,
Криклій Олена Анатоліївна,
Гриценко Костянтин Григорович та інші

ТЕОРІЯ ТА ПРАКТИКА ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ КІБЕРПРОСТОРУ КРАЇНИ

Монографія
За загальною редакцією О. В. Кузьменко, Г.М. Яровенко

Відповідальний за випуск О. В. Кузьменко
Редактор _____
Комп'ютерне верстання _____

Підп. до друку , поз.
Формат 60х84/16. Ум. друк. арк. . Обл.-вид. арк. . Тираж пр. Зам. №
Собівартість вид. грн к.

Видавець і виготовлювач
ФОП Ширяєв Д.І.,
вул. Воскресенська, 14, м. Суми, 40000
Свідоцтво суб'єкта видавничої справи _____