УДК 004.3-185.4; 004.7-185.4, 330.4, 336; 336.01;
336.11; 336.741.28; 336.7
УКПП
№ держреєстрації 0121U109559
Інв. №

Міністерство освіти і науки України
Сумський державний університет (СумДУ)
40007, м. Суми, вул. Р.-Корсакова, 2; тел. 66-50-37
cyber@uabs.sumdu.edu.ua

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

НАЦІОНАЛЬНА БЕЗПЕКА ЧЕРЕЗ КОНВЕРГЕНЦІЮ СИСТЕМ ФІНАНСОВОГО МОНІТОРИНГУ ТА КІБЕРБЕЗПЕКИ: ІНТЕЛЕКТУАЛЬНЕ МОДЕЛЮВАННЯ МЕХАНІЗМІВ РЕГУЛЮВАННЯ ФІНАНСОВОГО РИНКУ

(остаточний)

Частина 2

2023

3 ФОРМУВАННЯ УПРАВЛІНСЬКИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФІНАНСОВОГО КІБЕРПРОСТОРУ НА МІКРО- ТА МАКРОРІВНІ

3.1 Концепція створення експертної алгоритмізованої системи ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи

3.1.1 Імітаційна модель діяльності інсайдера у банку

Інсайдери в банках - це особи чи групи, які спеціалізуються на використанні технологій для незаконного доступу до конфіденційної інформації фінансових установ. Вони використовують різноманітні методи атак, такі як фішинг, соціальний інжиніринг, вразливості програмного забезпечення та інші. Головною метою їхньої діяльності є отримання несанкціонованого доступу до банківської інформації, такої як реквізити клієнтів, фінансові та особисті дані. Кіберінсайдери можуть використовувати атаки для крадіжки грошей, використання крадених ідентифікаційних даних для шахрайства або навіть для викрадення конфіденційної інформації для подальших шантажів чи продажу на чорному ринку. Вони вкладають значні зусилля в те, щоб залишити сліди із свого діяння, щоб уникнути виявлення та відстеження з боку банківських служб безпеки. Для банків це становить серйозну загрозу, оскільки кіберінсайдери можуть завдати серйозної шкоди як фінансовій стійкості установи, так і довірі клієнтів. Щоб протидіяти таким загрозам, банки повинні постійно вдосконалювати свої системи кібербезпеки, моніторити підозрілі активності та надавати співробітникам і клієнтам інструменти для захисту від кібератак.

Створення імітаційної моделі для моделювання діяльності кіберінсайдера у банках може бути важливою стратегією для підвищення рівня кібербезпеки та підготовки фінансових установ до можливих кібератак. Ось кілька аргументів, які обгрунтовують необхідність такої імітаційної моделі:

1. Тестування заходів безпеки. Імітаційна модель надасть можливість випробувати та аналізувати ефективність систем безпеки банку в умовах симульованої кібератаки. Це дозволить виявити слабкі місця та ризики в існуючих заходах безпеки і підготувати відповідні заходи для їх подолання.

2. Навчання персоналу. Моделювання діяльності кіберінсайдера може бути використане для тренування персоналу банку в розпізнаванні та реагуванні на кіберзагрози. Це допоможе персоналу розвинути навички реагування на кібератаки в реальному часі та зменшити ймовірність людських помилок.

3. Оптимізація реакції на інциденти. Створення імітаційної моделі дозволяє банкам визначити ефективні процедури та стратегії для виявлення, аналізу та реагування на кіберінциденти. Це допоможе вдосконалити механізми реагування та скорочувати час відновлення після атаки.

4. Вдосконалення культури кібербезпеки. Регулярне моделювання кібератак сприяє формуванню культури кібербезпеки серед працівників банку. Це робиться шляхом своєчасного інформування та навчання персоналу щодо нових методів атак та заходів для їх запобігання.

5. Підвищення відповідальності. За допомогою імітаційної моделі банк може визначити основні загрози та визначити відповідальних осіб за виявлення та реагування на потенційні атаки.

6. Аналіз інноваційних рішень. Моделювання діяльності кіберінсайдера може служити площиною для випробування та впровадження нових інноваційних рішень в галузі кібербезпеки.

Усі ці аспекти підкреслюють важливість створення імітаційних моделей для ефективного вдосконалення заходів з кібербезпеки в банках та підготовки їх до реальних кіберзагроз.

Для побудови імітаційної моделі діяльності шахрая у відділі банку використаємо програмне забезпечення AnyLogic 8 PLE.

Основним елементом у імітаційній моделі виступає агент «swindler», який відповідає операції, яка потенційно може мати певні ознаки шахрайської операції. Опис характеристик агенту «swindler» наведений у таблиці 3.1.

Таблиця 3.1 – Характеристики агенту «swindler»

Назва	Опис	Тип даних	Початкове значення
fraud	Відповідає за розташування отримувача або відправника транзакції у «чорному списку». За замовчуванням значення false, при генерації об'єктів із заданою для експеримента ймовірністю може набути значення true.	boolean	false
sleep_acc	Відповідає за характеристику використання «сплячого рахунку». Значення за замовчуванням false, при генерації об'єктів із заданою ймовірністю може набути значення true.	boolean	false
tr_sum	Генерація можливого обсягу операції. Початкове значення дорівнює 100000, при створенні агентів із заданою ймовірністю може бути змінене.	double	100000
bank_ norm	Покажчик чи згенерований агент буде відповідати банківським нормативам чи ні. Початкове значення true, при створенні агентів із заданою ймовірністю може бути змінене.	boolean	true
insider	Змінна, що сигналізує про наявність шахрая-інсайдера у відділенні банку, діяльність якого впливає на дотримання часу обробки операції та може впливати на рух агентів по моделі. Значення за замовчуванням false, проте із заданою ймовірністю шахрай-інсайдер може «активізуватись» у системі.	boolean	false
insider_ delay	Змінна, яка відповідає за час прискорення обробки операції під впливом шахрая-інсайдера. Початкове значення 1, може змінюватись інтерактивно під впливом дослідника для оцінки різної інтенсивності впливу шахрая.	double	1
sec_pol	Змінна, що сигналізує чи операція відпадає під політики безпеки банку чи ні. Значення за замовчуванням false, при генерації об'єктів із заданою ймовірністю може набути значення true.	boolean	true

Графічне зображення змінних, що характеризують агента-операцію у системі зображено на рисунку 3.1.

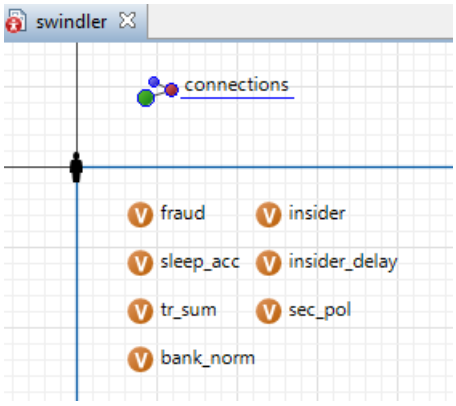


Рисунок 3.1 – Зображення змінних агенту «swindler»

Для характеристики поведінки шахрая-інсайдера при обробці операцій у відділенні банку потрібно змоделювати роботу відділення у нормальному режимі, після чого включити діяльність інсайдера. З метою спрощення в моделі не розглядаються деталі обробки операцій. Розглядається час здійснення операції та послідовність операцій.

Для реалізації поставлених задач було використано ряд інструментів панелей «Process Modeling Library», «System Dynamic», «Agent», «Analysis» та «Controls». Їх перелік з описом приведено у таблиці 3.2.

Таблиця 3.2 – Інструменти імітаційного моделювання

Елемент	Опис
source	Початковий елемент моделі, що відповідає за створення нових агентів та визначення їх характеристик
queue	Черга агентів. Представляє собою пул створених агентів-операцій, які чекають обробки системою
Delay	Елемент часової затримки. Відповідає за виділення часу на обробку операції в системі
SelectOutput	Розгалуження моделі з одним входом та двома виходами true чи false в залежності від виконання чи невиконання умови.
sink	Кінцевий елемент, що відповідає за знищення агентів. У моделі знищення агенту означає що операція була виконана або створенням звіту про підозрілість операції або у звичайному режимі.
timeMeasureStart	Елемент початку відліку часу для відслідковування часу перебування агенту в системі.
timeMeasureEnd	Елемент кінця відліку часу для відслідковування часу перебування агенту в системі.
Slider	Елемент керування, що дозволяє експериментатору в режимі реального часу маніпулювати елементами системи.
Dynamic Variable	Динамічна змінна, яка в ході виконання моделі може змінювати свій стан.
Time Plot	Часовий графік для візуалізації результатів моделювання
Connector	Лінія-поєднувач елементів у системі

Визначивши всі необхідні інструменти була створена імітаційна модель діяльності шахрая-інсайдера у банку (рисунок 3.2).

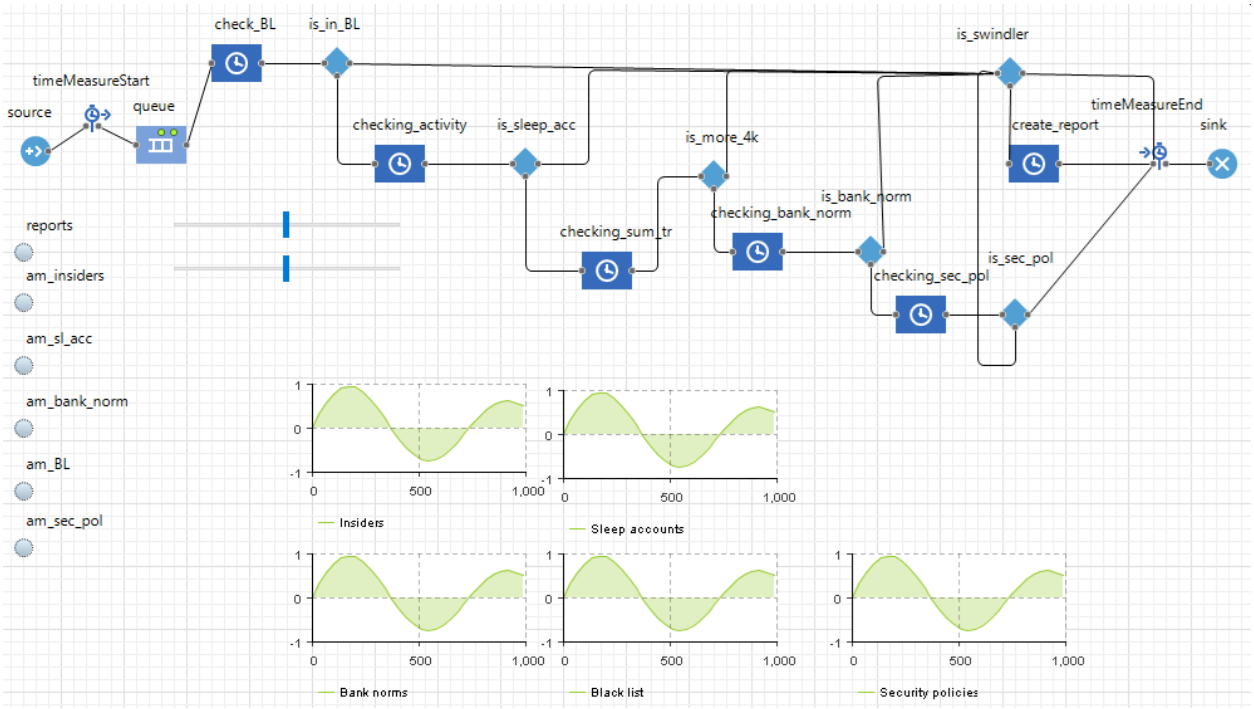


Рисунок 3.2 – Імітаційна модель діяльності шахрая-інсайдера у банку

Опис елементів моделі наведено у таблиці 3.3.

Таблиця 3.3 – Характеристика елементів моделі діяльності шахрая-інсайдера у банку

Ім’я	Тип	Призначення
source	source	Створення агентів
timeMeasureStart	timeMeasureStart	Початок відліку часу для агента у системі
queue	queue	Черга агентів
check_BL	Delay	Перевірка чи власник операції знаходиться у чорному списку
checking_activity	Delay	Перевірка активності по рахунку з метою виявлення застосування «сплячих рахунків»
checking_sum_tr	Delay	Перевірка на допустимість лімітів по операції
checking_bank_norm	Delay	Перевірка на відповідність банківським нормам
checking_sec_pol	Delay	Перевірка на відповідність політикам безпеки банку
create_report	Delay	Створення звіту про підозрілу операцію
is_in_BL	SelectOutput	Перенаправлення операції або на подальшу перевірку або на створення звіту про підозрілу операцію
is_sleep_acc	SelectOutput	
is_more_4k	SelectOutput	
is_bank_norm	SelectOutput	
is_sec_pol	SelectOutput	
is_swindler	SelectOutput	Імітація діяльності шахрая-інсайдера, який може відступити від правил і норм та допустити операцію до виконання

Ім’я	Тип	Призначення
timeMeasureEnd	timeMeasureEnd	Зупинка відліку часу для агента в системі
sink	sink	Знищення агентів
reports	Dynamic Variable	Підрахунок кількості створених звітів про підозрілі операції
am_insiders	Dynamic Variable	Підрахунок кількості операцій на які вплинув шахрай-інсайдер
am_sl_acc	Dynamic Variable	Підрахунок кількості операцій зі «сплячим рахунком»
am_bank_norm	Dynamic Variable	Підрахунок кількості операцій з порушенням банківських норм
am_BL	Dynamic Variable	Підрахунок кількості операцій пов’язаних з особами у чорному списку
am_sec_pol	Dynamic Variable	Підрахунок кількості операцій, при здійсненні яких будуть порушуватись правила безпеки банку
plot_insiders	Time Plot	Графік для відображення кількості операцій під впливом інсайдера-шахрая
plot_bank_norm	Time Plot	Графік для відображення кількості операцій з порушенням банківських норм
plot_sleep_acc	Time Plot	Графік для відображення кількості операцій зі «сплячим рахунком»
plot_BL	Time Plot	Графік для відображення кількості операцій пов’язаних з особами у чорному списку
plot_sec_pol	Time Plot	Графік для відображення кількості операцій, при здійсненні яких будуть порушуватись правила безпеки банку
slider_insider_influence	Slider	Керування ступенем впливу шахрая-інсайдера на проведення операції
slider_insider_influence_prob	Slider	Керування ймовірністю впливу шахрая-інсайдера на операцію

Розглядаючи детально імітаційну модель, звернемо увагу на властивості її елементів.

Елемент «source» відповідає за створення агентів та відправлення їх у модель. Відповідно до наших умов, налаштовуємо властивості «Arrival rate» = 1, що означає що буде створюватись один агент у секунду модельного часу (рисунок 3.3). Для проведення імітації обмежимось 1000 створених агентів, встановивши значення «Maximum number of arrivals» = 1000. У полі «On exit» блоку властивостей «Actions» встановлюється значення події, яка відбувається коли агент покидає елемент. Відповідно, наведений на рисунку 3.3 програмний код генерує властивості агента-події коли він залишає блок «source».

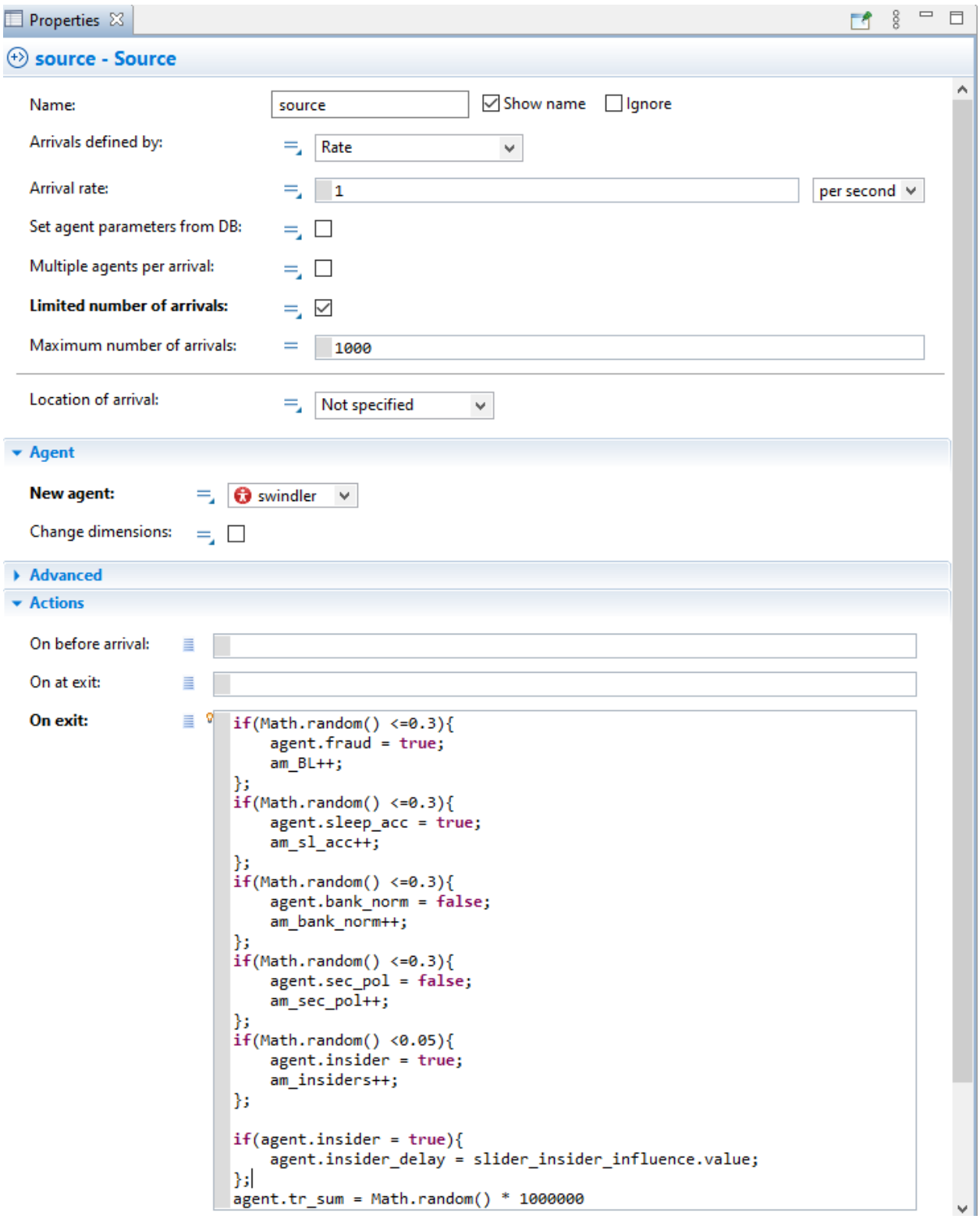


Рисунок 3.3 – Властивості елементу «source»

У пропонованій імітаційній моделі значення властивостей «fraud», «sleep_acc», «bank_norm» та «sec_pol» змінюється від початкового з ймовірністю 0.3. Одночасно значення відповідних змінних «am_BL», «am_sl_acc»,

«am_bank_norm» та «am_sec_pol» інкрементується, якщо відповідна умова при створенні агента виконується.

Ймовірність обробки операції шахраєм-інсайдером очікується в розмірі 0.05. Також встановлюємо значення впливу шахрая-інсайдера з прив'язкою до значення елементу «slider_influence_value» щоб мати змогу інтерактивно змінювати параметри впливу під час виконання моделі.

Значення параметру «tr_sum» випадковим чином встановлюємо від 0 до 1000000 для кожного новоствореного агента.

Далі агенти потрапляють послідовно до блоків «timeMeasureStart» та «queue». Блок «timeMeasureStart» прикріплює часову мітку входу агента у модель, яку потім зчитає блоку «timeMeasureEnd». Блок «queue» є технічним та являє собою пул на 100 місць для агентів-операцій, які чекають перевірки у моделі.

Далі агент потрапляє у блок «check_BL» типу «Delay». В ньому агент затримається на певний час, який визначається за допомогою функції triangular() у полі властивостей «Delay time». Функція triangular(min, max, mode) у AnyLogic 8 PLE повертає значення обмеженого неперервного трьохкутового розподілу, де межі – параметри min та max, а mode – найбільш вірогідне значення. У побудованій моделі функція triangular() набуває вигляду triangular(0.5 * agent.insider_delay, 1.5 * agent.insider_delay, 1 * agent.insider_delay), де «agent.insider_delay» – властивість агента, на розмір якої може бути пришвидшений розгляд операції, оскільки шахрай-інсайдер в реальності не буде проводити всі необхідні за інструкцією перевірки, оскільки заздалегідь відомо що цю операцію необхідно пропустити (рисунок 3.4). Властивість «Capacity» визначає кількість операцій які відділення банку може проводити одночасно. Для імітаційної моделі встановлюється значення 3, оскільки в реальності кількість співробітників які проводять перевірку значно обмежена.

Інші блоки типу «Delay» у імітаційній моделі «checking_activity», «checking_sum_tr», «checking_bank_norm» та «checking_sec_pol» мають такі ж самі властивості як і елемент «check_BL».

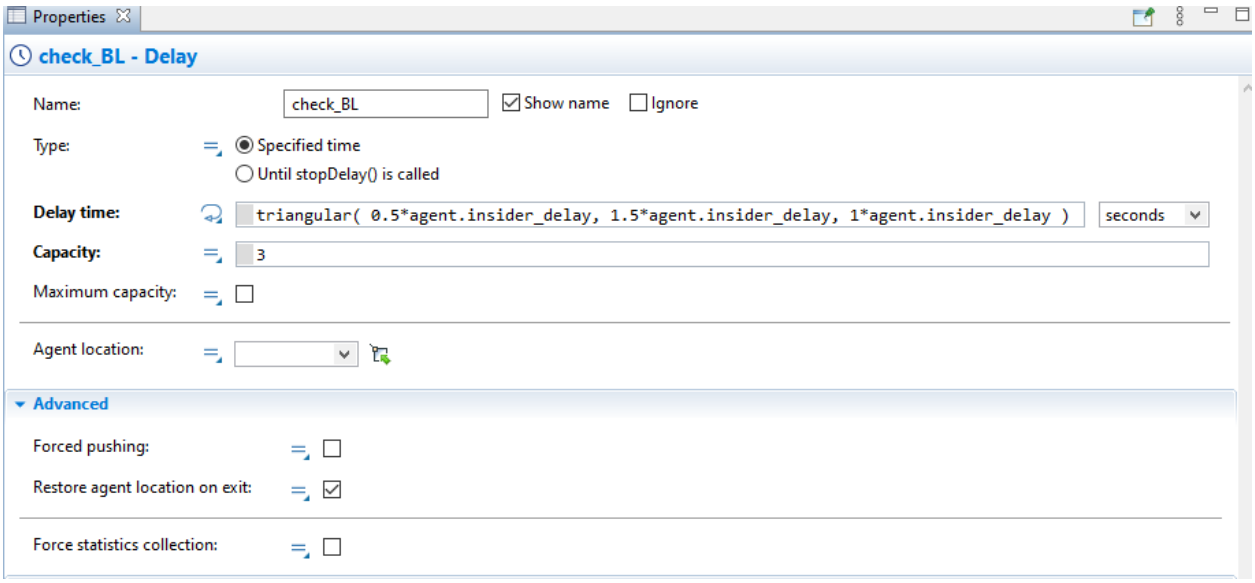


Рисунок 3.4 – Властивості елементу «check_BL»

На наступному кроці агент потрапляє до елементу «is_in_BL», де перевіряється умова agent.fraud == true, тобто чи агент відповідає операції, пов’язані особи з якою знаходяться у чорному списку (рисунок 3.5).

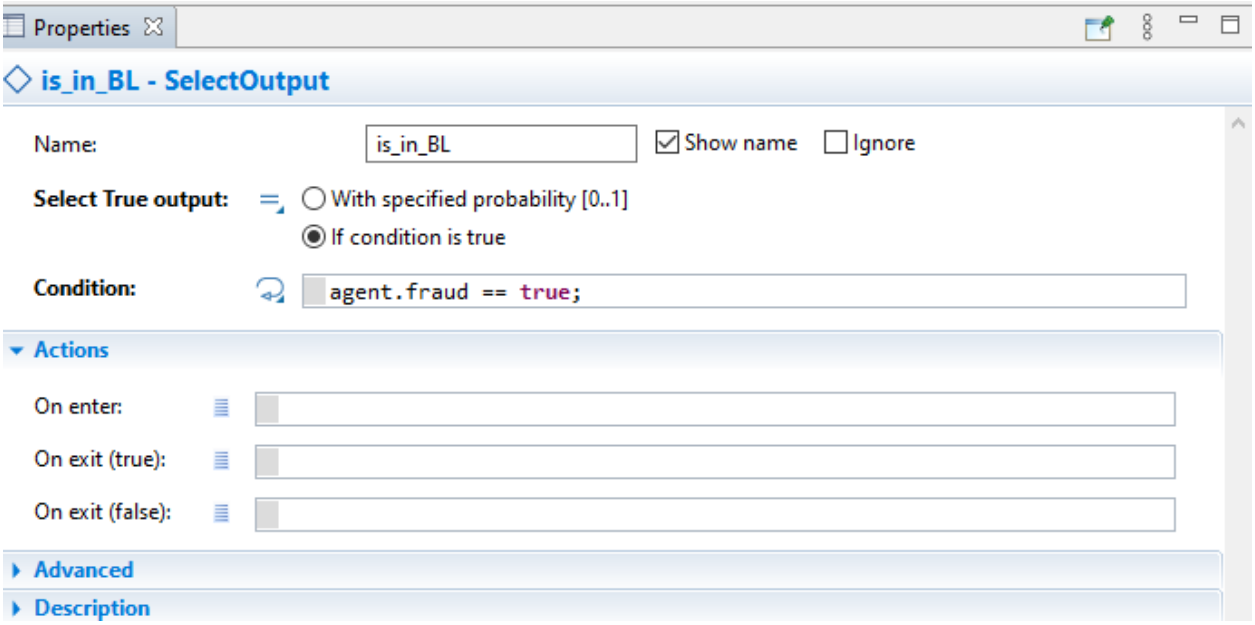


Рисунок 3.5 – Властивості блоку «is_in_BL»

Відповідно, якщо умова виконується, то агент направляється до блоку «is_swindler», який відповідає за діяльність шахрая-інсайдера у банку. Якщо ж умова не виконується, то агент переходить до блоку «checking_activity», який відповідає за перевірку чи є даний агент операцією з «сплячим рахунком».

За таким принципом відбуваються перевірки у елементах «checking_sum_tr», «checking_bank_norm», «checking_sec_pol». У елементах «is_sleep_acc», «is_more_4k», «is_bank_norm», «is_sec_pol» здійснюються перевірки умов «agent.sleep_acc == true;», «agent.tr_sum >=400000;», «agent.bank_norm == false;», «agent.sec_pol == true;». Якщо умови виконуються, то агент направляється у блок «is_swindler», а якщо ні – здійснюються поступові перевірки і агент переходить у блок «timeMeasureEnd» для визначення часу перебування агента у системі. Після цього агент направляється у блок «sink» де знищується. Властивості блоків «is_sleep_acc», «is_more_4k», «is_bank_norm», «is_sec_pol» зображені на рисунках 3.6-3.9.

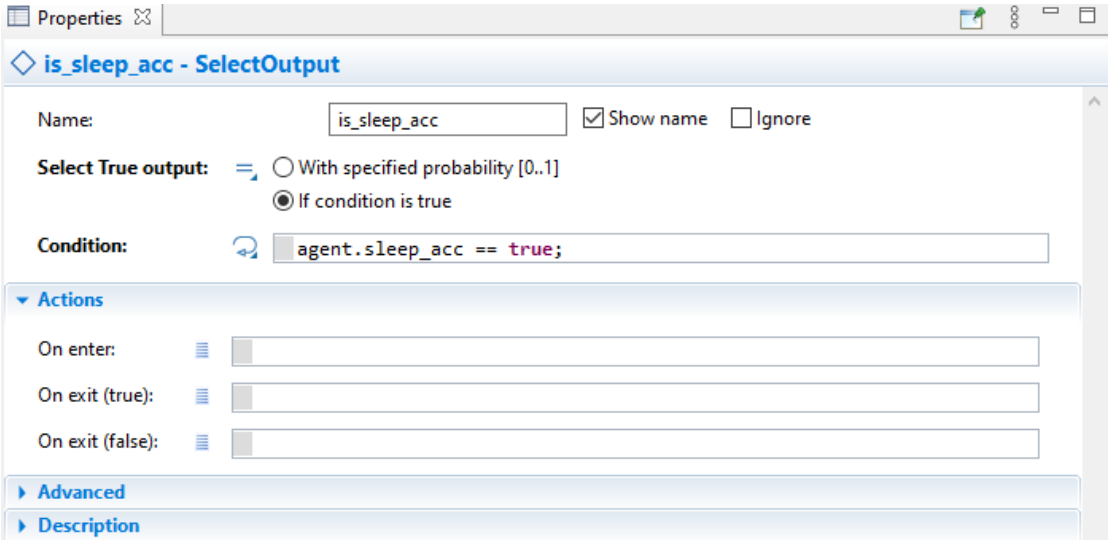


Рисунок 3.6 – Властивості блоку «is_sleep_acc»

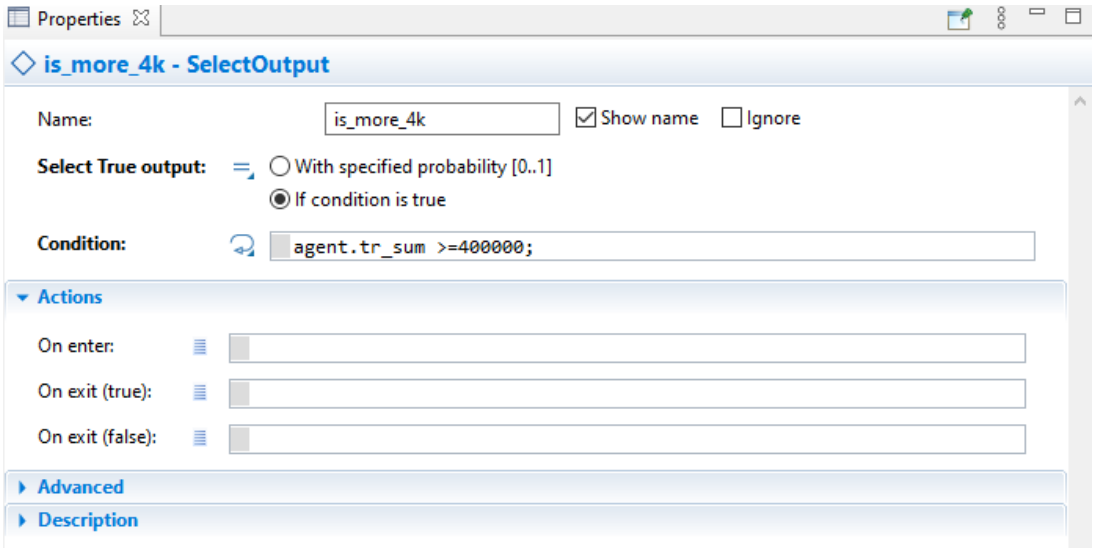


Рисунок 3.7 – Властивості блоку «is_more_4k»

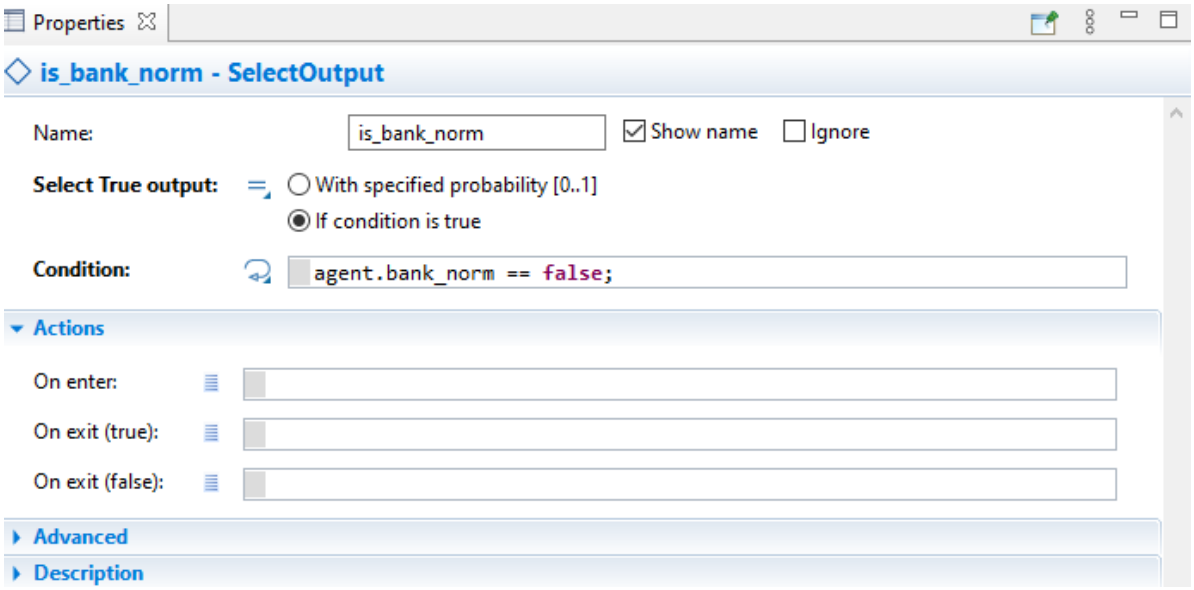


Рисунок 3.8 – Властивості блоку «is_bank_norm»

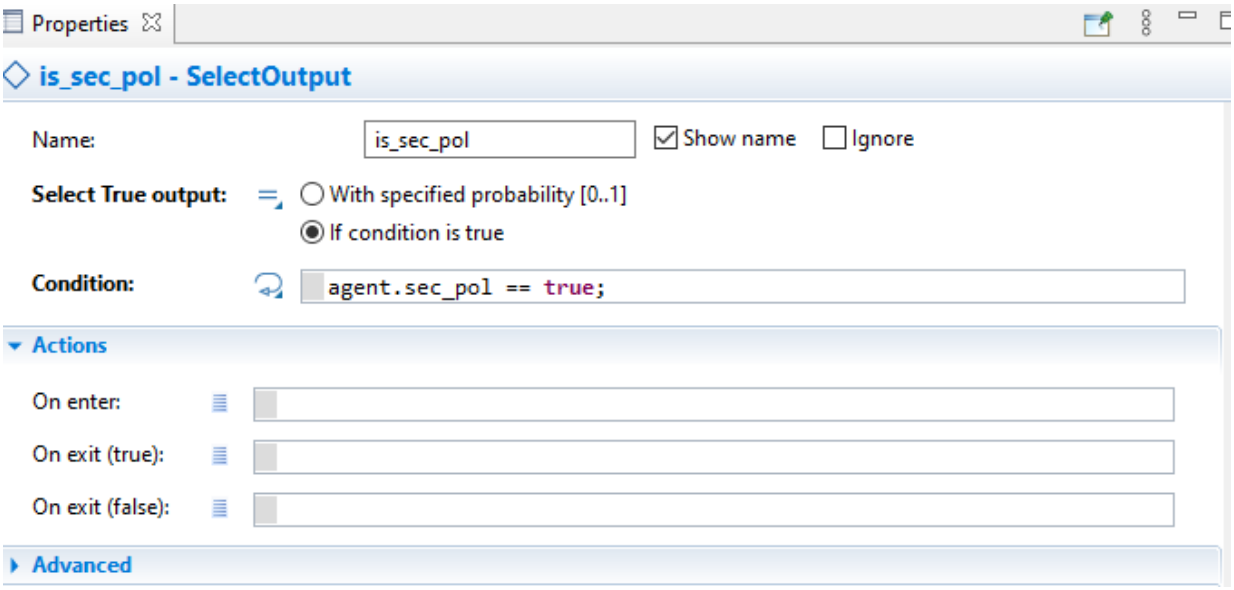


Рисунок 3.9 – Властивості блоку «is_sec_pol»

Якщо була виявлена хоча б одна із підозрілих ознак у агента-операції як така, про яку потрібно скласти звіт, такі агенти потрапляють у блок «is_swindler», який відображає роботу шахрая в банку та може за власним злим умислом не створювати звіти з роботи. Його основна властивість – із заданою ймовірністю пропускати агентів та не створювати по них звіти про підозрілість (рисунок 3.10). Дана властивість може коригуватись експериментатором в ході виконанням моделі.

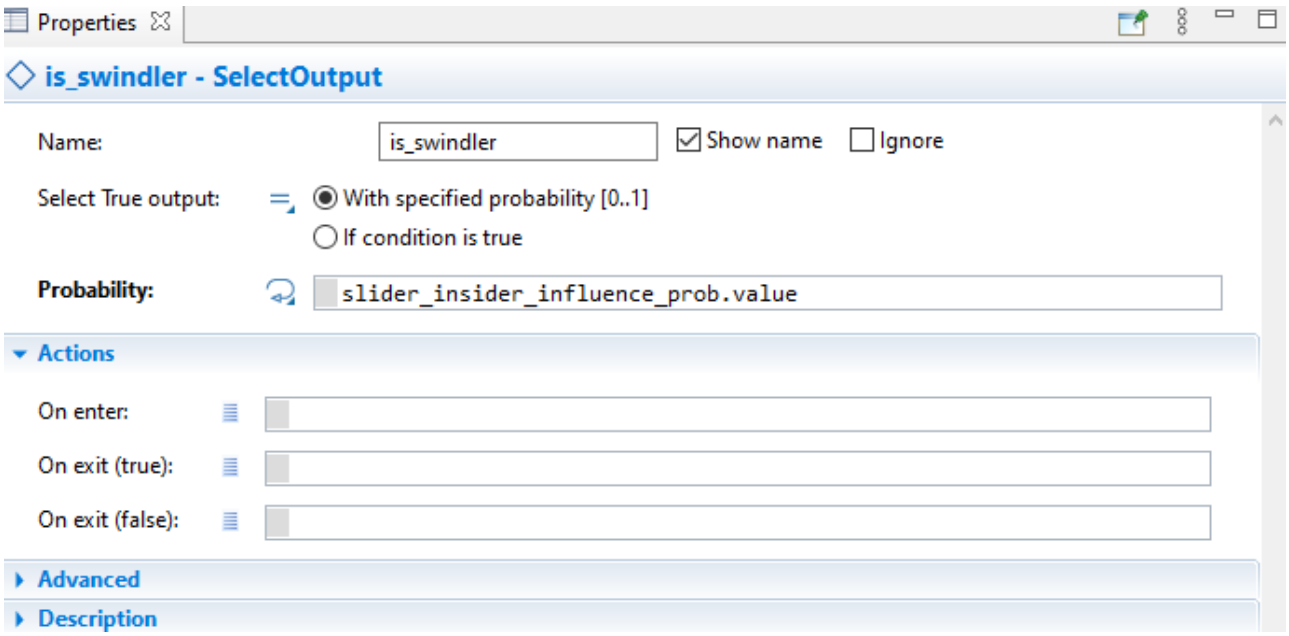


Рисунок 3.10 – Властивості елементу «is_swindler»

Після блоку «is_swindler» агенти потрапляють або у блок «create_report» або у блок «timeMeasureEnd». Блок «create_report» являє собою часову затримку на створення звіту про підозрілість операції. Властивість «On enter» панелі «Actions» (рисунок 3.11) програмно підраховує кількість створених звітів і зберігає їх у змінну.

Після цього блоку агенти потрапляють у блок «timeMeasureEnd» де считується часова мітка та у блок «sink» де агент знищується.

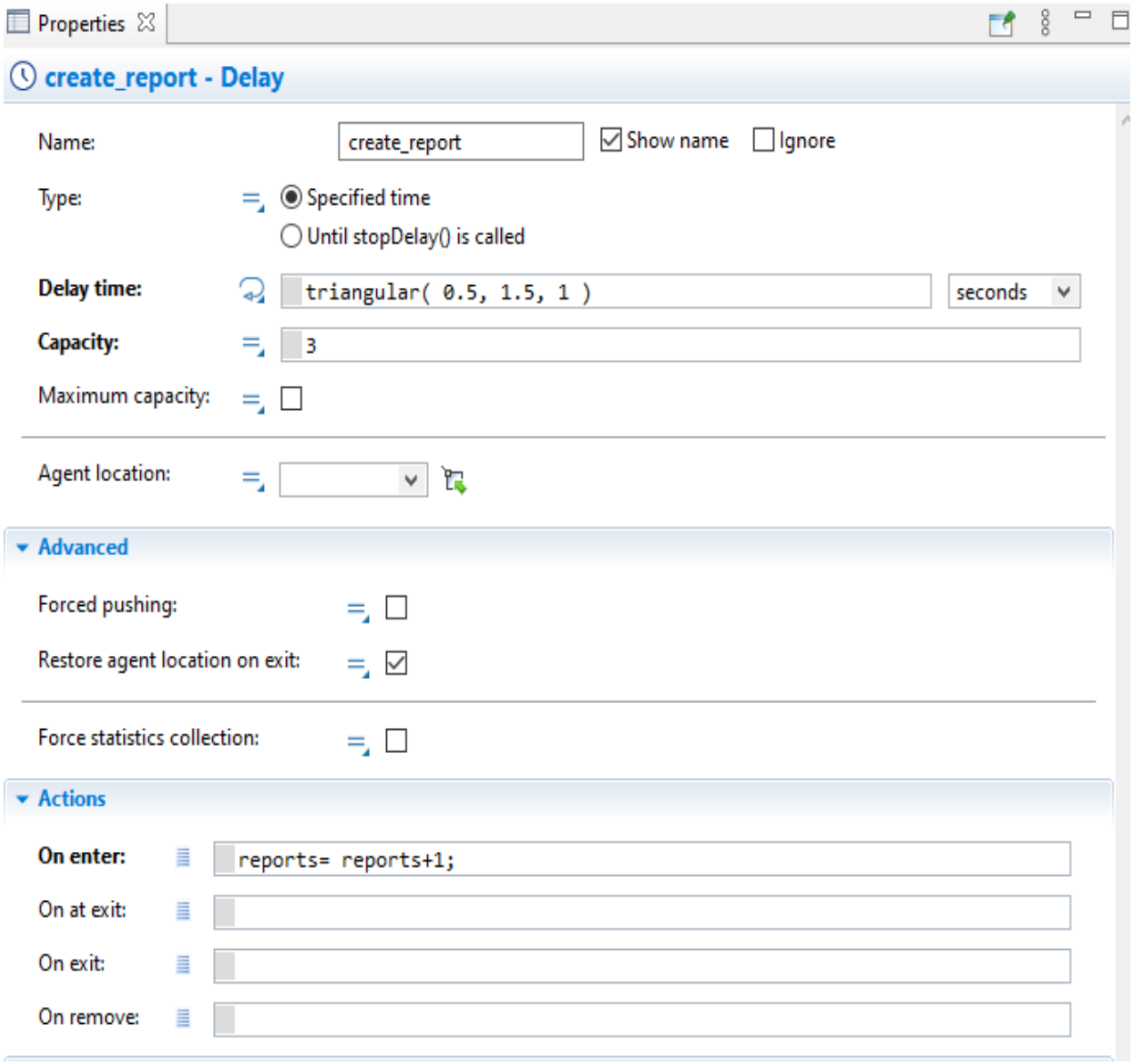


Рисунок 3.11 – Властивості елементу «create_report»

Наступним кроком буде проведення імітаційного експерименту для аналізу впливу діяльності шахрая у банку.

Для початку проведемо імітацію діяльності відділення без впливу шахрая (рисунок 3.12).

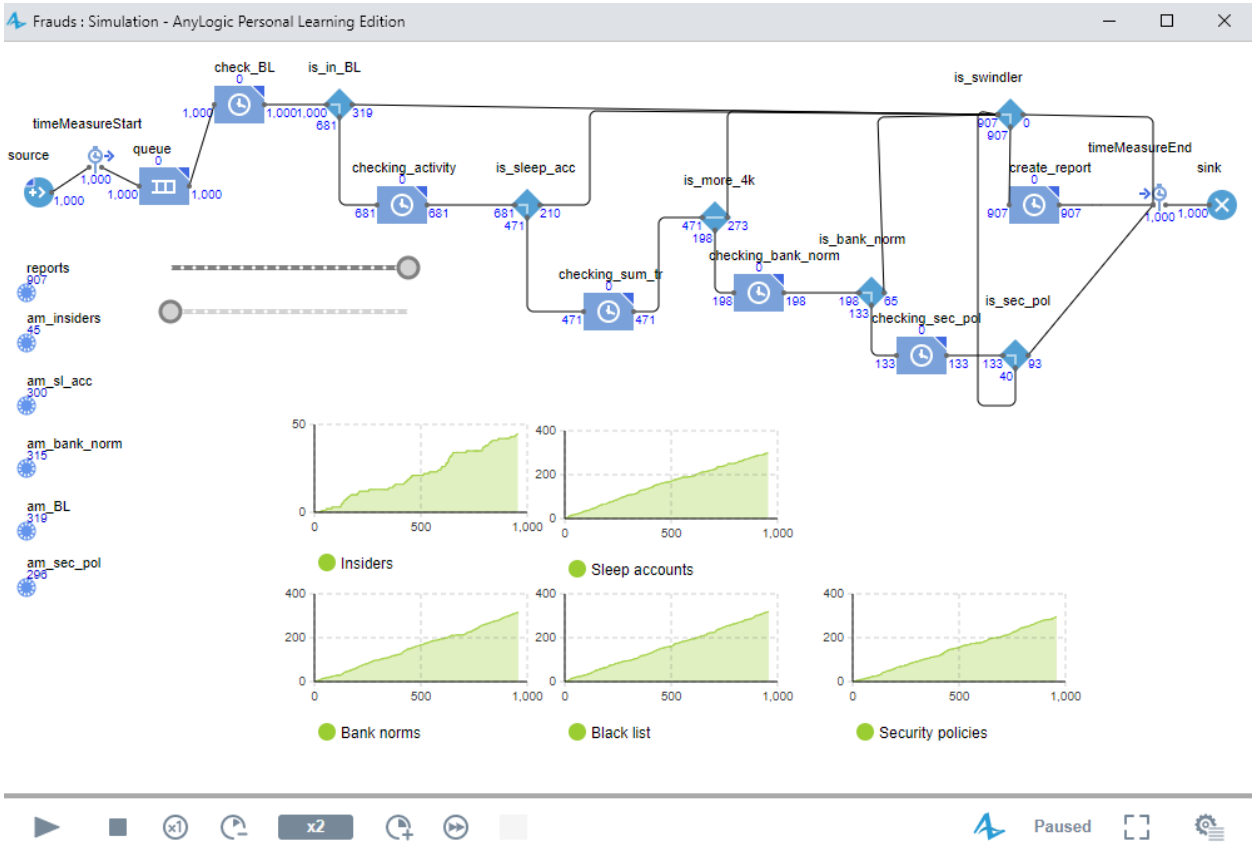


Рисунок 3.12 – Результат роботи імітаційної моделі без врахування впливу шахрая-інсайдера

Відповідно до рисунку 3.12, було створено 1000 агентів, серед яких 300 мали характеристику «сплячий рахунок», 315 – характеристику порушення банківських нормативів, 319 – пов’язані з операцією особи були у «чорному списку» та 296 порушували політики безпеки. Оскільки операція може поєднувати декілька характеристик, було створено 907 звітів про підозрілі операції.

Відповідно до часових вимірів (рисунок 3.13), то мінімальний час обробки операції склав 1,213 одиниць модельного часу (секунд), максимальний час – 6,821 одиниць модельного часу (секунд), а в середній час обробки склав 3,433 одиниць модельного часу (секунд). Затрачений час на обробку всіх агентів – 3442,88 одиниць модельного часу (секунд).

timeMeasureEnd

```
root.timeMeasureEnd: TimeMeasureEnd
  in:           1,000
  out:          1,000
Time distribution:
Count    1,000
Mean     3.443
Min      1.213
Max      6.821
Deviation        1.256
Mean confidence 0.078
Sum      3,442.88
From     To       PDF(hits)       CDF(cum hits)
1        1.4      3               3
1.4      1.8      66              69
1.8      2.2      150             219
2.2      2.6      103             322
2.6      3        84              406
3        3.4      109             515
3.4      3.8      94              609
3.8      4.2      101             710
4.2      4.6      93              803
4.6      5        66              869
5        5.4      55              924
5.4      5.8      41              965
5.8      6.2      20              985
6.2      6.6      12              997
6.6      7        3               1,000
```

Рисунок 3.13 – Результати часових замірів роботи моделі (блок «timeMeasureEnd»)

У даному імітаційному експерименті не враховувався вплив шахрая інсайдера, тобто властивості agent.insider_delay та slider_insider_influence_prob.value були рівні 0.

Для відображення діяльності шахрая-інсайдера, змінимо параметри за допомогою слайдерів та встановимо agent.insider_delay = 0,75 та slider_insider_influence_prob.value = 0,05, що дорівнює низькій активності шахрая-інсайдера (рисунок 3.14). Результати експерименту приведені на рисунку 3.15.

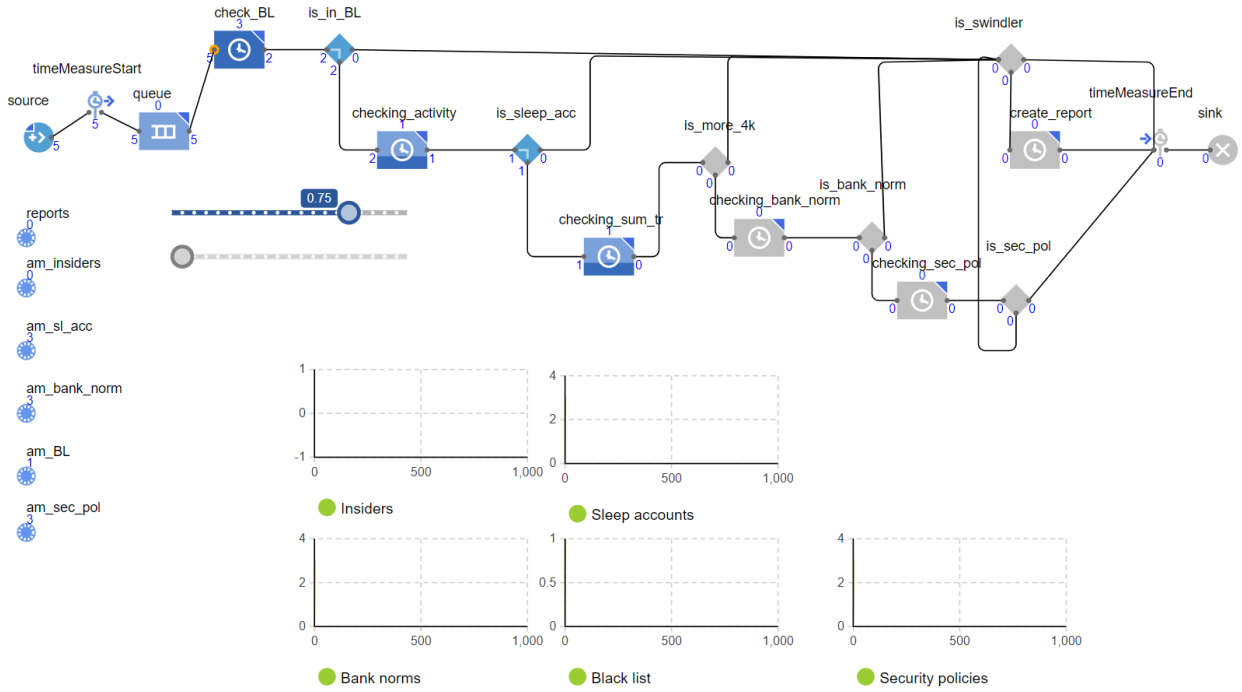


Рисунок 3.14 – Інтерактивне налаштування параметрів моделі

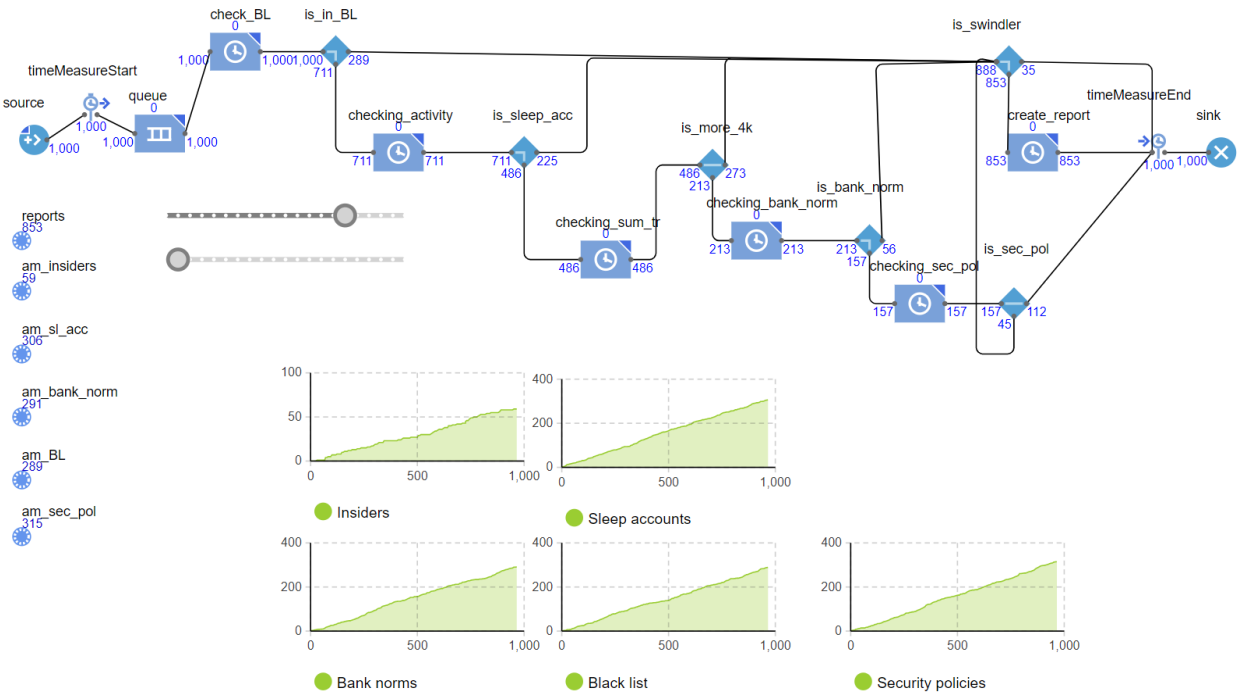
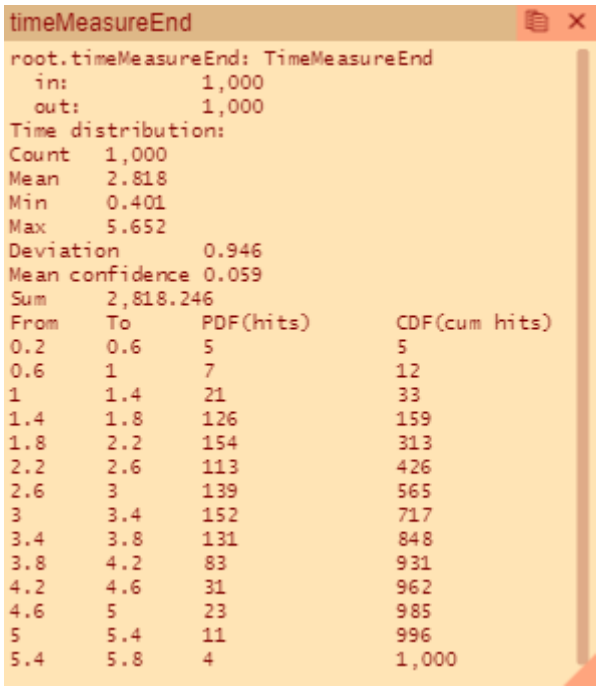


Рисунок 3.15 – Результати імітаційної моделі при низькій активності шахрая-інсайдера

Відповідно до отриманих результатів (рисунок 3.15), 306 агентів мали характеристику «сплячий рахунок», 291 – характеристику порушення

банківських нормативів, 289 – пов’язані з операцією особи були у «чорному списку» та 315 порушували політики безпеки. Біля блоку «is_swindler» відображено, що на вході було 888 агентів, тобто таких, щодо яких потрібно було складати звіт про підозрілість операції. На виході True – 35 агентів, що відповідає кількості операцій які шахрай-інсайдер помітив як не підозрілі та пропустив на вихід. І тільки 853 агенти пройшло через вихід False, тобто було складено 853 звіти про підозрілі операції.

Відповідно до часових замірів (рисунок 3.16), то в такому разі мінімальний час обробки операції знизився з 1,213 до 0,401 одиниць модельного часу (секунд), максимальний час – з 6,821 до 5,652 одиниць модельного часу (секунд), а в середньому, час оброки під впливом шахрая-інсайдера знизився на 0,615 одиниць модельного часу (секунд). Загальний час обробки операцій склав 2818,246 одиниць модельного часу (секунд).


timeMeasureEnd

root.timeMeasureEnd: TimeMeasureEnd
in: 1,000
out: 1,000
Time distribution:
Count 1,000
Mean 2.818
Min 0.401
Max 5.652
Deviation 0.946
Mean confidence 0.059
Sum 2,818.246

From	To	PDF(hits)	CDF(cum hits)
0.2	0.6	5	5
0.6	1	7	12
1	1.4	21	33
1.4	1.8	126	159
1.8	2.2	154	313
2.2	2.6	113	426
2.6	3	139	565
3	3.4	152	717
3.4	3.8	131	848
3.8	4.2	83	931
4.2	4.6	31	962
4.6	5	23	985
5	5.4	11	996
5.4	5.8	4	1,000

Рисунок 3.16 – Результати часових замірів роботи моделі з низькою активністю шахрая-інсайдера (блок «timeMeasureEnd»)

Третім експериментом проаналізуємо високоактивну поведінку шахрая-інсайдера. Для цього встановимо agent.insider_delay = 0,5 та

slider_insider_influence_prob.value = 0,15. Результати моделювання зображені на рисунку 3.17.

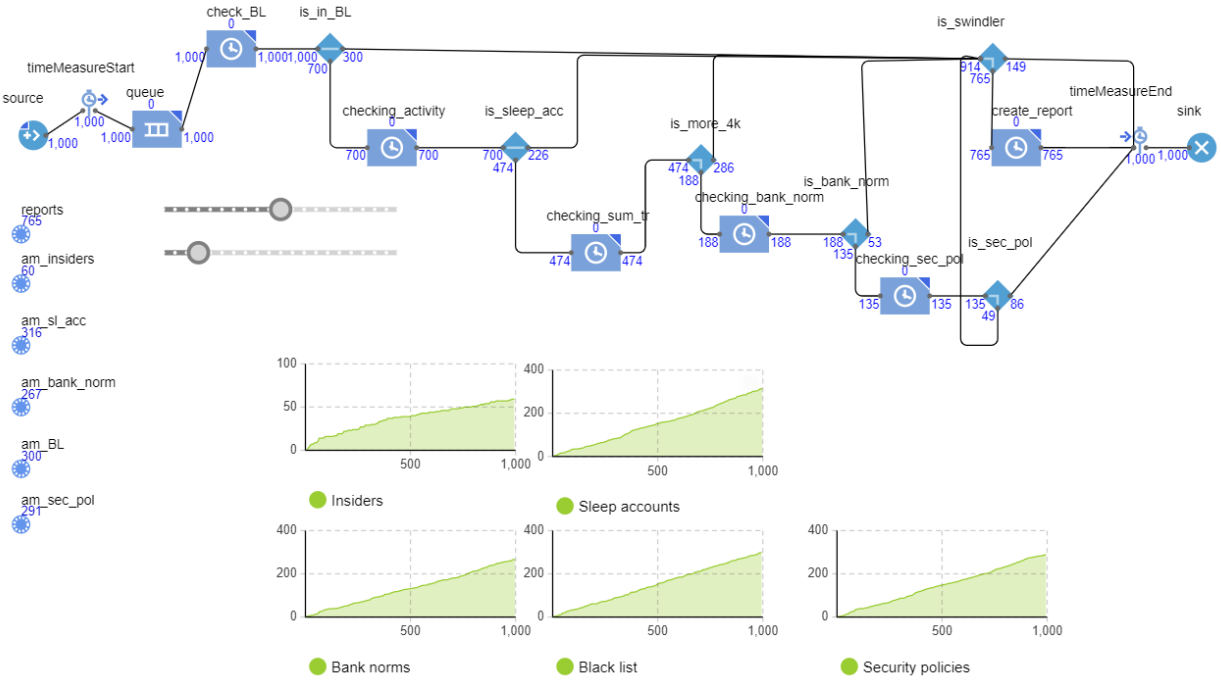


Рисунок 3.17 – Результати імітаційної моделі при високій активності шахрая-інсайдера

Відповідно до результатів моделювання високої активності шахрая-інсайдера (рисунок 3.17), 316 агентів мали характеристику «сплячий рахунок», 267 – характеристику порушення банківських нормативів, 300 – пов’язані з операцією особи були у «чорному списку» та 291 порушували політики безпеки.

149 операцій, які мають ознаки підозрілості шахрай-інсайдер пропустив повз блок «create_report», і тільки по 765 операціях було складено звіти.

Відповідно до часових результатів (рисунок 3.18), мінімальний час здійснення операції знизився до 0,272 одиниць модельного часу (секунд), максимальний – до 4,87 одиниць модельного часу (секунд). Середній час обробки операції склав 2,046 одиниць модельного часу, що на 1,397 та 0,772 одиниці модельного часу (секунд) менше за результати моделі при відсутності інсайдера та при його низькій активності відповідно. Загальний час обробки операцій склав 2045,999 одиниць модельного часу.

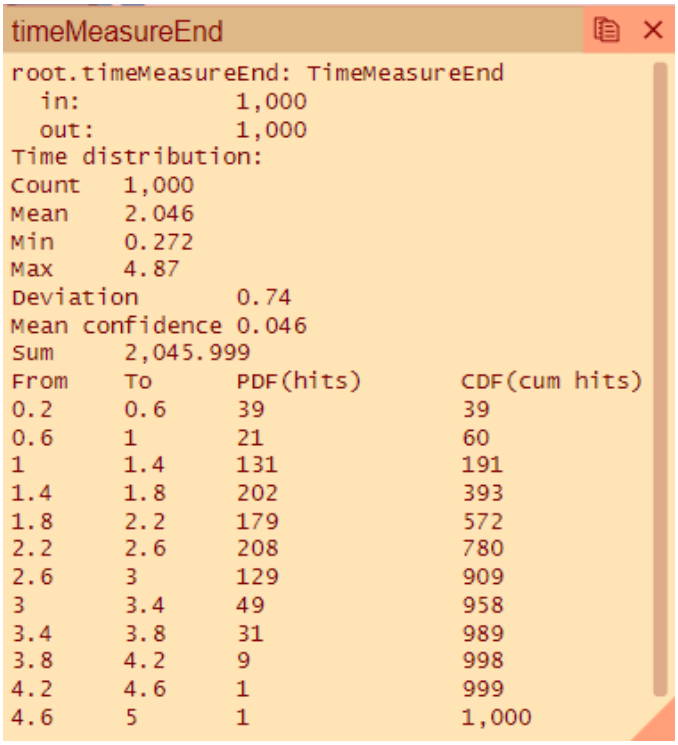


Рисунок 3.18 – Результати часових замірів роботи моделі з високою активністю шахрая-інсайдера (блок «timeMeasureEnd»)

Результати трьох експериментів відображені у таблиці 3.4.

Таблиця 3.4 – Порівняння результатів експериментів

Активність інсайдера	Відсутня	Низька	Висока
Кількість пропущених інсайдером агентів	0	35	149
Мінімальний час обробки агента	1,213	0,401	0,272
Максимальний час обробки агента	6,821	5,652	4,87
Середній час обробки агента	3,443	2,818	2,046
Загальний час обробки агента	3442,9	2818,2	2046

3.1.2 Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банку

Інсайдери-кібершахраї в банках використовують різні тактики та демонструють певну поведінку для здійснення своєї незаконної діяльності. Розуміння цих ключових аспектів може допомогти окремим особам і організаціям краще захистити себе від кіберзагроз.

Основна небезпека кібершахраїв, які діють як інсайдери в банку, полягає в їх потенціалі використовувати свій привілейований доступ і знання внутрішніх

систем і процесів банку. Інсайдерські загрози можуть становити значні ризики для безпеки та цілісності фінансових установ. Серед ключових загроз можуть бути: порушення даних і крадіжка; неавторизований доступ до внутрішньої системи та конфіденційних даних клієнтів, фінансових записів та іншої інформації; крадіжка даних; фінансове шахрайство; інсайдерська торгівля; саботаж і порушення; пошкодження даних; відмивання грошей; зловживання обліковими даними; соціальна інженерія та схеми шахрайства та ін. для того, щоб пом'якшити вплив негативних наслідків, пов'язаних з інсайдерськими загрозами, банкам необхідно запровадити надійні заходи кібербезпеки, включаючи контроль доступу, системи моніторингу та програми навчання співробітників. Регулярні аудити, репутація та культура обізнаності про безпеку також важливі для ефективного виявлення та запобігання внутрішнім загрозам.

В контексті поставленої мети даної роботи необхідно змоделювати імовірну поведінку інасайдерів-кібершахраїв у банку. Оскільки все, що має відношення до оцінки поведінкових аспектів людської діяльності носить більшою мірою суб'єктивний характер, основною складністю у проведенні подібних досліджень є підбір вхідних параметрів для цього. Передбачити стовідсотково як себе поведе людина в тій чи іншій ситуації, зокрема, інсайдер-кібершахрай банку не можливо так, як її поведінка обумовлюється рядом ендогенних та екзогенних кількісних та якісних факторів, вплив яких дуже складно проаналізувати. Враховуючи характер потенційних шахрайських дій інсайдера-кібершахрая банку, в якості масиву вхідних змінних, які дозволять оцінити його можливу поведінку, запропоновано використовувати можливі комбінації пошукових запитів в пошуковій системі Google. Всього в якості основи формування вхідного масиву даних для представленого дослідження сформовано два списки пошукових запитів: список запитів характеристики кібератак (таблиця 3.5) та список запитів, що характеризують рівень зменшення довіри до фінансових установ (таблиця 3.6).

Таблиця 3.5 – Вхідний масив даних, який включає список запитів характеристики кібератак

Ум. позн.	Пошуковий запит (укр.)	Пошуковий запит (англ.)
var1	Номер кіберполіції	Cyber police number
var2	Номер поліції	Police number
var3	Що робити, коли тебе зламали	What to do when you are hacked
var4	Перші дії при кібератаці	How to respond to a cyber attack
var5	Як посилити захист комп'ютера	How to protect your computer
var6	Як не допустити злому персональних даних (сайту, соціальних мереж)	How to prevent hacking
var7	Найпоширеніші кібератаки	The most common cyber attacks
var8	Як виявити кібератаку	Detection of a cyber attack
var9	Як захистити себе від кібератак	How to protect yourself from cyber attacks
var10	Як зрозуміти, що комп'ютер (телефон) зламали	How to find that phone is hacked

Таблиця 3.6 – Вхідний масив даних, який включає список запитів, що характеризують рівень зменшення довіри до фінансових установ

Ум. позн.	Пошуковий запит (укр.)	Пошуковий запит (англ.)
var11	Як заблокувати транзакцію	How to block a transaction
var12	Як заблокувати банківську карту	How to block a bank card
var13	Як змінити пароль на банківській картці	How to change password of bank card
var14	Як зменшити ліміт по банківській картці	How to reduce the credit limit
var15	Як зменшити ліміт розрахунків в інтернеті	Management of online payments
var16	Який банк найбільш захищений (в Інтернеті)	Which bank is the most secure online
var17	Рейтинг надійних банків (або рейтинг найбільш кіберстійких банків)	The most reliable banks
var18	Номер підтримки банку (або номер кол-центру банку)	Bank call center number
var19	Як змінити обслуговуючий банк (як перевести виплату зарплати з одного банку на інший)	How to change the bank
var20	Чорний список користувачів	Black list of customers

Засобами внутрішньої надбудови пошукової системи Google, Google Trends [282], отримано результати частоти звернень користувачів мережі Інтернет за представленими щотижневими пошуковими запитами протягом останніх п'яти років з 2018 р. до 2023 р. Всі пошукові запити досліджувались для всього світу, тому було прийнято рішення задавати їх в Google Trends англійською мовою. Проаналізуємо частоту отриманих результатів за сформованими пошуковими запитами за допомогою графічного представлення.

На рисунку 3.19 представлено динаміку запитів «Cyber police number», «Police number» та «What to do when you are hacked».

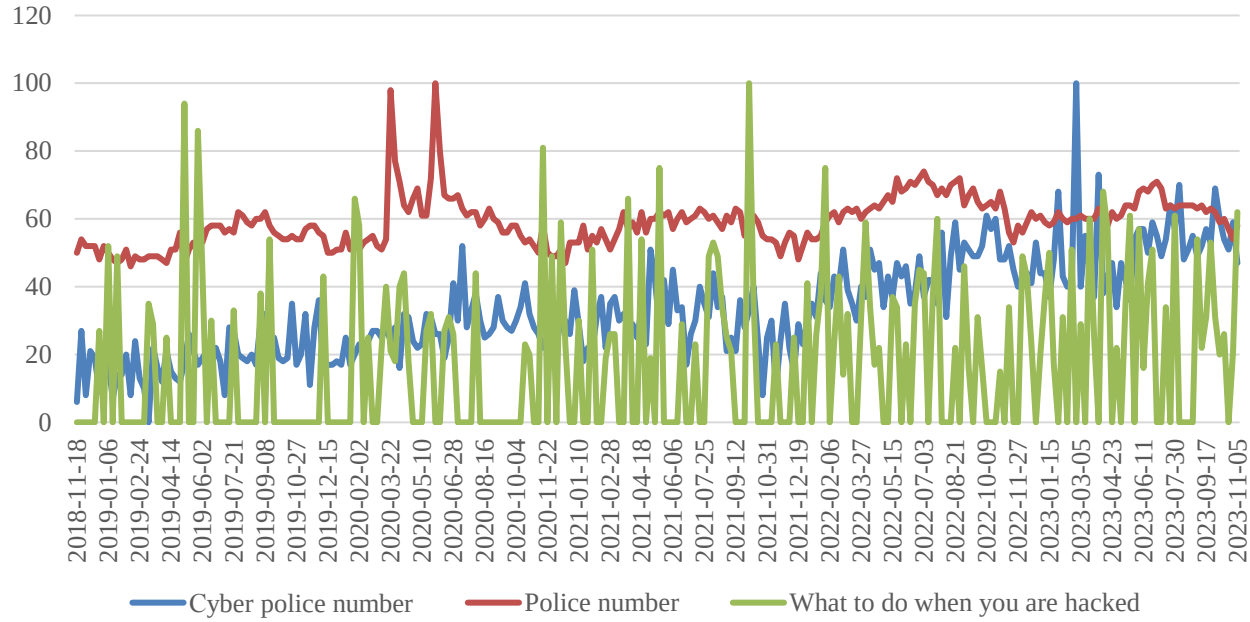


Рисунок 3.19 – Динаміка запитів «Cyber police number», «Police number» та «What to do when you are hacked» протягом 2018-2023 рр.

Джерело: складено на основі [247]

З огляду на представлений графік запити «Cyber police number» та «Police number» не втрачали популярності протягом всього досліджуваного періоду. Варто зазначити, що запит «Cyber police number» продовжує набирати популярності (на рис. 3.19 це підтверджується висхідним характером графіку), оскільки, починаючи із кінця 2022 року, він вперше за п’ять років перевищив за популярністю запит «Police number» і досягнув максимального значення (100 запитів на тиждень) в кінці лютого 2023 року. Це підтверджує актуалізацію проблему поширення кібершахрайств та потребу в усуненні їх наслідків. Щодо результатів для третього пошукового запиту, «What to do when you are hacked», то характер його динаміки носить стрибкоподібний характер і проте варто зазначити, що частота подібного запиту у світі є високою (близько 100 запитів на тиждень), що також підтверджує потребу населення в усуненні негативних наслідків кібератак власними зусиллями.

На наступному графіку (рис. 3.20) представлено динаміку зміни наступних трьох запитів зі списку запитів характеристики кібератак.

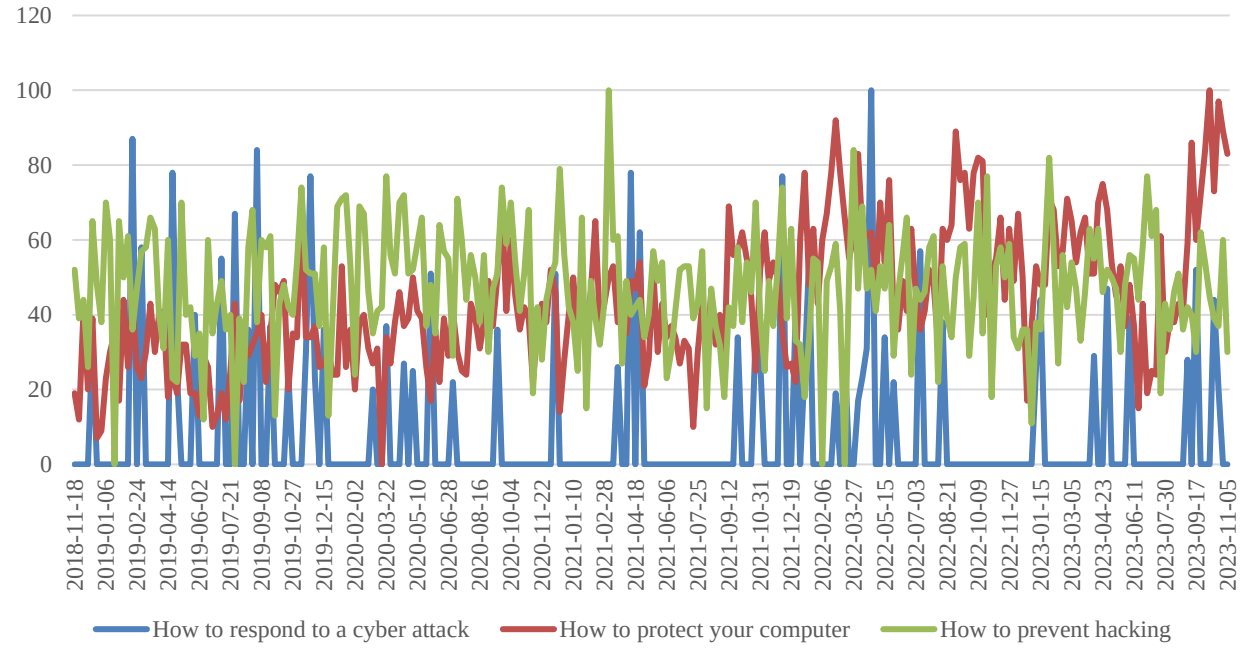


Рисунок 3.20 – Динаміка запитів «How to respond to a cyber attack», «How to protect your computer» та «How to prevent hacking» протягом 2018-2023 рр.

Джерело: складено на основі [247]

Активність пошукових запитів «How to prevent hacking» та «How to protect your computer» протягом досліджуваного періоду демонструють постійно високу популярність серед користувачів пошукової системи Google у світі. Крім того, людей більше цікавить питання як посилити захист комп'ютера в цілому і інтерес до даного питання почав активно зростати із кінця 2022 року. Щодо результатів частоти пошукового запиту «How to respond to a cyber attack», то тут досить схожа ситуація із пошуковим запитом «What to do when you are hacked», оскільки він також носить стрибкоподібний характер проте при цьому досягає пікових значень (близько 100 запитів на тиждень).

Аналіз результатів наступної пари пошукових запитів зі списку запитів характеристики кібератак зображено на наступному графіку (рис. 3.21).

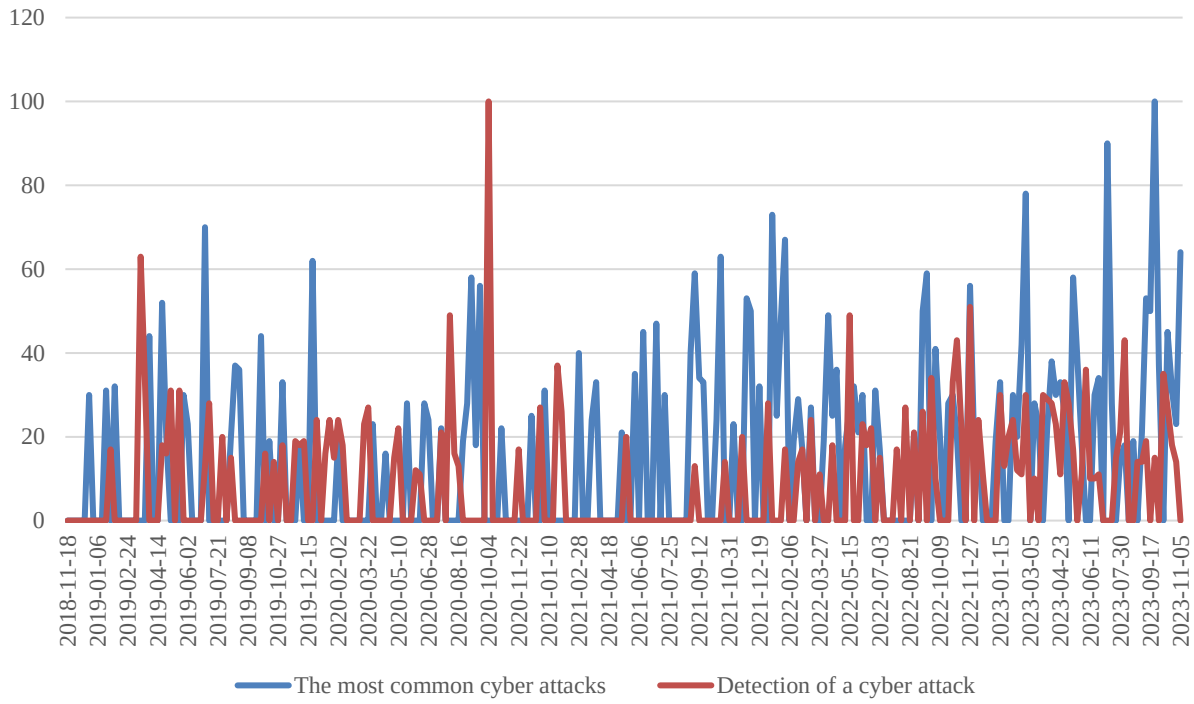


Рисунок 3.21 – Динаміка запитів «The most common cyber attacks» та «Detection of a cyber attack» протягом 2018-2023 рр.

Джерело: складено на основі [247]

Як бачимо, протягом 2018-2023 рр. тема найпоширеніших кібератак та способів їх виявлення є досить популярною і коливається в середньому від 10 до 60 запитів на тиждень. При цьому варто відзначити, що активність пошукового запиту серед користувачів Google за пошуковим запитом «The most common cyber attacks» є вищою ніж за запитом «Detection of a cyber attack». Це все пояснюється тим, що питанням найпоширеніших кібератак займаються представники різних напрямків діяльності – від науковців до журналістів. Крім того, з початку 2022 року кількість розглянутих пошукових запитів почала популяризуватись. Максимальне значення, 100, за пошуковим запитом «Detection of a cyber attack» було отримане у квітні 2020 року, а «The most common cyber attacks» – у середині вересня 2023 року.

Остання пара пошукових запитів зі списку запитів характеристики кібератак, присвячених особистому захисту від кібератак і розумінню, що комп’ютер або телефон було зламано, зображено на наступному графіку (рис. 3.22).

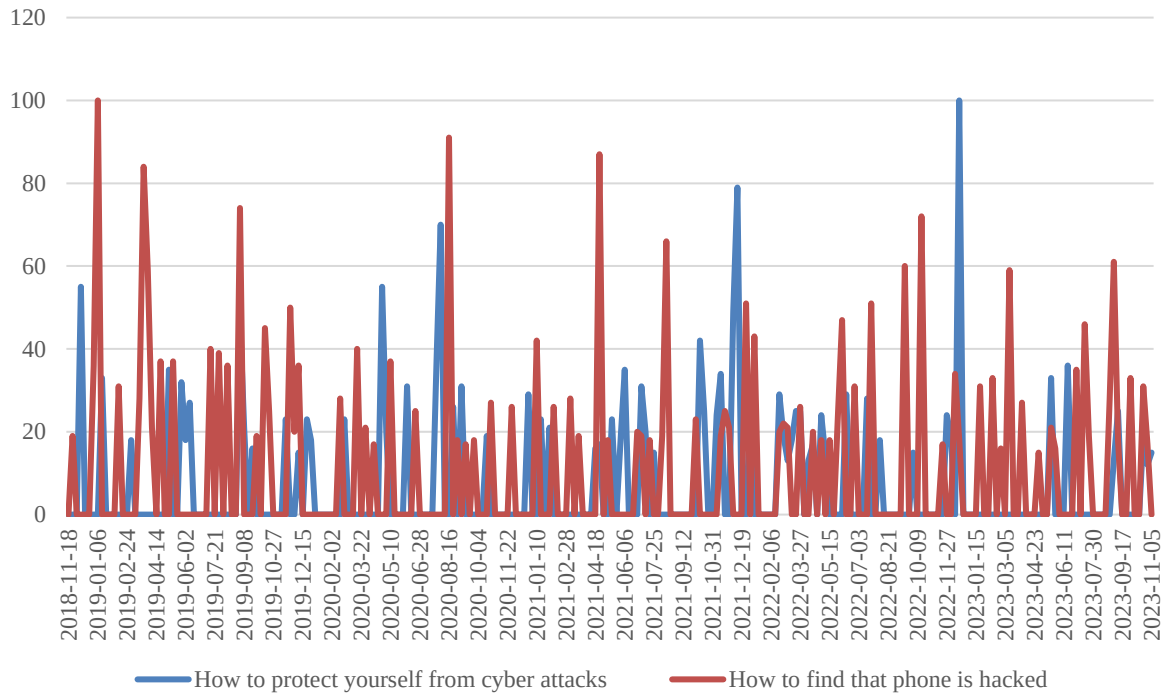


Рисунок 3.22 – Динаміка запитів «How to protect yourself from cyber attacks» та «How to find that phone is hacked» протягом 2018-2023 рр.

Джерело: складено на основі [247]

З огляду на представлений графік частота досліджуваних запитів протягом 2018-2023 рр. приблизно однакова і носит стрибкоподібний характер. Цікавим спостереженням є те, що людей у світі більше цікавить питання як виявити факт ураження ком'пютера або телефона тією чи іншою кібератакою. Протягом останніх п'яти років спостерігалося мінімум чотири тижні, коли кількість запитів «How to find that phone is hacked» перевищувала 60.

Таким чином, серед пошукових запитів зі списку запитів характеристики кібератак стабільну популярність протягом 2018-2023 рр. мають наступні пошукові запити: «Cyber police number», «Police number», «How to protect your computer» та «How to prevent hacking».

Проаналізуємо детальніше динаміку пошукових запитів із другого списку, який бере участь у дослідженні. На графіку 3.23 представлена динаміка перших трьох запитів із даного списку.

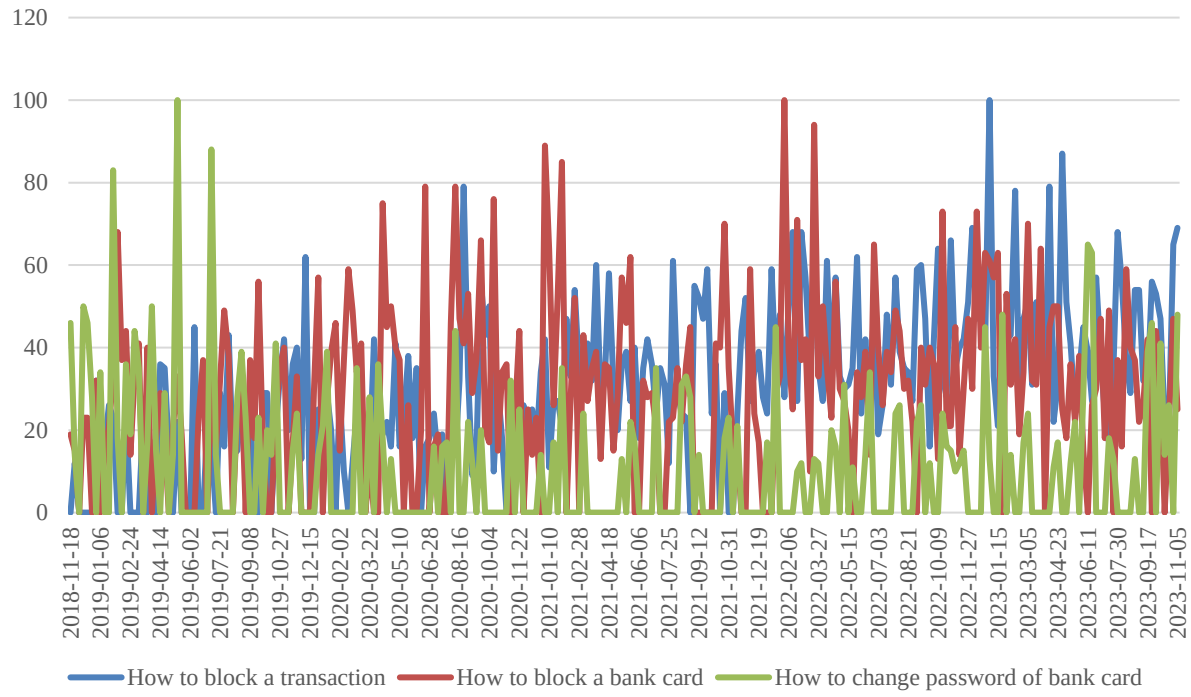


Рисунок 3.23 – Динаміка запитів «How to block a trasaction», «How to block a bank card» та «How to change password of bank card» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [247]

Частота пошукового запиту, який стосується зміни пароля від банківської картки дещо знизилась у 2022-2023 роках у порівнянні до 2018-2019 років. Однак, незважаючи на це, запити «How to block a trasaction» та «How to block a bank card» демонструють позитивну динаміку, що означає підвищений інтерес суспільства до проблеми збереження особистих банківських даних, пошкоджених імовірніше за все за рахунок кібершахрайства з огляду на результати попереднього блоку пошукових запитів.

Результати за наступними трьома пошуковими запитами представлені на графіку (рис. 3.24).

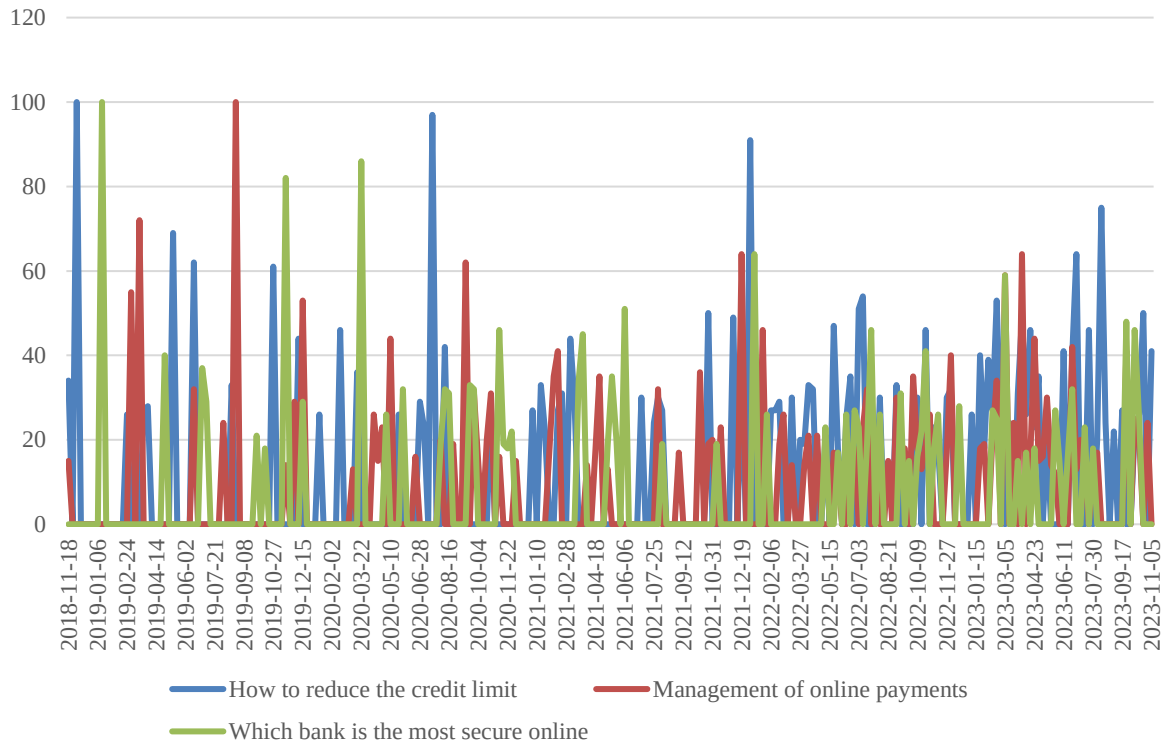


Рисунок 3.24 – Динаміка запитів «How to reduce the credit limit», «Management of online payments» та «Which bank is the most secure online» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [247]

Серед представленої трійки пошукових записів найвищу популярність має пошуковий запит «How to reduce the credit limit». Протягом досліджуваного періоду даний пошуковий запит досить часто з'являвся серед користувачів Google більше 60 разів на тиждень, особливо у період з 2018 до 2020 року. Два інші пошукові запити, які аналізуються на рисунку 2.6, мають приблизно однакову частоту у період 2021-2023 рр. До цього, починаючи із початку 2019 року і до весни 2020 року людей у світі особливо цікавило питання щодо найбільш захищеного банку в Інтернеті. Питання управління онлайн-платежами особливо актуалізувалось з осені 2021 року, що свідчить про зростання популярності безготівкових розрахунків у світі.

Наступний аналіз пошукових запитів, що характеризують рівень зменшення довіри до фінансових установ, «The most reliable banks» та «Bank call center number», представлені на рисунку 3.25.

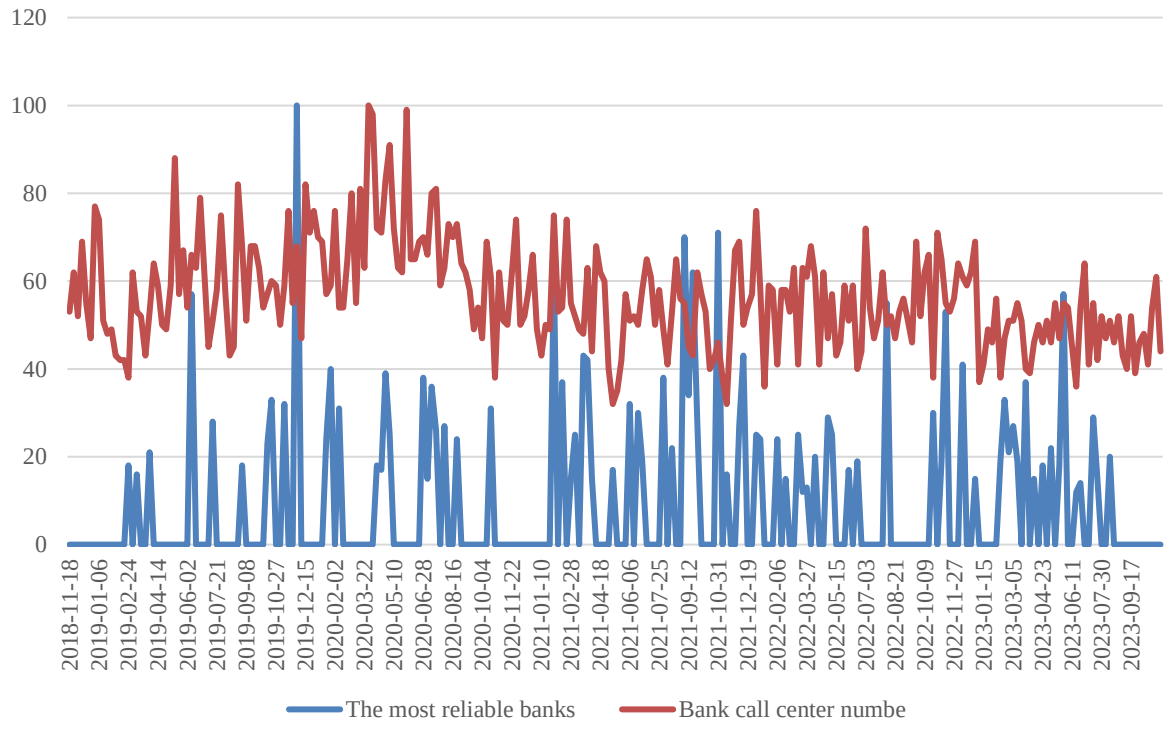


Рисунок 3.25 – Динаміка запитів «The most reliable banks» та «Bank call center number» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [247]

Як бачимо із рисунку 3.25 частота пошукового запиту, який стосується номеру кол-центру банку, зменшувалась позначки 30 на тиждень протягом досліджуваного періоду. Пікові значення частоти використання запиту «Bank call center number» припадають на весну 2020 року. Після цього зацікавленість користувачів почала знижуватись. З осені 2020 по осінь 2022 року вона знаходилась приблизно на односу рівні (40-60 запитів на тиждень). Починаючи із кінця 2022 року кількість подібних заходів знизилась до рівня понад 40 запитів на тиждень. Питання визначення найбільш надійних банків також цікавило користувачів Google, однак говорити про явно виражену тенденцію динаміки пошукового запиту «The most reliable banks» не можна, оскільки вона носить стрибкоподібний характер. Проте коливання частоти звернень за даним пошуковим запитом від 40 до 100 на тиждень свідчить про досить високий інтерес суспільства.

Остання пара пошукових запитів, які беруть участь у дослідженні, демонструє таку динаміку (рис. 3.26).

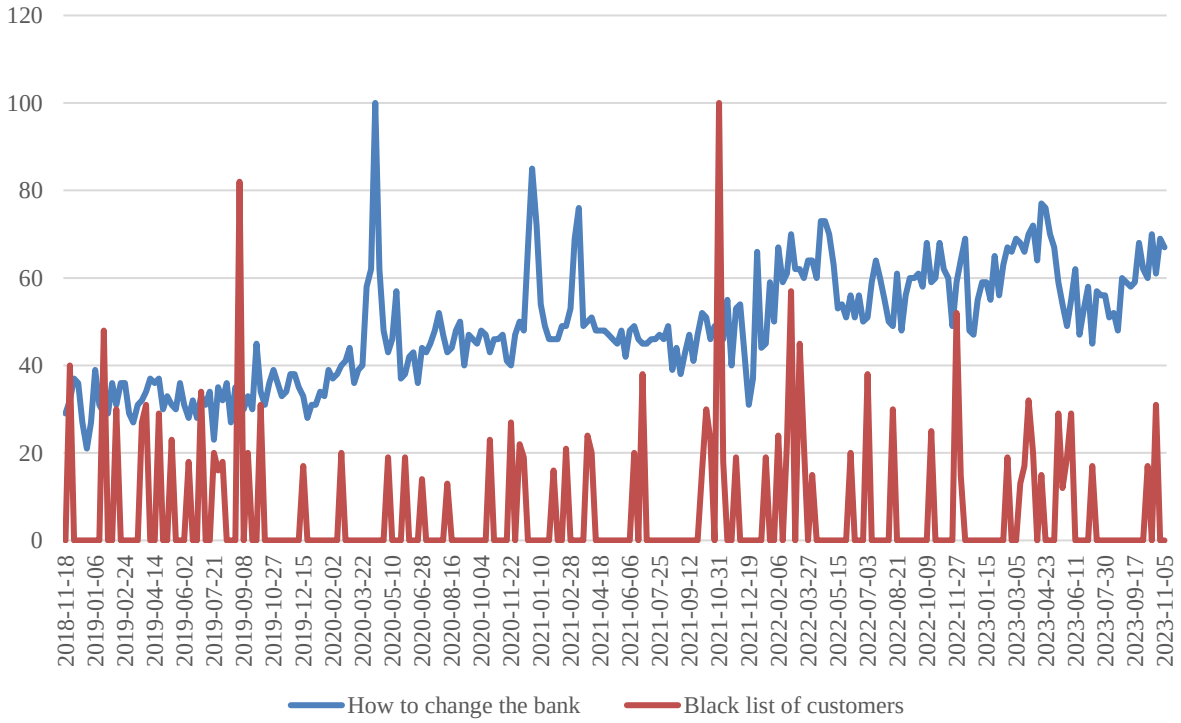


Рисунок 3.26 – Динаміка запитів «How to change the bank» та «Black list of customers» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [247]

Синя лінія на графіку (рис. 3.26) позначає динаміку частоти запиту користувачів пошукової системи Google стосовно потреби зміни обслуговуючого банку. Як бачимо протягом 2018-2023 років частота запиту «How to change the bank» демонструє постійну тенденцію до збільшення. Крім того, із весни 2020 року до початку 2021 року спостерігались пікові значення (від 78 до 100 запитів на тиждень) за даним запитом. Щодо другого пошукового запиту, «Black list of customers», то можна сказати, що він не є особливо популярним на відміну від попереднього, оскільки протягом останніх п’яти років користувачі Google досить нерегулярно здійснювали відповідний пошук. Причиною цього є стрибкоподібний характер динаміки даного пошукового запиту. Проте, варто також відзначити присутність на графіку пікових значень.

Таким чином, серед пошукових запитів зі списку запитів, що характеризують рівень зменшення довіри до фінансових установ, стабільну популярність протягом 2018-2023 рр. мають наступні пошукові запити: «How to block a trasaction», «How to block a bank card», «Bank call center number» та «How to change the bank».

Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках здійснюватиметься у три етапи.

На першому етапі за допомогою методу головних компонент (Principal Component Analysis) буде сформовано масив найбільш релевантних для проведення подальшого дослідження змінних, отриманих зі списку 20 ключових запитів, що представлені у таблицях 3.5-3.6.

Метод головних компонент – це статистичний метод, який використовується під час аналізу даних для зменшення розмірності даних, записаних у вигляді матриці (3.1) та виділення ключових компонент Comp.

$$X = \begin{matrix} x_{11} & x_{12} & \dots & x_{1j} & \dots & x_{1J} \\ x_{21} & x_{22} & \dots & x_{2j} & \dots & x_{2J} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{i1} & x_{i2} & \dots & x_{ij} & \dots & x_{iJ} \end{matrix} \quad (3.1)$$

Основною метою даного методу є перетворення даних великої розмірності в представлення меншої розмірності, фіксуючи якомога більше відхилень у даних. Алгоритм методу головних компонент має наступну послідовність:

– Центрування даних (віднімання середнього значення кожної змінної від кожного значення відповідного показника).

– Обчислення коваріаційної матриці (коваріаційна матриця описує зв’язки між усіма парами змінних у даних).

– Розкладання коваріаційної матриці на вектори власних значень, що представляють напрямки максимальної дисперсії в даних, а відповідні власні значення вказують на величину дисперсії вздовж цих напрямків.

– Вибір основних компонентів супроводжується ранжуванням векторів власних значень компонент в порядку спадання. Власний вектор із найвищим власним значенням є першою головною компонентою, другий за величиною є другою головною компонентою і так далі.

– Проектування даних на основні компоненти (початкові дані проектуються на вибрані основні компоненти, створюючи новий набір змінних (основних компонентів), які не корельовані та фіксують найважливішу інформацію в даних.

– Оцінка факторних навантажень вхідних показників у межах виділених компонент.

Визначившись із набором релевантних змінних на другому етапі моделювання необхідно провести кластеризацію методом k-середніх. Цей метод кластеризації був обраний для даного дослідження через свою популярність у використанні під час групування точок таким чином, щоб мінімізувати суму квадратів відстаней між точками даних і центроїдом кластера, до якого вони належать.

Алгоритм методу кластеризації k-середніх включає такі послідовні кроки:

– Первинний вибір центрів попередніх k кластерів (вибір k змінних за умови визначення максимальної між ними відстані).

– Первинний перерозподіл об’єктів між кластерами (принцип перерозподілу ґрунтується на визначенні мінімальної відстані між об’єктами).

– Запуск ітераційного процесу, який триває до тих пір, доки не буде сформовано оптимальну структуру кластерів, а загальна кількість ітерацій дорівнюватиме максимальному числу.

На третьому етапі загального дослідження передбачається побудова потенційних портретів інсайдерів-кібершахраїв у банках на основі відібраних змінних методом головних компонент та кластеризацією за допомогою методу асоціативного навчання [284].

Побудова асоціативних правил лежать в основі афінітивного аналізу (affinity analysis), суть якого полягає у виявленні взаємозв’язку між певними

подіями, що можуть мати принципову обумовленість. Напрямки найчастішого використання методу асоціативних правил: формування кошику покупця в магазині за рахунок його особистих уподобань, оцінка рівня задоволеності клієнтів від використання тих чи інших послуг, формування профілю користувачів нового мобільного застосунку або веб-сайту, ідентифікація можливих побічних ефектів від вживання нового лікарського препарату тощо.

Загальний алгоритм моделювання за допомогою асоціативних правил включає наступні кроки:

– Формування множини подій (транзакцій), які лежатимуть в основі моделювання.

– Дослідження структури асоціативного правила, яке має включати умову (antecedent) та наслідок (consequent) (X=>Y).

– Визначення основних характеристик асоціативного правила: підтримку (support), імовірність (confidence), ліфт (interest lift), левередж (leverage), доказ (conviction) та метрика Чжана (zhangs_metric).

Підтримка представляє собою набір транзакцій, які складаються із умови та наслідку (3.2).

$$S(X \to Y) = P(X \cap Y) = \frac{n(\{X;Y\} \in d_i)}{N}, \tag{3.2}$$

де N – загальний набір змінних;

d_i – конкретна транзакція із загальної кількості транзакцій D.

Імовірність у контексті асоціативного правила – це міра точності правила та дорівнює відношенню сукупної кількості транзакцій з умовою та наслідком до кількості транзакцій з умовою (3.3):

$$C(X \to Y) = P(X|Y) = \frac{n1(\{X;Y\} \in d_i)}{n1(\{X\} \in d_i)}. \tag{3.3}$$

Чим вищі значення підтримки та імовірності, тим вища імовірність того, що певна транзакція, яка містить умову, включатиме і наслідок.

Ліфт представляє собою відношення частоти умови та наслідку транзакції до частоти появи наслідку (чим більше значення, тим частіше умова обумовлює настання наслідку) (3.4):

$$L(X \to Y) = C(X \to Y)/P(Y). \quad (3.4)$$

У випадку, якщо ліфт рівний 1, то зв’язок між умовою та наслідком відсутній. Якщо значення близьке до 0, то присутній сильна зворотня залежність.

Левередж дорівнює різниці спостережуваної частоти, коли умова та наслідок ідентифікуються разом, і добутку частоти виявлення умови та наслідку (3.5):

$$T(X \to Y) = S(X \to Y) - P(X) * P(Y). \quad (3.5)$$

Доказ – це це міра, яка допомагає визначити чи випадково з'явилося правило (3.6). Високе значення доказу свідчить про те, що наслідок сильно залежить від умови. Якщо оцінка визначена ідеальною, то доказ визначається як «inf»:

$$K(X \to Y) = \frac{1-S(Y)}{1-C(X \to Y)}. \quad (3.6)$$

Метрика Чжана (3.7) дозволяє визначити як асоціацію, так і дисоціацію. Значення коливається від -1 до 1. Позитивне значення вказує на асоціацію, а негативне значення вказує на дисоціацію.

$$Z(X \to Y) = \frac{C(X \to Y) - C(X` \to Y)}{Max[C(X \to Y), C(X` \to Y)]}. \quad (3.7)$$

Формулювання висновків на основі отриманих асоціативних правил.

Таким чином, в представленому підрозділі представлено комплексне методологічне забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках на основі поєднання трьох методів статистичного дослідження: методу головних компонент для ідентифікації релевантних змінних, метод кластеризації *k*-середніх для формування кластерів дослідження та метод асоціативних правил для побудови потенційних портретів інсайдерів-кібершахраїв у банках. Всі необхідні обчислення в роботі проводитимуться за допомогою програмного статистичного пакету Stata 18 та мови програмування Python 3.

Відповідно до визначеної послідовності етапів моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках спочатку необхідно методом головних компонент відібрати найбільш релевантні змінні для проведення подальшого дослідження.

Проаналізуємо власні значення компонент, які отримані для 20 вхідних змінних (таблиця 3.7) та графік кам’янистого осипу (рис. 3.27). Це дозволить виявити оптимальну кількість компонент для подальшого аналізу.

Загальна кількість отриманих компонент відповідає загальній кількості вхідних змінних. З огляду на результати власних значень отриманих компонент, представлених у таблиці 3.6, то перші дев’ять компонент мають власне значення більше за 1. При цьому значення кумулятивної дисперсії для даних дев’яти компонент дорівнює 0,633, що означає, що більше ніж 63% досліджуваного явища пояснюється даними компонентами.

Таблиця 3.7 – Власні значення, дисперсія та кумулятивна дисперсія компонент

Компонента	Власне значення	Дисперсія	Кумулятивна дисперсія
Компонента 1	3,322	1,900	0,166
Компонента 2	1,423	0,082	0,237
Компонента 3	1,341	0,144	0,304
Компонента 4	1,197	0,066	0,364
Компонента 5	1,131	0,033	0,421
Компонента 6	1,098	0,021	0,476
Компонента 7	1,078	0,022	0,530

Компонента	Власне значення	Дисперсія	Кумулятивна дисперсія
Компонента 8	1,055	0,047	0,582
Компонента 9	1,008	0,045	0,633
Компонента 10	0,964	0,056	0,681
Компонента 11	0,907	0,053	0,726
Компонента 12	0,854	0,079	0,769
Компонента 13	0,775	0,017	0,808
Компонента 14	0,757	0,030	0,846
Компонента 15	0,727	0,052	0,882
Компонента 16	0,676	0,097	0,916
Компонента 17	0,579	0,101	0,945
Компонента 18	0,478	0,135	0,969
Компонента 19	0,343	0,056	0,986
Компонента 20	0,287	,	1,000

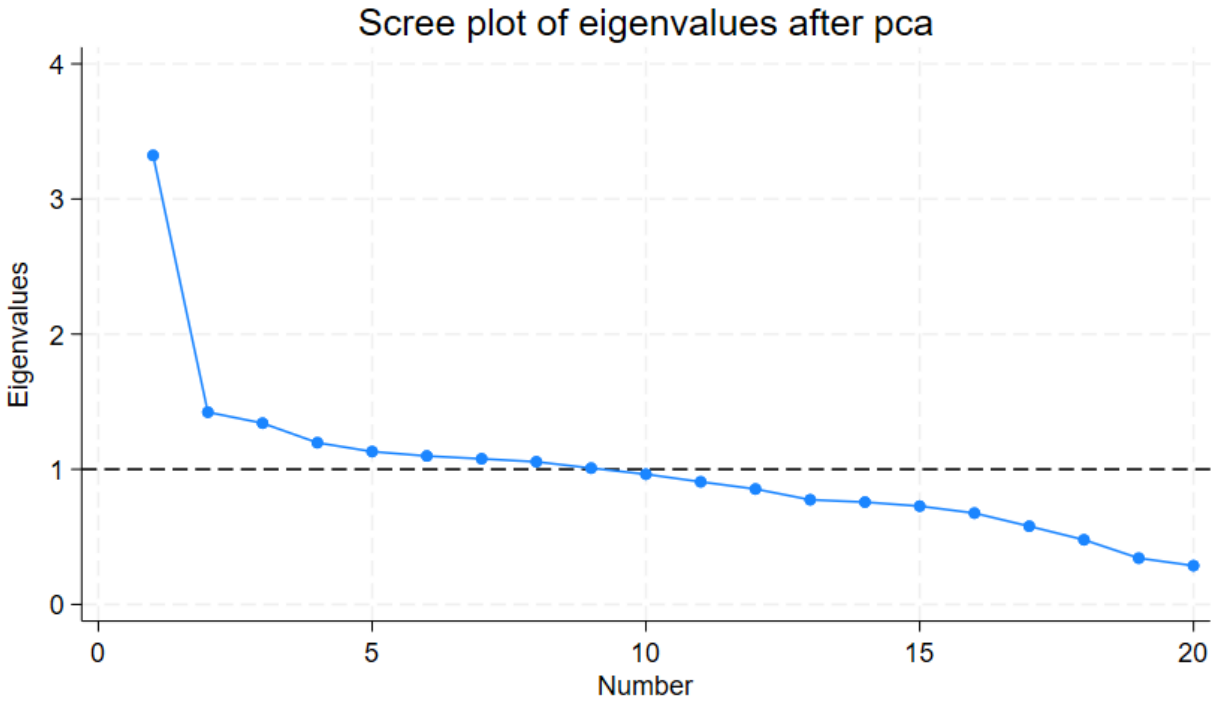


Рисунок 3.27 – Графік кам’янистого осипу

Графік кам’янистого осипу (рис. 3.27) дозволяє візуалізувати результати першого етапу методу головних компонент, оскільки демонструє власні значення кожної компоненти. Пунктирною лінією на графіку позначене місце, що відповідає оптимальній кількості компонент. У даному випадку – це 9.

Для того, щоб зрозуміти міру впливу кожної змінної в межах кожної компоненти, необхідно дослідити їх факторні навантаження (таблиця 3.8). По суті факторне навантаження представляє собою коефіцієнт кореляції відповідної змінної із компонентою, до якої вона потрапила. В контексті теми даного

дослідження кожна компонента представляє собою певний портрет потенційного інсайдера-кібершахрая в банку, а найбільші значення факторних навантажень змінних свідчать якими саме ознаками обумовлюється даний портрет.

Таблиця 3.8 – Факторні навантаження показників

Змінна	Комп 1	Комп 2	Комп 3	Комп 4	Комп 5	Комп 6	Комп 7	Комп 8	Комп 9	Комп10
var1	0,451	-0,019	-0,013	0,016	0,019	-0,098	-0,150	-0,091	-0,008	0,451
var2	0,271	-0,023	0,361	0,378	0,034	-0,130	-0,284	-0,122	0,076	0,271
var3	0,129	0,104	0,131	-0,168	-0,131	-0,135	0,422	0,030	0,473	0,129
var4	-0,046	0,195	-0,253	0,593	0,013	-0,017	0,082	0,048	-0,086	-0,046
var5	0,421	0,095	-0,152	0,020	0,058	0,029	0,119	0,032	-0,033	0,421
var6	0,052	-0,597	0,002	0,101	0,056	0,125	0,137	0,283	0,039	0,052
var7	0,213	0,236	-0,173	-0,070	-0,394	0,166	-0,041	-0,006	-0,165	0,213
var8	0,150	-0,091	-0,134	0,112	0,091	0,206	0,164	0,052	0,600	0,150
var9	-0,038	0,234	0,357	0,036	0,214	0,207	0,369	-0,118	0,129	-0,038
var10	-0,025	0,166	-0,309	0,175	0,057	-0,391	-0,158	0,307	0,196	-0,025
var11	0,378	0,117	0,107	0,015	-0,034	-0,113	-0,091	0,029	-0,073	0,378
var12	0,125	-0,085	0,044	0,037	0,173	-0,228	0,575	-0,094	-0,492	0,125
var13	-0,095	-0,171	-0,281	0,359	-0,017	0,239	0,144	-0,463	-0,057	-0,095
var14	0,130	-0,313	-0,241	-0,094	0,339	0,120	-0,232	-0,347	0,122	0,130
var15	0,161	-0,207	-0,057	0,037	-0,034	0,343	0,054	0,614	-0,187	0,161
var16	0,065	0,063	0,305	0,361	-0,397	0,363	-0,030	-0,031	0,038	0,065
var17	0,033	0,221	0,206	-0,176	0,417	0,434	-0,235	0,050	-0,126	0,033
var18	-0,170	-0,107	0,366	0,320	0,310	-0,245	-0,083	0,169	0,005	-0,170
var19	0,459	-0,050	0,015	-0,007	0,159	-0,097	0,055	-0,055	-0,034	0,459
var20	-0,012	0,425	-0,267	0,117	0,402	0,175	0,085	0,157	0,017	-0,012

Для кращого сприйняття отриманих результатів залишимо в даній таблиці лише ті значення факторних навантажень, які абсолютно перевищують значення 0,3 (табл. 3.9). Це дозволить ідентифікувати найбільш релевантні змінні в межах виділених компонент.

Як бачимо, кожна із представлених компонент обумовлюється різною комбінацією вхідних змінних. Це ще раз підтверджує можливість визначення різних потенційних портретів інсайдерів-кібершахраїв у банку.

Таблиця 3.9 – Факторні навантаження змінних, які перевищують 0,3 по модулю

Змінна	Комп1	Комп2	Комп3	Комп4	Комп5	Комп6	Комп7	Комп8	Комп9
var1	0,451								
var2			0,361	0,378					
var3							0,422		0,473
var4				0,593					
var5	0,421								
var6		-0,597							
var7					-0,394				
var8									0,590
var9			0,357				0,369		
var10			-0,309			-0,391		0,307	
var11	0,378								
var12							0,575		-0,491
var13				0,359				-0,463	
var14		-0,313			0,330			-0,346	
var15						0,343		0,614	
var16			0,305	0,361	-0,397	0,363			
var17					0,417	0,434			
var18			0,366	0,310	0,310				
var19	0,459								
var20		0,425			0,402				

В межах даного дослідження для проведення асоціативного аналізу та побудови наборів асоціативних правил зупинимось на більш детальному аналізу перших трьох компонент. На основі цих компонент та на підставі критерію Силует (Silhouette) (рис. 3.28), максимальне значення якого відповідає оптимальній кількості кластерів, які можуть сформуватись під час кластеризації методом k-середніх.

Найбільше значення критерію Силует (0,357) відповідає оптимальній кількості кластерів 2 або 3. Однак з урахуванням попереднього рішення щодо кількості відібраних компонент, для кластеризації методом k-середніх обрано 3 кластери. Візуальне представлення утворених кластерів зображено на рисунку 3.29.

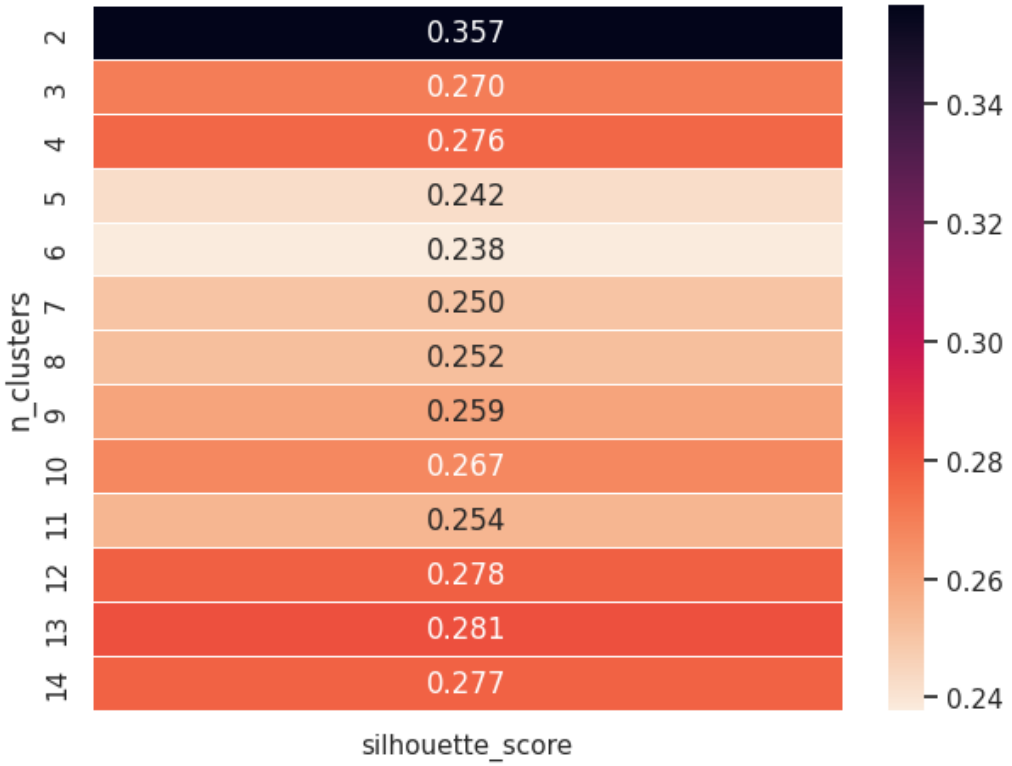


Рисунок 3.28 – Значення критерію Силует

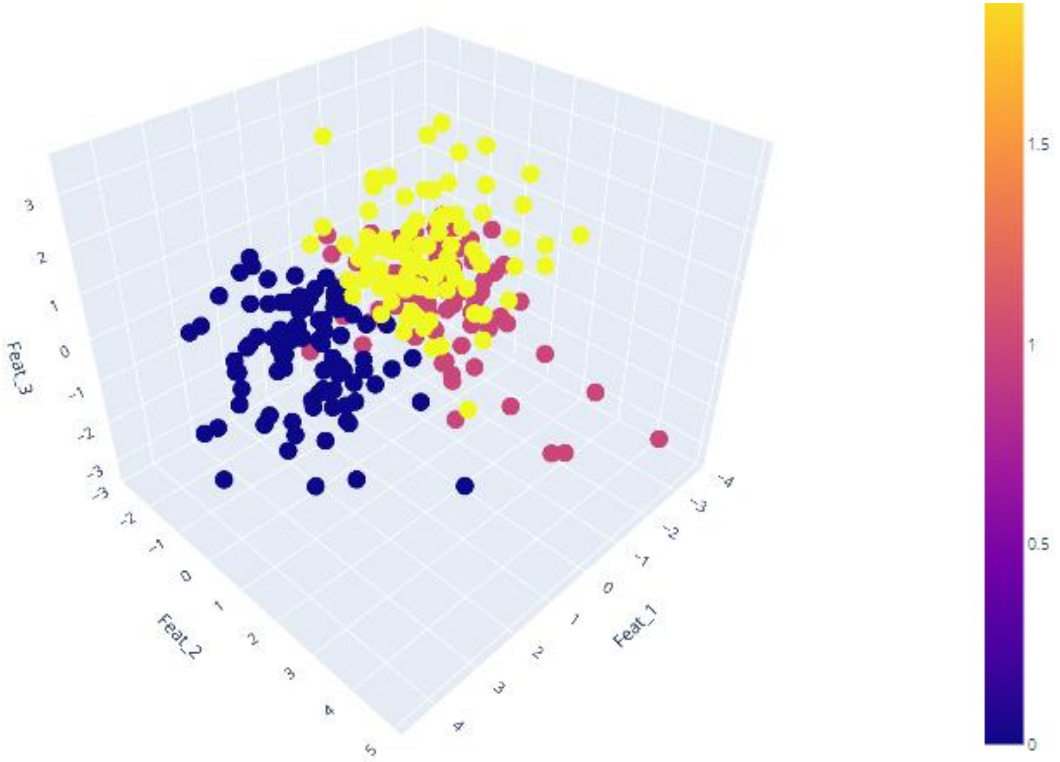


Рисунок 3.29 – Результати кластеризації методом k-середніх

Таблиця 3.9 – Відібрані групи змінних для проведення асоціативного аналізу

Група	Змінні

I	Номер кіберполіції
	Як посилити захист комп’ютера
	Як заблокувати транзакцію
	Як змінити обслуговуючий банк (як перевести виплату зарплати з одного банку на інший)
II	Як не допустити злому персональних даних (сайту, соціальних мереж)
	Як зменшити ліміт по банківській картці
	Чорний список користувачів
III	Номер поліції
	Як захистити себе від кібератак
	Як зрозуміти, що комп’ютер (телефон) зламали
	Який банк найбільш захищений (в Інтернеті)
	Номер підтримки банку (або номер кол-центру банку)

Таким чином, до першої групи потрапили змінні, які спрямовані на визначення політики безпеки від потенційних кібершахрайств, що з іншої сторони може бути можливістю для порушення даної безпеки інсайдерами-кібершахраями, банку зокрема.

Друга група об'єднує змінні, які мають безпосереднє відношення до захисту персональних даних клієнтів, що може бути основою для отримання необхідної інформації для інсайдерів-кібершахраїв.

До третьої групи увійшли змінні, які також мають відношення до забезпечення захищеності персональних даних користувачів, а також ідентифікації потенційних вразливостей банків.

Третій етап моделювання передбачає проведення асоціативного аналізу засобами Python 3. Для аналізу було використано бібліотеки «pandas» (під час роботи з даними) та «mlxtend» (безпосередньо під час проведення асоціативного аналізу). Також під час визначення асоціативних правил використовувався алгоритм «apriori».

Перш ніж починати визначення асоціативних правил за допомогою мови програмування Python необхідно вхідні дані перевести в бінарний вигляд (рис. 3.30).

```
[41] one_hot = pd.get_dummies(df[categorical_columns])

[42] one_hot
```

week	Cyber police number_0	Cyber police number_6	Cyber police number_7	Cyber police number_8	Cyber police number_9	Cyber police number_10	Cyber pol number
2018-11-18	0	1	0	0	0	0	
2018-11-25	0	0	0	0	0	0	
2018-12-02	0	0	0	1	0	0	
2018-12-09	0	0	0	0	0	0	
2018-12-16	0	0	0	0	0	0	
...	...	...	...	...	...	...	
2023-10-08	0	0	0	0	0	0	
2023-10-15	0	0	0	0	0	0	
2023-10-22	0	0	0	0	0	0	
2023-10-29	0	0	0	0	0	0	
2023-11-05	0	0	0	0	0	0	

260 rows × 252 columns

Рисунок 3.30 – Перетворення вхідних даних в бінарні значення за допомогою методу «one hot encoding»

Представлений нижче фрагмент програмного коду написаний на Python (рис. 3.31) є прикладом використання апріорного алгоритму та функції «association_rules», які зазвичай використовуються для аналізу ринкового кошика в галузі інтелектуального аналізу даних.

```
[45]
# Find frequent itemsets
frequent_itemsets = apriori(one_hot, min_support=0.01, use_colnames=True)

# Generate association rules
rules = association_rules(frequent_itemsets, metric="confidence", min_threshold=0.2)

rules
```

Рисунок 3.31 – Фрагмент програмного коду написаний на Python, що представляє собою приклад використання апріорного алгоритму та функції «association_rules»

Представлений код використовує алгоритм «apriori» та функцію «association_rules» для аналізу запитів користувачів в області аналізу даних. Структура «apriori» алгоритму наступна (3.8).

```
frequent_itemsets = apriori(one_hot, min_support=0.01,
                    use_colnames=True)
```
(3.8)

де one_hot – вхідні дані, у форматі one-hot encoding;
min_support=0.01 – набори, що зустрічаються в 1% транзакцій;
use_colnames=True – використовує значення змінних.

Процес створення правил асоціації має наступний вигляд (3.9).

```
rules = association_rules(frequent_itemsets,
metric="confidence", min_threshold=0,2)
```
(3.9)

де metric="confidence" – міра надійності правила;
min_threshold=0.2 – правила з достовірністю не менше 20%.

У результаті проведення асоціативного аналізу для перерахованих груп змінних було отримано три моделі асоціативних правил із відповідними критеріями якості. Результати даного моделювання представлені в додатку Ж (табл. Ж.1-Ж.4). Проаналізуємо отримані результати асоціативного аналізу за допомогою наступних харакетристик: підтримку (*support*), імовірність (*confidence*), ліфт (interest lift), левередж (leverage), доказ (*conviction*) та метрика Чжана (*zhangs_metric*).

З огляду на результати асоціативного аналізу для першої групи змінних, імовірність асоціативного правила коливається від 0,214 до 0,75. Тобто жодне правило не має 100% імовірності. Однак, зважаючи на цю обставину, проранжувавши отриману сукупність асоціативних правил за рівнем імовірності, що відповідає значенню в проміжку від 0,6 до 0,75, отримано наступні результати (табл. 3.10).

Таблиця 3.10 – Результати асоціативного аналізу для першої групи змінних, імовірність асоціативних правил яких знаходиться в діапазоні 0,6-0,75

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
How to change the bank_40	Cyber police number_24	0,023	0,600	26,000	0,011	2,442	0,980
How to protect your computer_54	How to block a transaction_31	0,027	0,600	22,286	0,011	2,433	0,974

З огляду на представлені результати в таблиці Ж.1 додатку Ж отримано всього 20 асоціативних правил, однак, провівши аналіз їх характеристик, спираючись в першу чергу на значення імовірності асоціативних правил, для підсумкового аналізу варто залишити лише два асоціативні правила (табл. 3.10). Як бачимо, із імовірністю 60% виконуються правила How to change the bank => Cyber police number та How to protect your computer => How to block a transaction. При цьому значення підтримки складає 2,3% і 2,7% відповідно, що означає те, що представлені правила зустрічаються в більше 2% усіх транзакцій. Відносно невисокий рівень значення підтримки в контексті виявлення потенційних шахрайських дій інсайдерів-кібершахраїв у банках є нормальним, оскільки із момент виявлення шахрайських дій є досить складним і може залежати від значного набору факторів. Високе значення ліфта для обох правил, 26 і 22,286 відповідно, свідчить про те, що представлені наслідки часто визначаються саме даними причинами, у порівнянні із ситуаціями, коли причини відсутні.

Значимість отриманих асоціацій, яка описується левереджем, є однаковою і становить 1,1%. Позитивне значення метрики Чжана для обох асоціативних правил є позитивним, 0,98 і 0,974 відповідно, що підтверджує факт присутності асоціації між причинами та наслідками.

Таким чином, якщо трансформувати отримані результати асоціативного аналізу для першої групи змінних на потенційного інсайдера-кібершахрая в банку, то можна зробити висновок, що причиною зміни обслуговуючого банку є саме кібершахрайство, оскільки імовірніше за все після цього є потреба в пошуку

номеру кіберполіції. Таким чином, інсайдер-кібершахрай банку може отримати доступ до персональної фінансової інформації клієнта, який постраждав. Друге асоціативне правило із табл. 3.10 надає інсайдеру-кібершахраю в банку по заблокованій транзакції зрозуміти потенційні уразливі моменти в захисті комп'ютера користувача-клієнта банку.

Результати асоціативного аналізу для другого набору змінних із табл. 3.9 представлені в таблиці Ж.2 додатку Ж. Як бачимо, від попередніх результатів, отримані асоціативні правила мають значення імовірностей асоціативних правил на рівні 100%, однак потрібно зважати також на вид транзакції, для якої було отримано відповідне значення імовірності.

Аналогічно до попереднього аналізу результатів відберемо ті асоціативні правила, які мають найвище значення асоціативної імовірності (табл. Ж.4). Як бачимо, багато асоціативних правил мають значення імовірності 100%, однак, враховуючи невисоку кількість попередньо отриманих результатів за пошуковими запитами «How to reduce the credit limit» та «Black list of customers» усі наслідки утворених асоціативних правил відповідають нулевій кількості відповідних запитів, що не дає можливості коректно дослідити зв'язок між умовою та наслідком. Крім того, значення ліфту для всіх пар асоціативних правил наближається до одиниці, що також підтверджують відсутність зв'язку між умовою та наслідком.

Результати асоціативного аналізу для третього набору змінних із табл. 3.9представлені в таблиці Ж.3 додатку Ж. Як бачимо, кількість отриманих асоціативних правил є великою, тому необхідно проаналізувати їхню якість. Аналогічно до попередніх результатів для даної групи змінних є також значення асоціативних імовірностей на рівні 100%, однак не для всіх побудованих асоціативних правил вона дійсно підтверджує присутність причинно-наслідкового зв'язку між умовою та наслідком. Тому виникає потреба в аналізі нижчих значень асоціативних імовірностей, на основі яких можна довести присутність якісного зв'язку між умовою та наслідком. В наступній таблиці (табл. 3.11) представлені асоціативні правила для даного набору змінних,

асоціативні імовірності для яких знаходяться в проміжку від 0,6 до 1, і пошукові запити при цьому не є нульовими.

Таблиця 3.11 – Результати асоціативного аналізу для третьої групи змінних, імовірність асоціативних правил яких знаходиться в діапазоні 0,6-1

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
1	2	3	4	5	6	7	8
How to protect yourself from cyber attacks_13	Police number_63	0,065	1,000	15,294	0,011	inf	0,946
How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
Which bank is the most secure online_0, How to protect yourself from cyber attacks_13	Police number_63	0,065	1,000	15,294	0,011	inf	0,946
How to protect yourself from cyber attacks_13	Which bank is the most secure online_0, Police number_63	0,042	1,000	23,636	0,011	inf	0,969
How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
How to find that phone is hacked_28	Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,035	0,750	21,667	0,011	3,862	0,969
Which bank is the most secure online_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964

Продовження таблиці 3.11

1	2	3	4	5	6	7	8
How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52	0,035	0,750	21,667	0,011	3,862	0,969
Which bank is the most secure online_0, How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
Which bank is the most secure online_0, How to find that phone is hacked_28	Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,035	0,750	21,667	0,011	3,862	0,969
How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52	0,035	0,750	21,667	0,011	3,862	0,969
How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,031	0,750	24,375	0,011	3,877	0,974

Як бачимо, пошуковий запит «Police number» є наслідком для причини «How to protect yourself from cyber attacks» з імовірністю 100%. В межах інших асоціативних правил, де також зустрічається «Police number», як наслідок або

частина наслідку разом із іншим пошуковим запитом, причина залишається незмінною.

Пошуковий запит «Bank call center number» присутній у семи отриманих асоціативних правилах і всі сім разів у вигляді наслідку. З імовірністю 75% даний пошуковий запит з'являється внаслідок іншого пошукового запиту – «How to find that phone is hacked». При чому варто зазначити, що даний причинно-наслідковий зв'язок присутній як безпосередньо між даною парою пошукових запитів, так і в сукупності із іншими пошуковими запитами.

Решта отриманих асоціативних правил містить пошукові запити, які мають нулеві значення частоти появи, тому інтерпретувати їх немає потреби.

При цьому значення підтримки для розглянутих асоціативних правил складає від 3,1% до 6,5%.Це означає, що представлені правила зустрічаються у від 3,1% до 6,5% усіх транзакцій. Даний результат є абсолютно нормальним, якщо мова йде про аналіз потенційних шахрайських схем. Високе значення ліфта для обох видів асоціативних правил, від 15,294 до 24,375 підтверджують, що представлені наслідки часто визначаються саме розглянутими причинами, у порівнянні із ситуаціями, коли причини відсутні.

Значимість отриманих асоціацій, яка описується левереджем, є однаковою і становить 1,1%. Позитивне значення метрики Чжана для обох асоціативних правил є позитивним, від 0,964 до 0,974, що підтверджує факт присутності асоціації між причинами та наслідками.

Отже, спираючись на результати третього асоціативного аналізу, потеційний інсайдер-кібершахрай у банку ще раз переконується у тому, що вразливість користувачів кібератаками супроводжується пошуком номеру поліції для усунення негативних наслідків, що ще раз підтверджує дієвість шахрайських дій за умови отримання доступу до персональних даних клієнтів банку. Друге асоціативне правило із табл. 3.11 надає інсайдеру-кібершахраю в банку розуміння, що більшість банківських транзакцій сучасним користувачем банківських послуг на сьогодні відбуваються за допомогою телефону, оскільки потреба у виявленні чи зламаний телефон кібершахраями імовірніше за все

супроводжується дзвінком до кол-центру банку. Тому інсайдер-кібершахрай банку може, отримавши фізичний доступ до телефону клієнта банку, здійснити ряд шахрайських дій із його банківським акаунтом.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [285].

3.2 Науково-методичний підхід до створення інформаційного забезпечення фінансової установи

3.2.1 Розроблення структури інформаційної бази експертної системи виявлення інсайдерських кіберзагроз у банках

Протидія кіберзагрозам, ініційованим інсайдерами в банках, визначається кількома ключовими аспектами. По-перше, це фінансові втрати, які можуть виникнути в результаті крадіжок коштів, фінансових маніпуляцій або зловживання привілеями. Другий аспект полягає в порушенні конфіденційності та можливому витоку конфіденційної інформації, що може спричинити втрату репутації та порушення законів про конфіденційність. Третій аспект стосується загроз інформаційній безпеці, які можуть включати атаки на інформаційні системи та мережі. Порушення внутрішнього порядку та регуляторних вимог також може виникнути через дії інсайдерів, призводячи до штрафів та судових справ. У зв'язку з цим виникає необхідність в створенні експертної системи для виявлення кіберзагроз від дій інсайдерів.

Така система забезпечить раннє виявлення аномалій та автоматизовану обробку великого обсягу даних, що є критичним у банківському середовищі. Застосування технологій машинного навчання дозволить системі навчатися на основі історичних даних та адаптуватися до нових видів загроз. Експертна система також забезпечить постійний моніторинг та можливість швидкого реагування на потенційні загрози, а її використання дозволить постійно вдосконалювати систему в залежності від змін у кіберзагрозах та інсайдерських методах.

Для надійної та ефективної роботи експертної системи, що протидіє діям інсайдерів у банківському середовищі, критично важливим є розроблення структури інформаційного забезпечення. Воно повинно включати можливості для виявлення аномалій, систематичного моніторингу дій користувачів, аналізу транзакцій та поведінки користувачів, попередження та реагування, тощо. Саме тому в даній статті буде запропоновано структуру інформаційної бази експертної системи виявлення кіберзагроз в результаті дій інсайдерів у банках.

Експертна система виявлення кіберзагроз в результаті дій інсайдерів у банках - це інформаційна система, яка використовується для виявлення та аналізу можливих загроз безпеці в межах банківського середовища, зумовлених внутрішніми (інсайдерськими) діями працівників. Інсайдери - це особи, які мають авторизований доступ до внутрішньої інформації та ресурсів організації, і вони можуть використовувати свій доступ для шкідливих або несанкціонованих дій. Експертні системи в цьому контексті використовують штучний інтелект для аналізу великої кількості даних та виявлення аномалій, які можуть свідчити про потенційні загрози безпеці. Основні функції експертної системи включають:

– моніторинг активності. Система виявляє незвичайні патерни або активності в системі, які можуть бути підозрілими;

– аналіз доступу. Перевірка та аналіз авторизацій та доступів працівників до різних ресурсів банку;

– виявлення аномалій. Система використовує алгоритми машинного навчання для виявлення аномалій в поведінці працівників чи використанні ресурсів;

– інтеграція з іншими системами безпеки. Взаємодія з іншими системами безпеки (наприклад, системами виявлення вторгнень) для отримання повної карти загроз;

– генерація тривог. Система може автоматично генерувати тривоги або повідомлення для операторів безпеки при виявленні потенційних загроз;

– ідентифікація ризикових патернів. Використання експертних знань для ідентифікації та аналізу патернів, які можуть свідчити про інсайдерські загрози.

Експертні системи такого роду допомагають банкам ефективно виявляти, відстежувати та вирішувати потенційні кіберзагрози, пов'язані з діями внутрішніх користувачів, зменшуючи ризики витоку інформації та інших безпекових проблем. Вони можуть складатися з різних компонентів, які спільно працюють для ефективного виявлення та відповіді на потенційні загрози безпеці. Основні компоненти такої системи включають:

– систему моніторингу та аудиту, яка відслідковує активності та події в банківській інфраструктурі, включаючи доступ до ресурсів, транзакції, зміни в правах доступу та інші події;

– модуль виявлення аномалій, який використовує алгоритми машинного навчання та аналізу даних для виявлення незвичайних патернів, що можуть свідчити про потенційні загрози з боку інсайдерів;

– базу даних та сховище інформації, яке зберігає інформацію про користувачів, ресурси, транзакції та інші дані, що використовуються для аналізу та виявлення аномалій;

– експертні правила та база знань, які включають в себе правила та експертні знання про типові патерни поведінки користувачів та інсайдерські загрози;

– модуль ідентифікації та аутентифікації, який відповідає за перевірку та аутентифікацію користувачів, а також контроль доступу до різних ресурсів;

– систему генерації тривог, що виробляє тривоги та повідомлення для операторів безпеки або інших відповідальних осіб при виявленні потенційних загроз;

– модуль відповідей та контрзаходів, який забезпечує автоматичні або рекомендації щодо контрзаходів та відповіді на виявлені загрози;

– інтеграцію з іншими системами безпеки, такими як системи виявлення вторгнень, для отримання повної картини безпекового стану;

– інтерфейс для адміністраторів та аналітиків, який забезпечує користувачам інтерфейс для налаштування системи, аналізу результатів та вживання заходів.

Ці компоненти спільно працюють, щоб створити комплексну систему, яка дозволяє ефективно виявляти, аналізувати та реагувати на кіберзагрози, пов'язані з інсайдерською діяльністю в банках.

Інформаційне забезпечення банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів - це сукупність ресурсів, процедур та технологій, які використовуються для забезпечення конфіденційності, цілісності та доступності інформації, що обробляється системою. Це включає в себе різноманітні заходи та засоби для захисту інформації від несанкціонованого доступу, втрати, викриття чи зміни.

Ключовим аспектом інформаційного забезпечення банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів є інформаційна база, яка представляє собою сукупність даних, знань, та ресурсів, які система використовує для виявлення та аналізу потенційних кіберзагроз, пов'язаних з інсайдерською діяльністю в банку. Ця інформаційна база служить основою для прийняття рішень та виявлення аномалій у поведінці користувачів та системи. Ключовими складовими інформаційної бази є:

1. дані про користувачів, які включають в себе інформацію про ідентифікацію та атрибути користувачів, їхні облікові записи, ролі, рівень доступу та історію взаємодії з системою;

2. дані про події та транзакції, які включають інформацію про всі події, транзакції та інші активності, які відбуваються в банківській системі, з врахуванням даних про час, місце та особливості кожної події;

3. історія доступу, яка надає деталі про те, які користувачі мали доступ до певних ресурсів, часи та обсяги цього доступу;

4. інформація про конфігурацію системи, що представляє собою дані про налаштування системи, включаючи параметри безпеки, версії програмного забезпечення та конфігураційні параметри;

5. експертні знання та правила, тобто знання, яке вбудоване в систему, включаючи експертні правила та алгоритми, розроблені для виявлення аномалій та потенційних загроз;

6. моделі аномалій та машинного навчання, що представляють собою моделі, побудовані на основі машинного навчання, які використовуються для виявлення незвичайних патернів та аномалій в поведінці користувачів чи системи;

7. інформація про поточний стан системи, яка включає дані про стан різних компонентів системи, враховуючи поточні тривоги, відомості про підключені пристрої та інші параметри безпеки.

Інформаційна база допомагає експертній системі аналізувати, виявляти аномалії та реагувати на можливі кіберзагрози в реальному часі. Використання різноманітних даних та знань дозволяє системі ефективно оцінювати ризики та приймати інформовані рішення щодо безпеки.

Пропонуємо наступну структуру бази даних (рис. 3.32).

Структура даних про користувачів в банківській експертній системі виявлення кіберзагроз може включати різноманітні елементи, які дозволяють ідентифікувати, атрибутізувати та відстежувати активності користувачів. Тут є деякі загальні елементи, які можуть бути частиною такої структури:

– «Ідентифікатор користувача» – унікальний код або номер, який ідентифікує конкретного користувача в системі. Це може бути логін, ID або інша унікальна мітка;

– «Ім'я та прізвище» – особисті дані про користувача, які можуть включати його ім'я та прізвище для легшої ідентифікації;

– «Облікові дані» – інформація, пов'язана з обліковим записом користувача, така як пароль, методи аутентифікації та інші параметри безпеки;

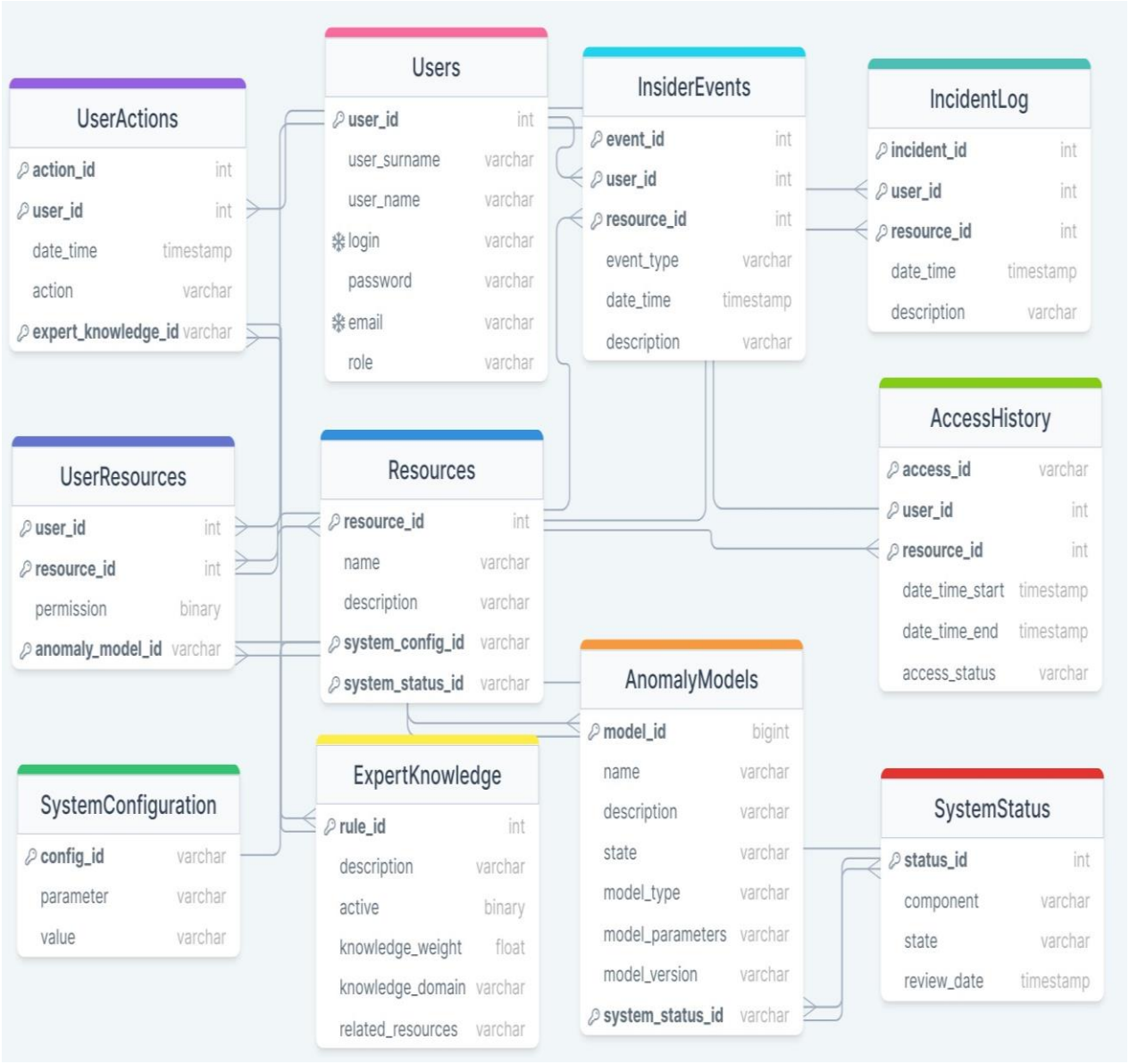


Рисунок 3.32 – Структура бази даних

– «Роль користувача» вказує на те, яку роль в системі виконує користувач. Наприклад, чи є він адміністратором, оператором чи звичайним користувачем;

– «Рівень доступу» визначає, до яких ресурсів, функцій чи даних має доступ користувач. Це може бути виражено числовим рівнем чи категорією;

– «Історія входів» – інформація про те, коли та де користувач увійшов в систему, включаючи дати та місця входу;

– «Доступ до ресурсів» – інформація про те, до яких конкретних ресурсів або об'єктів в системі має доступ користувач. Це може бути деталізовано для кожного окремого ресурсу;

– «Статус облікового запису» вказує на стан облікового запису, наприклад, чи він активний, заблокований або призупинений;

– «Дані про діяльність» – інформація про активності користувача в системі, така як взаємодія з додатками, внесення змін або інші дії.

Така структура даних про користувачів дозволяє системі експертного виявлення кіберзагроз ефективно аналізувати та виявляти незвичайні патерни або аномалії, що можуть вказувати на потенційні загрози безпеці. Збереження і моніторинг цих даних допомагає створити повну картину активності користувачів у системі.

Структура даних про події та транзакції в банківській експертній системі виявлення кіберзагроз повинна містити інформацію про різноманітні дії та події, що відбуваються в системі. Ці дані важливі для виявлення аномалій та потенційних загроз безпеці. Основні елементи структури можуть включати:

– «Ідентифікатор події/транзакції» – унікальний код або номер, який ідентифікує конкретну подію чи транзакцію в системі;

– «Дата та час» – інформацію про точний момент часу, коли відбулася подія чи транзакція;

– «Користувачі» – інформація про користувачів, які брали участь у події чи здійснили транзакцію, включаючи їхні ідентифікатори;

– «Тип події/транзакції» – категорія або класифікація, яка вказує на характер події чи транзакції (наприклад, вхід в систему, зміна даних, фінансова транзакція тощо);

– «Опис події/транзакції» – деталізований опис того, що саме відбулося під час події чи транзакції;

– «Ресурси» – інформація про ресурси, до яких було звернено під час події чи транзакції (наприклад, файли, бази даних, мережеві ресурси);

– «Результат» – інформація про результат чи стан системи після виконання події чи транзакції;

– «Місце події» – дані про локацію, де відбулася подія чи здійснилася транзакція (наприклад, IP-адреса, фізичне розташування);

– «Параметри транзакції» – у випадку, якщо це транзакція, то сюди входять інші параметри, що стосуються конкретної операції (наприклад, сума переказу, тип операції);

– «Інформація про безпеку» – записи щодо заходів безпеки, взятих під час події чи транзакції (наприклад, вірусні сканування, перевірка аутентифікації);

– «Контекст історії» – зв'язок події чи транзакції з попередніми подіями та контекстом історії.

Ця структура даних допомагає експертній системі аналізувати та відстежувати події, розглядати їх у відповідному контексті та виявляти аномалії, які можуть бути індикаторами можливих загроз безпеці в банківському середовищі.

Історія доступу в контексті банківської експертної системи виявлення кіберзагроз – це відображення того, які користувачі мали доступ до різних ресурсів системи, коли цей доступ відбувався, та яким чином він був здійснений. Історія доступу включає в себе інформацію про авторизований і неавторизований доступ, зміни рівнів доступу та інші відомості, які можуть бути важливими для виявлення незвичайних патернів та потенційних кіберзагроз. Структура історії доступу може містити наступні елементи:

– «Ідентифікатор доступу» – унікальний код або номер, що ідентифікує конкретний випадок доступу;

– «Ідентифікатор користувача» – унікальний ідентифікатор користувача, який отримав доступ;

– «Дата та час доступу» – інформація про точний момент часу, коли відбувався доступ;

– «Ресурс» – інформація про ресурс, до якого було звернено (наприклад, файл, база даних, додаток);

– «Тип доступу» вказує, чи був доступ авторизований чи неавторизований. Також може вказувати на тип доступу (наприклад, читання, запис, виконання);

– «Результат» – інформація про результат випадку доступу, наприклад, чи був успішним, чи спричинив помилку;

– «Місце доступу» – дані про локацію, з якої був здійснений доступ (наприклад, IP-адреса, фізичне розташування);

– «Деталі доступу» – додаткові відомості про сам доступ, такі як тип пристрою, використовувані агенти, параметри запиту тощо;

– «Інша метадані» – додаткова інформація, яка може бути корисною для аналізу, така як ідентифікатор сесії, номер транзакції, тощо.

Історія доступу надає адміністраторам та системам безпеки повний огляд того, яким чином користувачі взаємодіють з системою, і дозволяє вчасно виявляти аномальні або підозрілі дії, що може свідчити про потенційні загрози безпеці.

Інформація про конфігурацію системи включає в себе дані, які описують конфігурацію технічних аспектів системи, такі як параметри, налаштування, версії програмного забезпечення та інші важливі параметри, які визначають спосіб функціонування системи. Ця інформація важлива для забезпечення стабільності та безпеки системи. Структура об'єкту бази даних "Інформація про конфігурацію системи" може включати наступні елементи:

– «Ідентифікатор конфігурації» – унікальний код або номер, що ідентифікує конкретну конфігурацію системи;

– «Дата та час збереження конфігурації» – інформація про той час, коли була збережена інформація про конфігурацію;

– «Інформація про операційну систему» – версія операційної системи, тип архітектури, патчі та оновлення;

– «Інформація про апаратне забезпечення» – деталі про апаратні компоненти, такі як процесор, обсяг оперативної пам'яті, жорсткий диск та інші пристрої;

– «Версії програмного забезпечення» – інформація про версії встановленого програмного забезпечення, включаючи операційну систему, антивірусні програми, файєрволи та інші додатки;

– «Налаштування безпеки» – параметри та налаштування безпеки, такі як правила файєрволу, антивірусні налаштування та інші заходи безпеки;

– «Параметри мережі» – інформація про мережеві налаштування, включаючи IP-адресу, маску підмережі, шлюз, DNS-сервери та інші параметри мережі;

– «Ліцензійна інформація» – інформація про ліцензійні ключі та терміни дії ліцензій для встановлених програм;

– «Інші конфігураційні параметри» – додаткові параметри та конфігураційні налаштування, які можуть бути важливими для конкретної системи.

Ця інформація про конфігурацію системи допомагає забезпечити контроль над станом та функціональністю системи, а також сприяє вчасному виявленню змін, які можуть вказувати на потенційні проблеми або загрози.

Інформація про поточний стан системи включає в себе дані про актуальний стан різних компонентів та параметрів, що характеризують працездатність системи в реальному часі. Ця інформація важлива для моніторингу та виявлення аномалій або проблем в роботі системи. Структура об'єкта бази даних (БД) "Інформація про поточний стан системи" може включати такі елементи:

– «Дата та час останнього оновлення» – інформація про час, коли були отримані та оновлені дані про поточний стан системи;

– «Статус системи» – індикатор, який вказує на загальний стан системи, такий як "працює нормально", "проблеми", "відновлення", тощо;

– «Використання ресурсів» – дані про використання ресурсів, такі як CPU, RAM, дисковий простір та інші аспекти апаратної потужності;

– «Стан мережі» – інформація про стан мережі, включаючи доступність, пропускну здатність, пінги та інші параметри;

– «Активні процеси» – перелік активних процесів та їхні властивості, такі як ідентифікатори, використання ресурсів та інші;

– «Стан служб та додатків» – інформація про стан важливих служб та додатків, їхні версії, час їхньої роботи та інші параметри;

– «Інформація про події» – записи про останні події та активності в системі, такі як запуск процесів, помилки та інші важливі події;

– «Стан безпеки» – інформація про поточний стан заходів безпеки, включаючи антивірусний захист, стан брандмауера та інші аспекти;

– «Підключені пристрої» – інформація про пристрої, які підключені до системи, такі як USB-пристрої, мережеві пристрої та інші;

– «Інші параметри» – додаткові параметри та станові показники, які можуть бути важливими для конкретної системи.

Ця структура даних дозволяє ефективно відстежувати та аналізувати поточний стан системи, що є важливим для забезпечення її стабільності та безпеки.

Найважливішим компонентом інформаційної бази банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів є моделі аномалій. Вони використовуються для виявлення аномалій або незвичайних патернів в даних, наприклад, для виявлення підозрілих транзакцій чи несанкціонованого доступу. Структура об'єкту "Моделі аномалій виявлення кіберзагроз в результаті дій інсайдерів" може містити наступні ключові елементи:

– таблиця "Моделі аномалій" містить інформацію про різні моделі аномалій, які використовуються в системі для аналізу та виявлення невідповідностей та аномальних зразків в користувацькому поведінці чи системних діях. Така таблиця дозволяє ефективно управляти різними моделями аномалій, їхніми характеристиками та використанням у системі виявлення кіберзагроз;

– таблиця "Виявлені аномалії" містить інформацію про аномальні події, які були виявлені системою на основі моделей аномалій. Ця таблиця дозволяє системі зберігати та відстежувати інформацію про кожну виявлену аномалію, а також асоціювати її з конкретним користувачем, дією та моделлю аномалій, яка використовувалася для виявлення. Це важливо для подальшого аналізу, вдосконалення моделей та прийняття відповідних заходів безпеки;

– таблиця "Параметри моделі" дозволяє зберігати налаштування кожної моделі, що може включати в себе різні параметри, які визначають її поведінку. Ця таблиця важлива для динамічного управління параметрами моделей, що може бути корисним під час настройки та оптимізації системи виявлення аномалій. Зміни в параметрах можуть бути внесені під час експлуатації системи для покращення її ефективності та адаптації до змін в оточенні.

Елемент бази даних "Експертні знання та правила" для банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів може включати в себе різноманітні компоненти для зберігання експертних знань, правил і відомостей, які використовуються для аналізу та класифікації подій. Нижче подано ключові елементи, які можуть бути включені в такий об'єкт бази даних:

– таблиця "Експертні знання" містить інформацію про експертні знання, які використовуються для аналізу подій та виявлення аномалій. Вона дозволяє системі зберігати та організовувати експертні знання, які використовуються для визначення нормального та аномального поведінки в банківській експертній системі. Інформація в цій таблиці може бути використана для визначення експертних правил та алгоритмів виявлення кіберзагроз;

– таблиця "Правила виявлення" містить інформацію про правила виявлення, які визначають, як система аналізує події та визначає їх як аномальні чи небезпечні. Вона надає можливість експертній системі визначати, які події або дії вважаються аномальними чи потенційно загрозливими, а також які заходи повинні бути прийняті при виявленні таких аномалій;

– таблиця "Історія виявлень" служить для відстеження історії виявлених аномалій та подій в системі. Вона забезпечує зберігання історії аномалій та виявлених подій, що є важливим для подальшого аналізу, статистики та вдосконалення експертних моделей системи виявлення кіберзагроз.

Розробка структури інформаційної бази для експертної системи виявлення кіберзагроз внаслідок дій інсайдерів у банках є надзвичайно важливим завданням в контексті зростаючого обсягу кіберзагроз та потенційно серйозних наслідків для банківської сфери. Ця система повинна виявляти та відвертати загрози, забезпечуючи високий рівень безпеки та довіри. У даному дослідженні було надано інформацію про компоненти, структури та елементи, які складають інформаційну базу експертної системи. Важливо враховувати, що інформаційна база включає в себе такі компоненти, як інформація про користувачів, події та транзакції, експертні знання та правила, а також моделі аномалій для застосування машинного навчання.

Структура даних про користувачів передбачає детальний аналіз особистих та робочих аспектів працівників банку, враховуючи їхні повноваження та історію доступу. Дані про події та транзакції включають історію фінансових операцій, доступ до конфіденційної інформації та інші аспекти, що можуть слугувати підставою для виявлення аномалій. Інформаційна база також враховує історію доступу та поточний стан системи, надаючи можливість для ефективного моніторингу та виявлення незвичайної активності. Інформаційна база також включає дані про конфігурацію системи, що дозволяє ефективно взаємодіяти з різними компонентами та забезпечувати стабільність системи.

Одним із ключових аспектів є використання моделей аномалій та машинного навчання для виявлення та аналізу незвичайної активності. Ці моделі вбудовуються в інформаційну базу, навчаючись на основі історичних даних та виявляючи нові патерни та загрози. Таблиці, такі як "Моделі аномалій", "Виявлені аномалії", "Параметри моделі", "Експертні знання", "Правила виявлення" та "Історія виявлень", створюють структуровану основу для

зберігання та аналізу даних, що сприяє ефективному функціонуванню експертної системи.

Важливість протидії кіберзагрозам ініційованим інсайдерами у банках виявляється через можливі наслідки, такі як фінансові втрати, порушення конфіденційності даних, репутаційні ризики та загрози економічній та національній безпеці. Розробка ефективної експертної системи та відповідної інформаційної бази для неї є критичною для забезпечення стійкості та надійності банківської сфери перед різноманітними кіберзагрозами.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [290].

3.2.2 Підхід щодо розробки онтологічної моделі для формалізації інформаційного забезпечення фінансової установи

Проблема боротьби з інсайдерськими кіберзагрозами у банках полягає в тому, що вони виникають через дії осіб з легальним доступом до систем та інформації у банку. Це може включати зловживання довіри або неправомірне використання повноважень, призводячи до втрати конфіденційної інформації, фінансових збитків та системних ризиків. Сутність проблеми також включає соціальну інженерію, атаки, що використовують маніпулювання людьми для отримання конфіденційної інформації. Працівники банку можуть стати жертвами фішингу, обману чи інших соціально-інженерних методів, що може відкрити доступ до важливих ресурсів. Неадекватність управління правами доступу також є проблемою, де проблеми з управлінням можуть призвести до надання зайвих або непотрібних прав користувачам. Недостатня або надмірна аутентифікація та авторизація може відкривати можливості для інсайдерських атак. Брак ефективних систем моніторингу та аудиту ускладнює виявлення незвичайної чи підозрілої активності. Відсутність реакції на надто розгалужену або аномальну активність може зробити інсайдерські атаки важкими для виявлення.

Актуальність теми підтримується зростанням інсайдерських загроз, фінансовими наслідками, регуляторними вимогами та зростанням обсягів даних у банківському секторі, що підвищує ризик витоку та зловживання інформацією. Загальна архітектура та моделювання інсайдерських загроз стає критичною для ефективного виявлення та запобігання інсайдерським атакам.

Для боротьби з інсайдерськими кіберзагрозами необхідні ефективні стратегії управління доступом, моніторингу активності користувачів та застосування технологій, що спрямовані на розпізнавання аномалій та запобігання невірному використанню привілеїв. В якості такої стратегії є необхідність формалізації процесу виявлення інсайдерських кіберзагроз, що дозволить чітко розуміти, як формувати інформаційне забезпечення систем кіберзахисту. Застосування онтологічного підходу з цією метою сприятиме розробці якісної структури концепцій, об'єктів, відносин, та правил в даній предметній області.

Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках – це структурований опис та репрезентація концепцій, об'єктів, відносин, та правил в даній предметній області, яка дозволяє систематизувати та узгоджувати знання про інсайдерські загрози в контексті банківської безпеки. Ця модель використовується для формалізації та стандартизації розуміння експертами та системами конкретних аспектів, пов'язаних із виявленням інсайдерських загроз у банківському секторі. Такий опис робить можливим розуміння та обробку інформації комп'ютерами, що дозволяє їм ефективно взаємодіяти з даними в певній області.

Онтологія використовується для створення формалізованих моделей предметних областей, які полегшують обробку та обмін інформацією між системами. Такі онтології можуть використовуватися в різних галузях, таких як веб-пошук, інтелектуальні системи, обробка природної мови та інші області, де важлива концептуальна ясність та узгодженість в розумінні термінів і відносин.

Створення онтології для формалізації моделі виявлення інсайдерських кіберзагроз у банках вимагає врахування конкретних особливостей банківської

галузі та кіберзахисту. Ось деякі загальні вимоги та критерії для побудови такої онтології:

– ретельний аналіз особливостей банківської діяльності, процесів та інфраструктури, та визначення основних аспектів, які піддаються ризику внаслідок інсайдерських загроз;

– створення чітких визначень термінів, пов'язаних із загрозами та вразливостями, та здійснення їх узгодження з загальноприйнятими стандартами та визначеннями;

– розробка сценаріїв, які описують можливі дії інсайдерів, та визначення можливих шляхів атак та їхніх етапів;

– ідентифікація важливих атрибутів, що визначають стан систем та ідентифікацію загроз, та включення тих, які дозволяють виявляти аномальні або підозрілі дії;

– узгодженість інтеграції даних онтології з існуючими системами та стандартами в галузі кіберзахисту;

– визначення алгоритмів та правил для виявлення аномалій та інсайдерських дій, та розробка механізмів кореляції даних для визначення складних взаємозв'язків;

– створення системи класифікації для об'єктів та подій, пов'язаних із загрозами, та визначення метаданих для опису різних елементів онтології;

– розгляд можливостей включення динамічних аспектів та визначення зміни стану системи під час атаки;

– створення онтології таким чином, щоб вона була відкритою для розширення новими знаннями та даними.

Ці критерії допоможуть забезпечити створення ефективної та потужної онтології для виявлення інсайдерських кіберзагроз у банках. Розробка онтологічної моделі включає кілька ключових етапів:

1. визначення конкретної області банківської безпеки, на яку буде спрямована онтологічна модель, обсягу та мети моделі;

2. детальний аналіз різних бізнес-процесів банку, ідентифікація потенційних загроз в рамках цих процесів та врахування особливостей банківської галузі та її ризиків;

3. встановлення основних понять, які визначають предметну область (інсайдер, кіберзагроза, банківський процес і т. д.) та визначення відносин між цими поняттями;

4. створення онтологічних класів для представлення об'єктів і понять, таких як користувачі, системи, процеси тощо, а також визначення властивостей для класів, які вказують на їхні характеристики та взаємозв'язки;

5. впорядкування класів в ієрархію, щоб відображати спільні абстракції та специфікації, та забезпечення логічної та чіткої структури;

6. перевірка і узгодження моделі з існуючими стандартами безпеки та кіберзахисту з використанням відомих онтологічних мов чи стандартів, таких як OWL (Web Ontology Language) або RDF (Resource Description Framework);

7. визначення властивостей для опису стану об'єктів та систем, та врахування часових та просторових аспектів стану;

8. формулювання правил, які обмежують допустимі взаємодії між об'єктами в системі, а також визначення умов, за яких може виникнути інсайдерська загроза;

9. проведення тестів для перевірки коректності та ефективності моделі та здійснення валідації моделі на реальних чи симульованих даних;

10. підтримка гнучкості та здатності до оновлення моделі для включення нових загроз та висновків із досліджень;

11. розробка документації, яка пояснює структуру, правила та використання онтології, а також забезпечення ефективної комунікації між розробниками та користувачами онтології.

Ці етапи допомагають створити ефективну та гнучку онтологічну модель, що сприяє покращенню кібербезпеки в цій галузі.

Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках може включати в себе такі елементи:

– основні класи об'єктів та концепцій в галузі банківської безпеки, наприклад, "Інсайдер", "Користувач", "Система", "Транзакція" та інші;

– властивості класів, які вказують на їхні характеристики та атрибути. Наприклад, для класу "Інсайдер" може бути властивість "Рівень доступу";

– встановлення взаємозв'язків між класами. Наприклад, відносини між "Інсайдером" та "Транзакцією" можуть вказувати на можливість інсайдера впливати на фінансові операції;

– формалізація правил та обмежень, які визначають допустимі взаємодії між об'єктами та стан системи;

– визначення стану об'єктів та системи в різний час. Це важливо для виявлення аномалій та змін стану, що можуть свідчити про інсайдерські загрози;

– узгодження часових та просторових аспектів для визначення моменту виявлення та географічного розташування інсайдера;

– врахування інших аспектів безпеки, таких як методи аутентифікації, контроль доступу, шифрування тощо.

Класи онтологічної моделі представляють об'єкти, концепції та аспекти, що важливі для формалізації процесу виявлення інсайдерських кіберзагроз у банках. Нижче наведено детальний огляд можливих класів для такої моделі (Таблиця 3.12).

Таблиця 3.12 – Потенційні класи та їх властивості в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва класу	Характеристика класу	Властивості класу
Інсайдер	Описує особу, яка має легальний доступ до систем банку, але використовує цей доступ нелегально або шкідливо	Ім'я, роль в банку, рівень доступу тощо
Користувач	Загальний клас, що описує будь-якого користувача системи, включаючи інсайдерів та легітимних користувачів	Ім'я, ідентифікатор, роль, рівень доступу
Транзакція	Визначає операції або обміни даними, які відбуваються в банківській системі	Сума, тип транзакції, дата та час
Система	Представляє інформаційну та технічну інфраструктуру банку	Версія ПЗ, типи баз даних, технічні параметри
Аномалія	Описує будь-які незвичайні події або стани, які можуть свідчити про можливу інсайдерську загрозу	Час виявлення, характер аномалії, ступінь загрози
Заходи безпеки	Визначає заходи та політики, які застосовуються для запобігання та виявлення інсайдерських кіберзагроз	Тип заходу, термін дії, область застосування
Вразливість	Описує слабкі місця в системі, які можуть бути використані інсайдерами для здійснення атак	Опис вразливості, рівень критичності
Правила виявлення	Визначає правила та алгоритми для виявлення аномальних дій чи поведінки, які можуть свідчити про інсайдерську загрозу	Тип правила, умови виявлення
Запитання безпеки	Описує запитання, які можуть бути використані для перевірки легітимності користувача в процесі взаємодії з системою	Тип запитання, область застосування

Класи і їхні властивості взаємодіють між собою через визначені відносини, що дозволяє створити комплексну модель для виявлення інсайдерських кіберзагроз у банках. Також відносини визначають структуру та взаємодії між класами. При цьому важливо враховувати конкретні особливості банківської галузі та взаємодії між різними сутностями та подіями. Нижче наведено детальний огляд можливих відносин, які можуть існувати в такій моделі (Таблиця 3.13).

Таблиця 3.13 – Потенційні відносини між класами в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва відносин	Класи, між якими встановлюються відносини	Значення відносин
Має доступ	"Інсайдер" та "Система"	Визначає, які інсайдери мають доступ до конкретних систем в банку
Здійснює транзакцію	"Інсайдер" та "Транзакція"	Показує, на які транзакції можуть впливати інсайдери
Використовує правило виявлення	"Інсайдер" та "Правила виявлення"	Вказує, які правила виявлення використовуються для виявлення інсайдерської діяльності
Застосовує заходи безпеки	"Інсайдер" та "Заходи безпеки"	Показує, які заходи безпеки застосовуються для запобігання інсайдерським загрозам
Виявляє аномалію	"Система" та "Аномалія"	Показує, які аномалії в системі можуть свідчити про інсайдерські дії
Має рівень доступу	"Користувач" та "Система"	Визначає, які користувачі мають певний рівень доступу до системи
Взаємодіє з вразливістю	"Інсайдер" та "Вразливість"	Вказує, які вразливості можуть бути використані інсайдером для атаки
Здійснює запитання безпеки	"Користувач" та "Запитання безпеки"	Показує, які запитання безпеки використовуються для перевірки легітимності користувача

Правила та обмеження в онтологічній моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках визначають умови, обмеження та норми, які регулюють взаємодію між різними класами та об'єктами в системі. В таблиці 3.14 представлено детальний огляд можливих правил та обмежень.

Таблиця 3.14 – Правила та обмеження онтологічної моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва правила / обмеження	Опис правила / обмеження	Приклад правила / обмеження
Правила виявлення	Визначає умови та методи виявлення інсайдерських дій в системі	Якщо користувач проводить несподівано велику кількість транзакцій протягом короткого періоду, то система визначає це як потенційно підозрілу активність
Обмеження рівня доступу	Визначає, які ресурси та функціонал доступні різним рівням користувачів або систем	Інсайдерам обмежено доступ до критичних фінансових операцій
Аудит та логування	Визначає правила збору та зберігання журналів подій для аналізу та виявлення аномалій	Усі спроби доступу до конфіденційної інформації записуються в системному журналі
Обмеження використання заходів безпеки	Визначає обов'язкове використання конкретних заходів безпеки, таких як двофакторна аутентифікація чи шифрування	Усі користувачі повинні пройти двофакторну аутентифікацію для доступу до фінансових систем
Часові обмеження	Визначає правила та обмеження для доступу до системи в певні періоди часу	Користувачі з підозрілою активністю можуть бути обмежені в доступі під час некритичних годин
Обмеження аномалій	Визначає, які аномалії вважати нормальними та які є підозрілими	Пересилання великої кількості конфіденційної інформації на зовнішні адреси може викликати попередження
Обмеження вразливостей	Визначає правила для зменшення вразливостей системи та даних	Всі важливі патчі та оновлення мають бути встановлені в системі протягом певного періоду
Автоматичне реагування	Визначає автоматичні дії, які слід вжити у випадку виявлення підозрілої активності	Автоматична блокування акаунту при підозрілій аутентифікації

Визначені правила та обмеження взаємодіють у складі системи виявлення інсайдерських кіберзагроз, забезпечуючи безпеку та виявлення потенційно небезпечних дій у банківському середовищі.

Стан об'єктів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках відображає поточний статус та характеристики різних об'єктів в системі. Детальний огляд можливих аспектів стану об'єктів в такій моделі представлено в таблиці 3.15

Таблиця 3.15 – Характеристика станів об’єктів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва стану	Опис стану	Приклади властивостей
Інсайдер	Вказує на поточний статус інсайдера в системі, його активності та легітимності	– Рівень доступу (високий, середній, низький) – Стан легітимності (підозрілий, нормальний)
Користувач	Відображає стан та активність користувачів в системі банку	– Остання активність – Статус облікового запису (активний, заблокований) – Історія вхідних та вихідних транзакцій
Транзакція	Визначає поточний статус та характеристики фінансових транзакцій	– Сума транзакції – Час та дата проведення – Статус (успішна, відхилена, в очікуванні)
Система	Вказує на стан технічної інфраструктури та інформаційних систем банку	– Версія програмного забезпечення – Доступність системи – Статус безпеки (захищена, під загрозою)
Аномалія	Показує, чи виникла аномалія та як це може вплинути на безпеку системи	– Час виявлення – Тип аномалії (вихід за межі норми, атака, несподівана активність)
Заходи безпеки	Вказує на поточний статус застосованих заходів безпеки в системі	– Термін дії заходу безпеки – Активність (включений, виключений)
Вразливість	Показує ступінь небезпеки та статус виправлення вразливостей в системі	– Рівень критичності вразливості. – Дата патчу чи виправлення
Правила виявлення	Вказує на стан та ефективність правил для виявлення інсайдерських загроз	– Частота виявлення підозрілих подій. – Ступінь впевненості виявлення

Стан об'єктів може змінюватися в залежності від дій та подій в системі. Моніторинг та аналіз цих станів допомагає виявляти аномалії та потенційні загрози для банківської безпеки.

Часові та просторові аспекти визначають контекст виявлення інсайдерських кіберзагроз у банках та допомагають покращити ефективність системи безпеки. Їх характеристику запропоновано у таблиці 3.16.

Таблиця 3.16 – Часові та просторові аспекти в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва аспекту	Опис аспекту	Приклад аспект
Часові аспекти		
Час виявлення аномалій	Визначає, як швидко система може виявити аномалії та підозрілі активності	Певні аномалії можуть бути виявлені тільки після виявлення взірців поведінки протягом тривалого часу
Часові обмеження для заходів безпеки	Визначає, наскільки тривалим є застосування певних заходів безпеки та чи вони мають термін дії	Ліміти на період дії аутентифікаційних токенів для користувачів
Часові маркери та тайм-штампи транзакцій	Використовується для фіксації часу та порядку подій, щоб легше визначити хронологію та послідовність транзакцій	Кожна транзакція має тайм-штамп, який вказує час її виконання
Часові проміжки для аналізу поведінки	Визначає інтервали часу, протягом яких аналізується поведінка користувачів для виявлення аномалій	Система аналізує активність користувачів протягом останніх 30 днів
Просторові аспекти		
Географічне розташування користувачів	Визначає, з яких місць користувачі можуть отримувати доступ до системи та чи є це типовим для їхньої поведінки	Виявлення доступу із незвичайних географічних областей для конкретного користувача
Мережева топологія	Визначає, як об'єкти взаємодіють у мережевому середовищі та чи є це відповідно до типової поведінки	Виявлення незвичайних мережевих з'єднань, які можуть свідчити про атаку або нелегітимний доступ
Локації фізичних об'єктів	Визначає, де розташовані фізичні об'єкти, такі як сервери та дата-центри, та як це впливає на їх безпеку	Забезпечення фізичної безпеки дата-центрів для уникнення фізичних атак
Топологія систем та їхній зв'язок	Визначає, які системи взаємодіють між собою та як це впливає на загальну безпеку	Виявлення непередбачених з'єднань між системами, які можуть бути використані для атаки
Локації вразливостей	Визначає, де знаходяться вразливості в системі та як це впливає на потенційні загрози	Виявлення вразливостей у важливих компонентах системи та їх негайне виправлення

Поза часовими та просторовими аспектами, існує ряд інших важливих аспектів безпеки в онтологічній моделі для виявлення інсайдерських кіберзагроз у банках. Вони враховують важливі методи та стратегії для забезпечення безпеки в банківському секторі, щоб ефективно виявляти інсайдерські кіберзагрози. Їх характеристику наведено у таблиці 3.17.

Таблиця 3.17 – Характеристика інших аспектів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках

Назва аспекту	Опис аспекту	Приклад аспекту
Методи аутентифікації		
Однофакторна аутентифікація	Використання одного засобу аутентифікації, такого як пароль чи біометричні дані	Введення пароля для входу в банківський обліковий запис
Двофакторна аутентифікація	Використання двох різних методів аутентифікації для підтвердження ідентичності користувача	Комбінація пароля та одноразового коду, отриманого через SMS
Мультифакторна аутентифікація	Використання трьох чи більше факторів для підтвердження ідентичності	Пароль, відбиток пальця та RFID-карта
Контроль доступу		
Рівні доступу	Визначення рівнів доступу до різних ресурсів залежно від ролі користувача	Адміністратори мають повний доступ, клієнти — обмежений
Контроль прав доступу	Встановлення обмежень на доступ до конкретних операцій чи даних	Користувачі можуть переглядати баланс, але не мати права на внесення змін
Логічний та фізичний контроль	Забезпечення доступу до інформації як логічно, так і фізично	Фізичний доступ до серверних приміщень обмежений картками доступу
Шифрування		
Шифрування даних в спокої	Захист інформації в непередбачуваному стані, коли вона не використовується	Зберігання паролів у зашифрованому вигляді в базі даних
Шифрування даних в русі	Захист інформації під час передачі по мережі чи інших комунікаційних каналах	Використання протоколу HTTPS для зашифрованого обміну даними між клієнтом і сервером
Шифрування сховища	Захист інформації в базі даних чи інших сховищах даних	Зашифроване зберігання конфіденційних клієнтських даних
Інші аспекти безпеки		
Захист від атак	Включає в себе заходи для виявлення та запобігання різним видам кібератак, таким як DDoS атаки чи SQL-ін'єкції	Використання систем виявлення вторгнень (IDS) та витончених механізмів фільтрації трафіку
Захист від витоків інформації	Запобігання витокам конфіденційної інформації внаслідок атак або помилок	Використання Data Loss Prevention (DLP) систем
Автоматизоване виявлення інсайдерських загроз	Використання аналітики та систем виявлення аномалій для ідентифікації підозрілої активності	Моніторинг надмірного доступу до конфіденційних даних

Вирішення проблеми побудови онтологічної моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках є критичним завданням у сучасному контексті кібербезпеки. Онтологічні моделі стають важливим інструментом для представлення знань та взаємозв'язків в складних системах, таких як інформаційні технології банківських установ. Успішне вирішення цієї проблеми передбачає ретельне проектування та розробку онтологічної моделі, яка враховує специфіку банківського сектору. Моделювання процесів виявлення інсайдерських кіберзагроз є необхідним для адекватного відображення всіх можливих сценаріїв та взаємодій між різними елементами системи. Онтологічна модель повинна бути тісно пов'язана з бізнес-процесами та стратегіями банку. Вона повинна відображати не тільки технічні аспекти, але й брати до уваги правила та регуляції, яким підлягає банк. Онтологічна модель повинна бути здатною інтегруватися з існуючими системами без втрати ефективності та швидкості виявлення кіберзагроз, враховувати вимоги до безпеки та захисту конфіденційної інформації, забезпечуючи високий рівень захисту від несанкціонованого доступу, бути гнучкою та легко адаптовуватися до змін в банківському середовищі, включаючи технологічні оновлення та зміни в законодавстві.

Запропонована у статті онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках враховує всі ключові аспекти виявлення загроз, забезпечуючи узгодженість з бізнес-процесами та інтеграцію з існуючими системами. Результат опису елементів онтологічної моделі демонструє необхідність та доцільність впровадження комплексного підходу до виявлення та протидії інсайдерським кіберзагрозам у банківському секторі. Важливим завданням є не тільки побудова самої моделі, але й постійна підтримка та оптимізація її функціональності. Це вимагає командної роботи експертів із кібербезпеки, фахівців з області банківського бізнесу та інженерів знань, щоб забезпечити повноту та ефективність онтологічної моделі в контексті виявлення інсайдерських кіберзагроз.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [287].

3.3 Концепція стратегічного ребілдингу архітектоніки системи держфінмоніторингу на основі його конвергенції з системою кібербезпеки

3.3.1 Формування соціально-економічних профілів країн - жертв кіберзлочинів

Наслідки Четвертої промислової революції призвели до активного впровадження комп'ютерних технологій в усі сфери життєдіяльності людини. Розробка Розумних заводів, потужних кіберфізичних систем, Інтернету речей та послуг сприяли та продовжують сприяти активному економічному та соціальному розвитку багатьох країн світу. З іншого боку, масова комп'ютеризація та цифровізація вплинули на появу кіберзлочинності, яка за останнє десятиліття набула великих масштабів в розрізі країн та світу. Масові кіберзлочини в наш час здійснюються не тільки заради отримання фінансових вигід для окремих осіб, але й задля ненасильницького впливу на конкретні групи людей, компанії, уряди, цілі держави. Ознаки масовості та впливу на життєво важливі об'єкти інфраструктури країни для порушення їх функціонування або виведення з активного стану можуть ідентифікувати кібератаки як кібервійна. Хоча Smith і заперечує подібне ототожнення [288]. Але Lucas вважає здійснення масових кібератак однією з головних ознак кібервійн [289]. Не дивлячись на розбіжності у поглядах на ідентифікацію даного явища достовірним фактом є те, що найбільш потужні у світовому кіберпросторі країни світу, такі як США, Китай, Великобританія, Росія, Нідерланди, Франція, Німеччина, Канада, Японія та Австралія, застосовують його інструменти для виконання інколи зовсім немирних цілей [290].

Так, у 2016 році Росія втрутилася у проведення президентських виборів в США, що було підтверджено Департаментом внутрішньої безпеки та Офісом директора національної розвідки США [291]. У 2017 році була здійснена

масштабна кібератака із використанням шкідливих програм-вимагачів Petya (NotPetya) та WannaCry, які були націлені на різні компанії України, але потім вірус поширився на інші країни світу, в результаті чого постраждали великі компанії, такі як американська фармацевтична корпорація Merck, датська судноплавна компанія Maersk, Національна служба охорони здоров'я Великобританії, німецька логістична компанія DHL, австралійська шоколадна фабрика Cadbury та багато інших [292]. У 2019 році Об'єднані Арабські Емірати здійснили серію кібератак на своїх політичних опонентів, які приймали участь у проєкті, присвяченому організації заходів для стеження за бойовиками та терористами [293]. У 2020 році Індія здійснила серію масштабних кібератак у бік державних служб Пакистану, про що заявила газета Tribune [294]. Через вразливості у програмному забезпеченні Microsoft китайський підрозділ кібершпигунів зламав 30,000 американських організацій, що значно вплинуло на їх роботу [295]. У 2022 році Україна стала об'єктом військової агресії з боку Росії. Цьому передувала масова серія DoS-атак та атак програм-вимагачів, які були вчинені на український уряд 13-14 січня 2022 року [296]. Можна навести багато інших прикладів кіберзлочинів, але, не дивлячись на різницю в їх цілях та засобах досягнення, їх вплив на події та процеси в різних країнах є вагомий.

Чому одні країни стають частіше жертвами кіберзлочинів, а інші не представляють жодного інтересу для масових кібератак, шпигунства, тероризму чи інших форм кібервійни? Які фактори сприяють зниженню зацікавленості кіберзлочинців та підвищують захисні резерви для протидії даного явища? Дане дослідження спрямоване на отримання відповідей на ці питання. З цією метою сформуємо декілька гіпотез, для доведення або відхилення яких будуть проведені аналітичні розрахунки в даній статті, які дозволять сформувати профайли країн-жертв кіберзлочинів на базі найважливіших показників соціально-економічного розвитку. Першою гіпотезою є те, що країни, які є найпотужнішими країнами світу та які є ініціаторами кіберзлочинів також виступають жертвами більше, ніж ті, які мають слабкий вплив на світовій арені. Іншою гіпотезою є те, що рівень соціально-економічного розвитку країн може

бути опосередкованою мотивацією кіберзлочинців для масових кібератак. Доведення запропонованих тверджень потребують застосування різних аналітичних методів. Для вирішення першого питання доцільно утворити групи країн в залежності від впливу різної кількості спрямованих на них кібератак. Формування висновків за другою гіпотезою можливі тільки за умови утворення профайлів на основі ключових індикаторів, які характеризують соціально-економічний розвиток країн.

Для проведення дослідження було обрано два набори даних. Один із них використовувався для формування кластерів країн в залежності від рівня виявлених кіберзлочинів, спрямованих на них. Джерелом даних є ресурс Лабораторії Касперського [297]. Другий набір даних було сформовано із індикаторів, які характеризують соціально-економічний рівень розвитку країн з урахуванням їх впливу на макро- та глобальні процеси. Це дозволило провести аналіз потенційної привабливості для кібершахраїв та виявити ті напрямки, які потребують уваги з боку міжнародних організації та уряду для протидії кіберзлочинності.

Перший набір даних було сформовано для 93 країн світу, який представляє собою обсяги трьох видів кіберзлочинів за місяць за період з 21.04.23 по 20.05.23. До першого виду було обрано кількість шкідливих програм та вірусів, знайдених із використанням антивірусів “Mail Anti-Virus” (MAV). Цей вибір обґрунтовується тим, що фішингові кібератаки із використанням поштових сервісів займають перше місце серед інших видів злочинів за 2022 рік (Statista, 2023). На рисунку 3.33 представлена карта розповсюдження даного виду кіберзлочинів, побудована на основі аналізованих показників. Найбільш атакованими країнами є Іспанія, Мексика, Туреччина, В’єтнам, Італія, Об’єднані Арабські Емірати, Німеччина, Бразилія, Колумбія та Малайзія. Найменш атакованими є Норвегія, Монголія, Киргизстан, Люксембург, Нікарагуа, Руанда, Нова Зеландія, Швеція, Данія та Ефіопія.

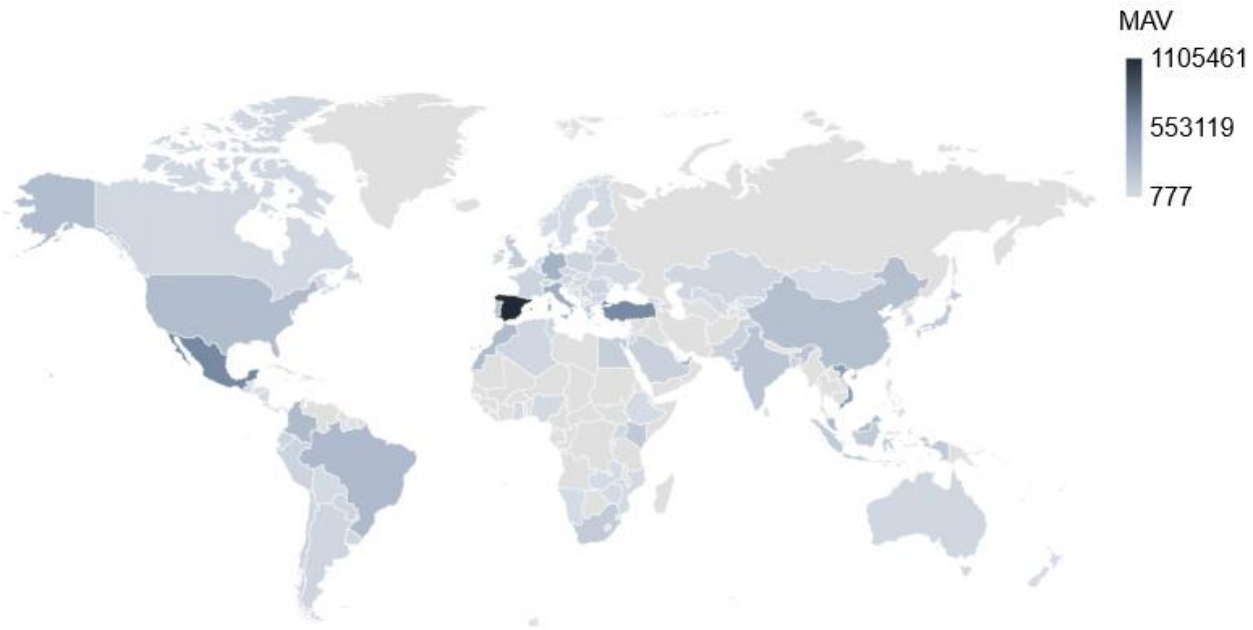


Рисунок 3.33 – Карта виявлення шкідливих програм та вірусів, розповсюджених через поштові сервіси

Джерело: складено на основі [261]

Другим видом кіберзлочину було обрано мережеві кібератаки, які були виявлені системою “Intrusion Detection Scan” (IDS). Якщо перший вид кіберзлочинів направлений конкретно на цільового користувача, то другий вид має більш шкідливі наслідки, оскільки відбувається ураження цілої мережі, що призводить до порушення роботи цілої компанії. Мета здійснення такого злочину – завдання масової шкоди якомога більшій кількості користувачів державного та корпоративного сектору. Мережеві атаки призводять до виникнення простоїв в компаніях, втрат великих обсягів даних, та, як наслідок, збільшення фінансових збитків. Країнами, які стали ціллю для такого виду кіберзлочинів, є Китай, США, Бразилія, Мексика, В’єтнам, Франція, Індія, Індонезія, Німеччина та Іспанія (рисунок 3.34). Найменш атакованими є Норвегія, Руанда, Албанія, Зімбабве, Грузія, Нова Зеландія, Гватемала, Монтенегро, Замбія та Кіпр.

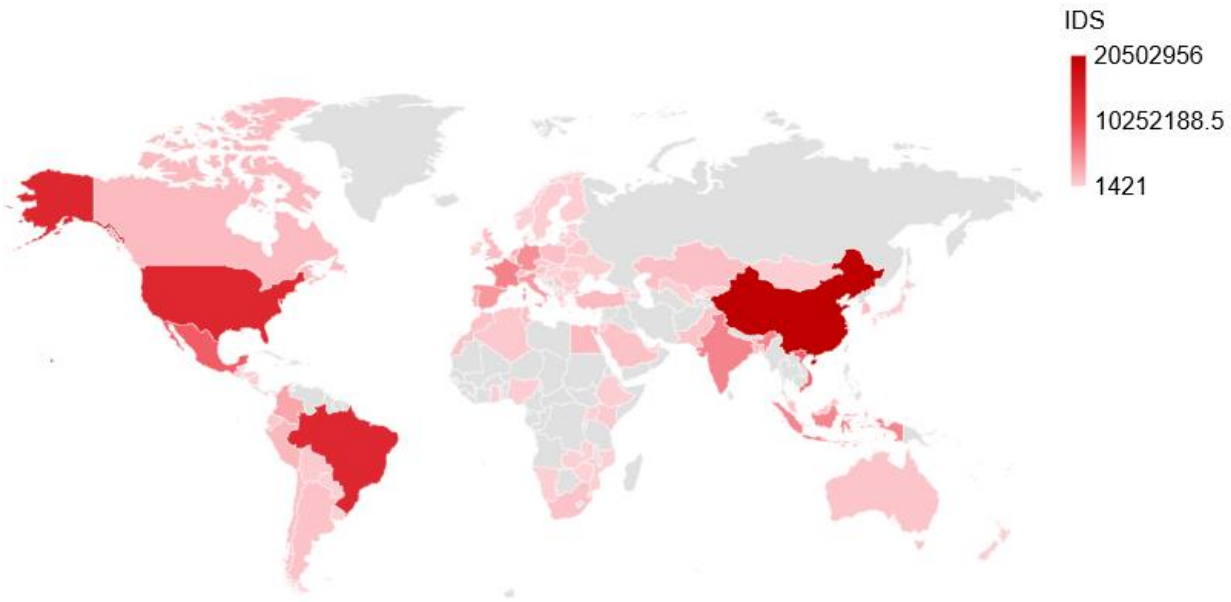


Рисунок 3.34 – Карта виявлення мережевих атак

Джерело: складено на основі [261]

Рисунок 3.35 – Карта виявлення вразливостей в системах

Джерело: складено на основі [261]

Вразливості у програмному забезпеченні, комп'ютерах та мережах за часту сприяють кіберзлочинцям проводити більш активні кібератаки та порушувати безпеку різних видів користувачів. Такі загрози виникають завдяки недосконалому програмуванню та неправильній конфігурації маршрутизаторів, серверів додатків, веб-серверів, брандмауерів та інших технічних та програмних засобів. Для їх аналізу було обрано кількість вразливостей у інформаційних системах ("Vulnerability" – VUL), які виявляються за допомогою програм-

сканерів. США, Німеччина, Франція, Бразилія, Італія, Японія, Іспанія, В’єтнам, Канада та Індія – це топ-10 країн, які зазнали найбільшої кількості атак спрямованих на виявлення слабких місць в інформаційних системах (рисунок 3.35). Нікарагуа, Монтенегро, Грузія, Вірменія, Уругвай, Фінляндія, Пакистан, Кіпр, Киргизстан та Монголія в найменшій мірі зіткнулися із кіберзлочинами даного типу.

Аналіз базових статистик обраних видів кіберзлочинів, представлений в Таблиці 3.18, свідчить про те, що існує велика різниця між обсягом кібератак для різних країн. Так, користувачі деяких країн можуть практично не зазнавати кібервторгнень через поштові сервіси, мережеві атаки або вразливості системи, про що свідчить їх мінімальне значення, яке в тисячі-десятки тисяч разів менше максимального. З іншого боку, ряд країн зазнають жорстоких кібератак, про що свідчать колосальні максимальні значення кількості інцидентів. Розраховані показники медіани, середнього значення, асиметрії та ексцесу свідчать про нерівномірність розподілу кількості кіберзлочинів. Можна зробити висновок, що є ряд країн, які є прямою цільовою аудиторією для кіберзлочинців, а є країни, які або мають значні ресурси для протидії, або не є привабливими для кібервійн.

Таблиця 3.18 – Базові статистики, визначені для трьох видів кіберзлочинів

Статистичні індикатори	MAV	IDS	VUL
Mean	92015.30	1500464.72	20193.98
Mode	–	–	–
Standard Error	16935.15	330862.77	4210.08
Standard Deviation	163316.68	3190725.02	40600.58
Kurtosis	17.30	17.53	11.64
Skewness	3.68	3.92	3.23
Minimum	777.00	1421.00	72.00
First quartile	7920.00	110523.00	1340.00
Median	31154.00	363228.00	3315.00
Third quartile	91051.00	1099658.00	15018.00
Maximum	1105461.00	20502956.00	227940.00
Sum	8557423.00	139543219.00	1878040.00
Count	93.00	93.00	93.00
Confidence Level (95.0%)	33634.67	657122.02	8361.59

Для виявлення характеристик, за якими можна ідентифікувати привабливість країни для кіберзлочинців, було обрано ряд індикаторів соціально-економічного розвитку за 2022 рік для 93 країн світу. В першу чергу було обрано National Cyber Security Index (NCSI), який дозволяє оцінити рівень країни протидіяти кіберзагрозам [298]. Високий ступінь національної кібербезпеки дозволяє формувати потужну базу захисту на основі правового, інформаційного, технічного, програмного, організаційного та інших видів забезпечення системи безпеки. Це повинно сприяти зниженню привабливості країни для масових кібератак. Оскільки кіберзлочини в наш час використовуються для розповсюдження кібертероризму, то вибір індикатора Global Terrorism Index (GTI) дозволить виявити вплив країни на рівень глобального тероризму в цілому [299]. Тобто країни із найвищим рівнем тероризму можуть бути найбільшими жертвами масових хакерських атак або їх ініціаторами, тоді як країни з найнижчим впливом навпаки не стануть їх ціллю. Важливим для формування профайлу щодо потенційної привабливості для кіберзлочинців є розуміння обставин щодо стану злочинності всередині країни, що вимірює Crime Index, CI [300]. Він дозволяє оцінити внутрішню ситуацію формування умов сприятливих для розвитку та підтримки різного роду злочинів для конкретної країни. Оскільки сьогодні зростає популярність Darknet і більшість кримінальних дій відбувається із використанням комп’ютерних технологій, то аналіз даного індикатора дозволить оцінити як внутрішнє середовище сприяє формуванню умов для підтримки кіберзлочинності, що може перетворювати країну не тільки на її жертву, але й на активного кібертерориста. На імідж країни в кіберпросторі може впливати й рівень корупції, яка формує відповідну площину для легалізації коштів, незаконного перерозподілу грошових потоків, здійснення порушень у законодавстві, тощо. Для аналізу даної характеристики було обрано Corruption Perceptions Index (CPI) [301].

На формування соціально-економічного профілю країни впливає рівень його економічної свободи, який дозволяє вимірювати взаємовідносини між різними сферами економіки: державними фінансами, бізнесом, податками,

інвестиційною та податковою сферами, торгівлею, чесністю уряду та ефективністю судової системи, тощо. Як правило, економічна складова є драйвером розвитку науково-технічного прогресу, що впливає на створення відповідного кіберсередовища окремої країни. Тому для аналізу у даній площині було вибрано Index of Economic Freedom, IEF [302]. Окрім економічного благополуччя важливими є задоволеність населення від якості сфери здоров'я, освіти, мистецтва, культури, навколишнього середовища, можливостей забезпечення працею та психологічної підтримки. Оцінювання цих аспектів можливе за допомогою Happiness Index, HI [303]. Найбільш щасливі країни у порівнянні із менш щасливими можуть приваблювати кіберзлочинців саме для отримання фінансових вигід від такого роду злочинів. Life Expectancy at Birth (LE) є індикатором, який характеризує рівень соціально-економічного розвитку країн. Найвищі його значення відповідають економічно розвиненим країнам, найнижчі – тим, що є найменш розвиненими [304]. Останньою обраною характеристикою є рівень демократії, який дозволяє оцінити рівень громадянських та політичних свобод, що викликають повагу з боку уряду країни. Для цього використовується Democracy Index (DI) [305]. Наявність або відсутність таких прав та свобод серйозно впливає на формування несприятливого середовища для стійкого соціально-економічного розвитку країни, що також може викликати певну зацікавленість для кіберзлочинців.

Перелічені індикатори було обрано для 93 країн світу за 2022 рік. Результати аналізу їх базових статистик наведені у Таблиці 3.19. В цілому спостерігається невеликий дисбаланс серед даних, про що свідчать значення таких показників, як Mean, Minimum, Maximum, First quartile, Third quartile, Median, але це пояснюється тим, що до обраного набору увійшли країни із різним ступенем соціально-економічного розвитку. Значення ексцесу та асиметрії свідчать, що більшість даних є наближеними до нормального розподілу та прийнятними для подальшого аналізу. Є декілька викидів по країнам для Happiness Index та Life Expectancy at Birth, що критично не вплине на подальші результати аналізу. Для таких індикаторів, як Crime Index, Global Terrorism Index

та Corruption Perceptions Index спостерігається те, що більшість країн входять до 3-го та 4-го квартилів, як для інших, навпаки, до 1-го та 2-го. Це пов’язано із тим, що перелічені показники є за своїм змістом дестимуляторами, а інші – стимуляторами, що потрібно врахувати в процесі нормалізації та присвоєння рейтингу.

Таблиця 3.19 – Базові статистики, визначені для показників соціально-економічного розвитку

Статистичні індикатори	NCSI	CPI	DI	HI	LE	GTI	IEF	CI
Mean	59.5870	49.3548	6.1411	5.8568	74.1943	2.1476	64.0323	43.3312
Mode	59.7400	36.0000	7.9700	4.5160	–	0.0000	74.4000	46.1000
Standard Error	2.2611	1.9753	0.2248	0.1076	0.7185	0.2437	1.0954	1.4213
Standard Deviation	21.8056	19.0495	2.1680	1.0375	6.9287	2.3506	10.5637	13.7063
Kurtosis	-0.7821	-0.9355	-0.8826	-0.0889	0.0707	-0.3215	-0.3272	-0.7468
Skewness	-0.3059	0.4706	-0.3728	-0.4704	-0.6294	0.8727	-0.2389	0.0851
Minimum	9.0900	19.0000	1.9400	2.9950	52.6760	0.0000	33.1000	15.1000
First quartile	41.5600	36.0000	4.5500	5.1730	70.2300	0.0000	55.7000	32.1000
Median	62.3400	45.0000	6.4500	6.0220	74.2560	1.2430	65.1000	45.4000
Third quartile	76.6200	63.0000	7.9500	6.4800	80.8756	4.1060	71.8000	53.7000
Maximum	94.8100	90.0000	9.8100	7.8210	84.4456	8.2330	84.4000	76.1000
Count	93	93	93	93	93	93	93	93
Confidence Level (95.0%)	4.4908	3.9232	0.4465	0.2137	1.4270	0.4841	2.1756	2.8228

Таким чином, сформовано два набори даних для проведення аналізу профілів груп країн, які виступають жертвами внаслідок здійснення кібератак через поштові сервіси, мережі та вразливості інформаційних систем.

Методологія дослідження соціально-економічних профайлів країн, які є жертвами кіберзлочинів здійснювалася в три етапи. Реалізація першого пов’язана із проведенням попередньої обробки даних, визначенням наявності чи відсутності мультиколінеарності між трьома видами кіберзлочинів та у проведенні стандартизації значень спостережень. Другий етап пов'язаний із кластеризацією країн, яка проводиться, виходячи з кількісного значення тих

видів кіберзлочинів, які не є мультиколінеарними. Також тут передбачена перевірка узгодженості кластерів за допомогою Silhouette методу. Третій етап необхідний для виявлення соціально-економічних закономірностей, властивих для визначених груп країн, який реалізується за допомогою асоціативного аналізу.

Перший етап дослідження полягав у здійсненні попередньої обробки вхідних даних. Оскільки вони збиралися вручну, то необхідність у обробці пропущених значень була відсутньою. Також дані не потребували дослідження на аномальність, оскільки у нашому випадку наявність таких спостережень свідчить про надмірність кібератак у бік даної країни.

Для реалізації кластерного аналізу обов'язково провести перевірку на мультиколінеарність та здійснити стандартизацію даних. Стандартизація дозволяє прибрати середнє значення та збільшити масштаб до значення дисперсії. Дану процедуру було проведено за формулою (3.10):

$$x_{ij}^{scaled} = \frac{x_{ij} - \overline{x_j}}{\sigma_j}, \tag{3.10}$$

де x_{ij}^{scaled} – стандартизоване значення j–th виду кіберзлочину в розрізі i–th країни;

x_{ij} – фактичне значення j–th виду кіберзлочину в розрізі i–ї країни;

$\overline{x_j}$ – середнє значення вибірки для j–th виду кіберзлочину;

σ_j – стандартне відхилення вибірки для j–th виду кіберзлочину.

Для перевірки даних на мультиколінеарність застосовувався алгоритм Farrar–Glauber, який передбачає розрахунок Chi-squared за формулою (3.11):

$$\mathrm{X}^2 = -\left((n-1) - \frac{2m+5}{6}\right) \times ln|R|, \tag{3.11}$$

де X^2 – розраховане значення Chi-squared;

n – кількість спостережень в масиві змінних, яке дорівнює 93 країні;

m – кількість пояснювальних змінних, яке дорівнює 3 видам кіберзлочинів;

$|R|$ – визначник матриці, яка формується з попарних коефіцієнтів кореляції, тобто:

$$R = \begin{pmatrix} 1 & r_{12} & r_{13} \\ r_{21} & 1 & r_{23} \\ r_{31} & r_{32} & 1 \end{pmatrix}, \tag{3.12}$$

де r_{kj} – значення коефіцієнтів кореляції між парами пояснювальних змінних, які відповідають досліджуваним видам кіберзлочинів ($k = 1 \div 3$; $j = 1 \div 3$), яке розраховується за формулою (3.13):

$$r_{kj} = \frac{\sum_{i=1}^{n}\left(\left(x_i^k - \overline{x^k}\right)\left(x_i^j - \overline{x^j}\right)\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i^k - \overline{x^k}\right)^2 \sum_{i=1}^{n}\left(x_i^j - \overline{x^j}\right)^2}}. \tag{3.13}$$

Розраховане значення Chi-squared порівнюється із критичним при $\frac{1}{2}m(m-1)$ – ступенів вільності та відповідному рівню значущості α. Якщо $X^2 > X_{cr}^2$, то в масиві змінних існує мультиколінеарність і перевірку потрібно продовжити далі, в іншому випадку мультиколінеарність відсутня і перевірка не проводиться.

Для подальшого дослідження обчислюється критерій Фішера за формулою (3.14), який дозволяє визначити корельованість окремого фактору з іншими:

$$F_k = (a_{kk} - 1) \times \frac{(n-m)}{(m-1)}, \tag{3.14}$$

де F_k –значення критерія Фішера, розраховане окремо для кожної з трьох змінних;

a_{kk} – діагональний елемент матриці, оберненої до матриці R. Розраховане значення критерія Фішера порівнюється із критичним $F_{cr}(\alpha, k_1, k_2)$, де α – відповідний рівень значущості, $k_1 = n - m$ та $k_2 = m - 1$. Якщо $F_k > F_{cr}$, то відповідна змінна корелює з іншими. В протилежному, вона не корелює з іншими.

Далі розраховуються частинні коефіцієнти кореляції за формулою (3.15), які показують тісноту зв'язку між двома змінними без врахування впливу інших змінних:

$$r_{kj}^{*} = \frac{-a_{kj}}{\sqrt{a_{kk} a_{jj}}}, \tag{3.15}$$

де r_{kj}^{*} – значення частинних коефіцієнтів кореляції між парами пояснювальних змінних, які відповідають досліджуваним видам кіберзлочинів ($k = 1 \div 3; j = 1 \div 3$);

a_{kj}, a_{jj} – відповідні елементи матриці, оберненої до матриці R. Якщо розраховані значення наближаються до 1 або -1, то це свідчитеме про наявність тісного кореляційного зв'язку між змінними. Для отримання уточненого висновку можна скористатися критичними значеннями $r_{cr}(\alpha, v)$, отриманими з таблиці Fisher–Yates, де α – відповідний рівень значущості, $v = n - l - 2$, де l – число виключених величин у випадку частинної кореляції, n – кількість спостережень.

На останньому кроці розраховується критерій Стьюдента за формулою (3.16) для перевірки статистичної значущості частинних коефіцієнтів кореляції:

$$t_{kj} = \frac{r_{kj}^{*}\sqrt{n - m}}{\sqrt{1 - {r_{kj}^{*}}^{2}}}. \tag{3.16}$$

Отримані значення критерія Стьюдента порівнюють із його критичним значенням $t_{cr}(\alpha, k)$, де α – відповідний рівень значущості, $k = n - m$. Якщо $|t_{kj}| > t_{cr}$, то кореляційна залежність між змінними є статистично значущою, в іншому випадку залежність не є статистично значущою.

На другому етапі дослідження було здійснено кластерний аналіз за допомогою методу k-means та перевірку узгодженості кластерів за допомогою Silhouette техніки. K-means clustering є одним з методів Data Mining, який дозволяє проводити розбиття набору даних на певну кількість груп (кластерів), за умови, що кожне спостереження є близьким до відповідного кластерного центроїду (середнього значення). Тобто ціллю кластерного аналізу є мінімізація дисперсії всередині кластеру та знаходження оптимальної відстані спостереження до середини групи, що можна представити у вигляді формули (3.17):

$$\arg\min_{C} \sum_{i=1}^{k} \sum_{x_p \in C_i} \left|\left| x_p - \mu_i \right|\right|^2 = \arg\min_{C} \sum_{i=1}^{k} |C_i| \, Var C_i, \tag{3.17}$$

де $(x_1, x_2, \dots, x_p)$ – набір змінних, кожен з яких представляє собою d – мірний вектор з n – спостережень в кожному;

μ_i – центроїд i-th кластеру, який визначається за формулою (3.18):

$$\mu_i = \frac{1}{|C_i|} \sum_{p \in C_i} x_p, \tag{3.18}$$

де $C = \{C_1, C_2, \dots, C_k\}$ – набори змінних, які відповідають i-th кластеру при $i = 1 \div k$. При цьому належність спостережень i-th кластеру зазначається як формула (3.19):

$$\mathrm{C}_i = \{p | if\ x_p\ belongs\ to\ the\ i^{th}\ cluster\}. \tag{3.19}$$

Silhouette є методом перевірки узгодженості даних у кластерах за допомогою візуалізації, який було запропоновано в [306]. Дана техніка передбачає визначення коефіцієнту silhouette для всіх зразків з урахуванням середньої відстані всередені кластеру та середньої відстані до найближчого кластера за формулою (3.20):

$$\begin{cases} s(i) = \dfrac{b(i) - a(i)}{max\{a(i), b(i)\}}, if\ |C_I| > 1, \\ s(i) = 0, if\ |C_I| = 1 \end{cases} \tag{3.20}$$

де $s(i)$ – a silhouette value for i-th observation from the data set;

$a(i)$ – середня відстань між i-th та іншими спостереженнями у кластері, яка розраховується за формулою (3.21);

$b(i)$ – середня відстань від i-th спостереженням у кластері до інших спостережень інших кластерів, яка розраховується за формулою (3.22);

$|C_I|$– множина спостережень одного кластера:

$$a(i) = \frac{1}{|C_I| - 1} \sum_{j \in C_I, i \neq j} d(i, j), \tag{3.21}$$

$$b(i) = \min_{J \neq I} \frac{1}{|C_J|} \sum_{j \in C_J} d(i, j), \tag{3.22}$$

де $d(i, j)$ – відстань від i-th спостереження до j-th.

Для ідентифікації результатів необхідно, щоб $-1 \leq s(i) \leq 1$. Якщо значення silhouette наближатиметься до 1, то це свідчитиме про групування даних належним чином. Якщо його значення буде близьким до 0, то дані

знаходяться на межі двох кластерів і їх важко віднести до певного кластеру. Якщо silhouette наближатиметься до -1, до дані належать іншому кластеру.

Третій етап дослідження потребує попередньої обробки даних, які відповідають соціально-економічним факторам. Спочатку їх потрібно нормалізувати за формулою (3.23), якщо показник є стимулятором, та формулою (3.24), якщо показник є дестимулятором:

$$x'_{ij} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}}, \tag{3.23}$$

$$x'_{ij} = \frac{x_j^{max} - x_j}{x_j^{max} - x_j^{min}}, \tag{3.24}$$

де x'_{ij} – нормалізоване значення i-th спостереження для j-th змінної;

x_j^{min} та x_j^{max} – відповідно, мінімальне та максимальне значення для j-th змінної.

Для реалізації асоціативного аналізу є потреба у заміні даних на рейтингові групи. Це пов’язані із невеликою кількістю спостережень та великою варіацією їх значень. Для цього скористуємося формулою (3.25):

$$x_{ij}^{*} = \begin{cases} x_{ij} = 1, if\ 0 < x_{ij} \leq 0.25 \\ x_{ij} = 2, if\ 0.25 < x_{ij} \leq 0.50 \\ x_{ij} = 3, if\ 0.5 < x_{ij} \leq 0.75 \\ x_{ij} = 4, if\ 0.75 < x_{ij} \leq 1 \end{cases}, \tag{3.25}$$

де x_{ij}^{*} – рейтингове значення i-th спостереження для j-th змінної;

1 – рейтингове значення, яке відповідає низькому значенню показника, що входить в перші 25%;

2 – рейтингове значення, яке відповідає нижче середньому значенню показника, що входить до другого квартилю значень вибірки;

3 – рейтингове значення, яке відповідає вище середньому значенню показника, що входить до третього квартилю значень вибірки;

4 – рейтингове значення, яке відповідає високому значенню показника, що входить до четвертого квартилю значень вибірки.

Даний етап дослідження полягає у проведенні асоціативного аналізу, який дозволить виявити правила причин з'єднання аналізованих індикаторів для певного кластеру країн. Це сприятиме формуванню профайлу країн-жертв кіберзлочинів на основі факторів їх соціально-економічного розвитку, що допоможе розуміти мотивацію злочинців щодо здійснення цілеспрямованих кібератак. Для реалізації даного виду аналізу використовується алгоритм Apriori, який базується на виявленні частотних множин даних в наборі, що дозволить сформувати перелік типових факторів для кластерів країн. Також його побудова на асоціації та кореляції сприятиме виявленню причинно-наслідкових зв'язків в рамках окремої групи країн. Для виявлення асоціативних правил визначаються наступні показники за формулою (3.26):

$$supp(X \Longrightarrow Y) = \frac{F(X,Y)}{N},$$

$$conf(X \Longrightarrow Y) = \frac{F(X,Y)}{F(X)}, \tag{3.26}$$

$$lift(X \Longrightarrow Y) = \frac{S(X \Rightarrow Y)}{S(X) \times S(Y)},$$

де $supp\,(support)$ – показник, який характеризує частоту появи набору елементів X та Y;

$conf\ (confidence)$ – показник, який дозволяє визначити відсоток елементів, які задовольняють умові елементу X, які також задовольняють й умові елементу Y;

$lift$ – показник, який демонструє рівень зацікавленості в елементі Y за умови існування зацікавленості в елементі X.

Якщо $lift(X \Rightarrow Y) = 1$ – кореляція в наборі даних відсутня. Якщо $lift(X \Rightarrow Y) > 1$ – кореляція позитивна, тобто ймовірність сумісної реалізації елементів X та Y є дуже високою. Якщо $lift(X \Rightarrow Y) < 1$ – кореляція від'ємна, тобто сумісна реалізація елементів X та Y є мало ймовірною. Оскільки розрахунки асоціативного аналізу відбувалися у аналітичному пакеті STATISTICA, то позначення показника $lift$ відбувалося як $correlation$.

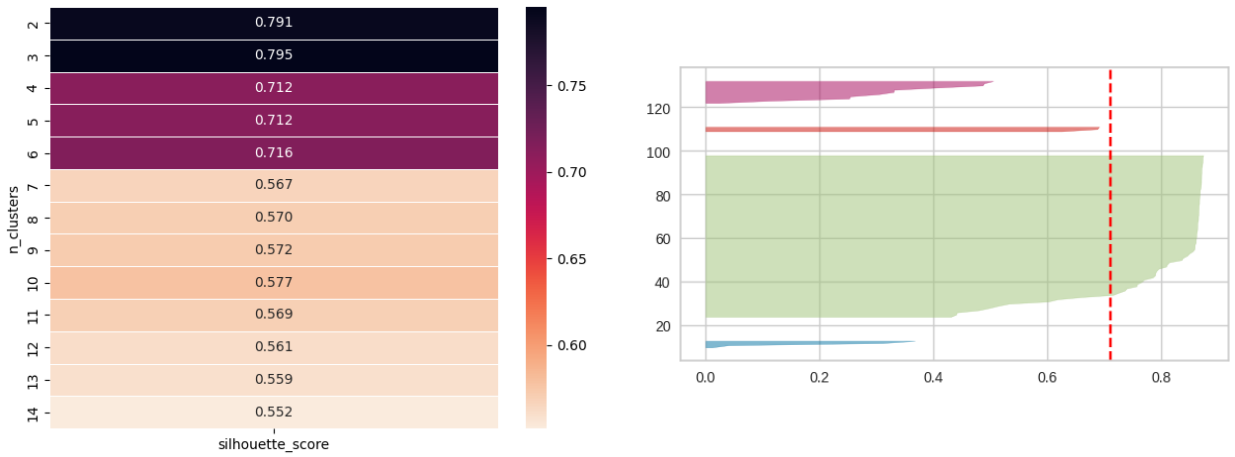
Таблиця 3.20 – Результати тесту Фаррара–Глобера

Розрахунковий критерій	Розрахункове значення	Знак нерівності	Критичний критерій	Критичне значення	Результати перевірки
X^2	81.6434	>	X^2_{cr}	7.8147	Присутня мульти-колінеарність
F_{MAV}	16.8229	<	F_{cr}	19.4846	Немульти-колінеарний
F_{IDS}	39.5230	>			Мульти-колінеарний
F_{VUL}	42.7960	>			Мульти-колінеарний
$r_{MAV,IDS}$	0.2040	<	r_{cr}	0.2050	Немульти-колінеарний
$r_{MAV,VUL}$	0.2781	>			Мульти-колінеарний
$r_{IDS,VUL}$	0.5702	>			Мульти-колінеарний
$t_{MAV,IDS}$	1.9767	<	t_{cr}	1.9867	Статистично значущий
$t_{MAV,VUL}$	2.7466	>			Статистично незначущий
$t_{IDS,VUL}$	6.5848	>			Статистично незначущий

Розрахунки першого етапу методології щодо стандартизації даних та перевірки їх на наявність мультиколінеарності за допомогою тесту Фарара-Глобера відбувалися із використанням програмного забезпечення MS Excel. Результати тесту представлені в Таблиці 3.20, де можна побачити, що в масиві даних, сформованому на основі трьох видів кіберзлочинів, присутня мультиколінеарність, оскільки $X^2 > X^2_{cr}$.

Подальша перевірка із використанням критерії Фішера, часткової кореляції та Стьюдента виявила, що змінна, яка відповідає кількості шкідливих програм та вірусів, розповсюджених через поштові сервіси, не є мультиколінеарною з іншими. Щодо фактору кількості мережевих атак, то у поєднанні із попередньою змінною він не є мультиколінеарним ($r_{MAV,IDS} < r_{cr}$, $t_{MAV,IDS} < t_{cr}$). Третя змінна, яка характеризує кількість виявлених атак на вразливості системи, є колінеарною з іншими ($r_{IDS,VUL} > r_{cr}$, $t_{IDS,VUL} > t_{cr}$, $r_{MAV,VUL} > r_{cr}$, $t_{MAV,VUL} > t_{cr}$). Для усунення мультиколінеарності з масиву змінних найкращим способом є метод головних компонент, але у нашому випадку його застосування не призвело до отримання набору даних, який б задовольняв всім умовам. Тому для проведення кластеризації було прийнято рішення усунути змінну VUL та здійснити кластеризацію з урахуванням тільки двох змінних.

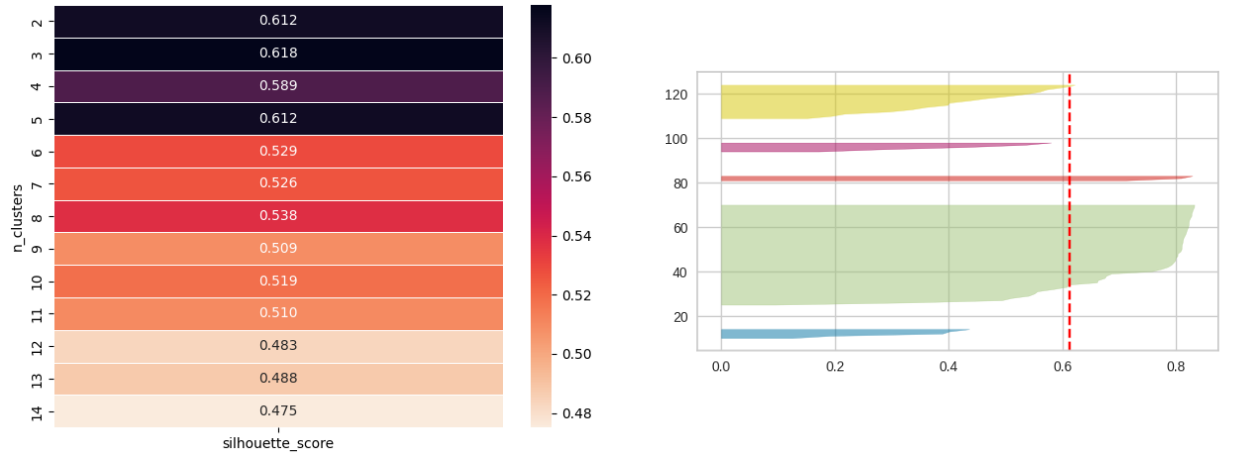
Проведення кластерного аналізу та здійснення перевірки узгодженості кластерів за допомогою Silhouette методу проводилося із використанням мови програмування Python. Оскільки кластеризація дозволила отримати нерівномірні розміри кластерів, то виникла необхідність у проведенні даної процедури в декілька етапів за прикладом ієрархічної кластеризації. Результати першого етапу представлені на рисунку 3.36.



a) b)

Рисунок 3.36 – Результати першого етапу кластеризації: a) Silhouette score; b) Silhouette plot

Найвищі Silhouette score відповідають ситуації розбиття даних на 3 кластери (Рисунок 3.36a). Але за цієї умови було також отримано й частку неправильної класифікації, тобто деякі країни (Німеччина), віднесені до кластеру, насправді до нього не належать. Для зменшення частки неправильної класифікації було прийнято рішення здійснити кластерний аналіз для 4 груп. Рисунок 3.36b підтверджує правильність такого розбиття. Але також можна побачити, що аналіз виділив кластер, який містить 80.65% усіх даних. Це обумовлено нерівномірним розподілом початкових даних, що викликано, нерівномірністю здійснення кібератак на країни. При цьому ті, які були атаковані найбільше, не потрапили до даного кластеру. Тому було проведено наступний етап кластеризації для тих країн, що увійшли до найбільшого кластеру. Результати другого етапу представлені на рисунку 3.37.

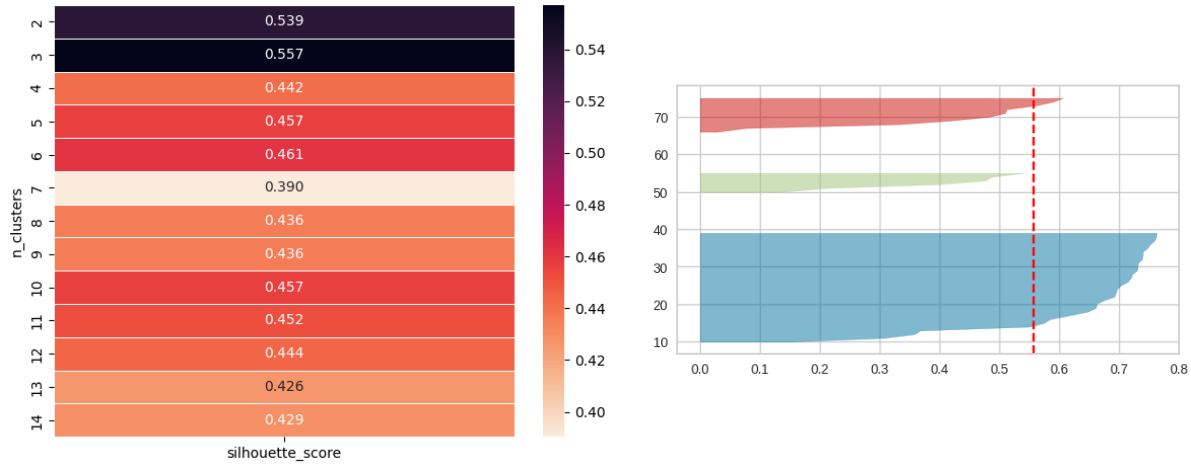


a) b)

Рисунок 3.37 – Результати другого етапу кластеризації: a) Silhouette score; b) Silhouette plot

Хоча найвищі Silhouette score відповідають трикластерному розбиттю даних, але для даної ситуації також було отримано й частку неправильної класифікації. Дана процедура віднесла Сербію до іншого кластеру, про що свідчить від'ємне значення Silhouette score (-0.1090). Використання п'ятьох кластерів дозволяє уникнути неправильно класифікованих об'єктів, що підтверджує Рисунок 3.37b, що говорить про доцільність застосування саме цього виду розподілу. Не дивлячись на кількість кластерів, отримано висновок, що один з них містить 61.33% даних вибірки. Тобто існує потреба у подальшому розбитті вибірки, отриманої на другому етапі.

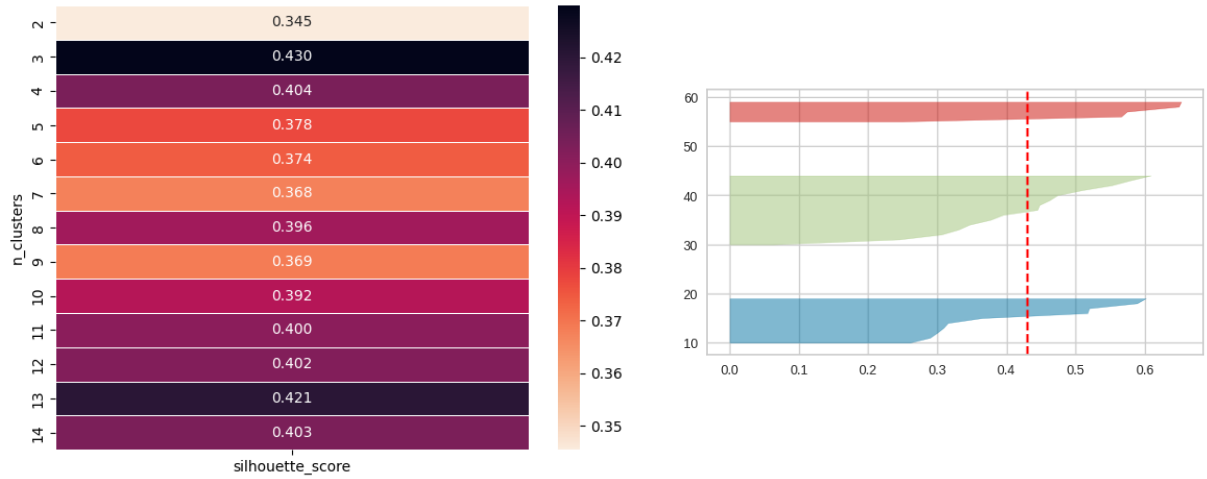
Результати третього кроку кластеризації для країн, які увійшли до найбільшого кластеру, представлені на Рисунку 3.38. Отримані Silhouette score є значними для трикластерного розподілу (Рисунок 3.38a). При цьому всі країни були класифіковано правильно (Рисунок 3.38b). Але й на даному кроці також було сформовано кластер, який містить 65.22% всіх спостережень вибірки, узятої для даного етапу, що свідчить про продовження процедури кластеризації даних для найбільшої групи країн.



a) b)

Рисунок 3.38 – Результати третього етапу кластеризації: a) Silhouette score; b) Silhouette plot

Результати четвертого останнього етапу кластеризації представлено на Рисунку 3.39. Найвище значення Silhouette score відповідає трикластерному розподілу (Рисунок 3.39a). Візуалізація Silhouette підтверджує правильність отриманих результатів із відсутністю частки неправильної класифікації об’єктів (Рисунок 3.39b). Хоча тут присутній один кластер, який складається з 50% вибірки, але це значення відповідає 16% генеральної сукупності, що є прийнятним для аналізу даних. Недоцільність подальшої кластеризації також підтверджує зниження Silhouette score, що відбувається від етапу до етапу.



a) b)

Рисунок 3.39 – Результати четвертого етапу кластеризації: a) Silhouette score; b) Silhouette plot

На Рисунку 3.40 представлена карта країн, розподілених за визначеними кластерами, а в Таблиці 3.21наведені усереднені за кластером значення по кожній групі кіберзлочинів. Тут також враховано й той вид, який було усунуто із процесу кластеризації. Найбільш атакованими є країни кластерів 1.3, 1.2 та 1.1. Найменш атакованими є країни, які належать до груп 4.1, 4.2 та 4.3.

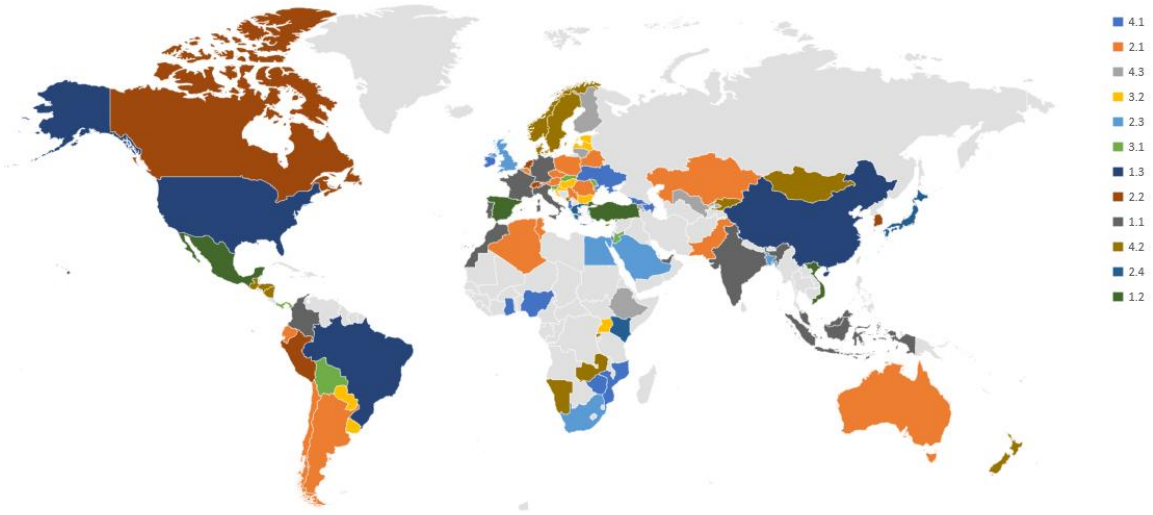


Рисунок 3.40 – Карта країн, поділених на кластери в залежності від виявлених кіберзлочинів

Таблиця 3.21 – Результати кластерного аналізу

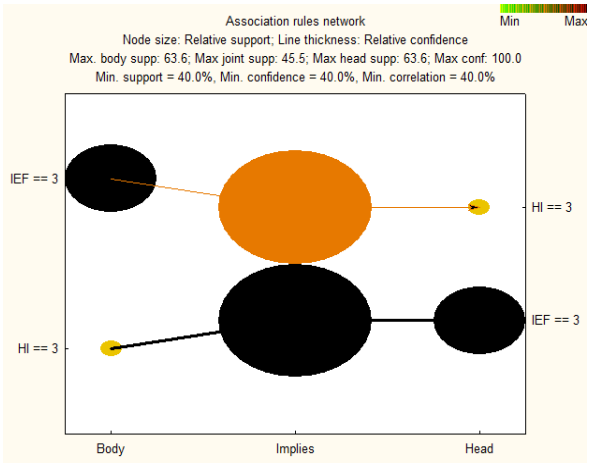
Кластер	Країни	Середнє значення MAV	Середнє значення IDS	Середнє значення VUL
1.1	Франція, Німеччина, Індія, Італія, Колумбія, Індонезія, Іран, Малайзія, Марокко, Португалія, Об'єднані Арабські Емірати	226463.27	3191437.27	54251.55
1.2	Мексика, В'єтнам, Туреччина, Іспанія	709347.25	5406983.75	60429.00
1.3	США, Китай, Бразилія	241351.33	16181266.33	136751.33
2.1	Алжир, Австралія, Австрія, Польща, Аргентина, Білорусь, Бельгія, Чехія, Еквадор, Казахстан, Румунія, Туніс, Чилі, Пакистан, Сербія, Сінгапур	51759.31	775175.06	12641.88
2.2	Нідерланди, Канада, Швейцарія, Південна Корея, Перу	37788.00	1751951.40	23692.20
2.3	Бангладеш, Єгипет, Південна Африка, Саудівська Аравія, Велика Британія	107084.20	1188240.80	22990.40
2.4	Японія, Греція, Кенія	132841.67	256754.33	38421.00
3.1	Панама, Болівія, Йорданія, Молдова, Словаччина, Словенія	16229.17	346157.33	1560.67
3.2	Бахрейн, Болгарія, Хорватія, Естонія, Угорщина, Парагвай, Уганда, Уругвай, Танзанія, Латвія	29107.20	167196.00	1904.50
4.1	Албанія, Азербайджан, Грузія, Гана, Ірландія, Зімбабве, Ізраїль, Мозамбік, Нігерія, Україна	9014.10	65207.00	1973.40
4.2	Кіпр, Гватемала, Гондурас, Киргизстан, Люксембург, Монголія, Чорногорія, Нова Зеландія, Нікарагуа, Норвегія, Руанда, Замбія, Данія, Намібія, Швеція	2873.93	69052.33	1702.13
4.3	Вірменія, Ефіопія, Фінляндія, Литва, Узбекистан	6430.40	190978.20	936.40

Для доведення або відхилення висунутої першої гіпотези скористуємося статичними даними Power Index, який визначається на базі 50 факторів, що поєднуються за військовим, економічним та культурним потенціалом [307]. За даним рейтингом тільки 25 країн світу відносяться до найбільш потужних. При цьому 12 з них відносяться до країн, що є найбільш атакованими, тобто є країнами кластерів 1.3 (США, Китай та Бразилія), 1.2 (Іспанія, Туреччина та В’єтнам) та 1.1 (Франція, Німеччина, Італія, Індія, Індонезія та Іран). Тобто країни, які є найбільш атакованими, є також найбільш потужними країнами

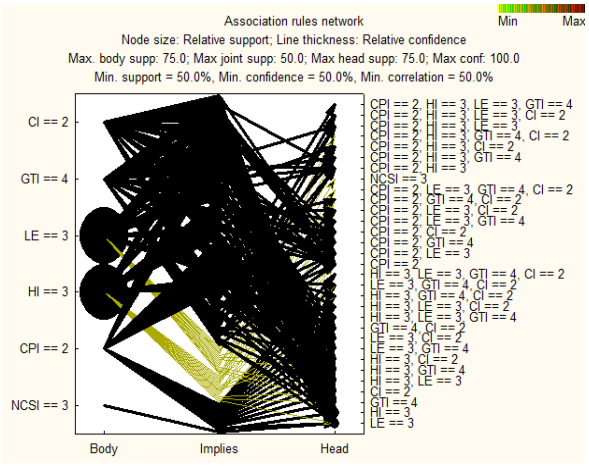
світу. При цьому, до топ-10 країн, які здійснюють кібератаки у бік інших, відносяться Китай (18.83%), США (17.05%), Бразилія (5.63%), Індія (5.33%), Німеччина (5.10%), В'єтнам (4.23%), Тайланд (2.51%), Росія (2.46%), Індонезія (2.41%), Нідерланди (2.20%) [308]. Сім країн з даного переліку – це країни кластерів 1.1, 1.2 та 1.3. Інформація щодо Тайланду та Росії відсутні у обраній для даного дослідження вибірці. Щодо Нідерландів, то дана країна не попала до кластерів із країнами-найбільшими жертвами кіберзлочинів, але також її не було віднесено й до кластерів з найменшими.

Таким чином, можна сказати, що перша гіпотеза, висунута на початку дослідження, підтверджується для таких країн, як США, Китай, Бразилія, Іспанія, В'єтнам, Франція, Німеччина, Італія, Індія, Індонезія, Іран, та Туреччина, які з одного боку, є найбільш потужними країнами у світі та є найбільшими джерелами кібератак у світі. З іншого боку, вони також належать до кластерів країн, які є найбільшими жертвами кібератак. І хоча багато фахівців заперечують наявність кібервійн, то отриманий висновок може свідчити про наявність прихованих та неприхованих кібервійн, які здійснюють потужні країни світу, оскільки мають найбільший військовий потенціал у світі. Причинами цього, на нашу думку, є створення протистояння таких країн та сприяння ними зниження впливу інших на світовому рівні, нанесення шкоди їх економічному, соціальному, політичному секторам, та формування негативного іміджу на міжнародній політичній арені.

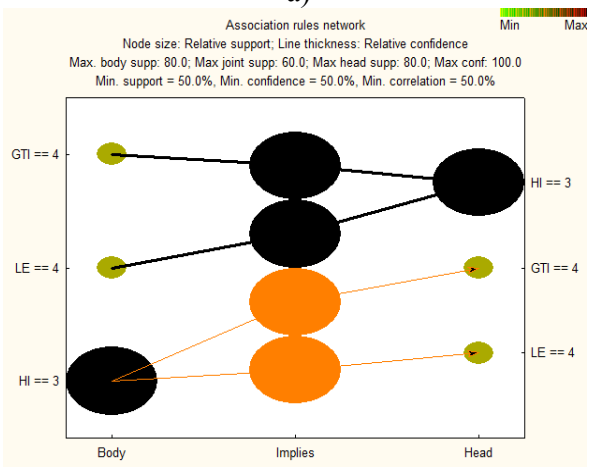
Для прийняття чи відхилення другої гіпотези необхідно проаналізувати соціально-економічні профайли кластерів країн, сформованих в залежно від рівня виявлених кіберзлочинів. Для цього було проведено асоціативний аналіз із використанням аналітичного пакету STATISTICA. Його результати представлені на Рисунках 3.41-3.42.



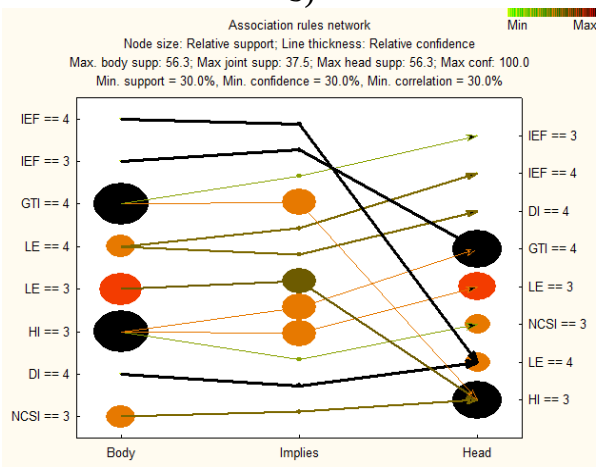
a)



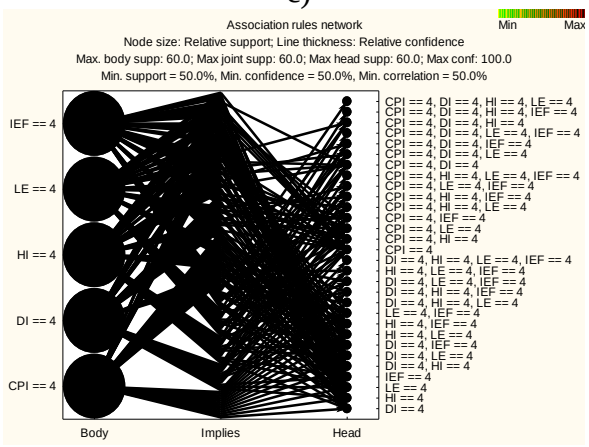
b)



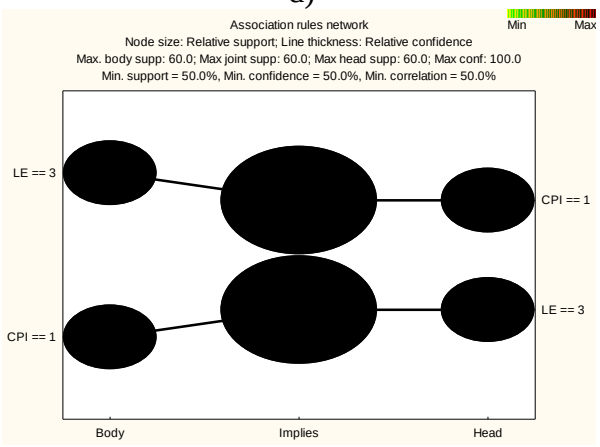
c)



d)

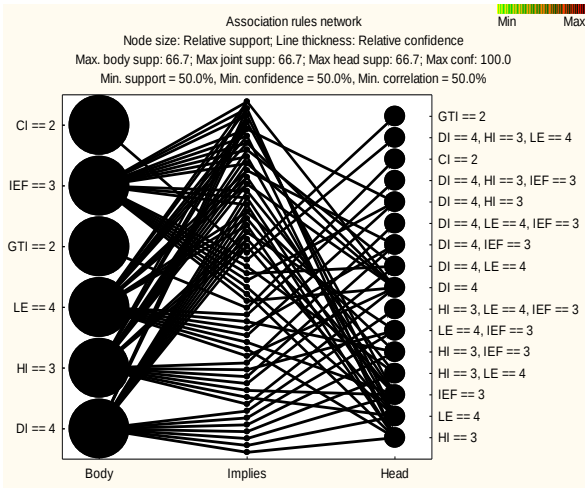


e)

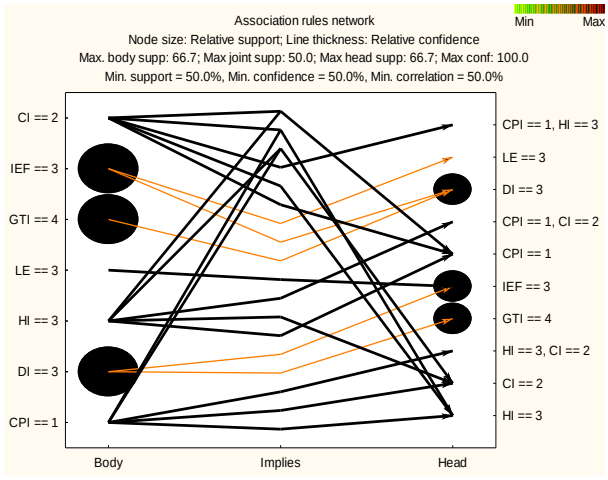


f)

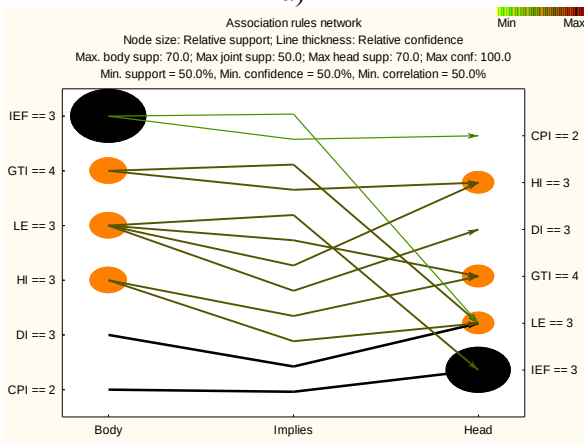
Рисунок 3.41 – Результати асоціативного аналізу для кластерів: a) 1.1; b) 1.2; c) 1.3; d) 2.1; e) 2.2; f) 2.3



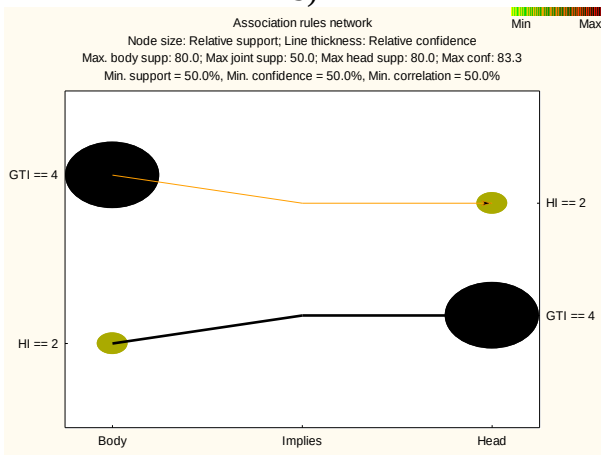
a)



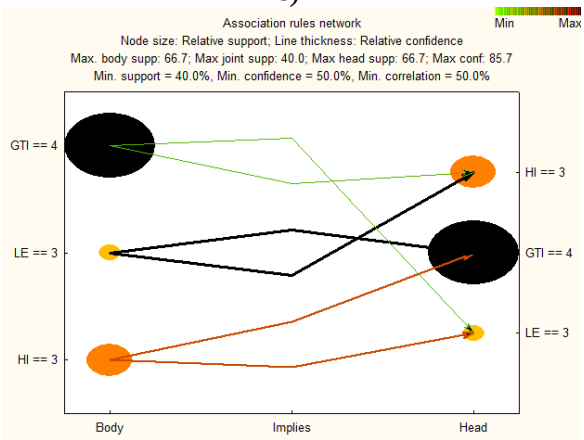
b)



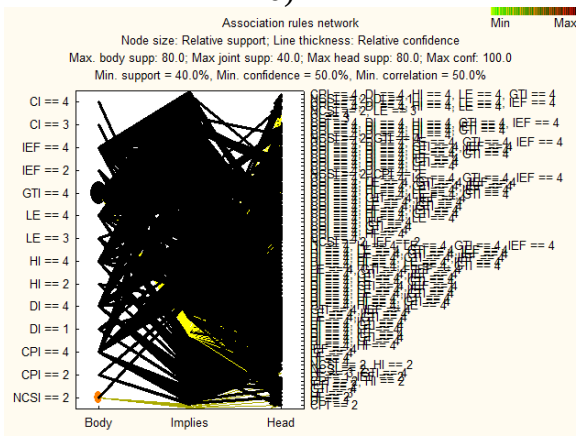
c)



d)



e)



f)

Рисунок 3.42 – Результати асоціативного аналізу для кластерів: a) 2.4; b) 3.1; c) 3.2; d) 4.1; e) 4.2; f) 4.3

Кластер 1.1 містить країни, які сильно відрізняються за своїм соціально-економічним розвитком. Саме тому результати асоціативного аналізу, представлені на Рисунку 3.41a, показують тільки дві спільні характеристики, за якими ці країни можуть належати до даної групи. Це Index of Economic Freedom

та Happiness Index. При цьому рівень економічної свободи вище середнього (IEF = 3) є однією з причин щастя на вище середньому рівні (HI = 3). Даний зв'язок є взаємообумовленим. Сумісна підтримка спостережень для цього кластеру дорівнює 45.45%, рівень достовірності коливається від 71.42% до 100%, а ймовірність того, що країни будуть знаходитися в одному кластері, дорівнює 0.85. Тобто, для ряду країн кластеру 1.1 є характерним те, що частка з них є дуже потужними, входять до топ-країн, що є ініціаторами кібератак та мають взаємообумовлений зв'язок між рівнем економічної свободи та щастя.

Рисунок 3.41b демонструє результати асоціативного аналізу кластеру 1.2, країни якого є найбільшими жертвами кібератак. Встановлено, що суттєвими характеристиками є ті, яким відповідають таким індикаторам, як National Cyber Security Index, Crime Index, Corruption Perceptions Index, Global Terrorism Index, Happiness Index та Life Expectancy at Birth. Результати містять 182 асоціативних правила, для яких сумісна підтримка спостережень дорівнює 50%, рівень достовірності коливається від 66.67% до 100%, а ймовірність знаходження країн з обраними характеристиками дорівнює 0.67-1.00. Тобто, країни кластеру 1.2 це країни з низьким рівнем тероризму, вище середнього рівнем розвитку національної кібербезпеки, очікуваної тривалості життя, щастя, корупції та злочинності в країні. З одного боку, для них характерним є комбінація соціально-економічного розвитку та присутність злочинності, корупції, що може сформувати певний імідж для кіберзлочинців, як країн-цілей кібершахрайств з метою отримання фінансово-економічних вигід.

Асоціативний аналіз кластеру 1.3 країн – найбільших жертв кібератак, дозволив виявити суттєві характеристики цієї групи, яким відповідають Global Terrorism Index, Happiness Index та Life Expectancy at Birth (Рисунок 3.41c). При цьому всі три виступають один для одного й причиною, й наслідком. Наприклад, низький рівень впливу країни на глобальний рівень тероризму (GTI = 4) є однією з причин щастя на вище середньому рівні (HI = 3), який з іншого боку є причиною для високого рівня очікуваної тривалості життя (LE = 4). Сумісна підтримка спостережень, для яких одночасно є вірним причина та наслідок дорівнює 60%.

При цьому рівень достовірності для всіх спостережень коливається від 75% до 100%, а ймовірність того, що країни з обраними характеристиками будуть знаходитися в одному кластері, є досить високою і дорівнює 0.87. Тобто, в більшості випадків країни кластеру 1.3 є країни з низьким рівнем тероризму, високим рівнем очікуваної тривалості життя та рівнем щастя вище середнього. Інші характеристики для цих країн сильно відрізняються.

Кластери 2.1, 2.2 та 2.3 характеризуються також високим рівнем кібератак, але у порівнянні із країнами груп 1.1, 1.2 та 1.3, вони атакуються значно менше (Таблиця 3.21). Рисунок 3.41d демонструє асоціативні правила для кластеру 2.1, які визначили суттєві характеристики, яким відповідають National Cyber Security Index, Democracy Index, Happiness Index, Life Expectancy at Birth, Global Terrorism Index, та Index of Economic Freedom. Хоча значення сумісної підтримки спостережень коливається від 31.25% до 37.50%, але рівень достовірності знаходиться від 55.56% до 100% та кореляції від 66.67% до 84.52%. Тобто, третина країн кластеру 2.1 це країни з високим рівнем демократії, низьким рівнем впливу на глобальний тероризм, вище середнього рівнем щастя та кібербезпеки, високим та вище середнього рівнями економічної свободи та очікуваною тривалістю життя. На жаль, для формування профайлів інших країн з даного кластеру необхідно розширити перелік обраних для аналізу характеристик. Також можна припустити, що на це можуть впливати фактори, які виявити аналітичним шляхом дуже складно, або взагалі відсутність скритих мотивів кіберзлочинців.

Рисунок 3.41e показує, що для країн кластеру 2.2 є характерними високий рівень економічної свободи, очікуваної тривалості життя, демократії суспільства, щастя та низький рівень корупції. При цьому рівень підтримки дорівнює 60% для всіх асоціативних правил, рівень достовірності та кореляції – 100%. Тобто 60% країн даного кластеру відносяться до країн з високим рівнем соціально-економічного розвитку, що може стати метою кіберзлочинів. Для країн з групи 2.3 асоціативні правила дозволили виявити такі характеристики як Corruption Perceptions Index та Life Expectancy at Birth (Рисунок 3.41f). При цьому

характерним для країн даного кластеру є високий рівень корупційної складової. Рівень підтримки для даної групи країн дорівнює 60%, рівень достовірності та кореляції – 100%. Слід сказати, що фактор високого рівня корупції може бути індикатором для формування іміджу країни, привабливого для кіберзлочинців.

Країни, які належать до кластерів 2.4, 3.1 та 3.2, також виступають жертвами кібератак, але у порівнянні із попередніми групами, вони становилися їх цілями значно менше (Таблиця 3.21). Асоціативні правила для групи 2.4 представлені на Рисунку 3.42a та демонструють такі суттєві характеристики, як Crime Index, Democracy Index, Happiness Index, Life Expectancy at Birth, Global Terrorism Index, та Index of Economic Freedom. Це є справедливим для 66.67% країн (Греція та Японія) при рівнях достовірності та кореляції 100%. Слід відмітити, що ця група характеризується високим та вище середнього рівнями розвитку економіки, щастя, тривалості життя та демократичних свобод. Також у даній групі є країни з рейтингом “2” (Греція та Кенія) для впливу на глобальний рівень тероризму та злочинності. Тобто кластер поєднав країни за полярними характеристиками – позитивним соціально-економічним розвитком та проблемами злочинного характеру.

Рисунок 3.42b демонструє характеристики для країн кластеру 3.1, до яких було віднесено низький рівень впливу на глобальний тероризм, вище середнього рівні щастя, демократії, економічної свободи, очікуваної тривалості життя, злочинності, а також високий рівень корупції. Визначені правила виконуються для 50% країн із достовірністю та кореляцією від 75% до 100%. Для країн кластеру 3.2 є характерним вище середнього рівні демократії, економічного розвитку, тривалості життя та щастя, корупції та низький вплив на глобальний рівень тероризму (Рисунок 3.42c). Це забезпечується із 50% підтримкою, достовірністю від 71.43% до 100.00% та кореляцією від 77.15% до 91.29%. Виходячи із отриманих міркувань для країн 3.1 та 3.2 кластерів рівень корупції може бути ключовим фактором для здійснення кіберзлочинів, але його вплив не може бути досить суттєвим.

Кластерами, до яких відносяться країни із найменшим рівнем кіберзлочинів, є кластери 4.1, 4.2 та 4.3 (Таблиця 3.21). Рисунок 3.42d показує, що для кластера 4.1 було виявлено тільки два правила, які характеризують причинно-наслідкові зв’язки між Global Terrorism Index та Happiness Index. При чому розмір кола, який відповідає Global Terrorism Index є великим, що свідчить про високий рівень підтримки для причини та для наслідку з боку даної характеристики, ніж для Happiness Index. Сумісна підтримка спостережень в цьому випадку дорівнює 50%, рівень достовірності коливається від 62.5% до 83.3%, а ймовірність знаходження в одному кластері дорівнює 0.72. Отримані показники є суттєвими. Тобто країни даного кластеру мають низький рівень впливу на глобальний тероризм, що відповідно робить їх не привабливими для масових кібератак. Рисунок 3.42e відображає результати асоціативного аналізу для кластеру 4.2. Виявлено, що характеристиками країн даної групи виступають Global Terrorism Index, Life Expectancy at Birth та Happiness Index. Сумісна підтримка асоціацій дорівнює 40% при досить високих значеннях рівня достовірності від 60% до 85.71%, а також ймовірності від 0.67 до 0.80. Для країн даного кластеру, так як і попередньої групи, характерним є низький вплив на рівень глобального тероризму (GTI = 4), але також суттєвим є сильний зв'язок між причиною очікуваної тривалості життя та іншими показниками (LE = 3 $\Rightarrow$ GTI = 4; LE = 3 $\Rightarrow$ HI = 3). Асоціативний аналіз для країн кластеру 4.3 виявив 642 асоціативних правила між характеристиками, яким відповідають вісім аналізованих індикаторів (Рисунок 3.42f). При цьому сумісна підтримка асоціацій дорівнює 40% при досить високих значеннях рівня достовірності від 50% до 100%, а також ймовірності від 0.58 до 1.00. Тобто дану групу складають країни, які можуть мати різну комбінацію соціально-економічних характеристик. Так, сюди входять країни із високим рівнем демократичних та економічних вільностей для населення, щастя, очікуваної тривалості життя, низьким рівнем корупції та впливу на глобальний тероризм. Інша група, це країни із низьким рівнем демократії, впливом на глобальний тероризм та нижче середнього рівнем кібербезпеки, щастя та економічної свободи. Тобто, групи країн, які мають у

своєму профайлі перелічені комбінації соціально-економічних характеристик в найменшій мірі є привабливими для масових кібератак та війн з боку інших країн.

Таким чином, виявлені характеристики профайлів кластерів країн із найбільшим та найменшим рівнем кібератак можуть підтвердити другу гіпотезу щодо опосередкованого впливу соціально-економічного розвитку країн на їх привабливість для кіберзлочинців. Про це говорить той факт, що знайдені асоціативні правила у більшості випадків характерні для країн із високим та вище середнього рейтингом соціально-економічного розвитку. Для інших країн закономірності не були встановлені або виявлено вплив окремих з них, таких як рівень корупції, злочинності, впливу на глобальний тероризм. Це свідчить про існування невиявлених в процесі дослідження факторів, що потребує подальших досліджень для їх ідентифікації.

В умовах сьогодення проблема кіберзлочинності є невід’ємною складовою науково-технічного прогресу, вирішення якої потребує багатьох зусиль з боку світових організацій, урядів країн і просто зацікавлених осіб. Але вона також становиться зручним інструментом для маніпулювання та досягнення політичних, фінансових, військово-стратегічних, психологічних та інших цілей як з боку окремих груп осіб, так й державних представників. Масова кіберзлочинність призводить до значних фінансових втрат, дестабілізації політичних, соціальних та економічних процесів, тому дане питання за часту ставиться на повістки дня такими міжнародними організаціями, як Економічна і Соціальна Рада ООН, Рада Європи, Міжнародна організація по боротьбі з кібертероризмом "ІМПАКТ", Міжнародний союз електрозв’язку та Управління ООН з наркотиків і злочинності та інші. В рамках такого співробітництва здійснюється розробка комплексу наукових, правових та організаційних заходів, які дозволяють формувати стратегії щодо регулювання та захисту поведінки користувачів у кіберпросторі. Це актуально в умовах здійснення кібервійн окремими країнами для зменшення наслідків їх агресії у бік інших. Тому запропоноване дослідження буде цікавим аналітичним підрозділам міжнародних

організацій з метою виявлення потенційних жертв кіберзлочинів та розробці спеціальних заходів протидії та відповідальності у випадках цілеспрямованих кібератак, які призвели до катастрофічних наслідків.

В рамках даного дослідження було висунуто гіпотезу, що потужні за Power Index країни одночасно є ініціаторами кіберзлочинів у бік інших країн та є жертвами кіберагресій у більшій мірі, ніж країни зі слабким впливом на світовому рівні. Дана гіпотеза була підтверджена повністю на основі проведеного кластерного аналізу та порівняння його результатів із доступними статистичними даними. Виявлено, що найбільш потужні країни в світі, а саме США, Китай, Бразилія, Іспанія, В'єтнам, Франція, Німеччина, Італія, Індія, Індонезія, Іран, та Туреччина, піддаються кіберзлочинам більше, ніж інші. При цьому вони також є джерелами активних кібератак у бік інших. Висновки цього дослідження можуть стати підґрунтям для розробки відповідних стратегій стримування таких країн у випадках їх активних дій. Ці знання будуть корисними для формування попереджувального комплексу дій, націленого на відслідковування потоків різного роду транзакцій саме з тих країн, які є джерелами кібератак та належать до критичних групам. Накопичення ретроспективних даних за більш тривалий період часу та їх використання для розширення запропонованої методики дослідження дозволить сформувати більш ймовірні структури кластерів країн – жертв кіберзлочинів та країн – кіберхижаків.

Соціально-економічні профайли кластерів країн, визначені за обсягами виявлених кібератак, що здійснювалися через поштові сервіси та мережу, було сформовано на основі проведення асоціативного аналізу. Його результати дозволили виявити ті характеристики, які є властивими для більшості країн визначених груп. При чому було виділено як їх комбінації, так й окремі з них, що може стати ключовим фактором у розумінні мотивів кіберзлочинів у світовому масштабі. Аналіз профайлів груп країн, які атакуються в меншій мірі, засвідчив, що важливим аспектом відсутності мотивації для кіберзлочинців є низький вплив даних країн на глобальний рівень тероризму. Також сюди увійшли країни

як з високим рівнем соціально-економічного розвитку, так й менш розвинені. Аналіз профайлів кластерів країн – найбільших жертв кібератак показав, що за більшістю характеристик сюди увійшли країни з високим та вище середнього рейтингом соціально-економічного розвитку, більшість з яких є потужними та тими, які є джерелом масових кібератак. Щодо інших кластерів важливим є аспект впливу високого рівня корупції, що може бути індикатором для таргетованих кібератак для отримання фінансових вигід. Отримані результати дозволили підтвердити висунуту гіпотезу, що рівень соціально-економічного розвитку країн може бути опосередкованою мотивацією кіберзлочинців для масових кібератак, а саме на це може впливати рівень корупції, злочинності та впливу на глобальний тероризм. Висновки даного аналізу можуть допомогти в удосконаленні стратегії боротьби із кіберзлочинністю, як на рівні окремої країни, так і світу в цілому, з урахуванням ключових індикаторів, які впливають на мотивацію кіберзлочинців.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [309].

3.3.2 Методика оцінювання потреб суб'єктів економіки у розвитку кібербезпеки

Сучасний розвиток людства супроводжується стрімким науково-технічним прогресом, який багато дослідників окреслили як Четверта промислова революція або Індустрія 4.0. Її феномен досліджено та обґрунтовано німецьким економістом, засновником Всесвітнього економічного форуму Klaus Martin Schwab [310]. Дане явище пов'язують із розробкою та впровадженням надсучасних технологій у різні сфери життєдіяльності суспільства, такі як штучний інтелект, хмарні та квантові обчислення, Інтернет речей, блокчейни, доповнена та віртуальна реальність, нано- та нейротехнології, автономні роботи, великі дані та інше. Більшість з них вже активно впроваджені та використовуються у бізнесі та показали свою ефективність на практиці. Зовнішні фактори також вносять корективи у організацію бізнесу та сприяють його переведенню в кіберплощину. Наприклад, світова пандемія COVID-

19 стала поштовхом для активної цифрової трансформації 46.3% підприємств, починаючи з 2021 року [311].

З одного боку, ці процеси призвели до масової діджиталізації та автоматизації господарських відносин, а з іншого боку, стали причиною появи кіберзлочинності, тобто незаконних дій, вчинених за допомогою комп'ютерних технологій. За останні п'ятдесят років вартість комп'ютерів та їх складових значно знизилася. Наприклад, у 1970 році комп'ютерний чіп із 2000 транзисторами коштував $1000, а сьогодні його можна придбати за $0.02 [311]. Дана тенденція призвела до того, що ринок пристроїв для хакерів пропонує засоби для вчинення злочинів, починаючи з $1 [312]. Діджиталізація та автоматизація бізнес-процесів, доступність технологій будь-якому користувачу створюють сприятливі передумови для здійснення масових вірусних та DDoS атак, кібератак на POS-термінали, фішингу, соціальної інженерії, контролю над IT-системою, тощо. Не дарма для підприємств ризик кібер небезпеки є одним з головних. За даними World Economic Forum для бізнесу він знаходиться на четвертій позиції після кризи вартості життя, стихійних лих та екстремальної погоди та геоекономічного протистояння [313].

Експерти оцінили, що за 2022 рік вартість глобальних втрат від кіберзлочинів склала 8.44 трильйонів доларів США і прогнозується їх зростання у 2027 році до 23.82 трильйонів доларів США [314]. У більшості випадків від кібератак страждають компанії, результатом чого є витік даних, зупинка виробничих процесів, втрата клієнтів, продукції тощо. Найбільш таргетованими є підприємства таких секторів, як фінанси, інформація, професійна діяльність, охорона здоров'я, виробництво, державне управління та освіта [315]. 91% компаній, розмір яких менше ніж 50 мільйонів доларів США, у 2018 році втратили менше ніж 10 мільйонів доларів США. При цьому 28% компаній, розмір яких перевищує one мільярдів доларів США, отримали збитків більше ніж 100 мільйонів доларів США [316]. Найбільш дорога атака була внаслідок поширення ExPetr / NotPetya вірус, в результаті чого компанії втратили 10 мільярдів доларів США [317]. Також можна навести ряд прикладів наслідків для компаній в результаті масових кіберзлочинів, спрямованих проти них. Наприклад, найбільша енергетична компанія в Індії Tata

Power Company Limited стала жертвою кібератаки у жовтні 2022 року, в результаті чого постраждала її IT-інфраструктура [318]. Канадська компанія з виробництва м'яса Maple Leaf Foods була змушена відключити IT-системи внаслідок хакерських дій [319]. У лютому 2022 року Toyota Motor Corporation призупинила виробничий процес на 28 лініях на 14 заводах, в результаті чого було скорочено випуск автомобілів на 5%, що було еквівалентно третині світового ринку [320].

Побудова система безпеки будь-якої компанії передбачає розробку концепції управління ризиками, в тому числі й кіберризиками, що включає аналіз та оцінку небезпек, пов'язаних із її функціонуванням у глобальному кіберсередовищі. Сьогодні багато компаній готові витрачати значні кошти для впровадження провідних технологій у їх процеси, але багато з них тих, особливо малих, які не підвищують витрати IT-бюджетів саме для удосконалення системи кібербезки. Це відбувається тому, що вони не мають достовірних даних та відповідних методик для оцінювання загроз та відповідних тенденцій щодо готовності компаній їм протистояти. Саме тому метою даного дослідження є розробка композитного індикатору кібербезпеки бізнесу, який дозволить здійснювати оцінювання потреби розвитку системи кібербезпеки підприємств виходячи з темпів приросту кіберзагроз у світі та рівня кіберризиків, які вони можуть викликати. Це сприятиме формуванню готовності підприємств розвивати систему кіберзахисту для забезпечення безпеки їх діяльності.

Для розробки композитного індикатору кібербезпеки бізнесу CICCS (Composite Indicator of Companies Cyber Security) було використано модифікацію метода Портера – нелінійну форму згортки релевантних показників на основі матричного підходу. Його реалізація передбачала формування масиву вхідних даних. З цією метою було обрано десять індикаторів: 1) частка організацій, які зазнали принаймні однієї успішної кібератаки; 2) частка організацій, які зазнали шість та більше успішних кібератак; 3) частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»; 4) частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «дуже вірогідною»; 5) індекс

загрози, що відображає загальну стурбованість щодо кібератак; 6) індекс занепокоєння безпекою; 7) частка організацій із зростаючим бюджетом безпеки; 8) частка організацій, які відчувають нестачу кваліфікованого персоналу з IT-безпеки; 9) частка організацій, уражених програмами-вимагачами; 10) вартість викрадених або скомпрометованих облікових даних.

Джерелом отримання статистичних даних щодо показників 1-9 є Cyberthreat Defense Report, який щорічно готує CyberEdge Group, базуючись на результатах опитування представників 17 країн світу [321]. Джерелом отримання статистичної інформації для показника 10 є звіт IBM [322]. В межах кожного року опитування проходить більше ніж 1200 спеціалістів з IT-безпеки та понад 500 співробітників компаній зі сфери фінансів, державного управління, телекомунікацій й технологій, виробництва, охорони здоров'я, освіти та роздрібної торгівлі. Найбільшу питому вагу мають респонденти з США – більше ніж 29%, частка респондентів з Великобританії становить 8,3%, з Німеччини та Франції – 6,3%. Частка респондентів з інших країн (Австралія, Бразилія, Канада, Китай, Колумбія, Італія, Японія, Мексика, Саудівська Аравія, Сінгапур, Південна Африка, Іспанія, Туреччина) складає менше 5%. Таким чином, обрані показники базуються на експертній думці професіоналів в досліджуваній сфері та адекватно характеризують розуміння суб'єктами господарювання існуючих цифрових небезпек, готовність менеджменту компаній витрачати власні фінансові ресурси на подолання кіберризиків.

Перший та другий показники (Додаток И, Таблиця И.1, Рядок 1-2) характеризують частку організацій, які в цілому зазнали хоча б однієї кібератаки. Якщо перший показник характеризує наявність успішної кібератаки на організацію, то другий – частоту даних атак. Протягом 2014-2022 рр. частка організацій, які зазнали принаймні однієї успішної кібератаки, зростала в середньому більше ніж на 4 %, а останні три роки (2020-2021 рр.) вона неодмінно перевищувала 80%. Тобто, частота атак була ще більш активною. Середній темп приросту частки організацій, які зазнали шість та більше успішних кібератак, становив 13,5%, а його значення протягом 2020-2022 рр. не знижувалось нижче ніж

рівень у 35%. Це свідчить про те, що з кожним роком зростає не тільки кількість суб'єктів господарювання, цифрова система яких піддається кібератакам, але й чисельність кібератак на одну компанію.

Третій та четвертий показники (Додаток И, Таблиця И.1, Рядок 3-4) характеризують очікування економічних агентів щодо рівня успішності кібератаки. Починаючи з 2016 р., більше ніж 60% респондентів вважали, що протягом року на їх компанію вірогідно буде здійснена кібератака, а починаючи з 2019 р. більше ніж 20% опитаних були впевнені в тому, що кібератака на компанію буде дуже успішною та призупинить її діяльність на невизначений строк.

П'ятий та шостий показники (Додаток И, Таблиця И.1, Рядок 5-6) характеризують стурбованість економічних агентів щодо кіберзагроз. Індекс загрози та індекс занепокоєння безпекою, починаючи з 2015 р., мають циклічну тенденцію з незначним розмахом. Так, після помірного зменшення абсолютного значення досліджуваних індексів у 2018-2019 рр. прослідковується їх неодмінне поступальне зростання протягом наступного року (більше ніж на 7%) та у 2021 й 2022 рр. Виходячи з результатів аналізу, зазначимо, що суб'єкти господарювання занепокоєні як наростаючою загрозою реалізації кібератак, так і неспроможністю власної системи цифрової безпеки протистояти новим викликам діджиталізації.

Сьомий та восьмий показники (Додаток И, Таблиця И.1, Рядок 7-8) характеризують бюджетне та кадрове забезпечення політики підсилення кіберзахисту компаній у відповідь на кібервиклики. Зважаючи на зростаючу загрозу кібератак, підприємства та організації щороку збільшують свої бюджети на цифрову безпеку. Так, починаючи з 2018 р. більше ніж 77% суб'єктів господарювання неодмінно збільшували власні витрати на формування механізмів по боротьбі з кіберризиками. Підтвердженням активної політики суб'єктів господарювання в сфері кібербезпеки виступає й показник частки організацій, які відчувають нестачу кваліфікованого персоналу з IT-безпеки. Так, протягом 2018-2022 рр. досліджуваний показник стабільно переважав 80%.

Дев'ятий та десятий показники (Додаток И, Таблиця И.1, Рядок 9-10) характеризують глобальні світові наслідки кіберзагроз. Поширеними в останні

часи є й кібератаки, пов'язані з програмами-викрадачами, які торкнулись як великого, так і малого бізнесу та призвели до 70% ураження усіх опитаних респондентів у 2022 р. Кібератаки призвели й до значних фінансових втрат. Так протягом 2016-2022 рр. щорічно суб'єкти господарювання втрачали в середньому 3,9 млн дол. США в результаті викрадених або скомпрометованих облікових даних. Таким чином, справедливо зауважити, що протягом 2014-2022 рр. активність кіберзагроз для суб'єктів неодмінно збільшувалась, проте незважаючи на збільшення питомої ваги бюджету на цифрову безпеку та намагання розширити контингент спеціалістів з ІТ-безпеки, здійснюваних заходів не вистачає щоб зменшити отримані збитки та мінімізувати час вимушеного призупинення діяльності від реалізації кіберризиків.

Для формування композитного індикатора CICCS обрані показники необхідно було привести у співставний вигляд, оскільки вони представлені у трьох різних одиницях вимірювання. З цією метою для показників-дестимуляторів було використано метод Севіджа, формалізований за допомогою формули (3.27).

$$k_{normij} = \frac{\max\limits_{j}\{k_{ij}\} - k_{ij}}{\max\limits_{j}\{k_{ij}\} - \min\limits_{j}\{k_{ij}\}} \qquad (3.27)$$

де k_{normij} – нормалізовані значення i-того показника у j-ому році;

k_{ij} – фактичне значення i-го показника у j-ому році;

i= 1÷9;

j= 2016÷2022.

До складу показників – дестимуляторів було віднесено: k_1 – частка організацій, які зазнали принаймні однієї успішної кібератаки, k_2 – частка організацій, які зазнали шість та більше успішних кібератак, k_3 – частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», k_4 – частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «дуже

вірогідною», k_5 – індекс загрози, що відображає загальну стурбованість щодо кібератак, k_6 – індекс занепокоєння безпекою, k_7 – частка організацій, які відчувають нестачу кваліфікованого персоналу з ІТ-безпеки, k_8 – частка організацій, уражених програмами-вимагачами, k_9 – вартість викрадених або скомпрометованих облікових даних.

У свою чергу для показник- стимулятора (k_{10} – частка організацій із зростаючим бюджетом безпеки) запропоновано застосовувати метод природньої нормалізації (формула 3.28).

$$k_{norm\,ij} = \frac{k_{ij} - \min\limits_j \{k_{ij}\}}{\max\limits_j \{k_{ij}\} - \min\limits_j \{k_{ij}\}} \qquad (3.28)$$

де $k_{norm\,ij}$ – нормалізовані значення i-того показника у j-ому році;

k_{ij} – фактичне значення i-го показника у j-ому році;

$i = k_{10}$;

j= 2016÷2022.

Періодом для розрахунків обрано 2016-2022 рр. Це пов’язано з відсутністю статистичної інформації за 2014-2017 рр. для частки організацій із зростаючим бюджетом безпеки, частки організацій, які відчувають нестачу кваліфікованого персоналу з ІТ-безпеки, частки організацій, уражених програмами-вимагачами, вартість викрадених або скомпрометованих облікових даних. Отримані в процесі нормалізації результати зведені в таблицю И.2 Додатку И.

На наступному кроці розраховано темпи приросту кожного з показників, що є складовими композитного індикатора CICCS (Додаток И, Таблиця И.3). Виходячи з мінімального, максимального та середнього значення темпів приросту цих показників, встановлюються чотири проміжки характеристики кіберзагрози:

1) випереджаюче зростання кіберзагрози: для 2016 р. – темп приросту більше 16%, для 2017 р. – темп приросту більше 19%, для 2018 р. – темп приросту більше 3,5 %, для 2019 р. – темп приросту більше 7,5%, для 2020 р. – темп

приросту більше 14%, для 2021 р. – темп приросту більше 10%, для 2022 р. – темп приросту більше 8%;

2) швидке зростання кіберзагрози: для 2016 р. – темп приросту в межах 10%–16%, для 2017 р. – темп приросту в межах 9%–19%, для 2018 р. – темп приросту в межах 0%–3,5%, для 2019 р. – темп приросту в межах 4%–7,5%, для 2020 р. – темп приросту в межах 8%–14%, для 2021 р. – темп приросту в межах 6%–10%, для 2022 р. – темп приросту в межах 0%–8%;

3) помірне зростання кіберзагрози: для 2016 р. – темп приросту в межах 8%–10%, для 2017 р. – темп приросту в межах 0%–9%, для 2018 р. – темп приросту в межах -2%–0%, для 2019 р. – темп приросту в межах 0%–4%, для 2020 р. – темп приросту в межах 2%–8%, для 2021 р. – темп приросту в межах 0%–6%, для 2022 р. – темп приросту в межах -8%–0%;

4) зменшення кіберзагрози: для 2016 р. – темп приросту менше 8%, для 2017 р. – темп приросту менше 0%, для 2018 р. – темп приросту менше -2%, для 2019 р. – темп приросту менше 0%, для 2020 р. – темп приросту менше 2%, для 2021 р. – темп приросту менше 0%, для 2022 р. – темп приросту менше -8%.

Далі всі показники, що є складовими CICCS, запропоновано згрупувати в залежності від рівня даного ризику (на основі нормалізованих значень цих показників) таким чином:

- критичний рівень кіберризику (від 0,75 до 1,00);
- високий рівень кіберризику (від 0,50 до 0,75);
- середній рівень кіберризику (від 0,25 до 0,50);
- низький рівень кіберризику (від 0,00 до 0,25).

У зв’язку із нерівномірним розподілом показників в межах інтервалу від 0 до 1 виключенням стали 2016 р. та 2021 р.:

- у 2016 р.: 0,00-0,25 – низький рівень кіберризику; 0,25-0,60 – середній рівень кіберризику; 0,60-0,75 – високий рівень кіберризику; 0,75-1,00 – критичний рівень кіберризику;

– у 2021 р.: 0,00-0,07 – низький рівень кіберризику; 0,07-0,15 – середній рівень кіберризику; 0,15-0,23 – високий рівенькібер ризику; 0,23-0,30 – критичний рівень кіберризику.

Далі необхідно побудувати карту показників, що є складовими CICCS, у вигляді перехресної матриці. В залежності від розрахованого темпу приросту кіберзагрози та рівня кіберризику виділяється та групуються ті показники, які мають спільні характеристики. У комірках матриці суперпозиції показників ($a_{ij}, i = 1 \div 4, j = 1 \div 4$), що є складовими CICCS, зазначається кількість тих, які за відповідними значеннями темпів приросту кіберзагрози й рівня кіберризику відносяться до даної комірки матриці (Таблиця 3.22).

Таблиця 3.22 – Матриця суперпозиції показників, що є складовими CICCS

Рівень кіберризику / темп приросту кіберзагрози	Критичний	Високий	Середній	Низький
Випереджаючий приріст	a_{11}	a_{12}	a_{13}	a_{14}
Швидкий приріст	a_{21}	a_{22}	a_{23}	a_{24}
Помірний приріст	a_{31}	a_{32}	a_{33}	a_{34}
Спадаючий приріст	a_{41}	a_{42}	a_{43}	a_{44}

В основі побудови матриці суперпозиції показників, що є складовими CICCS (таблиця 3.22) знаходиться матриця B (формула (3.29)):

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}. \quad (3.29)$$

Дуже часто виникає ситуація, коли при формуванні матриці B декілька її елементів b_{ij} набувають нульових значень. У такому випадку відбувається корегування елементів матриці шляхом додавання до них одиниці.

Далі на основі матриці B розраховується кількісне значення індикатору CICCS за формулою (3.30) шляхом обчислення співвідношення визначника матриці B, а також кореня суми добутків елементів, що формують матрицю:

$$CICCS = \frac{detB}{\sqrt{\begin{matrix} b_{11}b_{12}b_{13}b_{14} + b_{21}b_{22}b_{23}b_{24} + \\ +b_{31}b_{32}b_{33}b_{34} + b_{41}b_{42}b_{43}b_{44} + \\ +b_{11}b_{21}b_{31}b_{41} + b_{12}b_{22}b_{32}b_{42} + \\ +b_{13}b_{23}b_{33}b_{43} + b_{14}b_{24}b_{34}b_{44} \end{matrix}}} \quad (3.30)$$

де *CICCS* –Composite Indicator of Business Cyber Security;

B – матриця суперпозиції показників, що є складовими CICCS;

$detB$ – визначник матриці B;

$b_{ij}, i = 1 \div 4, j = 1 \div 4$– кількість показників, які за відповідними значеннями темпів приросту кіберзагрози й рівня кіберризику відносяться до даної комірки матриці.

Чисельник формули (3.30) обраховується за допомогою співвідношення (3.31):

$$detB = |B| = \sum_{(i_1, i_2, \ldots, i_n)} (-1)^{\sigma(i_1, i_2, \ldots, i_n)} b_{1_{i1}}\, b_{2_{i2}} \ldots b_{n_{in}}, \quad (3.31)$$

де $\sigma(i_1, i_2, \ldots, i_n)$ - кількість інверсій у перестановці.

З метою спрощення математичного виразу проведено агрегування знаменнику дробу та трансформуємо у формулу (3.32):

$$CICCS = \frac{detB}{\sqrt{\begin{matrix}\prod_{j=1}^{4} b_{1j} + \prod_{j=1}^{4} b_{2j} + \prod_{j=1}^{4} b_{3j} + \prod_{j=1}^{4} b_{4j} + \\ + \prod_{j=1}^{4} b_{j1} + \prod_{j=1}^{4} b_{j2} + \prod_{j=1}^{4} b_{j3} + \prod_{j=1}^{4} b_{j4}\end{matrix}}} \quad (3.32)$$

Подальші перетворення, а саме узагальнення суми складових в межах рядків та стовпчиків матриці B, призведуть до отримання математичного співвідношення (3.33):

$$CICCS = \frac{detB}{\sqrt{\sum_{i=1}^{4} \prod_{j=1}^{4} b_{ij} + \sum_{j=1}^{4} \prod_{i=1}^{4} b_{ij}}} \quad (3.33)$$

Враховуючи проміжні розрахунки, наведені в формулах (3.30) – (3.33), остаточний варіант розрахунку композитного індикатора CICCS набуває вигляду (3.34):

$$CICCS = \frac{\sum_{(i_1,i_2,\dots,i_n)} (-1)^{\sigma(i_1,i_2,\dots,i_n)} b_{1_{i1}} b_{2_{i2}} \dots b_{n_{in}}}{\sqrt{\sum_{i=1}^{4} \prod_{j=1}^{4} b_{ij} + \sum_{j=1}^{4} \prod_{i=1}^{4} b_{ij}}}, \quad (3.34)$$

де $|...|$ – абсолютне значення CICCS.

В процесі реалізації запропонованої методики було отримано матриці суперпозиції показників з нульовими значеннями. Для отримання остаточного значення композитного індикатору було розраховано кореговані матриці (Таблиці 3.23 – 3.29).

Таблиця 3.23 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2016 р.

2016 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.24 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2017 р.

2017 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.25 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2018 р.

2018 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.26 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2019 р.

2019 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.27 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2020 р.

2020 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.28 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2021 р.

2021 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Таблиця 3.29 – Скоригована матриця суперпозиції показників, що є складовими CICCS, для 2022 р.

2022 рік		Верхня межа рівня кібер ризику	1	0,75	0,6	0,25
Нижня межа темпу приросту кібер загрози	Верхня межа темпу приросту кібер загрози	Нижня межа рівня кібер ризику	0,75	0,6	0,25	0
16			2	1	1	1
10	16		2	1	3	1
8	10		1	1	1	1
	8		6	1	1	2

Отримані значення матриць дозволили визначити композитний індикатор CICCS для кожного року періоду дослідження (Таблиця 3.30).

Таблиця 3.30 – Розраховані значення CICCS за 2016-2022 рр.

ISIDP	Рік						
	2016	2017	2018	2019	2020	2021	2022
	0,28	0,23	0,23	0,13	0,39	0,40	0,39

Крім абсолютних значень CICCS, важливого значення також набуває якісна інтерпретація отриманих результатів. За допомогою середньоквадратичного відхилення сформуємо три інтервали, а саме:

1) CICCS від 0,34 до 0,50 – висока потреба розвитку кібербезпеки в світі;
2) CICCS від 0,17 до 0,33 – середня потреба розвитку кібербезпеки в світі;
3) CICCS від 0,00 до 0,16 – низька потреба розвитку кібербезпеки в світі.

Потреба розвитку кібербезпеки в світі суттєво зросла в останні три роки, досягнувши свого максимального значення у 2021 р. (індикатор CICCS у 2021 р. становив 0,4 од.). Це обумовлено умовами, в яких світ опинився внаслідок пандемії COVID-19 [323]. Вони вимагали швидкого прийняття рішень на підприємствах та переорієнтації бізнес-процесів у кіберплощину. Тобто збільшилася кількість випадків кіберзагроз, які перетворилися на реальні кіберризики для компаній. З іншого боку, зросла й їх готовність боротися із даними ризиками та впроваджувати більш потужні та дієві заходи безпеки [324]. Три попередні роки (2016-2018 рр.) потреба розвитку кібербезпеки в світі була

середньою, оскільки значення CICCS коливались в межах від 0,23 од. до 0,28 од. У 2019 р потреба розвитку кібербезпеки в світі був низьким (абсолютне значення індикатора CICCS дорівнювало 0,13 од.). На дане значення могло вплинути або те, що для підприємств кіберзагрози 2019 року не стали критичними ризиками, або вони були краще підготовлені до подібних ситуацій.

Отримані розрахунки індикатору CICCS співставимо із трендами, які характеризують перспективи Індустрії 4.0, які є важливими для розвитку системи кібербезпеки підприємств. Одним із таких напрямів є технології штучного інтелекту, які використовуються для розробки інтелектуальних машин та застосовуються в інженерії, робототехніці, медичних системах, електронній комерції, тощо. Оскільки в основу штучного інтелекту знаходяться принципи функціонування людського мозку, то в майбутньому він може замінити людину в процесі вирішення різних задач, тому зараз відбувається активне їх впровадження у бізнес сферу. Рисунок 3.43 демонструє динаміку потреб у розвитку кібербезпеки та доходів від технологій штучного інтелекту. Тобто спостерігається стрімке зростання впровадження та використання даного виду технологій для світового ринку додатків підприємств. При цьому прогнозується їх збільшення у 2023 році приблизно на 45%, а у 2024 році приблизно у 2 рази. Оскільки відбувається потреба у розвитку кібербезпеки, то така тенденція в поведінці ринку технологій штучного інтелекту сприятиме також й задоволенню попиту на системи безпеки, в яких вони реалізовані. Рисунок 3.43 показує, що відбуватиметься розрив між аналізованими показниками, що може свідчити про перспективи штучного інтелекту в організації систем безпеки підприємств.

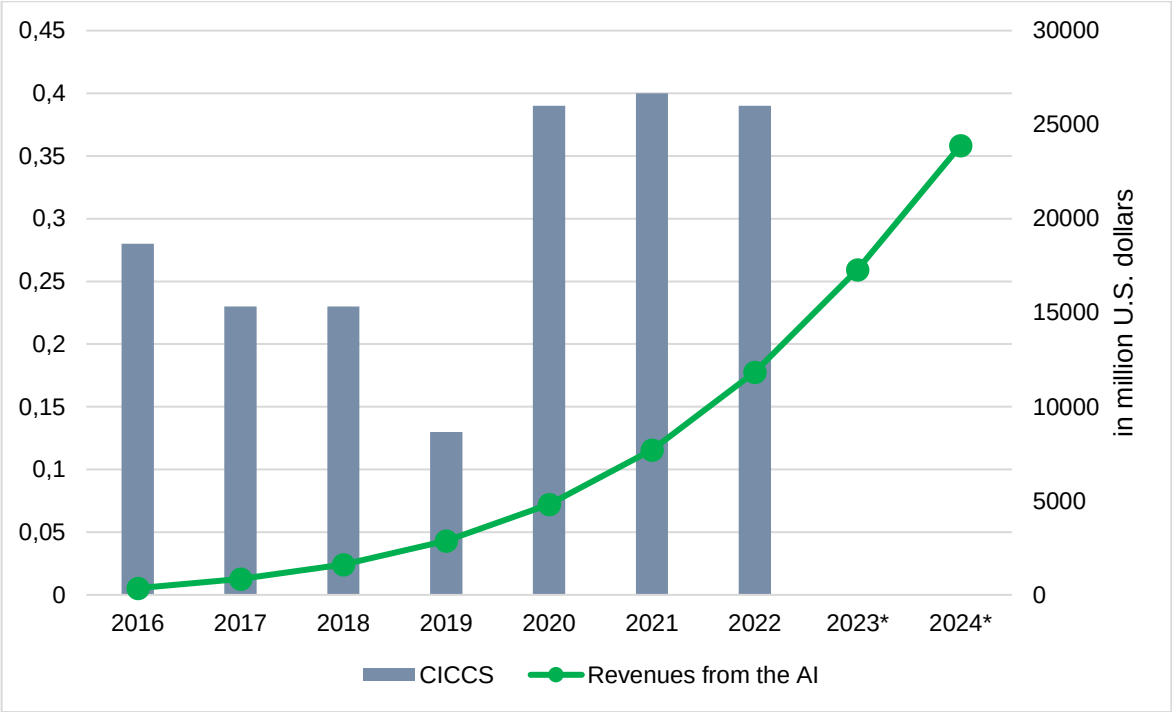


Рисунок 3.43 – Динаміка індикатору CICCS та доходів від технологій штучного інтелекту для світового ринку додатків підприємств за 2016-2024 рр.

**2023 та 2024 містять прогнозні оцінки*

Наступним перспективним напрямком Індустрії 4.0 є застосування промислових роботів для виконання різних операцій на промислових та технологічних лініях. Їх застосування сприяє підвищенню продуктивності праці, а можливості дистанційного управління сприяють підвищенню рівня безпеки для працівників компаній. З іншого боку, в процесі кібератак на інфраструктуру підприємства в першу чергу страждатимуть роботизовані системи. Тому вони потребуватимуть більш дієвих заходів кіберзахисту, які дозволять зменшити простої виробництва та витрати на відновлення їх працездатності внаслідок кіберзагрози. Рисунок 3.44 показує порівняння динаміки потреб у розвитку системи кібербезпеки та обсягів встановлених промислових роботів. Починаючи із 2020 року спостерігається їх зростання і прогнози також свідчать про позитивну динаміку. Оскільки потреби у надійній системі кіберзахисту зростають за останні три роки, то у порівнянні із збільшенням попиту на промислові роботи вони перевищують той рівень загроз, який може бути викликаний кібератаками на промислову інфраструктуру. Хоча до 2020 року підприємства також активно

впроваджували даний вид технологій, але потреби у їх кіберзахисті були значно меншими.

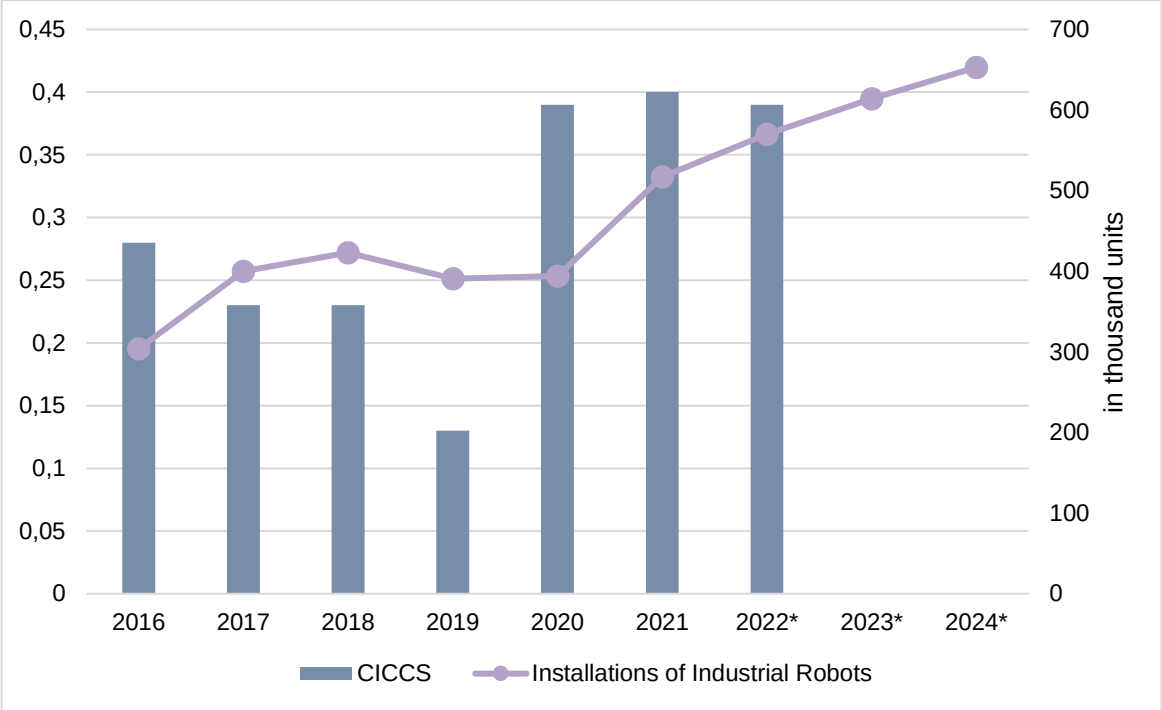


Рисунок 3.44 – Динаміка індикатору CICCS та Установки промислових роботів за 2016-2024 рр.

**2023 та 2024 містять прогнозні оцінки*

Блокчейн технології стали активно впроваджуватися на фінансових ринках, але сфера їх застосування значно розширюється за рахунок їх безпекових можливостей для організації децентралізованих баз даних. На рисунку 3.45 представлена динаміка світового ринку блокчейн технологій за 2016-2022 роки, яка демонструє цілком позитивну тенденцію його розвитку. Але порівнюючи потреби розвитку кібербезпеки з даним технологічним напрямком, можна сказати, що він потребує більше зусиль для організації системи захисту. Той рівень кіберзагроз, який спостерігався за аналізований період часу, був досить серйозним для тих компаній, які застосовували блокчейн. За 2022 рік ця тенденція змінилася, що може свідчити тільки про створення сприятливих умов розвитку системи кіберзахисту по відношенню до блокчейн-технологій.

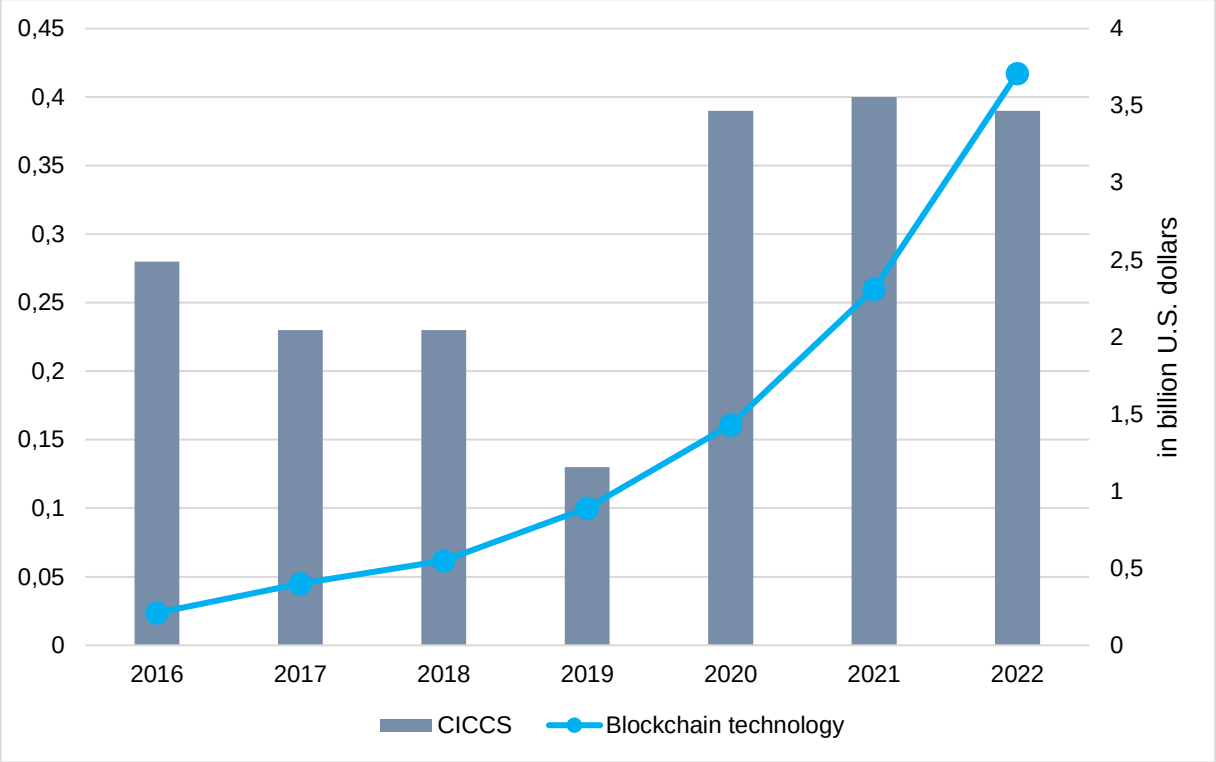


Рисунок 3.45 – Динаміка індикатору CICCS та світового ринку блокчейн технологій за 2016-2022 рр.

Технології Інтернету речей стали частиною середовища для автоматизації промислових завдань. Основними ризиками, пов’язаними із їх використанням, є ризики порушення конфіденційності та витоку інформації, що вимагає застосування спеціальних систем та протоколів кіберзахисту. Рисунок 3.46 демонструє позитивну динаміку щодо глобальної встановленої бази пристроїв, підключених до Інтернету речей, яка також включає й прогнозоване значення зростання їх обсягів. Порівнюючи даний напрям із потребами у розвитку системи кібербезпеки, можна побачити, що вони переважають обсяги встановлених баз даних. Оскільки вони функціонують через віддалений доступ, то сучасні безпекові заходи на 100% не усувають потенційні кіберризики, що потребує додаткового кіберзахисту.

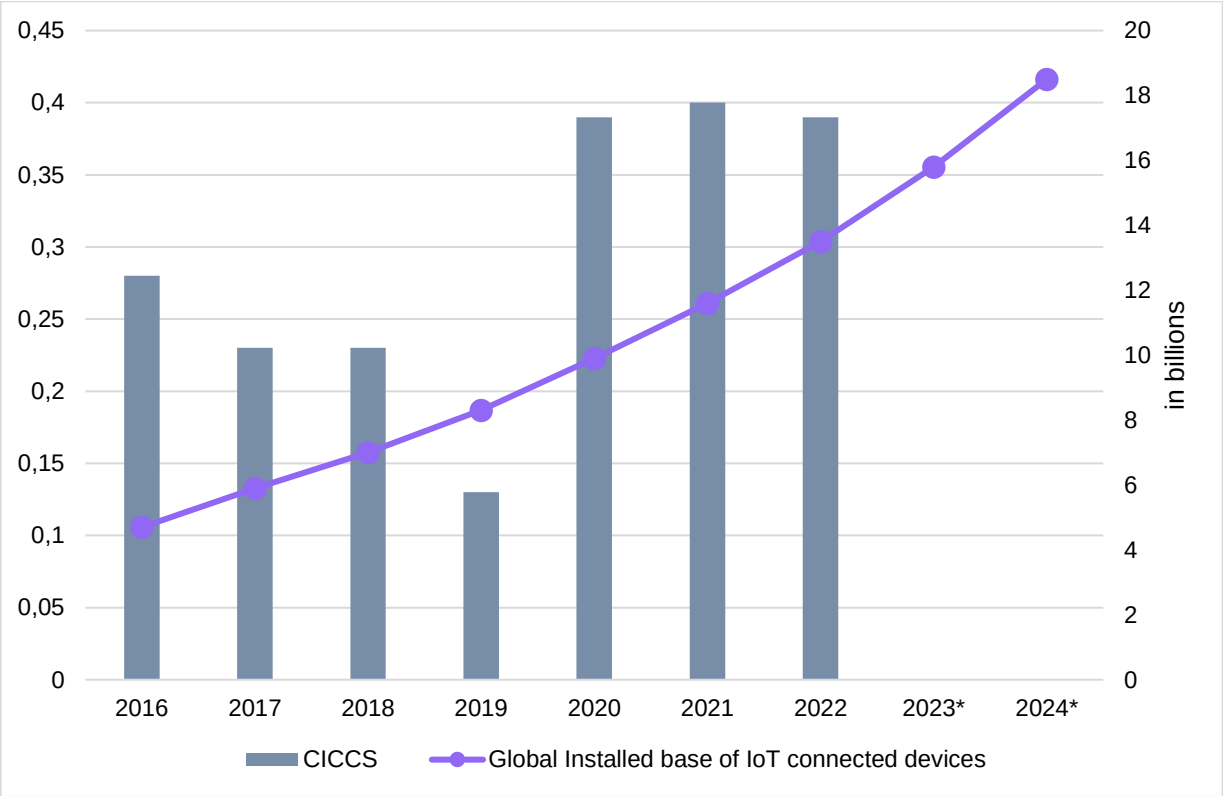


Рисунок 3.46 – Динаміка індикатору CICCS та Глобальна встановлена база пристроїв, підключених до Інтернету речей за 2016-2024 рр.

**2023 та 2024 містять прогнозні оцінки*

На рисунку 3.47 представлено порівняння динаміки витрат в IT та потреб у розвитку кіберзахисту. До 2020 року IT бюджети компаній могли покривати витрати даної сфери, але починаючи з 2020 року потреби у кібербезпеці значно зросли, що вимагає від підприємств нових управлінських підходів. Багато малих підприємств не виділяють додаткових коштів на власну кібербезпеку, оскільки вважають, що витрати на неї можуть бути більшими, ніж втрати від кібератак. Для великих компаній ситуація є оберненою, хоча вони можуть не відчувати зростання витрат на захист в контексті загальних витрат на інформаційні технології.

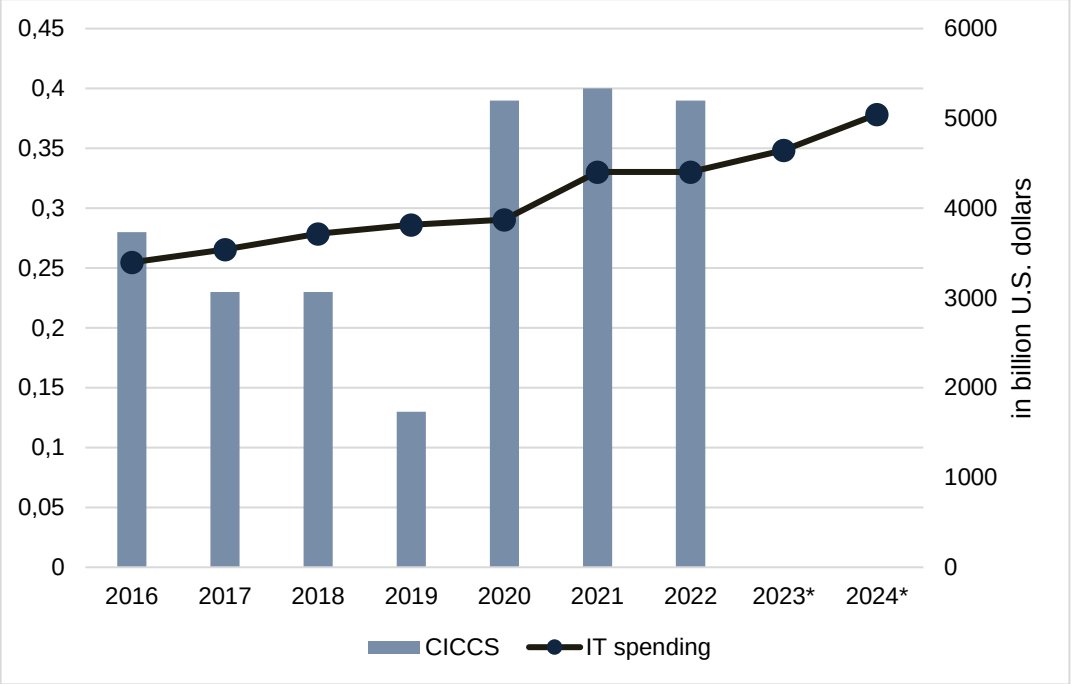


Рисунок 3.47 – Динаміка індикатору CICCS та витрат на інформаційні технології за 2016-2024 рр.

**2023 та 2024 містять прогнозні оцінки*

Порівнюючи витрати на світову кібербезпеку із потребами її розвитку, слід зазначити, що 2020-2021 роки характеризувалися у превалюванні потреб над витратами, що могло бути викликано ситуацією, пов'язаною із COVID-19 (Рисунок 3.48). 2022 рік показує баланс між даними показниками, що може свідчити про заспокоєння флуктуацій, викликаних пандемією та зростанням обсягів діджиталізації та цифровізації компаній.

Проведений порівняльний аналіз потреб у розвитку кібербезпеки та напрямків, які характеризують розвиток Індустрії 4.0, дозволяє зробити наступні висновки. По-перше, активне зростання впровадження сучасних технологій потребує створення надійної системи кіберзахисту. Але за останні три роки потреби в цій системі є значними, що вимагає більш ефективних рішень. По-друге, витрати на IT та кібербезпеку зростають прямо пропорційно до зростання обсягів сучасних технологій. Хоча вони не покривали потреб у розвитку кібербезпеки в період пандемії, але останній рік продемонстрував певну збалансованість, що свідчить про розуміння компаніями тих кіберзагроз, які перед ними виникають.

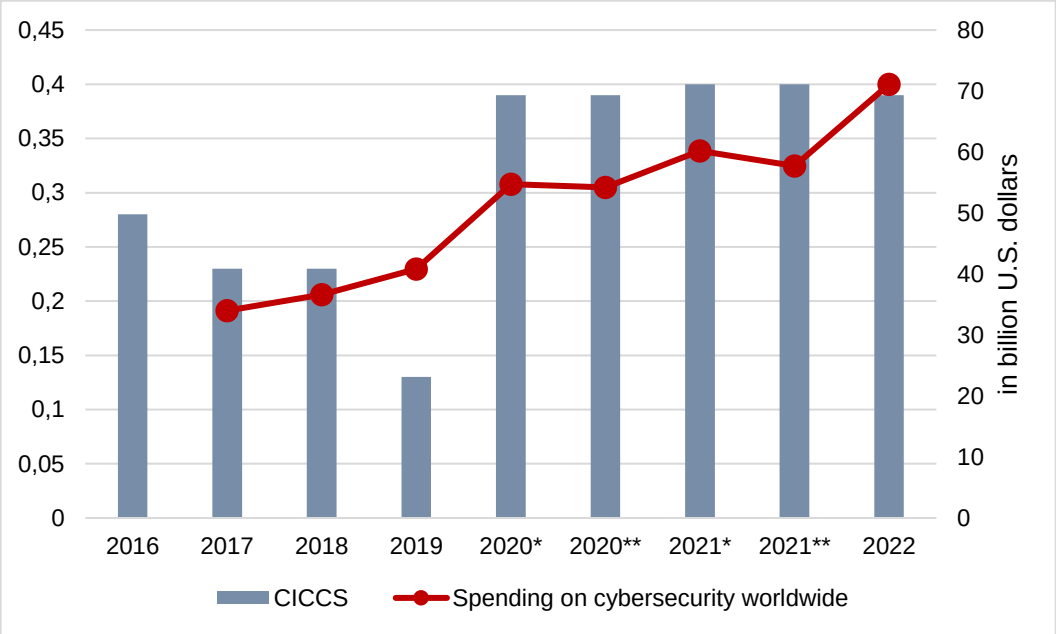


Рисунок 3.48 – Динаміка індикатору CICCS та витрат на світову кібербезпеку за 2016-2022 рр.

**2020 та 2021 – найкращий сценарій з урахуванням COVID-19; **2020 та 2021 – найгірший сценарій з урахуванням COVID-19*

Науково-технічний прогрес є невід'ємною частиною розвитку людства. Його результати суттєво впливають на систему безпеки компаній за рахунок впровадження сучасних технологій, які дозволяють зменшувати загрози та ризики, пов'язані із порушенням виробничих, логістичних, технологічних та інших процесів. Кіберризики є найбільш непрогнозованим видом ризиків, тому створення надійної та ефективної системи кібербезпеки є сьогодні важливим завданням для забезпечення безпеки підприємств в цілому. Дане дослідження спрямоване на розробку композитного індикатору кібербезпеки бізнесу на основі модифікованого матричного підходу Портера. Запропонований підхід та розрахунки дозволяють провести оцінювання потреби розвитку системи кібербезпеки підприємств з урахуванням темпів приросту кіберзагроз у світі та рівня кіберризиків, які вони можуть викликати.

Отримані результати дозволили сформувати наступні висновки дослідження. По-перше, у світі відбувається стрімке зростання впровадження та використання

таких сучасних технологій, як штучний інтелект, блокчейн-технології, промислові роботи, IoT та інші. Фактичні та прогнозні емпіричні дані підтверджують, що зараз є активна фаза розвитку Індустрії 4.0. По-друге, застосування аналізованих технологій вимагає підвищення заходів кібербезпеки, що потребує створення надійної та ефективної системи захисту для підприємств. По-третє, розрахунок композитного індикатору кібербезпеки компаній демонструє значне зростання їх потреб у кіберзахисті. В першу чергу це було викликано наслідками пандемії COVID-19, які призвели до зростання кіберзагроз та кіберризиків для підприємств. По-четверте, потреби у кіберзахисті превалюють над сучасним станом технологічного розвитку, хоча компанії демонструють повну готовність удосконалювати захисні механізми, особливо в частині кібербезпеки. По-п’яте, витрати в IT та кіберзахист не покривають зростаючих потреб у протидії кіберзагрозам, хоча за останній рік можна спостерігати баланс між ними. Тобто компанії продемонстрували своє розуміння наслідків кіберзагроз та збільшили витрати для забезпечення їх протидії.

Основними користувачами запропонованого підходу можуть бути асоціації підприємств індустрії кібербезпеки, галузеві асоціації, а також окремі підприємства не залежно від сфери та розмірів діяльності. По-перше, його використання сприятиме формуванню інформаційної бази для оцінювання ризиків, потреб та очікувань щодо кібербезпеки. По-друге, отримані результати допоможуть у формуванні стратегії розвитку системи кібербезпеки для підприємств та окремих галузей. По-третє, запропонована методика дозволить швидко зпрогнозувати тенденції потреб компаній у розвитку кібербезпеки з метою протидії збільшення невиправданих витрат на даний напрям.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [325, 326].

3.4. Модель стійкого розвитку країни, що інтегрує композитні таргети економічного, соціального, політичного та кібербезпекового регуляторних вимірів

В сучасних умовах розвитку суспільства важливим аспектом є комп'ютеризація, цифровізація та інформатизація багатьох процесів, що відбуваються у ньому. Це напряму пов'язано із наслідками стрімкого впровадження результатів промислових революцій Індустрії 4.0 та 5.0 у різні сфери його життєдіяльності. Особливо це помітно в діяльності суб'єктів економіки: сімейних господарств, суб'єктів господарювання та держави. Наприклад, дані процеси призвели до розвитку автономних роботів у промисловості, електронної комерції та Інтернету речей, великих даних та їх аналітики, хмарних рішень, доповненої реальності та штучного інтелекту, тощо. З одного боку, застосування перелічених технологій дало поштовх для появи нових видів виробництв, підвищення ефективності людської праці, формування нових професій, пов'язаних з інформаційними та комп'ютерними технологіями, тобто вони стали важливими драйверами для економічного та соціального розвитку країн та їх населення. З іншого боку, комп'ютеризація та цифровізація призвели до появи такого явища як кіберзлочинність, тобто здійснення злочинів за допомогою інформаційно-комунікаційних технологій.

На сьогоднішній день, її вважають одним з головних ризиків, які впливають на сталий розвиток та дестабілізують збалансованість економіки та соціуму, що було зазначено у звітах Світового форуму [313]. При цьому прогнози є невтішними. Так, очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15 відсотків щорічно, досягнувши 8 трильйонів доларів США у 2023 році та 10,5 трильйонів доларів США у 2025 році, що перевищуватиме показник 2015 році у 2,6 та 3,5 разів відповідно [327]. Найбільш популярним видом кіберзлочинів є фішинг, збитки від якого у 2022 році перевищили 10,3 мільярда доларів, при цьому середня вартість порушень, спричинених викраденими або скомпрометованими обліковими даними,

становила 4,50 мільйона доларів США [328]. Кіберзлочинність розвивається швидкими темпами. Так, в середньому кожні 39 секунд відбувається 1 кібератака в світі [329], що робить даний вид злочину наймасовим та найбільш непередбачуваним. Оскільки тенденції його розповсюдження постійно зростають, то це потребує відповідних мір у сфері кіберзахисту. Наприклад, 66% компаній продовжують нарощувати свої інвестиції у кібербезпеку [330]. Також світові організації схвильовані цією проблемою. ООН на міжнародному рівні розробила та запропонувала 11 норм відповідальної поведінки країн у кіберпросторі [331]. Їх зміст відображає очікування міжнародної спільноти від кожної держави та регіональної організації щодо формування лінії безпекового простору. Вони були створені для боротьби з діями тих держав, які потенційно можуть нести серйозну загрозу міжнародному миру та безпеці та добробуту громадян.

На сьогоднішній день дана проблематика висвітлюється в науковій літературі науковцями з усього світу. Слід відмітити її дослідження у різних галузях: банківська система (Тіан С., Чжао Б. та Оліварес Р. О. [332]),охорони здоров’я (Гафні Р., Павел Т. [333]), електроенергетика (Гейманн Ф., Генрі С., Галус М. [334]), туризм (Параскева А. [335]), морська галузь (Пунт Е., Монштадт Дж., Френк С., Вітте П. [336]), тощо. Але аналізуючи публікації у журналах, що індексуються у базі-даних Scopus за запитом "cybersecurity" & "economic development" було виявлено всього 61 публікацію за період з 2007 по 2023 рік. Це свідчить про низький рівень висвітлення даної проблеми у наукових журналах, хоча з 2018 року кількість публікацій зросла [337]. Це пов’язано з мультидисциплінарністю даної проблеми та специфікою відслідковування наслідків впливу кіберзлочинності на соціально-економічний розвиток країн.

Процеси розповсюдження кіберзлочинності важко зупинити, оскільки вони пов'язані з технологічним розвитком, який полегшує доступ людини до технологій та надає впевненості отримати гроші легким шляхом без прямого впливу на життя людини. Саме тому даний фактор потребує більш детального вивчення, особливо в контексті його впливу на соціально-економічний розвиток

країн. Оскільки кіберзлочинність є негативним фактором, то його дослідження повинно відбуватися з боку можливостей країн йому протидіяти, тобто з боку забезпечення кібербезпеки.

Для реалізації дослідження було обрано чотири групи показників, які ідентифікують чотири сфери розвитку країни: економічну, соціальну, політичну та кібербезпекову. В розрізі кібербезпекового напрямку було обрано інтегральний індекс – національний індекс кібербезпеки (National Cybersecurity Index – NCSI) [338]. Його вибір обумовлено тим, що він дозволяє оцінити ступінь забезпечення кіберзахисту країни на національному рівні, її спроможність захистити різні сфери життєдіяльності від різного рівня кіберзагроз. Даний індикатор за своєю сутністю є показником-стимулятором, що буде враховано в процесі подальшої нормалізації.

Для ідентифікації економічної сфери було обрано три показника: ВВП на душу населення (GDP per capita) [339], інфляція (Inflation, GDP deflator (annual %)) [340] та чиста міграція (Net migration) [341]. Вибір ВВП на душу населення обумовлений тим, що він відображає рівень економічної активності та якості життя населення в окремих країнах, який у підсумку символізує рівень економічного зростання та розвитку країни. Інфляція вимірює швидкість змін цін в економіці в цілому та дає уявлення про реальні зміни в економіці. Чим більше його значення, тим більша залежність ВВП від зростання цін, що характеризує негативні процеси в економіці. Показник чистої міграції не є індикатором, що прямо характеризує рівень економічного розвитку, але його застосування може дати опосередкований висновок, щодо економічної ситуації в країні. Якщо кількість людей, що виїжджають з країни, перевищує кількість тих, що залишається, тобто має місце негативний коефіцієнт міграції, то можна сказати, що рівень життя в даній країні є несприятливим. В більшості випадків причинами міграції є економічні причини та військові дії. В результаті міграційних процесів страждає економіка країни, оскільки виїжджає економічно активне населення. Тому саме цей індикатор було обрано для ідентифікації

економічних детермінант. ВВП на душу населення та чиста міграція є показниками-стимуляторами, а інфляція є показником-дестимулятором.

Політичний розвиток країни залежить від багатьох факторів і є важливим в тому плані, що в залежності від прийняття правильних рішень урядом, формування демократичних вільностей населення та створення «здорового» політичного «клімату» в країні, формується стійкий фундамент для сталого розвитку країни в цілому. В групу політичних детермінант було обрано наступні: оцінка політичної стабільності і відсутність насильства/тероризму (Political Stability and Absence of Violence/Terrorism: Estimate) [342], оцінка ефективності уряду (Government Effectiveness: Estimate) [343], оцінка верховенства права (Rule of Law: Estimate) [344], оцінка контролю корупції (Control of Corruption: Estimate) [345] та оцінка голосу та відповідальності (Voice and Accountability: Estimate) [346]. Політична стабільність та відсутність насильства/тероризму вимірює сприйняття ймовірності політичної нестабільності та/або політично вмотивованого насильства, включаючи тероризм. Ефективність уряду характеризує якість державних послуг та служби, ступінь її незалежності від політичного тиску, якість реалізації політики країни та довіру населення до неї. Індикатор верховенства права оцінює ситуацію в країні, наскільки її суб’єкти довіряють правилам суспільства та дотримуються. Оцінка контролю корупції характеризує міру використання влади для приватних цілей, а також її «захоплення» елітами. Голос та відповідальність надає уявлення про ступінь свободи слова в країні, свободи асоціацій і вільностей ЗМІ, а також незалежного вибору населення країни. Обрані індикатори є стимуляторами, які надають висновок щодо потенціалу незалежного та демократичного політичного розвитку країни.

Групу показників соціального розвитку сформували: робоча сила (Labor force, total) [347], рівень безробітних (Unemployment, total (% of total labor force) (modeled ILO estimate)) [348], очікувана тривалість життя при народженні (Life expectancy at birth, total (years)) [349], наймані працівники (Wage and salaried workers, total (% of total employment) (modeled ILO estimate)) [350]. Показник

робочої сили демонструє кількість людей, які зараз працюють, є безробітними, але шукають роботу, а також ті, хто вперше шукає роботу. Для адекватного порівняння та аналізу було прийнято рішення скоректувати цей показник на кількість населення країни. Рівень безробітних представляє собою частку робочої сили, яка не має роботи, але готова та шукає її. Очікувана тривалість життя при народженні визначається як довго в середньому може прожити новонароджена дитина, якщо поточні показники смертності не змінюються, на що впливає соціальний розвиток країни та якість життя. Показник найманих працівників характеризує відсоток зайнятих у державному чи приватному секторі з оплатою праці. Індикатори робочої сили, очікуваної тривалості життя та найманих працівників є показниками-стимуляторами. Рівень безробіття виступає показником-дестимулятором.

Дослідження проводилося на прикладі 147 країн світу за період 2022 рік. Для проведення розрахунків необхідно здійснити нормалізацію обраних показників, оскільки вони вимірюються у різних одиницях. З цією метою для показників стимуляторів було використано формулу природньої нормалізації, а для дестимуляторів – нормалізацію Севіджа. Результати розрахунків наведено у Додатку К.

На наступному кроці необхідно провести процес згортки показників для отримання інтегральних індикаторів, що характеризують економічний, соціальний та політичний розвиток. Оскільки для сфери кібербезпеки було обрано тільки один показник, то потреба у згортці для даного напрямку відпадає. Для здійснення даної операції визначимо ваги кожного показника. При цьому будемо враховувати таку аксіому, що стан системи кіберзахисту залежить від рівня економічного, соціального та політичного розвитку. Реалізацію даного кроку виконаємо на основі побудови стандартизованих рівнянь регресії (3.35 – 3.37):

$$\widehat{y_i^c} = a_1 X^e_{1\,i} + a_2 X^e_{2\,i} + a_3 X^e_{3\,i}, \tag{3.35}$$

$$\widehat{y_i^c} = b_1 X^s_{1\,i} + b_2 X^s_{2\,i} + b_3 X^s_{3\,i} + b_4 X^s_{4\,i}, \tag{3.36}$$

$$\widehat{y_i^c} = c_1 X^p_{1\,i} + c_2 X^p_{2\,i} + c_3 X^p_{3\,i} + c_4 X^p_{4\,i} + c_5 X^p_{5\,i} \quad (3.37)$$

де $\widehat{y_i^c}$ – модельоване значення національного індексу кібербезпеки для і-ї країни;

$X^e_{1\,i}, X^e_{2\,i}, X^e_{3\,i}$ – значення показників, що характеризують економічний розвиток для і-ї країни;

$X^s_{1\,i}, X^s_{2\,i}, X^s_{3\,i}, X^s_{4\,i}$ – значення показників, що характеризують соціальний розвиток для і-ї країни;

$X^p_{1\,i}, X^p_{2\,i}, X^p_{3\,i}, X^p_{4\,i}, X^p_{5\,i}$ – значення показників, що характеризують політичний розвиток для і-ї країни;

a_1, a_2, a_3; b_1, b_2, b_3, b_4; c_1, c_2, c_3, c_4, c_5 – параметри стандартизованої регресії.

Перед знаходженням параметрів регресії побудуємо кореляційну матрицю, яка демонструватиме значення коефіцієнтів кореляції між усіма парами аналізованих показників. Результати її побудови із використанням мови програмування Python представлені на рисунку 3.49.

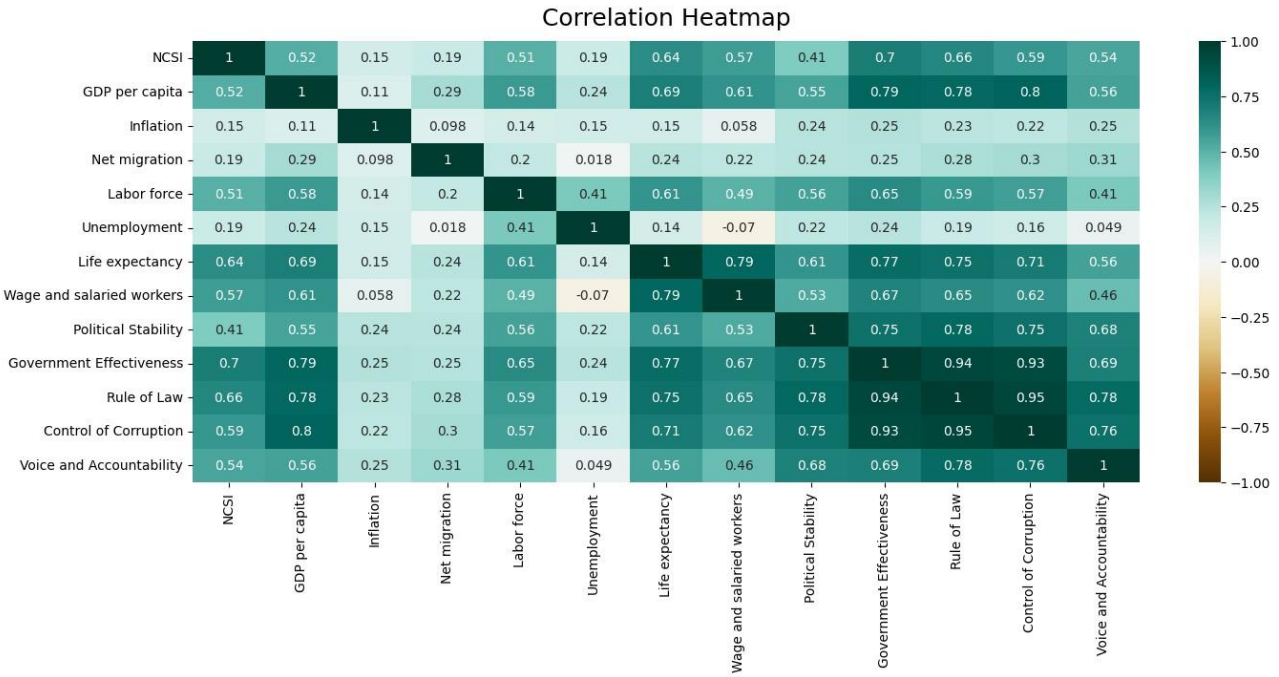


Рисунок 3.49 – Кореляційна матриця

Отримані значення коефіцієнтів кореляції свідчать, що між деякими парами показників існує тісний кореляційний зв'язок, що говорить про наявність мультиколінеарності. Але оскільки нам потрібно визначити вагові коефіцієнти для всіх показників, то усунення деяких з моделі не дозволить досягти поставленої мети дослідження. Тому для побудови стандартизованих рівнянь регресії використаємо методи Lasso, Ridge та ElasticNet, які дозволять отримати не завищені за рахунок мультиколінеарності оцінки. Дану процедуру виконаємо із використанням мови програмування Python та для отримання адекватних значень проведемо її на двох наборах даних – тренувальному та тестовому (сформовану вибірку даних поділимо у пропорції 70% на 30%). Результати розрахунків представлені на рисунках: 3.50 для оцінювання впливу показників економічного розвитку на сферу кібербезпеки; 3.51 для оцінювання впливу показників соціального розвитку на сферу кібербезпеки; 3.52 для оцінювання впливу показників політичного розвитку на сферу кібербезпеки.

```
Результати LASSO регресії

[0.38606457 0.06176941 0.        ]
MSE train: 0.7553134, test: 0.7145047
R^2 train: 0.2540572, test: 0.2563019

Результати RIDGE регресії

[0.45040267 0.13514392 0.10673364]
MSE train: 0.732, test: 0.732
R^2 train: 0.277, test: 0.238

Результати ElasticNet регресії

[0.40112526 0.09673254 0.04586067]
MSE train: 0.741, test: 0.717
R^2 train: 0.268, test: 0.254
```

Рисунок 3.50 – Результати оцінювання параметрів Lasso, Ridge та ElasticNet для показників економічного розвитку

```
Результати LASSO регресії

[0.11856685 0.         0.4182953  0.06149936]
MSE train: 0.5924758, test: 0.5409084
R^2 train: 0.4148746, test: 0.4369910

Результати RIDGE регресії

[0.13833823 0.08647025 0.40262278 0.1716068 ]
MSE train: 0.573, test: 0.510
R^2 train: 0.434, test: 0.469

Результати ElasticNet регресії

[0.13314749 0.04569486 0.37228496 0.13783944]
MSE train: 0.579, test: 0.520
R^2 train: 0.428, test: 0.459
```

Рисунок 3.51 – Результати оцінювання параметрів Lasso, Ridge та ElasticNet для показників соціального розвитку

```
Результати LASSO регресії

[-0.          0.56481654  0.          0.          0.00774867]
MSE train: 0.5726216, test: 0.4354145
R^2 train: 0.4344825, test: 0.5467951

Результати RIDGE регресії

[-0.43983537  1.14621023  0.44061109 -0.76953516  0.22221238]
MSE train: 0.427, test: 0.429
R^2 train: 0.579, test: 0.553

Результати ElasticNet регресії

[-0.14357351  0.583423    0.05248227 -0.          0.09283668]
MSE train: 0.528, test: 0.410
R^2 train: 0.479, test: 0.573
```

Рисунок 3.52 – Результати оцінювання параметрів Lasso, Ridge та ElasticNet для показників політичного розвитку

Розраховані показники середньоквадратичної похибки (MSE) та коефіцієнта детермінації (R^2) є найкращими для моделі Ridge регресії для трьох груп показників (рисунки 3.50-3.52). Вони демонструють найменше значення похибки та найвище значення коефіцієнту детермінації. При цьому це є явним як

для тренувального, так і для тестового набору даних. Для показників соціального та політичного розвитку було визначено, що існує середній зв'язок між цими показниками та системою кіберзахисту. Це підтверджує значення коефіцієнту детермінації, близького до 0,5. Що стосується економічного впливу на сферу кібербезпеки, то зв'язок між ними є слабким. Це відбувається за рахунок слабкого впливу інфляції та чистої міграції. Оскільки економічний розвиток характеризується не тільки виробленим валовим внутрішнім продуктом, що є позитивним ефектом, але й може стримуватися такими негативними ефектами як інфляція та міграційні процеси, то залишаємо дані показники для подальших розрахунків.

Отримані Ridge параметри показали, що найбільший вплив на кібербезпеку країни здійснює ВВП на душу населення (рисунок 3.50), очікувана тривалість життя при народженні (рисунок 3.51), політична стабільність і відсутність насильства/тероризму, ефективність уряду, верховенство права та контроль корупції (рисунок 3.52).

Визначення інтегрального показника в розрізі кожної групи проведемо за допомогою трансформованої згортки Кіні:

$$K_{jg} = \frac{1}{G} \cdot \prod_{i} \left(1 + G \cdot w_{ig} \cdot n_{igj}\right), \tag{3.38}$$

де K_{jg} – інтегральний показник Кіні в розрізі j-ї країни в межах g-тої групи показників;

G – загальна кількість показників в розрізі g-тої групи;

n_{igj} – нормалізоване значення і-го показника g-тої групи в розрізі j-ї країни;

w_{ig} – ваговий коефіцієнт і-го показника в межах g-тої групи, визначений на основі отриманих параметрів Ridge регресії для кожної групи показників. Оскільки ваги у сукупності повинні дорівнювати 1, то визначені коефіцієнти

регресії перерахуємо у пропорційному відношенні, щоб їх сума складала 1. Ті параметри, які є від'ємними, беруться за їх абсолютним значенням. Результат розрахунку вагових коефіцієнтів представлено у таблиці 3.31.

Таблиця 3.31 – Розрахунок вагових коефіцієнтів для формування інтегральних показників

Назва групи показників	Назва індикатора	Значення вагового коефіцієнта
Економічний розвиток	ВВП на душу населення	0,650607
	Інфляція	0,195216
	Чиста міграція	0,154177
Соціальний розвиток	Робоча сила	0,173131
	Рівень безробітних	0,108218
	Очікувана тривалість життя при народженні	0,503884
	Наймані працівники	0,214767
Політичний розвиток	Оцінка політичної стабільності і відсутність насильства/тероризму	0,145718
	Оцінка ефективності уряду	0,37974
	Оцінка верховенства права	0,145975
	Оцінка контролю корупції	0,254948
	Оцінка голосу та відповідальності	0,073619

Застосовуючи формулу 3.4 та результати визначених вагових коефіцієнтів, проведено розрахунок інтегральних показників на основі економічних, соціальних та політичних детермінант розвитку країн. Для подальшого дослідження є необхідність в отриманні значень від 0 до 1, тому застосуємо формулу природньої нормалізації для отримання нормалізованих значень інтегральних показників.

На наступному кроці проведемо кластерний аналіз визначення груп країн, близьких за рівнем збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант. З цією метою застосуємо метод самоорганізованих карт Кохонена, оскільки для даного методу проблема мультиколінеарності не є критичною. Реалізацію даного процесу буде виконано за допомогою аналітичного пакету Viscovery SOMine. Розподіл кластерів буде

здійснюватися з використанням методу Уорда, який дозволяє провести агломеративну ієрархічну кластеризацію, в якій критерієм вибору є оптимальне значення цільової функції, в якості якої виступає сума квадратів похибок. В результаті було отримано чотири кластери країн (Рисунок 3.53).

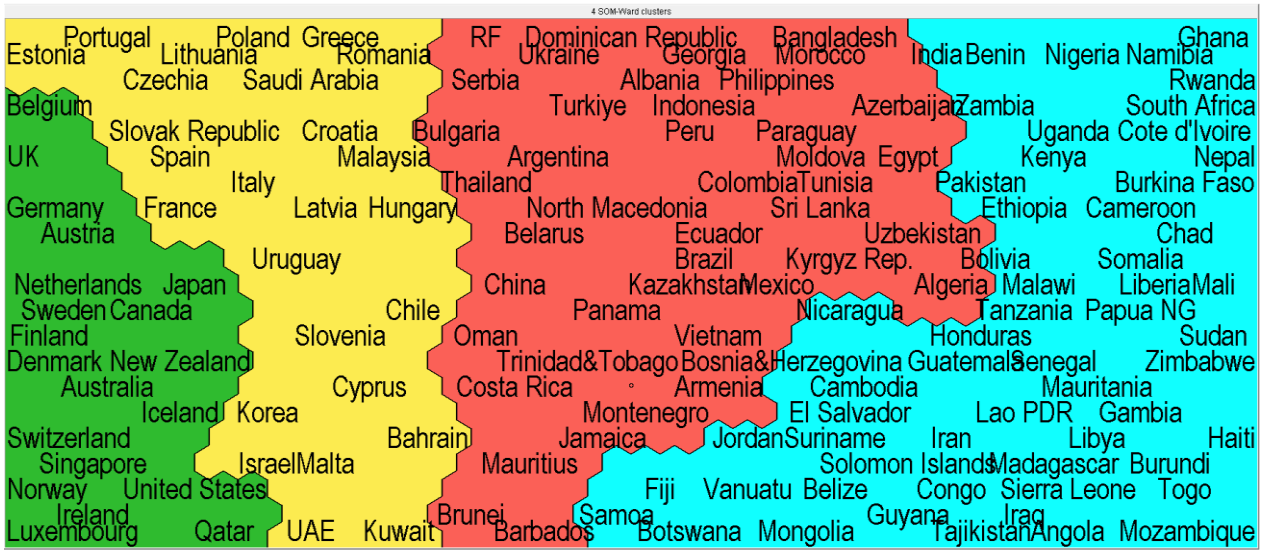


Рисунок 3.53 – Результати кластерного аналізу

Зелений кластер (кластер 4) сформували країни, які відносяться до розвинених країн згідно класифікації ООН (рисунок 3.53). Їх можна охарактеризувати як країни з високим рівнем збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант. У жовтий кластер (кластер 3) увійшли більшість розвинених країн та тих, що розвиваються. При цьому рівень рівноваги між аналізованими сферами відповідає достатньому. Червона група (кластер 2) – це країни, які розвиваються, і для яких є характерним середній ступінь збалансованості між кібербезпековою, економічною, соціальною та політичною сферами. Блакитний кластер (кластер 1) сформовано на основі країн, які розвиваються або є найменш розвиненими. Їм відповідає низький рівень збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант.

Проаналізуємо результати кластеризації, проведеної за кібербезпековою детермінантою. На рисунку 3.54 можна спостерігати неоднорідний розподіл

країн. Так до четвертого найбільш збалансованого кластеру увійшли країни, для яких рівень кібербезпеки знаходиться в межах від 0,5285 до 1. Країни третього кластеру мають великий розкид значень – від 0,3428 до 0,9857. Країни другого кластеру – від 0,1714 до 0,8428. Країни першого кластеру – від 0 до 0,5142. Це можна пояснити тим, що збалансованість досягається за рахунок рівнозначного розвитку кібербезпекової, економічної, соціальної та політичної сфер. Тому недостатній розвиток системи кіберзахисту буде компенсовано за рахунок більш високого рівня розвитку інших сфер. Наприклад, Люксембург демонструє показник кібербезпеки на рівні вище середнього (0,6856), але за рахунок високого рівня економічного (1,000) та політичного (0,8999) розвитку, він підпадає до категорії країн з найвищим рівнем збалансованої взаємодії аналізованих чотирьох сфер. За даних умов такі країни, як Люксембург, мають відповідні резерви для підвищення безпекового рівня країни.

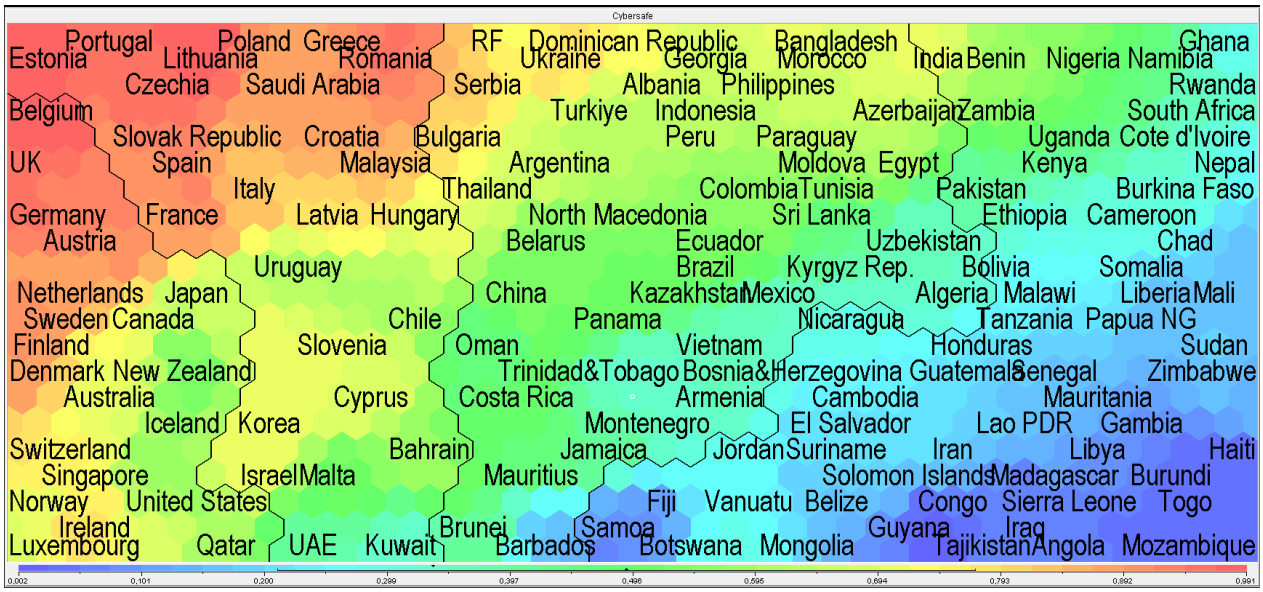


Рисунок 3.54 – Результати кластерного аналізу країн, згрупованих за кібербезпоковою детермінантою

Візуалізація результатів кластеризації, проведеної за соціальною детермінантою, демонструє більш рівномірний розподіл (рисунок 3.55). Так, країни четвертого кластеру – це країни, соціальний розвиток яких коливається навколо середнього значення 0,8071 і для яких характерні високі стандарти

соціального розвитку. Це Катар, Сингапур, Японія, Норвегія та Ісландія. Для країн третього кластеру середнє значення їх інтегрального показника соціального розвитку дорівнює 0,6757. Серед них виділяються ОАЕ, Кувейт, Бахрейн, Мальта та Південна Корея. Країнам другого кластеру відповідає середнє значення соціального розвитку на рівні 0,4642, країнам першого кластеру – 0,2397. Аналізуючи результати, представлені на рисунках 3.54 та 3.55, можна зробити висновок, що країни з високим рівнем кіберзахисту мають нижчий рівень соціального захисту і навпаки. Це можна спостерігати практично в усіх кластерах. Наприклад, Бельгія має найвищий рівень кібербезпеки, при цьому соціальний розвиток знаходиться на рівні вище середнього. І навпаки, Катар є країною з найвищим рівнем соціальних стандартів, при цьому кіберзахист є середнім. Можливе пояснення даному факту є сприяння розвитку IT-сфери, яка дозволить стимулювати розвиток соціальної сфери.

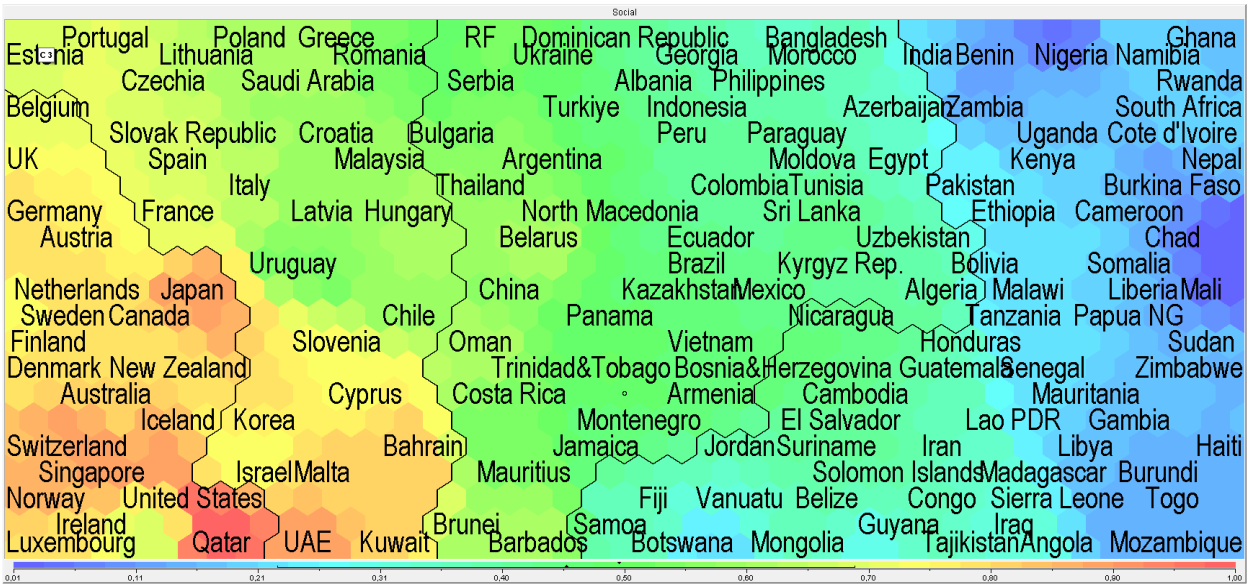


Рисунок 3.55 – Результати кластерного аналізу країн, згрупованих за соціальною детермінантою

Візуальний аналіз результатів кластеризації за економічною детермінантою показує також більш рівномірний розподіл (рисунок 3.56). Є певні викиди, які відповідають 4-му (Люксембург з найвищим рівнем ВВП на душу населення у світі) та 1-му кластурам (Судан та Пакістан із найнижчими показниками економічного розвитку). Країнам четвертого кластеру відповідає

середнє значення інтегрованого показника економічного розвитку 0,6360, які представлені тільки економічно розвинутими країнами. До топ п'яти країн цієї групи відносяться Люксембург, США, Норвегія, Ірландія та Швейцарія. Країни третього кластеру – це країни економічно розвинені або ті, що розвиваються. Середнє значення їх економічної детермінанти дорівнює 0,3398. Серед них виділяються Франція, Іспанія, Ізраїль, ОАЕ та Кувейт. Країнам другого кластеру відповідає середнє значення економічного розвитку на рівні 0,2039, країнам першого кластеру – 0,1610. Кластерний аналіз економічної та кібербезпекової детермінанти не показує певних закономірностей, оскільки рівень кореляції між ними є середнім (0,5247). Тобто економічно розвинені країни можуть мати як високий, так і середній рівень розвитку кіберсфери. Економіка може стимулювати дані процеси, але на даному етапі на це впливають в більшій мірі соціальні фактори.

Рисунок 3.56 – Результати кластерного аналізу країн, згрупованих за економічною детермінантою

На рисунку 3.57 представлені результати кластерного аналізу країн, згрупованих за політичною детермінантою, які демонструють також розкид значень для певних груп. Четвертий кластер демонструє найбільшу збалансованість. Сюди увійшли країни, для яких середній рівень політичної детермінанти відповідає 0,8066. Топ п'ять країн сформували Данія, Фінляндія, Швейцарія, Норвегія та Люксембург. Середнє значення для країн третьої групи

дорівнює 0,4557 і сюди відносяться Естонія, Франція, Португалія, Уругвай та Південна Корея. Країни другого та першого кластерів представлені тими, які мають відповідні обмеження у демократичних свободах та є політично незбалансованими. Відповідно, середнє значення для другого кластеру знаходиться на рівні 0,2268, для першого – 0,1567. Кореляційний зв'язок між політичної та кібербезпековою детермінантою дорівнює 0,6046. І хоча його тіснота є середньою, але зв'язок між парами соціальна та кібербезпекова, політична та кібербезпекова детермінанти є вищим.

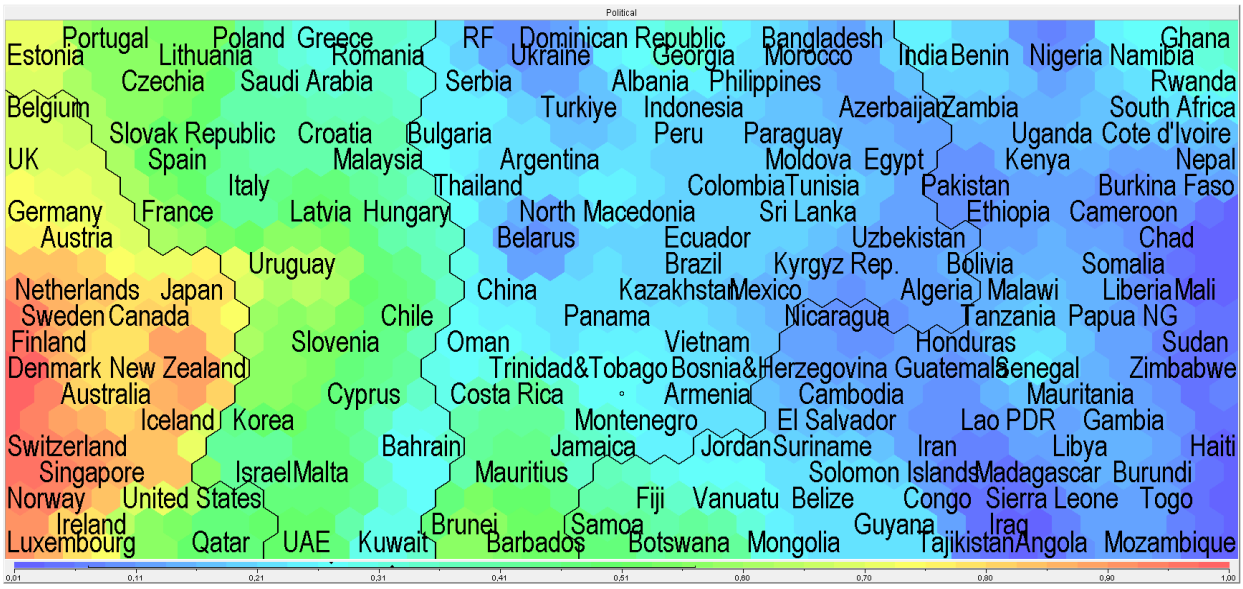


Рисунок 3.57 – Результати кластерного аналізу країн, згрупованих за політичною детермінантою

Аналіз якості проведеного кластерного аналізу представлений на рисунках Л.1-Л.3 Додатку Л. Помилка квантування, яка демонструє різницю вхідних вибірок порівняно з відповідними змодельованими нейронами, знаходиться в межах 5% і не перевищує 0,0203. Особливо помітні викиди в четвертому та третьому кластерах. Частота спостережень для кластерів переважно є високою, тільки окремі спостереження вирізняються в окремих кластерах, що є допустимим в розрізі проведення кластерного аналізу. Оцінка розмірності свідчить про те, що більшість спостережень груповані за двома та більше ознаками, що дозволяє прийняти результати аналізу, як якісні.

Основним висновком даного етапу дослідження є те, що в основному ступінь збалансованого розвитку країни досягається за рахунок сталості її окремих сфер. При цьому на кібербезпекова детермінанта в більшій мірі залежить від соціального та політичного впливу, хоча її розвиток є компенсацією для розвитку інших сфер.

Перед реалізацією останнього етапу проведемо розрахунок інтегрального показника збалансованого розвитку країн в залежності від взаємодії соціальних, економічних, політичних та кібербезпекових детермінант, для чого скористуємося згорткою Кінні за формулою 3.4, а потім застосуємо формулу природньої нормалізації для приведення його значень в межах від 0 до 1. Результати розрахунків представлені у Додатку М. В процесі згортки застосуємо однакові ваги для всіх детермінант, що буде свідчити про однаковий їх внесок у формування інтегрального показника та забезпечення збалансованого рівня.

На останньому кроці проведемо аналіз охоплення даних (Data Envelopment Analysis – DEA) для окремого кластеру країн, який дозволить оцінити ефективність збалансованого розвитку країн в залежності від взаємодії соціальних, економічних, політичних та кібербезпекових детермінант. При цьому буде враховуватись можливість стимулювання сфери кібербезпеки як потенційного драйверу забезпечення сталого розвитку країн.

В основі проведення аналізу охоплення даних знаходяться оптимізаційні моделі CCR, яку було запропоновано Чарнсом А., Купером У. та Родесом Е., та та її модифікований варіант BCC, розроблену Банкером Р., Чарнсом А. та Купером У. Вони орієнтовані на вхід (ресурси) та їх мінімазацію, а також вихід (результуючі показники) та його максимізацію. Математичний апарат даних моделей представлений формулами (3.39) – (3.42) [49]:

$$\max_{u,v} \theta_s = \sum_{p=1}^{z} u_{ps} y_{ps} \qquad (3.39)$$

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

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

$$\begin{cases} \sum_{i=1}^{m} v_{is}x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps}y_{pj} + k_s \le \sum_{i=1}^{m} v_{is}x_{ij} \\ u_p, v_i \ge \gamma \\ k_s - \ unconstrained \end{cases} \tag{3.40}$$

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

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - k_s \ge \sum_{p=1}^{z} \alpha_p y_{pj} \\ \alpha_p, \beta_i \ge \gamma \\ k_s - \ unconstrained \end{cases} \tag{3.41}$$

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

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - \sum_{p=1}^{z} \alpha_p y_{pj} \ge 0 \\ \alpha_p, \beta_i \ge \gamma \end{cases} \tag{3.42}$$

де θ – рівень ефективності збалансованої взаємодії кібербезпекової, економічної, політичної та соціальної детермінант, визначений як коефіцієнт між зваженою сумою виходів та входів;

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

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

y_p – p-та характеристика умовних виходів, тобто значень індексу збалансованої взаємодії кібербезпекової, економічної, політичної та соціальної детермінант для кожної країни;

x_i – i-та характеристика умовних входів, тобто значень кібербезпекової, економічної, політичної та соціальної детермінант;

γ – це невелике додатне дійсне число, яке виключає можливість набуття змінними нульового значення [49].

Моделі CCR (3.39) та BCC (3.40) направлені на оцінку структурної ефективності розподілу кібербезпекової, економічної, соціальної та політичної детермінант із забезпеченням їх мінімального входу, якщо виходом є інтегральний показник ефективності їх збалансованої взаємодії. Моделі CCR (3.41) та BCC (3.42) дозволяють оцінити ефективність збалансованої взаємодії чотирьох детермінант шляхом визначення максимального значення їх інтегрального індексу.

DEA-аналіз було реалізовано за допомогою аналітичного пакету “Frontier Analyst”. Для дослідження в кожному кластері країн було обрано 12 країн, які мають найвище та найнижче значення інтегрального індексу, для яких проводився Data Envelopment Analysis. Це було продиктовано необхідністю демо-версії даної програми. Мінімальне значення вагів у програмі було встановлено на рівні 0,25 для кожної детермінанти. Результати CCR моделі відповідатимуть більш реалістичному сценарію розвитку, BCC –

відображатимуть умови кардинальних змін віддачі від масштабу, що є більш нереалістичним для макроекономічних систем.

Проаналізуємо результати DEA-аналізу для країн 4-го кластеру. За умови мінімазації входів та забезпечення виходу на тому самому рівні країни цієї групи мають значний резерв, особливо в соціальній сфері (-34,16%) (Рисунок Н.1 Додатку Н). Найменший запас пов'язаний з кібербезпековою детермінантою, що свідчить про необхідність її посилення в майбутньому. Це найбільш актуальним для США, Великобританії та Нової Зеландії (Рисунок Н.2 Додатку Н). Для досягнення зростання рівня збалансованості на 20,1% потрібне збільшення кожної з аналізованих детермінант від 19,46% до 20,42% (Рисунок Н.3 Додатку Н). За даних умов досягнення ефективності буде для всіх країн на рівні 100% (Рисунок Н.4 Додатку Н). За умов максимізації ефективності за рахунок досягнення максимального рівня збалансованості чотирьох детермінант, а саме на 3,4% (Рисунок Н.5 Додатку Н), країни 4-го кластеру мають резерв соціальної сфери на рівні 34,51%, політичної – 28,09%, економічної – 22,87%, кібербезпекової – 11,13%. Це можливо, якщо країни даного кластеру забезпечують ефективність, представлену на рисунку Н.6 Додатку Н. Максимальний вихід може бути отриманий на 19,61%, але всі сфери потребують більш стрімкого розвитку (Рисунок Н.7 Додатку Н). При цьому всі країни матимуть 100% ефективного розвитку (Рисунок Н.8 Додатку Н).

Моделі яких країн демонструють більш стійку ефективність при взаємодії пар детермінант? Аналіз пари взаємодії економічної та кібербезпекової детермінанти свідчить про наступне (рисунок 3.58). Японія та Данія досягають більшої ефективності в кібербезпекові сфері, Люксембург та Норвегія – в економічній. Найбільшу збалансованість демонструє Швейцарія. Всі інші країни показують значний дисбаланс цих двох напрямків.

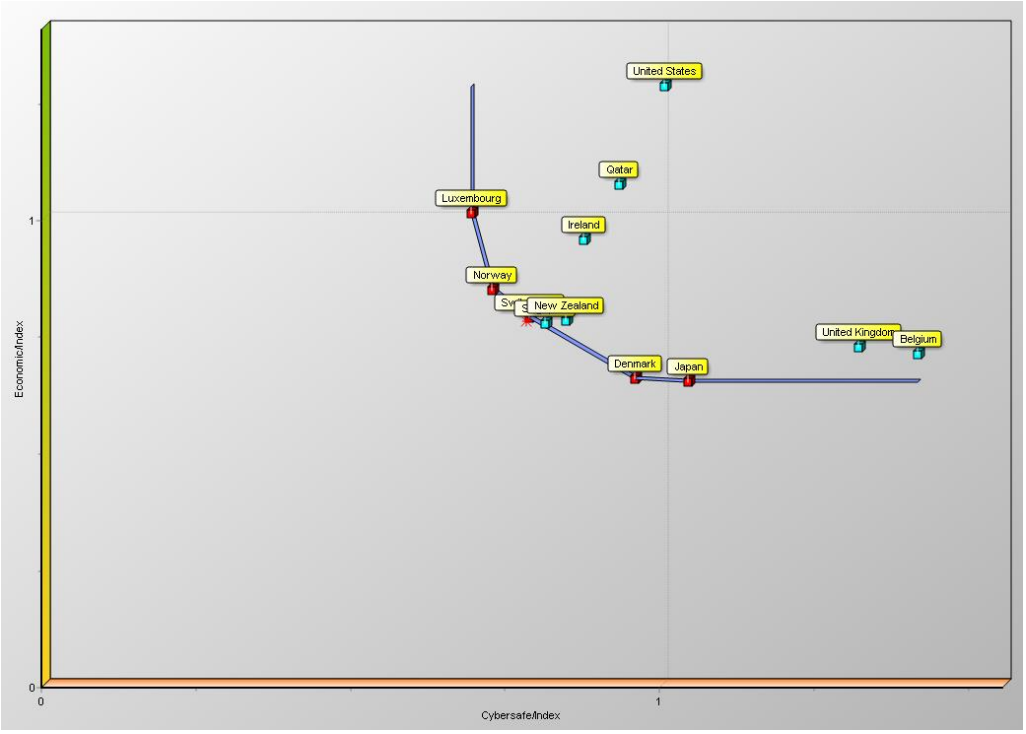


Рисунок 3.58 – Фронтірна діаграма ефективності збалансованої взаємодії економічних та кібербезпекових детермінант для країн 4-го кластеру

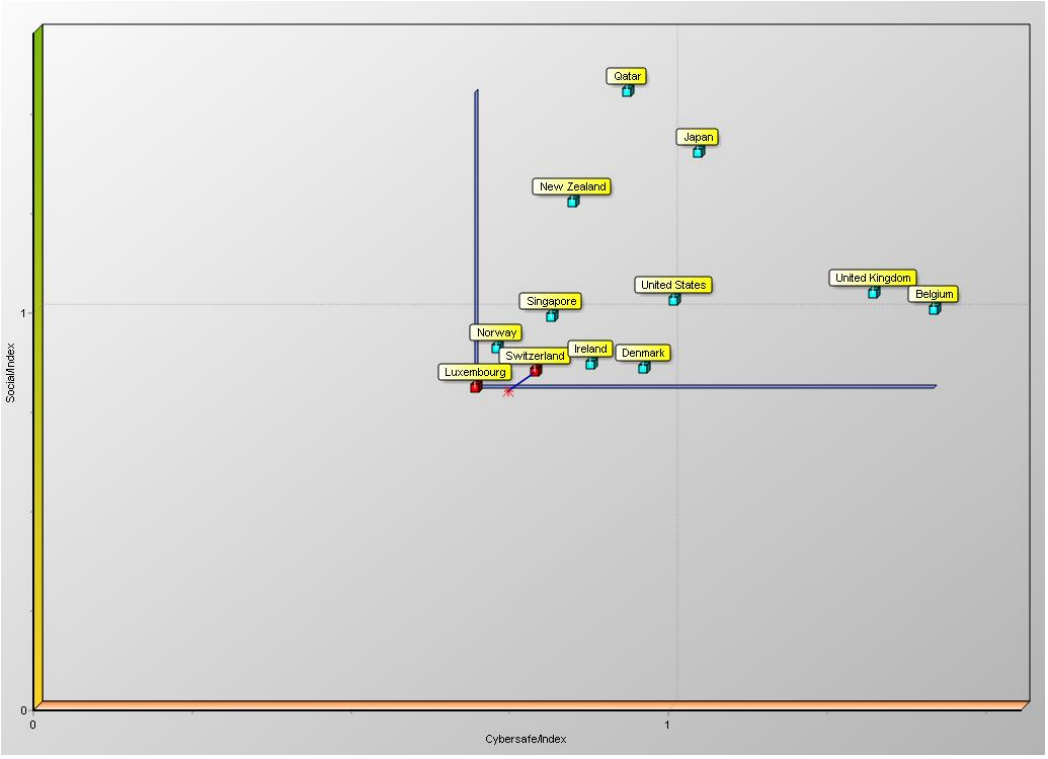


Рисунок 3.59 – Фронтірна діаграма ефективності збалансованої взаємодії соціальних та кібербезпекових детермінант для країн 4-го кластеру

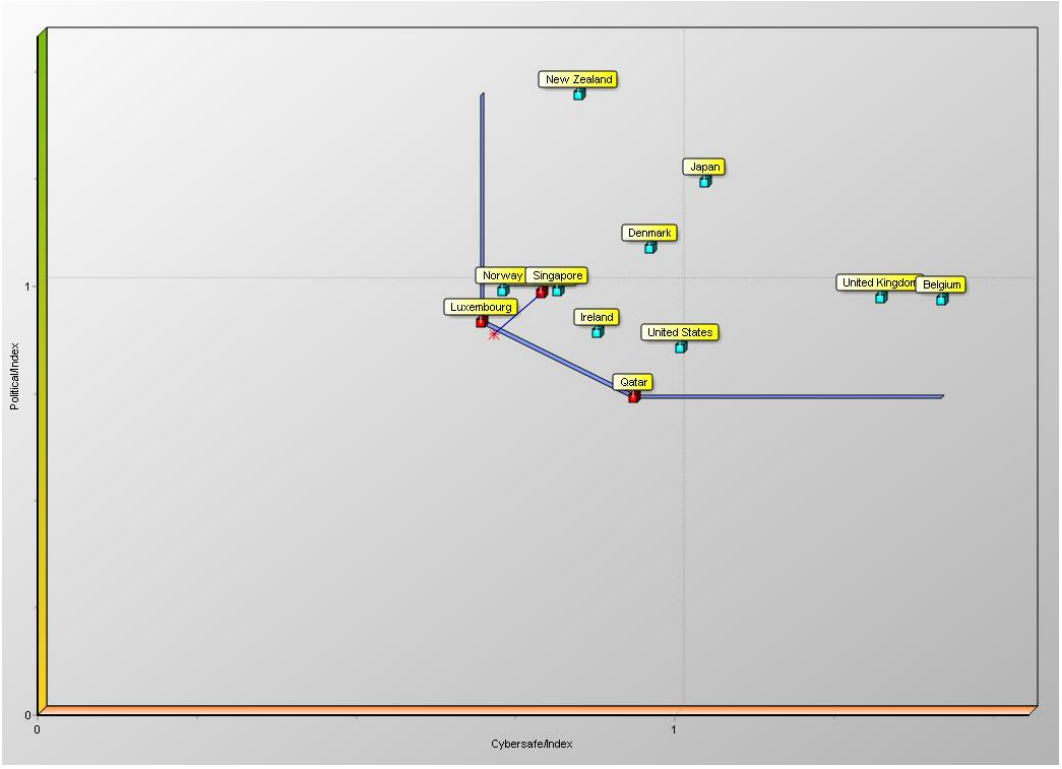


Рисунок 3.60 – Фронтірна діаграма ефективності збалансованої взаємодії політичних та кібербезпекових детермінант для країн 4-го кластеру

При порівняння соціальних та кібербезпекових детермінант (рисунок 3.59) найбільш ефективною є їх збалансованість для Люксембургу. Швейцарія є дуже близькою до забезпечення ефективності цих двох детермінант. На рисунку 3.60 можна побачити, що для Люксембургу найвища ефективність є для політичної детермінанти, а для Катару – кібербезпекової. При цьому Сингапур також наближається до забезпечення ефективності політичного розвитку.

Проведемо аналіз результатів оцінки ефективності для країн 3-го кластеру. Для забезпечення мінімазації входів та виходу на тому самому рівні країни цієї групи мають резерви по всім чотирьом детермінантам. Але найбільші значення відповідають соціальній сфері (34,4%) та кібербезпековій (25,83%) (Рисунок Н.9 Додатку Н). Неможливість досягнення 100% ефективності характерно для Чілі, Угорщини, Чехії та Малайзії (Рисунок Н.10 Додатку Н). В умовах здійснення більш критичних змін країни даного кластеру мають можливості досягнення збалансованості всіх чотирьох сфер, якщо запас кібербезпеки сягатиме 47,66% (Рисунок Н.11 Додаток Н). Всі країни, окрім Чехії, матимуть можливості

потенційного розвитку за даних умов на рівні 100% ефективної збалансованої взаємодії 4 детермінант (Рисунок Н.12 Додаток Н). За умов досягнення максимального рівня збалансованості чотирьох детермінант, а саме підвищення її на 50,84% (Рисунок Н.13 Додатку Н), країни 3-го кластеру мають резерв соціальної сфери на рівні 35,42% та кібербезпекової – 13,51%. Для всіх інших потрібно забезпечити зростання на 0,12%. Чилі, Чехії, Угорщині та Малайзії важко буде досягти 100% ефективності за цих умов (рисунок Н.14 Додатку Н). Максимальний вихід може бути отриманий на рівні 27,79%. При цьому резерв кібербезпекової сфери повинен бути на рівні 71,67%, всі сфери потребують зростання (Рисунок Н.15 Додатку Н). Практично всі країни матимуть 100% ефективність (Рисунок Н.16 Додатку Н).

Аналіз пари взаємодії економічної та кібербезпекової детермінанти для країн 3-го кластеру показує наступне (рисунок 3.61). Естонія досягають більшої ефективності в кібербезпекові сфері, Кувейт та Південні Корея – в економічній. Всі інші країни показують значний дисбаланс цих двох напрямків. При цьому вони фактично тяжіють до більшої ефективності кібербезпекової детермінанти. При порівняння соціальної та кібербезпекової сфери (рисунок 3.62) найбільш ефективною є їх збалансованість для Кувейту та Південної Кореї, але завдяки вищим їх соціальним можливостям. Франція та Естонія демонструють збалансованість, яка спрямована на кібербезпекові заходи. Для інших країн результати показують неефективність збалансування цих сфер у напрямку до кібербезпекового. На рисунку 3.63 можна побачити, що для Кувейту та Бахрейну характерне ефективне співвідношення політичної та кібербезпекової детермінант. При цьому для першої країни ефективність переважає для політичної сфери, а для другої – кібербезпекової. Естонія прямує також до забезпечення ефективного балансу аналізованих сфер.

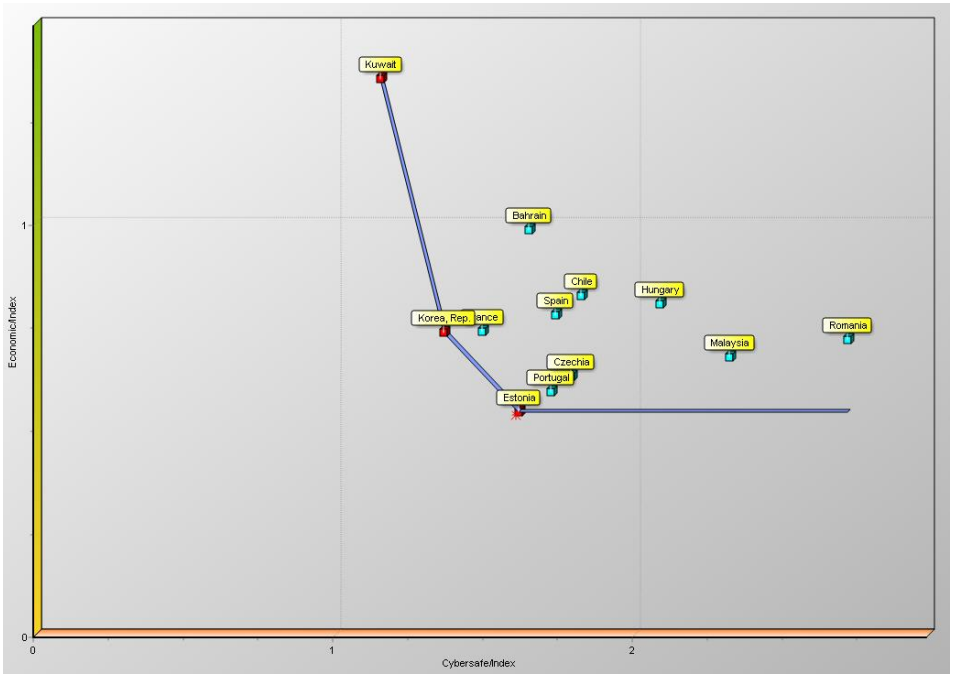


Рисунок 3.61 – Фронтірна діаграма ефективності збалансованої взаємодії економічних та кібербезпекових детермінант для країн 3-го кластеру

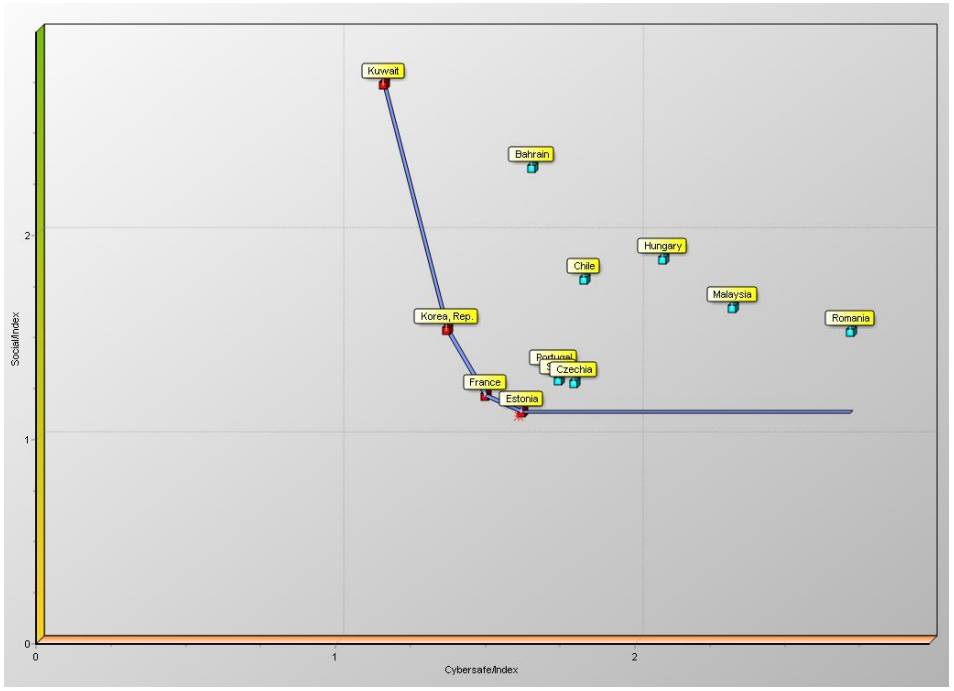


Рисунок 3.62 – Фронтірна діаграма ефективності збалансованої взаємодії соціальних та кібербезпекових детермінант для країн 3-го кластеру

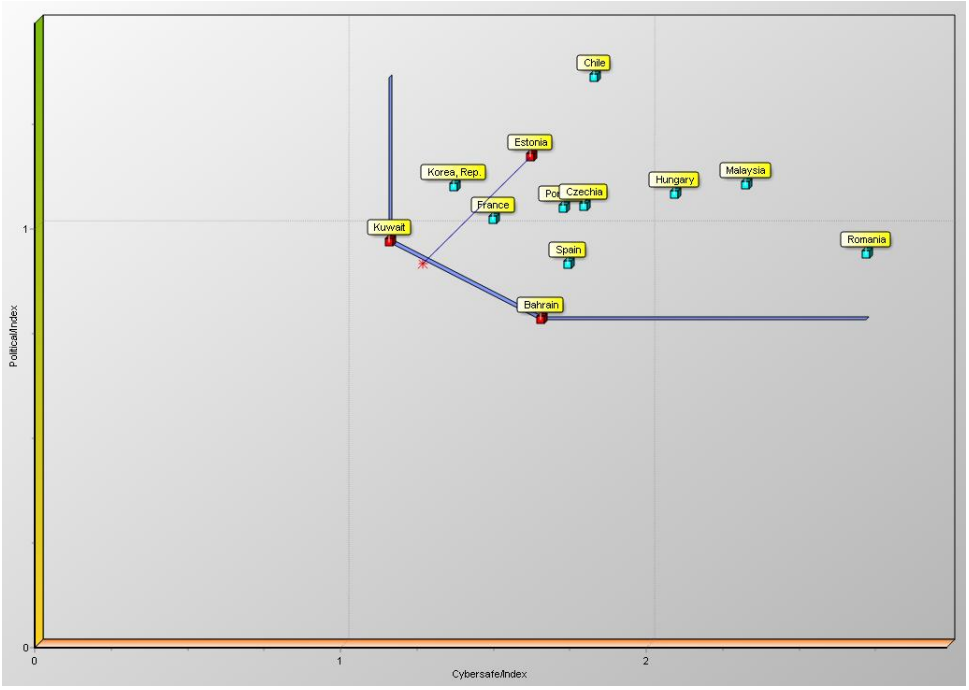


Рисунок 3.63 – Фронтірна діаграма ефективності збалансованої взаємодії політичних та кібербезпекових детермінант для країн 3-го кластеру

Аналіз оцінки ефективності для країн 2-го кластеру дозволив прийти до наступних висновків. Для мінімазації входів та виходу на тому самому рівні країни цієї групи мають запаси по всім чотирьом детермінантам. Найвищі значення відповідають соціальній сфері (40,19%) та економічній (32,02%) (Рисунок Н.17 Додатку Н). 100% ефективність демонструють тільки Бруней, Болгарія, Маурітус, Сербія та Україна (Рисунок Н.18 Додатку Н). За необхідності більш гнучкого розвитку країни даного кластеру мають можливості досягнення збалансованості всіх чотирьох сфер, якщо запас політичної детермінанти сягатиме 63,2% т соціальної 30,26% (Рисунок Н.19 Додаток Н). Всі країни, окрім Вірменії та Коста Рики, матимуть можливості потенційного розвитку за даних умов на рівні 100% (Рисунок Н.20 Додаток Н). Якщо планується максимізувати збалансованість взаємодії 4-х детермінант та підвищити її на 21,74% (Рисунок Н.21 Додатку Н), країни 2-го кластеру можуть це здійснити за рахунок соціальної сфери (43,78%) та економічної – 30,9%. Тільки Бруней, Болгарія, Маурітус, Сербія та Україну зможуть досягти 100% ефективності за цих умов (рисунок Н.22 Додатку Н). Максимальний вихід на рівні 8,12% може бути отриманий,

фкщо запас політичної сфери сягатиме 61,66% і соціальної 29,76% (Рисунок Н.23 Додатку Н). Але Вірменія та Коста Рика не зможуть досягти 100% ефективності (Рисунок Н.24 Додатку Н).

Аналіз взаємодії економічної та кібербезпекової детермінанти для країн 2-го кластеру показує наступні результати ефективності (рисунок 3.64). Сербія, Україна та Маурітус досягають більшої ефективності в кібербезпековій сфері, Бруней – в економічній. Всі інші країни показують низький рівень ефективності цих двох сфер. Порівняння соціальної та кібербезпекової сфери (рисунок 3.65) виявляє ефективну збалансованість тільки для Брунею. На рисунку 3.66 спостерігати 3 країни, для яких забезпечується ефективне співвідношення відповідних сфер до інтегрального показника. Для Брунею це відбувається у бік політичної детермінанти, для України та Болгарії – кібербезпекової. Але попарне порівняння для країн цього кластеру свідчить, що все ж таки вони розвиваються незбалансовано, що є результатом слабкої політики.

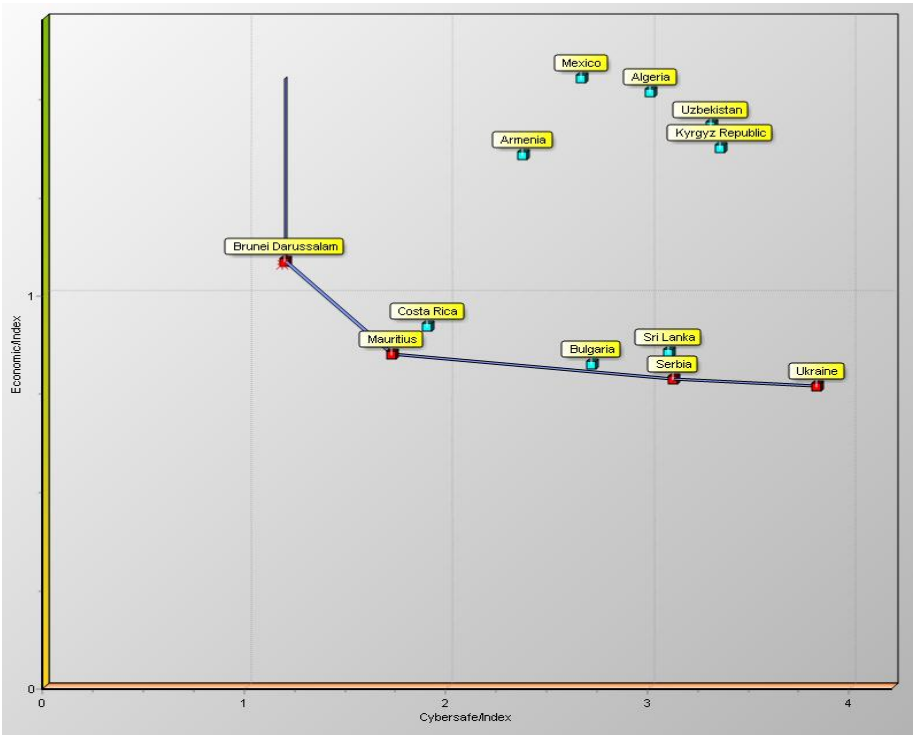


Рисунок 3.64 – Фронтірна діаграма ефективності збалансованої взаємодії економічних та кібербезпекових детермінант для країн 2-го кластеру

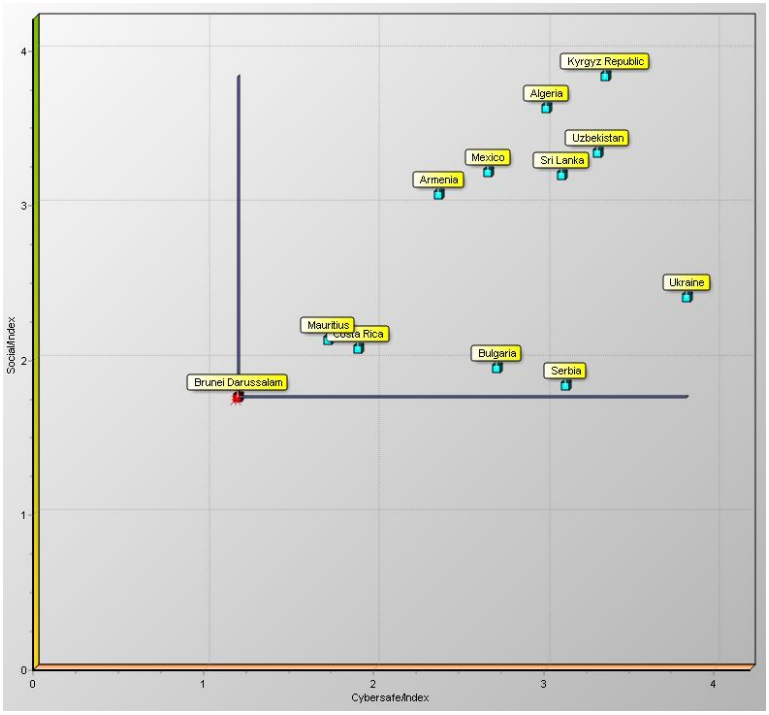


Рисунок 3.65 – Фронтірна діаграма ефективності збалансованої взаємодії соціальних та кібербезпекових детермінант для країн 2-го кластеру

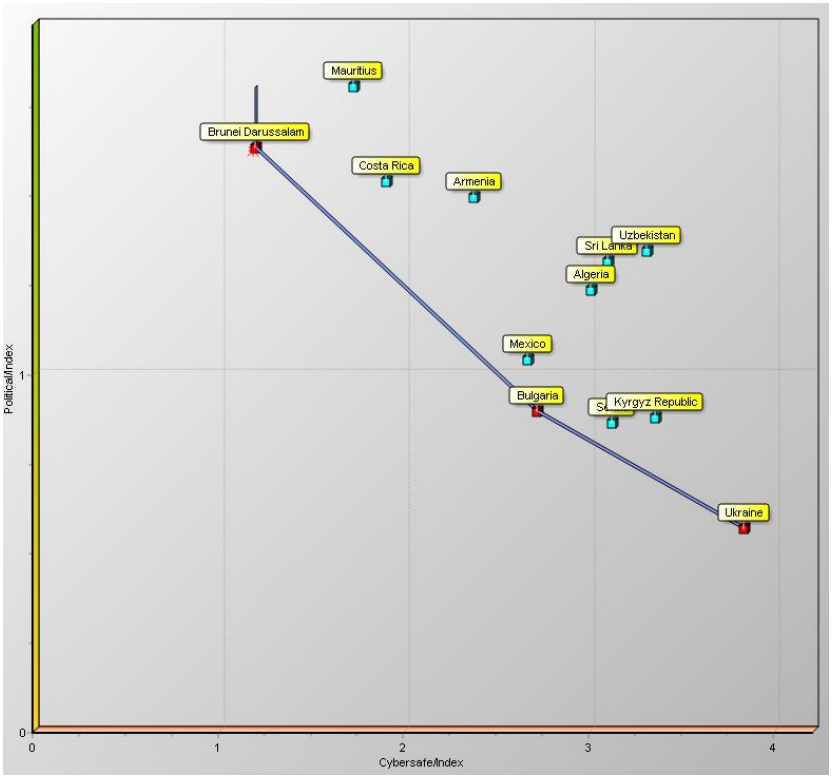


Рисунок 3.66 – Фронтірна діаграма ефективності збалансованої взаємодії політичних та кібербезпекових детермінант для країн 2-го кластеру

Проаналізуємо результати DEA-аналізу для країн 1-го кластеру. Мінімазація входів та забезпечення виходу на тому самому рівні можлива за рахунок забезпечення резервів в соціальній сфері (-26,15%), політичної (-22,34%), економічної (-28,78%), кібербезпекової (22,73%) (Рисунок Н.25 Додатку Н). Найгірша ситуація для країн даної групи характерна для Бурунді, Чаду, Конго, Гаїті та Вануату (Рисунок Н.26 Додатку Н). За умов кардинальних змін поточний рівень збалансованості можливо досягти в умовах формування ефективних політичних рішень (-69,04%) (Рисунок Н.27 Додатку Н). Але для Бурунді, Чаду та Вануату розподіл ефективності за даними сферами у такому співвідношенні також не дозволить досягти 100% ефективності (Рисунок Н.28 Додатку Н). Якщо максимізувати ефективність за рахунок досягнення максимального рівня збалансованості чотирьох детермінант, то це можна забезпечити на рівні 96,16% (Рисунок Н.29 Додатку Н). Але для деяких країн це важко досягти (Рисунок Н.30 Додатку Н). Максимальний вихід може бути отриманий на 46,19% рівні, але за умов забезпечення ефективності політики даних країн (-53,4%) (Рисунок Н.31 Додатку Н). Бурунді, Чад і Вануату не зможуть досягти 100% ефективності (Рисунок Н.32 Додатку Н).

Попарний аналіз взаємодії 4-х детермінант не є інформативним для країн даного кластеру за рахунок їх низької ефективності. Оскільки деякі країни мають великий рівень розбалансованості сфер.

Таким чином, було проведено оцінювання ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант для 147 країн світу. В результаті реалізації запропонованої методики було виявлено чотири кластери країн, які характеризуються високим, достатнім, середнім та низьким рівнями збалансованості. При цьому країни розподілені більш рівномірно за соціальною, економічною та політичною детермінантами, хоча є відповідний розкид у групах. Що стосується кібербезпекової, то спостерігається певний дисбаланс по всім групам, але це може пов’язано з тим, що дана сфера сьогодні є перспективною, тому деякі країни, особливо з

економікою, що розвивається, виводять її у пріоритет, що може слугувати відповідним драйвером для подальшого економічного та соціального розвитку.

В процесі проведення фронтірного аналізу було встановлено, що країни з високим рівнем збалансованості чотирьох детермінант мають найбільший потенціал соціального розвитку, а найменший – кібербезпекового. При попарному порівнянні детермінант найкращий результат показали Японія, Данія, Люксембург, Норвегія, Швейцарія та Катар. Країни з достатнім рівнем збалансованості продемонстрували наявність потенціалу соціальної та кібербезпекової детермінант, при цьому стрімкий розвиток останньої може забезпечити значну збалансованість. Естонія, Кувейт, Південна Корея, Франція та Бахрейн показали найкращий рівень збалансованості при здійсненні попарного порівняння. Країни із середнім ревнем збалансованості мають відповідний потенціал економічної та соціальної детермінанти в умовах постійного зростання та соціальної і політичної – в умовах гнучкого. Сербія, Україна, Болгарія, Бруней, Маурітус продемонстрували різний тип збалансованості. Наприклад, Україна тяжіє більше до кібербезпекової детермінанти, що свідчить про наявність значного потенціалу розвитку даної сфери. Країнам з низьким рівнем збалансованості потрібно орієнтуватися на політичну детермінанту, яка сприятиме прийняттю ефективних рішень й для розвитку інших сфер.

Даний пункт було виконано із використанням матеріалів публікацій виконавців [351].

ВИСНОВКИ

Серед основних результатів, зазначених у першому розділі, що мають наукову новизну і практичну значущість, слід зазначити наступні:

- проведений аналіз та характеристика поняття, цілей, задач, напрямів та моделей конвергенції систем фінансового моніторингу і кібербезпеки дозволив сформувати фундаментальне підґрунтя для досліджуваної проблеми. В результат встановлено, що поглиблені дослідження вектору фінансового моніторингу та вектору кібербезпеки дозволять зорієнтувати дослідження на створення комплексних заходів, пов’язаних із інтеграцією систем кібербезпеки та фінансового моніторингу на основі узагальнення, структурування теоретичних надбань світової та вітчизняної літератури;
- проведене оцінювання умов, сформованих в різних країнах світу, які характеризують поточний рівень їх кібербезпеки та фінансового моніторингу, дозволив провести попередній аналіз процесу конвергенції систем фінансового моніторингу і кібербезпеки. Результати статистичного аналізу дозволили виявити неоднорідність ряду показників, що обумовлено нерівномірністю розвитку країн в напрямку забезпечення ефективної системи кіберзахисту та фінансового моніторингу. Результати канонічного аналізу дозволили встановити, що між групами обраних показників існує тісний зв'язок, при цьому рівень кібербезпеки виступає наслідком, а рівень фінансового моніторингу – причиною. Результати кореляційного аналізу дозволили провести оптимізацію даних та виключити із дослідження такі показники, як індекс розвитку інформаційно-комунікаційних технологій та індекс сприйняття корупції;
- на основі біфуркаційного аналізу побудовані фазові портрети «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» діючої системи протидії фінансовим та кібершахрайствам. Це дозволило побудувати інтегральний індекс конвергенції систем на основі методу згортки Сундаровського; ідентифікувати релевантні предиктори впливу на інтегральний індекс кібербезпеки за допомогою методу сигма-обмеженої параметризації та

Парето-оптимізації; побудувати залежності інтегрального індексу кібербезпеки від релевантних предикторів на основі нелінійної регресії з покроковим виключенням; провести біфуркаційний аналіз зрілості діючої системи протидії фінансовим та кібершахрайствам та побудовані фазові портрети її «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості»; довести доцільність опису динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, за допомогою фазового портрету типу «нестійкий фокус» та «нестійкий вузол» в залежності від розглянутої проекції в розрізі «зрілості» та «релаксаційних коливань втрати стійкості»;

- розроблено ключові алгоритми систем фінансового моніторингу та кібербезпеки в розрізі ідентифікації та верифікації клієнта, моніторингу транзакцій, реакції на спробу-злочин, перевірки дій інсайдерів на ознаки кібершахрайств. Запропонований підхід дозволив провести моделювання існуючих процесів захисту інформації; здійснити симуляційні експерименти залежно від витрат часу та ресурсів при здійсненні окремої операції та виявлення на цій основі «вузьких» місць; провести моделювання процесів захисту інформації з урахуванням проведених оптимізаційних процедур та ліквідації виявлених недоліків; здійснити повторні симуляційні експерименти із метою підтвердження ефективності внесених змін до системи захисту інформації;
- розроблено математичне забезпечення алгоритмів виявлення кібершахрайських операцій з кредитними картками як найбільш поширених видів кіберзагроз. Це дозволило побудувати із застосуванням інтелектуального аналізу логістичну регресію, дерево рішень та нейронну мережу, які можна використовувати як універсальні інструменти для виявлення кібершахрайських операцій;
- із використанням методу визначення центра мас розроблено чотириполюсні барицентричні моделі збалансованого розвитку національної економіки, що інтегрують композитні індикатори економічного, соціального й політичного розвитку країни, а також рівня її протидії фінансовим шахрайствам

та кібербезпеки. Це дозволило провести розрахунки моделей з урахуванням трьох компонентів: значень композиційних цілей (як середнє геометричне), рівня парного балансу (як суми протилежних пар чотирикутних кутів) та всіх чотирьох цілей (як відстань між фактичним і нормативним значенням центру мас). За результатами аналізу було виявлено країни з найбільш ефективними таргетами, країни з дисбалансом цільових пар, а також розподіл країн за аналізом відстаней центрів мас;

- проведено оцінювання рівня потенційної конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів і фінансуванню тероризму на основі визначення їх інтегральних показників та застосування функції Харрінгтона – Менчера. Це дозволило визначити сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку в залежності від інтегрального рівня кібербезпеки, інтегрального рівня протидії легалізації кримінальних доходів, загального рівня конвергенції;
- розроблена методика оцінювання ефекту від конвергенції систем фінансового моніторингу та кібербезпеки з урахуванням потенційних зон вразливості та аберацій в інтеграційній моделі на основі методу лінійного непараметричного програмування DEA. Практичне запровадження такої моделі надасть можливість провести аналіз ефективності процесу конвергенції систем фінансового моніторингу і кібербезпеки для різних кластерів країн, побудувати візуалізацію результатів ефективності, визначити слабкі та сильні сторони системи за умови формування резервів наявних ресурсів, а також досягнення максимально можливого ефекту від здійснення інтеграційних процесів системи протидії фінансовим кібершахрайствам і кібербезпеки.

Серед основних результатів другого розділу, що мають наукову новизну і практичну значущість, слід зазначити наступні:

- запропоновано концептуальну модель розробки прогнозних моделей кібератак, яка ідентифікує всі етапи процесу прогнозування; проведено статистичний аналіз базових статистик, декомпозиційний аналіз трендів,

проведено перевірку на стаціонарність за допомогою розширеного тесту Дики-Фулера, на відповідність нормальному розподілу за допомогою тесту Харка-Бера. Це дозволило виявити: неоднорідність даних та встановити причини; відсутність трендової складової, наявність сезонності, вид зв'язків між компонентами часових рядів; доведення стаціонарності рядів; невідповідність нормальному розподілу. Отримані висновки дозволили здійснити процедури над даними та підготувати їх до наступних етапів багатошарового аналізу;

- проведено регресійний аналіз шляхом побудови об’єднаної регресії та регресій із випадковими та фіксованими ефектами для змінних “Mail Anti Virus”, “Kaspersky Anti-Spam” та “Intrusion Detection Spam”. Це дозволило визначити найбільш ефективну модель для прогнозування різних видів кібератак, якою виявилася модель об’єднаної регресі;
- проведено прогнозування на основі об’єднаної регресії та LSTM моделі на валідаційному наборі даних для різних країн світу. В результаті оцінок якості отриманих прогнозів було встановлено, що найбільш якісні прогнози генерує LSTM модель, не дивлячись на недостатній обсяг вхідних даних, але об’єднана регресія більш якісно описує початкові дані, тобто перший вид моделювання доцільно використати для створення прогнозів, а другий – в рамках здійснення багатошарового аналізу;
- у контексті діджиталізації сучасного суспільства досліджено теоретичні засади поняття "протидія легалізації доходів, отриманих незаконним шляхом". Аналіз показав, що зростання використання цифрових технологій робить цю проблему актуальнішою. Загальний висновок полягає в тому, що розвиток цифрових технологій вимагає відповідного адаптивного підходу до протидії легалізації доходів, а спеціалізовані стратегії повинні бути орієнтовані на нові виклики та можливості, що виникають в контексті цифрової трансформації суспільства;
- було запропоновано науково-методичний підхід до оцінювання ризиків конвергенції системи протидії фінансовим і кібершахрайствам на основі проведення сегментації країн із використанням кластерного аналізу за рівнем їх

кібербезпеки, ризику відмивання кримінальних доходів, інтегрального рівня конвергенції систем протидії фінансовим і кібершахрайствам, побудові класифікаційної моделі дерева рішень оцінки ризиків конвергенції. В результаті було встановлено кластери країн, для яких було означено 9 груп ризику, що дозволяє оцінити можливості країн щодо спроможності та готовності систем їх фінансового моніторингу та кібербезпеки інтегруватися в єдину та комплексну систему фінансового кіберзахисту;

- було побудовано нейромережеву модель потенційної конвергенції систем фінансової та кібербезпеки, для чого було проведено статистичний та канонічний аналізи, застосовано метод головних компонент, побудовано автоматичну нейронну мережу та мережу на сітці, а також регресію. В результаті було встановлено, що важливими показниками в сфері кібербезпеки та протидії фінансовим шахрайствам є фактори рівня цифрової трансформації і фактори, які характеризують легкості ведення бізнесу в країні, рівень споживчих цін та фінансової таємниці. Найбільш ефективною виявилася нейронна мережа, побудована на сітці, яка дозволяє прогнозувати рівень конвергенції систем фінансової та кібербезпеки в залежності від їх визначених ключових характеристик;
- було проведено профілювання жертв кіберзлочинів на основі гендерного аналізу щодо використання ними пристроїв для доступу до Інтернету, їх активності в Інтернеті, відношення до ситуацій кібершахрайства, впевненості в ситуаціях із кібершахрайствами та способів захисту від кібершахрайства. В результаті було визначено, що саме чоловіки мають більшу схильність до того, щоб стати жертвою кібершахрайства, ніж жінки, а також було окреслено фактори, які можуть цьому сприяти;
- було проведено профілювання кіберзлочинів для випадків кібершахрайств із кредитними операціями, для чого було визначено найбільш ефективні підходи до виявлення їх характеристик, а також застосовано метод кластеризації «Очікування-максимізація» до набору вхідних даних щодо клієнтів банку і побудовано кіберпрофілі на основі 10 кластерів потенційних

зловмисників. В результаті запропонованої методики профілювання встановлено п’ять найбільш значущих кластерів, які було сформовано під впливом таких характеристик, як сімейний стан, тип нерухомості, побутові умови, рівень освіти, тощо. Його використання не тільки дозволить виявити потенційних зловмисників, але й прийняти більш ефективне рішення щодо кредитування клієнтів, які мають статус потенційної загрози для банку;

- було розроблено алгоритми ідентифікації кіберзлочинців на основі методів інтелектуального аналізу даних, в результаті чого було побудовано об’єднану, LASSO, RIDGE, Elastic Net регресії, класифікаційне дерево рішення та нейронну мережу. Це дозволило визначити, що найбільш ефективними є алгоритми дерева рішення та нейронної мережі, які дозволятимуть з 90% рівнем упевненості ідентифікувати кіберзлочинця;
- було проведено дослідження інформаційних трендів трьох видів кібератак на комп’ютерні системи, мережеву та хмарну інфраструктуру фінансової установи, яке дозволило визначити інструмент моделювання та побудувати адитивні та мультиплікативні циклічні моделі експоненційного згладжування без тренду, з лінійним, експоненційним, затухаючим трендами та з урахуванням сезонної складової. Це дозволило виявити найкращі моделі для прогнозування конкретного виду кібератак та здійснити прогнози на короткострокову перспективу;
- було запропоновано ударно-хвильову модель впливу трьох видів кібератак на рівень фінансової безпеки, яка дозволила виявити моменти розриву інформаційної бульбашки, сформованої під найбільшим впливом кібершахрайських атак на рівень фінансової безпеки. Застосування даного підходу дозволяє прогнозувати пікові моменти кібератак, що сприяє формуванню комплексу превентивних дій в конкретних випадках та для конкретних видів кібератак.

Серед основних результатів третього розділу, що мають наукову новизну і практичну значущість, слід зазначити наступні:

- у даному дослідженні була проведена розробка імітаційної моделі діяльності інсайдера у банку з використанням програмного забезпечення AnyLogic. Отримані результати дозволяють здійснити глибокий аналіз потенційних загроз та ризиків, пов'язаних із внутрішнім фактором безпеки в банківській сфері. Модель враховує основні аспекти діяльності інсайдера, такі як доступ до конфіденційної інформації, можливість взаємодії з банківськими системами та ефективність заходів безпеки. Це дозволяє не лише ідентифікувати потенційні проблемні місця, але й розробляти та впроваджувати ефективні стратегії протидії інсайдерським загрозам. Імітаційна модель може бути використана для тренування персоналу, а також для тестування та удосконалення стратегій реагування на потенційні внутрішні загрози в банківському середовищі;
- запропоновано методологічний підхід моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках із трьох етапів. Перші два етапи включають в себе використання методів головних компонент та кластеризації k-середніх для формування найбільш релевантних змінних для подальшого аналізу, що в результаті дало дванадцять ключових змінних, розподілених у три списки. На третьому етапі застосовано асоціативний аналіз для створення трьох моделей асоціативних правил. За допомогою цих моделей зроблено висновок, що основним об'єктом інтересу потенційних інсайдерів-кібершахраїв у банках є персональна фінансова інформація клієнтів, доступ до їхніх особистих кабінетів і заволодіння їхніми телефонами. З цього випливає, що для мінімізації наслідків дій інсайдерів-кібершахраїв у банку необхідно вживати відповідні профілактичні заходи, а клієнтам рекомендується дбайливо ставитися до захисту своїх персональних даних;
- запропоновано методологію створення інформаційної бази для експертної системи виявлення кіберзагроз від інсайдерів у банках, яка є важливим кроком у контексті зростаючого обсягу кіберзагроз та їх потенційно серйозних наслідків для банківської сфери. Розроблені компоненти, структура та елементи інформаційної бази враховують різні аспекти, такі як дані про

користувачів, події та транзакції, експертні знання та правила, а також моделі аномалій для застосування машинного навчання. Зокрема, враховано детальний аналіз особистих та робочих аспектів працівників банку, історію доступу, фінансові операції та інші параметри для виявлення незвичайної активності. Використання моделей аномалій та машинного навчання дозволяє ефективно виявляти нові патерни та загрози. За рахунок структурованих таблиць для зберігання та аналізу даних, таких як "Моделі аномалій", "Виявлені аномалії", "Параметри моделі" та інші, створено основу для оптимальної функціональності експертної системи;

- усунення інсайдерських кіберзагроз у банках потребує впровадження онтологічної моделі, яка враховує складні взаємодії та специфіку банківського сектору. Запропонована модель відзначається узгодженістю з бізнес-процесами, інтеграцією з існуючими системами та врахуванням технічних, регуляторних та правових аспектів. Її успішна реалізація вимагає командної роботи експертів з кібербезпеки, фахівців з банківського бізнесу та інженерів знань. Не лише побудова моделі, але й її постійна оптимізація та підтримка є ключовими етапами для ефективного виявлення та протидії інсайдерським кіберзагрозам у банківському секторі;
- на основі асоціативного аналізу було створено соціально-економічні профілі кластерів країн, які були об'єднані за обсягами виявлених кібератак через поштові сервіси та мережу. Результати аналізу дозволили визначити спільні характеристики для більшості країн у кожному кластері, включаючи як їх комбінації, так і окремі особливості. Це може відігравати ключову роль у розумінні мотивів кіберзлочинів на глобальному рівні. Аналіз профілів груп країн, які менше піддаються кібератакам, підтверджує, що низький вплив цих країн на глобальний рівень тероризму є важливим аспектом відсутності мотивації для кіберзлочинців. Серед таких країн виявлено як ті, що мають високий рівень соціально-економічного розвитку, так і менш розвинені. Аналіз профілів кластерів країн, які є основними жертвами кібератак, показав, що вони, зазвичай, мають високий рівень соціально-економічного розвитку і виступають

як джерела масових кібератак. Додатковим аспектом у цьому контексті є вплив високого рівня корупції, який може слугувати індикатором таргетованих кібератак з метою отримання фінансової вигоди;

- реалізоване дослідження, яке спрямоване на створення композитного індикатора кібербезпеки для бізнесу, використовуючи модифікований матричний підхід Портера. Запропонований підхід та обчислення дозволяють оцінити необхідність розвитку системи кібербезпеки підприємств, враховуючи темпи зростання кіберзагроз у світі та рівень кіберризиків, які вони можуть призвести. Отримані результати призвели до наступних висновків. По-перше, в світі спостерігається стрімке впровадження та використання сучасних технологій, таких як штучний інтелект, блокчейн, промислові роботи, Інтернет речей та інші, що підтверджують фактичні та прогнозні дані про розвиток Індустрії 4.0. По-друге, застосування цих технологій вимагає посилення заходів кібербезпеки, обов'язкового створення надійної та ефективної системи захисту для підприємств. По-третє, розрахунок композитного індикатора кібербезпеки компаній вказує на значний ріст їхнього попиту на кіберзахист. Це в основному пов'язано з наслідками пандемії COVID-19, що спричинила зростання кіберзагроз та кіберризиків для підприємств. По-четверте, потреби в кіберзахисті перевершують сучасний рівень технологічного розвитку, хоча компанії виявляють повну готовність удосконалювати свої захисні механізми, особливо у сфері кібербезпеки. По-п'яте, витрати на IT та кіберзахист не відповідають зростаючим потребам у протидії кіберзагрозам, хоча за останній рік можна відзначити певний баланс між ними. Компанії продемонстрували своє розуміння наслідків кіберзагроз і збільшили витрати для ефективного протидії їм;
- у результаті оцінювання взаємодії соціальних, економічних, політичних та кібербезпекових детермінант для 147 країн світу визначено чотири рівні збалансованості. Країни розподілені за соціальним, економічним і політичним впливом. В галузі кібербезпеки спостерігається деякий дисбаланс, що може бути пов'язано з перспективністю даного напрямку. Фронтірний аналіз

показав, що країни з високим рівнем збалансованості чотирьох детермінант виявили найбільший потенціал для соціального розвитку, але менший у кібербезпеці. Країни з достатньою збалансованістю мають потенціал у соціальній та кібербезпековій сферах, при цьому розвиток останньої може забезпечити значну збалансованість. Країни із середньою збалансованістю мають потенціал у економічній та соціальній сферах, при постійному зростанні, тоді як соціальний та політичний вплив гнучше розвивається. Країни з низьким рівнем збалансованості повинні акцентувати увагу на політичних аспектах, які сприятимуть прийняттю ефективних рішень для розвитку інших сфер. Запропонована методика дозволяє виявляти основні детермінанти та сприяє більш ефективному розгляду країн з точки зору їхньої збалансованості та потенціалу розвитку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25. Karpunina E.K., Mikhailov A.M., Bondareva N.A., Lyubimenko O.A., Fedotova E.V. Blockchain Technologies as a Reflection of Modern Reality: Diversity of Opportunities Versus Security Risks. *Studies in Systems, Decision and Control*. 2021, № 314. P. 3–14. DOI: https://doi.org/10.1007/978-3-030-56433-9_1.

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

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

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

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

30. Gagliani G. Cybersecurity, Technological Neutrality, and International Trade Law. *Journal of International Economic Law*. 2020, № 23(3). P. 723–745. DOI: https://doi.org/10.1093/jiel/jgaa006.

31. Dawson M. Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*. 2018, № 35(2). P. 60–67. DOI: https://doi.org/10.1177/0266382118773624.

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

33. Кузьменко О.В., Яровенко Г.М., Радько В.В. Попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу країн. *Економіка та суспільство*. 2021, № 32. DOI: 10.32782/2524-0072/2021-32-3.

34. Глинников Н. Оптимизация нагрузки создаваемой сайтом на виртуальном хостинге. *ActiveCloud* : вебсайт. URL:

https://my.activecloud.com/ru/index.php?/Knowledgebase/Article/View/317/36/optimizcija-ngruzki-sozdvemojj-sjjtom-n-virtulnom-khostinge.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

50. Tackling Illicit Financial Flows and Cyberattacks for Enhancing National Security : monograph / O. Kuzmenko, H. Yarovenko, V. Bozhenko. Szczecin: Centre of Sociological Research. 2021.

51. Сучасні інформаційні технології в соціально-економічних системах [Текст] : звіт про НДР (остаточний) / кер. Г. М. Яровенко. — Суми : СумДУ. — 147 с.

52. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України [Текст]: звіт про НДР (проміжний) / кер. О.В. Кузьменко. - Суми: СумДУ, 2018. - 199 с.

53. Vasilyeva T., Yarovenko H., Bestuzheva S., Frolova N., Smirnova T., Shylovtseva N. Balanced of countries development determinants: barycentric model. *Heritage and Sustainable Development*, 2022, 4(2), pp. 145–164 10.37868/hsd.v4i2.148

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

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

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

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

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

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

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

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

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

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

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

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

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

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

68. Zou W., Straub D., Vance A., Yan J. The differential role of alternative data in SME-focused fintech lending. In *International Conference on Information Systems, ICIS 2020 - Making Digital Inclusive: Blending the Local and the Global*, *ICIS*. 2021. Code 167844.

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

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

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

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

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

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

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

76. Melnyk L., Sineviciene L., Lyulyov O., Pimonenko T., Dehtyarova I. Fiscal decentralization and macroeconomic stability: The experience of Ukraine's economy. *Problems and Perspectives in Management*. 2018, № 16(1). P. 105-114. DOI: https://doi.org/10.21511/ppm.16(1).2018.10.

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

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

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

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

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

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

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

84. Didenko I., Paucz-Olszewska J., Lyeonov S., Ostrowska-Dankiewicz A., Ciekanowski Z. Social safety and behavioral aspects of populations financial inclusion:

A multicountry analysis. *Journal of International Studies*. 2020, № 13(2). P. 347-359. DOI: https://doi.org/10.14254/2071-8330.2020/13-2/23.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

135. Ukraine cyber-attack: Russia to blame for hack, says Kyiv. *BBC* : website. URL: https://www.bbc.com/news/world-europe-59992531 (дата звернення 10.12.2022).

136. Ukraine's defence ministry and two banks targeted in cyberattack. *Euronews* : website. URL: https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack (дата звернення 10.12.2022).

137. Report: Recent 10x Increase in Cyberattacks on Ukraine. *Krebsonsecurity* : website. URL: https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/ (дата звернення 10.12.2022).

138. UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects. *CyberPeace Institute* : website. URL: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (дата звернення 10.12.2022).

139. Mortgage Loan Fraud Connections with Other Financial Crime: An Evaluation of Suspicious Activity Reports Filed By Money Services Businesses, Securities and Futures Firms, Insurance Companies and Casinos. Office of Law *Enforcement Support Financial Crimes Enforcement Network* : website. URL: https://www.fincen.gov/sites/default/files/shared/mortgage_fraud.pdf (дата звернення 10.12.2022).

140. The connected defense: Elevating the fight against financial crime. Using 4IR technologies to prevent and detect the growing ecosystem of financial crime. *Deloitte Development LLC* : website. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-elevating-the-fight-against-financial-crime.pdf (дата звернення 10.12.2022).

141. Building a united front on financial crimes. *PwC* : website. URL: https://www.pwc.com/gx/en/financial-services/pdf/united-front-financial-crimes-2018-pwc.pdf (дата звернення 10.12.2022).

142. The Global Risk Report. *World Economic Forum* : website. URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата звернення 10.12.2022).

143. Cost of a Data Breach Report 2022. *IBM Security* : website. URL: https://www.ibm.com/downloads/cas/3R8N1DZJ (дата звернення 10.12.2022).

144. Mclean M. Must-Know Cyber Attack Statistics and Trendshttps. *Embroker* : website. URL: www.embroker.com/blog/cyber-attack-statistics/ (дата звернення 10.12.2022).

145. Reports largest single day virus spike. *Abcnews* : website. URL: https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 (дата звернення 10.12.2022).

146. Stacey P., Taylor R., Spanaki K. Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management.* 2021, vol. 58, art. num. 102298. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102298.

147. Shandler R., Gomez M. A. The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology and Politics*. 2022. DOI: https://doi.org/10.1080/19331681.2022.2112796.

148. Lonsdale D. J. The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics*. 2020, vol. 19(1). P. 20–39. DOI: https://doi.org/10.1080/15027570.2020.1764694.

149. Bolpagni M. Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality and Quantity*. 2022, vol. 56(3). P. 1643–1659. DOI: https://doi.org/10.1007/s11135-021-01199-3.

150. Simons G., Danyk Y., Maliarchuk T. Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace and Security*. 2020, vol. 32(3). P. 337–342. DOI: https://doi.org/10.1080/14781158.2020.1732899.

151. Weaver G. A., Feddersen B., Marla L., Wei D., Rose A., Van Moer M. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies.* 2022, vol. 137, art. num. 103423. DOI: https://doi.org/10.1016/j.trc.2021.10342.

152. Leroy I. The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International Journal of Electronic Security and Digital Forensics*. 2022, vol. 14(4). P. 309–317. DOI: https://doi.org/10.1504/IJESDF.2022.123891.

153. Akoto W. International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*. 2021, vol. 58(5). P. 1083–1097. DOI: https://doi.org/10.1177/0022343320964549.

154. Lallie H. S., Shepherd L. A., Nurse J. R.C., Erola A., Epiphaniou G., Maple C., Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*. 2021, vol. 105, Art. Num. 102248. DOI: https://doi.org/10.1016/j.cose.2021.102248.

155. Definition and How to Run an F-Test. *Statistics How To* : website. URL: https://www.statisticshowto.com/probability-and-statistics/hypothesis-testing/f-test/ (дата звернення 10.12.2022).

156. Яровенко Г.М., Кобзенко В.В. Попередній аналіз і підготовка даних для прогнозування трендів кібератак. *Економіка та суспільство*. 2022, №45. DOI: https://doi.org/10.32782/2524-0072/2022-45-42

157. Statsmodels. *Statsmodels* : website. URL: https://www.statsmodels.org/stable/index.html (дата звернення 10.12.2022).

158. Akaike Information Criterion | When & How to Use It (Example). *Scribbr* : website. URL: https://www.scribbr.com/statistics/akaike-information-criterion/ (дата звернення 10.12.2022).

159. How to Interpret Log-Likelihood Values (With Examples). *Statology* : website. URL: https://www.statology.org/interpret-log-likelihood/ (дата звернення 10.12.2022).

160. Residual Standard Deviation/Error: Guide for Beginners. *Quantifyinghealth* : website. URL: https://quantifyinghealth.com/residual-standard-deviation-error/ (дата звернення 10.12.2022).

161. How to Calculate Standardized Residuals in Python. *Statology* : website. URL: https://www.statology.org/standardized-residuals-python/ (дата звернення 10.12.2022).

162. The Breusch-Pagan Test: Definition & Example. *Statology* : website. URL: https://www.statology.org/breusch-pagan-test/ (дата звернення 10.12.2022).

163. Train-Test Split for Evaluating Machine Learning Algorithms. *Machinelearningmaster* : website. URL: https://machinelearningmastery.com/train-test-split-for-evaluating-machine-learning-algorithms/ (дата звернення 10.12.2022).

164. LabelEncoder. *Scikit-learn.org* : website. URL: https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.LabelEncoder.html (дата звернення 10.12.2022).

165. RMSE: Root Mean Square Error. *Statisticshowto.com* : website. URL: https://www.statisticshowto.com/probability-and-statistics/regression-analysis/rmse-root-mean-square-error/ (дата звернення 10.12.2022).

166. Sequence Classification with LSTM Recurrent Neural Networks in Python with Keras. *Machinelearningmaster* : website. URL: https://machinelearningmastery.com/sequence-classification-lstm-recurrent-neural-networks-python-keras/ (дата звернення 10.12.2022).

167. Кобзенко В.В. Моделювання та прогнозування трендів кібератак : робота на здобуття кваліфікаційного рівня магістр : спец. 051 - економіка / наук. кер. Г. М. Яровенко. Суми : СумДУ, 2022. 73 с.

168. Загальні тенденції тіньової економіки у 2021 році. Міністерство економіки України. URL: https://www.me.gov.ua/Documents/Download?id=74e86de5-126a-4849-94d5-7d4ea048e4b8

169. Гордійчук М. Тіньова економіка: позитивні та негативні аспекти. *Траєкторія науки*. 2019. №5(3). С. 2001-2007. URL: https://pathofscience.org/index.php/ps/article/download/599/613.

170. Живко З. Б., Родченко С. С., Висоцька І. Б. Вплив легалізації доходів, отриманих незаконним шляхом, на економічну безпеку. *Соціально-гуманітарний вісник*. 2021. №37. С. 48-51. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/4195/1/вплив%20легалізації%20доходів.pdf

171. High-Risk Jurisdictions subject to a Call for Action – 21 October 2022. The Financial Action Task Force (FATF). URL: https://www.fatf-

gafi.org/publications/high-risk-and-other-monitoredjurisdictions/documents/call-for-action-october-2022.html

172. Типологічне дослідження «Ризики використання суб'єктів з непрозорою структурою власності у схемах відмивання кримінальних доходів». Державна служба фінансового моніторингу України. URL: https://fiu.gov.ua/ assets/userfiles/411/Типолог%20ДСФМУ/2018%2012%2028_Ty pology2018_UA.pdf

173. Типологічне дослідження «Актуальні методи і способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму». Державна служба фінансового моніторингу України. URL: https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/2012 %2027%2012_2012.pdf

174. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом,- «Використання готівки у схемах відмивання злочинних доходів». Державна служба фінансового моніторингу України. URL: https://fiu.gov.ua/assets/userfiles/411/Типолог%20 ДСФМУ/2011%2012%2029_gotivka.pdf

175. Lemire K.A. Cryptocurrency and anti-money laundering enforcement. Reuters. URL: https://www.reuters.com/legal/ transactional/cryptocurrency-anti-money-laundering-enforcement2022-09-26

176. Що таке NFT і як на ньому заробити. МінфінМедіа. URL: https://minfin.com.ua/ua/invest/articles/scho-take-nft-i-yakna-nomu-zarobyty/

177. PayPal в Україні під час війни спростив отримання міжнародних переказів на банківські картки. Як саме? Економічна правда. URL: https://www.epravda.com.ua/publications/2022/06/16/ 688135

178. В Україні з'явилися перші криптомати для біткойнів. Радіо Свобода. URL: https://www.radiosvoboda.org/a/ 28729154.html (дата звернення: 06.12.2022)

179. Dobrowolski Z., Sułkowski Ł. Implementing a Sustainable Model for Anti-Money Laundering in the United Nations Development Goals. *Sustainability*. 2020. 12(1):244. DOI: https://doi.org/10.3390/su12010244

180. Ferwerda J., Kleemans E.R. Estimating Money Laundering Risks: An Application to Business Sectors in the Netherlands. *Eur J Crim Policy Res*. 2019. №25, P. 45–62. URL: https://doi.org/10.1007/s10610-018-9391-4

181. Salehi A., Ghazanfari M., Fathian M. Data mining techniques for anti money laundering. *International Journal of Applied Engineering Research*. 2017. №12(20). P. 10084–10094. DOI: https://doi.org/10.5120/ijca2016910953

182. Canhoto A.I. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*. 2021. №131. P. 441-452. DOI: https://doi.org/10.1016/j.jbusres.2020.10.012

183. Vovk V, Zhezherun Y, Bilovodska O, Babenko V, Biriukova A. Financial Monitoring in the Bank as a Market Instrument in the Conditions of Innovative Development and Digitalization of Economy: Management and Legal Aspects of the Risk-Based Approach. *IJIEPR*, 2020. №31(4). P. 559-570 URL: http://ijiepr.iust.ac.ir/article-1-1141-en.html

184. Said Kh., Karimi D. Impact de la Digitalisation sur la Performance Bancaire dans la Prévention et la Lutte contre le Blanchiment de Capitaux. *African Scientific Journal*. 2022. №3(12). P. 461-476. DOI: https://doi.org/10.5281/zenodo.6874059

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

186. Boiko A., Zwolińska-Ligaj M., Bozhenko V., Florczak E., Ovcharenko V. Readiness for implementing innovations in banking in advanced and emerging economies. *Journal of International Studies*. 2021. №14(4). P. 236-250. doi:10.14254/2071-8330.2021/14-4/16

187. Djalilov K., Hölscher J. Comparative analyses of the banking environment in transition countries. *Economic Annals*. 2016. 61(208). P. 7-25. DOI: 10.2298/EKA1608007D

188. Djalilov K., Hartwell C. Do social and environmental capabilities improve bank stability? evidence from transition countries. *Post-Communist Economies*. 2021. №34(5). P.624-646. DOI: 10.1080/14631377.2021.1965359

189. Kuzior A., Kettler K., Rąb Ł. Digitalization of work and human resources processes as a way to create a sustainable and ethical organization. *Energies*. 2022. №15(1). 172. DOI: 10.3390/en15010172

190. Antonyuk N., Plikus I., Jammal M. Human Capital Quality Assurance under the Conditions of Digital Business Transformation and COVID-19 Impact. *Health Economics and Management Review*. 2021. 2(3). 39-47. DOI: https://doi.org/10.21272/hem.2021.3-04

191. Addo A., Senyo PK. Digitalization and government corruption in developing countries: towards a framework and research agenda. *Academy of Management Proceedings*. 2020. №1. DOI: 10.5465/AMBPP.2020.16765abstract

192. de Castro Halis D. Digitalization and Dissent in Legal Cultures. Chinese and Other Perspectives. *Naveiñ Reet: Nordic Journal of Law and Social Research (NNJLSR)*. 2019. №9. P. 127-152. URL: https://tidsskrift.dk/nnjlsr/issue/download/8857/1189#page=129

193. MulyanaY. Digitalization of the court in the settlement of cases. *International Journal of Latin Notary*. 2021. №1(2). P. 36-42. URL: https://i-latinnotary.notariat.unpas.ac.id/index.php/jurnal/article/view/6

194. Wronka C. Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*. 2022. №25(1), P.79-94. DOI: https://doi.org/10.1108/JMLC-02-2021-0017

195. Dupuis D., Gleason K. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*. 2020. №28(1). P. 60-74. DOI: https://doi.org/10.1108/JFC-06-2020-0113

196. Миненко С.В. Теоретичні засади до розуміння сутності поняття «протидія легалізації доходів отриманих незаконним шляхом» в умовах діджиталізації суспільства. Moderní aspekty vědy: XXVI. Díl mezinárodní

kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2022. S. 537-556.

197. Миненко С.В. Трансформація системи протидії легалізації кримінальних доходів в умовах діджиталізації національної економіки: дис. ... д-ра філософії : 051. Суми, 2023. 204 с.

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

199. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. Information Technology and Security. 2017, vol. 5(1). P. 82-95. URL: http://nbuv.gov.ua/UJRN/inftech_2017_5_1_11.

200. Institute of Risk Management. *Theirm* : website. URL : https://www.theirm.org/knowledge-and resources/thought-leadership/cyber-risk (дата звернення 10.12.2022).

201. National Cybersecurity Index. NCSI : website. URL: https://ncsi.ega.ee/ (дата звернення 10.12.2022).

202. Basel AML Index Assessing Money Laundering Risks Around The World. Basel ALM Index : website. URL: https://index.baselgovernance.org/ (дата звернення 10.12.2022).

203. Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Working Paper*. 2018. 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 10.12.2022).

204. Understanding Systemic Cyber Risk, Global Agenda Council on Risk & Resilience, White Paper, October 2022. *World Economic Forum* : website. URL: https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf (дата звернення 10.12.2022).

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

206. Яровенко Г.М., Рожкова М.С. Оцінка ризику конвергенції системи протидії відмивання грошей та кібербезпеки. *Економіка та суспільство*. 2022, № 45. DOI: https://doi.org/10.32782/2524-0072/2022-45-84

207. Кібербезпека у фінансовій сфері. *Risk-practice* : website. URL: https://risk-practice.ru/magazine/112/eau_112_659/ (дата звернення 10.12.2022).

208. Мельничук Я.О., Кравченко С.М. Аналіз даних та візуалізація за допомогою мови Python. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/11/54.pdf .

209. NumPy. *Wikipedia* : website. URL: https://ru.wikipedia.org/wiki/NumPy (дата звернення 10.12.2022).

210. Global Cybersecurity Index. *ITU* : website. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата звернення 10.12.2022).

211. Networked Readiness Index. *Wikipedia* : website. URL: https://en.wikipedia.org/wiki/Networked_Readiness_Index#:~:text=The%20Networked%20Readiness%20Index%20is,by%20information%20and%20communications%20technology (дата звернення 10.12.2022).

212. Візуалізація даних. *Oracle* : website. URL: https://www.oracle.com/ru/business-analytics/what-is-data-visualization/ (дата звернення 10.12.2022).

213. Гістограми. *Sixsigmaonline* : website. URL: http://sixsigmaonline.ru/baza-znanij/gistogrammy-chto-ehto-kak-postroit-kak-predstavit-dannye-kak-provesti-analiz (дата звернення 10.12.2022).

214. Matplotlib: Наукова графіка в Python. *Pythonworld* : website. URL: https://pythonworld.ru/novosti-mira-python/scientific-graphics-in-python.html (дата звернення 10.12.2022).

215. Яровенко Г. М. Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2020, № 31. С. 160–167.

216. Principal component analysis. *Royalsocietypublishing* : website. URL: https://royalsocietypublishing.org/doi/10.1098/rsta.2015.0202 (дата звернення 10.12.2022).

217. Svitlychna A. O. Modelling the potential convergence of the cybersecurity system and combating money laundering : bachelor's qualification work : specialty 051 – economics / head H. Yarovenko. Sumy : Sumy State University, 2022. 56 p.

218. Average cost of a data breach worldwide from 2014 to 2022 (in a million U.S. dollars). *Statista* : website. URL: https://www.statista.com/statistics/987474/global-average-cost-data-breach/ (дата звернення 10.12.2022).

219. Average cost of a data breach worldwide from May 2020 to March 2022, by industry (in a million U.S. dollars). *Statista* : website. URL: https://www.statista.com/statistics/387861/cost-data-breach-by-industry/ (дата звернення 10.12.2022).

220. UAE victims of cybercrime lose $746m a year. *The National* : website. URL: https://www.thenationalnews.com/business/technology/2021/08/13/uae-victims-of-cybercrime-lose-746m-a-year/ (дата звернення 10.12.2022).

221. Bhardwaj G., Bawa R. K. Machine learning techniques based exploration of various types of crimes in India. *Indian Journal of Computer Science and Engineering*. 2022, vol. 13(4). P. 1293–1307. DOI: https://doi.org/110.21817/indjcse/2022/v13i4/221304142.

222. Syeda R. Z., Chishti M. A., Baba A. I., Wu F. Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*. 2022, vol. 23(2). P. 197–214. DOI: https://doi.org/10.1016/j.eij.2021.12.003.

223. Monika, Bhat A. Automatic Twitter Crime Prediction Using Hybrid Wavelet Convolutional Neural Network with World Cup Optimization. *International Journal of Pattern Recognition and Artificial Intelligence.* 2022, vol. 36(5). DOI: https://doi.org/10.1142/S0218001422590054.

224. Gomathi C., Jayasri K. Rain Drop Service and Biometric Verification Based Blockchain Technology for Securing the Bank Transactions from Cyber Crimes Using Weighted Fair Blockchain (WFB) Algorith. *Cybernetics and Systems.* 2022. DOI: https://doi.org/10.1080/01969722.2022.2103229.

225. Dupont B., Holt T. The Human Factor of Cybercrime. *Social Science Computer Review.* 2022, vol. 40(4). P. 860–864. DOI: https://doi.org/10.1177/08944393211011584.

226. Lazarus S., Button M., Kapend R. Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *Howard Journal of Crime and Justice.* 2022, vol. 61(3). P. 381–398. DOI: https://doi.org/10.1111/hojo.12485.

227. Connolly A. Y., Borrion H. Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Computers and Security.* 2022, vol. 119. DOI: https://doi.org/10.1016/j.cose.2022.102760.

228. Witsenboer J. W. A., Sijtsma K., Scheele F. Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers and Education.* 2022, vol. 186. DOI: https://doi.org/10.1016/j.compedu.2022.104536.

229. Drury B., Drury S.M., Rahman Md A., Ihsan U. A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media.* 2022, vol. 30. DOI: https://doi.org/10.1016/j.osnem.2022.100211.

230. Lee Yi Y., Gan C. L., Liew T. W. Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. *Journal of Adult Protection.* 2022, vol. 24(3-4). P. 179–194. DOI: https://doi.org/10.1108/JAP-06-2022-0011.

231. Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime). *Data.europa.eu* : website. URL: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en (дата звернення 10.12.2022).

232. Glossary on gender-related terms. *OSCE.org* : website. URL: https://www.osce.org/files/f/documents/1/2/26397.pdf (дата звернення 10.12.2022)

233. Gender Impact Assessment: Gender Mainstreaming Toolkit. *EIGE.europa.eu* : website. URL: https://eige.europa.eu/sites/default/files/mh0416171enn.pdf (дата звернення 10.12.2022).

234. Cyber crime categories that were reported most often in 2021, by number of victims. *Statista* : website. URL: https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime/ (дата звернення 10.12.2022).

235. Yarovenko H. Victims of cyberfraud: gender analysis. Laperspectiva de género en los procesos de formación y evaluación del Sistema universitario. Ed. Sainz de Baranda Andújar, Clara. 2023. P. 105-118. ISBN: 978-84-16829-80-4

236. Яровенко Г.М., Римар В.О. Особливості формування профілів кіберзлочинців. *"MODERNÍ ASPEKTY VĚDY" Moderní aspekty vědy: XXVII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o.*, 2023.

237. Удосконалення системи запобігання та протидії фінансовим кібершахрайствам: теоретико-методологічні та практичні аспекти / за заг. ред. д-ра екон. наук, проф. А.О.Бойка та д-ра екон. наук, доц. Г.М.Яровенко. – Суми : Сумський державний університет, 2023. – 215 с.

238. Yarovenko H., Rymar V. Development of modern cyber fraud profiles. *Міжнародний науковий журнал «Грааль науки», 2022. : за матеріалами V Міжнародної науково-практичної конференції «An integrated approach to science modernization: methods, models and multidisciplinarity»*, що проводилася 23 грудня 2022 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ

«International Centre Corporative Management» (Відень, Австрія). P. 267-268. DOI: https://doi.org/10.36074/grail-of-science.23.12.2022.40.

239. Nuha M., Mahmud S., Sattar A. (2021). A case study and fraud rate prediction in e-banking systems using machine learning and data mining. Soft *Computing Techniques and Applications*. 2022. P. 71-83. DOI: https://doi.org/10.1007/978-981-15-7394-1_6.

240. Ланде Д. В., Субач І. Ю., Бояринова Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2018. 300 с.

241. Дюк В., Самойленко А. Data Mining: учебный курс (+CD). СПб: Изд. Питер, 2001. 368 с. URL: https://www.azstat.org/Kitweb/zipfiles/11337.pdf (дата звернення 10.12.2022).

242. Alshamasi S., Menai M. Ensemble-based clustering for writing style change detection in multi-authored textual documents. *Paper presented at the CEUR Workshop Proceedings*. 2022, art. no. 3180. P. 2357-2374.

243. Lekha K. C., Prakasam S. Data mining techniques in detecting and predicting cyber crimes in banking sector. Paper presented at *the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS*. 2017. P. 1639–1643. DOI: https://doi.org/10.1109/ICECDS.2017.8389725.

244. Vinayakumar R., Alazab M., Soman K. P., Poornachandran P., Al-Nemrat A., Venkatraman S. Deep learning approach for intelligent intrusion detection system. *IEEE Access*. 2019, vol. 7. P. 41525–41550. DOI: https://doi.org/10.1109/ACCESS.2019.2895334.

245. Kanimozhi V., Prem Jacob T. Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. Paper presented at the *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing*, *ICCSP*. 2019. P. 33-36. DOI: https://doi.org/10.1109/ICCSP.2019.8698029.

246. Syniavska O., Dekhtyar N., Deyneka O., Zhukova T., Syniavska O. Modeling the process of counteracting fraud in e-banking. Paper presented at *the CEUR Workshop Proceedings*. 2019, vol. 2422. P. 100–110.

247. Fedotova G. V., Gontar A. A., Titov V. A., Kurbanov A. K., Kuzmina E. V. Increasing the economic security of information banking systems. In book: *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*. 2019. P. 1153-1161. DOI: https://doi.org/10.1007/978-3-030-13397-9_118.

248. Akinbowale O. E., Klingelhöfer H. E., Zerihun M. F. Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*. 2020, vol. 27(3). P. 945-958. DOI: https://doi.org/10.1108/JFC-03-2020-0037.

249. Yarovenko H. Development of algorithms for recognizing the cyber fraudsters' behaviour. *Міжнародний науковий журнал «Грааль науки», 2022. : за матеріалами V Міжнародної науково-практичної конференції «An integrated approach to science modernization: methods, models and multidisciplinarity»*, що проводилася 23 грудня 2022 року ГО «Європейська наукова платформа» (Вінниця, Україна) та ТОВ «International Centre Corporative Management» (Відень, Австрія). P. 265-266. DOI: https://doi.org/10.36074/grail-of-science.23.12.2022.39.

250. Яровенко Г.М. Жертва кіберзлочинів: ознаки та методи виявлення. Здобутки та досягнення прикладних та фундаментальних наук XXI століття: матеріали IV Міжнародної наукової конференції, м. Вінниця, 16 грудня, 2022 р. / Міжнародний центр наукових досліджень. – Вінниця: Європейська наукова платформа, 2022. С. 204-205. https://doi.org/10.36074/mcnd-16.12.2022.

251. Vojinovic I. (2022). More Than 70 Cybercrime Statistics - A $6 Trillion Problem. *Dataprot* : website. URL: https://dataprot.net/statistics/cybercrime-statistics/ (дата звернення 10.12.2022).

252. Cybersecurity. *Statista* : website. URL: https://www.statista.com/outlook/tmo/cybersecurity/worldwide (дата звернення 10.12.2022).

253. Estimated value of cyber insurance premiums written worldwide in 2018, 2020 and 2025. *Statista* : website. URL: https://www.statista.com/statistics/976526/global-cyber-insurance-market-size/ (дата звернення 10.12.2022).

254. Cyber defence. *NATO* : website. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення 10.12.2022).

255. Cybersecurity. *United Nations* : website. URL: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity (дата звернення 10.12.2022).

256. FACT SHEET: Act Now to Protect Against Potential Cyberattacks. *The White House* : website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/ (дата звернення 10.12.2022).

257. Maintaining a sustainable strengthened cyber security posture. *National Cyber Security Centre* : website. URL: https://www.ncsc.gov.uk/guidance/maintaining-a-sustainable-strengthened-cyber-security-posture (дата звернення 10.12.2022).

258. Leonov S., Frolov S., Plastun V. Potential of institutional investors and stock market development as an alternative to households' savings allocation in banks. *Economic Annals-XXI*. 2014, vol. 11-12. P. 65-68. URL: http://soskin.info/en/material/1/about-journal.html.

259. Brychko M., Bilan Y., Lyeonov S., Mentel G. Trust crisis in the financial sector and macroeconomic stability: A structural equation modelling approach. *Economic Research-Ekonomska Istrazivanja*. 2021, vol. 34(1). P. 828-855. DOI: https://doi.org/10.1080/1331677X.2020.1804970.

260. Tiutiunyk I. V., Zolkover A. O., Lyeonov S. V., Ryabushka L. B. The impact of economic shadowing on social development: challenges for macroeconomic

stability. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2022, vol. 1. P. 183-191. DOI: https://doi.org/10.33271/nvngu/2022-1/183.

261. Sarwar M., Akram M., Shahzadi S. Bipolar fuzzy soft information applied to hypergraphs. *Soft Computing*. 2021, vol. 25(5). P. 3417-3439. DOI: https://doi.org/10.1007/s00500-021-05610-x.

262. Lyeonov S., Żurakowska-Sawa J., Kuzmenko O., Koibichuk V. Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies*. 2020, vol. 13(4). P. 259-272. DOI: https://doi.org/10.14254/2071-8330.2020/13-4/18.

263. Kuzmenko O., Šuleř P., Lyeonov S., Judrupa I., Boiko A. Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions. *Journal of International Studies*. 2020, vol. 13(3). P. 332-339. DOI: https://doi.org/10.14254/2071-8330.2020/13-3/22.

264. Sivakumar P., Jayabalaguru V., Ramsugumar R., Kalaisriram S. Real Time Crime Detection Using Deep Learning Algorithm. In *2021 International Conference on System, Computation, Automation and Networking, ICSCAN 2021*. 2021. DOI: https://doi.org/10.1109/ICSCAN53069.2021.9526393.

265. Obeid H., Hillani F, Fakih R., Mozannar K. Artificial Intelligence: Serving American Security and Chinese Ambitions. *Financial Markets, Institutions and Risks*. 2020, vol. 4(3). P. 42-52. DOI: https://doi.org/10.21272/fmir.4(3).42-52.2020.

266. Kuzmenko, O., Cyburt, A., Yarovenko, H., Yersh, V., Humenna, Y. Modeling Of "Information Bubbles" In The Global Information Space. *Journal Of International Studies*. 2021, № 14. № 4. pp. 270–285 10.14254/2071-8330.2021/14-4/18

267. Pakhnenko O., Rubanov P., Girzheva O., Ivashko L., Britchenko I., Bondarenko S. Cryptocurrency: Value Formation Factors and Investment Risks. *Journal of Information Technology Management*. 2022, № 14. P. 179-200 10.22059/JITM.2022.88896

268. Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: forecasting information trends. *Journal of Risk Financial Management*. 2022, vol. 15. Art. no. 613. DOI: https://doi.org/10.3390/jrfm15120613.

269. Kuzmenko O.V., Kubálek J., Bozhenko V.V., Kushneryov O.S., Vida I. An approach to managing innovation to protect financial sector against cybercrime | Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością. *Polish Journal of Management Studies*. 2021, 24(2). P. 276–291.

270. Boiko A., Zwolińska-Ligaj M., Bozhenko V., Florczak E., OvcharenkoV. Readiness for implementing innovations in banking in advanced and emerging economies. Journal of International Studies. 2021, 14(4). P. 236-250. doi: 10.14254/2071-8330.2021/14-4/16

271. Lieonov S., Hlawiczka R., Boiko A., Mynenko S., Garai-Fodor M. Structural modelling for assessing the effectiveness of system for countering legalization of illicit money. *Journal of International Studies*. 2022, 15(3). P. 215-233. DOI: https://doi.org/10.14254/2071-8330.2022/15-3/15.

272. Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brożek P. Global digital convergence: impact of cyber security, business transparency, economic transformation and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*. 2022, vol. 8. P. 195. DOI: https://doi.org/10.3390/joitmc8040195.

273. Vasilyeva T.A., Kuzmenko O.V., Stoyanets N.V., Artyukhov A.E., Bozhenko V.V. The depiction of cybercrime victims using data mining techniques. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2022, vol. 5. P. 174 – 178.

274. Kuzmenko O., Yarovenko H., Perkhun L. Assessing the maturity of the current global system for combating financial and cyber fraud. *Statistics in Transition New Series*. 2023. Vol. 24(1). P. 229–258. https://doi.org/10.59170/stattrans-2023-013

275. Kuzior A., Krawczyk D., Brożek P., Pakhnenko O., Vasylieva T., Lyeonov S. Resilience of smart cities to the consequences of the COVID-19 pandemic

in the context of sustainable development. *Sustainability (Switzerland)*. 2022, vol. 14(19). DOI: https://doi.org/10.3390/su141912645.

276. Яровенко Г.М., Кочережченко Р.Д. Аналіз та моделювання соціально-економічного розвитку країн з урахуванням рівня їх кібербезпеки. *Вісник СумДУ. Серія «Економіка»*. 2022, № 1. С. 53-62. DOI: https://doi.org/10.21272/ 1817-9215.2022.1-5.

277. Кузьменко О.В., Яровенко Г.М., Скринька Л.О. Аналіз математичних моделей протидії банківським кібершахрайствам. *Вісник СумДУ. Серія «Економіка»*. 2022, № 2. С. 111-120 DOI: https://doi.org/10.21272/1817-9215.2022.2-13.

278. Яровенко Г.М., Ліцман М.А. Аналіз і прогнозування впливу рівня цифровізації країни на її економічний розвиток. *Вісник СумДУ. Серія «Економіка»*. 2021, № 4. С. 203-214. DOI: https://doi.org/10.21272/1817-9215.2021.4-24.

279. Кузьменко О.В., Бойко А.О, Доценко Т.В. Ризик легалізації коштів клієнтом банку від азартних ігор, що проводяться в мережі інтернет: підходи до вимірювання. *Вісник СумДУ. Серія «Економіка»*. 2022, № 3. С. 31-41. DOI: https://doi.org/10.21272/1817-9215.2022.3-3.

280. Yarovenko H., Rogkova M. Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system. *Financial Markets, Institutions and Risks*. 2022, 6(3). P. 93-104. DOI: https://doi.org/10.21272/fmir.6(3).93-104.2022.

281. Яровенко Г.М., Колотіліна О.В. Оцінювання взаємозалежності між втратою довіри до публічної влади та макроекономічною стабільністю України. *Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки"*. 2022, №11. DOI: https://doi.org/10.25313/2520-2294-2022-11-8437.

282. Google Trends. URL: https://trends.google.com/trends/?hl=ru (дата звернення 05.11.2023).

283. Рапута А.О. Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках : робота на здобуття кваліфікаційного ступеня магістра :

спец. 051 - економіка / наук. кер. Г. М. Яровенко. Суми : Сумський державний університет, 2023. 83 с.

284. Коваленко, І. І., Давиденко, Є. О., Швед, А. В. Методика пошуку асоціативних правил. *Вісник Черкаського державного технологічного університету.* 2019. (3), 50–55. https://doi.org/10.24025/2306-4412.3.2019.176909.

285. Рапута А.О. Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках : робота на здобуття кваліфікаційного ступеня магістра : спец. 051 - економіка / наук. кер. Г. М. Яровенко. Суми : Сумський державний університет, 2023. 83 с.

286. Яровенко Г.М., Петренко К.Ю., Ульяновська. Ю. В., Небаба Н. О., Мормуль М. Ф. Розроблення структури інформаційної бази експертної системи виявлення інсайдерських кіберзагроз у банках. *Академічні візії.* 2023. № 26. https://academy-vision.org/index.php/av/article/view/777

287. Яровенко Г.М., Перхун Л.П., Небаба Н.О., Булгакова О.Ф., Костенко В.В. Розробка моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках: онтологічний підхід. *Актуальні проблеми економіки.* 2023. №10(268). С. 71-83. https://doi.org/10.32752/1993-6788-2023-1-268-71-83

288. Smith E.T. Cyber warfare: a misrepresentation of the true cyber threat. *American Intelligence Journal.* 2013. 31(1). P. 82-85. Retrieved from:: https://www.jstor.org/stable/26202046

289. Lucas G. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford University Press. – 2016.

290. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Retrieved from: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

291. U.S. Department of Homeland Security. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. Retrieved from: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

292. Perlroth N., Scott M., Frenkel S. Cyberattack Hits Ukraine Then Spreads Internationally. Retrieved from: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

293. Bing C., Schectman J. Inside the UAE's secret hacking team of American mercenaries. Retrieved from: https://www.reuters.com/investigates/special-report/usa-spying-raven/

294. Tribune. Major cyber attack by Indian intelligence identified: ISPR. Retrieved from: https://tribune.com.pk/story/2259193/major-cyber-attack-by-indian-intelligence-identified-ispr

295. Krebs B. At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software. Retrieved from: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

296. Deutsche Welle. Ukrainian websites hacked in 'global attack'. Retrieved from: https://www.dw.com/en/ukraine-government-websites-hacked-in-global-attack/a-60421475

297. Kaspersky. Cyberthreat real-time map. Retrieved from: https://cybermap.kaspersky.com/

298. E-Governance Academy. National Cyber Security Index. Retrieved from: https://ncsi.ega.ee/ncsi-index/

299. Institute for Economics and Peace. Global Terrorism Index 2022. Retrieved from: https://reliefweb.int/report/world/global-terrorism-index-2022

300. Numbeo. Crime Index by Country 2022. Retrieved from: https://www.numbeo.com/crime/rankings_by_country.jsp?title=2022

301. Transparency International. Corruption_Perceptions_Index. Retrieved from: https://www.transparency.org/en/cpi/2021?gclid=CjwKCAjw67ajBhAVEiwA2g_jEPyd355cvDdhD7SdWVteYeer5WvV3BZFHMo-Ox6p3vXSGk9wKi4p4BoCRJgQAvD_BwE

302. The Heritage Foundation. 2023 Index of Economic Freedom. Retrieved from: https://www.heritage.org/index/download

303. World Happiness Report. World Happiness Report 2022. Retrieved from: https://worldhappiness.report/ed/2022/

304. The World Bank. Life expectancy at birth, total (years). Retrieved from: https://data.worldbank.org/indicator/SP.DYN.LE00.IN

305. Economist Intelligence. Democracy Index. Retrieved from: https://www.eiu.com/n/campaigns/democracy-index-2022/?utm_source=google&utm_medium=paid-search&utm_campaign=democracy-index-2022&gclid=CjwKCAjwgqejBhBAEiwAuWHioAEruOQA25JyHg-61MBEiYNJp9hvu3Pf91E_tWO2W0nauZ6on003ORoC6UsQAvD_BwE

306. Rousseeuw P.J. Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis. *Computational and Applied Mathematics*. 1987. 20. P. 53–65. doi: 10.1016/0377-0427(87)90125-7.

307. Wisevoter. Most Powerful Countries in the World. Retrieved from: https://wisevoter.com/country-rankings/most-powerful-countries-in-the-world/

308. DavidPur N. Which Countries are Most Dangerous? Cyber Attack Origin – by Country. Retrieved from: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous

309. Yarovenko H., Lopatka A., Vasilyeva T., Vida I. Socio-economic profiles of countries - cybercrime victims. *Economics & Sociology*. 2023. Vol. 16(2). P. 167–194. https://doi.org/10.14254/2071-789x.2023/16-2/11

310. Schwab K. The Fourth Industrial Revolution. Retrieved from https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

311. Michael P. Technology statistics: How fast is Tech advancing? [growth charts] 2023. Retrieved from https://mediapeanut.com/how-fast-is-technology-growing-statistics-facts/

312. Rapp N., Hackett R. A Hacker's Tool Kit. Retrieved from https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

313. World Economic Forum. The Global Risks Report 2023 18th Edition. Retrieved from

https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*b8k930*_up*MQ..&gclid=Cj0KCQjw4s-kBhDqARIsAN-ipH0GJ_KEe3g7TllDlfjkfZYkSDl oZdCTiyNtIbwdFolQsKTBQL_ycFAaAlyCEALw_wcB

314. Fleck A. Cybercrime Expected to Skyrocket in Coming Years. Retrieved from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

315. Statista. Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022. Retrieved from https://www.statista.com/statistics/221293/cyber-crime-target-industries/#statisticContainer

316. Statista. Estimated worst potential loss in value due to a cyber incident according to senior executives worldwide as of February 2018, by company revenue size. Retrieved from https://www.statista.com/statistics/881519/estimated-worst-potential-loss-value-cyber-incident-company-revenue-size/

317. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

318. Lakshmanan R. Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack. Retrieved from Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack (thehackernews.com)

319. Maple Leaf Foods (2022). Maple Leaf Foods Confirms System Outage Linked to Cybersecurity Incident. Retrieved from Confirms System Outage Linked to Cybersecurity Incident (mapleleaffoods.com)

320. Hope A. Toyota’s Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output. Retrieved from https://www.cpomagazine.com/cyber-security/toyotas-supply-chain-cyber-attack-stopped-production-cutting-down-a-third-of-its-global-output/

321. Cyberthreat Defense Report. Retrieved from https://cyber-edge.com/cyberthreat-defense-report-2022/

322. IBM. Cost of a data breach 2022. Retrieved from https://www.ibm.com/reports/data-breach

323. Dluhopolskyi O., Pakhnenko O., Lyeonov S., Semenog A., Artyukhova N., Cholewa-Wiktor M., Jastrzębski W. Digital financial inclusion: COVID-19 impacts and opportunities. *Sustainability (Switzerland)*. 2023. 15(3). doi:10.3390/su15032383

324. Chen Y., Xu S., Lyulyov O., Pimonenko T. China's digital economy development: incentives and challenges. *Technological and Economic Development of Economy*. 2023. 29(2). 518-538. doi:10.3846/tede.2022.18018

325. Kuzior A., Yarovenko H., Brozek P., Sidelnyk N., Boyko A., Vasilyeva T. Company Cybersecurity System: Assessment, Risks and Expectations. *Production Engineering Archives.* 2023. Vol. 29(4). P. 379-392. https://doi.org/10.30657/pea.2023.29.43

326. Сідельник Н.Ю. Розвиток страхування в контексті інноваційних соціально-економічних трансформацій. дис. ... д-ра філософії : 072. Суми, 2023. 262 с.

327. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics. Retrieved from https://cybersecurityventures.com/cybersecurity-almanac-2023/

328. 50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted. Retrieved from https://www.techopedia.com/cybersecurity-statistics

329. 160 Cybersecurity Statistics 2023 [Updated]. Retrieved from https://www.getastra.com/blog/security-audit/cyber-security-statistics/

330. 239 Cybersecurity Statistics (2023). Retrieved from https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/.

331. Hogeveen, B. (2023). The UN norms of responsible state behaviour in cyberspace. Retrieved from https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

332. Tian S., Zhao B., Olivares R.O. Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Finance Research Letters*. 2023. Vol. 53. Art. num. 103609. DOI: 10.1016/j.frl.2022.103609.

333. Gafni R., Pavel T. Cyberattacks against the health-care sectors during the COVID-19 pandemic. *Information and Computer Security*. 2022. Vol. 30, № 1. P. 137-150. DOI: 10.1108/ICS-05-2021-0059.

334. Heymann F., Henry S., Galus M. Cybersecurity and resilience in the swiss electricity sector: Status and policy options. *Utilities Policy*. 2022. Vol. 79. Art. num. 101432. DOI: 10.1016/j.jup.2022.101432.

335. Paraskevas A. Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism*. Cham: Springer International Publishing, 2022. P. 1605-1628.

336. Punt E., Monstadt J., Frank S., Witte P. Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam. *Digital Policy, Regulation and Governance*. 2023. In press. DOI: 10.1108/DPRG-12-2022-0150.

337. Результат запиту "cybersecurity" & "economic development". Retrieved from https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=35534e48c35ca02001cc301b2462bdba&sot=a&sdt=a&sl=53&s=TITLE-ABS-KEY%28%22cybersecurity%22%26%22economic+development%22%29&origin=resultslist&count=10&analyzeResults=Analyze+results

338. National Cybersecurity Index. Retrieved from https://ncsi.ega.ee/ncsi-index/

339. GDP per capita (current US$). Retrieved from https://data.worldbank.org/indicator/NY.GDP.PCAP.CD

340. Inflation, GDP deflator (annual %). Retrieved from https://data.worldbank.org/indicator/NY.GDP.DEFL.KD.ZG

341. Net migration. Retrieved from https://data.worldbank.org/indicator/SM.POP.NETM

342. Political Stability and Absence of Violence/Terrorism: Estimate. Retrieved from https://databank.worldbank.org/source/worldwide-governance-indicators/Series/PV.EST

343. Government Effectiveness: Estimate. Retrieved from https://databank.worldbank.org/source/worldwide-governance-indicators/Series/GE.EST

344. Rule of Law: Estimate. Retrieved from https://databank.worldbank.org/source/worldwide-governance-indicators/Series/RL.EST

345. Control of Corruption: Estimate. Retrieved from https://databank.worldbank.org/source/worldwide-governance-indicators/Series/CC.EST

346. Voice and Accountability: Estimate. Retrieved from https://databank.worldbank.org/source/worldwide-governance-indicators/Series/VA.STD.ERR

347. Labor force, total. Retrieved from https://data.worldbank.org/indicator/SL.TLF.TOTL.IN

348. Unemployment, total (% of total labor force) (modeled ILO estimate). Retrieved from https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS

349. Life expectancy at birth, total (years). Retrieved from https://data.worldbank.org/indicator/SP.DYN.LE00.IN

350. Wage and salaried workers, total (% of total employment) (modeled ILO estimate). Retrieved from https://data.worldbank.org/indicator/SL.EMP.WORK.ZS

351. Колотіліна О.В. Економіко-математичне моделювання стійкого та збалансованого розвитку національної економіки: дис. ... д-ра філософії : 051. Суми, 2023. 295 с.

352. Kuzmenko O., Krukhmal O., Koibichuk V., Hrytsenko K., Kushneryov O., Hordiienko V. Survival Analysis Methods for Assessing the Anti-Money

Laundering System Effectiveness. *WSEAS Transactions on Business and Economics*. 2023, 20, pp. 1185–1206. 10.37394/23207.2023.20.106

353. Yarovenko H., Lyeonov S., Wojcieszek K. A., Szira Z. Do IT users behave responsibly in terms of cybercrime protection? *Human Technology*. 2023. Vol. 19(2). P. 178–206. https://doi.org/10.14254/1795-6889.2023.19-2.3

354. Kuzmenko O., Bilan Y., Bondarenko E., Gavurova B., Yarovenko H. Dynamic stability of the financial monitoring system: Intellectual analysis. *PLoS ONE*. 2023. Vol. 18. e0276533. https://doi.org/10.1371/journal.pone.0276533

355. Lyeonov, S.,Toušek, Z., Bozhenko, V., & Kérmárki-Gally, S. E. (2023). The impact of corruption in climate finance on achieving net zero emissions. *Journal of International Studies*, 16(1), 142-159. doi: 10.14254/2071-8330.2023/16-1/10 (*Scopus, Q2*)

356. Filatova, H., Tumpach, M., Reshetniak, Y., Lyeonov, S., & Vynnychenko, N. (2023). Public policy and financial regulation in preventing and combating financial fraud: a bibliometric analysis. *Public and Municipal Finance.* Volume 12, Issue 1, Pages 48 – 61 10.21511/pmf.12(1).2023.05

ДОДАТКИ

Додаток А

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

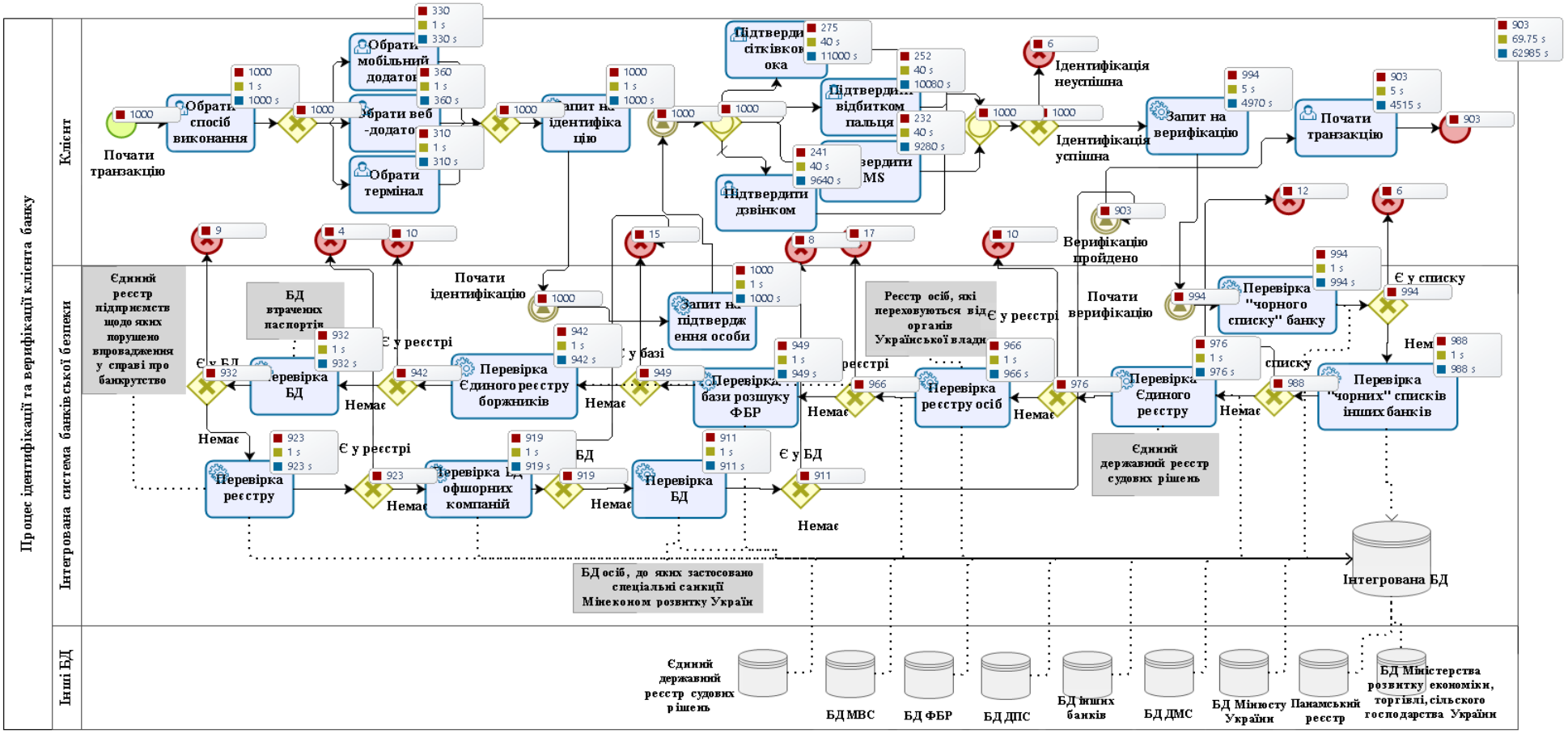


Рисунок А.1 – Результати симуляції за часом для бізнес-моделі процесу ідентифікації та верифікації клієнта

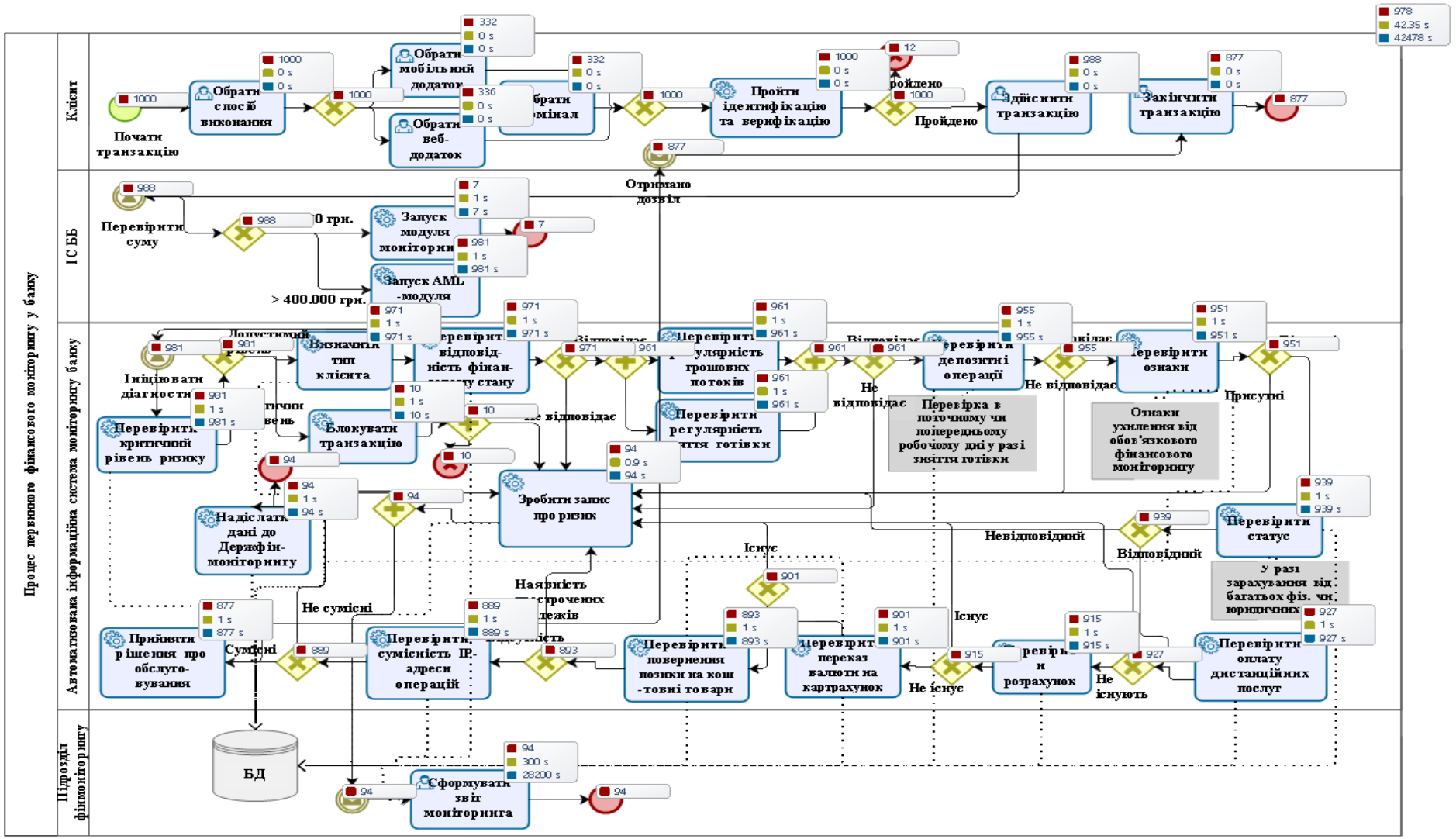


Рисунок А.2 – Результати симуляції за часом для бізнес-моделі процесу автоматизованого фінансового моніторингу

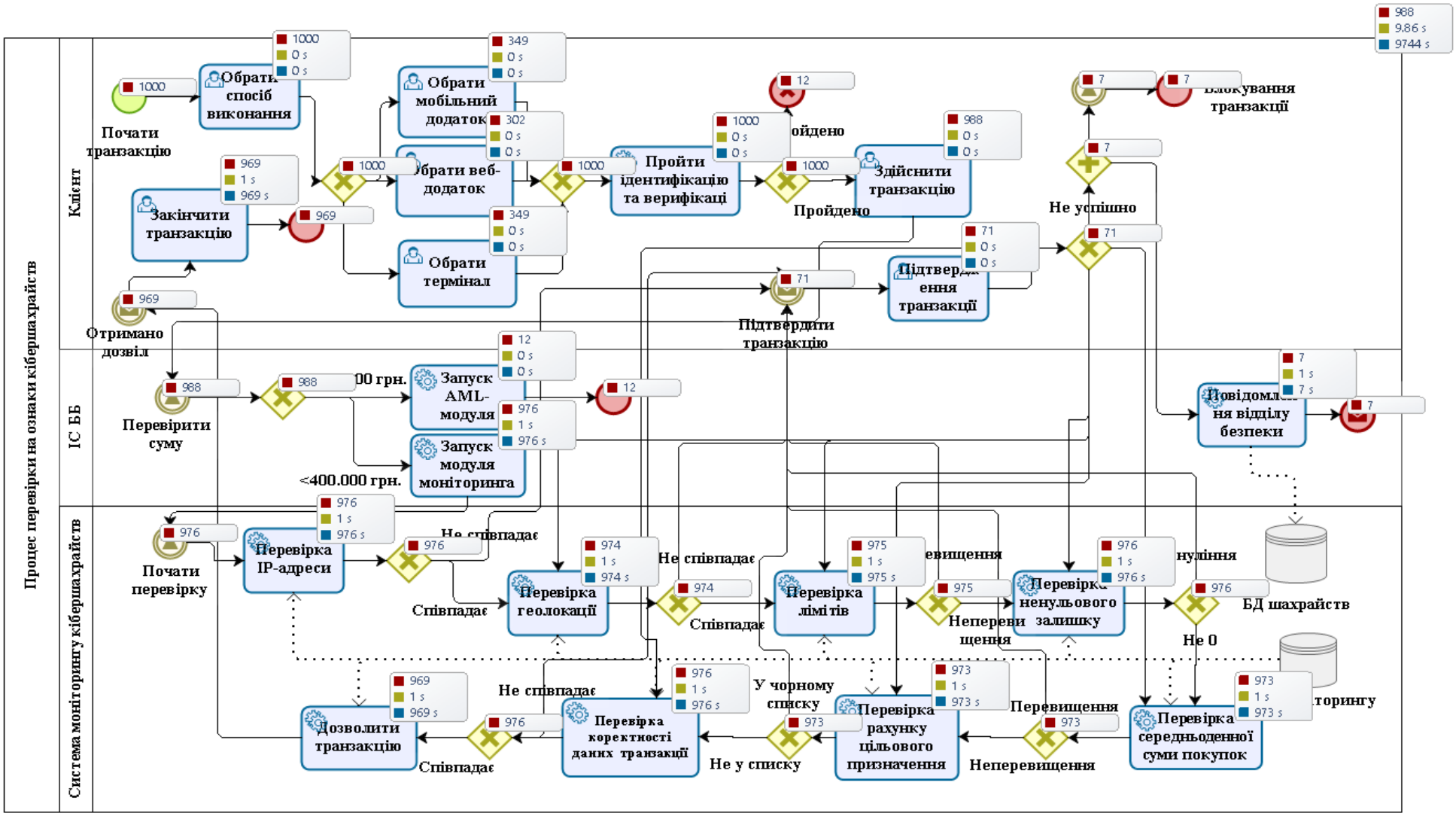


Рисунок А.3 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки зовнішніх кібершахрайств

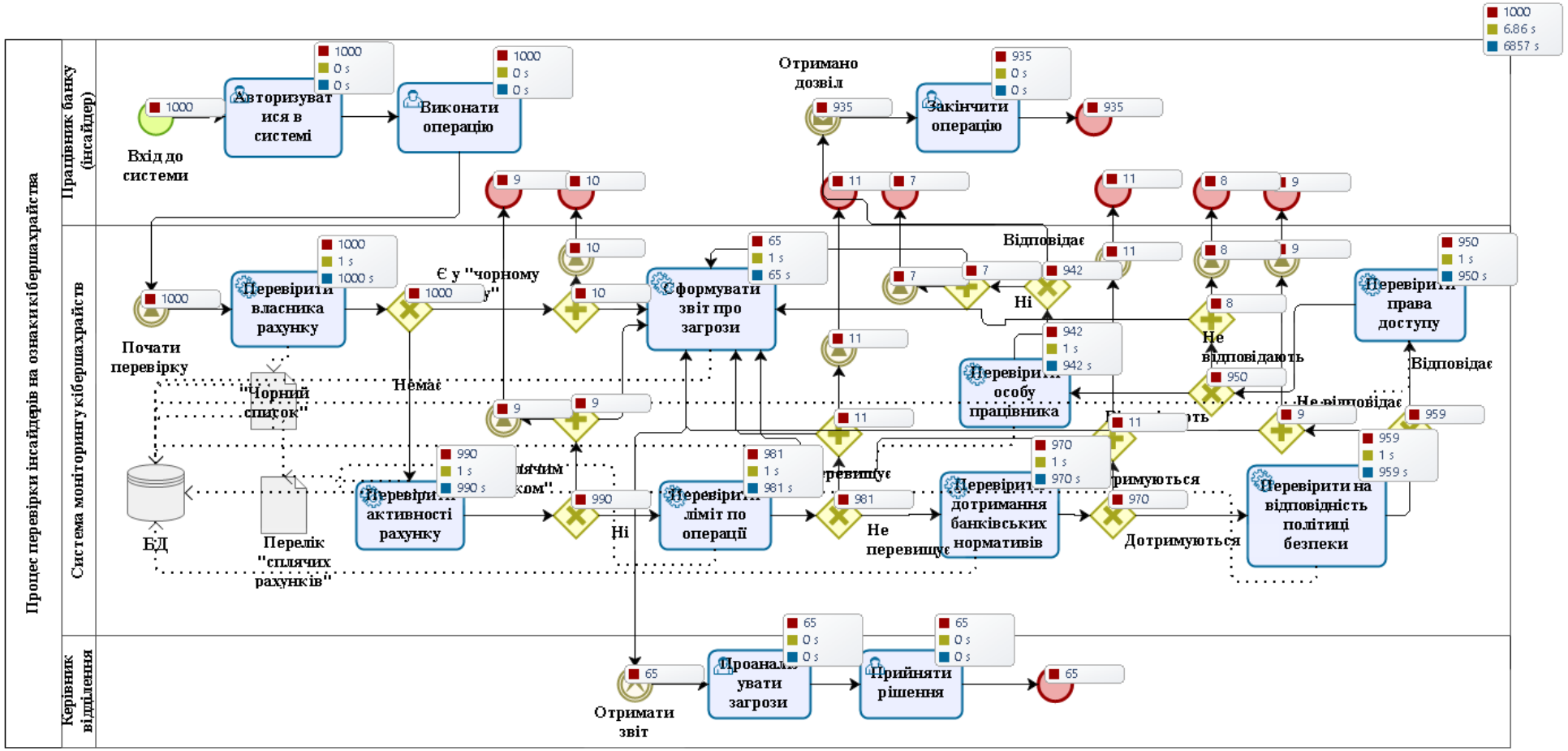


Рисунок А.4 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки кібершахрайств з боку інсайдерів

Додаток Б

Гістограми розподілу змінних

```
df.hist('PSI')
plt.ylabel("Frequency")
```

```
Text(0, 0.5, 'Frequency')
```

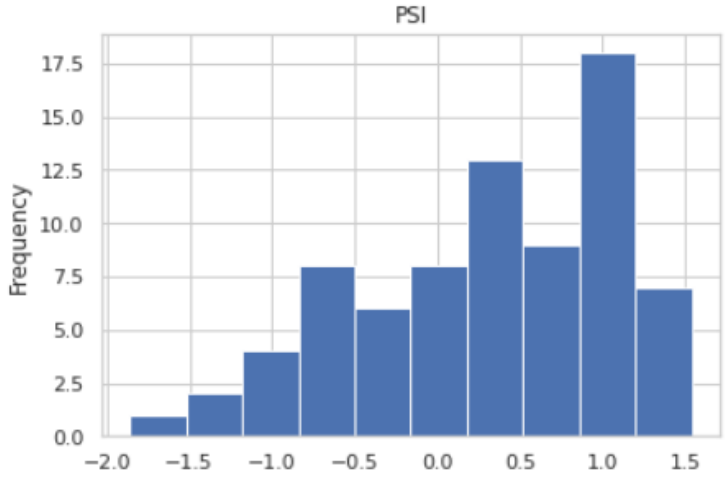


Рисунок Б.1 – Гістограма розподілу показника «PSI»

```
df.hist('EDB')
plt.ylabel("Frequency")
```

```
Text(0, 0.5, 'Frequency')
```

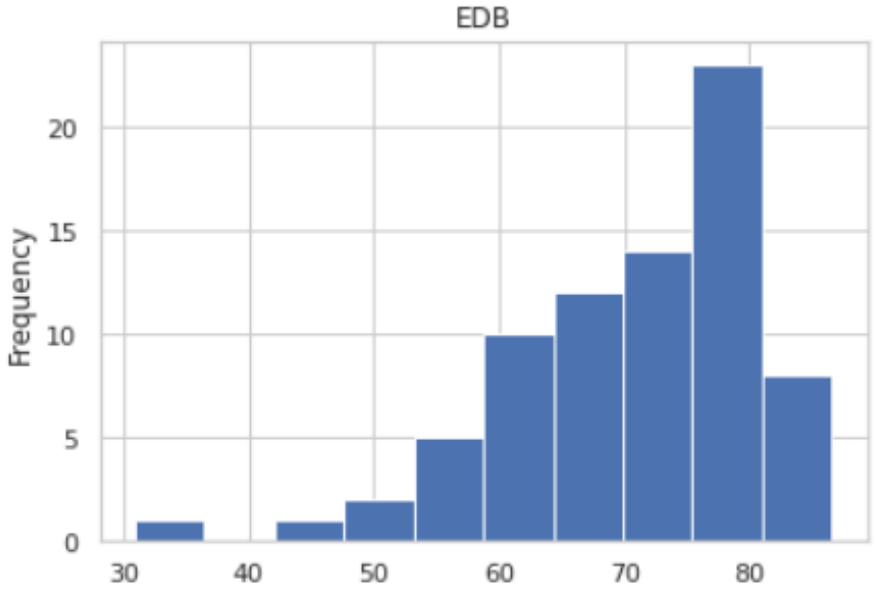


Рисунок Б.2 – Гістограма розподілу показника «EDB»

```
df.hist('CI')
plt.ylabel("Frequency")
```

```
Text(0, 0.5, 'Frequency')
```

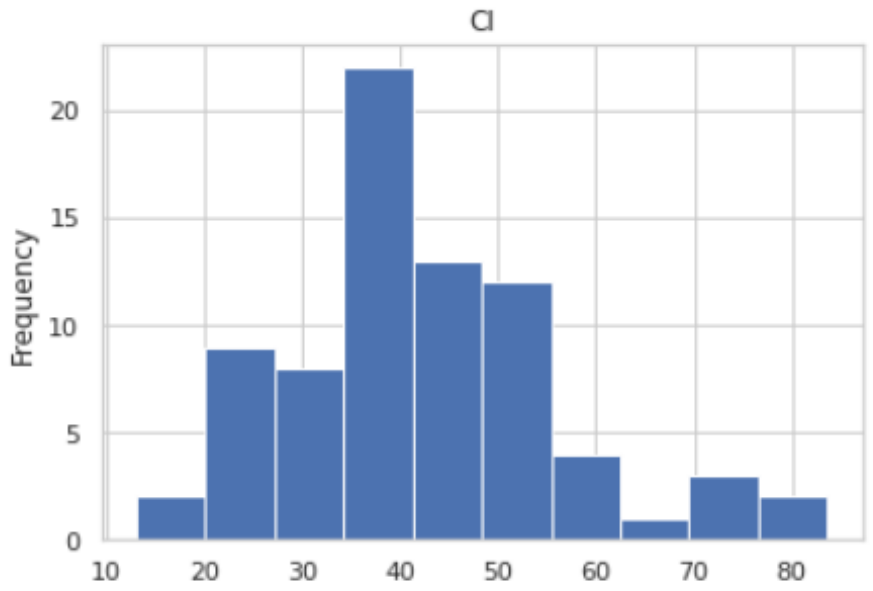


Рисунок Б.3 – Гістограма розподілу показника «CI»

```
df.hist('CPI')
plt.ylabel("Frequency")
```

```
Text(0, 0.5, 'Frequency')
```

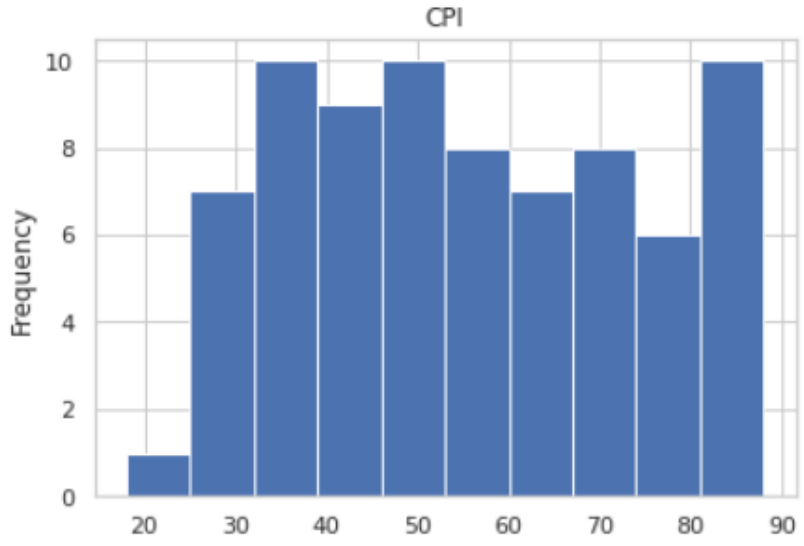


Рисунок Б.4 – Гістограма розподілу показника «CPI»

```
df.hist('GTI')
plt.ylabel("Frequency")
```

```
Text(0, 0.5, 'Frequency')
```

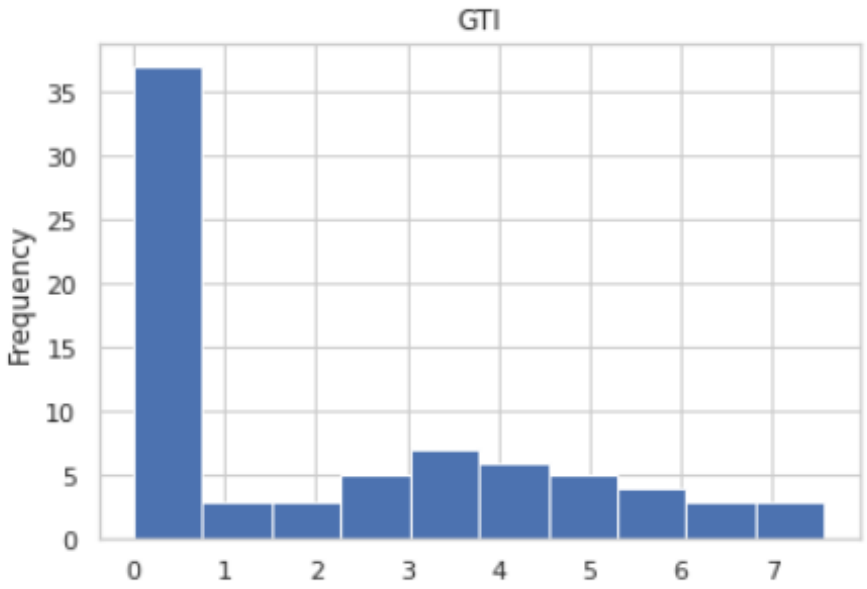


Рисунок Б.5 – Гістограма розподілу показника «GTI»

Додаток В
Результати канонічного аналізу

N=76	Canonical Analysis Summary (Convergensy.sta) Canonical R: .75906 Chi²(7)=60.519 p=0.0000	
	Left Set	Right Set
No. of variables	1	7
Variance extracted	100.000%	21.8918%
Total redundancy	57.6170%	12.6134%
Variables: 1	ICTDI	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок В.1 - Результати канонічного аналізу.

N=76	Canonical Analysis Summary (Convergensy.sta) Canonical R: .71093 Chi²(7)=49.636 p=0.0000	
	Left Set	Right Set
No. of variables	1	7
Variance extracted	100.000%	15.8106%
Total redundancy	50.5428%	7.99112%
Variables: 1	NRI	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок В.2 - Результати канонічного аналізу.

N=76	Canonical Analysis Summary (Convergensy.sta) Canonical R: .74559 Chi²(7)=57.225 p=0.0000 **Left Set**	Right Set
No. of variables	1	7
Variance extracted	100.000%	42.1733%
Total redundancy	55.5897%	23.4440%
Variables: 1	NCSI	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок В.3 - Результати канонічного аналізу.

N=76	Canonical Analysis Summary (Convergensy.sta) Canonical R: .95472 Chi²(7)=170.94 p=0.0000 **Left Set**	Right Set
No. of variables	1	7
Variance extracted	100.000%	43.6225%
Total redundancy	91.1491%	39.7615%
Variables: 1	DDL	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок В.4 - Результати канонічного аналізу.

Додаток Г
Нейромережева сітка

```
{'cv': 5,
 'error_score': nan,
 'estimator__activation': 'relu',
 'estimator__alpha': 0.0001,
 'estimator__batch_size': 'auto',
 'estimator__beta_1': 0.9,
 'estimator__beta_2': 0.999,
 'estimator__early_stopping': False,
 'estimator__epsilon': 1e-08,
 'estimator__hidden_layer_sizes': (45, 45, 45),
 'estimator__learning_rate': 'constant',
 'estimator__learning_rate_init': 0.001,
 'estimator__max_fun': 15000,
 'estimator__max_iter': 500,
 'estimator__momentum': 0.9,
 'estimator__n_iter_no_change': 10,
 'estimator__nesterovs_momentum': True,
 'estimator__power_t': 0.5,
 'estimator__random_state': None,
 'estimator__shuffle': True,
 'estimator__solver': 'adam',
 'estimator__tol': 0.0001,
 'estimator__validation_fraction': 0.1,
 'estimator__verbose': False,
 'estimator__warm_start': False,
 'estimator': MLPRegressor(activation='relu', alpha=0.0001, batch_size='auto', beta_1=0.9,
              beta_2=0.999, early_stopping=False, epsilon=1e-08,
              hidden_layer_sizes=(45, 45, 45), learning_rate='constant',
              learning_rate_init=0.001, max_fun=15000, max_iter=500,
              momentum=0.9, n_iter_no_change=10, nesterovs_momentum=True,
              power_t=0.5, random_state=None, shuffle=True, solver='adam',
              tol=0.0001, validation_fraction=0.1, verbose=False,
              warm_start=False),
 'iid': 'deprecated',
 'n_jobs': -1,
 'param_grid': {'hidden_layer_sizes': [(40, 40, 40),
   (35, 35, 35),
   (30, 30, 30)],
  'max_iter': [100, 500],
  'activation': ['tanh', 'relu'],
  'solver': ['sgd', 'adam'],
  'alpha': [0.0001, 0.05],
  'learning_rate': ['constant', 'adaptive']},
 'pre_dispatch': '2*n_jobs',
 'refit': True,
 'return_train_score': False,
 'scoring': None,
 'verbose': 0}
```

Рисунок Г.1 – Характеристика параметрів нейромережевої сітки

Додаток Д

Результати кластерного аналізу і формування кіберпрофілів

Рисунок Д.1 – Формування кіберпрофілів (продовження)

Кластеры	4	3	1	7	9	5	6	0	8	2	Итого
	9311 (37,5%)	4593 (18,5%)	2990 (12,0%)	2930 (11,8%)	2544 (10,2%)	964 (3,9%)	567 (2,3%)	477 (1,9%)	417 (1,7%)	32 (0,1%)	
Поля / Показатели											
REG_REGION_NOT_WORK_REGION											
Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	98,7%	100,0%
Распределение											
False	9311 (100,0%)	4593 (100,0%)	2990 (100,0%)	2930 (100,0%)	2494 (98,0%)	81 (8,4%)	501 (88,4%)	477 (100,0%)	33 (7,9%)	27 (84,4%)	23437 (94,4%)
True	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	50 (2,0%)	883 (91,6%)	66 (11,6%)	0 (0,0%)	384 (92,1%)	5 (15,6%)	1388 (5,6%)
REG_REGION_NOT_LIVE_REGION											
Значимость	100,0%	100,0%	100,0%	100,0%	60,6%	100,0%	99,8%	99,6%	100,0%	100,0%	100,0%
Распределение											
False	9311 (100,0%)	4593 (100,0%)	2974 (99,5%)	2930 (100,0%)	2494 (98,0%)	671 (69,6%)	567 (100,0%)	477 (100,0%)	348 (83,5%)	27 (84,4%)	24392 (98,3%)
True	0 (0,0%)	0 (0,0%)	16 (0,5%)	0 (0,0%)	50 (2,0%)	293 (30,4%)	0 (0,0%)	0 (0,0%)	69 (16,5%)	5 (15,6%)	433 (1,7%)
9.0 HOUR_APPR_PROCESS_START											
Значимость	100,0%	100,0%	100,0%	99,5%	98,0%	100,0%	99,9%	99,0%	100,0%	5,9%	100,0%
Доверительный интервал											
Среднее	11,63590756	12,16011878	11,26407873	11,98231769	11,63663342	12,6421292	11,34744268	12,1815286	13,13329225	11,75	11,79733845
Стандартн. откл.	3,241909449	3,354384019	3,087345393	3,372272868	3,319035696	3,212653968	3,048070058	3,212693949	3,006106313	3,610021893	3,280111194
Стандартн. ошиб.	0,03359717155	0,04949536801	0,05646113759	0,06230012215	0,06580416305	0,1034726171	0,1280069104	0,1470991509	0,1472096595	0,6381677401	0,02081823649
9.0 REGION_RATING_CLIENT_W_CITY											
Значимость	100,0%	100,0%	32,4%	100,0%	100,0%	100,0%	100,0%	99,0%	100,0%	80,0%	100,0%
Доверительный интервал											
Среднее	2,214799699	2,040278685	2,138795987	2,068600683	2,201650943	1,995850622	2,220458554	2,075471698	1,683453237	2,25	2,134823766
Стандартн. откл.	0,4747547958	0,4994658391	0,4892281169	0,4996452353	0,4967662103	0,5094979535	0,4516218922	0,4963797909	0,6205918146	0,508000508	0,4999091464
Стандартн. ошиб.	0,004920069043	0,00736983165	0,008946966572	0,009230557672	0,009849030771	0,0164082414	0,01896633672	0,02272766934	0,03039051191	0,08980265101	0,003172827449
9.0 REGION_RATING_CLIENT											
Значимость	100,0%	100,0%	38,9%	100,0%	100,0%	100,0%	100,0%	98,9%	100,0%	83,3%	100,0%
Доверительный интервал											
Среднее	2,224250886	2,075332027	2,158528428	2,108191126	2,211477987	1,997925311	2,222222222	2,094339623	1,695443645	2,28125	2,153635448
Стандартн. откл.	0,4755870531	0,5154273114	0,4958366394	0,5175985904	0,4954471611	0,5095106387	0,4527107205	0,5036728901	0,6246563342	0,5226714875	0,5050516003
Стандартн. ошиб.	0,00492869405	0,007605349987	0,009067822727	0,009562231964	0,009822878918	0,01641023271	0,01901206321	0,02306159741	0,03058955229	0,09239613829	0,003205465618
CNT_FAM_MEMBERS											
Значимость	100,0%	99,9%	100,0%	99,9%	100,0%	98,9%	99,8%	40,6%	100,0%	29,8%	100,0%
Доверительный интервал											
Среднее	09.02.2000 23:29:32	04.02.2000 9:14:27	02.01.2000 15:31:04	07.02.2000 15:30:21	08.02.2000 20:03:24	03.02.2000 13:39:51	09.02.2000 14:53:18	06.02.2000 13:21:16	01.01.2000 18:18:29	08.02.2000 4:30:00	05.02.2000 20:43:24
Стандартн. откл.	29дн. 16:33:21	26дн. 19:15:16	18дн. 01:30:20	28дн. 02:37:39	28дн. 08:48:27	27дн. 09:47:25	27дн. 22:45:33	28дн. 03:33:51	24дн. 15:54:03	34дн. 09:04:03	28дн. 00:41:05
Стандартн. ошиб.	07:23:04	09:29:29	07:55:40	12:27:47	13:29:52	21:11:09	1дн. 04:10:09	1дн. 06:55:55	1дн. 04:59:07	6дн. 01:51:09	04:16:09

Рисунок Д.2 – Формування кіберпрофілів (продовження)

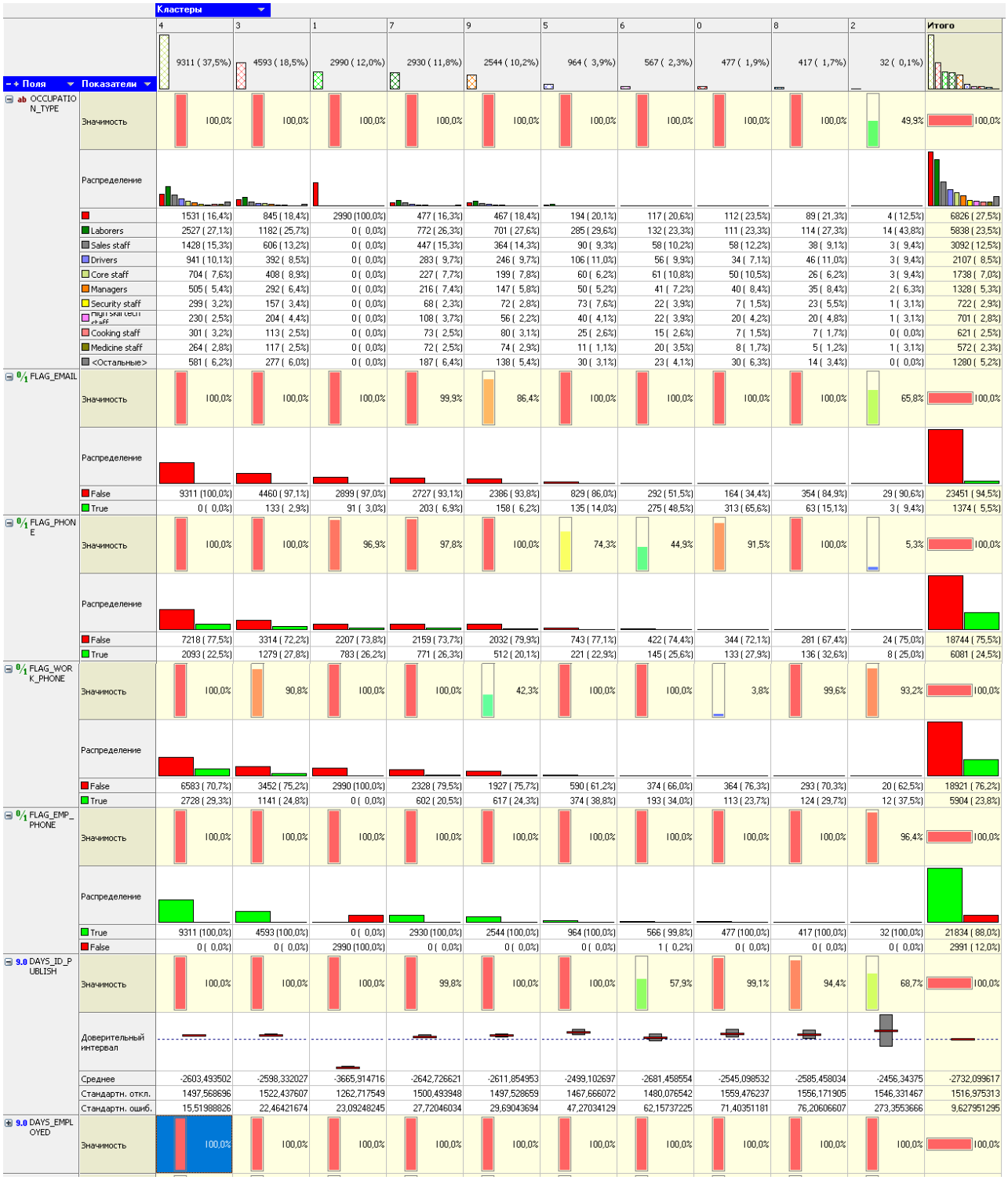


Рисунок Д.3 – Формування кіберпрофілів (продовження)

Поля	Показатели	4	3	1	7	9	5	6	0	8	2	Итого
		9311 (37,5%)	4593 (18,5%)	2990 (12,0%)	2930 (11,8%)	2544 (10,2%)	964 (3,9%)	567 (2,3%)	477 (1,9%)	417 (1,7%)	32 (0,1%)	
9.0 DAYS_EMPLOYED	Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%
	Доверительный интервал											
	Среднее	-1578,735796	-2052,988025	365243	-1875,920819	-1844,283412	-1151,283195	-4510,641975	-2093,8826	-1464,009592	-1088,09375	42394,67545
	Стандартн. откл.	1352,952523	2119,172125	0	1821,671059	1897,177045	1055,036468	3818,340369	2301,716142	1435,06535	871,0591758	119484,6343
	Стандартн. ошиб.	14,02117448	31,26928926	0	33,65395802	37,6139816	33,98043661	160,3552228	105,3883425	70,27545252	153,9829625	758,3460516
9.0 DAYS_BIRTH	Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	99,3%	100,0%	100,0%	100,0%	100,0%
	Доверительный интервал											
	Среднее	-13778,27666	-14320,0614	-21441,499	-14144,72526	-14025,77634	-13286,38278	-15306,46914	-13482,37526	-14149,57554	-12508,5	-14884,82808
	Стандартн. откл.	3480,155285	3619,295161	2388,188281	3471,81797	3554,2711	3426,997579	3696,991431	3392,249512	3602,402471	3105,534144	4192,844583
	Стандартн. ошиб.	36,06620603	53,40424498	43,67500553	64,13914061	70,4680083	110,37616	155,2590464	155,3204353	176,410408	548,9860632	26,61118021
REGION_POPULATION_RELATIVE	Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	98,0%	100,0%
	Распределение											
	0.035792000000000004	622 (6,7%)	85 (1,9%)	135 (4,5%)	61 (2,1%)	169 (6,6%)	30 (3,1%)	29 (5,1%)	17 (3,6%)	5 (1,2%)	0 (0,0%)	1153 (4,6%)
	0.025164	340 (3,7%)	266 (5,8%)	121 (4,0%)	154 (5,3%)	95 (3,7%)	23 (2,4%)	24 (4,2%)	21 (4,4%)	4 (1,0%)	0 (0,0%)	1048 (4,2%)
	0.030755	413 (4,4%)	102 (2,2%)	132 (4,4%)	71 (2,4%)	126 (5,0%)	48 (5,0%)	26 (4,6%)	22 (4,6%)	8 (1,9%)	2 (6,3%)	950 (3,8%)
	0.028663	305 (3,3%)	171 (3,7%)	150 (5,0%)	91 (3,1%)	92 (3,6%)	41 (4,3%)	47 (8,3%)	28 (5,9%)	11 (2,6%)	1 (3,1%)	937 (3,8%)
	0.031329	300 (3,2%)	254 (5,5%)	109 (3,6%)	145 (4,9%)	76 (3,0%)	11 (1,1%)	10 (1,8%)	8 (1,7%)	8 (1,9%)	0 (0,0%)	921 (3,7%)
	0.020246	316 (3,4%)	167 (3,6%)	117 (3,9%)	100 (3,4%)	102 (4,0%)	11 (1,1%)	13 (2,3%)	16 (3,4%)	9 (2,2%)	1 (3,1%)	852 (3,4%)
	0.020713	304 (3,3%)	185 (4,0%)	108 (3,6%)	131 (4,5%)	83 (3,3%)	8 (0,8%)	10 (1,8%)	11 (2,3%)	7 (1,7%)	0 (0,0%)	847 (3,4%)
	0.018029	314 (3,4%)	128 (2,8%)	87 (2,9%)	96 (3,3%)	74 (2,9%)	10 (1,0%)	15 (2,6%)	11 (2,3%)	1 (0,2%)	5 (15,6%)	741 (3,0%)
	0.026992000000000002	168 (1,8%)	215 (4,7%)	90 (3,0%)	138 (4,7%)	57 (2,2%)	7 (0,7%)	13 (2,3%)	23 (4,8%)	10 (2,4%)	1 (3,1%)	722 (2,9%)
	0.04622	124 (1,3%)	150 (3,3%)	48 (1,6%)	94 (3,2%)	42 (1,7%)	81 (8,4%)	5 (0,9%)	12 (2,5%)	107 (25,7%)	0 (0,0%)	663 (2,7%)
	<Остальные>	6105 (65,6%)	2870 (62,5%)	1893 (63,3%)	1849 (63,1%)	1628 (64,0%)	694 (72,0%)	375 (66,1%)	308 (64,6%)	247 (59,2%)	22 (68,8%)	15991 (64,4%)
AMT_GOODS_PRICE	Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	99,7%	96,4%	100,0%	91,8%	85,7%	100,0%
	Распределение											
	450000.0	2105 (22,6%)	124 (2,7%)	1018 (34,0%)	2929 (100,0%)	2291 (90,1%)	324 (33,6%)	179 (31,6%)	61 (12,8%)	136 (32,6%)	5 (15,6%)	9172 (36,9%)
	225000.0	1111 (11,9%)	632 (13,8%)	298 (10,0%)	0 (0,0%)	11 (0,4%)	91 (9,4%)	42 (7,4%)	74 (15,5%)	29 (7,0%)	6 (18,8%)	2294 (9,2%)
	675000.0	970 (10,4%)	636 (13,8%)	333 (11,1%)	0 (0,0%)	0 (0,0%)	114 (11,8%)	53 (9,3%)	45 (9,4%)	53 (12,7%)	0 (0,0%)	2204 (8,9%)
	900000.0	504 (5,4%)	347 (7,6%)	73 (2,4%)	0 (0,0%)	0 (0,0%)	52 (5,4%)	24 (4,2%)	19 (4,0%)	28 (6,7%)	1 (3,1%)	1048 (4,2%)
	180000.0	438 (4,7%)	253 (5,5%)	58 (1,9%)	0 (0,0%)	7 (0,3%)	35 (3,6%)	15 (2,6%)	24 (5,0%)	22 (5,3%)	2 (6,3%)	854 (3,4%)
	270000.0	405 (4,3%)	251 (5,5%)	75 (2,5%)	0 (0,0%)	11 (0,4%)	34 (3,5%)	23 (4,1%)	16 (3,4%)	14 (3,4%)	1 (3,1%)	830 (3,3%)
	135000.0	287 (3,1%)	129 (2,8%)	51 (1,7%)	0 (0,0%)	2 (0,1%)	28 (2,9%)	12 (2,1%)	15 (3,1%)	9 (2,2%)	1 (3,1%)	534 (2,2%)
	454500.0	232 (2,5%)	124 (2,7%)	99 (3,3%)	0 (0,0%)	6 (0,2%)	19 (2,0%)	20 (3,5%)	16 (3,4%)	7 (1,7%)	1 (3,1%)	524 (2,1%)
	1125000.0	207 (2,2%)	185 (4,0%)	63 (2,1%)	0 (0,0%)	8 (0,3%)	19 (2,0%)	13 (2,3%)	11 (2,3%)	10 (2,4%)	0 (0,0%)	516 (2,1%)
	360000.0	227 (2,4%)	122 (2,7%)	67 (2,2%)	0 (0,0%)	7 (0,3%)	17 (1,8%)	16 (2,8%)	18 (3,8%)	11 (2,6%)	2 (6,3%)	487 (2,0%)
	<Остальные>	2825 (30,3%)	1790 (39,0%)	855 (28,6%)	1 (0,0%)	201 (7,9%)	231 (24,0%)	170 (30,0%)	178 (37,3%)	98 (23,5%)	13 (40,6%)	6362 (25,6%)
AMT_CREDIT	Значимость	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	36,3%	90,4%	100,0%
	Распределение											
	450000.0	168 (1,8%)	247 (5,4%)	660 (22,1%)	1407 (48,0%)	2544 (100,0%)	138 (14,3%)	49 (8,6%)	80 (16,8%)	92 (22,1%)	2 (6,3%)	5387 (21,7%)
	545040.0	375 (4,0%)	1 (0,0%)	45 (1,5%)	251 (8,6%)	0 (0,0%)	42 (4,4%)	22 (3,9%)	5 (1,0%)	4 (1,0%)	1 (3,1%)	746 (3,0%)
	675000.0	301 (3,2%)	189 (4,1%)	95 (3,2%)	0 (0,0%)	0 (0,0%)	32 (3,3%)	16 (2,8%)	25 (5,2%)	10 (2,4%)	0 (0,0%)	668 (2,7%)
	225000.0	276 (3,0%)	201 (4,4%)	62 (2,1%)	0 (0,0%)	0 (0,0%)	24 (2,5%)	11 (1,9%)	15 (3,1%)	7 (1,7%)	1 (3,1%)	597 (2,4%)
	180000.0	311 (3,3%)	189 (4,1%)	23 (0,8%)	3 (0,1%)	0 (0,0%)	22 (2,3%)	7 (1,2%)	17 (3,6%)	18 (4,3%)	2 (6,3%)	592 (2,4%)
	521280.0	228 (2,4%)	4 (0,1%)	28 (0,9%)	174 (5,9%)	0 (0,0%)	26 (2,7%)	16 (2,8%)	2 (0,4%)	9 (2,2%)	0 (0,0%)	487 (2,0%)
	270000.0	222 (2,4%)	155 (3,4%)	29 (1,0%)	1 (0,0%)	0 (0,0%)	15 (1,6%)	9 (1,6%)	7 (1,5%)	9 (2,2%)	0 (0,0%)	447 (1,8%)
	640080.0	206 (2,2%)	1 (0,0%)	17 (0,6%)	149 (5,1%)	0 (0,0%)	17 (1,8%)	10 (1,8%)	4 (0,8%)	7 (1,7%)	1 (3,1%)	412 (1,7%)
	808650.0	157 (1,7%)	122 (2,7%)	74 (2,5%)	0 (0,0%)	0 (0,0%)	13 (1,3%)	9 (1,6%)	0 (0,0%)	14 (3,4%)	0 (0,0%)	389 (1,6%)
	284400.0	196 (2,1%)	103 (2,2%)	51 (1,7%)	0 (0,0%)	0 (0,0%)	13 (1,3%)	5 (0,9%)	11 (2,3%)	3 (0,7%)	1 (3,1%)	383 (1,5%)
	<Остальные>	6871 (73,8%)	3381 (73,6%)	1906 (63,7%)	945 (32,3%)	0 (0,0%)	622 (64,5%)	413 (72,8%)	311 (65,2%)	244 (58,5%)	24 (75,0%)	14717 (59,3%)

Рисунок Д.4 – Формування кіберпрофілів (продовження)

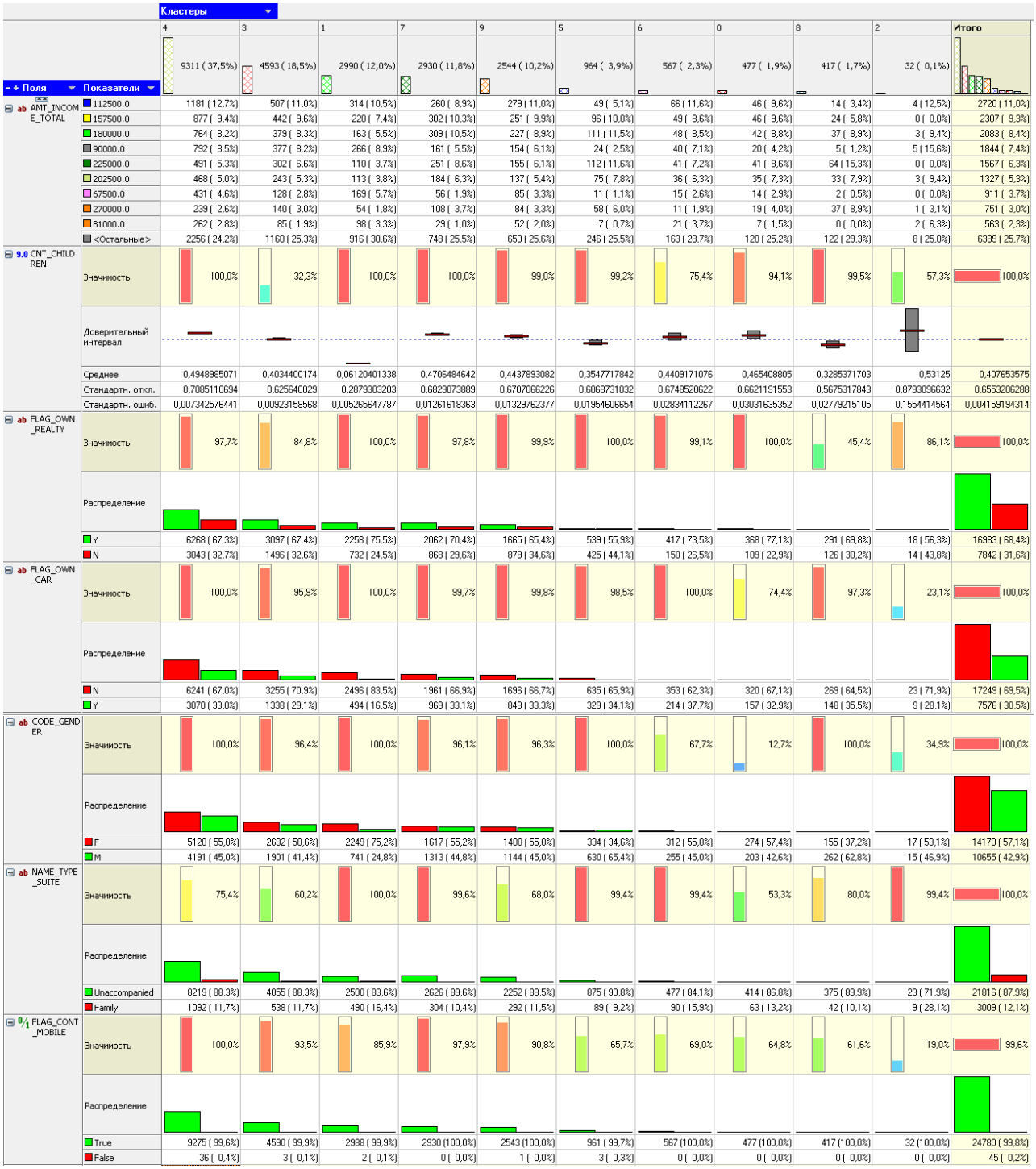


Рисунок Д.5 – Формування кіберпрофілів (завершення)

Додаток Е

Розрахунки для прогнозних моделей інформаційних трендів кібератак

Таблиця Е.1 – Значення циклічних складових інформаційних трендів запитів щодо кібератак на комп’ютерні системи, мережеву та хмарну інфраструктуру фінансової установи

Спостере-ження	CS	NI	CI	Спостере-ження	CS	NI	CI
1	-1,63689	-6,11530	-4,06617	25	-1,84210	1,41283	4,52446
2	-6,18898	-4,03717	-3,40992	26	0,44540	3,27533	2,42862
3	-0,69939	-2,39134	-3,92033	27	1,36207	9,50033	9,33279
4	-0,00148	-3,16738	-3,75367	28	0,86623	8,00866	13,63696
5	1,21207	5,62428	1,33487	29	-0,99210	0,76699	11,32029
6	0,92561	4,35866	-1,19117	30	3,42457	2,01283	-0,19221
7	0,85269	2,42637	-0,24846	31	2,66623	2,08783	2,77029
8	-1,15773	4,69720	-0,05054	32	5,04123	-0,52884	-0,73804
9	-5,46502	-2,29238	-3,58700	33	2,61623	1,20449	0,16196
10	-3,00668	-3,75592	1,90779	34	3,56623	0,55449	-2,74221
11	-2,29835	-0,02676	-0,69638	35	5,89540	6,08366	-1,06304
12	-2,07439	-1,82363	0,97550	36	3,00790	0,03783	-0,61721
13	-0,42856	-6,36530	2,64217	37	1,10373	-6,08717	-2,17554
14	-1,09523	-2,40697	0,99633	38	3,82457	3,71699	-0,27971
15	-3,49627	3,50449	3,92342	39	10,70373	4,72116	-1,03388
16	-4,42335	-1,83405	4,02237	40	9,60373	0,85449	-1,97138
17	-2,62648	-3,15176	1,88175	41	2,10790	-6,19551	-5,48804
18	-0,80877	1,03574	1,06404	42	3,20790	-0,80801	-0,96721
19	-4,70981	-7,51113	-1,30575	43	3,33290	-2,43301	-0,86721
20	-4,57439	-3,53197	-2,12867	44	-0,32127	-2,45801	-2,14638
21	-6,48064	4,44720	1,03279	45	1,40790	-5,09134	-3,67138
22	-5,88689	0,91595	-3,83700	46	-2,22960	-3,02884	-3,78804
23	-3,93898	-3,70905	1,33487	47	1,89436	2,86908	-2,35783
24	-5,81398	0,52533	-3,27971	48	3,12873	4,10866	-3,71721

Таблиця Е.2 – Прогнозований рівень кібератак на комп’ютерні системи, мережу та хмарну інфраструктуру фінансової установи

Дата	CS	NI	CI	Дата	CS	NI	CI
17.04.2022	70	75	46	04.12.2022	80	77	51
24.04.2022	72	69	51	11.12.2022	77	78	51
01.05.2022	68	76	47	18.12.2022	72	69	47
08.05.2022	75	74	55	25.12.2022	74	69	53
15.05.2022	78	72	52	01.01.2023	71	73	50
22.05.2022	79	81	59	08.01.2023	77	70	52
29.05.2022	79	76	64	15.01.2023	74	67	54
05.06.2022	78	70	61	22.01.2023	77	69	52
12.06.2022	82	75	50	29.01.2023	77	78	55
19.06.2022	80	76	53	05.02.2023	75	70	55
26.06.2022	84	71	49	12.02.2023	77	69	53
03.07.2022	83	76	50	19.02.2023	79	74	52
10.07.2022	80	74	47	26.02.2023	76	63	50
17.07.2022	84	80	49	05.03.2023	75	69	49
24.07.2022	77	73	50	12.03.2023	74	81	52
31.07.2022	81	66	48	19.03.2023	74	75	47
07.08.2022	82	78	50	26.03.2023	76	69	53
14.08.2022	88	76	49	02.04.2023	72	76	48
21.08.2022	90	75	48	09.04.2023	79	74	56
28.08.2022	79	65	45	16.04.2023	82	72	54
04.09.2022	84	75	49	23.04.2023	83	81	61
11.09.2022	82	69	50	30.04.2023	83	76	65
18.09.2022	75	70	48	07.05.2023	82	70	63
25.09.2022	82	69	47	14.05.2023	86	75	51
02.10.2022	79	67	47	21.05.2023	84	76	54
09.10.2022	79	75	48	28.05.2023	88	71	51
16.10.2022	82	78	47	04.06.2023	87	76	52
23.10.2022	81	64	47	11.06.2023	84	74	49
30.10.2022	77	72	47	18.06.2023	88	80	50
06.11.2022	80	73	47	25.06.2023	80	73	51
13.11.2022	79	67	47	02.07.2023	85	66	49
20.11.2022	80	85	52	09.07.2023	86	78	51
27.11.2022	80	79	50				

Додаток Ж

Результати асоціативного аналізу

Таблиця Ж.1 – Результати асоціативного аналізу для першої групи пошукових запитів

№	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_ metric
0	Cyber police number_17	How to block a transaction_0	0,131	0,444	3,399	0,011	1,565	0,731
1	Cyber police number_19	How to block a transaction_0	0,131	0,667	5,098	0,012	2,608	0,823
2	Cyber police number_21	How to block a transaction_0	0,131	0,500	3,824	0,011	1,738	0,762
3	How to change the bank_40	Cyber police number_24	0,023	0,600	26,000	0,011	2,442	0,980
4	Cyber police number_24	How to change the bank_40	0,019	0,500	26,000	0,011	1,962	0,984
5	Cyber police number_25	How to block a transaction_0	0,131	0,300	2,294	0,007	1,242	0,587
6	How to protect your computer_63	Cyber police number_49	0,023	0,500	21,667	0,011	1,954	0,976
7	Cyber police number_49	How to protect your computer_63	0,023	0,500	21,667	0,011	1,954	0,976
8	How to protect your computer_19	How to block a transaction_0	0,131	0,500	3,824	0,009	1,738	0,756
9	How to protect your computer_22	How to block a transaction_0	0,131	0,750	5,735	0,010	3,477	0,839
10	How to protect your computer_26	How to block a transaction_0	0,131	0,429	3,277	0,008	1,521	0,714
11	How to protect your computer_30	How to block a transaction_0	0,131	0,375	2,868	0,008	1,391	0,672
12	How to change the bank_55	How to protect your computer_48	0,023	0,600	26,000	0,011	2,442	0,980
13	How to protect your computer_48	How to change the bank_55	0,019	0,500	26,000	0,011	1,962	0,984
14	How to block a transaction_31	How to protect your computer_54	0,019	0,429	22,286	0,011	1,716	0,982
15	How to protect your computer_54	How to block a transaction_31	0,027	0,600	22,286	0,011	2,433	0,974
16	How to change the bank_31	How to block a transaction_0	0,131	0,273	2,086	0,006	1,195	0,544
17	How to change the bank_33	How to block a transaction_0	0,131	0,500	3,824	0,009	1,738	0,756
18	How to change the bank_36	How to block a transaction_0	0,131	0,364	2,781	0,010	1,366	0,669
19	How to change the bank_46	How to block a transaction_0	0,131	0,214	1,639	0,004	1,106	0,412

Таблиця Ж.2 – Результати асоціативного аналізу для другої групи пошукових запитів

№	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_metric
1	2	3	4	5	6	7	8	9
0	How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
1	How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
2	How to prevent hacking_22	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
3	How to prevent hacking_29	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
4	How to prevent hacking_30	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
5	How to prevent hacking_30	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
6	How to prevent hacking_34	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
7	How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
8	How to prevent hacking_35	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
9	How to prevent hacking_36	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
10	How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
11	How to prevent hacking_37	How to reduce the credit limit_0	0,673	0,500	0,743	-0,004	0,654	-0,262
12	How to prevent hacking_37	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
13	How to prevent hacking_38	How to reduce the credit limit_0	0,673	0,833	1,238	0,004	1,962	0,197
14	How to prevent hacking_38	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
15	How to prevent hacking_39	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
16	How to prevent hacking_39	Black list of customers_0	0,758	0,714	0,943	-0,001	0,848	-0,059
17	How to prevent hacking_40	How to reduce the credit limit_0	0,673	0,625	0,929	-0,001	0,872	-0,074
18	How to prevent hacking_40	Black list of customers_0	0,758	0,500	0,660	-0,008	0,485	-0,347
19	How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
20	How to prevent hacking_41	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
21	How to prevent hacking_42	How to reduce the credit limit_0	0,673	0,556	0,825	-0,004	0,736	-0,180
22	How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,008	inf	0,251
23	How to prevent hacking_43	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
24	How to prevent hacking_43	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
25	How to prevent hacking_44	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
26	How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
27	How to prevent hacking_46	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
28	How to prevent hacking_46	Black list of customers_0	0,758	0,571	0,754	-0,005	0,565	-0,251

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9
29	How to prevent hacking_47	How to reduce the credit limit_0	0,673	0,333	0,495	-0,012	0,490	-0,514
30	How to prevent hacking_47	Black list of customers_0	0,758	0,556	0,733	-0,007	0,545	-0,274
31	How to prevent hacking_48	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
32	How to prevent hacking_49	How to reduce the credit limit_0	0,673	0,833	1,238	0,004	1,962	0,197
33	How to prevent hacking_49	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
34	How to prevent hacking_50	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
35	How to prevent hacking_50	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
36	How to prevent hacking_51	How to reduce the credit limit_0	0,673	0,750	1,114	0,002	1,308	0,106
37	How to prevent hacking_51	Black list of customers_0	0,758	0,875	1,155	0,004	1,938	0,138
38	How to prevent hacking_52	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
39	How to prevent hacking_52	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
40	How to prevent hacking_53	How to reduce the credit limit_0	0,673	0,500	0,743	-0,005	0,654	-0,263
41	How to prevent hacking_53	Black list of customers_0	0,758	0,625	0,825	-0,004	0,646	-0,180
42	How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,010	inf	0,337
43	How to prevent hacking_54	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
44	How to prevent hacking_55	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
45	How to prevent hacking_56	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
46	How to prevent hacking_56	Black list of customers_0	0,758	0,714	0,943	-0,001	0,848	-0,059
47	How to prevent hacking_57	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
48	How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
49	How to prevent hacking_58	How to reduce the credit limit_0	0,673	0,600	0,891	-0,003	0,817	-0,112
50	How to prevent hacking_58	Black list of customers_0	0,758	0,800	1,056	0,002	1,212	0,055
51	How to prevent hacking_59	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
52	How to prevent hacking_59	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
53	How to prevent hacking_60	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
54	How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
55	How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
56	How to prevent hacking_61	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
57	How to prevent hacking_66	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
58	How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
59	How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
60	How to prevent hacking_69	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
61	How to prevent hacking_70	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
62	How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
63	How to prevent hacking_74	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
64	How to prevent hacking_77	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
65	How to reduce the credit limit_0	Black list of customers_0	0,758	0,766	1,011	0,005	1,034	0,032
66	Black list of customers_0	How to reduce the credit limit_0	0,673	0,680	1,011	0,005	1,022	0,043
67	Black list of customers_16	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
68	Black list of customers_17	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
69	Black list of customers_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
70	Black list of customers_19	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
71	Black list of customers_20	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
72	Black list of customers_30	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9
73	How to reduce the credit limit_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
74	How to reduce the credit limit_20	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
75	How to reduce the credit limit_23	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
76	How to reduce the credit limit_26	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
77	How to reduce the credit limit_27	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
78	How to reduce the credit limit_30	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
79	How to reduce the credit limit_33	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
80	How to reduce the credit limit_0, How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
81	Black list of customers_0, How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
82	How to prevent hacking_18	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
83	How to reduce the credit limit_0, How to prevent hacking_35	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
84	Black list of customers_0, How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
85	How to prevent hacking_35	How to reduce the credit limit_0, Black list of customers_0	0,515	0,800	1,552	0,005	2,423	0,363
86	How to reduce the credit limit_0, How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
87	Black list of customers_0, How to prevent hacking_36	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
88	How to prevent hacking_36	How to reduce the credit limit_0, Black list of customers_0	0,515	0,857	1,663	0,009	3,392	0,410
89	How to reduce the credit limit_0, How to prevent hacking_37	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
90	Black list of customers_0, How to prevent hacking_37	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
91	How to prevent hacking_37	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
92	How to reduce the credit limit_0, How to prevent hacking_38	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
93	Black list of customers_0, How to prevent hacking_38	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
94	How to prevent hacking_38	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
95	How to reduce the credit limit_0, How to prevent hacking_39	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
96	Black list of customers_0, How to prevent hacking_39	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
97	How to prevent hacking_39	How to reduce the credit limit_0, Black list of customers_0	0,515	0,429	0,832	-0,002	0,848	-0,172
98	How to reduce the credit limit_0, How to prevent hacking_40	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
99	Black list of customers_0, How to prevent hacking_40	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9
100	How to prevent hacking_40	How to reduce the credit limit_0, Black list of customers_0	0,515	0,375	0,728	-0,004	0,775	-0,279
101	How to reduce the credit limit_0, How to prevent hacking_41	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
102	Black list of customers_0, How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
103	How to prevent hacking_41	How to reduce the credit limit_0, Black list of customers_0	0,515	0,833	1,617	0,007	2,908	0,391
104	How to reduce the credit limit_0, How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
105	Black list of customers_0, How to prevent hacking_42	How to reduce the credit limit_0	0,673	0,556	0,825	-0,004	0,736	-0,180
106	How to prevent hacking_42	How to reduce the credit limit_0, Black list of customers_0	0,515	0,556	1,078	0,001	1,090	0,075
107	How to reduce the credit limit_0, How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
108	Black list of customers_0, How to prevent hacking_44	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
109	How to prevent hacking_44	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232
110	How to reduce the credit limit_0, How to prevent hacking_47	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
111	Black list of customers_0, How to prevent hacking_47	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
112	How to prevent hacking_47	How to reduce the credit limit_0, Black list of customers_0	0,515	0,333	0,647	-0,006	0,727	-0,361
113	How to reduce the credit limit_0, How to prevent hacking_49	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
114	Black list of customers_0, How to prevent hacking_49	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
115	How to prevent hacking_49	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232
116	How to reduce the credit limit_0, How to prevent hacking_50	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
117	Black list of customers_0, How to prevent hacking_50	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
118	How to prevent hacking_50	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
119	How to reduce the credit limit_0, How to prevent hacking_51	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
120	Black list of customers_0, How to prevent hacking_51	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9
121	How to prevent hacking_51	How to reduce the credit limit_0, Black list of customers_0	0,515	0,625	1,213	0,003	1,292	0,181
122	How to reduce the credit limit_0, How to prevent hacking_54	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
123	Black list of customers_0, How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
124	How to prevent hacking_54	How to reduce the credit limit_0, Black list of customers_0	0,515	0,750	1,455	0,007	1,938	0,323
125	How to reduce the credit limit_0, How to prevent hacking_56	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
126	Black list of customers_0, How to prevent hacking_56	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
127	How to prevent hacking_56	How to reduce the credit limit_0, Black list of customers_0	0,515	0,571	1,109	0,002	1,131	0,101
128	How to reduce the credit limit_0, How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
129	Black list of customers_0, How to prevent hacking_57	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
130	How to prevent hacking_57	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
131	How to reduce the credit limit_0, How to prevent hacking_58	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
132	Black list of customers_0, How to prevent hacking_58	How to reduce the credit limit_0	0,673	0,500	0,743	-0,005	0,654	-0,263
133	How to prevent hacking_58	How to reduce the credit limit_0, Black list of customers_0	0,515	0,400	0,776	-0,004	0,808	-0,231
134	How to reduce the credit limit_0, How to prevent hacking_59	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
135	Black list of customers_0, How to prevent hacking_59	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
136	How to prevent hacking_59	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
137	How to reduce the credit limit_0, How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
138	Black list of customers_0, How to prevent hacking_60	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
139	How to prevent hacking_60	How to reduce the credit limit_0, Black list of customers_0	0,515	0,571	1,109	0,002	1,131	0,101

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9
140	How to reduce the credit limit_0, How to prevent hacking_61	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
141	Black list of customers_0, How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
142	How to prevent hacking_61	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
143	How to reduce the credit limit_0, How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
144	Black list of customers_0, How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
145	How to prevent hacking_68	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
146	How to reduce the credit limit_0, How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
147	Black list of customers_0, How to prevent hacking_70	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
148	How to prevent hacking_70	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232

Таблиця Ж.3 – Фрагмент результатів асоціативного аналізу для третьої групи пошукових запитів

	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_metric
1	2	3	4	5	6	7	8	9
0	Police number_47	How to protect yourself from cyber attacks_0	0,750	0,750	1,000	0,000	1,000	0,000
1	Police number_47	How to find that phone is hacked_0	0,685	0,750	1,096	0,001	1,262	0,089
2	Police number_47	Which bank is the most secure online_0	0,765	1,000	1,307	0,004	inf	0,238
3	Police number_48	How to protect yourself from cyber attacks_0	0,750	0,714	0,952	-0,001	0,875	-0,049
4	Police number_48	How to find that phone is hacked_0	0,685	0,857	1,252	0,005	2,208	0,207
5	Police number_48	Which bank is the most secure online_0	0,765	0,857	1,120	0,002	1,642	0,110
6	Police number_49	How to protect yourself from cyber attacks_0	0,750	1,000	1,333	0,007	inf	0,257
7	Police number_49	How to find that phone is hacked_0	0,685	0,429	0,626	-0,007	0,552	-0,380
8	Police number_49	Which bank is the most secure online_0	0,765	0,857	1,120	0,002	1,642	0,110
9	Police number_50	How to protect yourself from cyber attacks_0	0,750	0,833	1,111	0,002	1,500	0,102
10	Police number_50	How to find that phone is hacked_0	0,685	0,833	1,217	0,003	1,892	0,183
11	Police number_50	Which bank is the most secure online_0	0,765	0,500	0,653	-0,006	0,469	-0,352
12	Police number_51	How to protect yourself from cyber attacks_0	0,750	0,917	1,222	0,008	3,000	0,191
13	Police number_51	How to find that phone is hacked_0	0,685	0,833	1,217	0,007	1,892	0,187
14	Police number_51	Which bank is the most secure online_0	0,765	1,000	1,307	0,011	inf	0,246
15	Police number_52	How to protect yourself from cyber attacks_0	0,750	0,857	1,143	0,003	1,750	0,128
16	Police number_52	How to find that phone is hacked_0	0,685	0,714	1,043	0,001	1,104	0,043
17	Police number_52	Which bank is the most secure online_0	0,765	1,000	1,307	0,006	inf	0,241
18	Police number_53	How to protect yourself from cyber attacks_0	0,750	0,615	0,821	-0,007	0,650	-0,187
19	Police number_53	How to find that phone is hacked_0	0,685	0,615	0,899	-0,003	0,820	-0,106
20	Police number_53	Which bank is the most secure online_0	0,765	1,000	1,307	0,012	inf	0,247
21	Police number_54	How to protect yourself from cyber attacks_0	0,750	0,867	1,156	0,007	1,875	0,143
22	Police number_54	How to find that phone is hacked_0	0,685	0,467	0,682	-0,013	0,591	-0,331
23	Police number_54	Which bank is the most secure online_0	0,765	0,800	1,045	0,002	1,173	0,046
24	Police number_55	How to protect yourself from cyber attacks_0	0,750	0,600	0,800	-0,006	0,625	-0,206
25	Police number_55	How to find that phone is hacked_0	0,685	0,700	1,022	0,001	1,051	0,023
26	Police number_55	Which bank is the most secure online_0	0,765	0,900	1,176	0,005	2,346	0,156
27	Police number_56	How to protect yourself from cyber attacks_0	0,750	0,643	0,857	-0,006	0,700	-0,150
28	Police number_56	How to find that phone is hacked_0	0,685	0,786	1,148	0,005	1,472	0,136
29	Police number_56	Which bank is the most secure online_0	0,765	0,714	0,933	-0,003	0,821	-0,070
30	Bank call center numbe_68	Police number_56	0,054	0,500	9,286	0,010	1,892	0,913
31	Police number_56	Bank call center numbe_68	0,023	0,214	9,286	0,010	1,243	0,943
32	Police number_57	How to protect yourself from cyber attacks_0	0,750	0,667	0,889	-0,003	0,750	-0,115

Продовження таблиці Ж.3

1	2	3	4	5	6	7	8	9
33	Police number_57	How to find that phone is hacked_0	0,685	0,778	1,136	0,003	1,419	0,124
34	Police number_57	Which bank is the most secure online_0	0,765	0,778	1,016	0,000	1,056	0,017
35	Police number_58	How to protect yourself from cyber attacks_0	0,750	0,750	1,000	0,000	1,000	0,000
36	Police number_58	How to find that phone is hacked_0	0,685	0,875	1,278	0,012	2,523	0,232
37	Police number_58	Which bank is the most secure online_0	0,765	0,688	0,898	-0,005	0,751	-0,108
38	Bank call center numbe_50	Police number_58	0,062	0,300	4,875	0,009	1,341	0,827
39	Police number_59	How to protect yourself from cyber attacks_0	0,750	0,786	1,048	0,002	1,167	0,048
40	Police number_59	How to find that phone is hacked_0	0,685	0,500	0,730	-0,010	0,631	-0,281
41	Police number_59	Which bank is the most secure online_0	0,765	0,786	1,027	0,001	1,095	0,027
42	Police number_59	Bank call center numbe_58	0,035	0,214	6,190	0,010	1,229	0,886
43	Bank call center numbe_58	Police number_59	0,054	0,333	6,190	0,010	1,419	0,869
44	Police number_60	How to protect yourself from cyber attacks_0	0,750	0,850	1,133	0,008	1,667	0,127
45	Police number_60	How to find that phone is hacked_0	0,685	0,500	0,730	-0,014	0,631	-0,286
46	Police number_60	Which bank is the most secure online_0	0,765	0,750	0,980	-0,001	0,938	-0,022
47	Bank call center numbe_51	Police number_60	0,077	0,214	2,786	0,007	1,175	0,678
48	Police number_61	How to protect yourself from cyber attacks_0	0,750	0,857	1,143	0,006	1,750	0,132
49	Police number_61	How to find that phone is hacked_0	0,685	0,857	1,252	0,009	2,208	0,213
50	Police number_61	Which bank is the most secure online_0	0,765	0,714	0,933	-0,003	0,821	-0,070
51	Police number_62	How to protect yourself from cyber attacks_0	0,750	0,524	0,698	-0,018	0,525	-0,320
52	Police number_62	How to find that phone is hacked_0	0,685	0,762	1,113	0,006	1,325	0,110
53	Police number_62	Which bank is the most secure online_0	0,765	0,762	0,995	0,000	0,985	-0,005

Таблиця Ж.4 – Результати асоціативного аналізу для першої групи змінних, імовірність асоціативних правил яких дорівнює 1

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
1	2	3	4	5	6	7	8
How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_22	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_29	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,008	inf	0,251
How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to prevent hacking_48	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,010	inf	0,337
How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to prevent hacking_66	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_69	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to prevent hacking_74	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_77	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_16	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
Black list of customers_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
Black list of customers_30	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to reduce the credit limit_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to reduce the credit limit_20	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245

Продовження таблиці Ж.4

1	2	3	4	5	6	7	8
How to reduce the credit limit_23	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to reduce the credit limit_26	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to reduce the credit limit_33	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to reduce the credit limit_0, How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_18	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
Black list of customers_0, How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
How to reduce the credit limit_0, How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to reduce the credit limit_0, How to prevent hacking_37	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to reduce the credit limit_0, How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
How to reduce the credit limit_0, How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to reduce the credit limit_0, How to prevent hacking_47	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
How to reduce the credit limit_0, How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_59	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to reduce the credit limit_0, How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
Black list of customers_0, How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331

Продовження таблиці Ж.4

1	2	3	4	5	6	7	8
How to reduce the credit limit_0, How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_68	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
How to reduce the credit limit_0, How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246

Додаток И

Допоміжні розрахунки для визначення CICCS

Таблиця И.1 – Інформаційна база формування CICCS за 2014-2022 рр.

Показник	2014	2015	2016	2017	2018	2019	2020	2021	2022
Частка організацій, які зазнали принаймні однієї успішної кібератаки, %	61,9	70,5	75,6	79,2	77,2	78,0	80,7	86,2	85,3
Частка організацій, які зазнали шість та більше успішних кібератак, %	16,2	22,6	23,8	32,9	27,4	31,5	35,2	39,7	40,7
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», %	38,1	51,9	62,1	61,5	62,3	65,2	69,3	75,6	76,1
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «дуже вірогідною», %	8,5	14,0	16,1	20,4	19,7	21,2	27,2	32,0	35,1
Індекс загрози, що відображає загальну стурбованість щодо кібератак, од	3,61	3,26	3,71	3,75	3,54	3,52	3,79	3,88	3,88
Індекс занепокоєння безпекою, од	2,94	2,99	3,37	3,41	3,18	3,19	3,53	3,65	3,64
Частка організацій із зростаючим бюджетом безпеки, %	-	-	-	76,0	78,7	83,5	85,4	77,8	83,2
Частка організацій, які відчувають нестачу кваліфікованого персоналу з ІТ-безпеки, %	-	-	-	-	80,9	84,2	84,8	87,0	84,1
Частка організацій, уражених програмами-вимагачами, %	-	-	-	-	55,1	56,1	62,4	68,5	71,0
Частка викрадених або скомпрометованих облікових даних, млн дол. США	-	-	3,62	3,86	3,92	3,95	4,24	4,35	3,62

Таблиця И.2 – Нормалізовані значення показників, що є складовими CICCS, за 2016-2022 рр.

Показник	2016	2017	2018	2019	2020	2021	2022
Частка організацій, які зазнали принаймні однієї успішної кібератаки	1,00	0,66	0,85	0,77	0,52	0,00	0,08
Частка організацій, які зазнали шість та більше успішних кібератак	1,00	0,46	0,79	0,54	0,33	0,06	0,00
Частка респондентів, які вважають, що успішна кібер атака на їх організацію протягом наступних 12 місяців буде «вірогідною»	0,96	1,00	0,95	0,75	0,47	0,03	0,00
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «дуже вірогідною»	1,00	0,77	0,81	0,73	0,42	0,16	0,00
Індекс загрози, що відображає загальну стурбованість щодо кібер атак	0,47	0,36	0,94	1,00	0,25	0,00	0,00
Індекс занепокоєння безпекою	0,60	0,51	1,00	0,98	0,26	0,00	0,02
Частка організацій із зростаючим бюджетом безпеки	0,00	0,13	0,38	0,82	1,00	0,29	0,80
Частка організацій, які відчувають нестачу кваліфікованого персоналу з ІТ-безпеки	1,00	0,90	0,80	0,37	0,29	0,00	0,38
Частка організацій, уражених програмами-вимагачами	1,00	0,86	0,71	0,66	0,38	0,11	0,00
Частка викрадених або скомпрометованих облікових даних	1,00	0,67	0,59	0,55	0,15	0,00	1,00

Таблиця И.3 – Темпи приросту показників, що є складовими CICCS, за 2014-2022 рр.

Показник	2016	2017	2018	2019	2020	2021	2022
Частка організацій, які зазнали принаймні однієї успішної кібератаки	7%	5%	-3%	1%	3%	7%	-1%
Частка організацій, які зазнали шість та більше успішних кібератак	5%	38%	-17%	15%	12%	13%	3%
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»	20%	-1%	1%	5%	6%	9%	1%
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «дуже вірогідною»	15%	27%	-3%	8%	28%	18%	10%
Індекс загрози, що відображає загальну стурбованість щодо кібератак	14%	1%	-6%	-1%	8%	2%	0%
Індекс занепокоєння безпекою	13%	1%	-7%	0%	11%	3%	0%
Частка організацій із зростаючим бюджетом безпеки	1%	2%	4%	6%	2%	-9%	7%
Частка організацій, які відчувають нестачу кваліфікованого персоналу з IT-безпеки	1%	1%	1%	4%	1%	3%	-3%
Частка організацій, уражених програмами-вимагачами	7%	7%	7%	2%	11%	10%	4%
Частка викрадених або скомпрометованих облікових даних	0%	7%	2%	1%	7%	3%	-17%

Додаток К

Результати етапу визначення інтегральних таргетів

Таблиця К.1 – Результат розрахунку інтегральних показників та їх нормалізованих значень

Країна	Інтегральний індикатор економічних детермінант		Інтегральний індикатор соціальних детермінант		Інтегральний індикатор політичниих детермінант	
	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований
Belgium	1.1374	0.4992	2.2428	0.7069	3.3499	0.6783
Lithuania	0.8505	0.3033	2.0229	0.6251	2.7364	0.5454
Estonia	0.8891	0.3297	2.1798	0.6834	3.5051	0.7119
Czechia	0.8973	0.3353	2.1571	0.6750	2.8039	0.5601
Germany	1.2333	0.5647	2.4768	0.7939	3.6723	0.7481
Romania	0.7702	0.2485	1.7558	0.5257	1.7144	0.3241
Greece	0.8251	0.2860	1.7863	0.5371	1.8379	0.3509
Portugal	0.8795	0.3231	2.2898	0.7244	2.8573	0.5716
United Kingdom	1.1611	0.5154	2.3429	0.7441	3.3986	0.6889
Spain	1.0144	0.4152	2.1778	0.6827	2.4673	0.4872
Poland	0.7998	0.2686	1.9955	0.6149	2.0021	0.3864
Austria	1.1515	0.5088	2.4034	0.7666	3.5481	0.7212
Finland	1.1352	0.4977	2.3084	0.7313	4.6100	0.9511
Saudi Arabia	0.8552	0.3065	2.0346	0.6294	1.5123	0.2804
France	1.0454	0.4364	2.2536	0.7109	3.0044	0.6035
Sweden	1.2127	0.5507	2.4648	0.7895	4.2256	0.8679
Denmark	1.2924	0.6051	2.4683	0.7908	4.8356	1.0000
Croatia	0.8027	0.2707	1.9417	0.5949	2.0136	0.3889
Slovak Republic	0.8364	0.2937	1.9750	0.6073	2.0221	0.3908
Netherlands	1.2050	0.5454	2.4580	0.7869	4.0503	0.8300
Serbia	0.7156	0.2112	1.6682	0.4931	1.2886	0.2320
Malaysia	0.7596	0.2412	1.9111	0.5835	2.0318	0.3929
Italy	0.9806	0.3921	2.0825	0.6473	2.1158	0.4111
Ukraine	0.6360	0.1569	1.6626	0.4910	0.7520	0.1157
Latvia	0.8282	0.2881	1.9015	0.5799	2.4471	0.4828
Ireland	1.6602	0.8562	2.4312	0.7770	3.8838	0.7939
Switzerland	1.5538	0.7835	2.6106	0.8437	4.7193	0.9748
Bulgaria	0.7485	0.2337	1.8264	0.5520	1.3875	0.2534
Dominican Republic	0.7184	0.2131	1.5046	0.4323	1.3900	0.2539
Russian Federation	0.8556	0.3068	1.7848	0.5365	0.6674	0.0974
Singapore	1.4420	0.7072	2.7659	0.9015	4.3702	0.8992
Morocco	0.6548	0.1697	1.2711	0.3454	1.1722	0.2067
Canada	1.2492	0.5755	2.4718	0.7921	3.8489	0.7863
Korea, Rep.	0.9706	0.3853	2.4894	0.7986	2.8680	0.5739
Bangladesh	0.6155	0.1428	1.3233	0.3648	0.7126	0.1072
India	0.5780	0.1172	0.9071	0.2100	1.3984	0.2557

Країна	Інтегральний індикатор економічних детермінант		Інтегральний індикатор соціальних детермінант		Інтегральний індикатор політичниих детермінант	
	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований
Hungary	0.8016	0.2699	2.0278	0.6269	1.8862	0.3614
Slovenia	0.9179	0.3493	2.3221	0.7364	2.7530	0.5490
Israel	1.1764	0.5258	2.3461	0.7453	2.1243	0.4129
Norway	1.6006	0.8155	2.6886	0.8727	4.5859	0.9459
Cyprus	0.9364	0.3619	2.3619	0.7512	2.2250	0.4347
Australia	1.3135	0.6195	2.5092	0.8060	3.8982	0.7970
Luxembourg	1.8708	1.0000	2.4856	0.7972	4.3733	0.8999
Georgia	0.6908	0.1943	1.3819	0.3866	1.8080	0.3444
Thailand	0.7001	0.2006	1.9070	0.5820	1.2396	0.2213
United States	1.6607	0.8566	2.1846	0.6852	2.8400	0.5679
Paraguay	0.6863	0.1912	1.4241	0.4023	0.9236	0.1529
Philippines	0.6456	0.1634	1.4000	0.3934	1.1210	0.1957
Indonesia	0.6686	0.1791	1.2841	0.3502	1.3670	0.2489
Azerbaijan	0.6614	0.1742	1.2161	0.3249	0.8168	0.1298
Argentina	0.6658	0.1772	1.7599	0.5273	1.2295	0.2192
Japan	1.0041	0.4082	2.7128	0.8817	3.8133	0.7786
Peru	0.7201	0.2142	1.4992	0.4303	0.9894	0.1672
Albania	0.6890	0.1930	1.5047	0.4323	1.3703	0.2496
Turkiye	0.5841	0.1214	1.6188	0.4748	0.9528	0.1592
Chile	0.8124	0.2773	1.9443	0.5958	2.3307	0.4576
Uruguay	0.8361	0.2935	1.8127	0.5469	3.1696	0.6392
Benin	0.6460	0.1636	0.6419	0.1113	1.1767	0.2077
North Macedonia	0.6919	0.1950	1.6559	0.4885	1.3654	0.2486
Qatar	1.4150	0.6888	3.0307	1.0000	2.3951	0.4715
Egypt, Arab Rep.	0.6584	0.1721	1.2759	0.3472	0.8357	0.1339
Moldova	0.6622	0.1747	1.4071	0.3960	1.1303	0.1977
Bahrain	0.9191	0.3501	2.5584	0.8243	1.4963	0.2769
Zambia	0.6436	0.1620	0.7175	0.1395	1.0514	0.1806
Iceland	1.3358	0.6347	2.7046	0.8787	4.0618	0.8324
Nigeria	0.6265	0.1503	0.4493	0.0397	0.5726	0.0769
Ecuador	0.7032	0.2027	1.5010	0.4309	1.0697	0.1846
Tunisia	0.6619	0.1745	1.4018	0.3940	1.1661	0.2054
Colombia	0.7372	0.2260	1.4049	0.3952	1.2013	0.2131
Belarus	0.7002	0.2007	2.0134	0.6215	0.6865	0.1016
Brazil	0.7197	0.2140	1.5819	0.4610	1.0673	0.1840
China	0.7043	0.2035	1.8842	0.5735	1.3079	0.2361
New Zealand	1.1189	0.4866	2.4836	0.7965	4.3730	0.8998
Uganda	0.6516	0.1675	0.7975	0.1692	0.8031	0.1268
Panama	0.8076	0.2740	1.6293	0.4787	1.2901	0.2323
Malta	0.9677	0.3833	2.5383	0.8168	2.4137	0.4756
Costa Rica	0.7605	0.2418	1.8027	0.5432	2.0855	0.4045
Kazakhstan	0.7185	0.2132	1.6503	0.4865	1.1810	0.2086
Ghana	0.6175	0.1442	0.8968	0.2062	1.4506	0.2670
Oman	0.8359	0.2933	2.0039	0.6180	1.5082	0.2795

Країна	Інтегральний індикатор економічних детермінант		Інтегральний індикатор соціальних детермінант		Інтегральний індикатор політичниих детермінант	
	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований
Cote d'Ivoire	0.6539	0.1691	0.7132	0.1378	1.0642	0.1833
Sri Lanka	0.5847	0.1218	1.5684	0.4560	1.0840	0.1876
Mauritius	0.7249	0.2175	1.8074	0.5449	2.3547	0.4628
Pakistan	0.5258	0.0816	0.9937	0.2422	0.6815	0.1005
Kenya	0.6383	0.1584	0.9125	0.2120	0.9621	0.1612
Jamaica	0.6770	0.1848	1.5650	0.4547	1.8003	0.3428
Brunei Darussalam	0.9570	0.3760	1.9733	0.6066	2.8320	0.5662
United Arab Emirates	1.1368	0.4988	2.7442	0.8934	2.4926	0.4927
Kyrgyz Republic	0.6289	0.1520	1.4817	0.4237	0.6650	0.0969
Mexico	0.7230	0.2162	1.5453	0.4474	0.8840	0.1443
Vietnam	0.6738	0.1826	1.6486	0.4859	1.2375	0.2209
Uzbekistan	0.6327	0.1546	1.3102	0.3600	0.8863	0.1448
South Africa	0.7008	0.2011	0.8838	0.2013	1.2875	0.2317
Armenia	0.6928	0.1956	1.5319	0.4424	1.2120	0.2154
Montenegro	0.7208	0.2148	1.5926	0.4650	1.4185	0.2601
Kuwait	0.9955	0.4023	2.5254	0.8120	1.5430	0.2870
Rwanda	0.6253	0.1496	0.8551	0.1906	1.5978	0.2989
Algeria	0.6489	0.1656	1.4068	0.3959	0.8383	0.1344
Trinidad and Tobago	0.8009	0.2694	1.7112	0.5091	1.4541	0.2678
Burkina Faso	0.6354	0.1564	0.6244	0.1048	0.7937	0.1248
Ethiopia	0.6027	0.1341	0.8962	0.2059	0.6918	0.1027
Cameroon	0.6432	0.1618	0.7658	0.1574	0.5930	0.0813
Bolivia	0.6672	0.1781	0.9683	0.2327	0.8385	0.1345
Nicaragua	0.6461	0.1637	1.5629	0.4539	0.5932	0.0814
Botswana	0.6943	0.1966	0.9202	0.2149	2.2729	0.4451
Nepal	0.7121	0.2088	0.8125	0.1748	0.9489	0.1584
Namibia	0.6757	0.1839	0.7508	0.1519	1.8111	0.3451
Bosnia and Herzegovina	0.6890	0.1930	1.6485	0.4858	0.8528	0.1376
Jordan	0.6797	0.1867	1.3577	0.3776	1.4187	0.2601
Malawi	0.6157	0.1430	0.9050	0.2092	1.0042	0.1704
Vanuatu	0.6612	0.1741	1.1921	0.3160	1.5842	0.2960
Tanzania	0.6452	0.1631	0.9376	0.2214	1.0610	0.1827
Guatemala	0.6763	0.1843	1.3855	0.3880	0.7022	0.1050
El Salvador	0.6716	0.1811	1.4736	0.4207	1.0211	0.1740
Cambodia	0.6424	0.1612	1.5179	0.4372	0.7996	0.1261
Honduras	0.6545	0.1695	1.2951	0.3543	0.7373	0.1126
Suriname	0.6269	0.1506	1.4721	0.4202	1.1351	0.1987
Papua New Guinea	0.6549	0.1698	0.8273	0.1803	0.8817	0.1438
Chad	0.6230	0.1480	0.4112	0.0255	0.4151	0.0428
Sudan	0.4937	0.0596	0.8148	0.1757	0.3606	0.0310
Liberia	0.6313	0.1537	0.7779	0.1619	0.6948	0.1034
Mali	0.6336	0.1552	0.6556	0.1164	0.4914	0.0593
Senegal	0.6404	0.1598	0.9450	0.2241	1.3971	0.2554
Iran, Islamic Rep.	0.6240	0.1486	1.2875	0.3515	0.5566	0.0734

Країна	Інтегральний індикатор економічних детермінант		Інтегральний індикатор соціальних детермінант		Інтегральний індикатор політичних детермінант	
	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований	Розра-хований	Норма-лізований
Barbados	0.8266	0.2870	2.0008	0.6169	2.6354	0.5236
Lao PDR	0.6329	0.1547	1.0011	0.2449	0.8693	0.1412
Belize	0.7057	0.2044	1.4263	0.4031	1.2896	0.2322
Mongolia	0.6653	0.1768	1.2839	0.3502	1.2561	0.2249
Somalia	0.6325	0.1544	0.3426	0.0000	0.2174	0.0000
Zimbabwe	0.4063	0.0000	0.7253	0.1424	0.5396	0.0698
Mauritania	0.6581	0.1719	0.7919	0.1671	0.8363	0.1340
Madagascar	0.6353	0.1564	0.8977	0.2065	0.7350	0.1121
Fiji	0.6818	0.1881	1.3047	0.3579	1.9993	0.3858
Gambia, The	0.6332	0.1549	0.7713	0.1595	1.1116	0.1936
Samoa	0.6663	0.1775	1.3721	0.3830	2.3830	0.4689
Tajikistan	0.6398	0.1594	1.2946	0.3541	0.5729	0.0770
Libya	0.6703	0.1802	1.1982	0.3183	0.3079	0.0196
Guyana	0.7901	0.2620	1.0966	0.2805	1.2696	0.2278
Angola	0.6528	0.1683	0.8187	0.1771	0.7392	0.1130
Mozambique	0.6335	0.1551	0.6934	0.1305	0.7109	0.1069
Burundi	0.6256	0.1497	0.7594	0.1550	0.4633	0.0532
Haiti	0.6081	0.1378	0.7722	0.1598	0.3228	0.0228
Sierra Leone	0.6145	0.1422	0.6066	0.0982	0.8461	0.1361
Iraq	0.6555	0.1702	1.1619	0.3048	0.3905	0.0375
Congo, Dem. Rep.	0.6230	0.1480	0.6495	0.1142	0.3325	0.0249
Solomon Islands	0.6505	0.1667	1.3324	0.3682	1.2521	0.2240
Togo	0.6422	0.1610	0.7406	0.1481	0.8631	0.1398

Додаток Л

Оцінка якості результатів кластерного аналізу за методом карт Кохонена

Рисунок Л.1 – Оцінка помилки квантування при формуванні кластерів

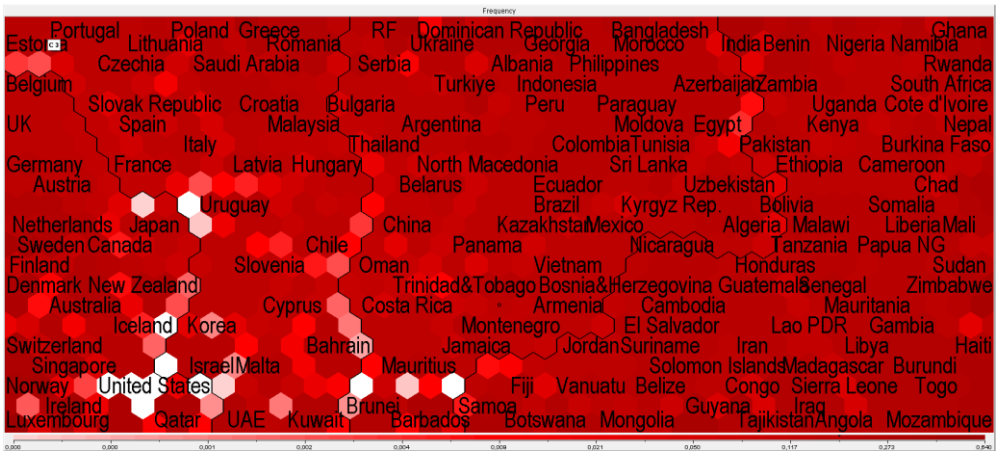


Рисунок Л.2 – Оцінка частоти спостережень, які формують відповідний кластер

Рисунок Л.3 – Оцінка розмірності самоорганізованих карт при формуванні кластерів

Додаток М

Таблиця М.1 – Результати розрахунку інтегрального показника збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант

Country	Index	Country	Index	Country	Index	Country	Index
Switzerland	1	Saudi Arabia	0.371182	Montenegro	0.1638	Pakistan	0.074182
Luxembourg	0.991784	Malaysia	0.358102	Bangladesh	0.156462	Senegal	0.073867
Norway	0.966013	Bahrain	0.356273	Lao PDR	0.055391	Tanzania	0.071547
Denmark	0.926427	Romania	0.347824	Azerbaijan	0.154212	Malawi	0.068557
Singapore	0.917157	Brunei Dar.	0.347469	Vietnam	0.154086	Nigeria	0.065857
Ireland	0.899675	Chile	0.337662	India	0.151586	Ethiopia	0.063568
Sweden	0.822565	Hungary	0.336218	Egypt	0.147034	Solomon Is.	0.060823
Finland	0.806781	Kuwait	0.298243	Armenia	0.144639	Iran	0.060633
Germany	0.805943	Bulgaria	0.284578	Sri Lanka	0.143122	Cameroon	0.056641
Netherlands	0.791682	Serbia	0.270419	Mexico	0.139594	Burkina Faso	0.056463
Australia	0.733454	Costa Rica	0.263744	Botswana	0.133586	Papua N. G.	0.055092
Iceland	0.731852	Mauritius	0.257203	Jordan	0.125618	Tajikistan	0.046959
Canada	0.719714	Oman	0.250507	Ghana	0.121105	Gambia, The	0.039529
Austria	0.719582	Thailand	0.248167	Bosnia & H	0.120217	Liberia	0.039255
UK	0.715203	rf	0.244576	Samoa	0.120137	Madagascar	0.038893
Belgium	0.707194	Dominican R.	0.240353	Vanuatu	0.115679	Mauritania	0.038849
United States	0.669159	Georgia	0.232971	Benin	0.113898	Libya	0.036051
Qatar	0.645082	Barbados	0.232238	Fiji	0.113175	Iraq	0.02919
Japan	0.631254	Argentina	0.224298	Kyrgyz Rep	0.110818	Angola	0.028102
New Zealand	0.625936	China	0.219024	Zambia	0.109756	Mali	0.026379
Estonia	0.611683	N. Macedonia	0.216632	Algeria	0.109375	Mozambique	0.019323
France	0.594313	Panama	0.21291	Uzbekistan	0.108115	Sudan	0.018834
Portugal	0.549057	Albania	0.212212	El Salvador	0.106262	Togo	0.018485
Spain	0.535806	Ukraine	0.205239	South Afr.	0.105429	Sierra Leone	0.01525
Czechia	0.535682	Peru	0.194862	Belize	0.105193	Burundi	0.012565
Korea, Rep.	0.525325	Belarus	0.192817	Rwanda	0.100569	Chad	0.012284
Lithuania	0.503612	Indonesia	0.191447	Nicaragua	0.099627	Haiti	0.007588
Israel	0.493542	Morocco	0.190244	Suriname	0.099455	Zimbabwe	0.004827
Slovenia	0.471463	Jamaica	0.189329	Namibia	0.097656	Somalia	0.000608
UAE	0.44814	Kazakhstan	0.185914	Uganda	0.097373	Congo, D.R.	0
Italy	0.446836	Trinidad & To	0.184795	Kenya	0.09509		
Cyprus	0.432333	Philippines	0.183355	Cambodia	0.09277		
Malta	0.417497	Brazil	0.183176	Cote d'Ivoire	0.091729		
Poland	0.400122	Colombia	0.182317	Mongolia	0.089858		
Slovak Rep.	0.397648	Paraguay	0.181353	Guatemala	0.087865		
Latvia	0.39536	Ecuador	0.176862	Bolivia	0.079132		
Uruguay	0.386228	Turkiye	0.174617	Guyana	0.07757		
Croatia	0.383608	Moldova	0.173847	Honduras	0.076465		
Greece	0.375818	Tunisia	0.167112	Nepal	0.074216		

Додаток Н

Результати фронтірного аналізу

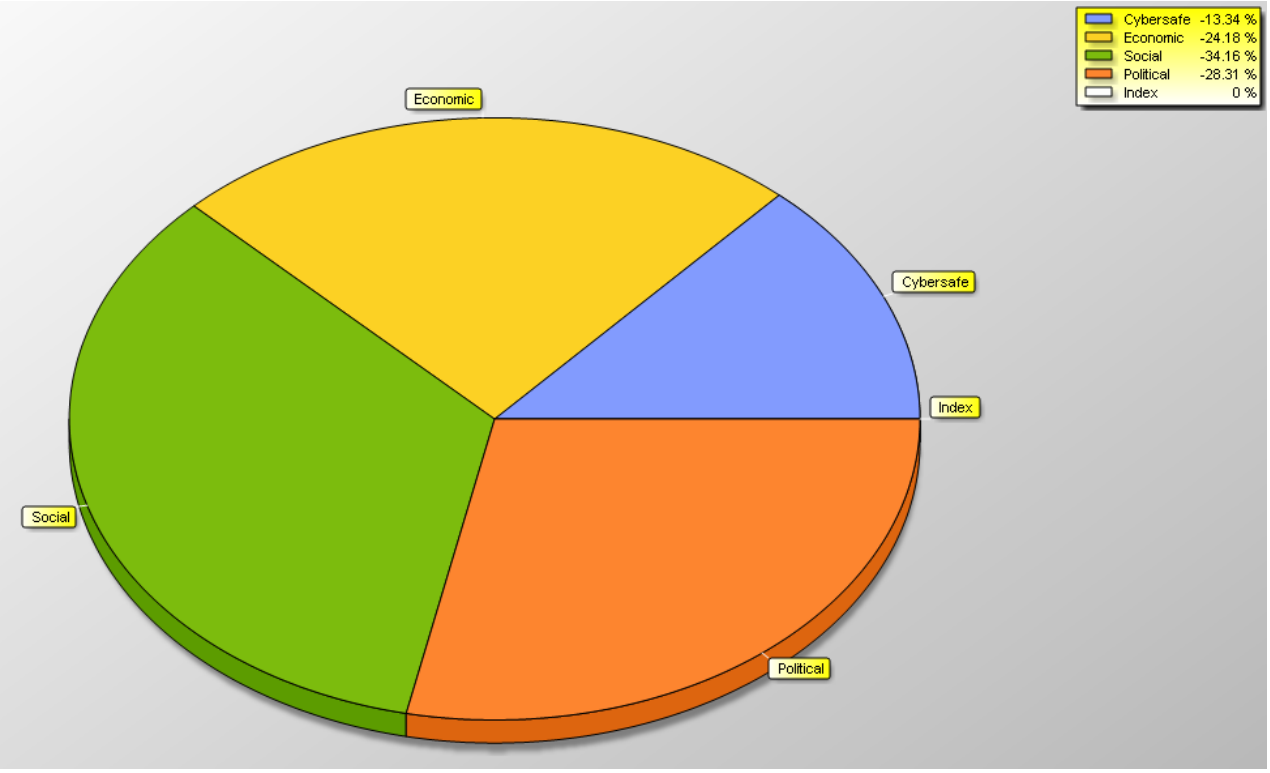


Рисунок Н.1 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Input-oriented CCRмоделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Belgium	100.0%	✓	
Denmark	100.0%	✓	
Ireland	100.0%	✓	
Japan	100.0%	✓	
Luxembourg	100.0%	✓	
New Zealand	97.1%		
Norway	100.0%	✓	
Qatar	100.0%	✓	
Singapore	100.0%	✓	
Switzerland	100.0%	✓	
United Kingdom	99.8%		
United States	99.8%		

Рисунок Н.2 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Input-oriented CCRмоделлю)

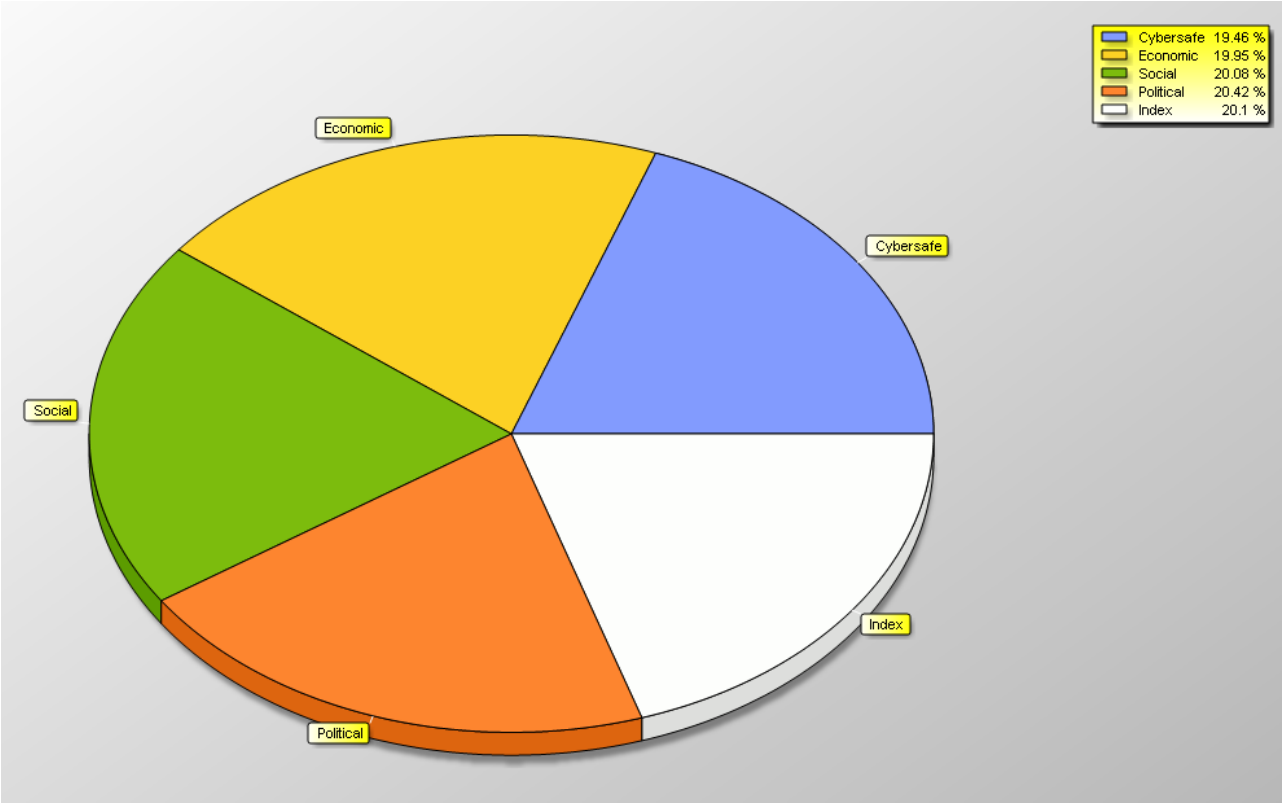


Рисунок Н.3 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Input-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Belgium	100.0%	✓	
Denmark	100.0%	✓	
Ireland	100.0%	✓	
Japan	100.0%	✓	
Luxembourg	100.0%	✓	
New Zealand	100.0%	✓	
Norway	100.0%	✓	
Qatar	100.0%	✓	
Singapore	100.0%	✓	
Switzerland	100.0%	✓	
United Kingdom	100.0%	✓	
United States	100.0%	✓	

Рисунок Н.4 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Input-oriented BCC моделлю)

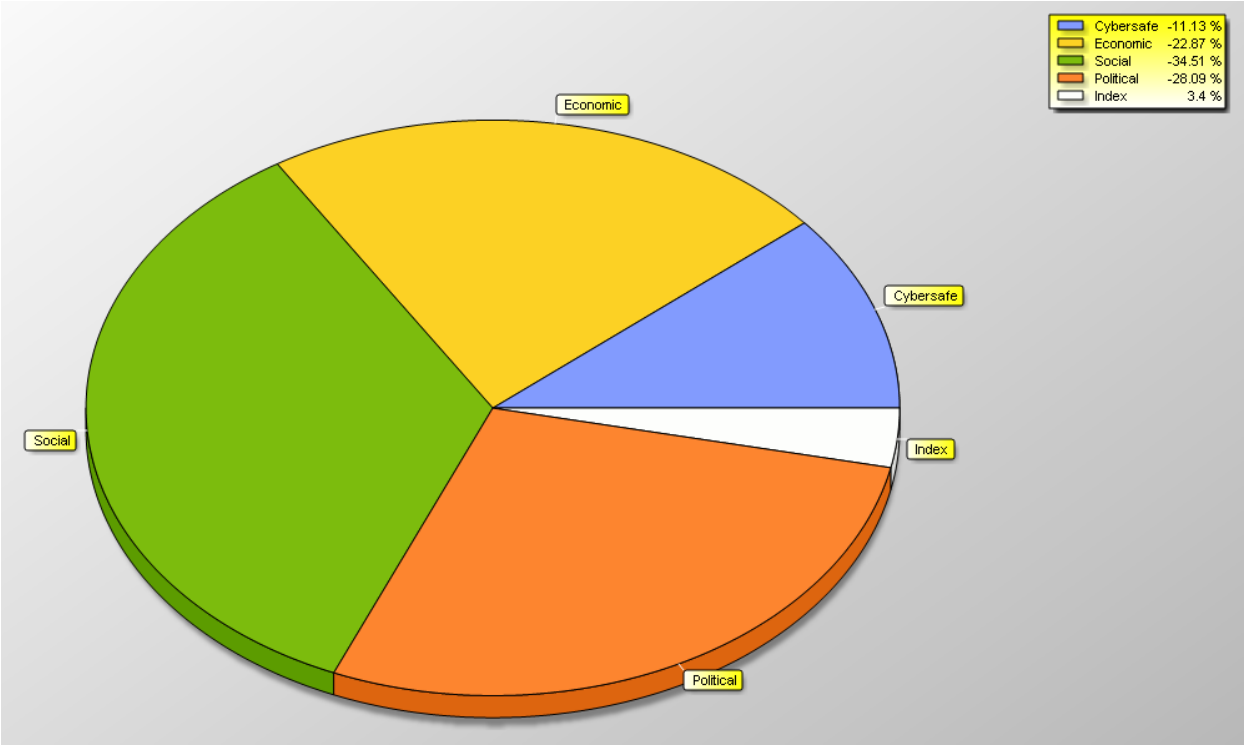


Рисунок Н.5 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Output-oriented CCR моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Belgium	100.0%	✓	
Denmark	100.0%	✓	
Ireland	100.0%	✓	
Japan	100.0%	✓	
Luxembourg	100.0%	✓	
New Zealand	97.1%		
Norway	100.0%	✓	
Qatar	100.0%	✓	
Singapore	100.0%	✓	
Switzerland	100.0%	✓	
United Kingdom	99.8%		
United States	99.8%		

Рисунок Н. 6 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Output-oriented CCR моделлю)

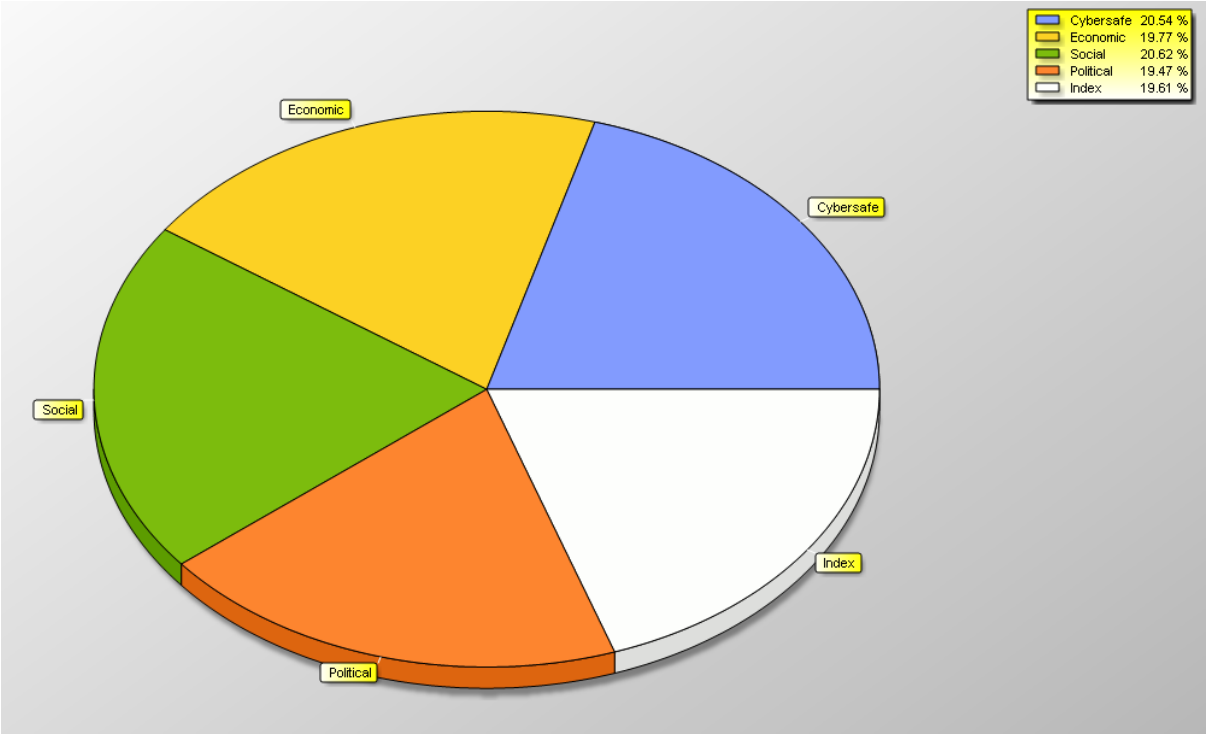


Рисунок Н.7 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Output-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Belgium	100.0%	✓	
Denmark	100.0%	✓	
Ireland	100.0%	✓	
Japan	100.0%	✓	
Luxembourg	100.0%	✓	
New Zealand	100.0%	✓	
Norway	100.0%	✓	
Qatar	100.0%	✓	
Singapore	100.0%	✓	
Switzerland	100.0%	✓	
United Kingdom	100.0%	✓	
United States	100.0%	✓	

Рисунок Н.8 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 4-го кластеру (за Output-oriented BCC моделлю)

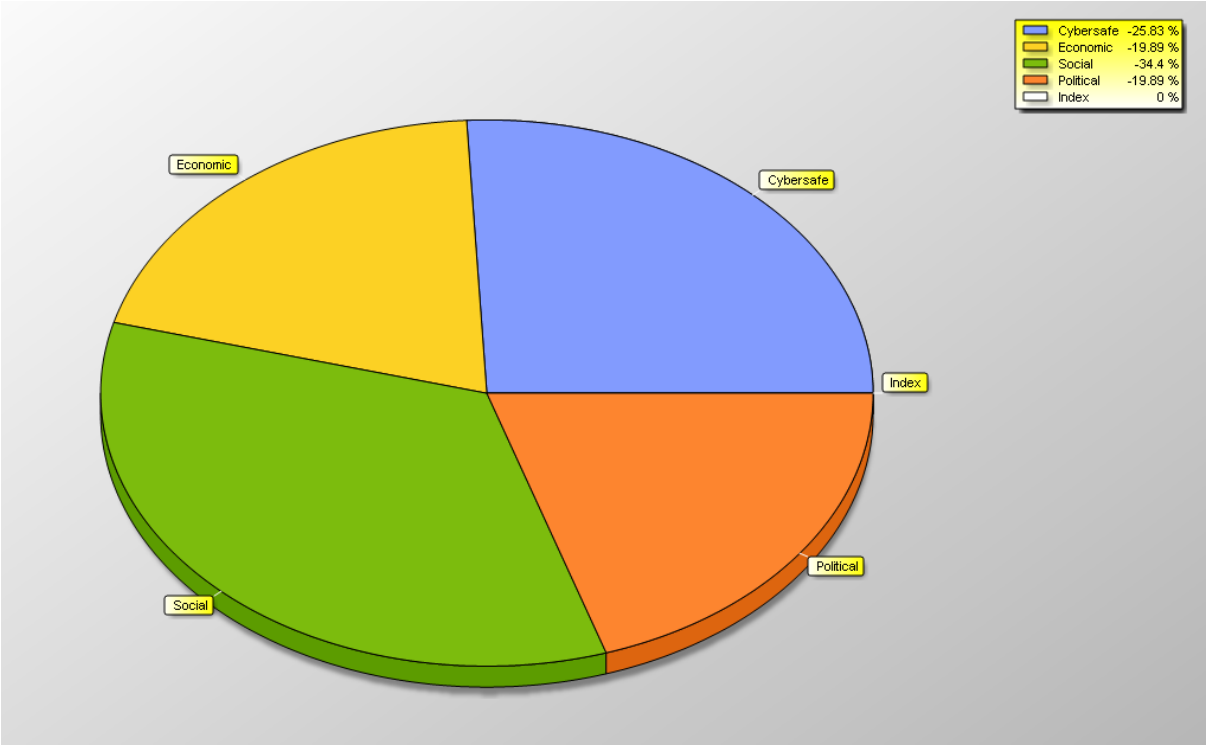


Рисунок Н.9 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Input-oriented CCRмоделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bahrain	100.0%	✓	
Chile	81.1%		
Czechia	99.5%		
Estonia	100.0%	✓	
France	100.0%	✓	
Hungary	88.5%		
Korea, Rep.	100.0%	✓	
Kuwait	100.0%	✓	
Malaysia	92.2%		
Portugal	100.0%	✓	
Romania	100.0%	✓	
Spain	100.0%	✓	

Рисунок Н.10 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Input-oriented CCRмоделлю)

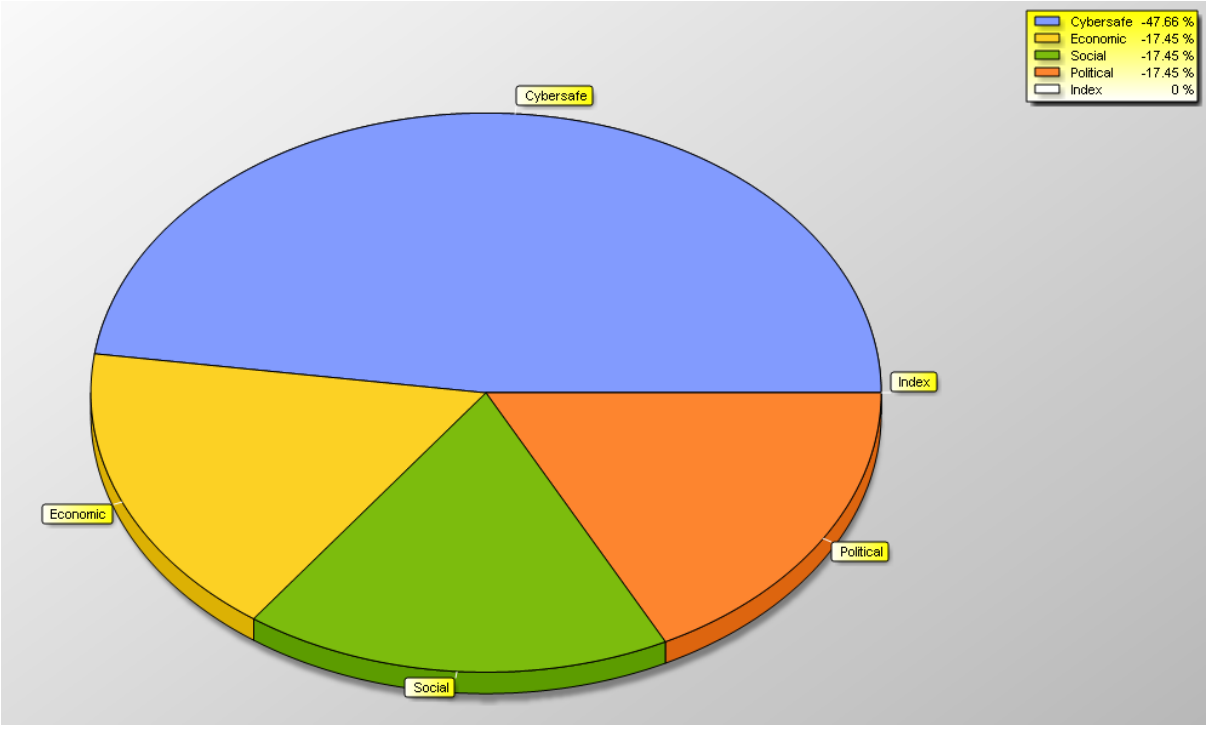


Рисунок Н.11 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Input-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bahrain	100.0%	✓	
Chile	100.0%	✓	
Czechia	99.8%		
Estonia	100.0%	✓	
France	100.0%	✓	
Hungary	100.0%	✓	
Korea, Rep.	100.0%	✓	
Kuwait	100.0%	✓	
Malaysia	100.0%	✓	
Portugal	100.0%	✓	
Romania	100.0%	✓	
Spain	100.0%	✓	

Рисунок Н.12 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Input-oriented BCC моделлю)

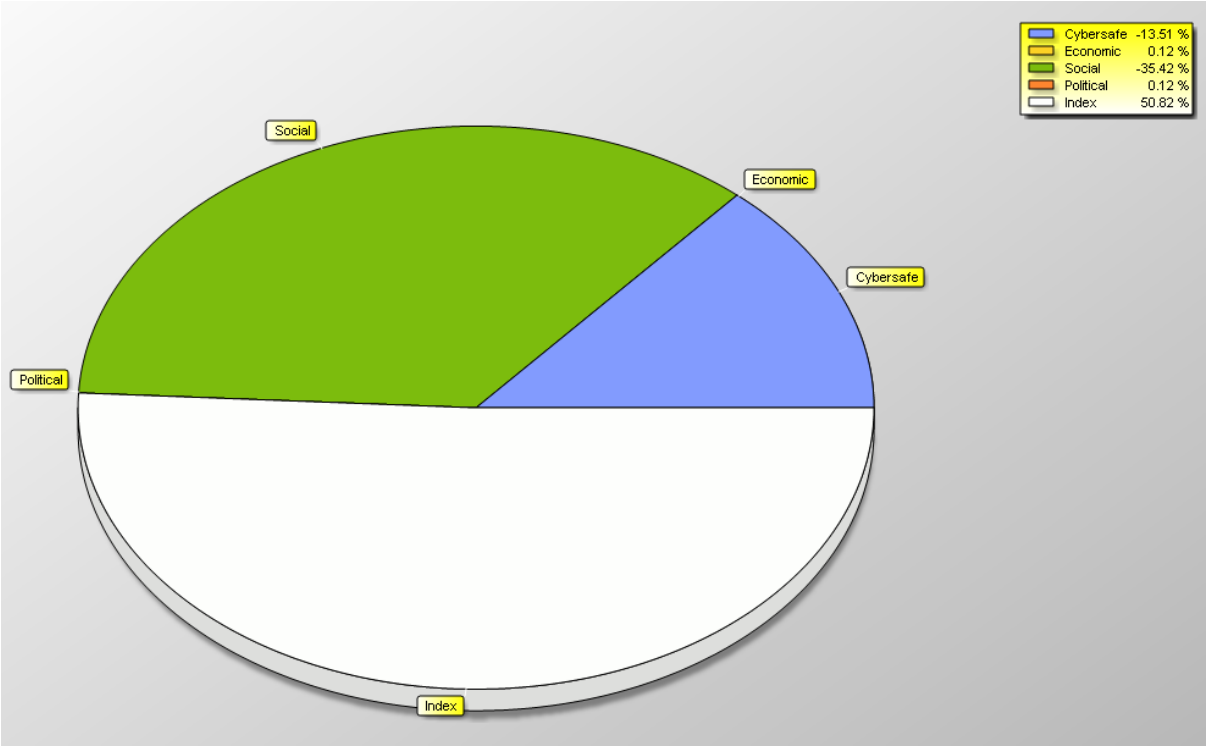


Рисунок Н.13 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Output-oriented CCR моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bahrain	100.0%	✓	
Chile	81.1%		
Czechia	99.5%		
Estonia	100.0%	✓	
France	100.0%	✓	
Hungary	88.5%		
Korea, Rep.	100.0%	✓	
Kuwait	100.0%	✓	
Malaysia	92.2%		
Portugal	100.0%	✓	
Romania	100.0%	✓	
Spain	100.0%	✓	

Рисунок Н.14 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Output-oriented CCR моделлю)

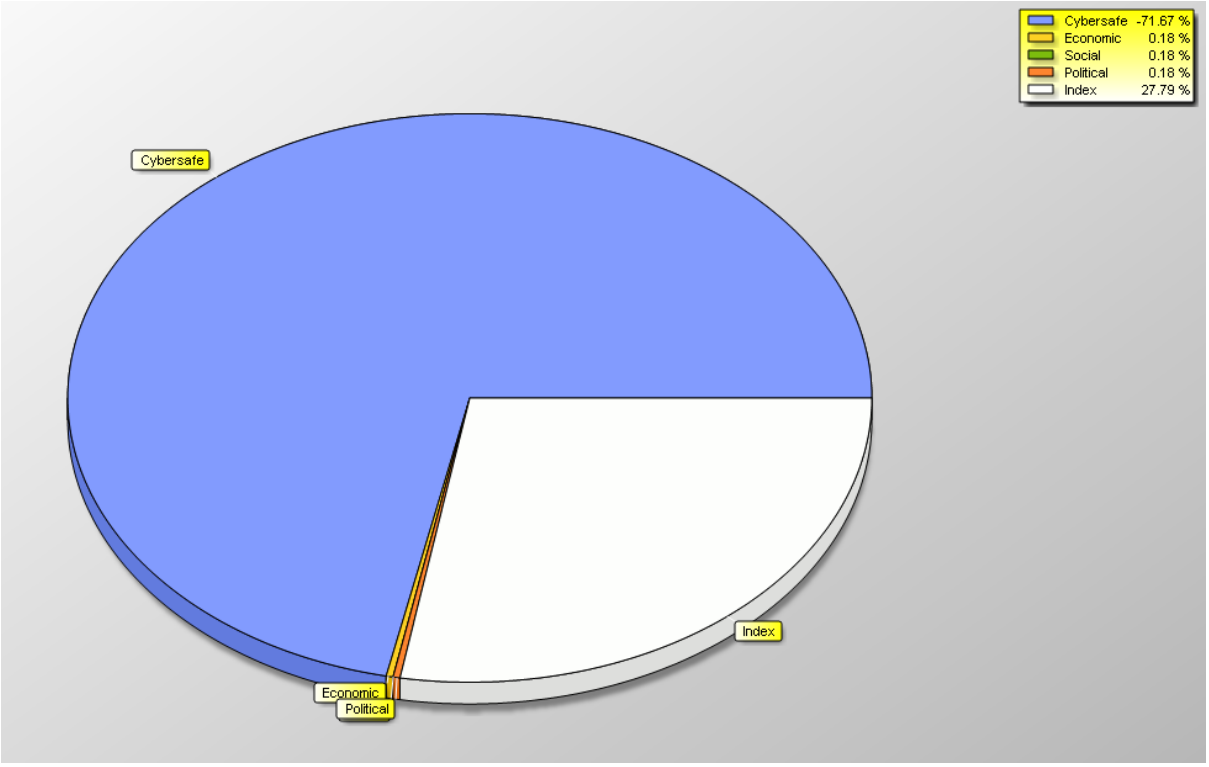


Рисунок Н.15 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Output-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bahrain	100.0%	✓	
Chile	100.0%	✓	
Czechia	99.8%		
Estonia	100.0%	✓	
France	100.0%	✓	
Hungary	100.0%	✓	
Korea, Rep.	100.0%	✓	
Kuwait	100.0%	✓	
Malaysia	100.0%	✓	
Portugal	100.0%	✓	
Romania	100.0%	✓	
Spain	100.0%	✓	

Рисунок Н.16 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 3-го кластеру (за Output-oriented BCC моделлю)

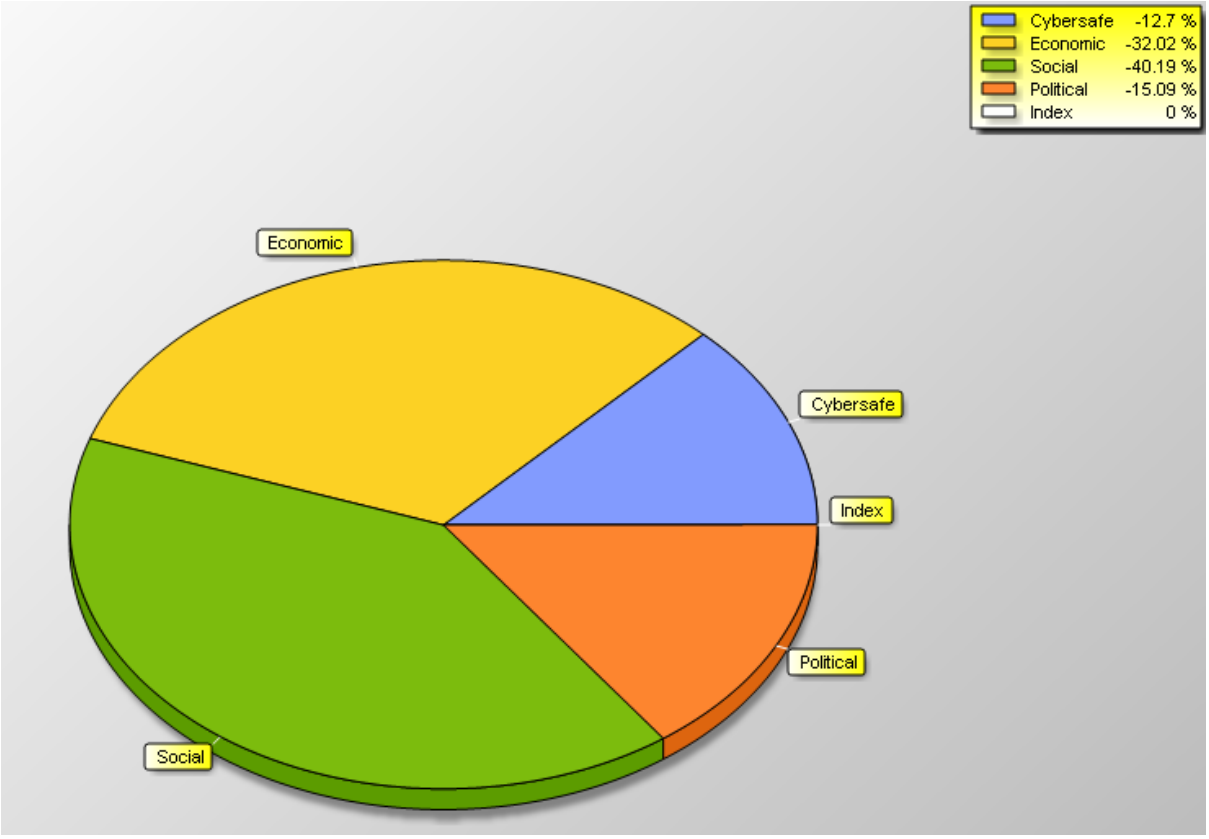


Рисунок Н.17 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Input-oriented CCRмоделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Algeria	82.0%		
Armenia	83.5%		
Brunei Darussalam	100.0%	✓	
Bulgaria	100.0%	✓	
Costa Rica	98.1%		
Kyrgyz Republic	90.6%		
Mauritius	100.0%	✓	
Mexico	94.7%		
Serbia	100.0%	✓	
Sri Lanka	93.0%		
Ukraine	100.0%	✓	
Uzbekistan	74.9%		

Рисунок Н.18 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Input-oriented CCRмоделлю)

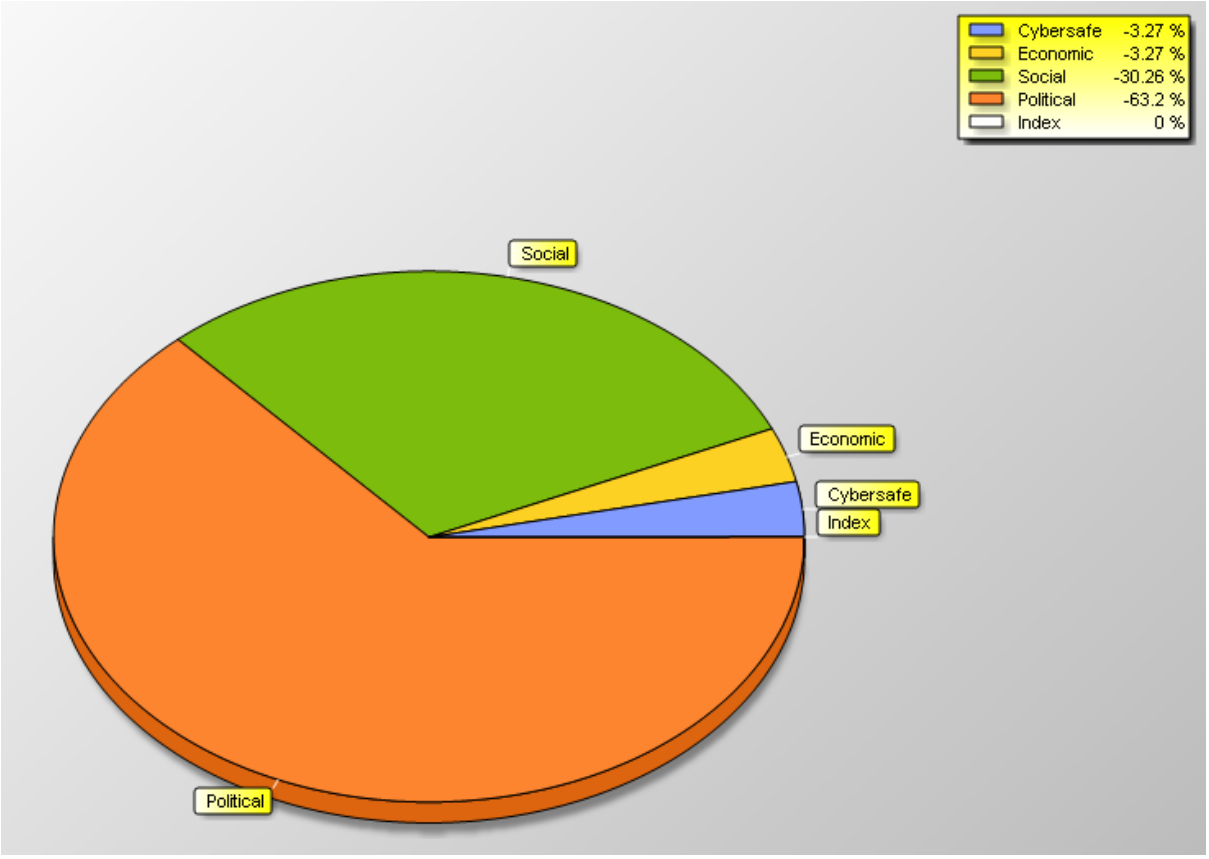


Рисунок Н.19 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Input-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Algeria	100.0%	✓	
Armenia	99.9%		
Brunei Darussalam	100.0%	✓	
Bulgaria	100.0%	✓	
Costa Rica	99.7%		
Kyrgyz Republic	100.0%	✓	
Mauritius	100.0%	✓	
Mexico	100.0%	✓	
Serbia	100.0%	✓	
Sri Lanka	100.0%	✓	
Ukraine	100.0%	✓	
Uzbekistan	100.0%	✓	

Рисунок Н.20 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Input-oriented BCC моделлю)

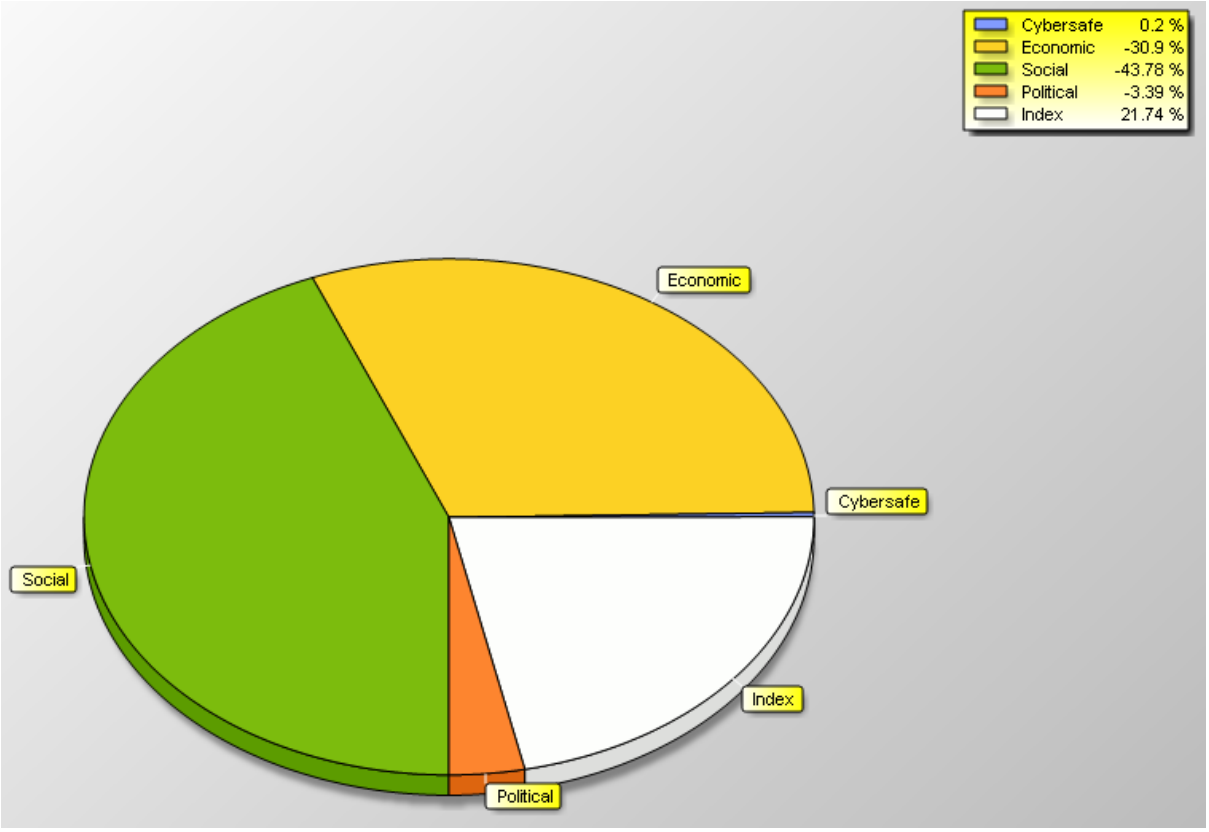


Рисунок Н.21 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Output-oriented CCR моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Algeria	82.0%		
Armenia	83.5%		
Brunei Darussalam	100.0%	✓	
Bulgaria	100.0%	✓	
Costa Rica	98.1%		
Kyrgyz Republic	90.6%		
Mauritius	100.0%	✓	
Mexico	94.7%		
Serbia	100.0%	✓	
Sri Lanka	93.0%		
Ukraine	100.0%	✓	
Uzbekistan	74.9%		

Рисунок Н.22 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Output-oriented CCR моделлю)

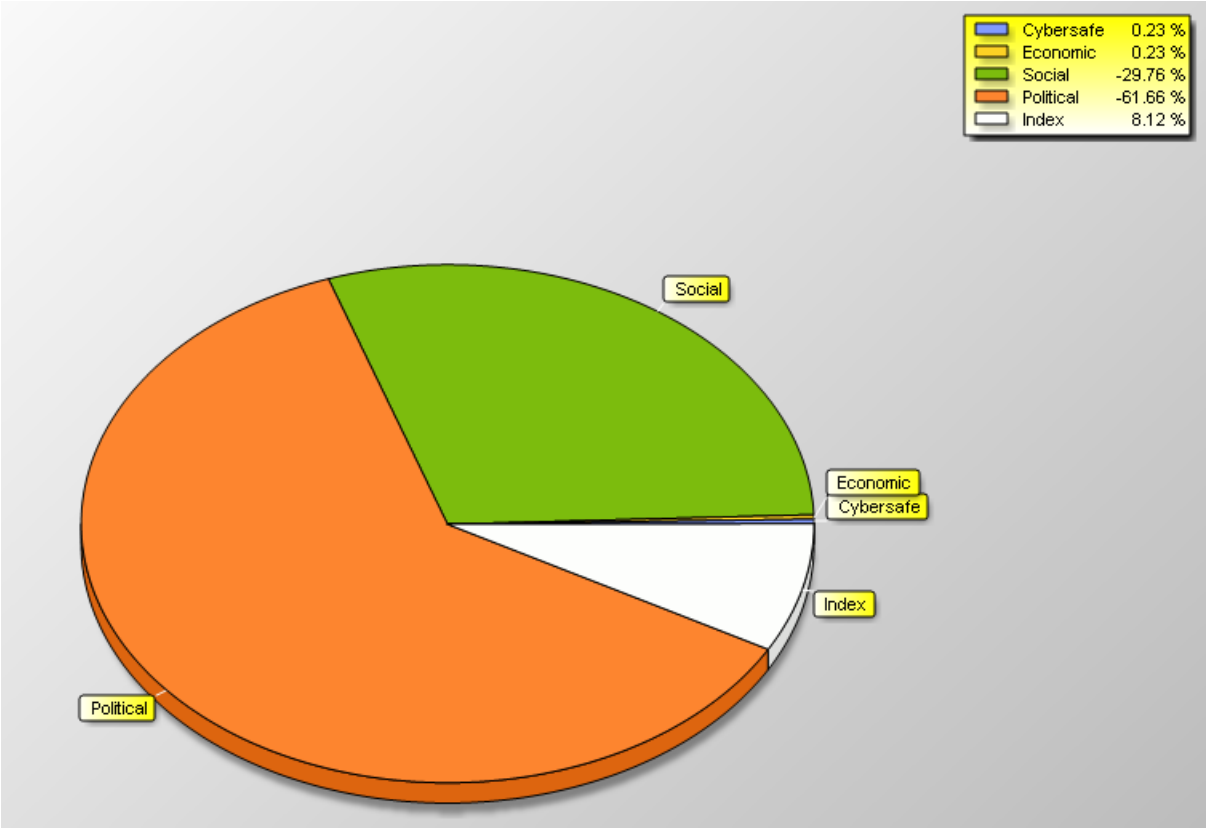


Рисунок Н.23 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Output-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Algeria	100.0%	✓	
Armenia	99.5%		
Brunei Darussalam	100.0%	✓	
Bulgaria	100.0%	✓	
Costa Rica	99.6%		
Kyrgyz Republic	100.0%	✓	
Mauritius	100.0%	✓	
Mexico	100.0%	✓	
Serbia	100.0%	✓	
Sri Lanka	100.0%	✓	
Ukraine	100.0%	✓	
Uzbekistan	100.0%	✓	

Рисунок Н.24 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 2-го кластеру (за Output-oriented BCC моделлю)

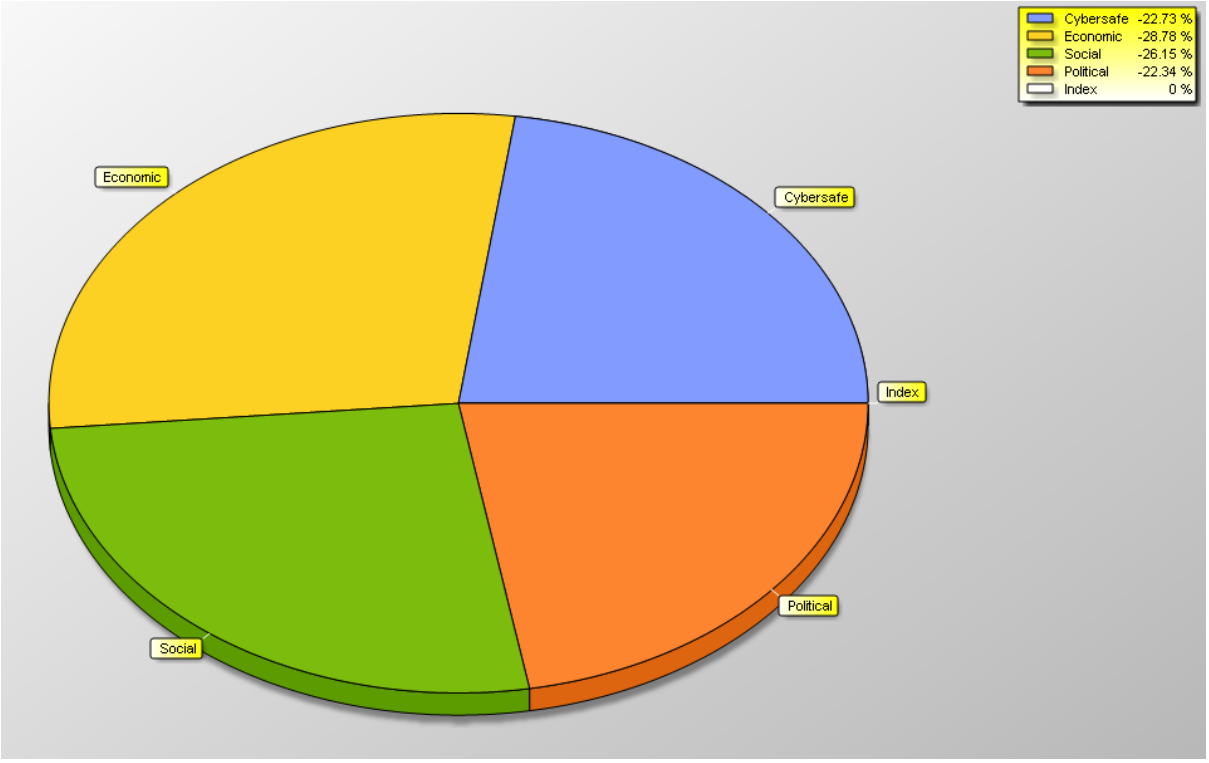


Рисунок Н.25 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Input-oriented CCRмоделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bosnia and Herzegovina	100.0%	✓	
Botswana	100.0%	✓	
Burundi	49.3%		
Chad	77.3%		
Congo, Dem. Rep.	1.0%		
Ghana	100.0%	✓	
Haiti	39.4%		
Jordan	100.0%	✓	
Samoa	100.0%	✓	
Somalia	100.0%	✓	
Vanuatu	97.0%		
Zimbabwe	100.0%	✓	

Рисунок Н.26 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Input-oriented CCRмоделлю)

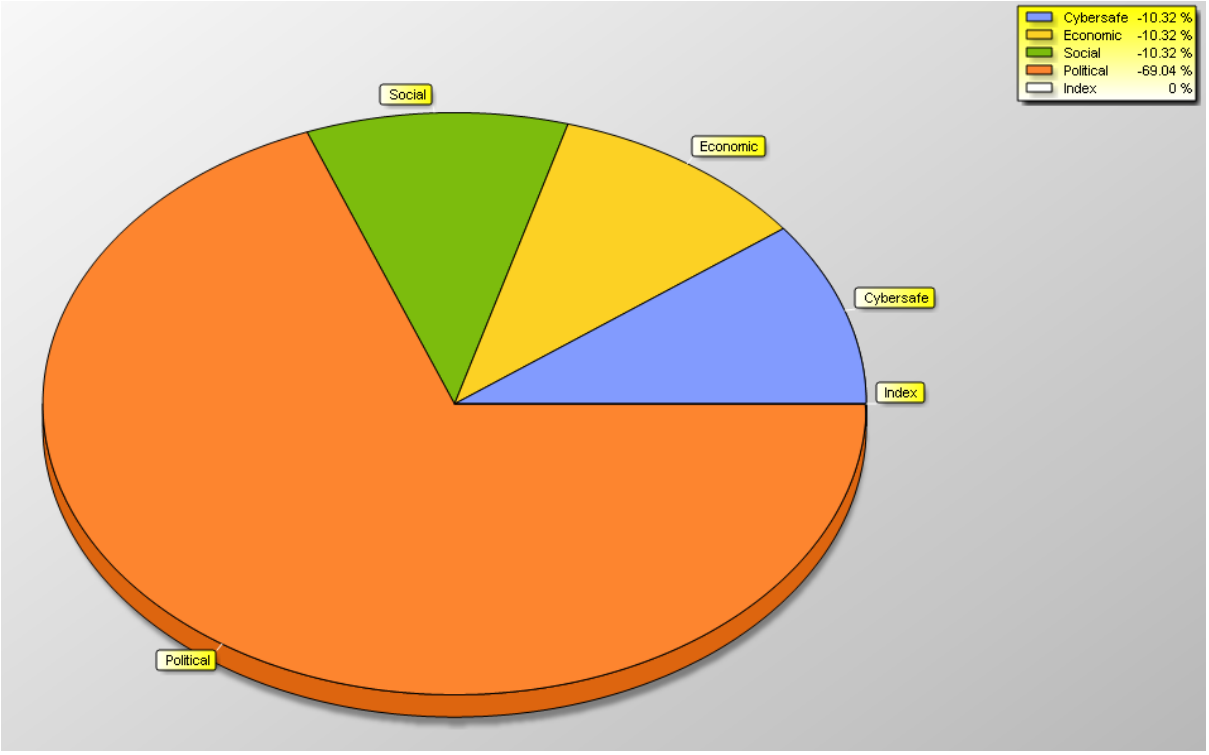


Рисунок Н.27 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Input-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bosnia and Herzegovina	100.0%	✓	
Botswana	100.0%	✓	
Burundi	95.6%		
Chad	99.6%		
Congo, Dem. Rep.	100.0%	✓	
Ghana	100.0%	✓	
Haiti	100.0%	✓	
Jordan	100.0%	✓	
Samoa	100.0%	✓	
Somalia	100.0%	✓	
Vanuatu	99.1%		
Zimbabwe	100.0%	✓	

Рисунок Н.28 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Input-oriented BCC моделлю)

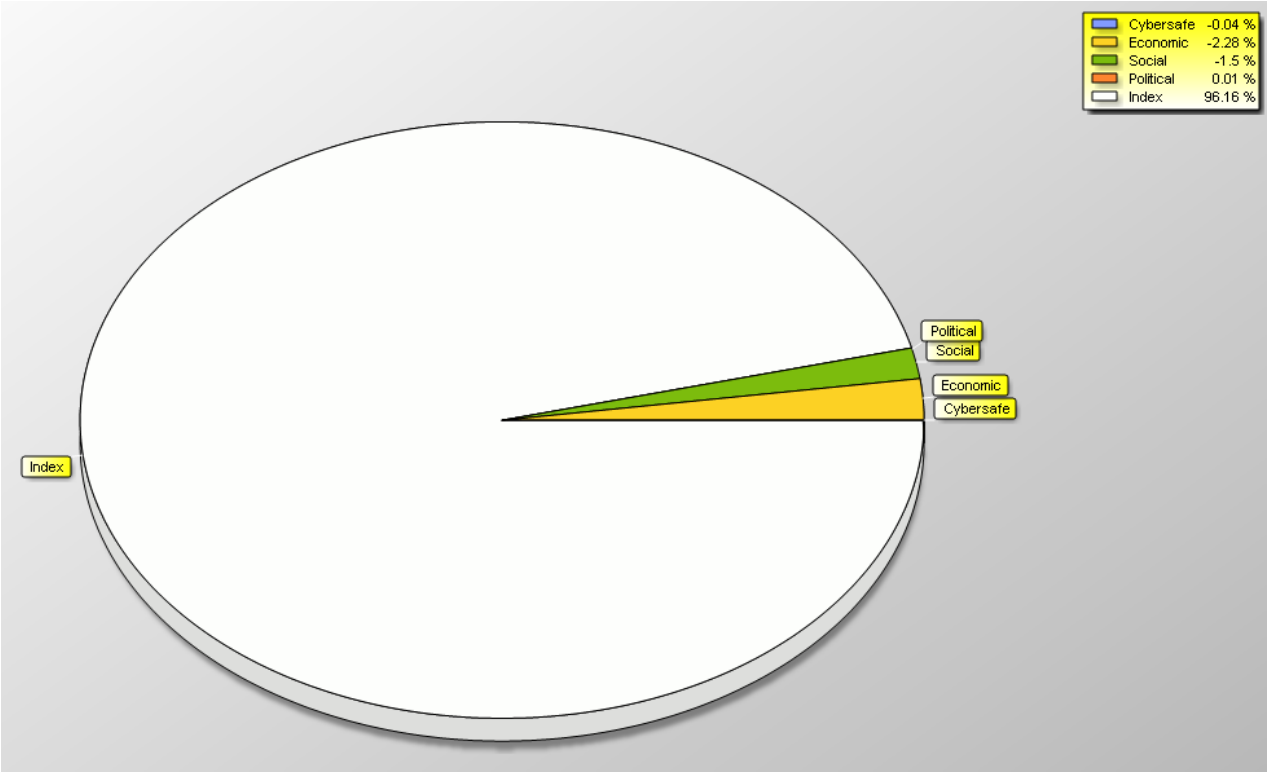


Рисунок Н.29 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Output-oriented CCR моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bosnia and Herzegovina	100.0%	✓	
Botswana	100.0%	✓	
Burundi	49.3%		
Chad	77.3%		
Congo, Dem. Rep.	1.0%		
Ghana	100.0%	✓	
Haiti	39.4%		
Jordan	100.0%	✓	
Samoa	100.0%	✓	
Somalia	100.0%	✓	
Vanuatu	97.0%		
Zimbabwe	100.0%	✓	

Рисунок Н.30 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Output-oriented CCR моделлю)

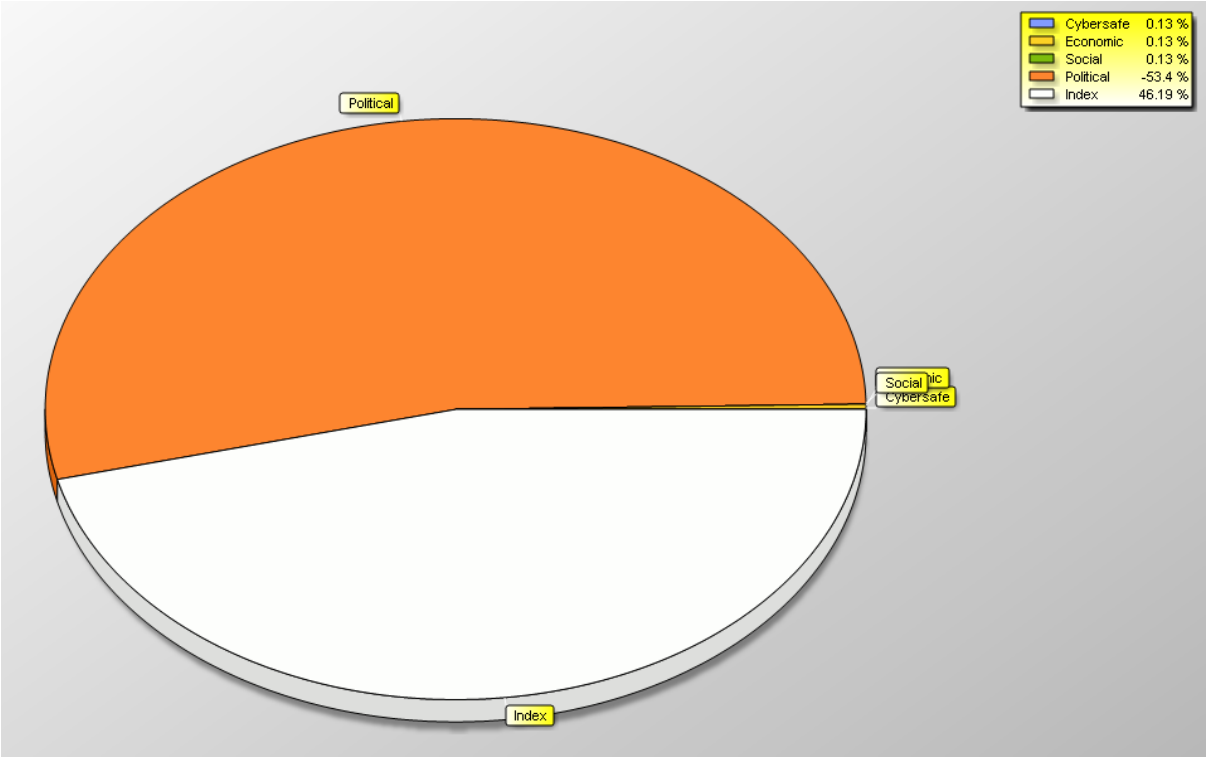


Рисунок Н.31 – Результати ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Output-oriented BCC моделлю)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bosnia and Herzegovina	100.0%	✓	
Botswana	100.0%	✓	
Burundi	82.0%		
Chad	97.1%		
Congo, Dem. Rep.	100.0%	✓	
Ghana	100.0%	✓	
Haiti	100.0%	✓	
Jordan	100.0%	✓	
Samoa	100.0%	✓	
Somalia	100.0%	✓	
Vanuatu	98.7%		
Zimbabwe	100.0%	✓	

Рисунок Н.32 – Результати оцінок загальної ефективності збалансованої взаємодії соціальних, економічних, політичних та кібербезпекових детермінант країн 1-го кластеру (за Output-oriented BCC моделлю)